

AWS Certified Cloud Practitioner

Por Stéphane Maarek y Joan Amengual



CURSO



EXÁMENES PRÁCTICOS



Advertencia: Estas diapositivas están protegidas por derechos de autor y son estrictamente para uso personal

- Este documento está reservado a las personas inscritas en el curso [AWS Certified Cloud Practitioner](#)
- **Por favor, no compartas este documento**, está destinado únicamente a uso personal y a la preparación del examen, gracias.
- Si has obtenido estas diapositivas de forma gratuita en un sitio web que no es el del curso, por favor, ponte en contacto con joan@blockstellart.com. ¡Gracias!
- **¡Mucha suerte para el examen y feliz aprendizaje!**

Tabla de contenidos

- [¿Qué es Cloud Computing?](#)
- [AWS Identity & Access Management](#)
- [Amazon EC2](#)
- [Almacenamiento de instancias de Amazon EC2](#)
- [Elastic Load Balancing y Auto Scaling Group](#)
- [Amazon S3](#)
- [Bases de datos y análisis](#)
- [Otros servicios informáticos](#)
- [Despliegue y administración de infraestructura a escala](#)
- [Infraestructura global](#)
- [Integración en el Cloud](#)

Tabla de contenidos

- [Monitorización del Cloud](#)
- [Amazon VPC](#)
- [Seguridad y normativa](#)
- [Machine Learning](#)
- [Gestión de cuentas, facturación y soporte](#)
- [Identidad avanzada](#)
- [Otros servicios de AWS](#)
- [Arquitectura y ecosistema de AWS](#)
- [Preparación del examen](#)
- [Enhorabuena](#)

Curso AWS Certified Cloud Practitioner

Bienvenidos. Empezamos en 5 minutos



- Vamos a preparar el examen **AWS Certified Cloud Practitioner**
- Es una certificación exigente, por lo que este curso será largo e interesante
- Los conocimientos básicos de IT son útiles, pero lo explicaré todo

- Cubriremos más de **50 servicios de AWS** (de los más de 200 de AWS)
- ¡Los principiantes de AWS / IT son bienvenidos! (pero tómate tu tiempo, no es una carrera)
- **Aprender haciendo - ¡técnica clave de aprendizaje!**
Este curso combina la teoría y la práctica

Ejemplo de pregunta: Cloud Practitioner

¿Qué servicio de AWS simplificaría la migración de una base de datos a AWS?

- A) AWS Storage Gateway <= lo aprenderemos
 - B) AWS Database Migration Service <= respuesta correcta
 - C) Amazon EC2 <= lo aprenderemos
 - D) Amazon AppStream 2.0 <= distractor (más de 200 servicios en AWS)
-
- https://dl.awsstatic.com/es_ES/training-and-certification/docs-cloud-practitioner/AWS-Certified-Cloud-Practitioner_Sample-Questions.pdf

Sobre nosotros

- **¡Stephane Maarek!**
- Ha trabajado como consultor de IT y arquitecto de soluciones de AWS, desarrollador y SysOps
- Ha trabajado con AWS durante muchos años: ha construido sitios web, aplicaciones, plataformas de streaming
- Instructor veterano en AWS (Certificaciones, CloudFormation, Lambda, EC2...)



Sobre nosotros

- **¡Joan Amengual!**
- Ingeniero Full Stack en una empresa tecnológica en Silicon Valley, USA
- He trabajado con AWS varios años en diversas empresas para la migración y el escalado de servicios en el Cloud
- Premiado como Joven Talento en Ingeniería
- Puedes encontrarme en:
 - LinkedIn: <https://www.linkedin.com/in/joanamengual7>
 - Frecuentemente hago publicaciones interesantes sobre AWS



Tu viaje de certificación de AWS

FOUNDATIONAL

Seis meses de conocimiento básico sobre la nube de AWS y el sector



PROFESSIONAL

Dos años de experiencia en el diseño, la operación y la solución de problemas con la nube de AWS



ASSOCIATE

Un año de experiencia solucionando problemas e implementando soluciones con la nube de AWS



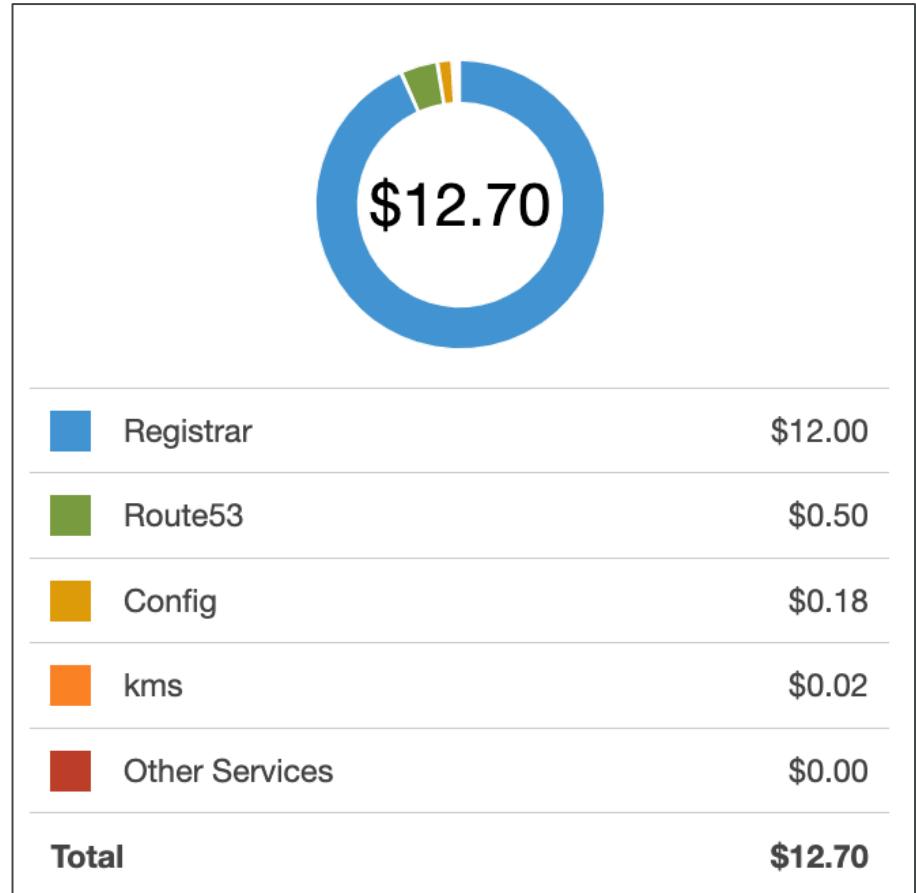
SPECIALTY

Experiencia técnica en la nube de AWS de nivel Specialty según lo especificado en la guía del examen



Coste estimado de este curso

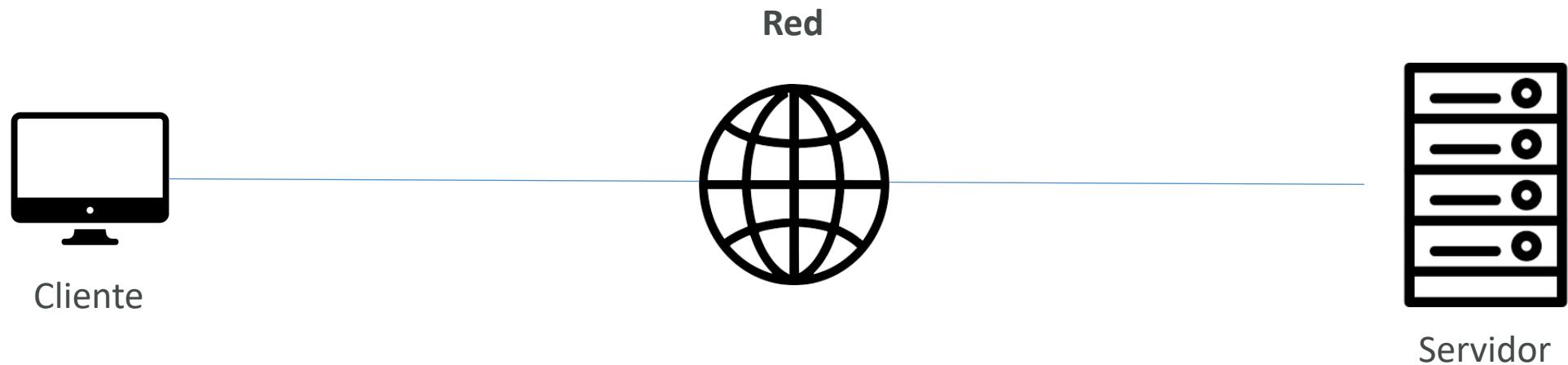
- La mayoría de los servicios que utilizaremos estarán dentro de la capa gratuita de AWS = 0\$
- Si utilizo un servicio que cueste dinero, lo mencionaré en el curso
- Puedes obtener más información sobre la capa gratuita de AWS en:
<https://aws.amazon.com/free/>



Consejos en Udemy

¿Qué es el Cloud Computing?

Cómo funcionan los sitios web



Los clientes tienen direcciones IP

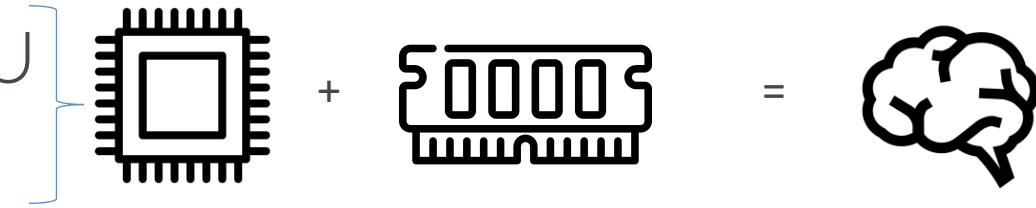
Los servidores tienen direcciones IP

Al igual que cuando se envía el correo postal

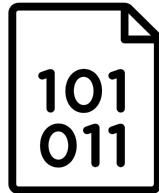


¿De qué se compone un servidor?

- Computación: CPU
- Memoria: RAM



- Almacenamiento: Información



- Base de datos: Almacenar los datos de forma estructurada

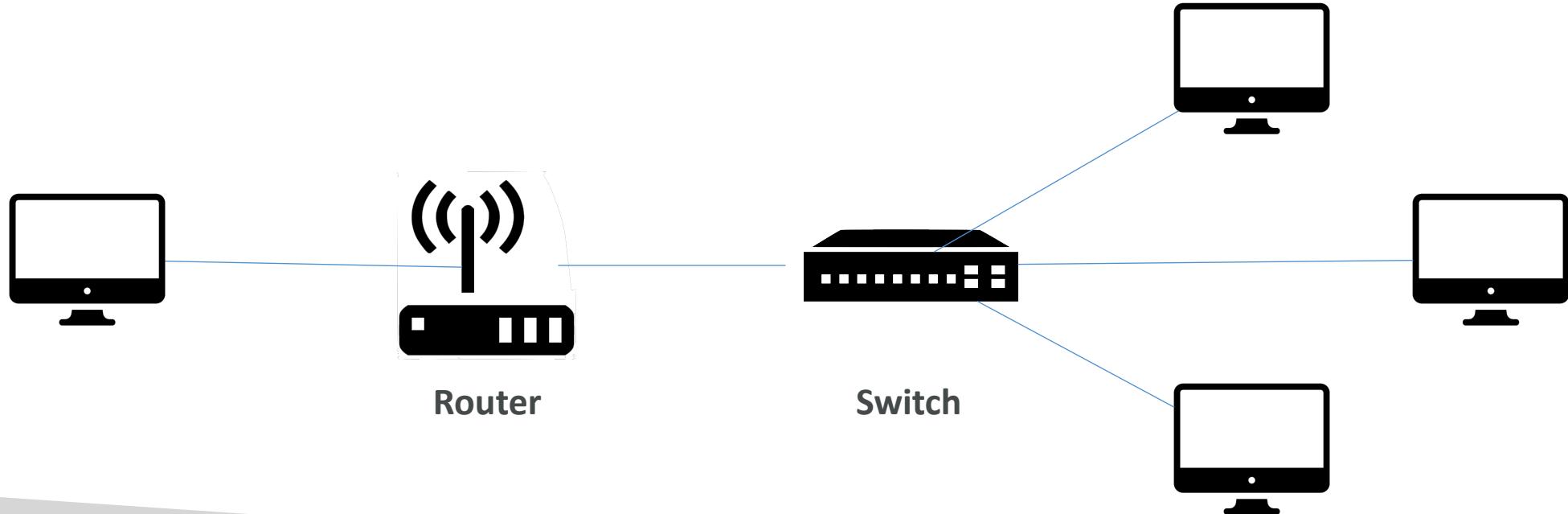


- Red: Routers, switch, servidor DNS

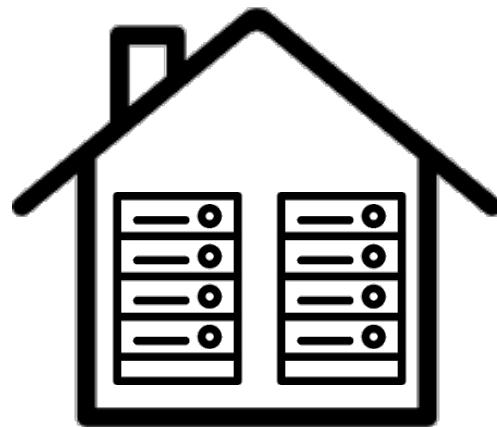


Terminología informática

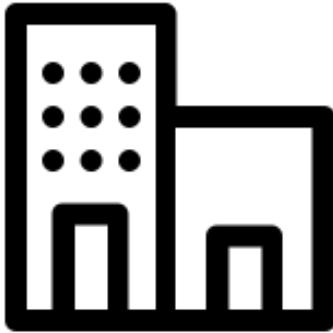
- **Red:** cables, routers y servidores conectados entre sí
- **Router:** Dispositivo de red que reenvía paquetes de datos entre redes de ordenadores. Saben dónde enviar los paquetes en Internet
- **Switch:** Toma un paquete y lo envía al servidor / cliente correcto en tu red



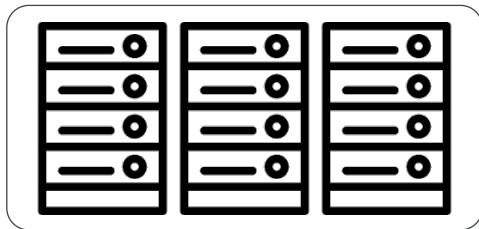
Tradicionalmente, la forma de construir infraestructuras



Casa o garaje



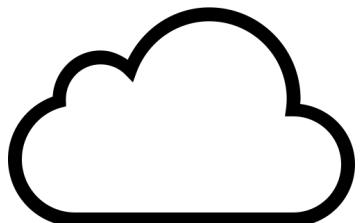
Oficina



Centro de datos

Problemas con el enfoque tradicional de las IT

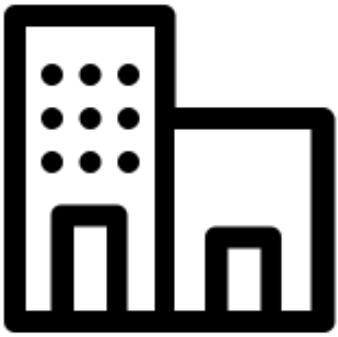
- Pagar el alquiler del centro de datos
- Pagar el suministro eléctrico, la refrigeración y el mantenimiento
- Añadir y sustituir el hardware lleva tiempo
- El escalado es limitado
- Contratar un equipo 24/7 para supervisar la infraestructura
- ¿Cómo hacer frente a las catástrofes? (terremoto, apagón, incendio...)
- ¿Podemos externalizar todo esto?



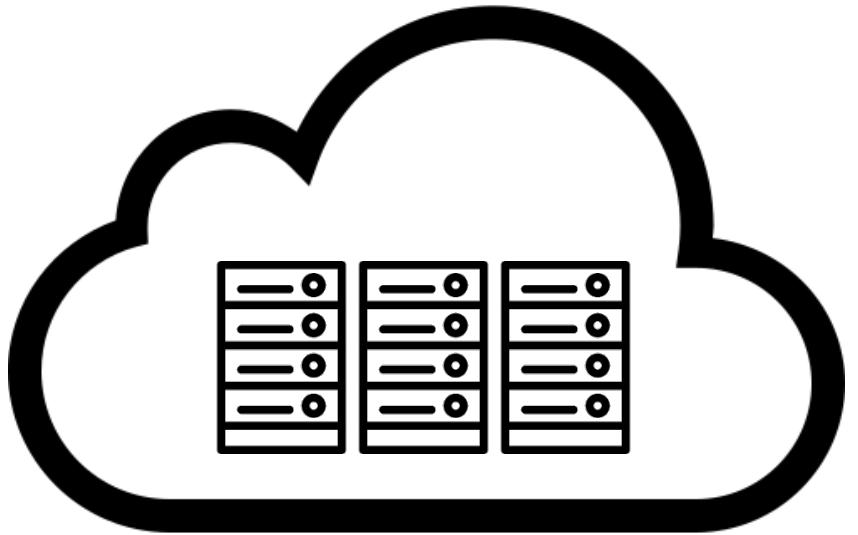
¿Qué es el Cloud Computing?



- El Cloud Computing (Computación en la nube) es el **suministro bajo demanda** de potencia de cálculo, almacenamiento en bases de datos, aplicaciones y otros recursos informáticos
- A través de una plataforma de servicios en el cloud con **precios de pago por uso**
- Puedes **aprovisionar exactamente el tipo y el tamaño** de los recursos informáticos que necesitas
- Puedes acceder a tantos recursos como necesites, **casi al instante**
- Forma sencilla de acceder a **servidores, almacenamiento, bases de datos** y un conjunto de **servicios de aplicaciones**
- Amazon Web Services (AWS) posee y mantiene el hardware conectado a la red necesario para estos servicios de aplicaciones, mientras que aprovisionas y utilizas lo que necesitas a través de una aplicación web.



Oficina



Cloud

¡Has utilizado algunos servicios Cloud!



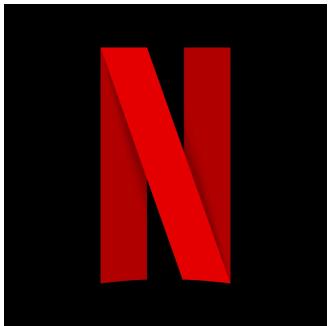
Gmail

- Servicio de correo electrónico en el Cloud
- Paga SOLO por tus correos electrónicos almacenados (sin infraestructura, etc.)



Dropbox

- Servicio de almacenamiento en el Cloud
- Originalmente construido en AWS



Netflix

- Construido en AWS
- Vídeo bajo demanda

Los modelos de despliegue del Cloud

Cloud privado:

- Servicios en el cloud utilizados por una sola organización, no expuestos al público
- Control total
- Seguridad para aplicaciones sensibles
- Satisfacer necesidades empresariales específicas



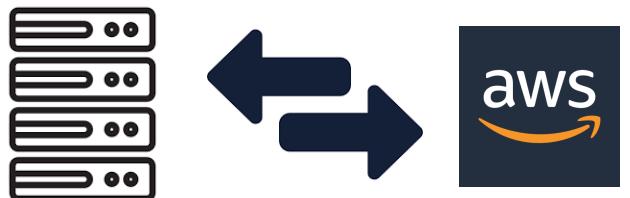
Cloud público:

- Recursos en el cloud que son propiedad de un proveedor de servicios en el cloud y son operados por él, y que se suministran a través de Internet
- Seis ventajas de la computación en el cloud



Cloud híbrido:

- Mantener algunos servidores en las instalaciones y extiende algunas capacidades al cloud
- Control de los activos sensibles en tu infraestructura privada
- Flexibilidad y rentabilidad del cloud público



Las cinco características del Cloud computing

- **Autoservicio bajo demanda (on-demand):**
 - Los usuarios pueden aprovisionar recursos y utilizarlos sin interacción humana del proveedor de servicios
- **Amplio acceso a la red:**
 - Los recursos están disponibles a través de la red, y pueden ser accedidos por diversas plataformas de clientes
- **Alquiler múltiple y agrupación de recursos:**
 - Varios clientes pueden compartir la misma infraestructura y aplicaciones con seguridad y privacidad
 - Múltiples clientes reciben servicio desde los mismos recursos físicos
- **Rápida elasticidad y escalabilidad:**
 - Adquirir y disponer de recursos de forma automática y rápida cuando sea necesario
 - Escala rápida y fácilmente en función de la demanda
- **Servicio medido:**
 - El uso se mide, los usuarios pagan correctamente por lo que han utilizado

Seis ventajas del Cloud computing

- **Cambia el gasto de capital (CAPEX) por el gasto operativo (OPEX)**
 - Pagar bajo demanda: no poseer el hardware
 - Reducción del coste total de propiedad (TCO) y de los gastos operativos (OPEX)
- **Te beneficias de economías de escala masivas**
 - Los precios se reducen ya que AWS es más eficiente debido a la gran escala
- **Deja de adivinar la capacidad**
 - Escala basada en el uso real medido
- **Aumentar la velocidad y la agilidad**
- **Deja de gastar dinero en el funcionamiento y el mantenimiento de los centros de datos**
- **Se global en minutos:** aprovecha la infraestructura global de AWS

Problemas resueltos por el Cloud

- **Flexibilidad:** cambia los tipos de recursos cuando sea necesario
- **Rentabilidad:** paga por lo que utilizas
- **Escalabilidad:** permite acomodar mayores cargas reforzando el hardware o añadiendo nodos adicionales
- **Elasticidad:** capacidad de reducir y aumentar la escala cuando sea necesario
- **Alta disponibilidad y tolerancia a los fallos:** construye a través de los centros de datos (data centers)
- **Agilidad:** desarrollar, testear y lanzar rápidamente aplicaciones de software

Tipos de Cloud Computing

- **Infraestructura como servicio (IaaS)**

- Proporciona bloques de construcción para la IT en el cloud
- Proporciona redes, ordenadores y espacio de almacenamiento de datos
- Máximo nivel de flexibilidad
- Fácil paralelismo con la IT tradicional en las instalaciones

- **Plataforma como servicio (PaaS)**

- Elimina la necesidad de que tu organización gestione la infraestructura subyacente
- Se centra en el despliegue y la gestión de tus aplicaciones

- **Software como servicio (SaaS)**

- Producto completo que es ejecutado y gestionado por el proveedor de servicios

En las instalaciones

- Aplicaciones
- Datos
- Tiempo de ejecución
- Middleware
- O/S
- Virtualización
- Servidores
- Almacenamiento
- Networking

Infraestructura como servicio (IaaS)

- Aplicaciones
- Datos
- Tiempo de ejecución
- Middleware
- O/S
- Virtualización
- Servidores
- Almacenamiento
- Networking

Plataforma como servicio (PaaS)

- Aplicaciones
- Datos
- Tiempo de ejecución
- Middleware
- O/S
- Virtualización
- Servidores
- Almacenamiento
- Networking

Software como servicio (SaaS)

- Aplicaciones
- Datos
- Tiempo de ejecución
- Middleware
- O/S
- Virtualización
- Servidores
- Almacenamiento
- Networking

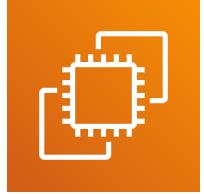
Gestionado por ti

Gestionado por otros

Ejemplo de tipos de Cloud Computing

- **Infraestructura como servicio:**

- Amazon EC2 (en AWS)
- GCP, Azure, Rackspace, Digital Ocean, Linode



- **Plataforma como servicio:**

- Elastic Beanstalk (en AWS)
- Heroku, Google App Engine (GCP), Windows Azure (Microsoft)



- **Software como servicio:**

- Muchos servicios de AWS (por ejemplo, Rekognition para el aprendizaje automático)
- Google Apps (Gmail), Dropbox, Zoom

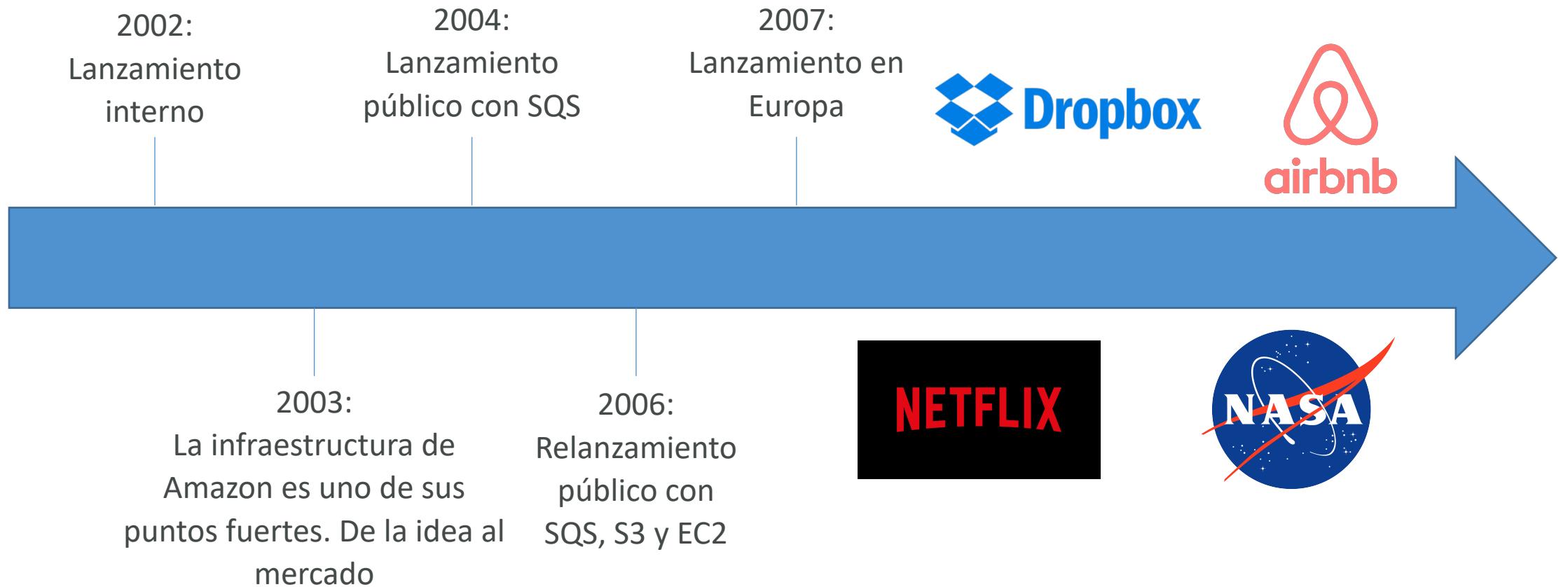


Precios del Cloud - Visión general rápida

- AWS tiene 3 fundamentos de precios, siguiendo el modelo de precios de pago por uso
- **Computación:**
 - Pagar por el tiempo de computación
- **Almacenamiento:**
 - Paga por los datos almacenados en el Cloud
- **Transferencia de datos FUERA del Cloud:**
 - La transferencia de datos hacia adentro es gratuita
 - Resuelve el costoso problema de las IT tradicionales



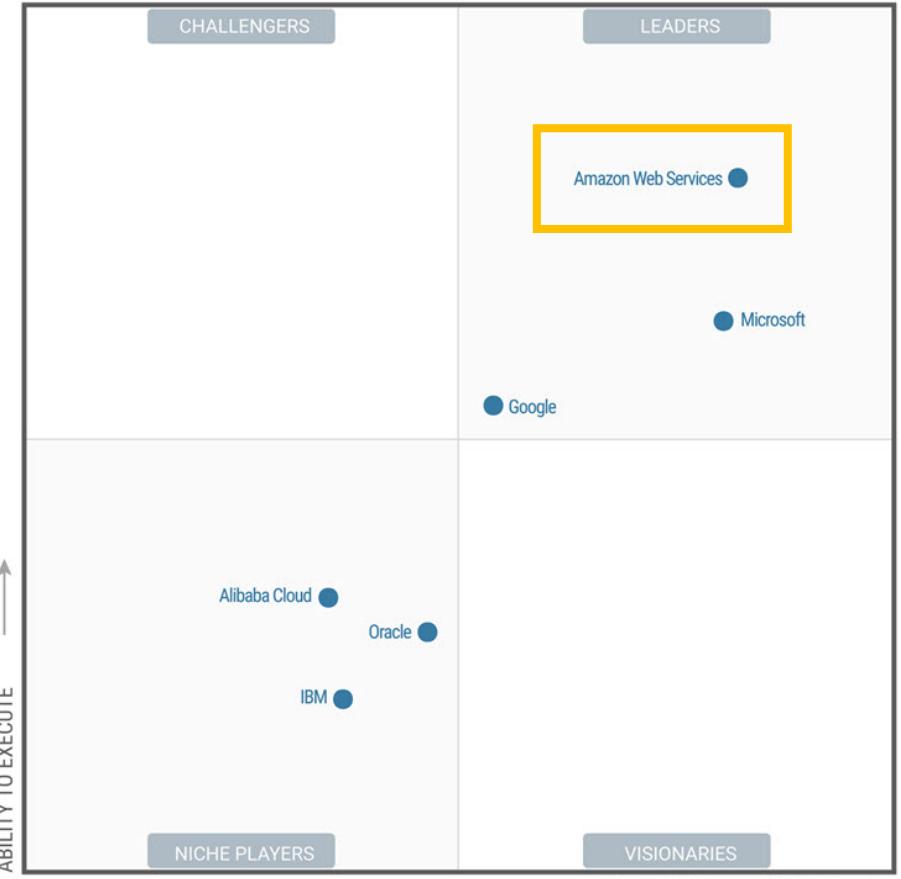
Historia del Cloud de AWS



Números de AWS

- En 2019, AWS tuvo 35.020 millones de dólares de ingresos anuales
- AWS representa el 47% del mercado en 2019 (Microsoft es el segundo con el 22%)
- Pionero y líder del mercado de Cloud por noveno año consecutivo
- Más de 1.000.000 de usuarios activos

Figure 1. Magic Quadrant for Cloud Infrastructure as a Service, Worldwide



Cuadrante mágico de Gartner

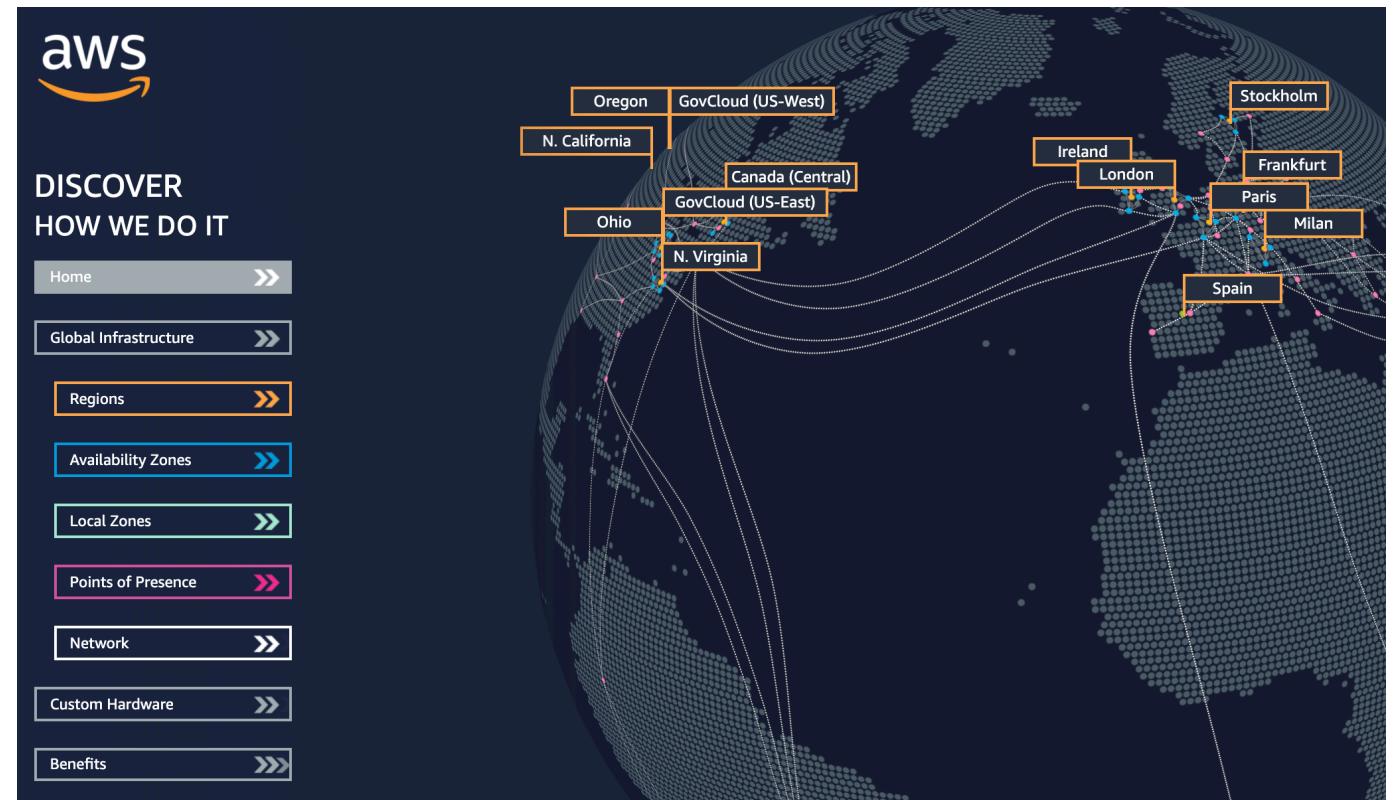
Casos de uso del Cloud de AWS

- AWS permite crear aplicaciones sofisticadas y escalables
- Aplicable a un conjunto diverso de industrias
- Los casos de uso incluyen
 - IT para empresas, copias de seguridad y almacenamiento, análisis de Big Data
 - Alojamiento de sitios web, aplicaciones móviles y sociales
 - Juegos



Infraestructura global de AWS

- AWS Regions
- Regiones de AWS
- AWS Availability Zones
- Zonas de disponibilidad de AWS
- AWS Data Centers
- Centros de datos de AWS
- AWS Edge Locations / Points of Presence
- Puntos de presencia de AWS
- <https://infrastructure.aws/>



Regiones de AWS

- AWS tiene **Regiones** en todo el mundo
- Los nombres pueden ser us-east-1, eu-west-3...
- Una región es un **grupo de centros de datos**
- **La mayoría de los servicios de AWS son de ámbito regional**



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

US East (N. Virginia) us-east-1

US East (Ohio) us-east-2

US West (N. California) us-west-1

US West (Oregon) us-west-2

Africa (Cape Town) af-south-1

Asia Pacific (Hong Kong) ap-east-1

Asia Pacific (Mumbai) ap-south-1

Asia Pacific (Seoul) ap-northeast-2

Asia Pacific (Singapore) ap-southeast-1

Asia Pacific (Sydney) ap-southeast-2

Asia Pacific (Tokyo) ap-northeast-1

Canada (Central) ca-central-1

Europe (Frankfurt) eu-central-1

Europe (Ireland) eu-west-1

Europe (London) eu-west-2

Europe (Paris) eu-west-3

Europe (Stockholm) eu-north-1

Middle East (Bahrain) me-south-1

South America (São Paulo) sa-east-1

¿Cómo elegir una región de AWS?

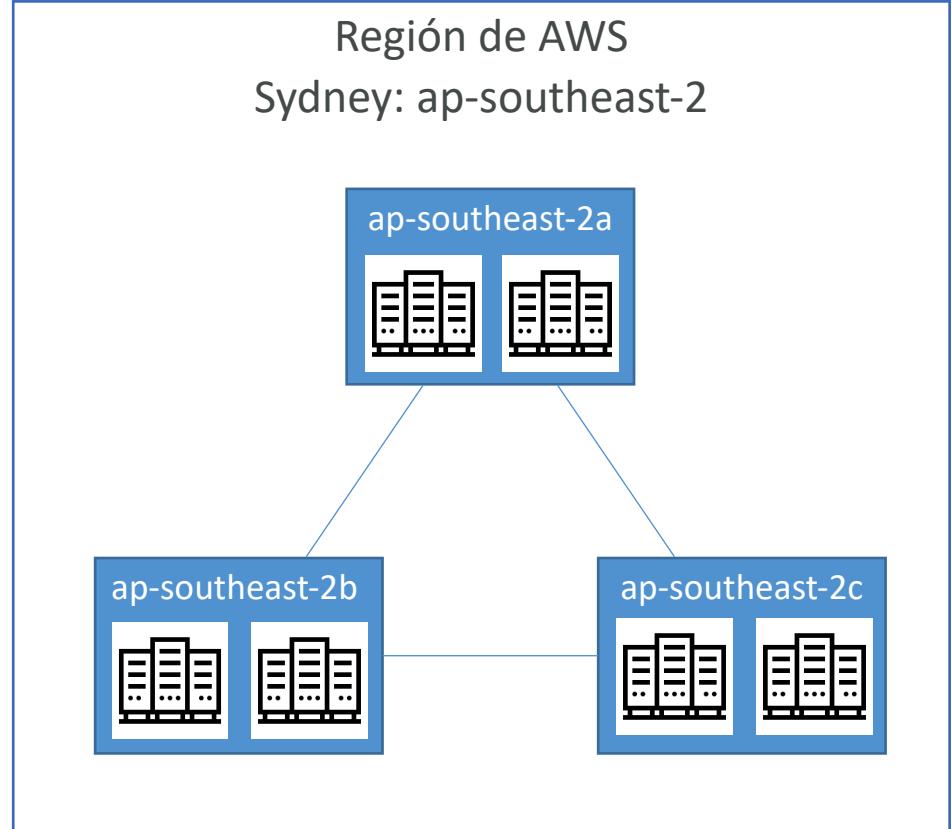
Si necesitas lanzar una nueva aplicación,
¿dónde debes hacerlo?



- **Cumplimiento de los requisitos legales y de gobernanza de datos:** los datos nunca salen de una región sin tu permiso explícito
- **Proximidad a los clientes:** latencia reducida
- **Servicios disponibles en una región:** los nuevos servicios y las nuevas funciones no están disponibles en todas las regiones
- **Precios:** los precios varían de una región a otra y son transparentes en la página de precios del servicio

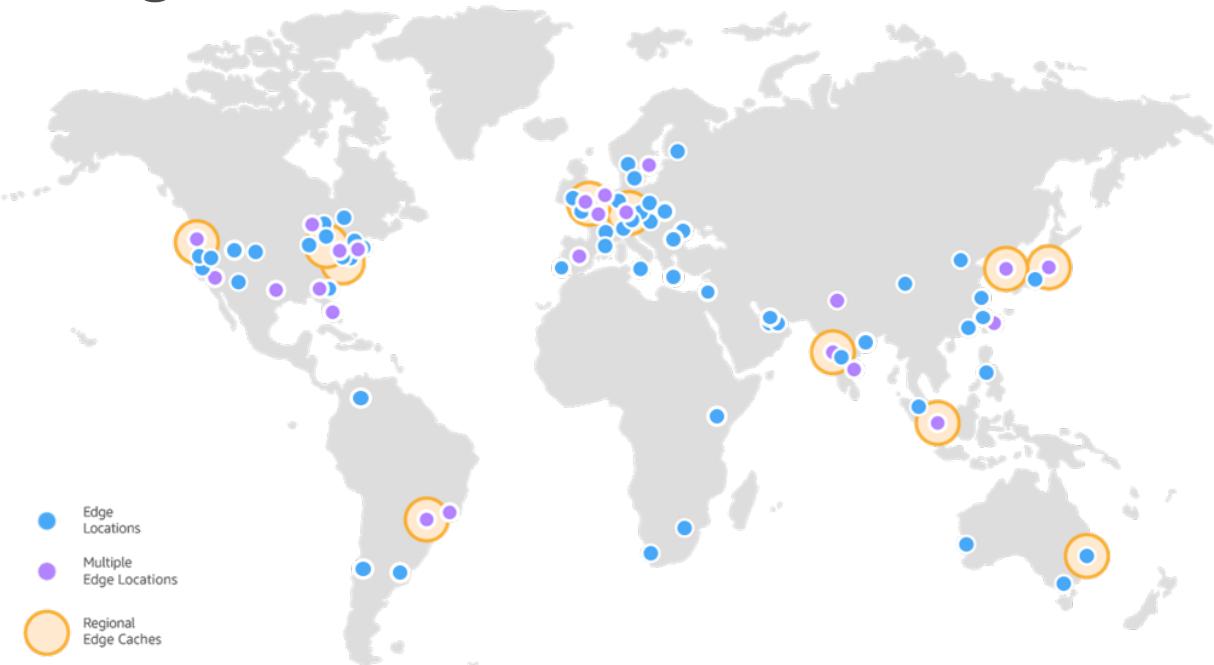
Zonas de disponibilidad de AWS

- Cada región tiene muchas zonas de disponibilidad (normalmente 3, el mínimo es 3, el máximo es 6). Ejemplo:
 - ap-southeast-2a
 - ap-southeast-2b
 - ap-southeast-2c
- Cada zona de disponibilidad (AZ) es uno o varios centros de datos discretos con alimentación, red y conectividad redundantes
- Están separadas unas de otras, de modo que están aisladas de las catástrofes
- Están conectadas con redes de alto ancho de banda y latencia ultrabaja



Puntos de presencia de AWS (Edge Locations)

- Amazon tiene +450 puntos de presencia (+10 cachés regionales) en +90 ciudades de +40 países
- El contenido se entrega a los usuarios finales con menor latencia



<https://aws.amazon.com/cloudfront/features/>

Tour por la consola de AWS



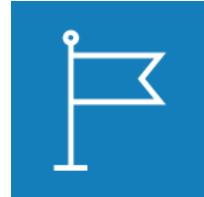
- **AWS cuenta con servicios globales:**

- Identity and Access Management (IAM)
- Route 53 (servicio DNS)
- CloudFront (Red de entrega de contenido)
- WAF (Firewall de aplicaciones web)



- **La mayoría de los servicios de AWS son de ámbito regional:**

- Amazon EC2 (Infraestructura como servicio)
- Elastic Beanstalk (Plataforma como servicio)
- Lambda (Función como servicio)
- Rekognition (Software como servicio)

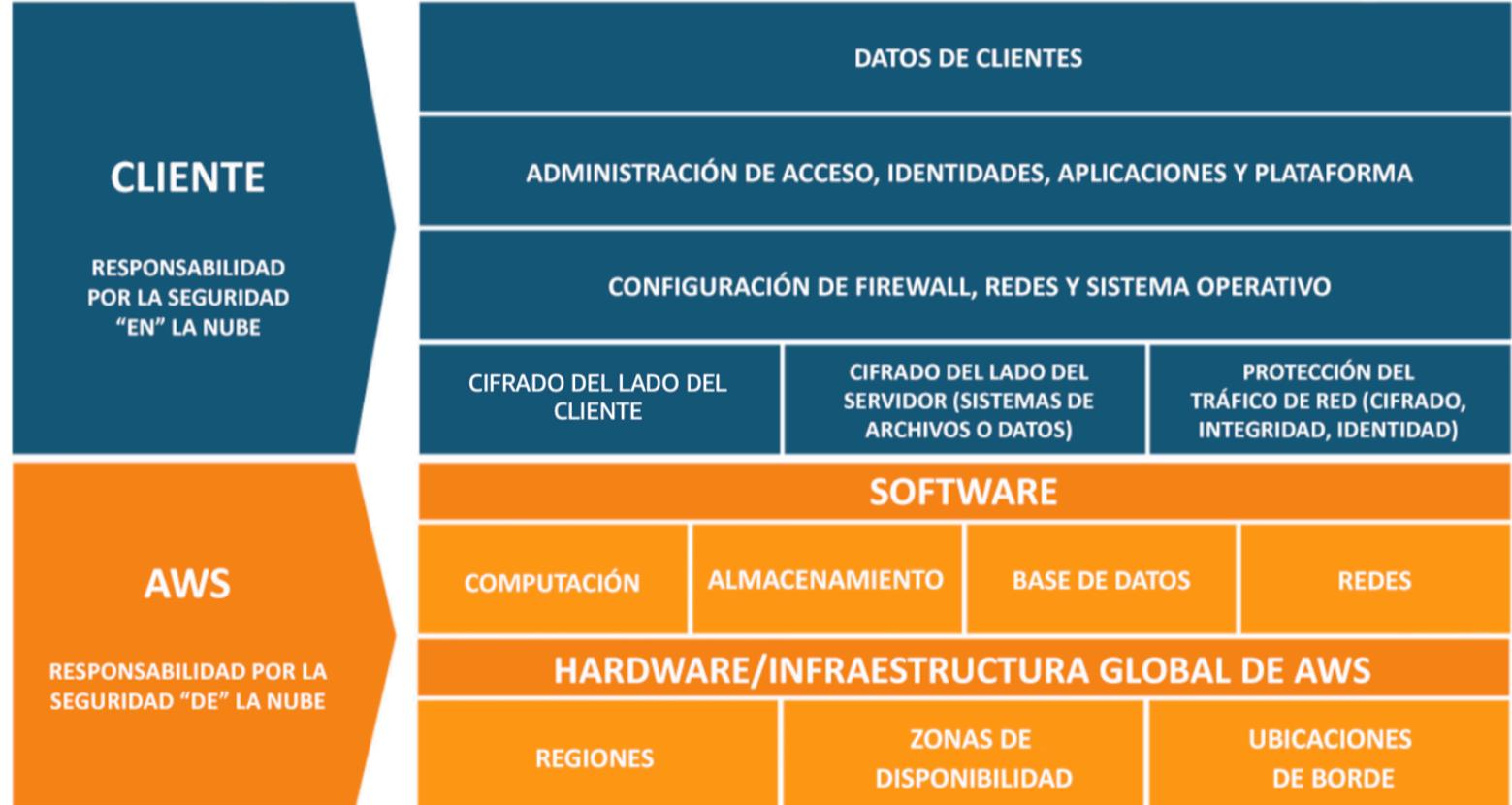


- **Tabla de regiones:** <https://aws.amazon.com/about-aws/global-infrastructure/regional-product-services>

Diagrama del modelo de responsabilidad compartida

CLIENTE = RESPONSABILIDAD POR LA SEGURIDAD DENTRO DEL CLOUD

AWS = RESPONSABILIDAD POR LA SEGURIDAD DEL CLOUD



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

Política de uso aceptable de AWS

- <https://aws.amazon.com/aup/>
- Ningún uso o contenido ilegal, dañino u ofensivo
- No a las violaciones de la seguridad
- No al abuso de la red
- No al abuso de correo electrónico u otros mensajes

IAM

IAM: Usuarios y Grupos



- IAM = Identity and Access Management, servicio **global**
- **Cuenta root / raíz** creada por defecto, no debe ser utilizada ni compartida
- Los **usuarios** son personas dentro de tu organización, y pueden ser agrupados
- Los **grupos** sólo contienen usuarios, no otros grupos
- Los usuarios no tienen que pertenecer a un grupo, y el usuario puede pertenecer a varios grupos



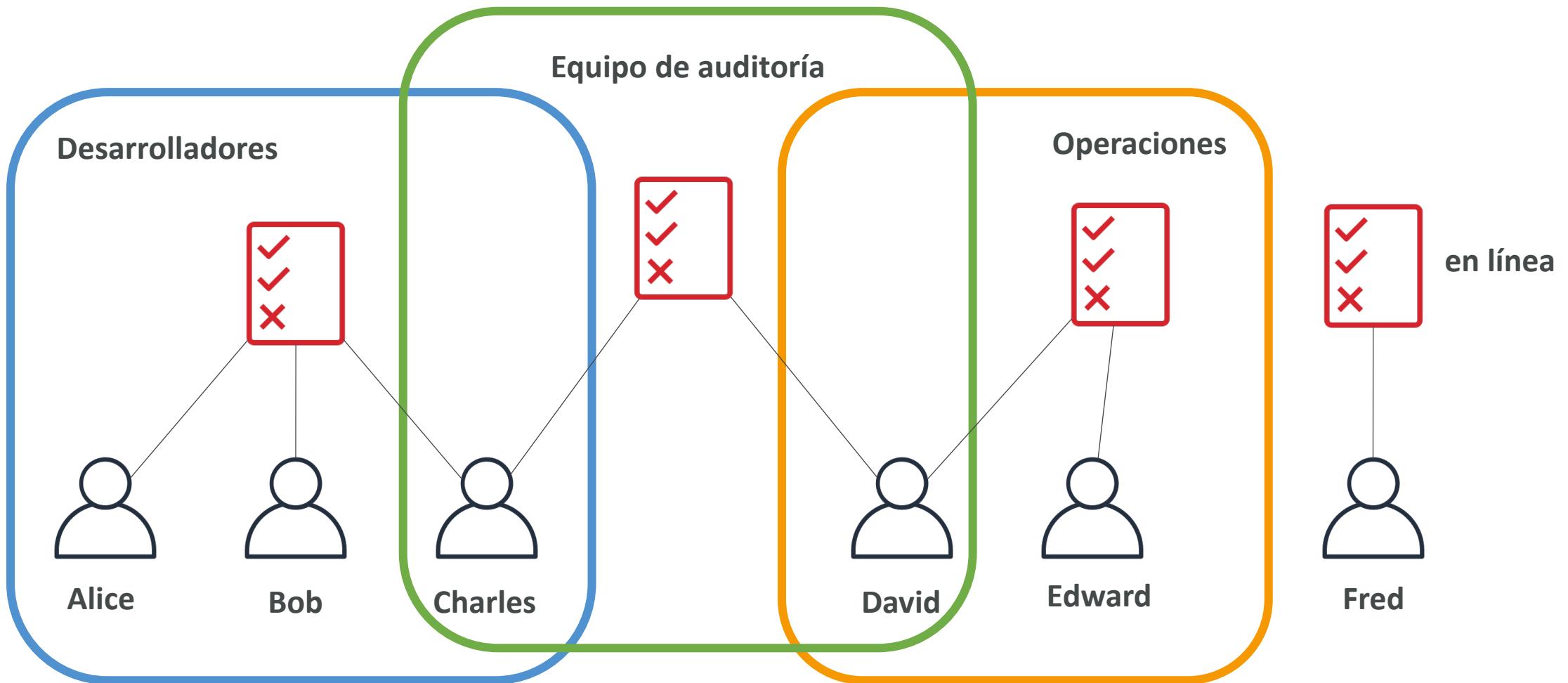
IAM: Permisos

- A los **usuarios o grupos** se les pueden asignar documentos JSON llamados políticas
- Estas políticas definen los **permisos** de los usuarios
- En AWS se aplica el **principio de mínimo privilegio**: no dar más permisos de los que un usuario necesita

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "ec2:Describe*",  
            "Resource": "*"  
        },  
        {  
            "Effect": "Allow",  
            "Action": "elasticloadbalancing:Describe*",  
            "Resource": "*"  
        },  
        {  
            "Effect": "Allow",  
            "Action": [  
                "cloudwatch>ListMetrics",  
                "cloudwatch:GetMetricStatistics",  
                "cloudwatch:Describe*"  
            ],  
            "Resource": "*"  
        }  
    ]  
}
```



Herencia de políticas IAM



Estructura de las políticas IAM

- Consta de:
 - **Version**: versión del lenguaje de la política, siempre incluye "2012-10-17"
 - **Id**: un identificador para la política (opcional)
 - **Statement**: una o más declaraciones individuales (obligatorio)
- Las declaraciones constan de:
 - **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
 - **Condition**: condiciones para cuando esta política está en efecto (opcional)

```
{  
  "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/*"]  
    }  
  ]  
}
```

IAM - Política de contraseñas

- Contraseñas fuertes = mayor seguridad para tu cuenta
- En AWS, puedes configurar una política de contraseñas:
 - Establecer una longitud mínima de contraseña
 - Requerir tipos de caracteres específicos:
 - incluyendo letras mayúsculas
 - letras minúsculas
 - números
 - caracteres no alfanuméricos
 - Permitir a todos los usuarios de IAM cambiar sus propias contraseñas
 - Requerir a los usuarios que cambien su contraseña después de un tiempo (caducidad de la contraseña)
 - Impedir la reutilización de la contraseña

Multi Factor Authentication - MFA



- Los usuarios tienen acceso a tu cuenta y posiblemente pueden cambiar configuraciones o eliminar recursos en tu cuenta de AWS
- **Quieres proteger tus cuentas root y los usuarios de IAM**
- MFA = contraseña que conoces + dispositivo de seguridad que posees



Alice

Contraseña +



=>

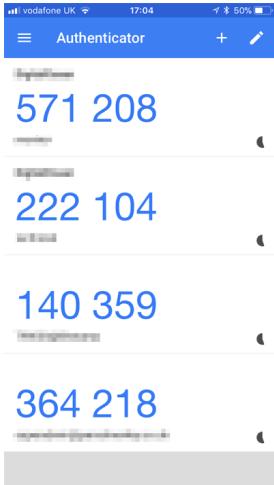
Login exitoso

- **Principal beneficio de MFA:**

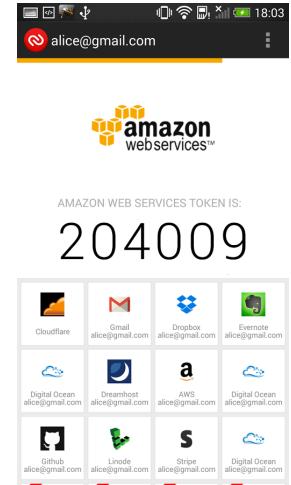
si una contraseña es robada o hackeada, la cuenta no se ve comprometida

Opciones de dispositivos MFA en AWS

Dispositivo virtual MFA



Autenticador de Google
(sólo en el teléfono)



Authy
(multi-dispositivo)

Soporte para múltiples tokens en un solo dispositivo.

Clave de seguridad del segundo factor universal (U2F)



YubiKey de Yubico (3rd party)

Soporte para múltiples usuarios root e IAM utilizando una única clave de seguridad

Opciones de dispositivos MFA en AWS

Dispositivo MFA de llavero por hardware



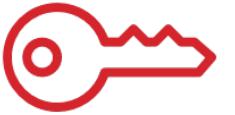
Proporcionado por Gemalto (3rd party)

Dispositivo MFA de llavero por hardware para AWS GovCloud (US)



Proporcionado por SurePassID (3rd party)

¿Cómo pueden los usuarios acceder a AWS?



- Para acceder a AWS, tienes tres opciones:
 - **Consola de administración de AWS** (protegida por contraseña + MFA)
 - **Interfaz de línea de comandos de AWS (CLI)**: protegida por claves de acceso
 - **AWS Software Developer Kit (SDK)** - para el código: protegido por claves de acceso
 - Las claves de acceso se generan a través de la consola de AWS
- Los usuarios gestionan sus propias claves de acceso
- **Las claves de acceso son secretas, como una contraseña. No las compartas**
- ID de la clave de acceso ~ = nombre de usuario
- Clave de acceso secreta ~ = contraseña

Ejemplo de claves de acceso (falsas)

Access keys

Use access keys to make secure REST or HTTP Query protocol requests to AWS service APIs. For your protection, you should never share your secret keys with anyone. As a best practice, we recommend frequent key rotation. [Learn more](#)

[Create access key](#)

Access key ID	Created	Last used	Status	
AKIASK4E37PV4TU3RD6C	2020-05-25 15:13 UTC+0100	N/A	Active	Make inactive X

- ID de la llave de acceso: AKIASK4E37PV4983d6C
- Clave de acceso secreta: AZPN3z0jWozWCndljhB0Unh8239a1bzBzO5fqkZq
- **Recuerda: no compartas tus claves de acceso**

¿Qué es la CLI de AWS?

- Una herramienta que permite interactuar con los servicios de AWS mediante comandos en tu shell de línea de comandos
- Acceso directo a las API públicas de los servicios de AWS
- Puedes desarrollar scripts para gestionar tus recursos
- Es de código abierto <https://github.com/aws/aws-cli>
- Alternativa al uso de la consola de administración de AWS

```
→ ~ aws s3 cp myfile.txt s3://ccp-mybucket/myfile.txt
upload: ./myfile.txt to s3://ccp-mybucket/myfile.txt
→ ~ aws s3 ls s3://ccp-mybucket
2021-05-14 03:22:52          0 myfile.txt
→ ~ █
```

¿Qué es el SDK de AWS?

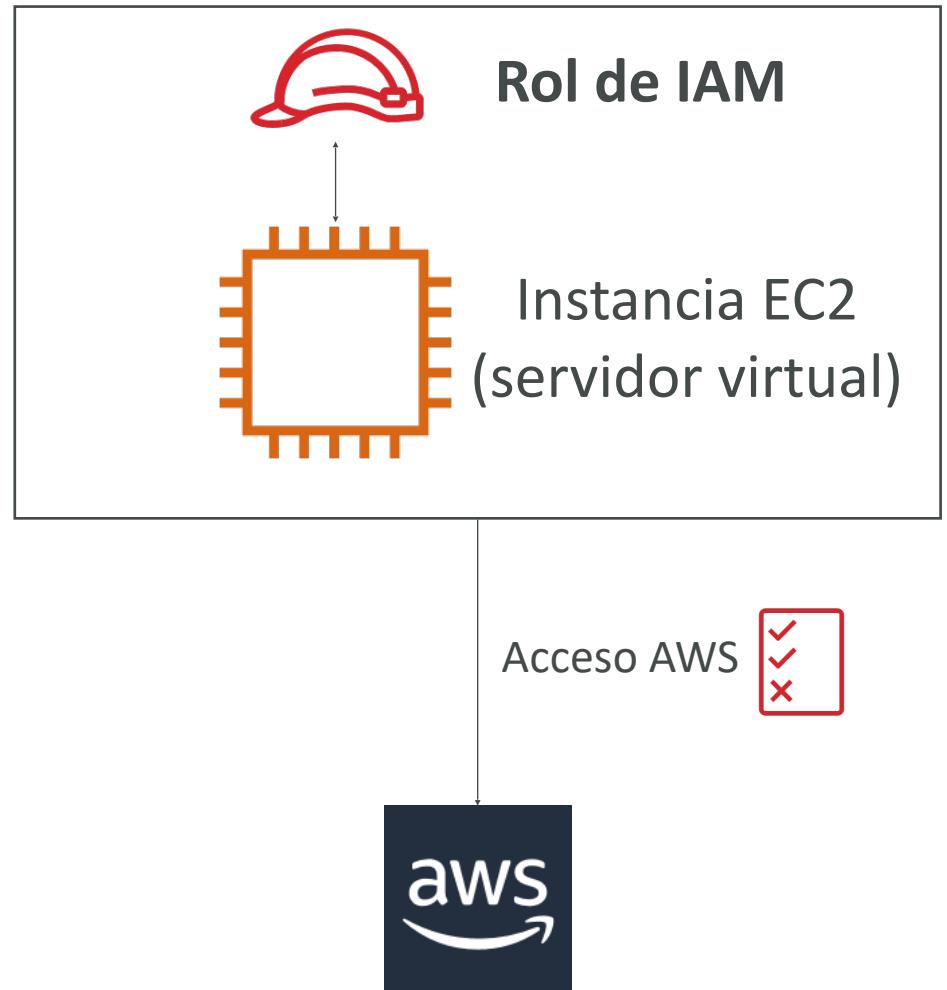


- Kit de desarrollo de software de AWS (AWS SDK)
- APIs específicas para cada lenguaje (conjunto de bibliotecas)
- Permite acceder y administrar los servicios de AWS mediante programación
- Integrado en la aplicación
- Admite:
 - SDKs (JavaScript, Python, PHP, .NET, Ruby, Java, Go, Node.js, C++)
 - SDKs para móviles (Android, iOS, ...)
 - SDKs para dispositivos IoT (Embedded C, Arduino, ...)
- Ejemplo: AWS CLI está construido sobre AWS SDK para Python



Roles IAM para los servicios

- Algún servicio de AWS tendrá que realizar acciones en tu nombre
- Para ello, asignaremos **permisos** a los servicios de AWS con **Roles IAM**
- Roles comunes:
 - Roles de Instancia EC2
 - Roles de la función Lambda
 - Roles para CloudFormation



Herramientas de seguridad IAM

- **IAM Credentials Report / Informe de credenciales de IAM (a nivel de cuenta)**
 - Un informe que enumera todos los usuarios de tu cuenta y el estado de tus diversas credenciales
- **IAM Access Advisor / Asesor de acceso de IAM (a nivel de usuario)**
 - Muestra los permisos de servicio concedidos a un usuario y cuando se accedió a esos servicios por última vez
 - Puedes utilizar esta información para revisar tus políticas

Directrices y buenas prácticas de IAM



- No utilices la cuenta root excepto para la configuración de la cuenta AWS
- Un usuario físico = Un **usuario** AWS
- **Asignar usuarios a grupos** y asignar permisos a grupos
- Crear una **política de contraseñas fuerte**
- Utilizar y reforzar el uso de la **autenticación multifactor (MFA)**
- Crear y utilizar **Roles** para dar permisos a los servicios de AWS
- Utilizar claves de acceso para el acceso programático (CLI / SDK)
- Revisar los permisos de tu cuenta con el informe de credenciales de IAM o el asesor de acceso de IAM
- **No compartir nunca los usuarios de IAM ni las claves de acceso**

Modelo de responsabilidad compartida para IAM



Tú

- Infraestructura (seguridad de la red global)
- Análisis de configuración y vulnerabilidad
- Validación de la conformidad
- Gestión y supervisión de usuarios, grupos, roles y políticas
- Habilitar MFA en todas las cuentas
- Rota todas tus claves con frecuencia
- Utiliza las herramientas IAM para aplicar los permisos adecuados
- Analiza los patrones de acceso y revisa los permisos

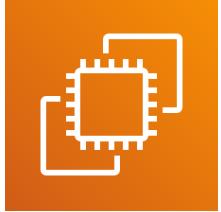
Resumen - IAM



- **Usuarios:** mapeado a un usuario físico, tiene una contraseña para la consola de AWS
- **Grupos:** contiene sólo usuarios
- **Políticas:** Documento JSON que describe los permisos para los usuarios o grupos
- **Roles:** para instancias EC2 o servicios AWS
- **Seguridad:** MFA + Política de contraseñas
- **AWS CLI:** gestiona tus servicios de AWS mediante la línea de comandos
- **AWS SDK:** gestiona tus servicios de AWS utilizando un lenguaje de programación
- **Claves de acceso:** accede a AWS mediante la CLI o el SDK
- **Auditoría:** Informes de credenciales de IAM y Asesor de acceso de IAM

EC2

Amazon EC2



- EC2 es una de las ofertas más populares de AWS
- EC2 = Elastic Compute Cloud = Infraestructura como servicio (IaaS)
- Consiste principalmente en la capacidad de :
 - Alquilar máquinas virtuales (EC2)
 - Almacenar datos en unidades virtuales (EBS)
 - Distribuir la carga entre las máquinas (ELB)
 - Escalar los servicios mediante un Auto Scaling Group (ASG) o también conocido en español como Grupo de Autoescalamiento
- Conocer EC2 es fundamental para entender el funcionamiento del Cloud

Opciones de tamaño y configuración de EC2

- Sistema operativo (**OS**): Linux, Windows o Mac OS
- Cuánta potencia de cálculo y núcleos (**CPU**)
- Cuánta memoria de acceso aleatorio (**RAM**)
- Cuánto espacio de almacenamiento:
 - Conectado a la red (**EBS y EFS**)
 - hardware (**EC2 Instance Store**)
- Tarjeta de red: velocidad de la tarjeta, dirección IP pública
- Reglas de firewall: **grupo de seguridad**
- Script de arranque (configurar en el primer lanzamiento): Datos de usuario de EC2

Datos del usuario de EC2

- Es posible arrancar nuestras instancias utilizando un script de datos de usuario de EC2.
- bootstrapping significa lanzar comandos cuando una máquina se inicia
- Ese script sólo se ejecuta una vez en el primer arranque de la instancia
- Los datos de usuario de EC2 se utilizan para automatizar tareas de arranque como:
 - Instalar actualizaciones
 - Instalación de software
 - Descarga de archivos comunes de Internet
 - Cualquier cosa que se te ocurra
- El script de datos de usuario de EC2 se ejecuta con el usuario root

Lanzamiento de una instancia EC2 con Linux

- Vamos a lanzar nuestro primer servidor virtual utilizando la consola de AWS
- Tendremos una primera aproximación de alto nivel a los distintos parámetros
- Veremos que nuestro servidor web se lanza utilizando los datos de usuario de EC2
- Aprenderemos a iniciar / parar / terminar nuestra instancia.

Tipos de instancias de EC2 - Visión general

- Puedes utilizar diferentes tipos de instancias EC2 optimizadas para diferentes casos de uso (<https://aws.amazon.com/ec2/instance-types/>)
- AWS tiene la siguiente convención de nombres:

m5.2xlarge

- m: clase de instancia
- 5: generación (AWS los mejora con el tiempo)
- 2xlarge: tamaño dentro de la clase de instancia

General Purpose
Compute Optimized
Memory Optimized
Accelerated Computing
Storage Optimized
Instance Features
Measuring Instance Performance

Tipos de instancias de EC2 - Propósito general

- Excelente para una diversidad de cargas de trabajo, como servidores web o repositorios de código
- Equilibrio entre:
 - Computación
 - Memoria
 - Red
- En el curso, utilizaremos la instancia t2.micro que es una instancia EC2 de propósito general

General Purpose

General purpose instances provide a balance of compute, memory and networking resources, and can be used for a variety of diverse workloads. These instances are ideal for applications that use these resources in equal proportions such as web servers and code repositories.

Mac	T4g	T3	T3a	T2	M6g	M5	M5a	M5n	M5zn	M4	A1
-----	-----	----	-----	----	-----	----	-----	-----	------	----	----

* Esta lista evolucionará con el tiempo, por favor, consulta el sitio web de AWS para obtener la información más reciente

Tipos de instancias EC2 - Computación optimizada

- Ideal para tareas de cálculo intensivo que requieren procesadores de alto rendimiento:
 - Cargas de trabajo de procesamiento por lotes
 - Transcodificación de medios
 - Servidores web de alto rendimiento
 - Computación de alto rendimiento (HPC)
 - Modelado científico y aprendizaje automático
 - Servidores dedicados a juegos

Compute Optimized

Compute Optimized instances are ideal for compute bound applications that benefit from high performance processors. Instances belonging to this family are well suited for batch processing workloads, media transcoding, high performance web servers, high performance computing (HPC), scientific modeling, dedicated gaming servers and ad server engines, machine learning inference and other compute intensive applications.

C6g C6gn C5 C5a C5n C4

* Esta lista evolucionará con el tiempo, por favor, consulta el sitio web de AWS para obtener la información más reciente

Tipos de instancias EC2 - Memoria optimizada

- Rápido rendimiento para cargas de trabajo que procesan grandes conjuntos de datos en memoria
- Casos de uso:
 - Alto rendimiento, bases de datos relacionales/no relacionales
 - Almacenes de caché distribuidos a escala web
 - Bases de datos en memoria optimizadas para BI (business intelligence)
 - Aplicaciones que realizan el procesamiento en tiempo real de grandes datos no estructurados

Memory Optimized

Memory optimized instances are designed to deliver fast performance for workloads that process large data sets in memory.

R6g

R5

R5a

R5b

R5n

R4

X1e

X1

High Memory

z1d

* Esta lista evolucionará con el tiempo, por favor, consulta el sitio web de AWS para obtener la información más reciente

Tipos de instancias EC2 - Almacenamiento optimizado

- Ideal para tareas de almacenamiento intensivo que requieran un acceso alto y secuencial de lectura y escritura a grandes conjuntos de datos en el almacenamiento local
- Casos de uso:
 - Sistemas de procesamiento de transacciones en línea (OLTP) de alta frecuencia
 - Bases de datos relacionales y NoSQL
 - Caché para bases de datos en memoria (por ejemplo, Redis)
 - Aplicaciones de almacenamiento de datos
 - Sistemas de archivos distribuidos

Storage Optimized

Storage optimized instances are designed for workloads that require high, sequential read and write access to very large data sets on local storage. They are optimized to deliver tens of thousands of low-latency, random I/O operations per second (IOPS) to applications.

I3	I3en	D2	D3	D3en	H1
----	------	----	----	------	----

* Esta lista evolucionará con el tiempo, por favor, consulta el sitio web de AWS para obtener la información más reciente

Tipos de instancias de EC2: ejemplo

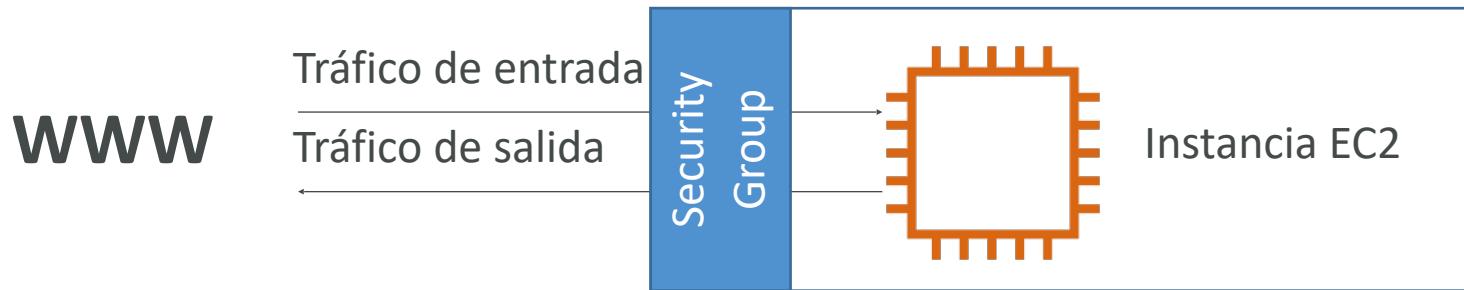
Instancia	vCPU	Mem (GiB)	Almacenamiento	Rendimiento de la red	Ancho de banda de EBS (Mbps)
t2.micro	1	1	Sólo EBS	Bajo a moderado	
t2.xlarge	4	16	Sólo EBS	Moderado	
c5d.4xlarge	16	32	1 x 400 NVMe SSD	Hasta 10 Gbps	4,750
r5.16xlarge	64	512	Sólo EBS	20 Gbps	13,600
m5.8xlarge	32	128	Sólo EBS	10 Gbps	6,800

t2.micro forma parte de la capa gratuita de AWS (hasta 750 horas al mes)

<https://instances.vantage.sh>

Introducción a los grupos de seguridad

- Los grupos de seguridad son la base de la seguridad de la red en AWS
- Controlan cómo se permite el tráfico dentro o fuera de nuestras Instancias EC2



- Los grupos de seguridad sólo contienen reglas de **permiso**
- Las reglas de los grupos de seguridad pueden hacer referencia por IP o por grupo de seguridad

Grupos de seguridad

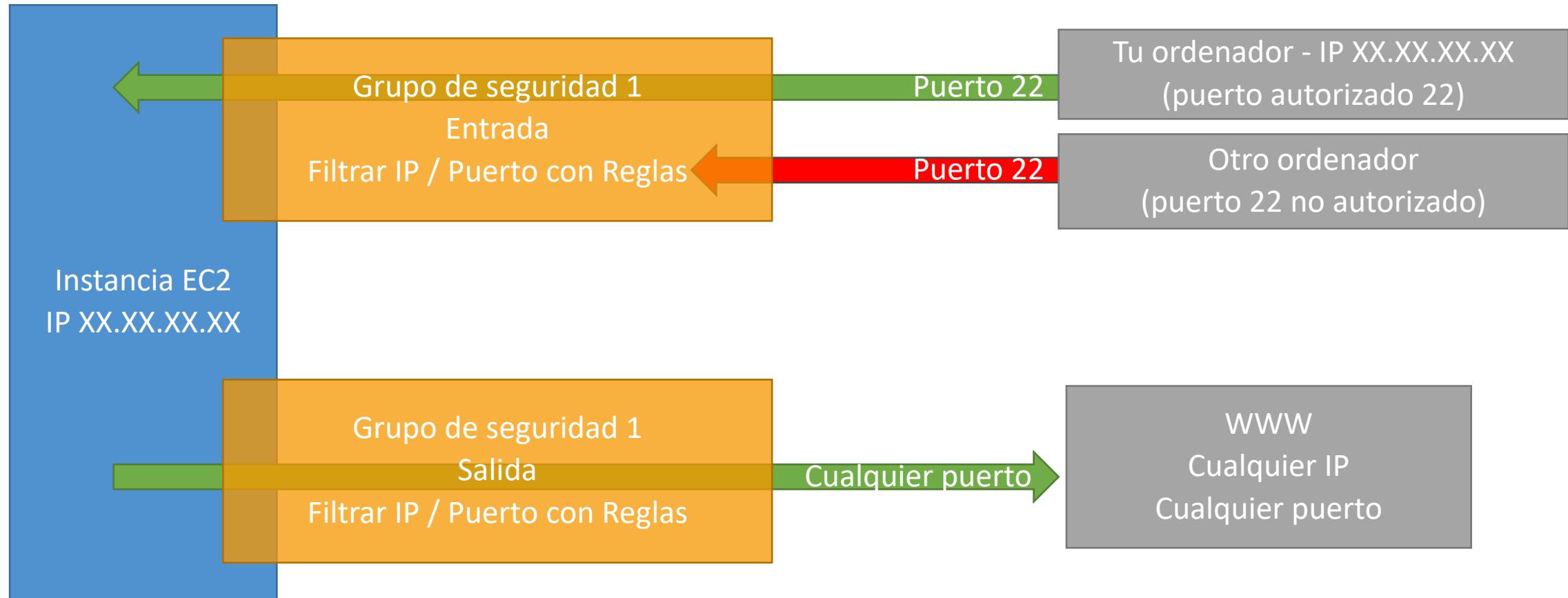
Inmersión más profunda

- Los grupos de seguridad actúan como un “firewall” en las instancias de EC2
- Regulan:
 - El acceso a los puertos
 - Rangos de IP autorizados - IPv4 e IPv6
 - Control de la red de entrada (de otros a la instancia)
 - Control de la red saliente (desde la instancia hacia otra)

Type	Protocol	Port Range	Source	Description
HTTP	TCP	80	0.0.0.0/0	test http page
SSH	TCP	22	122.149.196.85/32	
Custom TCP Rule	TCP	4567	0.0.0.0/0	java app

Grupos de seguridad

Diagrama



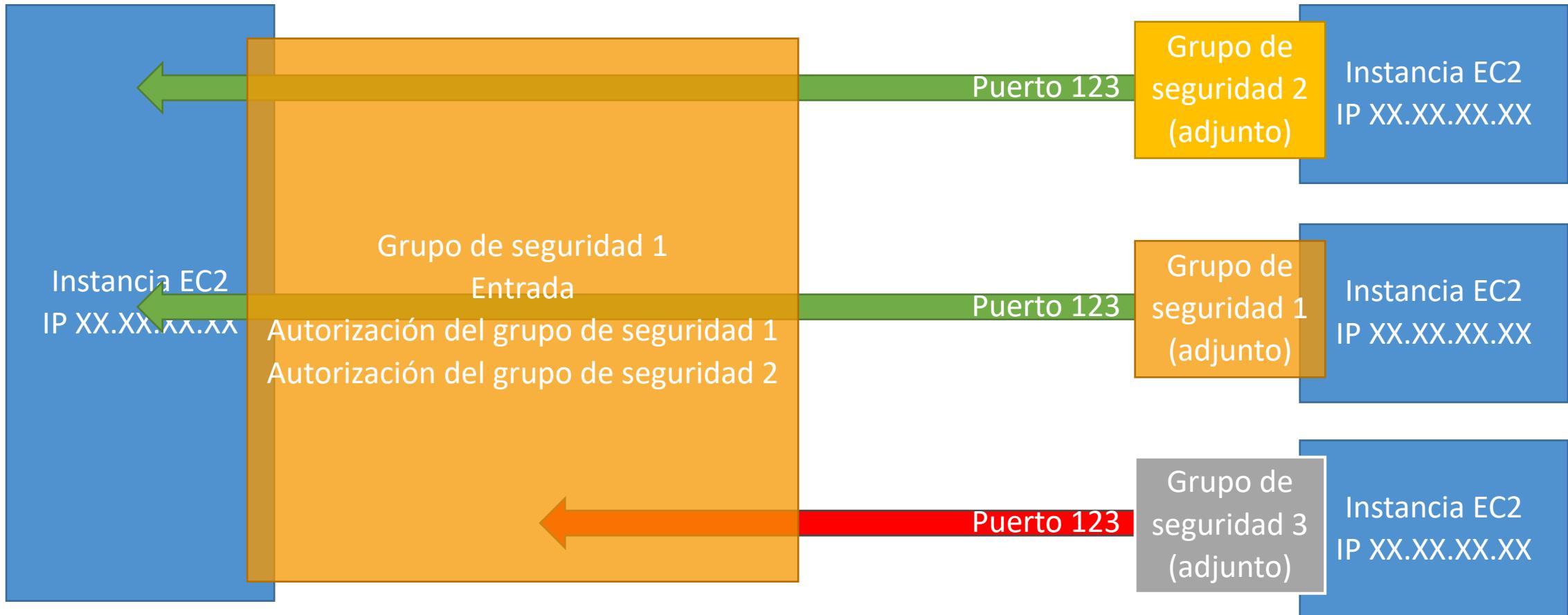
Grupos de seguridad

Es bueno saber

- Puede adjuntarse a múltiples instancias
- Bloqueado a una combinación de región / VPC
- Vive "fuera" del EC2 - si el tráfico está bloqueado, la instancia EC2 no lo verá
- Es bueno mantener un grupo de seguridad separado para el acceso SSH
- Si tu aplicación no es accesible (tiempo de espera), entonces es un problema de grupo de seguridad
- Si tu aplicación da un error de "conexión rechazada", entonces es un error de la aplicación o no se ha lanzado
- Todo el tráfico de entrada está **bloqueado** por defecto
- Todo el tráfico de salida está **autorizado** por defecto

Referencia a otros grupos de seguridad

Diagrama



Puertos clásicos que hay que conocer

- 22 = SSH (Secure Shell) - iniciar sesión en una instancia de Linux
- 21 = FTP (File Transfer Protocol) - subir archivos a un archivo compartido
- 22 = SFTP (Secure File Transfer Protocol) - subir archivos usando SSH
- 80 = HTTP - acceso a sitios web no seguros
- 443 = HTTPS - acceso a sitios web seguros
- 3389 = RDP (Remote Desktop Protocol) - iniciar sesión en una instancia de Windows

Tabla resumen SSH

	SSH	Putty	EC2 Instance Connect
Mac	✓		✓
Linux	✓		✓
Windows < 10		✓	✓
Windows >= 10	✓	✓	✓

Qué clases hay que ver

- **Mac / Linux:**
 - Clase de SSH en Mac/Linux
- **Windows:**
 - Clase sobre Putty
 - Si Windows 10: Clase sobre SSH en Windows 10
- **Todos los estudiantes:**
 - Clase de Instance Connect EC2

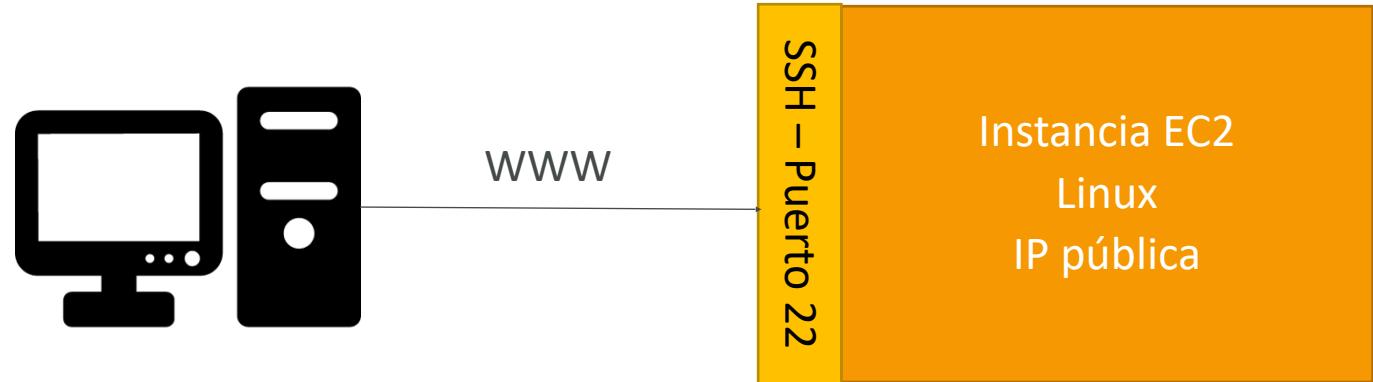
Solución de problemas de SSH

- **Los estudiantes son los que más problemas tienen con SSH**
- Si las cosas no funcionan...
 - Vuelve a ver la clase. Puede que te hayas perdido algo
 - Lee la guía de solución de problemas
 - Prueba con EC2 Instance Connect
- **Si uno de los métodos funciona (SSH, Putty o EC2 Instance Connect) estás bien**
- Si ningún método funciona, no pasa nada, el curso no utilizará mucho SSH

Cómo usar SSH en tu instancia EC2

Linux / Mac OS X

- Vamos a aprender cómo usar SSH en tu instancia EC2 usando [Linux / Mac](#)
- SSH es una de las funciones más importantes. Permite controlar una máquina remota, todo ello utilizando la línea de comandos.

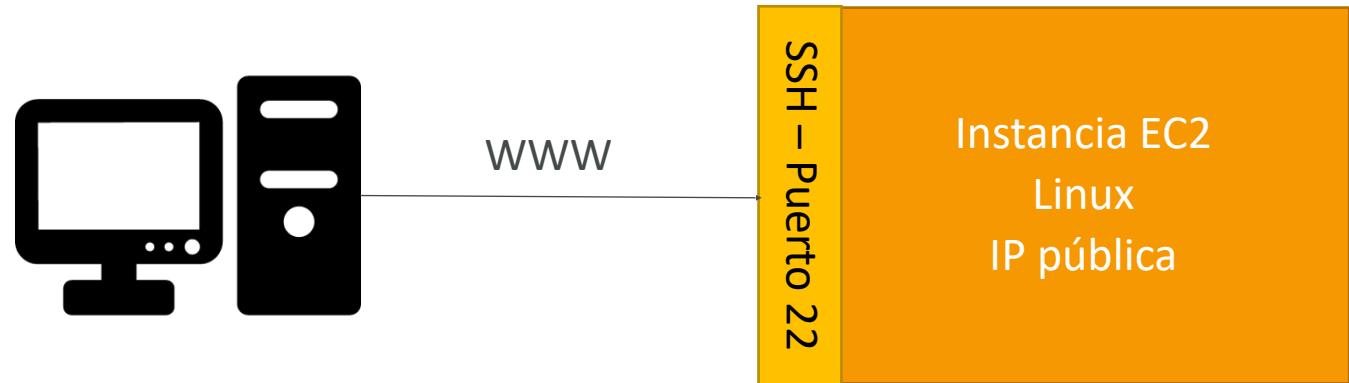


- Vamos a ver cómo podemos configurar OpenSSH [~/.ssh/config](#) para facilitar el SSH en nuestras instancias EC2

Cómo usar SSH en tu instancia EC2

Windows

- Vamos a aprender cómo usar SSH en tu instancia EC2 usando [Windows](#)
- SSH es una de las funciones más importantes. Permite controlar una máquina remota, todo ello utilizando la línea de comandos.



- Configuraremos todos los parámetros necesarios para hacer SSH en Windows utilizando la herramienta gratuita [Putty](#).

Instance Connect EC2

Conexión de instancias EC2

- Conéctate a tu instancia EC2 desde el navegador
- No es necesario utilizar el archivo de claves que se ha descargado
- La "magia" es que una clave temporal es cargada en EC2 por AWS
- **Funciona sólo out-of-the-box con Amazon Linux 2**
- Necesitas asegurarte de que el puerto 22 sigue abierto

Opciones de compra de instancias EC2

- **Instancias bajo demanda:** carga de trabajo corta, precio predecible, pago por segundos
- **Reservadas** (1 y 3 años)
 - **Instancias reservadas** - cargas de trabajo largas
 - **Instancias reservadas convertibles:** cargas de trabajo largas con instancias flexibles
- **Planes de ahorro** (1 y 3 años) - compromiso con una cantidad de uso, carga de trabajo larga
- **Instancias Spot** - cargas de trabajo cortas, baratas, pueden perder instancias (menos fiables)
- **Hosts dedicados:** reserve un servidor físico completo, controle la ubicación de las instancias
- **Instancias dedicadas** - ningún otro cliente compartirá tu hardware
- **Reservas de capacidad** - reserva de capacidad en una AZ específica para cualquier duración

EC2 bajo demanda

- Paga por lo que usas:
 - Linux o Windows - facturación por segundo, después del primer minuto
 - Todos los demás sistemas operativos: facturación por hora
 - Tiene el coste más elevado, pero no hay que pagar por adelantado
 - Sin compromiso a largo plazo
-
- Recomendado para **cargas de trabajo a corto plazo y sin interrupciones**, cuando no se puede predecir el comportamiento de la aplicación

Instancias reservadas de EC2

- Hasta un **72%** de descuento en comparación con el servicio bajo demanda
- Reserva de atributos de instancia específicos (**tipo de instancia, región, ocupación, sistema operativo**)
- **Periodo de reserva - 1 año** (+descuento) o **3 años** (+++descuento)
- **Opciones de pago - Sin pago inicial (+), Pago inicial parcial (++)**, **Pago inicial total (+++)**
- **Alcance de la instancia reservada** - Por **región** o por **zona** (capacidad de reserva en una AZ)
- Recomendado para aplicaciones de uso constante (piensa en una base de datos)
- Puedes comprar y vender en el Marketplace de instancias reservadas
- **Instancia reservada convertible:**
 - Puedes cambiar el tipo de instancia EC2, la familia de instancias, el SO, etc.
 - Hasta un **66%** de descuento

Nota: los % de descuento pueden ser diferentes a los del video ya que AWS los cambia con el tiempo - los números exactos no son necesarios para el examen. Esto es solo para fines ilustrativos ☺.

Planes de ahorro EC2

- Obtén un descuento basado en el uso a largo plazo (hasta el 72%)
- Comprométete a un determinado tipo de uso (10 \$/hora durante 1 o 3 años)
- El uso más allá de los planes de ahorro de EC2 se factura al precio bajo demanda
- Bloqueado a una familia de instancias específica y a una región de AWS (por ejemplo, M5 en us-east-1)
- Flexible a través de:
 - Tamaño de instancia (por ejemplo, m5.xlarge, m5.2xlarge)
 - Sistema operativo (por ejemplo, Linux, Windows)
 - Tenencia (Host, dedicado, por defecto)



Instancias EC2 Spot

- Puedes obtener un **descuento de hasta el 90%** en comparación con la demanda
- Instancias que puedes "perder" en cualquier momento si su precio máximo es inferior al precio spot actual
- Las instancias **MÁS rentables** de AWS
- **Útil para las cargas de trabajo que son resistentes a los fallos**
 - Trabajos por lotes (Batch Jobs)
 - Análisis de datos
 - Procesamiento de imágenes
 - Cualquier carga de trabajo **distribuida**
 - Cargas de trabajo con una hora de inicio y finalización flexible
- **No es adecuado para trabajos críticos o bases de datos**

Hosts dedicados EC2

- Un servidor físico con capacidad de instancia EC2 totalmente dedicado a su uso
- Permite abordar los requisitos de **normativas y utilizar licencias de software vinculadas al servidor existentes** (licencias de software por socket, por núcleo, por VM)
- Opciones de compra:
 - **Bajo demanda** - pago por segundo para el host dedicado activo
 - **Reservado** - 1 o 3 años (sin pago inicial, pago inicial parcial, pago inicial total)
- La opción más cara
- Útil para el software que tiene un modelo de licencia complicado (BYOL - Bring Your Own License)
- O para empresas que tienen fuertes necesidades de regulación o cumplimiento

Instancias dedicadas de EC2

- Las instancias se ejecutan en un hardware dedicado para ti
- Puedes compartir el hardware con otras instancias de la misma cuenta
- No hay control sobre la ubicación de las instancias (se puede mover el hardware después de la parada/arranque)

Characteristic	Dedicated Instances	Dedicated Hosts
Enables the use of dedicated physical servers	X	X
Per instance billing (subject to a \$2 per region fee)	X	
Per host billing		X
Visibility of sockets, cores, host ID		X
Affinity between a host and instance		X
Targeted instance placement		X
Automatic instance placement	X	X
Add capacity using an allocation request		X

Reservas de capacidad de EC2

- Reserva la capacidad de las instancias **bajo demanda** en una AZ específica para cualquier duración
- Siempre tendrás acceso a la capacidad de EC2 cuando la necesites
- **Sin compromiso de tiempo** (crear/cancelar en cualquier momento), **sin descuentos de facturación**
- Combina con las instancias regionales reservadas y los planes de ahorro para beneficiarte de descuentos en la facturación
- Se te cobra la tarifa bajo demanda tanto si ejecuta instancias como si no

- Adecuado para cargas de trabajo ininterrumpidas a corto plazo que necesitan estar en una AZ específica

¿Qué opción de compra me conviene?



- **Bajo demanda (On demand)**: venir y quedarse en el complejo cuando queramos, pagamos el precio completo
- **Reservada (Reserved)**: cómo planificar con antelación y si planeamos quedarnos durante mucho tiempo, podemos obtener un buen descuento
- **Planes de ahorro (Savings Plans)**: pagamos una cantidad por hora durante un periodo determinado y nos alojamos en cualquier tipo de habitación (por ejemplo, King, Suite, Vista al mar, ...)
- **Instancias de spot (Spot instances)**: el hotel permite que la gente puje por las habitaciones vacías y el mejor postor se queda con ellas. Puede ser expulsado en cualquier momento
- **Hosts dedicados (Dedicated Hosts)**: Se reserva un edificio entero del complejo turístico
- **Reservas de capacidad (Capacity Reservations)**: reservas una habitación por un periodo con el precio completo aunque no te alojes en ella

Comparación de precios

Ejemplo - m4.large - us-east-1

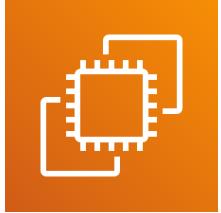
Tipo de precio	Precio (por hora)
Precio bajo demanda (On-demand)	0.10\$
Instancias de spot (Spot instances)	0.038\$ - 0.039\$ (hasta 61% de descuento)
Instancia reservada (1 año) (Reserved)	0,062\$ (sin anticipo) - 0,058\$ (todo por adelantado)
Instancia reservada (3 años) (Reserved)	0,043\$ (sin anticipo) - 0,037\$ (todo por adelantado)
Plan de ahorro EC2 (1 año) (Saving plan)	0,062\$ (sin anticipo) - 0,058\$ (todo por adelantado)
Instancia reservada convertible (1 año)	0,071\$ (sin anticipo) - 0,066\$ (todo por adelantado)
Host dedicado (Dedicated host)	Precio bajo demanda (On-demand)
Reserva de host dedicado (Dedicated host reservation)	Hasta el 70% de descuento
Reservas de capacidad (Capacity reservation)	Precio bajo demanda (On-demand)

Modelo de responsabilidad compartida para EC2



- Infraestructura (seguridad global de la red)
- Aislamiento en hosts físicos
- Sustitución de hardware defectuoso
- Validación de la normativa
- Reglas de los grupos de seguridad
- Parches y actualizaciones del sistema operativo
- Software y utilidades instaladas en la instancia EC2
- Roles IAM asignados a EC2 y gestión de acceso de usuarios IAM
- Seguridad de los datos en tu instancia

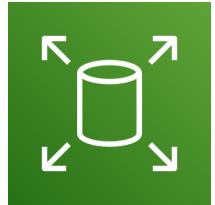
Resumen - EC2



- **Instancia EC2:** AMI (SO) + Tamaño de la Instancia (CPU + RAM) + Almacenamiento + Grupos de Seguridad + Datos de Usuario EC2
- **Grupos de seguridad:** Firewall adjunto a la instancia EC2
- **Datos de usuario de EC2:** Script lanzado en el primer arranque de una instancia
- **SSH:** iniciar un terminal en nuestras instancias EC2 (puerto 22)
- **Rol de la Instancia EC2:** enlace a los roles de IAM
- **Opciones de compra:** On-Demand, Spot, Reservada (Estándar + Convertible + Programada), Host Dedicado, Instancia Dedicada

Almacenamiento de instancias EC2

¿Qué es un volumen EBS?



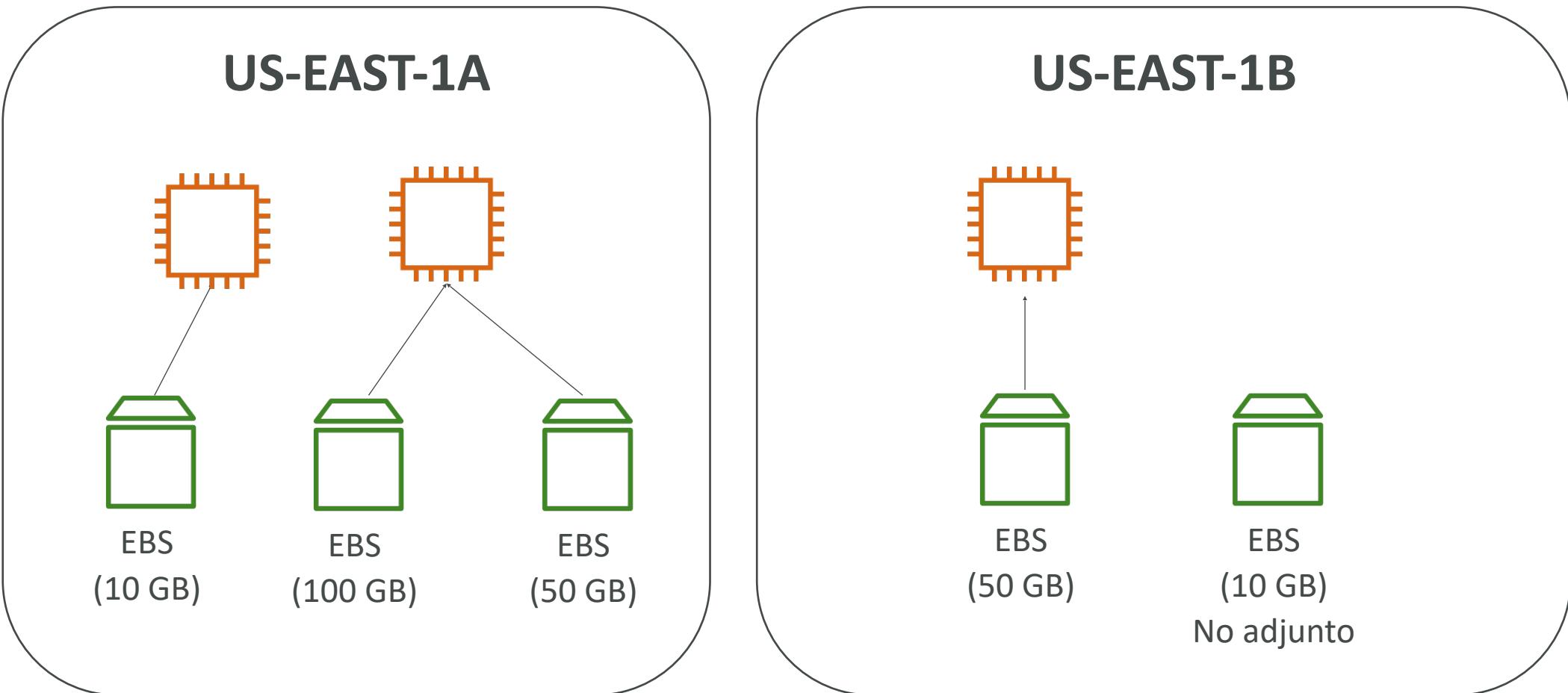
- Un **volumen EBS (Elastic Block Store)** es una **unidad de red** que puede adjuntar a las instancias mientras se ejecutan
- Permite que las instancias persistan los datos, incluso después de su finalización
- **Sólo pueden montarse en una instancia a la vez** (a nivel de CCP)
- Están vinculados **a una zona de disponibilidad específica**

- Analogía: Piensa en ellos como una "memoria USB de red"
- Nivel gratuito: 30 GB de almacenamiento EBS gratuito de tipo Propósito General (SSD) o Magnético al mes

Volumen EBS

- Es una unidad de red (es decir, no es una unidad física)
 - Utiliza la red para comunicar la instancia, lo que significa que puede haber un poco de latencia
 - Se puede separar de una instancia EC2 y conectarla a otra rápidamente
- Está bloqueado en una Zona de Disponibilidad (AZ)
 - Un volumen EBS en us-east-1a no puede adjuntarse a us-east-1b
 - Para trasladar un volumen, primero hay que hacer un snapshot del mismo
- Tener una capacidad provisionada (tamaño en GBs, e IOPS)
 - Se facturará toda la capacidad aprovisionada
 - Puede aumentar la capacidad de la unidad con el tiempo

Volumen EBS - Ejemplo



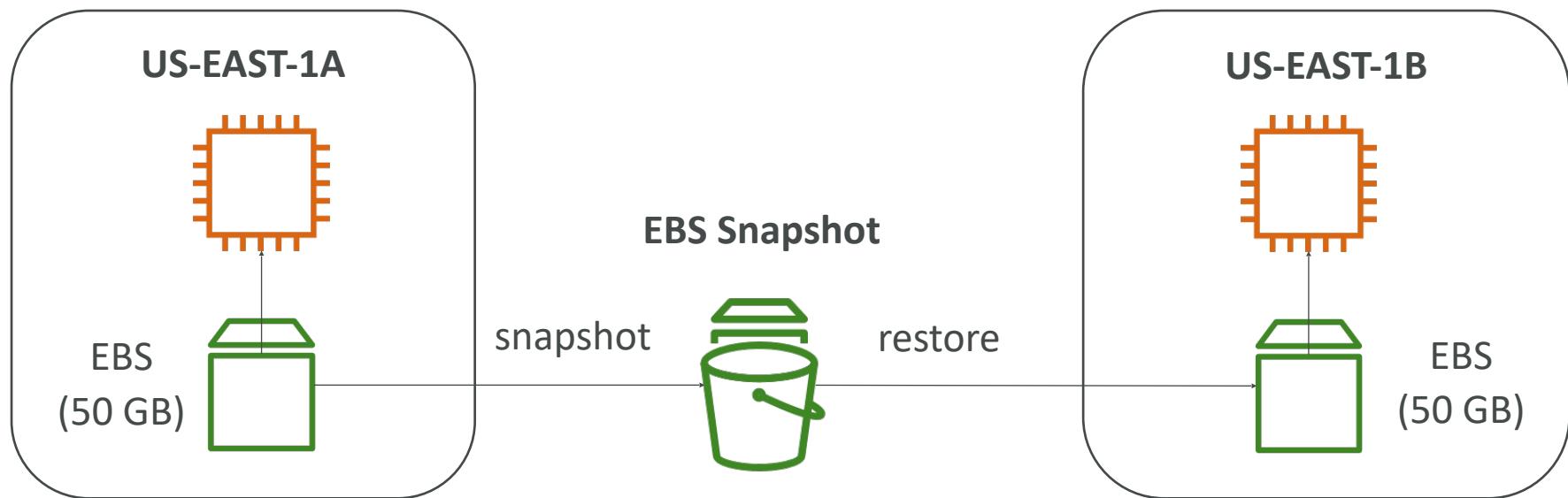
EBS - Atributo "Borrar al terminar"

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encryption
Root	/dev/xvda	snap-09f18f682fd23a1b1	8	General Purpose SSD (gp2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted
EBS	/dev/sdb	Search (case-insensit	8	General Purpose SSD (gp2)	100 / 3000	N/A	<input type="checkbox"/>	Not Encrypted
Add New Volume								

- Controla el comportamiento de EBS cuando una instancia EC2 termina
 - Por defecto, se elimina el volumen EBS root / raíz (atributo habilitado)
 - Por defecto, cualquier otro volumen EBS adjunto no se elimina (atributo deshabilitado)
- Esto puede ser controlado por la consola de AWS / AWS CLI
- **Caso de uso: preservar el volumen root / raíz cuando se termina la instancia**

Snapshot / Instantáneas de EBS

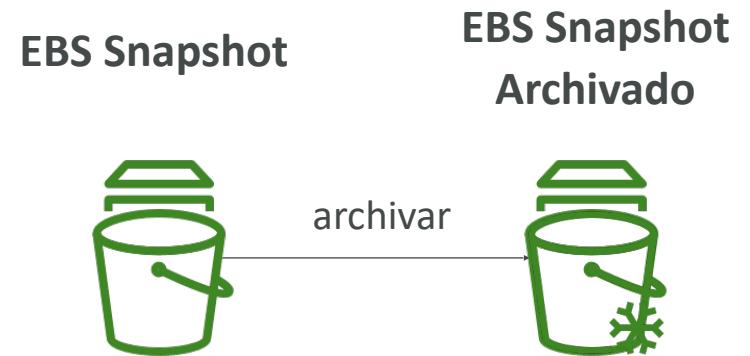
Haz una copia de seguridad (snapshot) de tu volumen EBS en un momento dado
No es necesario separar el volumen para hacer la instantánea, pero se recomienda
Puedes copiar las instantáneas a través de AZ o Región



Características de los Snapshots de EBS

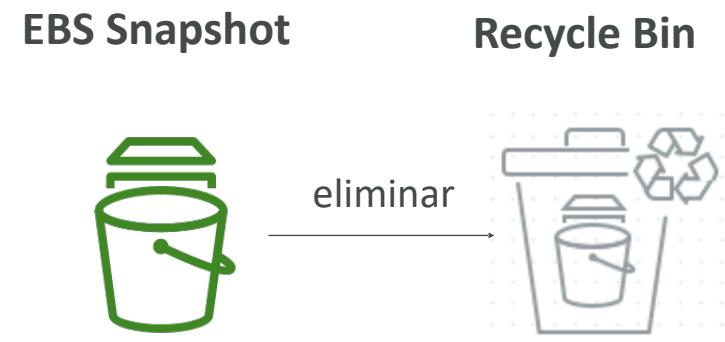
• Archivo de Snapshots de EBS

- Mover un snapshot a un "nivel de archivo" que es un 75% más barato
- La restauración del archivo tarda entre 24 y 72 horas



• Papelera de reciclaje para Snapshots EBS

- Configura reglas para retener los snapshots eliminados para poder recuperarlos después de un borrado accidental
- Especifica la retención (de 1 día a 1 año)





Visión general de AMI

- AMI = Amazon Machine Image
- Las AMI son una **personalización** de una instancia EC2
 - Añades tu propio software, configuración, sistema operativo, monitorización...
 - Tiempo de arranque/configuración más rápido porque todo el software está preempaquetado
- Las AMI se construyen para una **región específica** (y pueden copiarse entre regiones)
- Puedes lanzar instancias EC2 desde:
 - **Una AMI pública:** proporcionada por AWS
 - **Tu propia AMI:** la creas y la mantienes tú mismo
 - **Una AMI de AWS Marketplace:** una AMI hecha por otra persona (y potencialmente vendida)

Proceso AMI (desde una instancia EC2)

- Iniciar una instancia EC2 y personalizarla
- Detener la instancia (para la integridad de los datos)
- Construir una AMI - esto también creará instantáneas de EBS
- Lanzar instancias desde otras AMIs

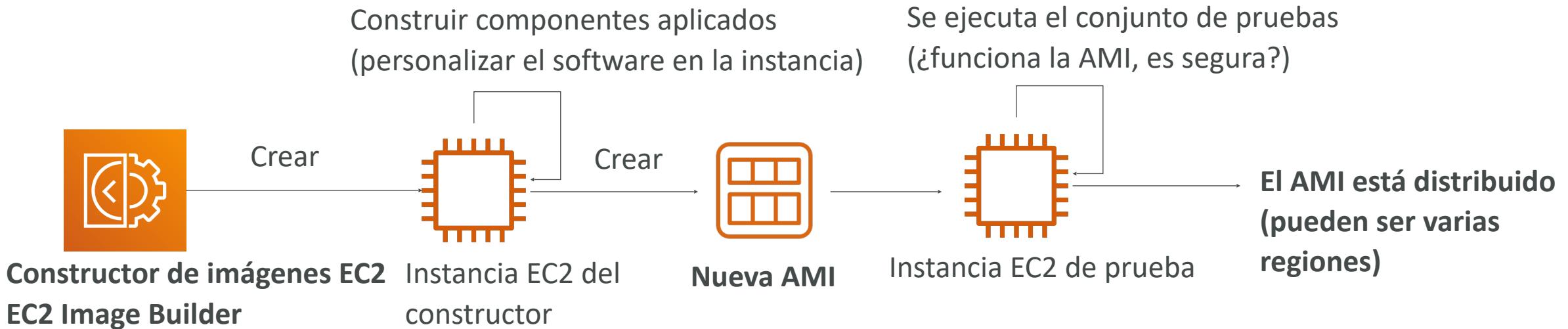


Constructor de imágenes EC2

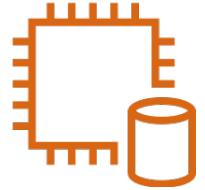
EC2 Image Builder



- Se utiliza para automatizar la creación de máquinas virtuales o imágenes de contenedores
- => Automatizar la creación, mantener, validar y probar las **AMIs de EC2**
- Puede ejecutarse de forma programada (semanalmente, cada vez que se actualizan los paquetes, etc...)
- Servicio gratuito (sólo se paga por los recursos subyacentes)



Almacén de instancias EC2



- Los volúmenes EBS son **unidades de red** con un rendimiento bueno pero “limitado”
- **Si necesitas un disco de hardware de alto rendimiento, utilizas EC2 Instance Store**

- Mejor rendimiento de E/S
- Los almacenes de instancias EC2 pierden su almacenamiento si se detienen (son efímeros)
- Bueno para el buffer / cache / datos de memoria virtual / contenido temporal
- Riesgo de pérdida de datos si el hardware falla
- Las copias de seguridad y la replicación son responsabilidad tuya

Almacén local de instancias EC2

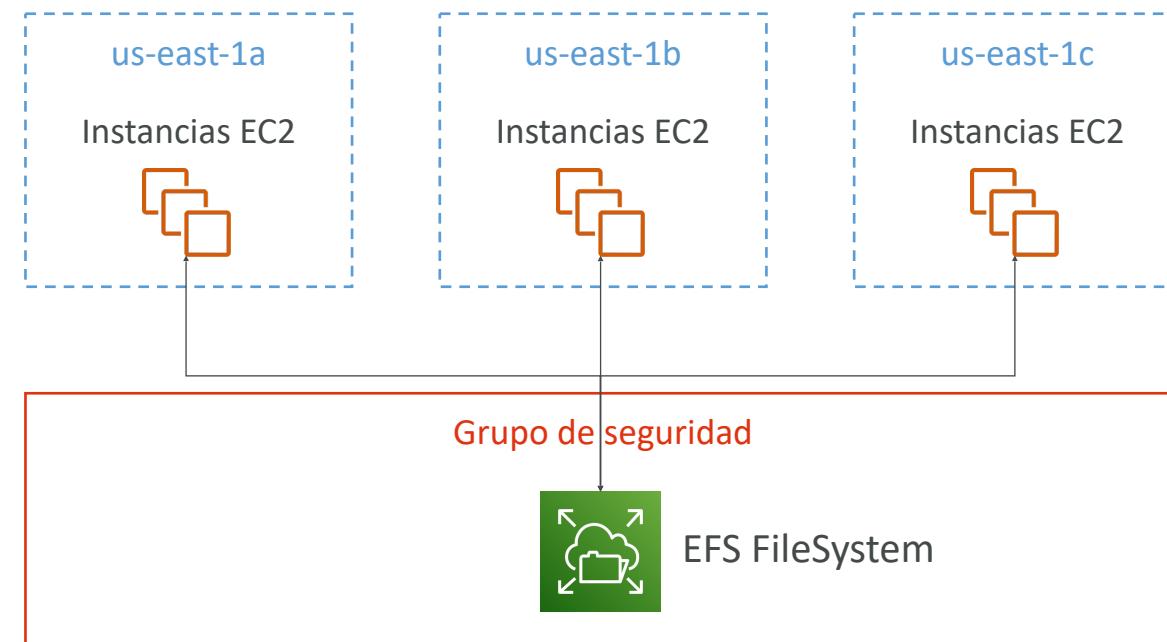
Instance Size	100% Random Read IOPS	Write IOPS
i3.large *	100,125	35,000
i3.xlarge *	206,250	70,000
i3.2xlarge	412,500	180,000
i3.4xlarge	825,000	360,000
i3.8xlarge	1.65 million	720,000
i3.16xlarge	3.3 million	1.4 million
i3.metal	3.3 million	1.4 million
i3en.large *	42,500	32,500
i3en.xlarge *	85,000	65,000
i3en.2xlarge *	170,000	130,000
i3en.3xlarge	250,000	200,000
i3en.6xlarge	500,000	400,000
i3en.12xlarge	1 million	800,000
i3en.24xlarge	2 million	1.6 million
i3en.metal	2 million	1.6 million

IOPS muy altas

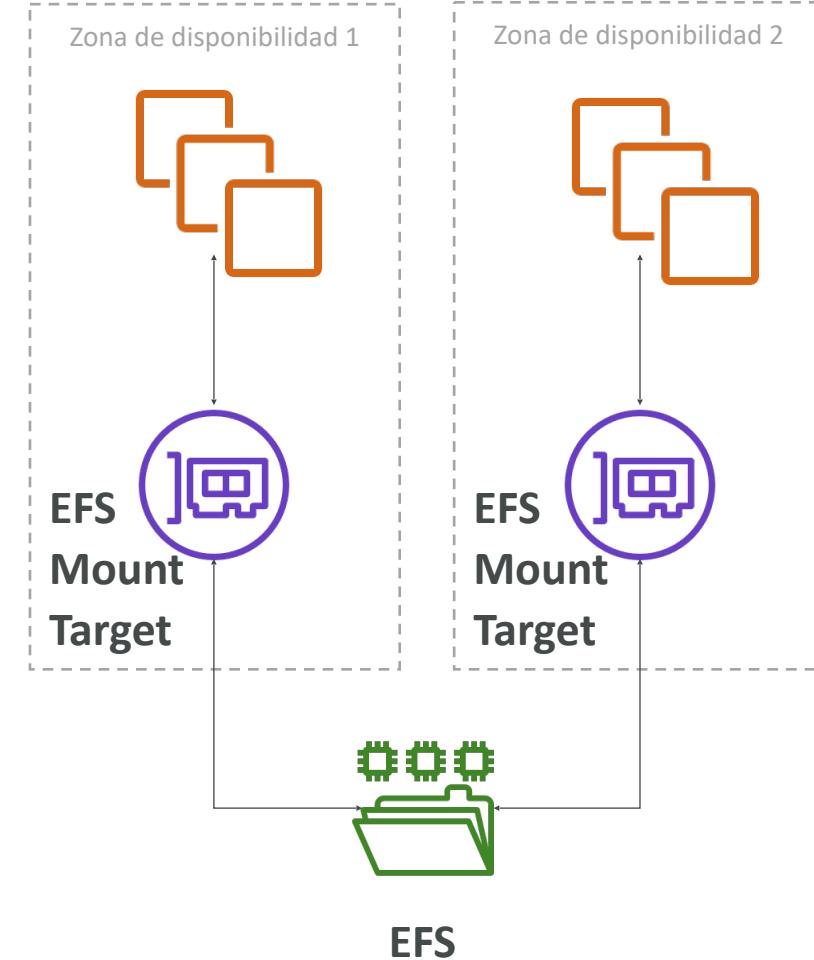
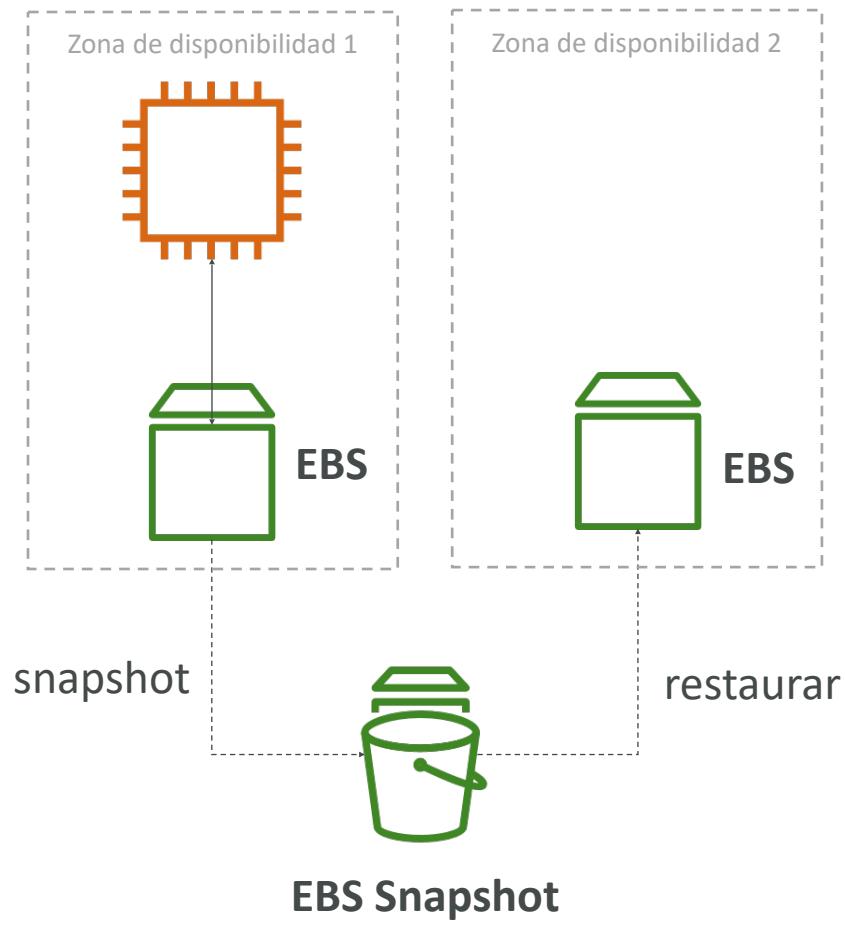
EFS – Elastic File System



- NFS (network file system / sistema de archivos de red) gestionado que **puede montarse en 100 EC2s**
- EFS funciona con instancias EC2 de **Linux** en **multi-AZ**
- Alta disponibilidad, escalable, caro (3x gp2), pago por uso, sin planificación de capacidad

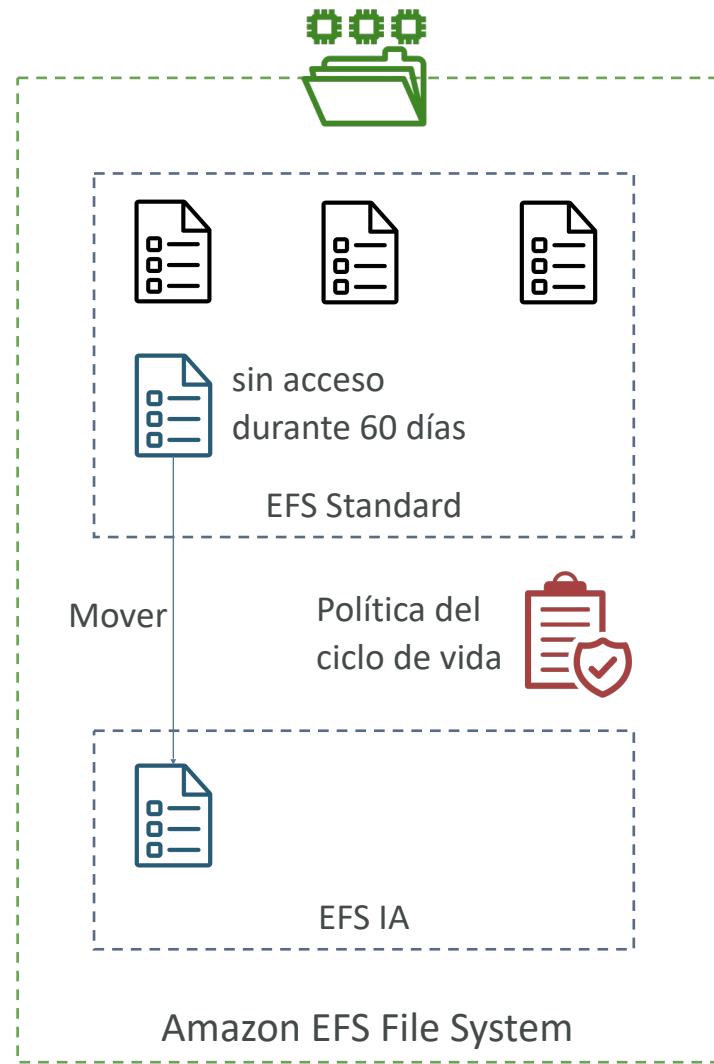


EBS vs EFS



EFS Infrequent Access (EFS-IA)

- **Clase de almacenamiento** con costes optimizados para los archivos a los que no se accedes a diario
- Hasta un 92% menos de coste en comparación con EFS Standard
- EFS moverá automáticamente tus archivos a EFS-IA basándose en la última vez que se accedió a ellos
- Habilita EFS-IA con una política de ciclo de vida (Lifecycle Policy)
- Ejemplo: mover a EFS-IA los archivos a los que no se ha accedido en 60 días
- Transparente para las aplicaciones que acceden a EFS



Modelo de responsabilidad compartida para el almacenamiento de EC2



- Infraestructura
- Replicación de datos para volúmenes EBS y unidades EFS
- Sustitución de hardware defectuoso
- Asegurar que sus empleados no puedan acceder a tus datos
- Configuración de procedimientos de copia de seguridad / instantánea
- Configuración de la encriptación de datos
- Responsabilidad de los datos en las unidades
- Comprender el riesgo de utilizar EC2 Instance Store

Amazon FSx - Visión general



- **Lanzar sistemas de archivos de alto rendimiento de terceros en AWS**
- Servicio totalmente gestionado



FSx para Lustre



**FSx para
Windows File
Server**

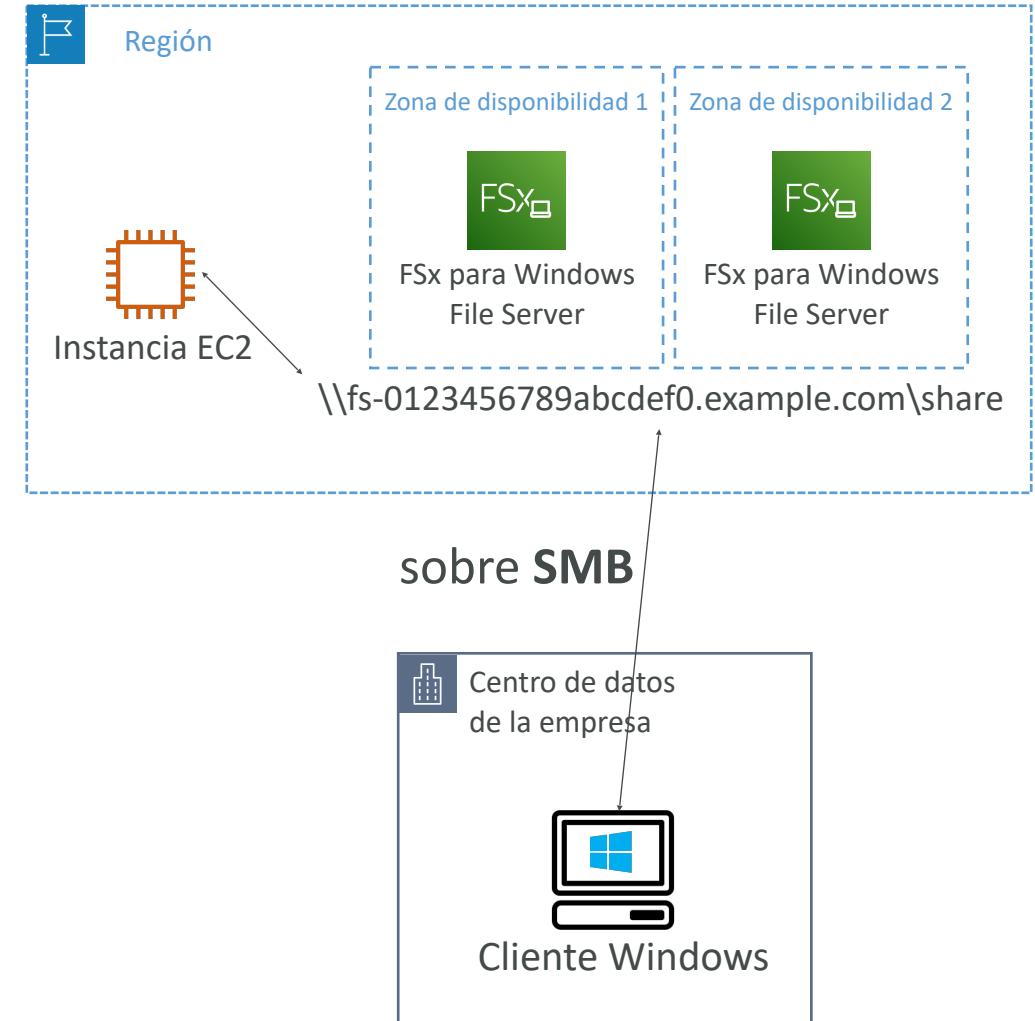


**Para
NetApp ONTAP**

Amazon FSx para Windows File Server



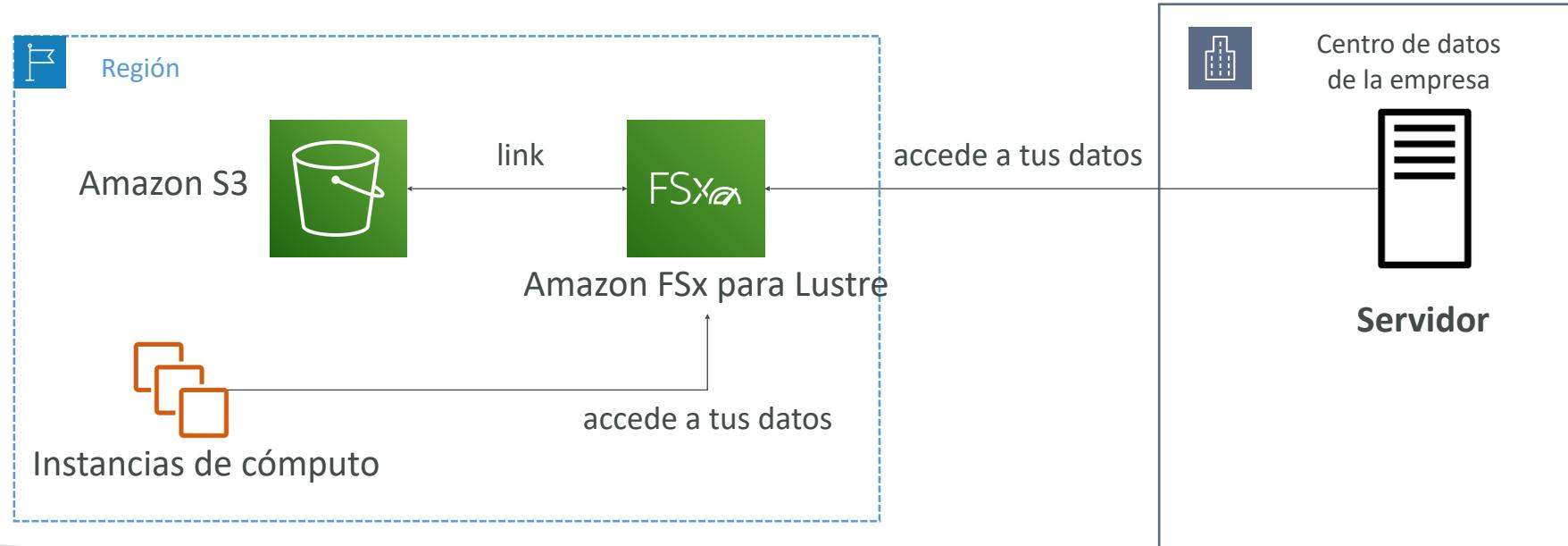
- Un sistema de archivos compartido **nativo de Windows** totalmente gestionado, altamente fiable y escalable
- Construido sobre **Windows File Server**
- Soporta el **protocolo SMB** y Windows NTFS
- Integrado con Microsoft Active Directory
- Se puede acceder desde AWS o desde tu infraestructura local



Amazon FSx para Lustre



- Un almacenamiento de archivos totalmente gestionado, de alto rendimiento y escalable para **High Performance Computing (HPC)**
- El nombre Lustre deriva de "Linux" y "cluster"
- Machine Learning, análisis, procesamiento de vídeo, modelado financiero, ...
- Escala hasta 100s GB/s, millones de IOPS, latencias sub-ms



Resumen - Almacenamiento de instancias EC2

- **Volúmenes EBS:**
 - Unidades de red adjuntas a una instancia EC2 a la vez
 - Asignados a una zona de disponibilidad
 - Puede utilizar EBS Snapshots para copias de seguridad / transferir volúmenes EBS a través de AZ
- **AMI:** crea instancias EC2 listas para usar con nuestras personalizaciones
- **EC2 Image Builder:** construye, prueba y distribuye automáticamente AMIs
- **EC2 Instance Store:**
 - Disco de hardware de alto rendimiento unido a nuestra instancia EC2
 - Se pierde si nuestra instancia se detiene / termina
- **EFS:** sistema de archivos en red, se puede adjuntar a 100s de instancias en una región
- **EFS-IA:** clase de almacenamiento de coste optimizado para archivos de acceso poco frecuente
- **FSx para Windows:** sistema de archivos en red para servidores Windows
- **FSx para Lustre:** sistema de archivos Linux de alto rendimiento informático

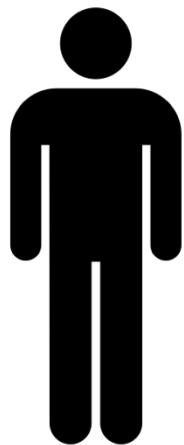
Elastic Load Balancing y Auto Scaling Groups

Escalabilidad y alta disponibilidad

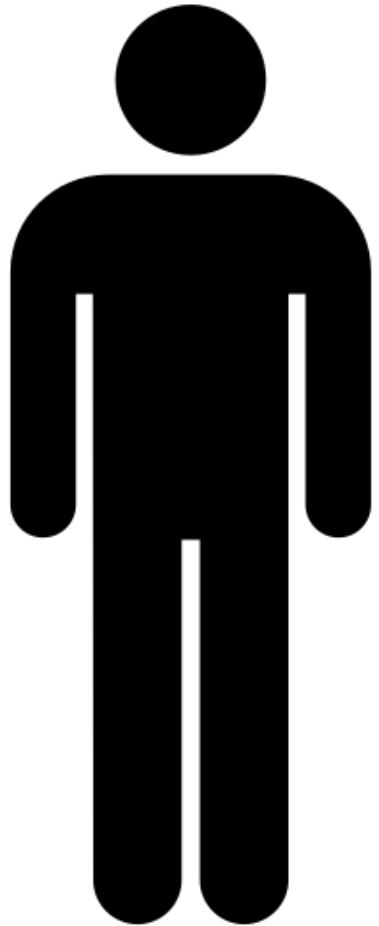
- La escalabilidad significa que una aplicación/sistema puede manejar mayores cargas adaptándose.
- Hay dos tipos de escalabilidad:
 - Escalabilidad vertical
 - Escalabilidad horizontal (= elasticidad)
- **La escalabilidad está vinculada pero es diferente a la alta disponibilidad**

Escalabilidad vertical

- La escalabilidad vertical significa aumentar el tamaño de la instancia
- Por ejemplo, tu aplicación se ejecuta en una instancia t2.micro
- Escalar esa aplicación verticalmente significa ejecutarla en una instancia t2.large
- La escalabilidad vertical es muy común para sistemas no distribuidos, como una base de datos
- Por lo general, hay un límite en cuanto a lo que se puede escalar verticalmente (límite de hardware)



operador junior

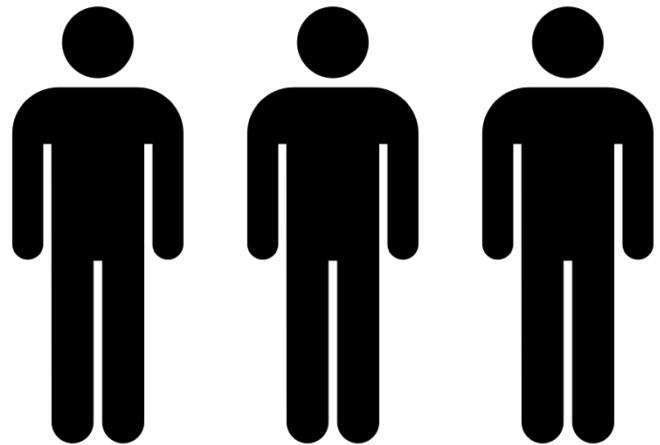
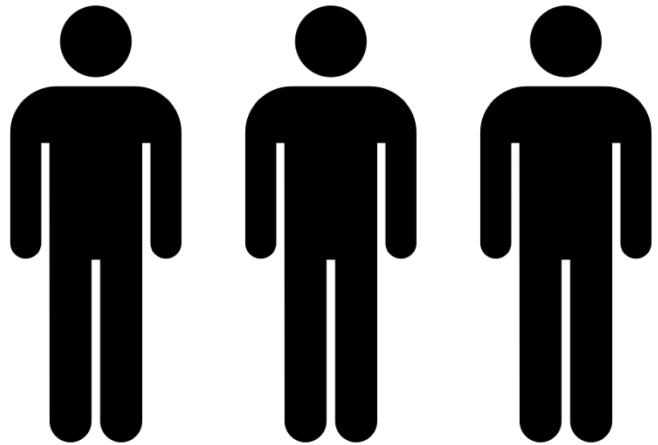


operador senior

Escalabilidad horizontal

- Escalabilidad horizontal significa aumentar el número de instancias / sistemas para la aplicación
- El escalado horizontal implica sistemas distribuidos.
- Esto es muy común para las aplicaciones web / aplicaciones modernas
- Es fácil escalar horizontalmente gracias a las ofertas en el Cloud como Amazon EC2

operador operador operador



operador operador operador

Alta disponibilidad

- La alta disponibilidad suele ir de la mano del escalado horizontal
- Alta disponibilidad significa ejecutar la aplicación / sistema en al menos 2 zonas de disponibilidad
- El objetivo de la alta disponibilidad es sobrevivir a la pérdida del centro de datos (desastre)



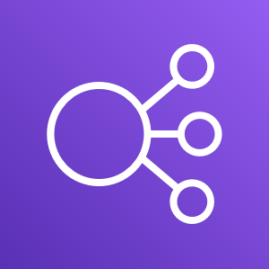
Alta disponibilidad y escalabilidad para EC2

- Escalado vertical: Aumentar el tamaño de la instancia (= escalar hacia arriba / abajo)
 - Desde: t2.nano - 0.5G de RAM, 1 vCPU
 - A: u-12tb1.metal - 12,3 TB de RAM, 448 vCPUs
- Escalado horizontal: Aumentar el número de instancias (= escalado hacia fuera / hacia dentro)
 - Auto Scaling Group
 - Load Balancer
- Alta disponibilidad: Ejecutar instancias para la misma aplicación a través de múltiples AZ
 - Auto Scaling Group multi AZ
 - Load Balancer multi AZ

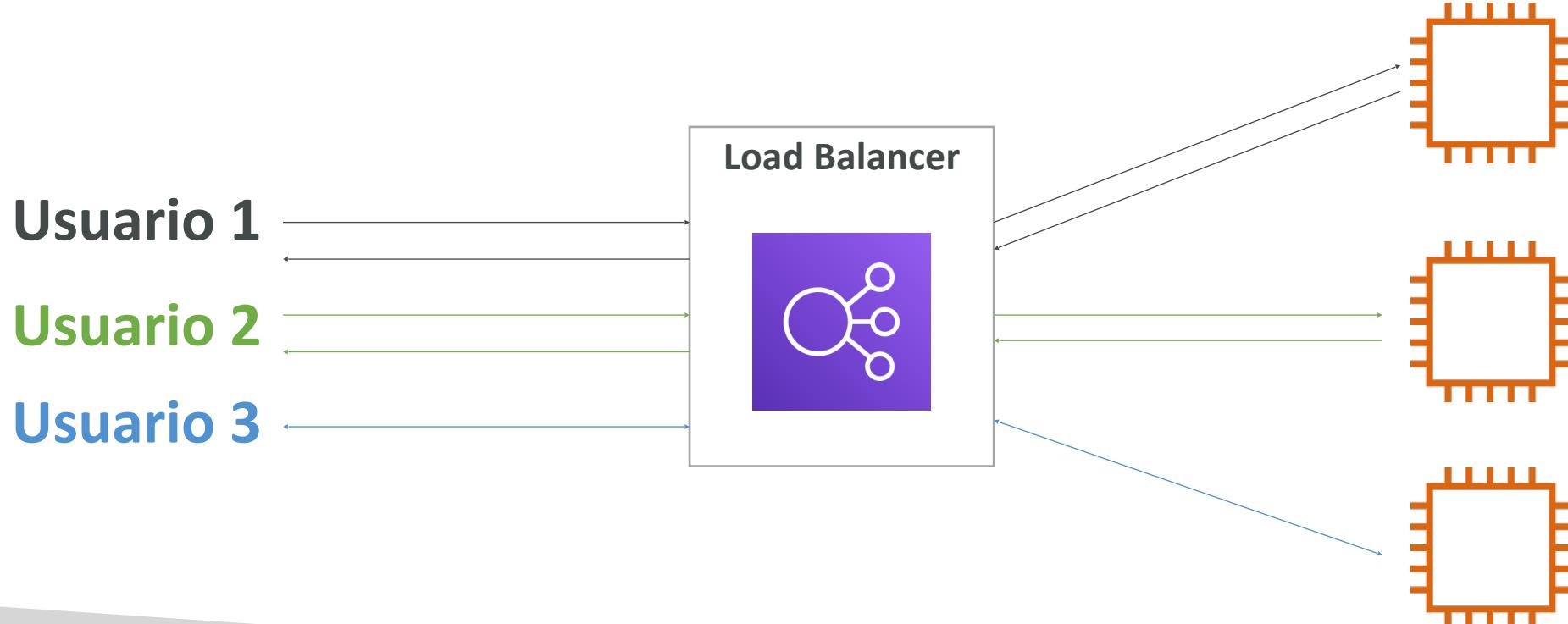
Escalabilidad vs. Elasticidad (vs. Agilidad)

- **Escalabilidad:** capacidad de acomodar una mayor carga reforzando el hardware (scale up), o añadiendo nodos (scale out)
- **Elasticidad:** una vez que un sistema es escalable, la elasticidad significa que habrá cierto "autoescalado" para que el sistema pueda escalar en función de la carga. Esto es "amigable con el Cloud": pago por uso, adecuación a la demanda, optimización de costes
- **Agilidad:** (no relacionado con la escalabilidad - distractor) los nuevos recursos de IT están a un clic de distancia, lo que significa que se reduce el tiempo para poner esos recursos a disposición de los desarrolladores de semanas a sólo minutos

¿Qué es el load balancing?



- Los Load Balancers (equilibradores de carga) son servidores que reenvían el tráfico de Internet a múltiples servidores (Instancias EC2) en sentido descendente



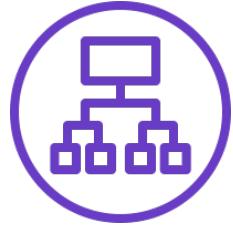
¿Por qué utilizar un Load Balancer?

- Distribuir la carga entre múltiples instancias descendentes
- Exponer un único punto de acceso (DNS) en tu aplicación
- Manejar sin problemas los fallos de las instancias descendentes
- Realiza comprobaciones periódicas del estado de tus instancias
- Proporcionar terminación SSL (HTTPS) para tus sitios web
- Alta disponibilidad entre zonas

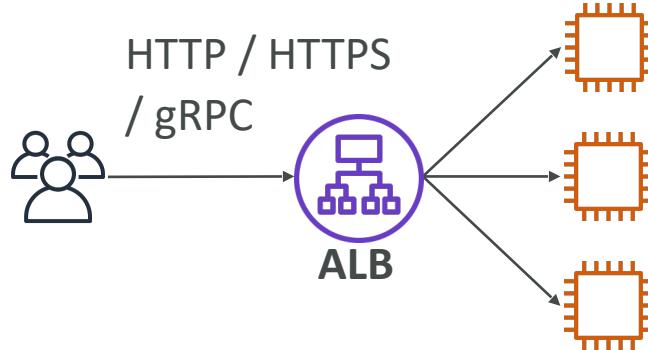
¿Por qué utilizar un Elastic Load Balancer (ELB)?

- Un ELB (Elastic Load Balancer) es un **Load Balancer (equilibrador de carga) gestionado**
 - AWS garantiza su funcionamiento
 - AWS se encarga de las actualizaciones, el mantenimiento y la alta disponibilidad
 - AWS sólo proporciona unos pocos controles de configuración
- Cuesta menos configurar tu propio Load Balancer pero te supondrá mucho más esfuerzo (mantenimiento, integraciones)
- Varios tipos de Load Balancer ofrecidos por AWS:
 - Application Load Balancer (sólo HTTP / HTTPS) - Capa 7
 - Network Load Balancer (rendimiento ultra alto, permite TCP) - Capa 4
 - Gateway Load Balancer - Capa 3
 - Classic Load Balancer (retirado en 2023) - Capa 4 y 7

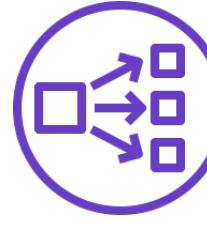
Application Load Balancer



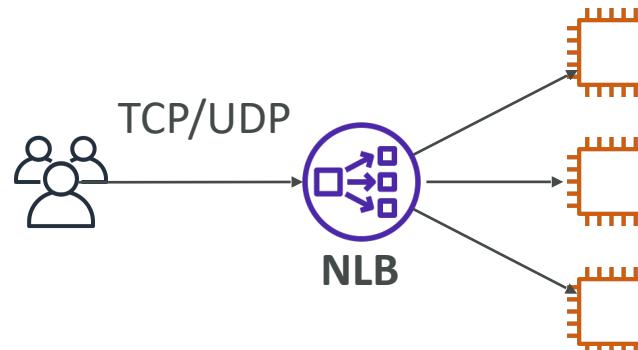
- **Protocolos HTTP / HTTPS / gRPC (Capa 7)**
- Funciones de **enrutamiento HTTP**
- **DNS estático (URL)**



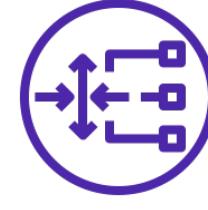
Network Load Balancer



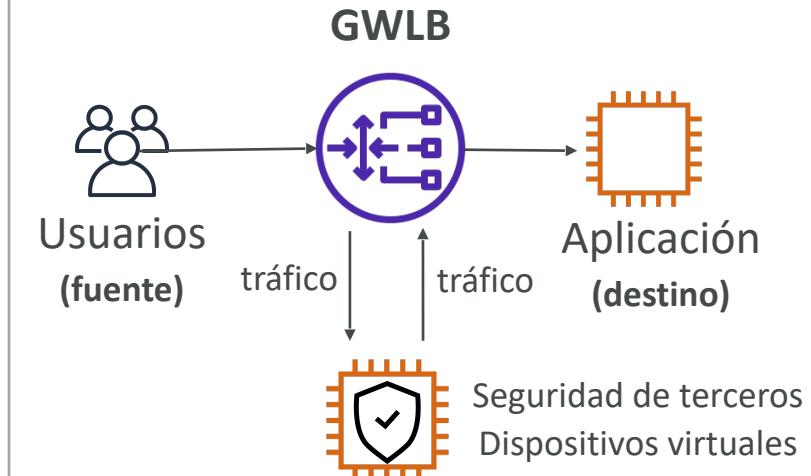
- **Protocolos TCP / UDP (Capa 4)**
- **Alto rendimiento:** millones de peticiones por segundo
- **IP estática** a través de IP elástica



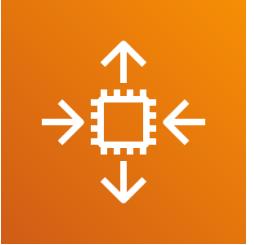
Gateway Load Balancer



- Protocolo GENEVE en paquetes IP (Capa 3)
- **Enrutar el tráfico a los firewalls** que gestionas en las instancias EC2
- **Detección de intrusos**



¿Qué es un Auto Scaling Group?

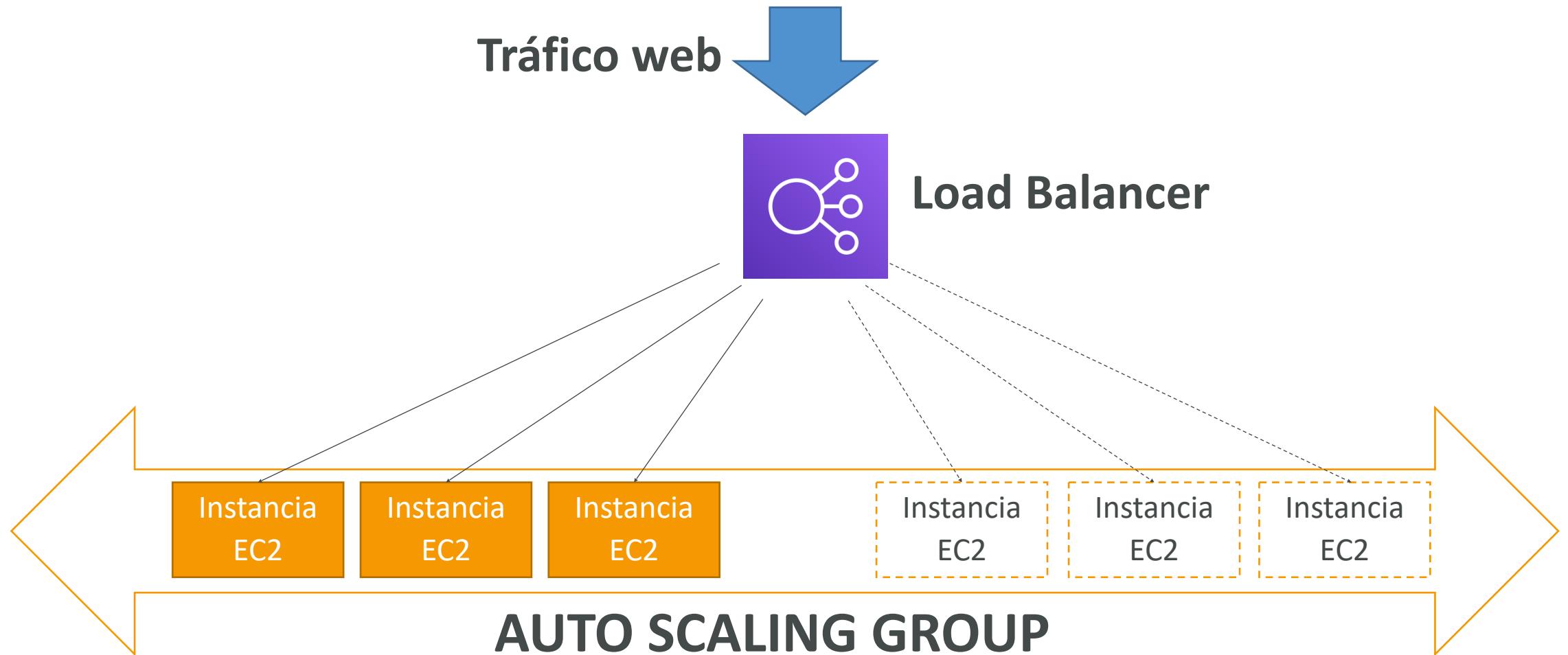


- En la vida real, la carga de tus sitios web y aplicaciones puede cambiar
- En el Cloud, puedes crear y deshacerte de servidores muy rápidamente
- El objetivo de un Auto Scaling Group (ASG) es:
 - Escalar para fuera (añadir instancias de EC2) para adaptarse a un aumento de la carga
 - Escalar para dentro (eliminar instancias EC2) para que coincida con una disminución de la carga
 - Asegurar que tenemos un número mínimo y máximo de máquinas en funcionamiento
 - Registrar automáticamente nuevas instancias en un Load Balancer
 - Reemplazar las instancias en mal estado
- Ahorro de costes: sólo se ejecuta a una capacidad óptima (principio del Cloud)

Auto Scaling Group (ASG) en AWS



Auto Scaling Group en AWS con Load Balancer



Auto Scaling Groups – Estrategias de escalado

- **Escalado manual:** Actualizar el tamaño de un ASG manualmente
- **Escalado dinámico:** Responde a los cambios en la demanda
 - **Escalado simple / por pasos**
 - Cuando se activa una alarma de CloudWatch (por ejemplo, CPU > 70%), se añaden 2 unidades
 - Cuando se dispara una alarma de CloudWatch (ejemplo CPU < 30%), entonces se elimina 1
 - **Escalado de seguimiento de objetivos**
 - Ejemplo: Quiero que la media de la CPU de ASG se mantenga en torno al 40%
 - **Escalado programado**
 - Anticipar un escalado basado en patrones de uso conocidos
 - Ejemplo: aumentar la capacidad mínima a 10 a las 17 horas de los viernes

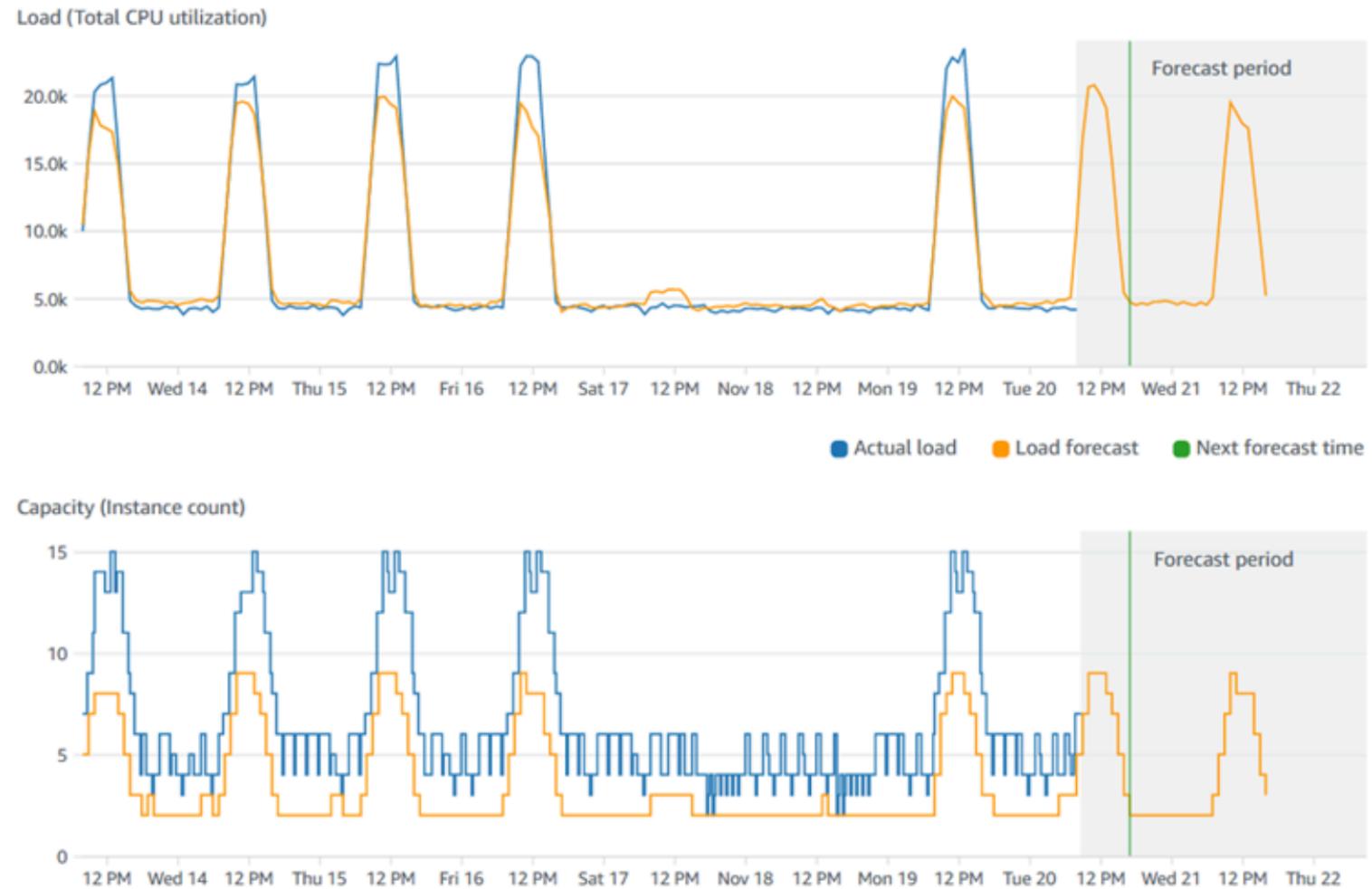
Auto Scaling Groups – Estrategias de escalado

- **Escalado predictivo**

- Utiliza el Machine Learning para predecir el tráfico futuro con antelación

- Aprovisiona automáticamente el número correcto de instancias EC2 por adelantado

- Útil cuando tu carga tiene patrones predecibles basados en el tiempo



Resumen - ELB y ASG

- **Alta disponibilidad vs escalabilidad** (vertical y horizontal) vs **elasticidad** vs **agilidad** en el Cloud
- **Elastic Load Balancers (ELB)**
 - Distribuyen el tráfico entre las instancias EC2 del backend, pueden ser Multi-AZ
 - Soporta chequeos de salud
 - 4 tipos: Classic (antiguo), Application (HTTP - L7), Network (TCP - L4), Gateway (L3)
- **Auto Scaling Groups (ASG)**
 - Implementa la elasticidad para tu aplicación, a través de múltiples AZ
 - Escala las instancias EC2 en función de la demanda de tu sistema, sustituye las instancias en mal estado
 - Integrado con el ELB

Amazon S3

Introducción de la sección



- Amazon S3 es uno de los principales bloques de construcción de AWS
- Se anuncia como almacenamiento de "escala infinita".
- Muchos sitios web utilizan Amazon S3 como columna vertebral
- Muchos servicios de AWS utilizan Amazon S3 como una integración también
- Tendremos una aproximación paso a paso a S3
- El examen CCP requiere un conocimiento "más profundo" sobre S3

S3 Casos de uso

- Copia de seguridad y almacenamiento
- Recuperación de desastres
- Almacenamiento en el Cloud híbrido
- Alojamiento de aplicaciones
- Alojamiento de medios
- Data Lakes y análisis de big data
- Entrega de software
- Sitio web estático



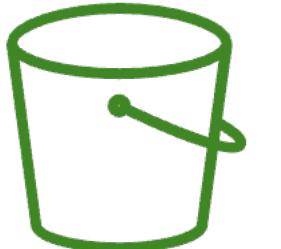
Nasdaq almacena 7 años de datos en S3 Glacier



Sysco analiza sus datos y obtiene información comercial

Amazon S3 - Buckets

- Amazon S3 permite almacenar objetos (archivos) en "buckets" (directorios)
- Los buckets deben tener un **nombre único global (en todas las regiones y todas las cuentas)**
- Los buckets se definen a nivel de región
- S3 parece un servicio global, pero los buckets se crean en una región
- Convención de nombres
 - Sin mayúsculas, sin guión bajo
 - De 3 a 63 caracteres
 - No es una IP
 - Debe empezar por letra minúscula o número
 - NO debe empezar por el prefijo **xn--**
 - NO debe terminar con el sufijo **-s3alias**



Bucket S3

Amazon S3 - Objetos

- Los objetos (archivos) tienen una clave
- La **clave** es la ruta **COMPLETA**:
 - s3://mi-bucket/mi-archivo.txt
 - s3://mi-bucket/mi_carpetal/otra_carpetal/mi-archivo.txt
- La clave se compone de **prefijo** + nombre del objeto
 - s3://mi-bucket/mi_carpetal/otra_carpetal/mi-archivo.txt
- No existe el concepto de "directorios" dentro de los buckets (aunque la interfaz de usuario te hará pensar lo contrario)

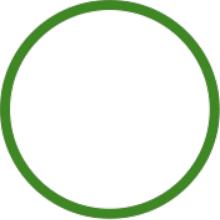


Objeto



Bucket S3 con
objetos

Amazon S3 - Objetos (cont.)



- Los valores de los objetos son el contenido del cuerpo:
 - Max. Tamaño del objeto es 5TB (5000GB)
 - Si subes más de 5GB, debes utilizar "subida multiparte"
- Metadatos (lista de pares clave / valor de texto - metadatos del sistema o del usuario)
- Etiquetas (par clave / valor - hasta 10) - útil para la seguridad / ciclo de vida
- ID de versión (si está activado el versionado)

Seguridad S3

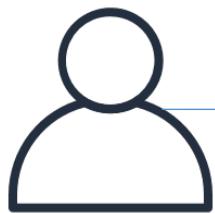
- **Basada en el usuario**
 - **Políticas IAM** - qué llamadas a la API deben permitirse a un usuario concreto desde IAM
- **Basada en recursos**
 - **Políticas de bucket** - reglas para todo el bucket desde la consola de S3 - permite cuentas cruzadas
 - **Lista de control de acceso a objetos (ACL)** - nivel de detalle profundo (puede desactivarse)
 - **Lista de control de acceso a bucket (ACL)** - menos común (puede desactivarse)
- **Nota:** un usuario IAM puede acceder a un objeto S3 si
 - Los permisos IAM del usuario LO PERMITEN \sqcap la política de recursos LO PERMITE
 - \sqcup no hay una DENEGACIÓN explícita
- **Cifrado:** cifra objetos en Amazon S3 utilizando claves de cifrado

Políticas de bucket S3

- Políticas basadas en JSON
 - Resource: buckets y objetos
 - Effect: permitir (Allow) o denegar (Deny)
 - Action: conjunto de API a permitir o denegar
 - Principal: la cuenta o usuario al que aplicar la política
- Utilizar una política de bucket S3 para:
 - Conceder acceso público al bucket
 - Forzar que los objetos se cifren al subirlos
 - Conceder acceso a otra cuenta (cuenta cruzada)

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "PublicRead",  
      "Effect": "Allow",  
      "Principal": "*",  
      "Action": [  
        "s3:GetObject"  
      ],  
      "Resource": [  
        "arn:aws:s3:::examplebucket/*"  
      ]  
    }  
  ]  
}
```

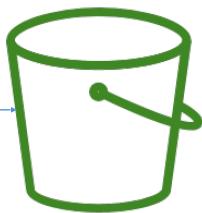
Ejemplo: Acceso público - Política de uso de bucket



Visitante anónimo del sitio web www

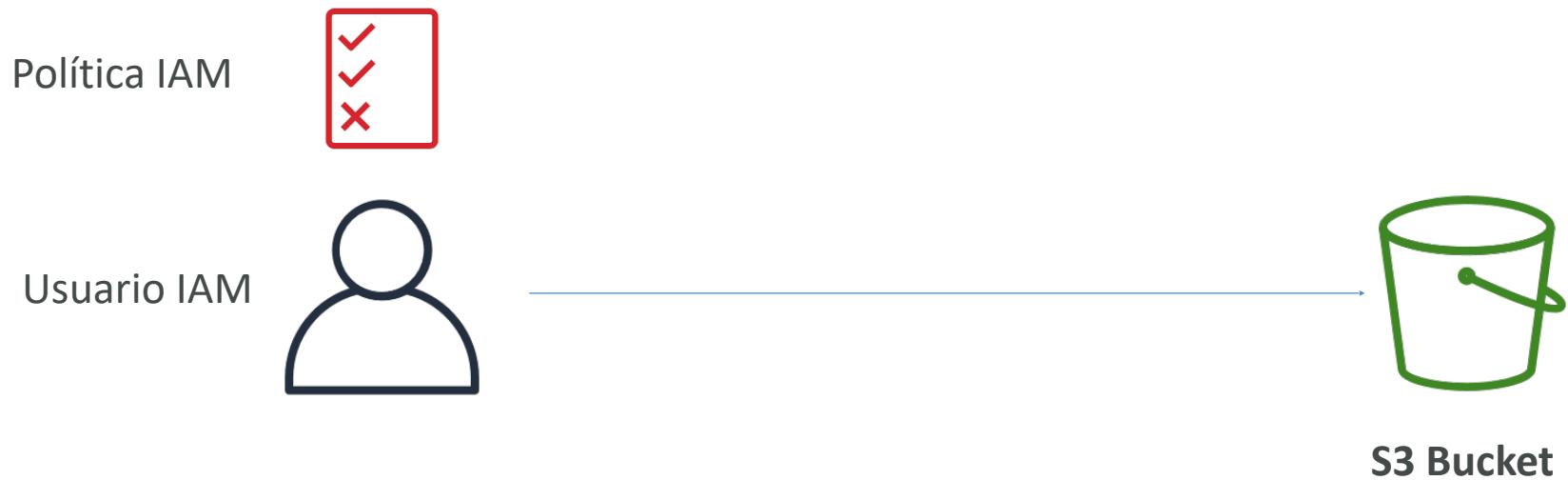


Política de bucket S3
Permite el acceso al público

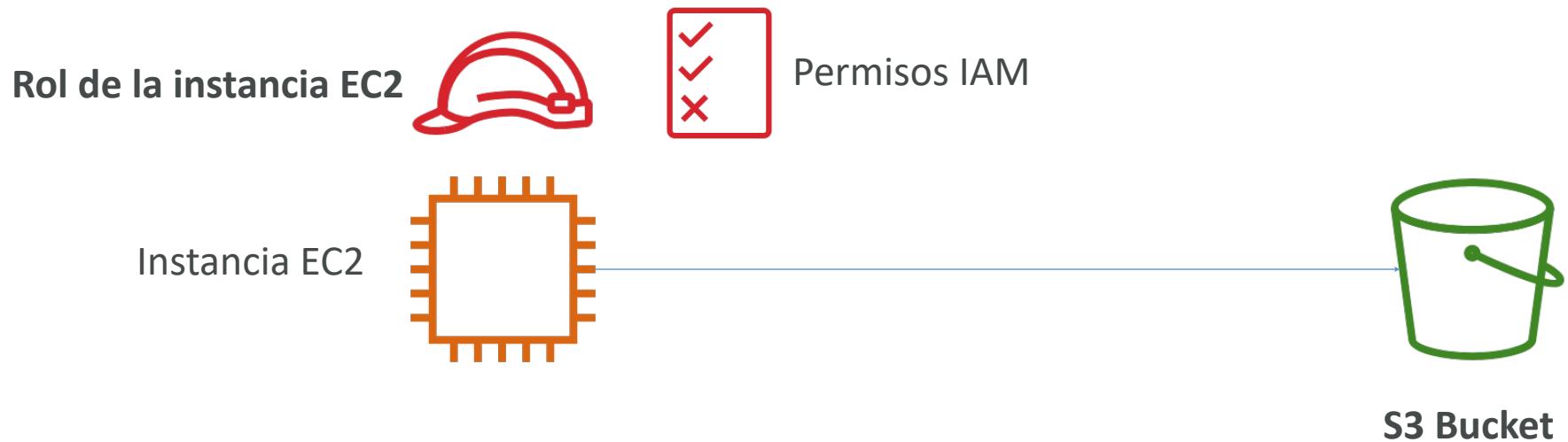


S3 Bucket

Ejemplo: Acceso del usuario al S3 - Permisos IAM



Ejemplo: Acceso de la instancia EC2 - Utilizar roles IAM



Avanzado: Acceso entre cuentas

Uso de la política de bucket

Usuario IAM
Otra cuenta de AWS

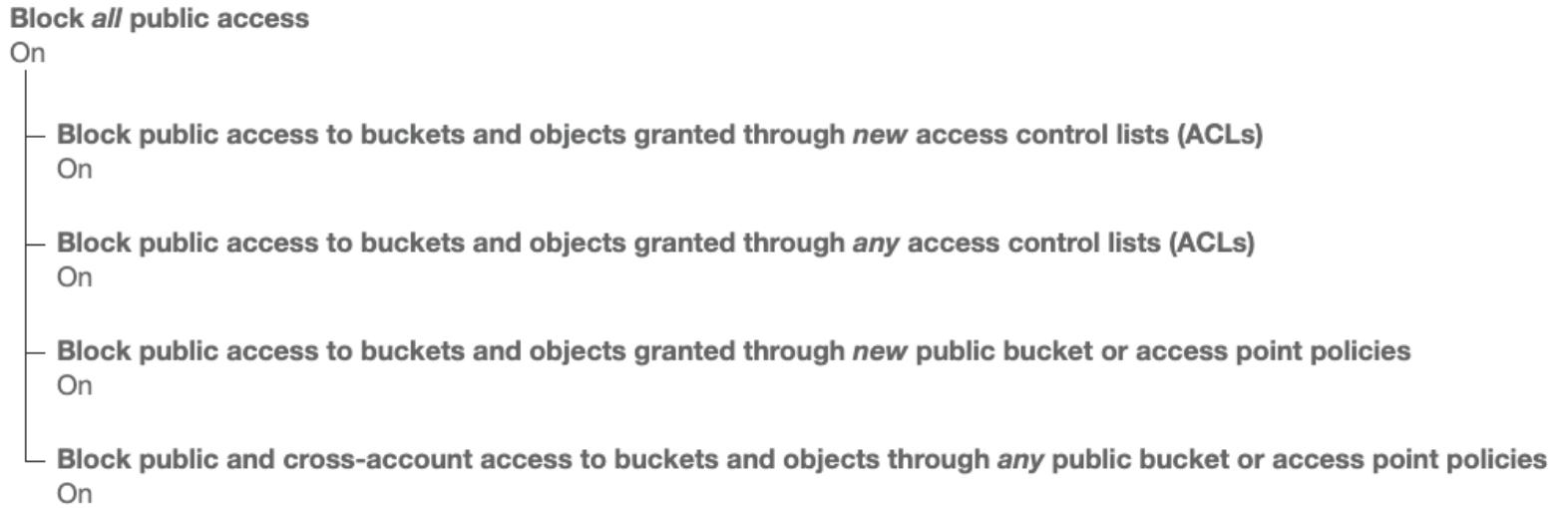


Política de bucket S3
Permite las cuentas cruzadas



S3 Bucket

Configuración del bucket para bloquear el acceso público



- **Estos ajustes se crearon para evitar la filtración de datos de la empresa**
- Si sabes que tu bucket no debe ser nunca público, déjalo activado
- Pueden establecerse a nivel de cuenta

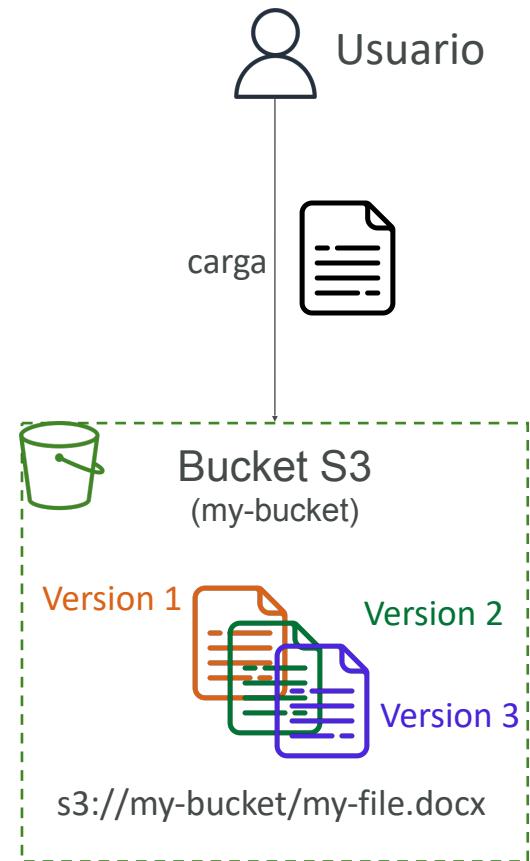
Amazon S3 - Alojamiento de sitios web estáticos

- S3 puede alojar sitios web estáticos y hacerlos accesibles en Internet
 - La URL del sitio web será (dependiendo de la región)
 - [http://bucket-name.s3-website-*aws-region*.amazonaws.com](http://bucket-name.s3-website-us-west-2.amazonaws.com)
 -
 - [http://bucket-name.s3-website.*aws-region*.amazonaws.com](http://bucket-name.s3-website.us-west-2.amazonaws.com)
 - Si recibes un error **403 Forbidden**, ¡asegúrate de que la política del bucket permite lecturas públicas!



Amazon S3 - Versionado

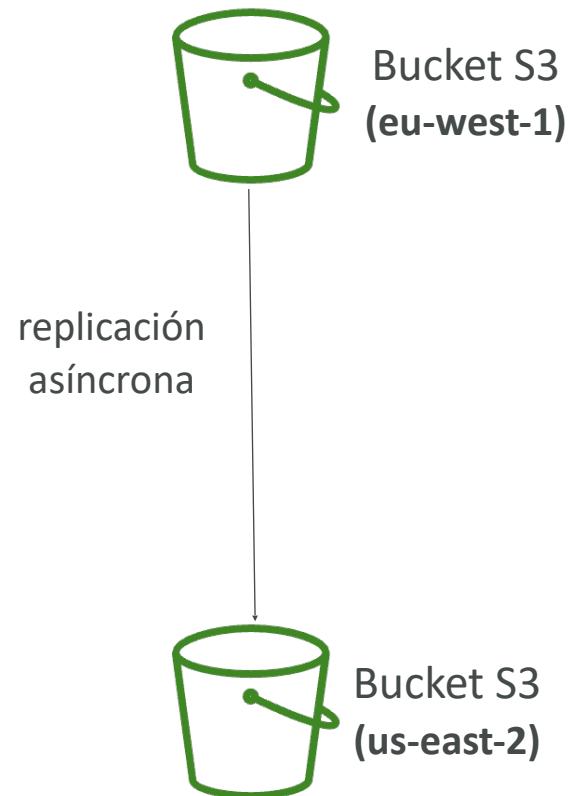
- Puedes versionar tus archivos en Amazon S3
- Se activa a **nivel de bucket**
- La misma clave de sobrescritura cambiará la "versión": 1, 2, 3....
- Es una buena práctica versionar tus buckets
 - Protege contra borrados involuntarios (posibilidad de restaurar una versión)
 - Rolling fácil a la versión anterior
- Nota:
 - Cualquier archivo que no esté versionado antes de activar el versionado tendrá la versión "nula".
 - Suspender el versionado no elimina las versiones anteriores



Amazon S3 – Replicación (CRR & SRR)



- Debes activar el **versionado** en los buckets de origen y destino
- **Replicación entre regiones (CRR)**
- **Replicación en la misma región (SRR)**
- Los buckets pueden estar en diferentes cuentas de AWS
- La copia es asíncrona
- Debes dar los permisos IAM adecuados a S3
- Casos de uso:
 - **CRR** - normativa, acceso de menor latencia, replicación entre cuentas
 - **SRR** - agregación de logs, replicación en vivo entre cuentas de producción y de test



Clases de almacenamiento S3

- Amazon S3 Standard - Uso general
- Amazon S3 Standard-Infrequent Access (IA)
- Amazon S3 One Zone-Infrequent Access
- Amazon S3 Glacier Instant Retrieval
- Amazon S3 Glacier Flexible Retrieval
- Amazon S3 Glacier Deep Archive
- Amazon S3 Intelligent Tiering
- Se puede pasar de una clase a otra manualmente o utilizando las configuraciones del ciclo de vida de S3

S3 Durabilidad y disponibilidad

- Durabilidad:
 - Alta durabilidad (99,99999999%, 11 9's) de los objetos a través de múltiples AZ
 - Si almacenas 10.000.000 de objetos con Amazon S3, puedes esperar una media de pérdida de un solo objeto una vez cada 10.000 años
 - Lo mismo para todas las clases de almacenamiento
- Disponibilidad:
 - Mide la disponibilidad de un servicio
 - Varía en función de la clase de almacenamiento
 - Ejemplo: El estándar S3 tiene una disponibilidad del 99,99% = no está disponible 53 minutos al año

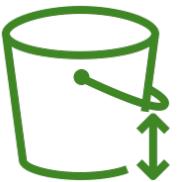
Standard S3 - Uso general



- Disponibilidad del 99,99%.
 - Se utiliza para datos de acceso frecuente
 - Baja latencia y alto rendimiento
 - Soporta 2 fallos concurrentes de la instalación
-
- Casos de uso: Análisis de Big Data, aplicaciones móviles y de juegos, distribución de contenidos...

Clases de almacenamiento S3 – Infrequent Access

- Clases de almacenamiento en S3
- Coste inferior al de S3 Standard
- **Amazon S3 Standard-Infrequent Access (S3 Standard-IA)**
 - Disponibilidad del 99,9%.
 - Casos de uso: Recuperación de desastres, copias de seguridad
- **Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)**
 - Alta durabilidad (99,99999999%) en una sola AZ; los datos se pierden cuando se destruye la AZ
 - Disponibilidad del 99,5%.
 - Casos de uso: Almacenamiento de copias de seguridad secundarias de datos locales, o de datos que puedes recrear



Clases de almacenamiento S3 – Amazon S3 Glacier

- Almacenamiento de objetos de bajo coste pensado para archivar / hacer copias de seguridad
- Precio: precio del almacenamiento + coste de recuperación del objeto
- **Amazon S3 Glacier Instant Retrieval**
 - Recuperación en milisegundos, ideal para datos a los que se accede una vez al trimestre
 - Duración mínima de almacenamiento de 90 días
- **Amazon S3 Glacier Flexible Retrieval** (antes Amazon S3 Glacier)
 - Acelerada (de 1 a 5 minutos), Estándar (de 3 a 5 horas), Masiva (de 5 a 12 horas) - gratis
 - Duración mínima de almacenamiento de 90 días
- **Amazon S3 Glacier Deep Archive - para almacenamiento a largo plazo:**
 - Estándar (12 horas), Masiva (48 horas)
 - Duración mínima de almacenamiento de 180 días





S3 Intelligent-Tiering

- Pequeña cuota mensual de monitorización y jerarquización automática
 - Mueve los objetos automáticamente entre los niveles de acceso en función del uso
 - No hay cargos por recuperación en S3 Intelligent-Tiering
-
- *Frequent Access tier (automático)*: nivel por defecto
 - *Infrequent Access tier (automático)*: objetos no accedidos durante 30 días
 - *Archive Instant Access tier (automático)*: objetos no accedidos durante 90 días
 - *Archive Access tier (opcional)*: configurable de 90 a más de 700 días
 - *Deep Archive Access tier (opcional)*: configurable de 180 días a 700+ días

Comparación de las clases de almacenamiento de S3

	Standard	Intelligent-Tiering	Standard-IA	One Zone-IA	Glacier Instant Retrieval	Glacier Flexible Retrieval	Glacier Deep Archive
Durabilidad	99.999999999% == (11 9's)						
Disponibilidad	99.99%	99.9%	99.9%	99.5%	99.9%	99.99%	99.99%
Acuerdo de nivel de servicio de disponibilidad	99.9%	99%	99%	99%	99%	99.9%	99.9%
Zonas de disponibilidad	>= 3	>= 3	>= 3	1	>= 3	>= 3	>= 3
Min. Duración del almacenamiento	Ninguno	Ninguno	30 Días	30 Días	90 Días	90 Días	180 Días
Min. Tamaño del objeto facturable	Ninguno	Ninguno	128 KB	128 KB	128 KB	40 KB	40 KB
Tasa de recuperación	Ninguno	Ninguno	Por GB recuperado	Por GB recuperado	Por GB recuperado	Por GB recuperado	Por GB recuperado

<https://aws.amazon.com/s3/storage-classes/>

Clases de almacenamiento S3 - Comparación de precios

Ejemplo: us-east-1

	Standard	Intelligent-Tiering	Standard-IA	One Zone-IA	Glacier Instant Retrieval	Glacier Flexible Retrieval	Glacier Deep Archive
Coste de almacenamiento (por GB al mes)	0.023\$	0.0025\$ - 0.023\$	%0.0125	0.01\$	0.004\$	0.0036\$	0.00099\$
Coste de recuperación (por cada 1000 solicitudes)	GET: 0.0004\$ POST: 0.005\$	GET: 0.0004\$ POST: 0.005\$	GET: 0.001\$ POST: 0.01\$	GET:\$0.001\$ POST: 0.01\$	GET: 0.01\$ POST: 0.02\$	GET: 0.0004\$ POST: 0.03\$ Expedited: 10\$ Standard: 0.05\$ Bulk: gratis	GET: 0.0004\$ POST: 0.05\$ Standard: 0.10\$ Bulk: 0.025\$
Tiempo de recuperación	Instantáneo					Expedited (1 – 5 mins) Standard (3 – 5 hours) Bulk (5 – 12 hours)	Standard (12 horas) Bulk (48 horas)
Coste de la monitorización (1000 objetos)		0.0025\$					

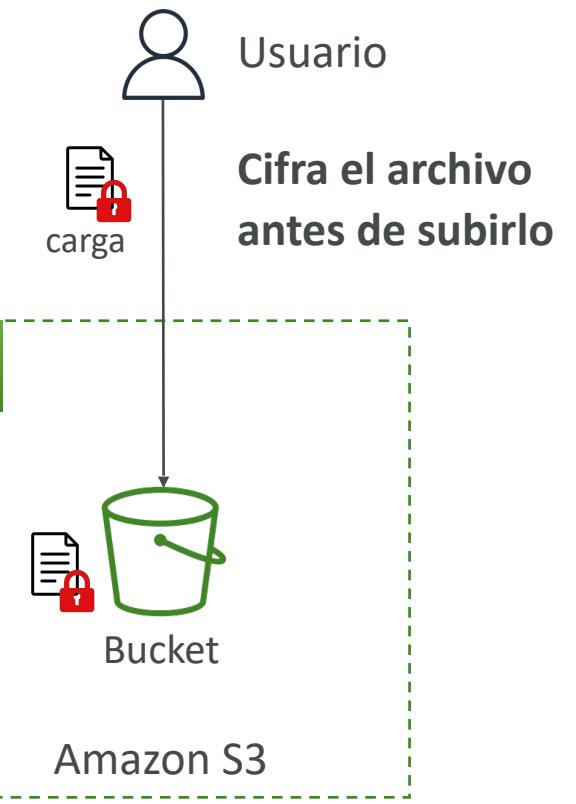
<https://aws.amazon.com/s3/pricing/>

Cifrado S3

Cifrado del lado del servidor (Por defecto)



Cifrado del lado del cliente



Modelo de Responsabilidad Compartida para S3



- Infraestructura (seguridad global, durabilidad, disponibilidad, sostener la pérdida concurrente de datos en dos instalaciones)
- Análisis de configuración y vulnerabilidad
- Validación de la normativa
- Versionado de S3
- Políticas de bucket S3
- Configuración de la replicación de S3
- Logs y monitorización
- Clases de almacenamiento de S3
- Encriptación de datos en reposo y en tránsito

Familia AWS Snow

- Dispositivos portátiles de alta seguridad para **recopilar, procesar datos, y migrar datos hacia y desde AWS**



Snowcone



Snowball Edge



Snowmobile

- **Migración de datos:**



Snowcone



Snowball Edge

- **Edge computing:**

Migraciones de datos con AWS Snow

	Tiempo de transferencia		
	100 Mbps	1Gbps	10Gbps
10 TB	12 días	30 horas	3 horas
100 TB	124 días	12 días	30 horas
1 PB	3 años	124 días	12 días

Desafíos:

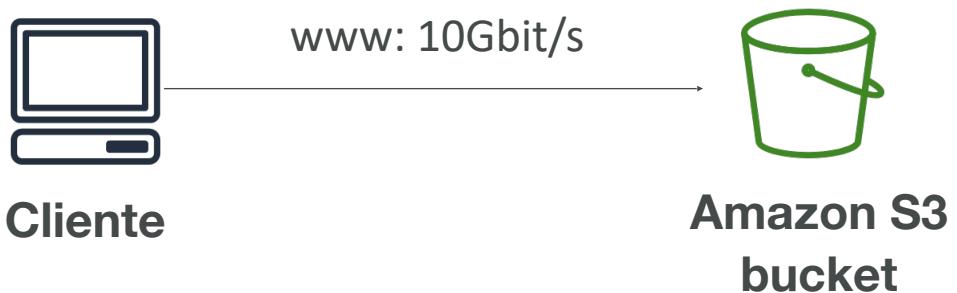
- Conectividad limitada
- Ancho de banda limitado
- Alto coste de la red
- Ancho de banda compartido
(no se puede maximizar la línea)
- Estabilidad de la conexión

Familia AWS Snow: dispositivos sin conexión para realizar migraciones de datos

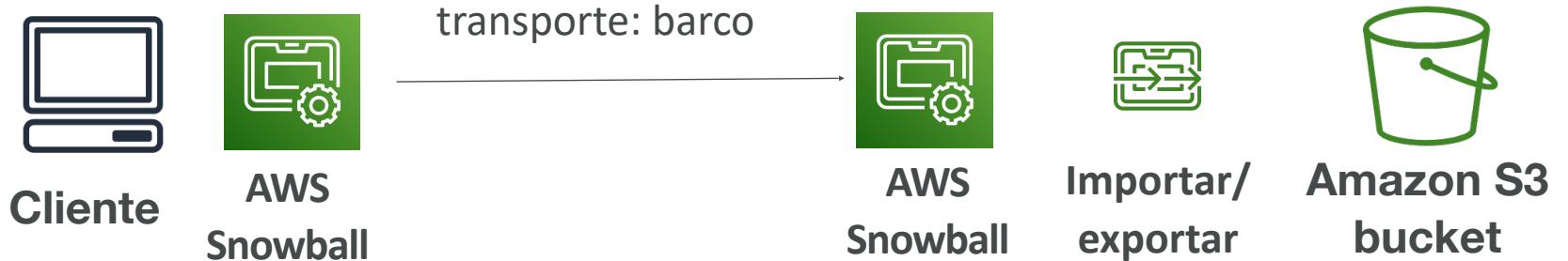
Si la transferencia a través de la red tarda más de una semana, ¡utiliza los dispositivos Snowball!

Diagramas

- Subida directa a S3:



- Con la Familia Snow:



Snowball Edge (para las transferencias de datos)



- Solución de transporte físico de datos: mover TBs o PBs de datos dentro o fuera de AWS
- Alternativa a mover datos a través de la red (y pagar tarifas de red)
- Paga por trabajo de transferencia de datos
- Proporciona almacenamiento de bloques y almacenamiento de objetos compatible con Amazon S3
- **Almacenamiento optimizado Snowball Edge**
 - 80 TB de capacidad de HDD para volumen de bloques y almacenamiento de objetos compatible con S3
- **Computación optimizada de Snowball Edge**
 - 42 TB de capacidad HDD o 28 TB de capacidad NVMe para volumen de bloques y almacenamiento de objetos compatible con S3
- Casos de uso: migraciones al Cloud de grandes volúmenes de datos, recuperación ante desastres



AWS Snowcone



- **Pequeño y portátil, en cualquier lugar, robusto y seguro, resiste entornos difíciles**
- Ligero (4,5 libras, 2,1 kg)
- Dispositivo utilizado para computación de borde, almacenamiento y transferencia de datos
- **Snowcone** - 8 TB de almacenamiento HDD
- **Snowcone SSD** - 14 TB de almacenamiento SSD
- Utiliza Snowcone donde no quepa Snowball (entorno con limitaciones de espacio)
- Debes proporcionar tu propia batería / cables
- Se puede enviar a AWS sin conexión, o conectarlo a internet y utilizar **AWS DataSync** para enviar los datos



AWS Snowmobile



- Transfiere exabytes de datos ($1 \text{ EB} = 1.000 \text{ PB} = 1.000.000 \text{ TBs}$)
- Cada Snowmobile tiene 100 PB de capacidad (utiliza varias en paralelo)
- Alta seguridad: temperatura controlada, GPS, videovigilancia 24/7
- **Mejor que la Snowball si transfieres más de 10 PB**

Familia AWS Snow para migraciones de datos



Snowcone



Snowball Edge



Snowmobile

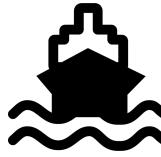
	Snowcone y Snowcone SSD	Almacenamiento optimizado Snowball Edge	Snowmobile
Capacidad de almacenamiento	8 TB HDD 14 TB SSD	80 TB utilizables	< 100 PB
Tamaño de la migración	Hasta 24 TB, online y offline	Hasta petabytes, sin conexión	Hasta exabytes, sin conexión
Agente DataSync	Preinstalado		

Familia AWS Snow - Proceso de uso

1. Solicita la entrega de dispositivos Snowball desde la consola de AWS
2. Instala el cliente Snowball / AWS OpsHub en tus servidores
3. Conecta el Snowball a tus servidores y copia los archivos utilizando el cliente
4. Devuelve el dispositivo cuando hayas terminado (va a la instalación de AWS adecuada)
5. Los datos se cargarán en un bucket de S3
6. La Snowball se borrará por completo

¿Qué es Edge Computing?

- Procesa los datos mientras se crean en **una Edge Location**
 - Un camión en la carretera, un barco en el mar, una estación minera bajo tierra...



- Estos lugares pueden tener
 - Acceso a Internet limitado / inexistente
 - Acceso limitado / no fácil a la potencia de cálculo
- Configuramos un dispositivo **Snowball Edge / Snowcone** para realizar Edge Computing
- Casos de uso de Edge Computing:
 - Preprocesamiento de datos
 - Machine Learning
 - Transcodificación de flujos multimedia
- Eventualmente (si es necesario) podemos devolver el dispositivo a AWS (para transferir datos, por ejemplo)

Snow Family – Edge Computing

- **Snowcone y Snowcone SSD (más pequeños)**

- 2 CPU, 4 GB de memoria, acceso por cable o inalámbrico
- Alimentación USB-C mediante un cable o la batería opcional



- **Snowball Edge - Computación optimizada**

- 104 vCPUs, 416 GiB de RAM
- GPU opcional (útil para procesamiento de vídeo o Machine Learning)
- Almacenamiento utilizable de 28 TB NVMe o 42 TB HDD
- Cluster de almacenamiento disponible (hasta 16 nodos)

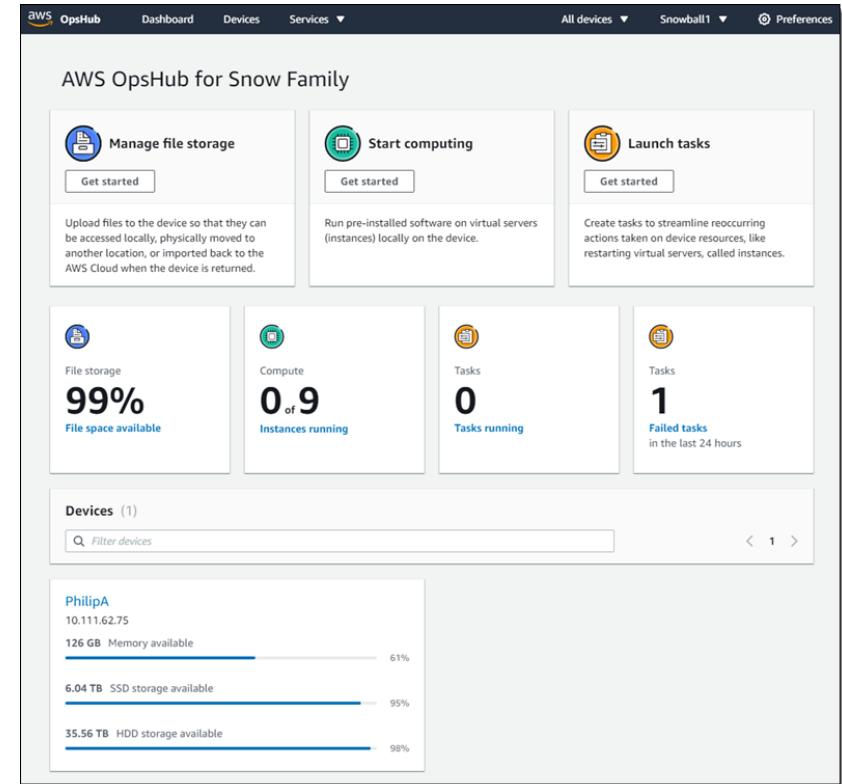


- **Snowball Edge - Almacenamiento optimizado**

- Hasta 40 vCPU, 80 GiB de RAM, 80 TB de almacenamiento
- Todos: Pueden ejecutar instancias EC2 y funciones AWS Lambda (utilizando AWS IoT Greengrass)
- Opciones de despliegue a largo plazo: 1 y 3 años con descuento

AWS OpsHub

- Históricamente, para utilizar los dispositivos de la Familia Snow, necesitabas una CLI (herramienta de interfaz de línea de comandos)
- Hoy en día, puedes utilizar **AWS OpsHub** (un software que instalas en tu ordenador/portátil) para administrar tu dispositivo de la Familia Snow
 - Desbloquear y configurar dispositivos individuales o en cluster
 - Transferir archivos
 - Lanzar y administrar instancias que se ejecutan en los dispositivos de la familia Snow
 - Supervisar las métricas del dispositivo (capacidad de almacenamiento, instancias activas en tu dispositivo)
 - Lanzar servicios de AWS compatibles en tus dispositivos (por ejemplo, instancias de Amazon EC2, AWS DataSync, Sistema de Archivos de Red (NFS))



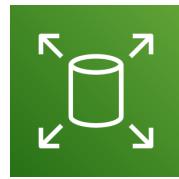
<https://aws.amazon.com/blogs/aws/aws-snowball-edge-update/>

Cloud híbrido para el almacenamiento

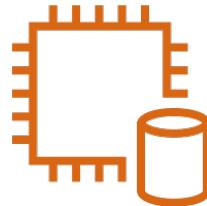
- AWS está impulsando el "cloud híbrido"
 - Parte de tu infraestructura está en las instalaciones
 - Parte de tu infraestructura está en el Cloud
- Esto puede deberse a:
 - Largas migraciones a el Cloud
 - Requisitos de seguridad
 - Requisitos de normativa
 - Estrategia de IT
- S3 es una tecnología de almacenamiento propia (a diferencia de EFS / NFS), así que ¿cómo expones los datos de S3 en las instalaciones?
- ¡AWS Storage Gateway!

Opciones nativas del Cloud de almacenamiento de AWS

BLOQUE



Amazon EBS



EC2 Instance
Store

FICHERO



Amazon EFS

OBJECTO



Amazon S3



Glacier

AWS Storage Gateway

- Puente entre los datos locales y los del Cloud en S3
- **Servicio de almacenamiento híbrido para permitir que las instalaciones utilicen sin problemas el Cloud de AWS**
- Casos de uso: recuperación de desastres, copias de seguridad y restauración, almacenamiento por niveles
- Tipos de Gateway de almacenamiento:
 - File Gateway
 - Volume Gateway
 - Tape Gateway
- No es necesario conocer los tipos en el examen



Resumen - Amazon S3

- **Buckets vs Objetos:** nombre único global, ligado a una región
- **Seguridad de S3:** política de IAM, política de bucket S3 (acceso público), cifrado S3
- **Sitios web de S3:** aloja un sitio web estático en Amazon S3
- **Versionado de S3:** múltiples versiones de archivos, para evitar borrados accidentales
- **Replicación de S3:** en la misma región o entre regiones, debe activar el control de versiones
- **Clases de almacenamiento S3:** Standard, IA, One Zone-IA, Intelligent, Glacier (Instant, Flexible, Deep)
- **Familia Snow:** importar datos a S3 a través de un dispositivo físico, edge computing
- **OpsHub:** aplicación de escritorio para gestionar los dispositivos de la Familia Snow
- **Storage Gateway:** solución híbrida para ampliar el almacenamiento local a S3

Bases de Datos



Introducción a las bases de datos

- El almacenamiento de datos en disco (EFS, EBS, EC2 Instance Store, S3) puede tener sus límites
- A veces, quieres almacenar datos en una base de datos...
- Puedes **estructurar** los datos
- Construyes **índices** para **consultar / buscar** eficientemente en los datos
- Defines **relaciones** entre tus **conjuntos de datos**

- Las bases de datos están **optimizadas para un propósito** y vienen con diferentes características, formas y restricciones

Bases de datos relacionales

- Tiene el mismo aspecto que las hojas de cálculo de Excel, ¡con enlaces entre ellas!
- Puede utilizar el lenguaje SQL para realizar consultas / búsquedas



Bases de datos NoSQL

- NoSQL = no-SQL = bases de datos no relacionales
- Las bases de datos NoSQL están creadas para modelos de datos específicos y tienen esquemas flexibles para construir aplicaciones modernas.
- Ventajas:
 - Flexibilidad: modelo de datos fácil de evolucionar
 - Escalabilidad: diseñadas para escalar utilizando clusters distribuidos
 - Alto rendimiento: optimizado para un modelo de datos específico
 - Alta funcionalidad: tipos optimizados para el modelo de datos
- Ejemplos: Bases de datos clave-valor, documento, gráfico, en memoria, de búsqueda

Ejemplo de datos NoSQL: JSON

- JSON = JavaScript Object Notation
- JSON es una forma común de datos que encaja en un modelo NoSQL
- Los datos pueden estar **anidados**
- Los campos pueden **cambiar** con el tiempo
- Soporte para nuevos tipos: **arrays**, etc.

```
{  
  "name": "John",  
  "age": 30,  
  "cars": [  
    "Ford",  
    "BMW",  
    "Fiat"  
  ],  
  "address": {  
    "type": "house",  
    "number": 23,  
    "street": "Dream Road"  
  }  
}
```

Bases de datos y responsabilidad compartida en AWS

- AWS ofrece el uso para **gestionar** diferentes bases de datos
- Los **beneficios** incluyen:
 - Aprovisionamiento rápido, alta disponibilidad, escalado vertical y horizontal
 - Copia de seguridad y restauración automatizadas, operaciones y actualizaciones
 - El parcheo del sistema operativo lo gestiona AWS
 - Monitorización, alertas
- Nota: muchas tecnologías de bases de datos pueden ejecutarse en EC2, pero debes ocuparte tú mismo de la resiliencia, las copias de seguridad, los parches, la alta disponibilidad, la tolerancia a fallos, el escalado...

Visión general de AWS RDS

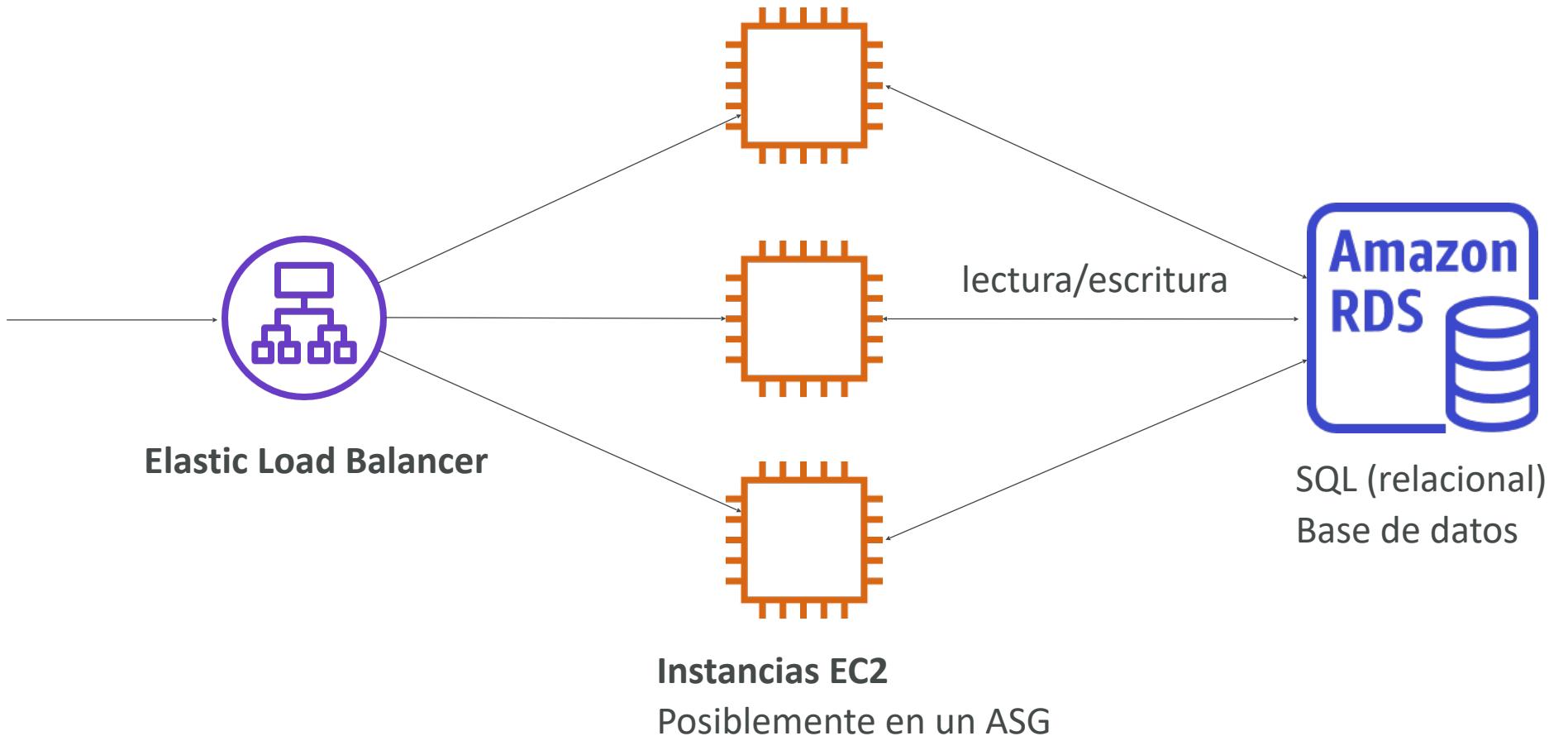


- RDS significa Servicio de Base de Datos **Relacional**
- Es un servicio de bases de datos gestionado para que las bases de datos utilicen **SQL** como lenguaje de consulta.
- Permite crear bases de datos en el Cloud que son gestionadas por AWS
 - Postgres
 - MySQL
 - MariaDB
 - Oracle
 - Microsoft SQL Server
 - Aurora (base de datos propia de AWS)

Ventaja sobre el uso de RDS frente al despliegue de la BD en EC2

- El RDS es un servicio gestionado:
 - Aprovisionamiento automatizado, parcheo del SO
 - Copias de seguridad continuas y restauración a una fecha determinada (Point in Time Restore)
 - Dashboards de monitorización
 - Rélicas de lectura para mejorar el rendimiento de lectura
 - Configuración multi AZ para DR (Disaster Recovery)
 - Ventanas de mantenimiento para actualizaciones
 - Capacidad de escalado (vertical y horizontal)
 - Almacenamiento respaldado por EBS (gp2 o io1)
- **PERO no puedes acceder por SSH a tus instancias**

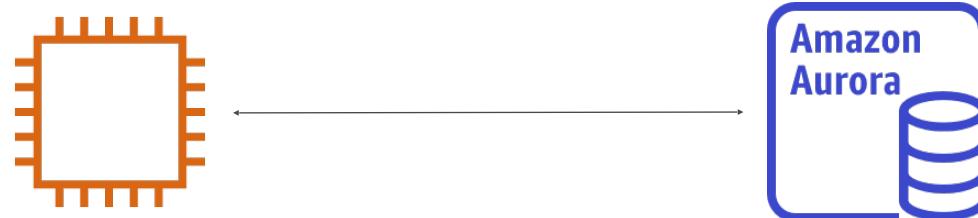
Arquitectura RDS



Amazon Aurora



- Aurora es una tecnología propietaria de AWS (no de código abierto)
- Tanto **PostgreSQL como MySQL** están soportadas como BD de Aurora
- Aurora está "optimizada para el Cloud de AWS" y afirma que mejora 5 veces el rendimiento de MySQL en RDS, y más de 3 veces el rendimiento de Postgres en RDS
- El almacenamiento de Aurora crece automáticamente en incrementos de 10 GB, hasta 128 TB
- Aurora cuesta más que RDS (un 20% más), pero es más eficiente
- No está en el nivel gratuito



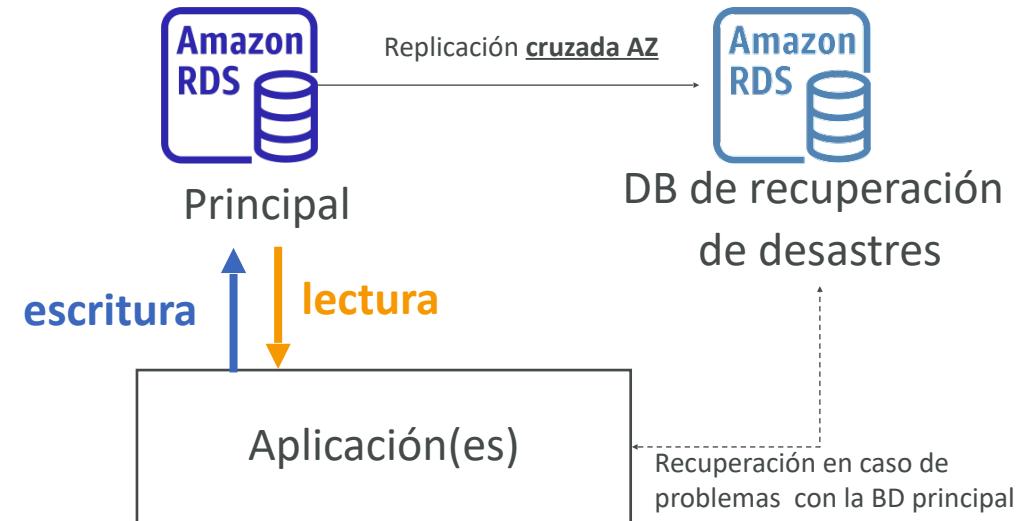
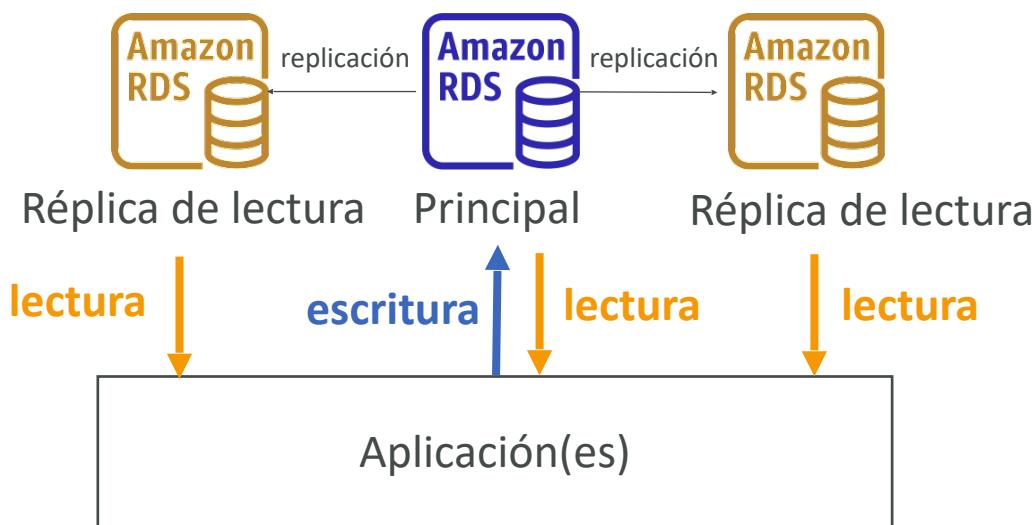
Despliegues RDS: Réplicas de lectura, Multi-AZ

- **Réplicas de lectura:**

- **Escala** la carga de trabajo de lectura de tu BD
- Puedes crear hasta 15 réplicas de lectura
- Los datos sólo se escriben en la BD principal

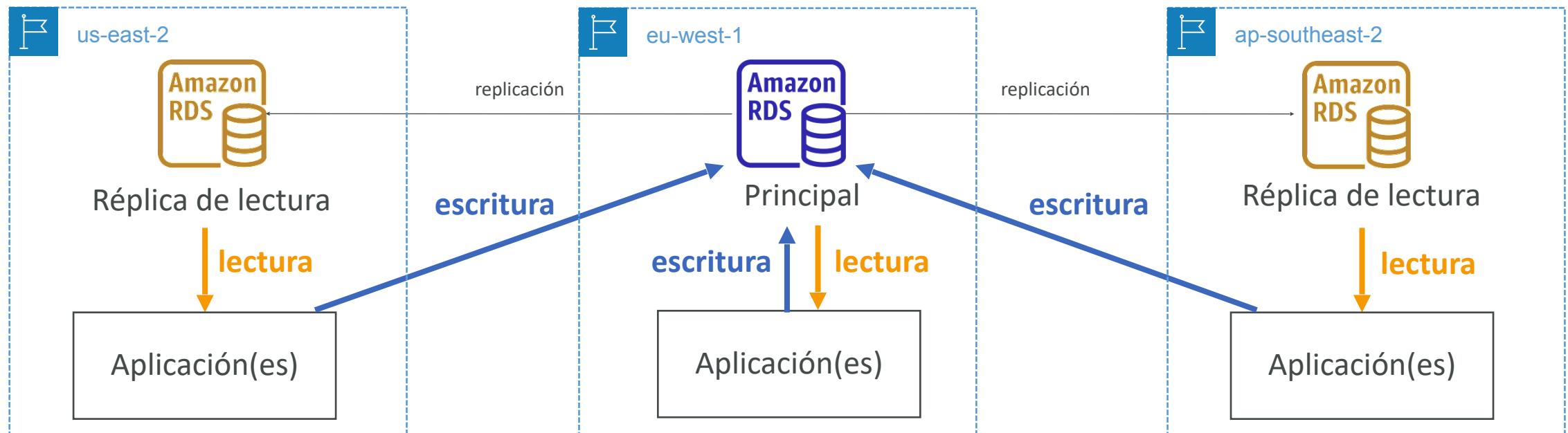
- **Multi-AZ:**

- **Recuperación** en caso de caída de la AZ (alta disponibilidad)
- Los datos sólo se leen/escriben en la base de datos principal
- Sólo se puede tener otra AZ como comutación por error



Despliegues de RDS: Multi-Región

- Multi-Región (Replicas de lectura)
 - Recuperación de desastres en caso de problema de región
 - Rendimiento local para lecturas globales
 - Coste de replicación

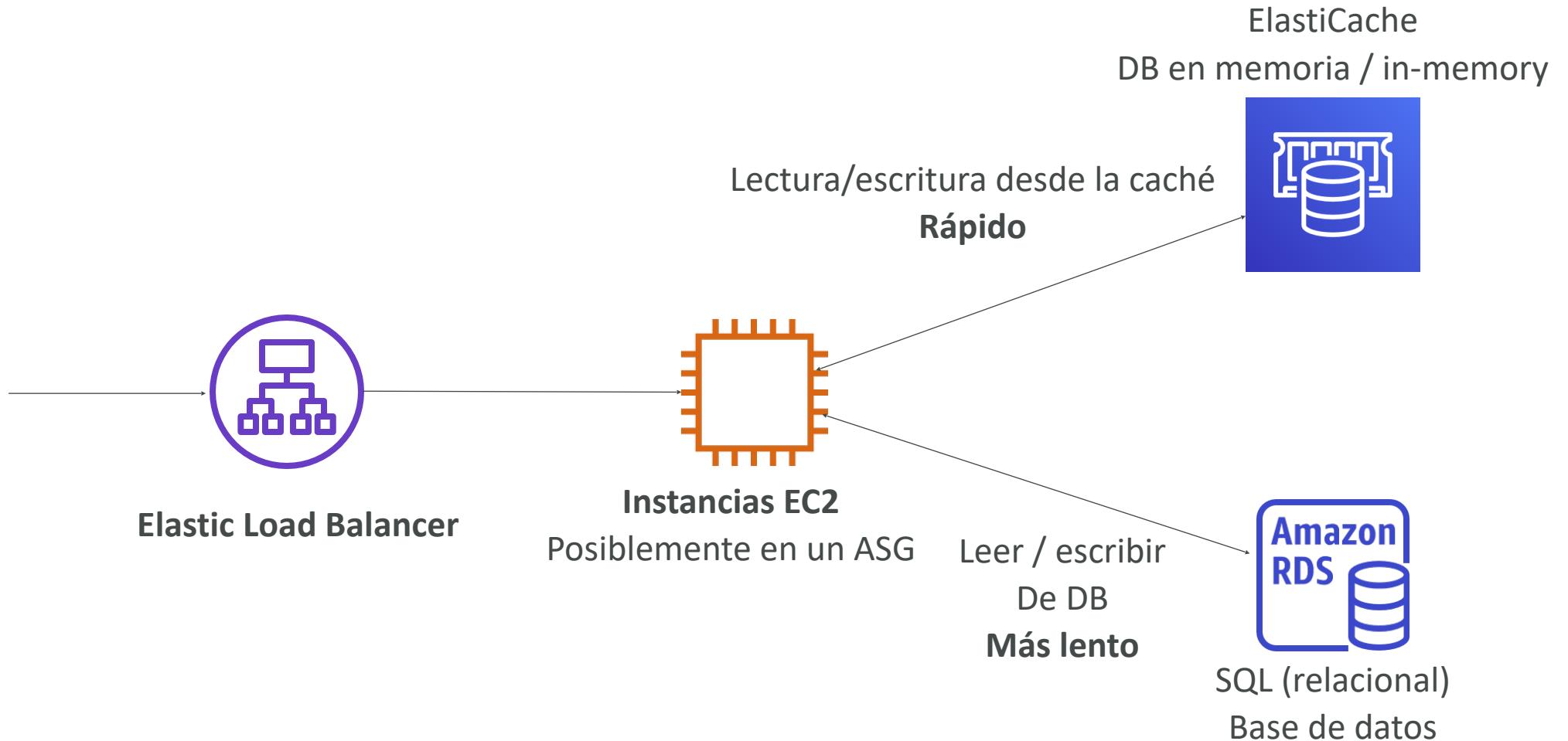


Visión general de Amazon ElastiCache



- De la misma manera que RDS es para conseguir bases de datos relacionales gestionadas...
- ElastiCache es para conseguir Redis o Memcached gestionados
- Cachés = **bases de datos en memoria** de alto rendimiento y baja latencia
- Ayuda a **reducir la carga de las bases de datos para cargas de trabajo de lectura intensiva**
- AWS se encarga del mantenimiento/parche del sistema operativo, las optimizaciones, la instalación, la configuración, la supervisión, la recuperación de fallos y las copias de seguridad

Arquitectura de ElastiCache - Caché



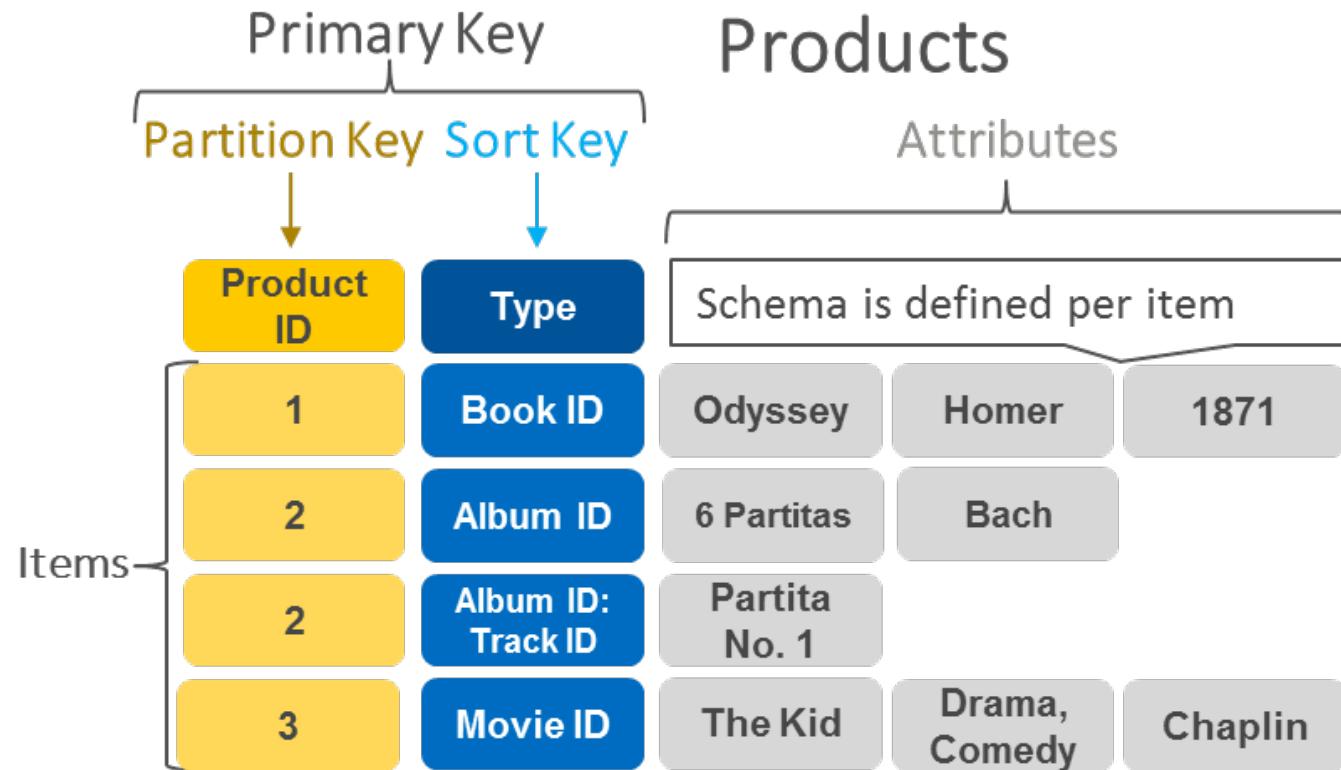
DynamoDB



- Totalmente gestionado con replicación a través de 3 AZ
- **Base de datos NoSQL - una base de datos no relacional**
- Escala a cargas de trabajo masivas, base de datos distribuida sin servidor
- Millones de peticiones por segundo, trillones de filas, cientos de TB de almacenamiento
- Rendimiento rápido y constante
- **Latencia de un milisegundo: recuperación de baja latencia**
- Integrada con IAM para seguridad, autorización y administración
- Bajo coste y capacidad de autoescalado
- Clase de tabla de acceso estándar e infrecuente (IA)

DynamoDB - tipo de datos

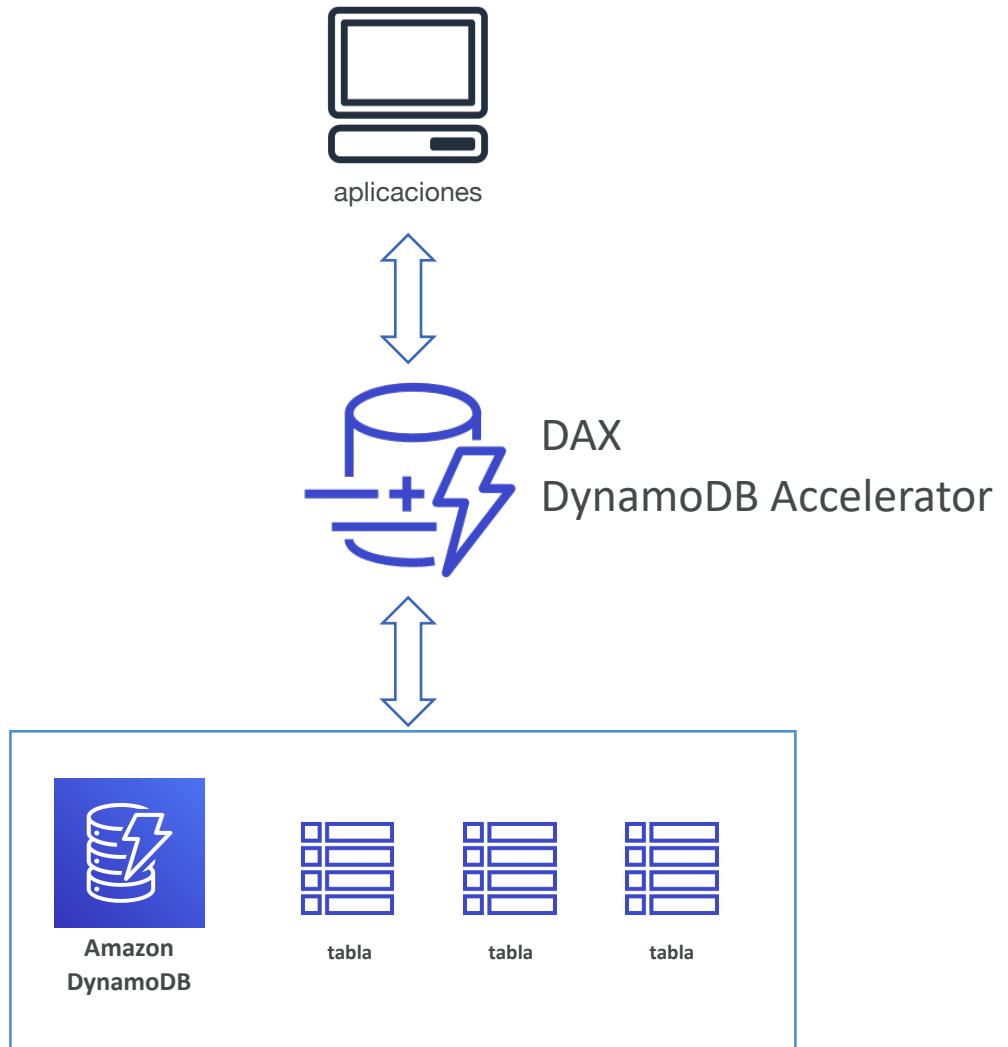
- DynamoDB es una base de datos clave/valor



<https://aws.amazon.com/nosql/key-value/>

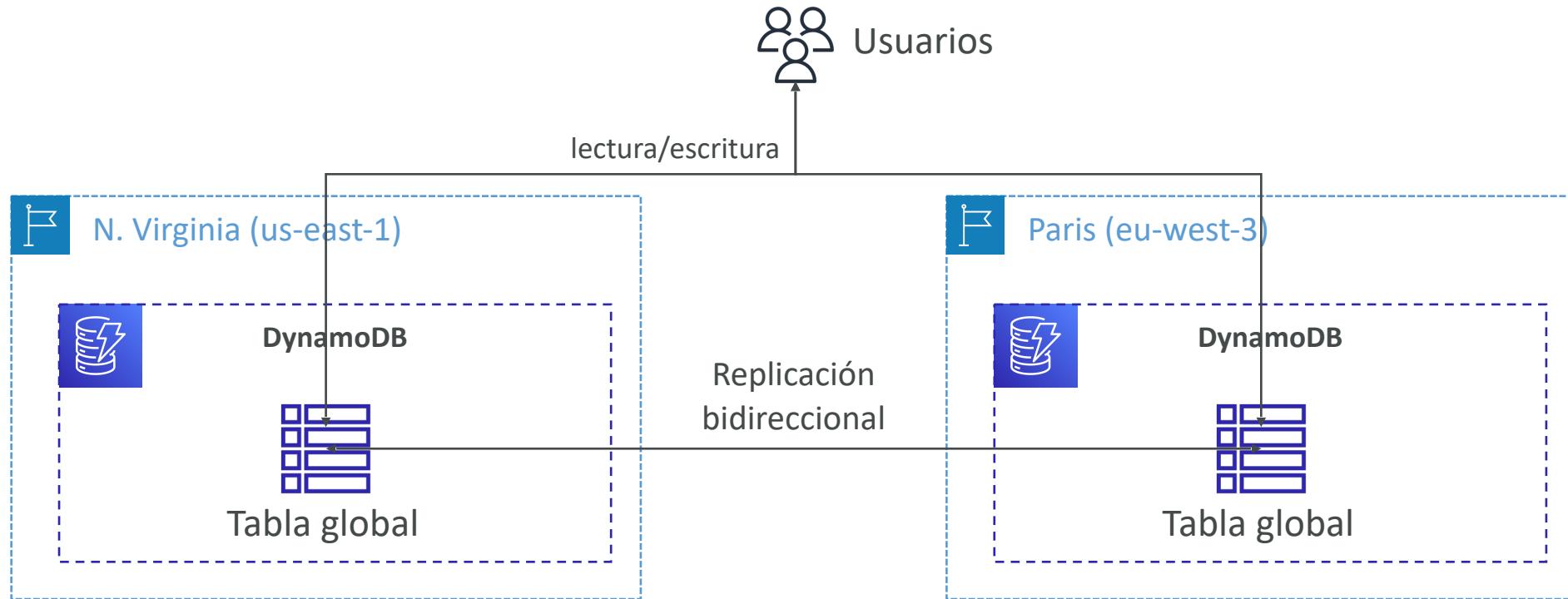
DynamoDB Accelerator - DAX

- **Caché en memoria** totalmente gestionada para DynamoDB
- **Mejora del rendimiento x 10** - latencia de un milisegundo a microsegundos - al acceder a tus tablas de DynamoDB
- Seguridad, alta escalabilidad y alta disponibilidad
- Diferencia con ElastiCache a nivel de CCP:
DAX sólo se utiliza y se integra con DynamoDB, mientras que ElastiCache puede utilizarse para otras bases de datos

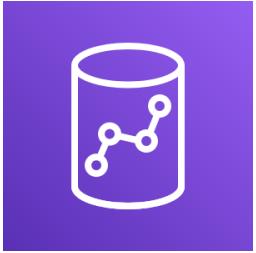


DynamoDB - Tablas globales

- Haz que una tabla de DynamoDB sea accesible con **baja latencia** en varias regiones
- Replicación **activa-activa (lectura/escritura)** en cualquier región de AWS)

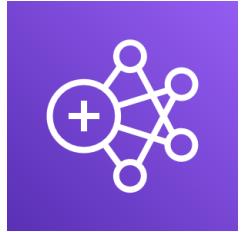


Visión general de Redshift



- Redshift se basa en PostgreSQL, **pero no se utiliza para OLTP**
- **Es OLAP - procesamiento analítico en línea (análisis y almacenamiento de datos)**
- Carga los datos una vez cada hora, no cada segundo
- Rendimiento 10 veces superior al de otros almacenes de datos, escala a PBs de datos
- Almacenamiento de datos **en columnas** (en lugar de en filas)
- Ejecución de consultas en paralelo masivo (MPP), con alta disponibilidad
- Paga a medida que avanzas en función de las instancias aprovisionadas
- Tiene una interfaz SQL para realizar las consultas
- Las herramientas de BI, como AWS Quicksight o Tableau, se integran con ella

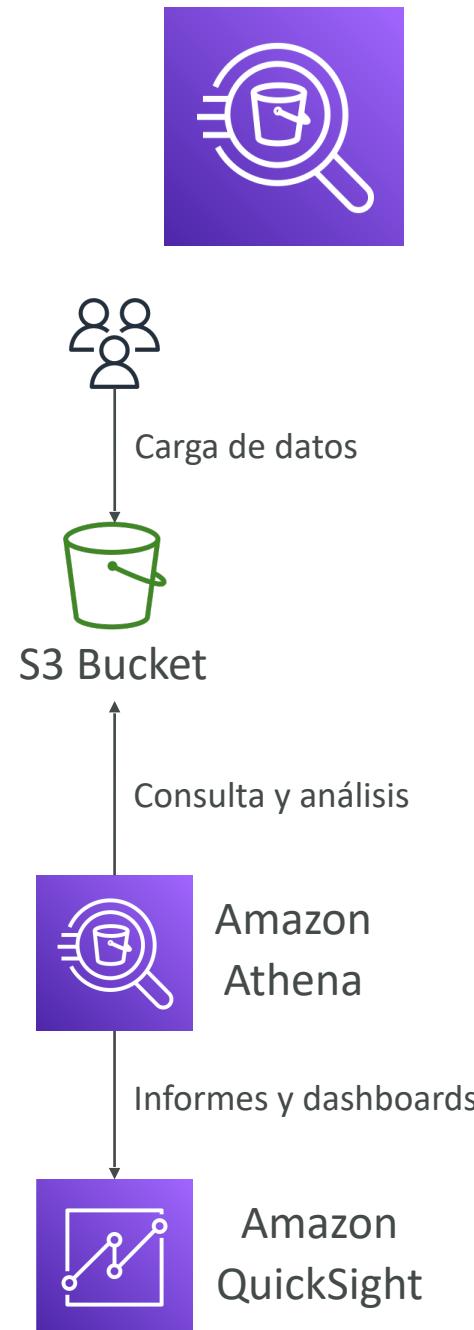
Amazon EMR



- EMR = Elastic MapReduce
- EMR ayuda a crear **clusters Hadoop (Big Data)** para analizar y procesar una gran cantidad de datos
- Los clusters pueden estar formados por **cientos de instancias EC2**
- También es compatible con Apache Spark, HBase, Presto, Flink...
- EMR se encarga de todo el aprovisionamiento y la configuración
- Autoescalado e integrado con instancias Spot
- **Casos de uso: procesamiento de datos, machine Learning, indexación web, big data...**

Amazon Athena

- **Servicio de consulta sin servidor para analizar los datos almacenados en Amazon S3**
- Utiliza el lenguaje SQL estándar para consultar los archivos
- Admite CSV, JSON, ORC, Avro y Parquet (construido sobre Presto)
- Precio: 5,00 dólares por TB de datos analizados
- Utiliza datos comprimidos o en columnas para ahorrar costes (menos escaneo)
- Casos de uso: Inteligencia empresarial/análisis/informes, analizar y consultar Logs de flujo de VPC, Logs de ELB, rastros de CloudTrail, etc.
- **Sugerencia de examen:** analiza los datos en S3 usando SQL sin servidor, usa Athena



Amazon QuickSight



- Servicio de inteligencia empresarial impulsado por Machine Learning sin servidor para crear dashboards interactivos
- Rápido, escalable automáticamente, integrable, con precios por sesión
- Casos de uso:
 - Análisis empresarial
 - Construir visualizaciones
 - Realizar análisis ad-hoc
 - Obtén información empresarial con los datos
- Integrado con RDS, Aurora, Redshift, S3...



<https://aws.amazon.com/quicksight/>

DocumentDB



- Aurora es una "implementación de AWS" de PostgreSQL / MySQL ...
- **DocumentDB es lo mismo que MongoDB (que es una base de datos NoSQL)**

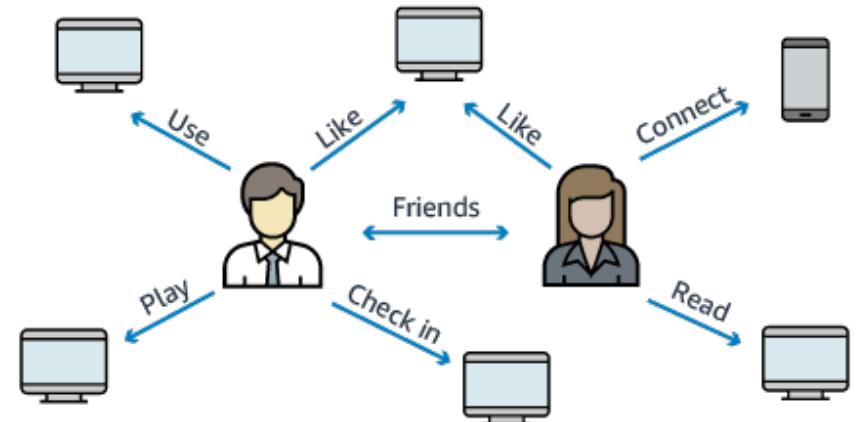
- MongoDB se utiliza para almacenar, consultar e indexar datos JSON
- “Conceptos de despliegue” similares a los de Aurora
- Totalmente gestionado, de alta disponibilidad con replicación a través de 3 AZ
- El almacenamiento de DocumentDB crece automáticamente en incrementos de 10 GB, hasta 128 TB

- Escala automáticamente a cargas de trabajo con millones de peticiones por segundo

Amazon Neptune



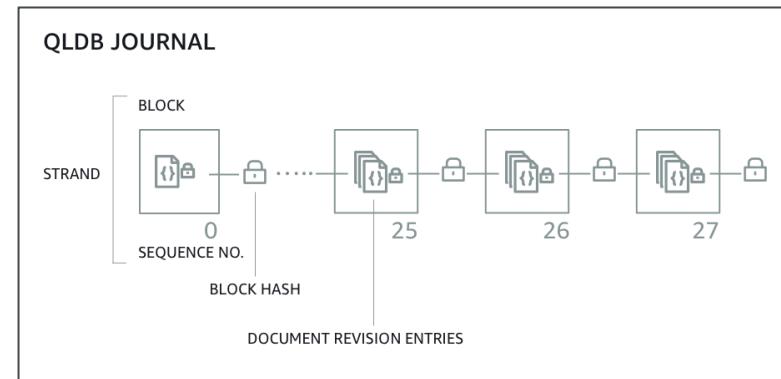
- Base de datos **gráfica** totalmente gestionada
- Un **conjunto de datos de grafos** popular sería una **red social**
 - Los usuarios tienen amigos
 - Las publicaciones tienen comentarios
 - Los comentarios tienen likes de los usuarios
 - Los usuarios comparten y les gustan las publicaciones...
- Alta disponibilidad en 3 AZ, con hasta 15 réplicas de lectura
- Construye y ejecuta aplicaciones que trabajen con conjuntos de datos altamente conectados, optimizados para estas complejas y difíciles consultas
- Puede almacenar hasta miles de millones de relaciones y consultar el gráfico con una latencia de milisegundos
- Alta disponibilidad con réplicas a través de múltiples AZs
- Excelente para grafos de conocimiento (Wikipedia), detección de fraudes, motores de recomendación, redes sociales



Amazon QLDB



- QLDB significa "Quantum Ledger Database" (base de datos de libros contables)
- Un libro de contabilidad es un libro que **registra las transacciones financieras**
- Totalmente gestionada, sin servidor, de alta disponibilidad, con replicación en 3 AZ
- Se utiliza para **revisar el historial de todos los cambios realizados en los datos de tu aplicación** a lo largo del tiempo
- Sistema **inmutable**: ninguna entrada puede ser eliminada o modificada, verificable criptográficamente



- Rendimiento 2-3 veces mejor que los marcos de blockchain de libro mayor común
- Diferencia con Amazon Managed Blockchain: **no hay componente de descentralización**, de acuerdo con las normas de regulación financiera

<https://docs.aws.amazon.com/qldb/latest/developerguide/ledger-structure.html>

Amazon Managed Blockchain



- Blockchain permite crear aplicaciones en las que varias partes pueden ejecutar transacciones **sin necesidad de una autoridad central de confianza.**
- Amazon Managed Blockchain es un servicio gestionado para:
 - Unirte a redes públicas de blockchain
 - O crear tu propia red privada escalable
- Compatible con los marcos Hyperledger Fabric y Ethereum



AWS Glue

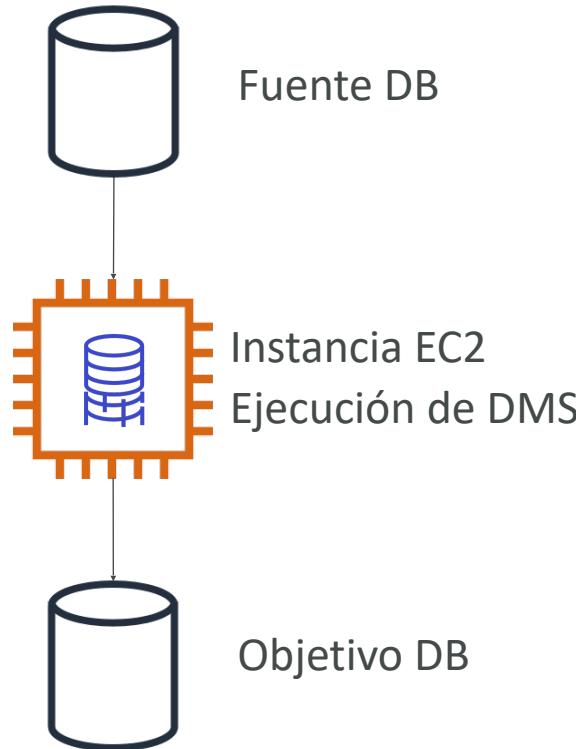


- Servicio gestionado de **extracción, transformación y carga (ETL)**
- Útil para preparar y transformar datos para la analítica
- Servicio totalmente **sin servidor / serverless**



- Catálogo de datos Glue: catálogo de conjuntos de datos
 - puede ser utilizado por Athena, Redshift, EMR

DMS – Database Migration Service



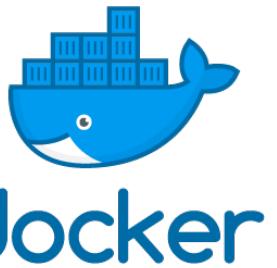
- Migra de forma rápida y segura las bases de datos a AWS, con capacidad de recuperación y autocuración
- La base de datos de origen sigue disponible durante la migración
- Soporta:
 - Migraciones homogéneas: por ejemplo, de Oracle a Oracle
 - Migraciones heterogéneas: por ejemplo, de Microsoft SQL Server a Aurora

Resumen de bases de datos y análisis en AWS

- **Bases de datos relacionales - OLTP:** RDS y Aurora (SQL)
- **Diferencias entre Multi-AZ, Rélicas de Lectura, Multi-Región**
- **Base de datos en memoria (in-memory):** ElastiCache
- **Base de datos de claves/valores:** DynamoDB (sin servidor) y DAX (caché para DynamoDB)
- **Warehouse - OLAP:** Redshift (SQL)
- **Cluster Hadoop:** EMR
- **Athena:** consulta de datos en Amazon S3 (sin servidor y SQL)
- **QuickSight:** dashboards sobre tus datos (sin servidor)
- **DocumentDB:** "Aurora para MongoDB" (JSON - base de datos NoSQL)
- **Amazon QLDB:** Libro de transacciones financieras (libro inmutable, verificable criptográficamente)
- **Amazon Managed Blockchain:** cadenas de bloques Hyperledger Fabric y Ethereum gestionadas
- **Glue:** Servicio gestionado de ETL (Extract-Transform-Load) y Catálogo de Datos
- **Database Migration:** DMS
- **Neptune:** base de datos gráfica

Otros servicios de computación

¿Qué es Docker?



- Docker es una plataforma de desarrollo de software para desplegar aplicaciones
- Las aplicaciones se empaquetan en **contenedores** que pueden ejecutarse en cualquier sistema operativo
- **Las aplicaciones se ejecutan igual, independientemente de dónde se ejecuten**
 - Cualquier máquina
 - No hay problemas de compatibilidad
 - Comportamiento predecible
 - Menos trabajo
 - Más fácil de mantener y desplegar
 - Funciona con cualquier lenguaje, cualquier sistema operativo y cualquier tecnología
 - Amplía y reduce los contenedores muy rápidamente (en segundos)

Docker en un Sistema Operativo

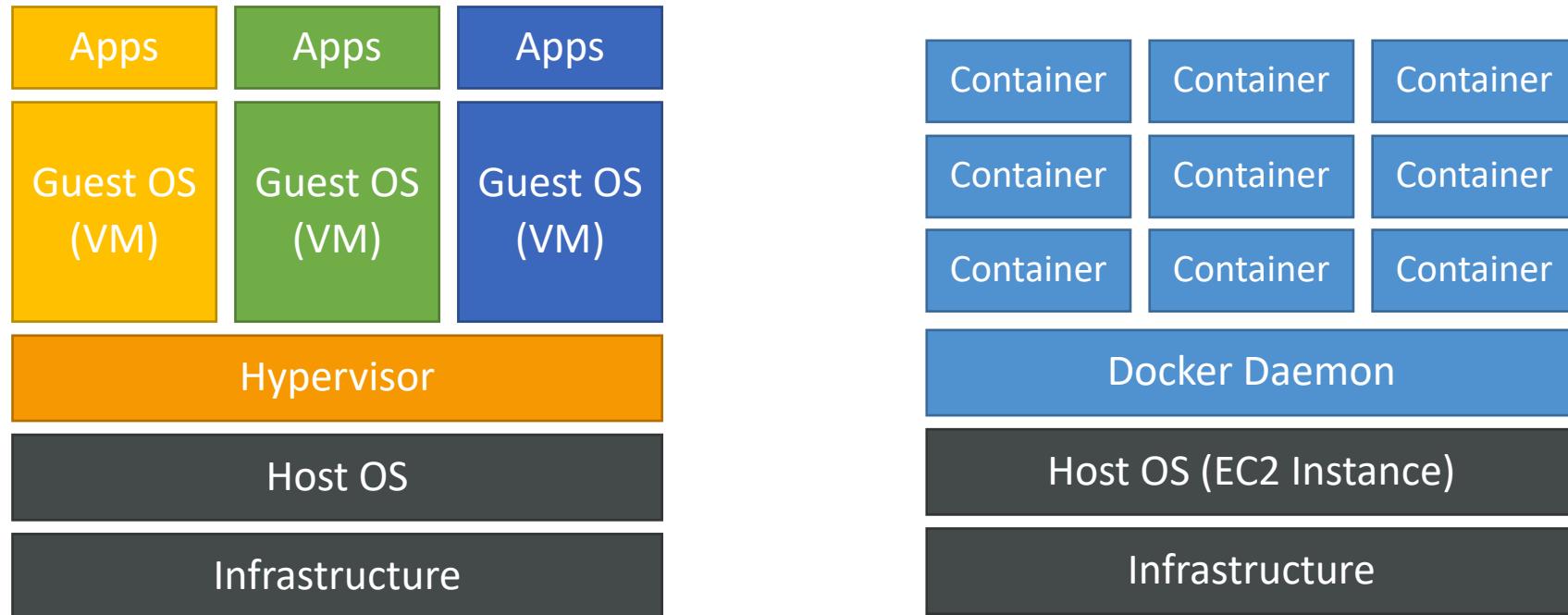


¿Dónde se almacenan las imágenes Docker?

- Las imágenes de Docker se almacenan en repositorios de Docker
- Públicos: Docker Hub <https://hub.docker.com/>
 - Encuentra imágenes base para muchas tecnologías o sistemas operativos:
 - Ubuntu
 - MySQL
 - NodeJS, Java...
- Privado: Amazon ECR (Elastic Container Registry)

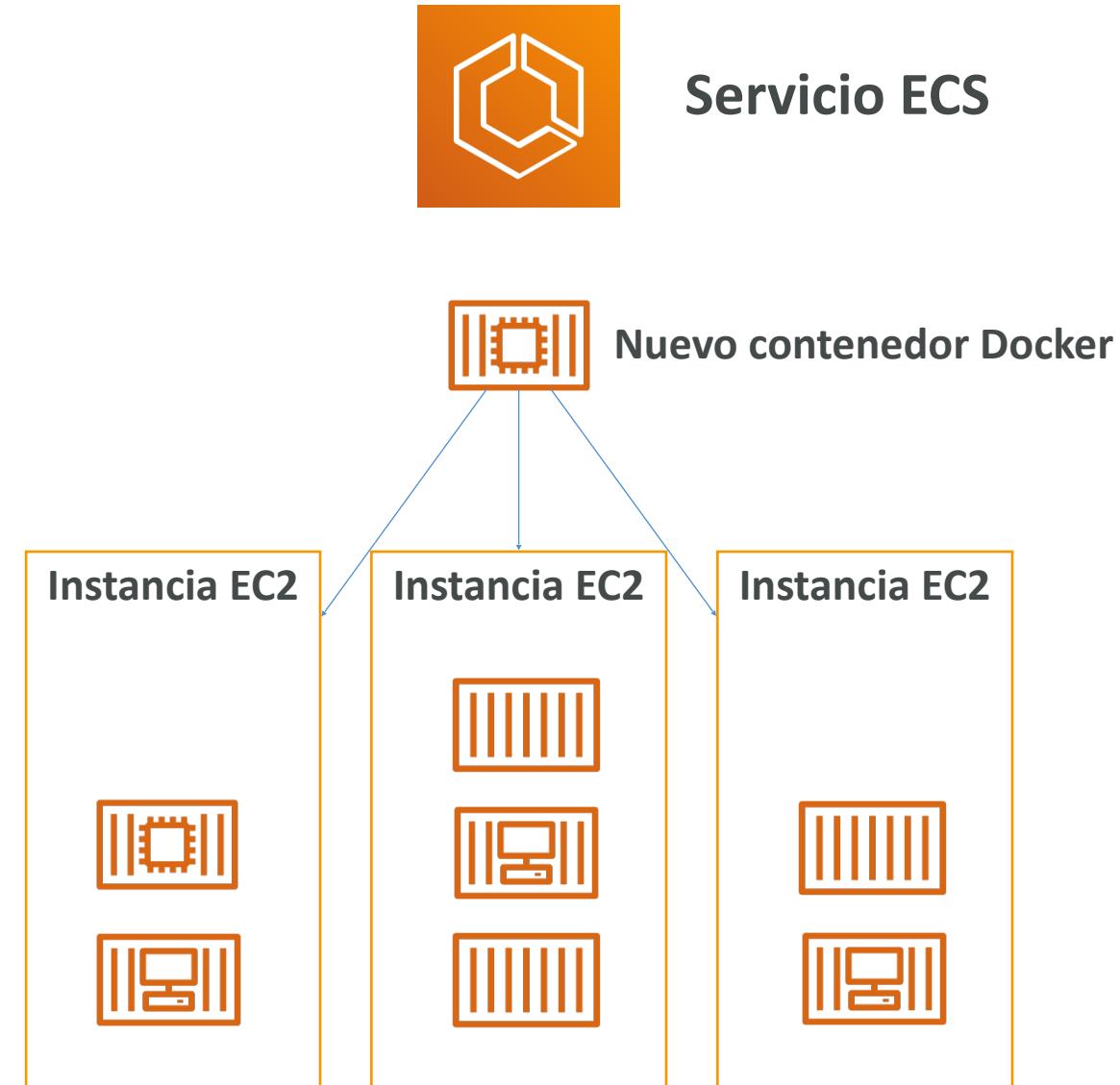
Docker frente a las máquinas virtuales

- Docker es una "especie" de tecnología de virtualización, pero no exactamente
- Los recursos se comparten con el anfitrión => muchos contenedores en un servidor



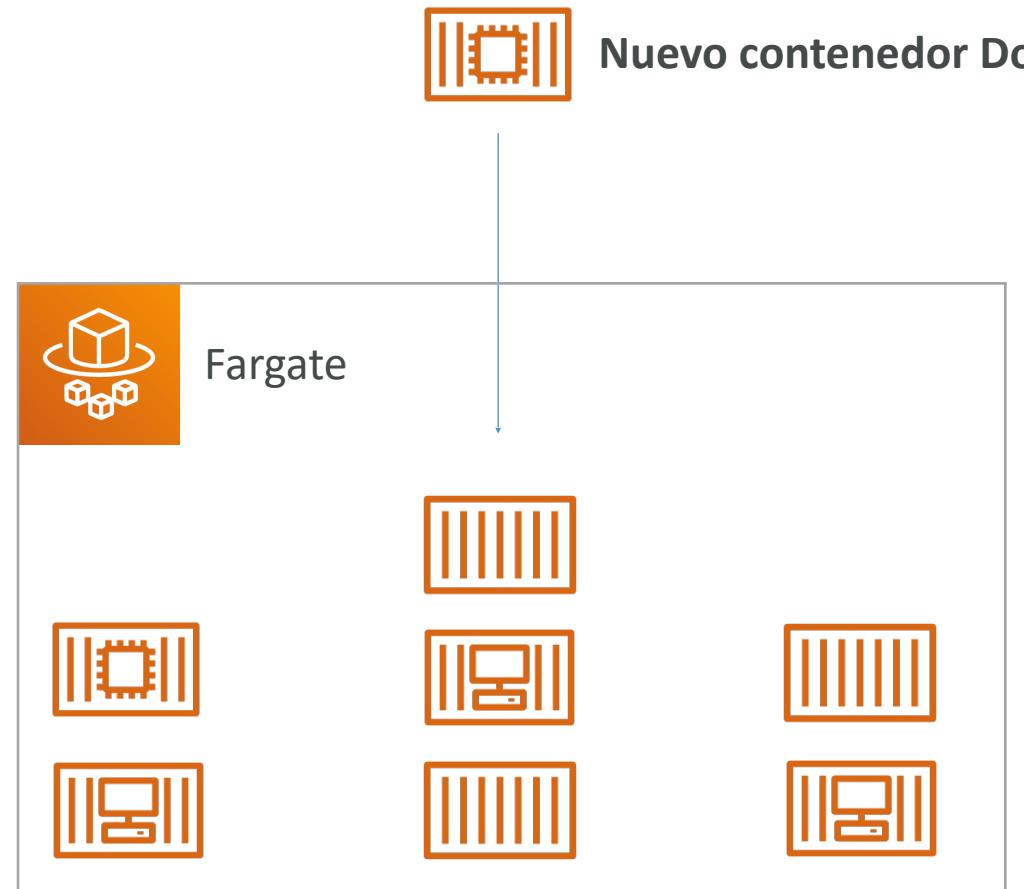
ECS

- ECS = Elastic Container Service
- Lanzar contenedores Docker en AWS
- **Debes aprovisionar y mantener la infraestructura (las instancias EC2)**
- AWS se encarga de iniciar/parar los contenedores
- Tiene integraciones con el Application Load Balancer



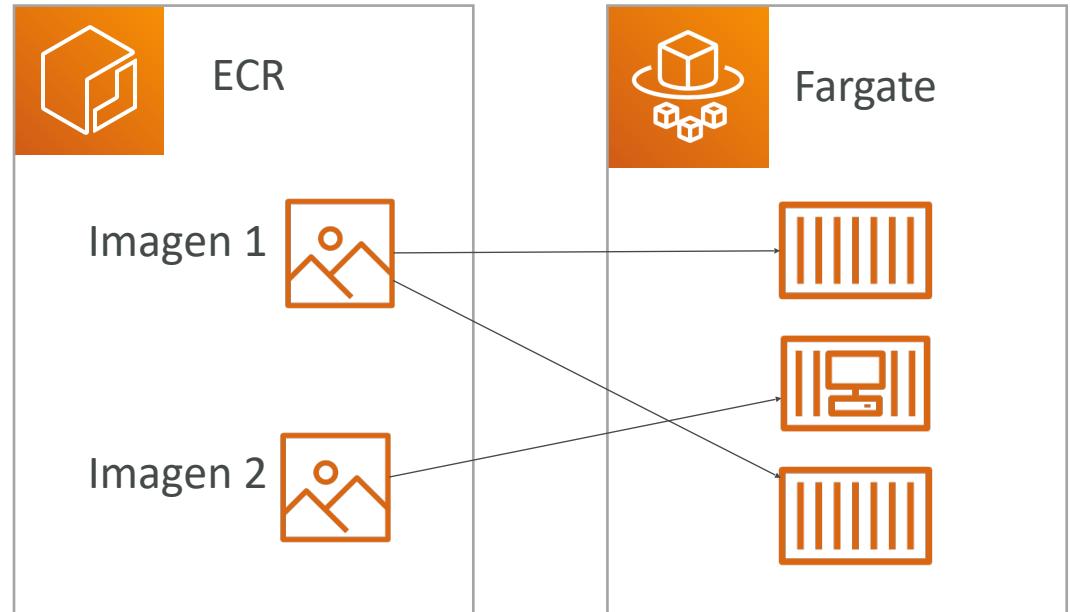
Fargate

- Lanza contenedores Docker en AWS
- **No aprovisionas la infraestructura (no hay instancias EC2 que gestionar) - ¡más sencillo!**
- **Oferta serverless**
- AWS sólo ejecuta los contenedores por ti en función de la CPU / RAM que necesites



ECR

- ECR = Elastic Container Registry
- Registro privado de Docker en AWS
- Aquí es donde **almacenas tus imágenes Docker** para que puedan ser ejecutadas por ECS o Fargate



¿Qué es el serverless?

- Serverless es un nuevo paradigma en el que los desarrolladores ya no tienen que gestionar servidores...
- Sólo despliegan código
- Sólo despliegan... ¡funciones!
- Inicialmente... Serverless == FaaS (Función como servicio)
- Serverless fue pionero por AWS Lambda, pero ahora también incluye todo lo que se gestiona "bases de datos, mensajería, almacenamiento, etc."
- **Serverless no significa que no haya servidores...** significa que simplemente no los gestionas / aprovisionas / ves

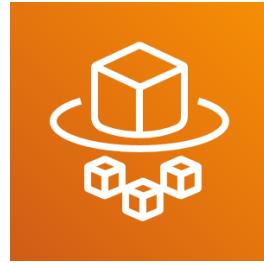
Hasta ahora en este curso...



Amazon S3



DynamoDB

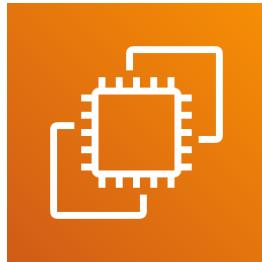


Fargate



Lambda

Por qué AWS Lambda



Amazon EC2

- Servidores virtuales en el Cloud
 - Limitado por la RAM y la CPU
 - Funcionamiento continuo
 - Escalar significa intervenir para añadir/quitar servidores
-



Amazon Lambda

- **Funciones** virtuales: ¡no hay servidores que gestionar!
- Limitado por el tiempo - **ejecuciones cortas**
- Ejecución **bajo demanda**
- **El escalado está automatizado**

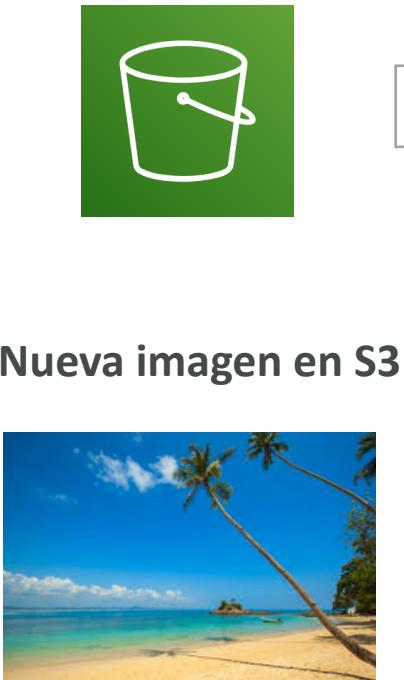
Beneficios de AWS Lambda

- Precios sencillos:
 - Paga por solicitud y tiempo de computación
 - Capa gratuita de 1.000.000 de solicitudes de AWS Lambda y 400.000 GB de tiempo de computación
- Integrado con todo el conjunto de servicios de AWS
- **Dirigido por eventos:** las funciones son invocadas por AWS cuando se necesitan
- Integrado con muchos lenguajes de programación
- Fácil monitorización a través de AWS CloudWatch
- Fácil de obtener más recursos por funciones (¡hasta 10 GB de RAM!)
- ¡El aumento de la RAM también mejorará la CPU y la red!

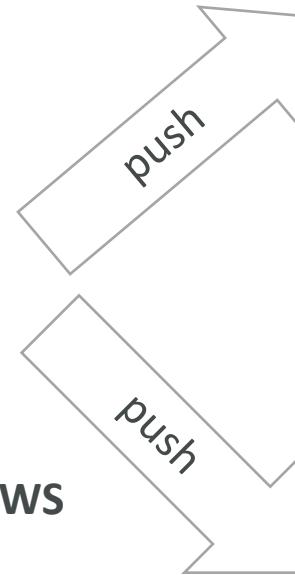
Soporte del lenguaje AWS Lambda

- Node.js (JavaScript)
- Python
- Java (compatible con Java 8)
- C# (.NET Core)
- Golang
- C# / Powershell
- Ruby
- API de tiempo de ejecución personalizado (compatible con la comunidad, ejemplo Rust)
- Imagen del contenedor Lambda
 - La imagen del contenedor debe implementar la API de tiempo de ejecución Lambda
 - Se prefiere ECS / Fargate para ejecutar imágenes Docker arbitrarias

Ejemplo: Creación de miniaturas Serverless



La función Lambda de AWS
crea una miniatura



Nueva miniatura en S3



Nombre de la imagen
Tamaño de la imagen
Fecha de creación
etc.

Metadata en DynamoDB

Ejemplo: Trabajo CRON Serverless



EventBridge

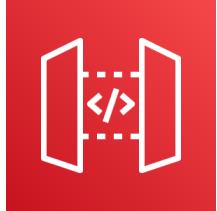


Función AWS Lambda
realiza una tarea

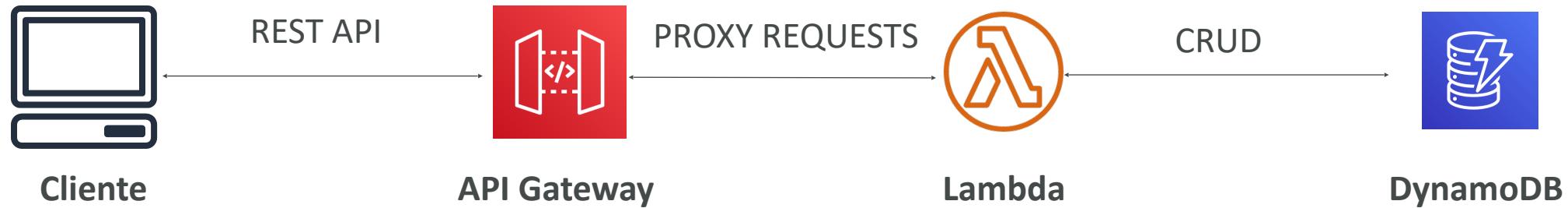
Precios de AWS Lambda: ejemplo

- Puedes encontrar información general sobre los precios aquí:
 - <https://aws.amazon.com/lambda/pricing/>
- Pago por **llamadas**:
 - Los primeros 1.000.000 de solicitudes son gratuitos
 - 0,20 \$ por cada millón de solicitudes a partir de entonces (0,0000002 \$ por solicitud)
- Pago por **duración**: (en incrementos de 1 ms)
 - 400.000 GB-segundos de tiempo de cálculo al mes GRATIS
 - == 400.000 segundos si la función es de 1 GB de RAM
 - == 3.200.000 segundos si la función es de 128 MB de RAM
 - Después, 1 dólar por 600.000 GB-segundos
- Suele ser muy barato ejecutar AWS Lambda, por lo que es muy popular

Amazon API Gateway

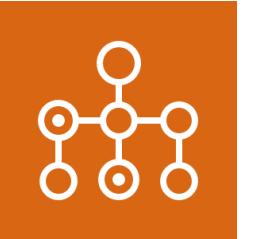


- Ejemplo: construir una API serverless



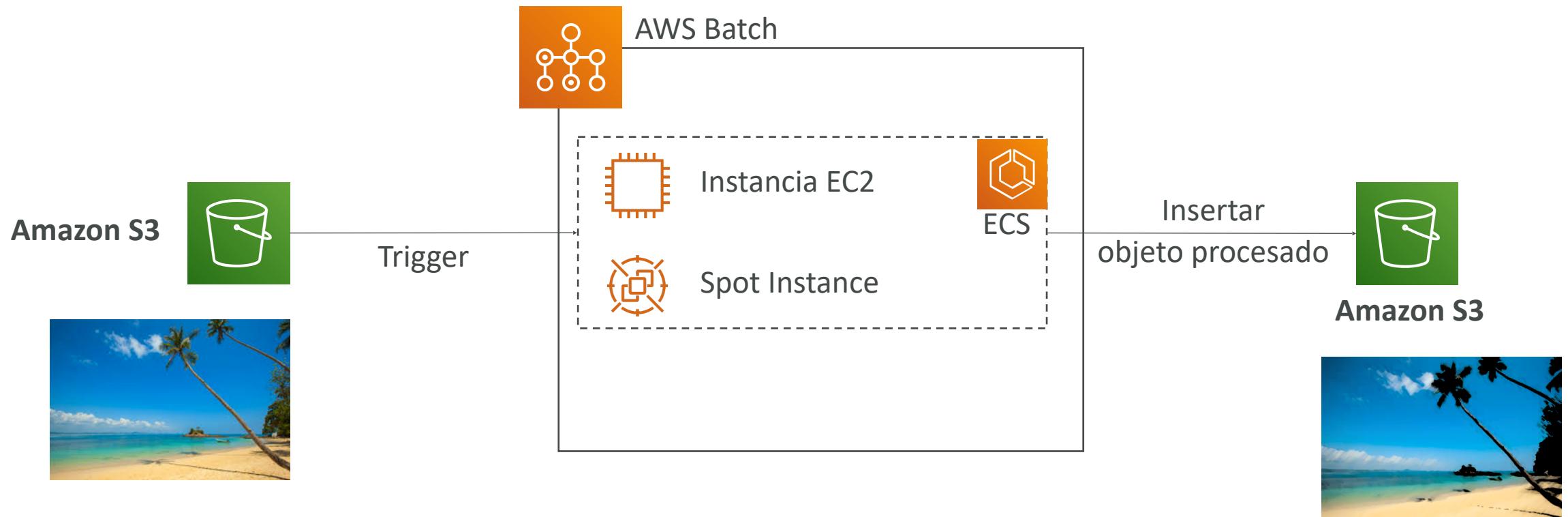
- Servicio totalmente gestionado para que los desarrolladores puedan crear, publicar, mantener, supervisar y asegurar fácilmente las API
- **Serverless** y escalable
- Soporta APIs RESTful y APIs WebSocket
- Soporta seguridad, autenticación de usuarios, claves de la API, monitorización...

AWS Batch



- **Procesamiento por lotes** totalmente gestionado a **cualquier escala**
- Ejecuta eficientemente 100.000 trabajos de computación por lotes en AWS
- Un trabajo "por lotes" es un trabajo con un inicio y un final (en contraposición a uno continuo)
- Batch lanzará dinámicamente **instancias EC2 o instancias Spot**
- AWS Batch proporciona la cantidad adecuada de computación / memoria
- Tú envías o programas los trabajos por lotes y AWS Batch se encarga del resto
- Los trabajos por lotes se definen como **imágenes Docker** y se **ejecutan en ECS**
- Útil para optimizar los costes y centrarse menos en la infraestructura

AWS Batch – Ejemplo simplificado



Batch vs Lambda

- Lambda:
 - Límite de tiempo
 - Tiempos de ejecución limitados
 - Espacio de disco temporal limitado
 - Serverless
- Por lotes:
 - Sin límite de tiempo
 - Cualquier tiempo de ejecución siempre que esté empaquetado como imagen Docker
 - Depende de EBS / almacén de instancias para el espacio en disco
 - Depende de EC2 (puede ser gestionado por AWS)



Amazon Lightsail



- Servidores virtuales, almacenamiento, bases de datos y redes
- Precios bajos y predecibles
- Alternativa más sencilla al uso de EC2, RDS, ELB, EBS, Route 53...
- Ideal para personas **con poca experiencia en el Cloud**
- Puedes configurar notificaciones y monitorización de tus recursos Lightsail
- Casos de uso:
 - Aplicaciones web sencillas (tiene plantillas para LAMP, Nginx, MEAN, Node.js...)
 - Sitios web (plantillas para WordPress, Magento, Plesk, Joomla)
 - Entorno de desarrollo/prueba
- Tiene alta disponibilidad pero no tiene autoescalado, integraciones limitadas con AWS

Resumen - Otros servicios de computación

- **Docker**: tecnología de contenedores para ejecutar aplicaciones
- **ECS**: ejecuta contenedores Docker en instancias EC2
- **Fargate**:
 - Ejecuta contenedores Docker sin aprovisionar la infraestructura
 - Oferta serverless (sin instancias EC2)
- **ECR**: Repositorio privado de imágenes Docker
- **Batch**: ejecuta trabajos por lotes en AWS a través de instancias EC2 gestionadas
- **Lightsail**: precios predecibles y bajos para pilas de aplicaciones y bases de datos sencillas

Resumen - Lambda

- Lambda es serverless, función como servicio, escalado sin fisuras, reactivo
- **Facturación de Lambda:**
 - Por el tiempo de ejecución x por la RAM aprovisionada
 - Por el número de invocaciones
- **Soporte de lenguajes:** muchos lenguajes de programación excepto (arbitrariamente) Docker
- **Tiempo de invocación:** hasta 15 minutos
- **Casos de uso:**
 - Crear miniaturas para imágenes subidas a S3
 - Ejecutar un trabajo cron sin servidor
- **Gateway de la API:** exponer las funciones Lambda como API HTTP

Despliegue y gestión de la infraestructura a escala



Qué es CloudFormation

- CloudFormation es una forma declarativa de esbozar tu infraestructura de AWS, para cualquier recurso (la mayoría de ellos son compatibles).
- Por ejemplo, dentro de una plantilla de CloudFormation, dices
 - Quiero un grupo de seguridad
 - Quiero dos instancias EC2 que utilicen este grupo de seguridad
 - Quiero un bucket S3
 - Quiero un load balancer (ELB) delante de estas máquinas
- Entonces CloudFormation los crea por ti, en el **orden correcto**, con la **configuración exacta** que especifiques

Ventajas de AWS CloudFormation (1/2)

- **Infraestructura como código**

- No se crean recursos manualmente, lo que es excelente para el control
- Los cambios en la infraestructura se revisan a través del código

- Coste

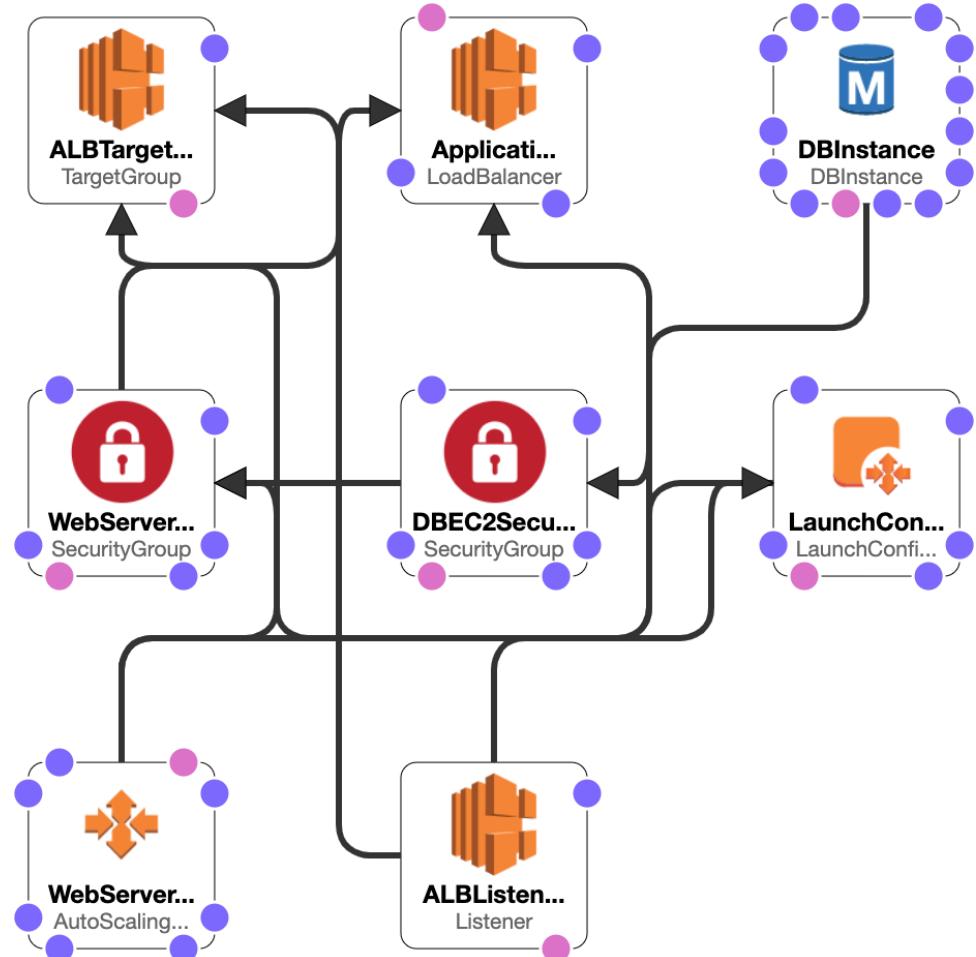
- Cada recurso dentro de la pila está etiquetado con un identificador para que puedas ver fácilmente cuánto te cuesta una pila
- Puedes estimar los costes de tus recursos utilizando la plantilla de CloudFormation
- Estrategia de ahorro: En Dev, podrías automatizar la eliminación de plantillas a las 5 de la tarde y volver a crearlas a las 8 de la mañana, de forma segura

Ventajas de AWS CloudFormation (2/2)

- Productividad
 - Posibilidad de destruir y volver a crear una infraestructura en el Cloud sobre la marcha
 - Generación automatizada de diagramas para tus plantillas
 - Programación declarativa (no es necesario averiguar el orden y la orquestación)
- No vuelvas a inventar la rueda
 - Aprovecha las plantillas existentes en la web
 - Aprovecha la documentación
- **Soporta (casi) todos los recursos de AWS:**
 - Todo lo que veremos en este curso es compatible
 - Puedes utilizar "recursos personalizados" para los recursos que no son compatibles

Stack Designer de CloudFormation

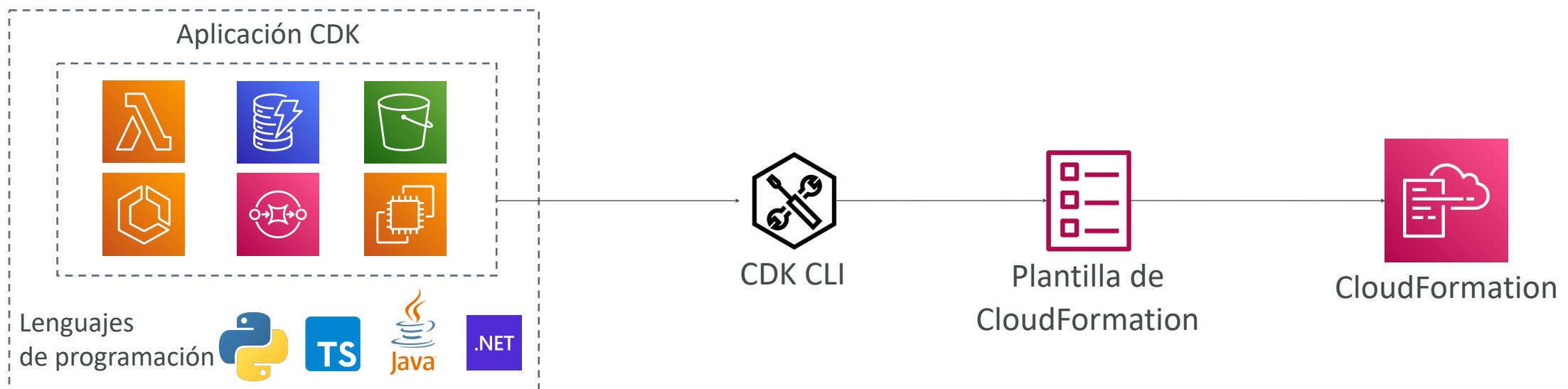
- Ejemplo: Stack de CloudFormation para WordPress
- Podemos ver todos los **recursos**
- Podemos ver las **relaciones** entre los componentes



AWS Cloud Development Kit (CDK)



- Define tu infraestructura de Cloud usando un lenguaje conocido:
 - JavaScript/TypeScript, Python, Java y .NET
- El código se "compila" en una plantilla de CloudFormation (JSON/YAML)
- **Por lo tanto, puedes desplegar juntos la infraestructura y el código de ejecución de la aplicación**
 - Genial para las funciones Lambda
 - Genial para contenedores Docker en ECS / EKS



Ejemplo de CDK

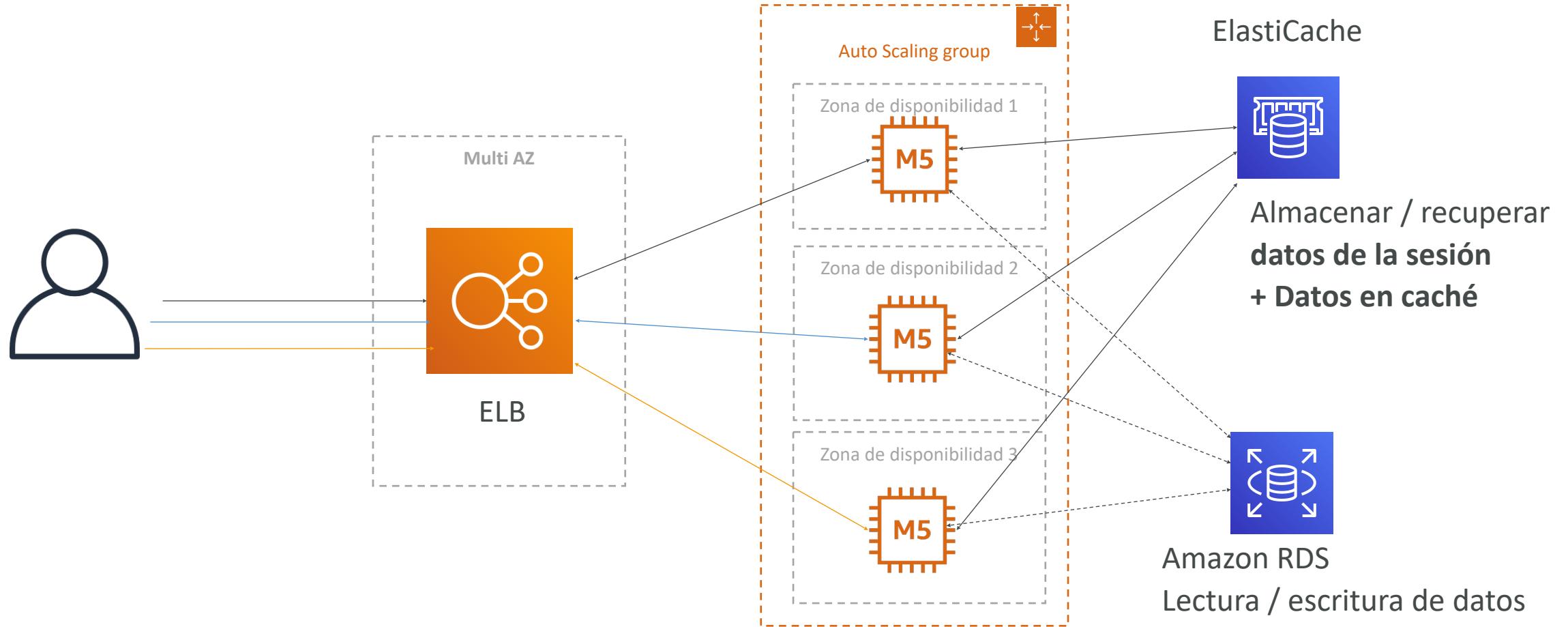
```
export class MyEcsConstructStack extends core.Stack {
  constructor(scope: core.App, id: string, props?: core.StackProps) {
    super(scope, id, props);

    const vpc = new ec2.Vpc(this, "MyVpc", {
      maxAzs: 1 // Default is all AZs in region
    });

    const cluster = new ecs.Cluster(this, "MyCluster", {
      vpc
    });

    // Create a load-balanced Fargate service and make it public
    new ecs_patterns.ApplicationLoadBalancedFargateService(this, "My
      cluster: cluster, // Required
      cpu: 512, // Default is 256
      desiredCount: 6, // Default is 1
      taskImageOptions: { image: ecs.ContainerImage.fromRegistry("an
      memoryLimitMiB: 2048, // Default is 512
      publicLoadBalancer: true // Default is false
    });
  }
}
```

Arquitectura típica: Web App de 3 niveles



Problemas de los desarrolladores en AWS

- Gestión de la infraestructura
 - Desplegar el código
 - Configurar todas las bases de datos, load balancers, etc.
 - Problemas de escalado
-
- La mayoría de las aplicaciones web tienen la misma arquitectura (ALB + ASG)
 - Lo único que quieren los desarrolladores es que su código se ejecute
 - Posiblemente, de forma consistente en diferentes aplicaciones y entornos

Visión general de AWS Elastic Beanstalk



- Elastic Beanstalk es una visión centrada en el desarrollador de la implementación de una aplicación en AWS
 - Utiliza todos los componentes que hemos visto antes: EC2, ASG, ELB, RDS, etc.
 - Pero todo está en una sola vista que es fácil de entender.
 - Seguimos teniendo un control total sobre la configuración
-
- **Beanstalk = Plataforma como servicio (PaaS)**
 - Beanstalk es gratuito, pero pagas por las instancias subyacentes

Elastic Beanstalk

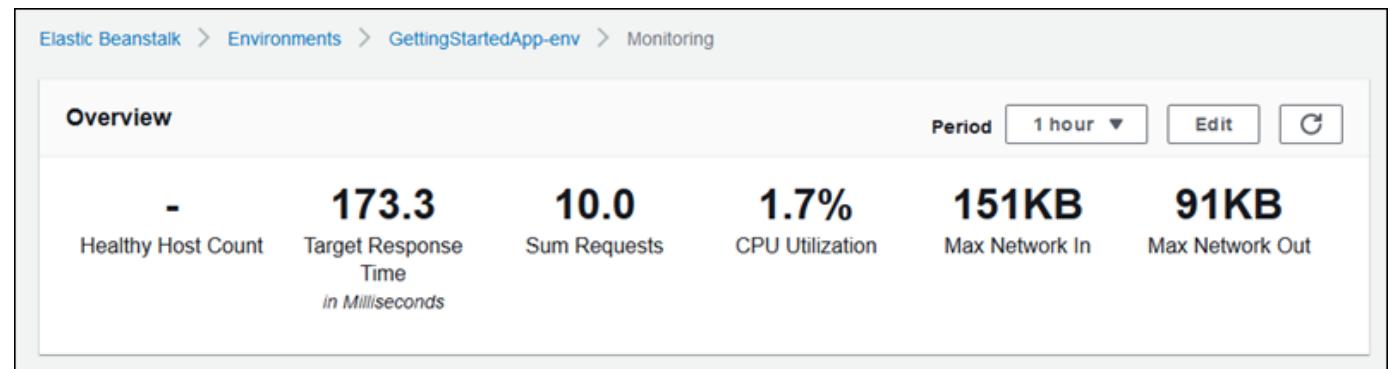
- Servicio gestionado
 - La configuración de la instancia / el sistema operativo es manejado por Beanstalk
 - La estrategia de despliegue es configurable pero la realiza Elastic Beanstalk
 - Aprovisionamiento de capacidad
 - Equilibrio de carga y autoescalado
 - Supervisión del estado de la aplicación y capacidad de respuesta
- **Sólo el código de la aplicación es responsabilidad del desarrollador**
- Tres modelos de arquitectura:
 - Despliegue de instancia única: bueno para el desarrollo
 - LB + ASG: ideal para aplicaciones web de producción o preproducción
 - Sólo ASG: ideal para aplicaciones no web en producción (trabajadores, etc.)

Elastic Beanstalk

- Soporte para muchas plataformas:
 - Go
 - Java SE
 - Java con Tomcat
 - .NET en Windows Server con IIS
 - Node.js
 - PHP
 - Python
 - Ruby
- Constructor de paquetes
- Docker de un solo contenedor
- Docker multicontenedor
- Docker preconfigurado
- Si no es compatible, puedes escribir tu plataforma personalizada (avanzado)

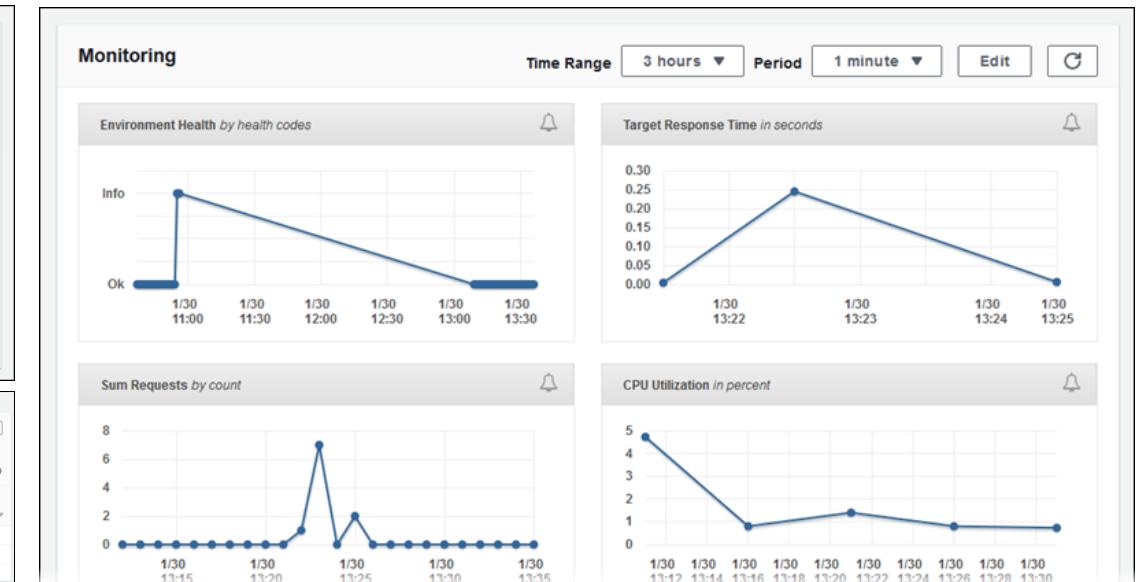
Elastic Beanstalk - Monitorización de salud

- El agente de salud envía las métricas a CloudWatch
- Comprueba la salud de la aplicación, publica los eventos de salud



Recent events

Time	Type	Details
2020-01-28 16:06:04 UTC-0800	INFO	Environment health has transitioned from Severe to Ok.
2020-01-28 16:05:04 UTC-0800	INFO	Added instance [i-03280193ba1ba4171] to your environment.
2020-01-28 16:05:04 UTC-0800	WARN	Removed instance [i-0a4a27bbb9994ba5] from your environment due to a EC2 health check failure.
2020-01-28 16:03:04 UTC-0800	WARN	Environment health has transitioned from Ok to Severe. ELB processes are not healthy on all instances. None of the instances are sending data. ELB health is failing or not available for all instances.
2020-01-28 15:19:06 UTC-0800	INFO	Environment health has transitioned from Info to Ok. Application update completed 75 seconds ago and took 22 seconds.



Enhanced health overview

Instances: 2 Total: 2 Ok

Filter by: Instance actions

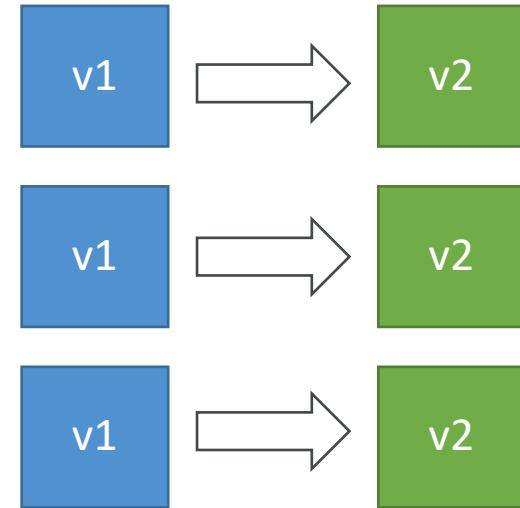
Instance ID	Status	Running	Deployment	Requests/sec	2xx Responses	3xx Responses	4xx Responses	5xx Responses	P99 Latency	P90 Latency	P75 Latency	P50 Latency	Load1 average	Load5 average	CPU utilization User%	CPU utilization Sys%	CPU utilization Idle%	CPU utilization I/O wait%
Overall	Ok	N/A	N/A	0.4	100%	0.0%	0.0%	0.0%	0.002	0.002	0.002	0.001	N/A	N/A	N/A	N/A	N/A	N/A
i-00227007c4ca1334	Ok	2 hours	3	0.2	2	0	0	0	0.002	0.002	0.002	0.002	0.00	0.00	0.0	99.9	0.0	0.0
i-03280193ba1ba4171	Ok	19 days	3	0.2	2	0	0	0.001	0.001	0.001	0.001	0.00	0.00	0.1	0.0	99.9	0.0	

AWS CodeDeploy

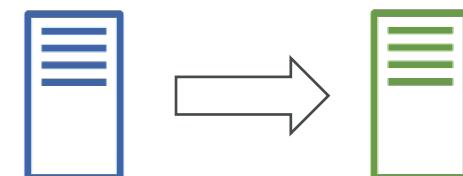


- Queremos desplegar nuestra aplicación **automáticamente**
- **Funciona con instancias EC2**
- **Funciona con servidores locales**
- **Servicio híbrido**
- Los servidores / instancias deben ser aprovisionados y configurados de antemano con el agente de CodeDeploy

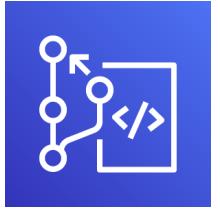
Instancias EC2 que se actualizan



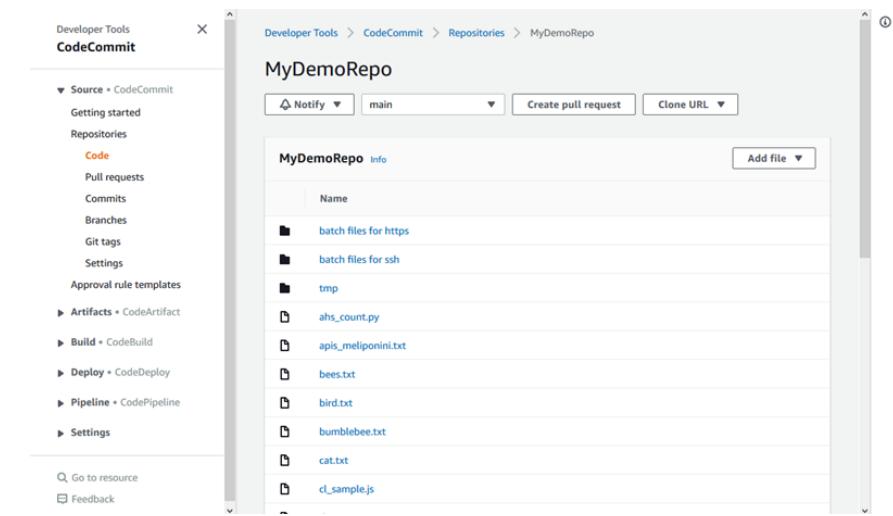
Servidores locales que se actualizan



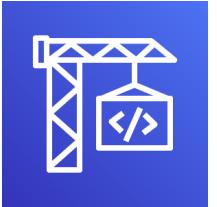
AWS CodeCommit



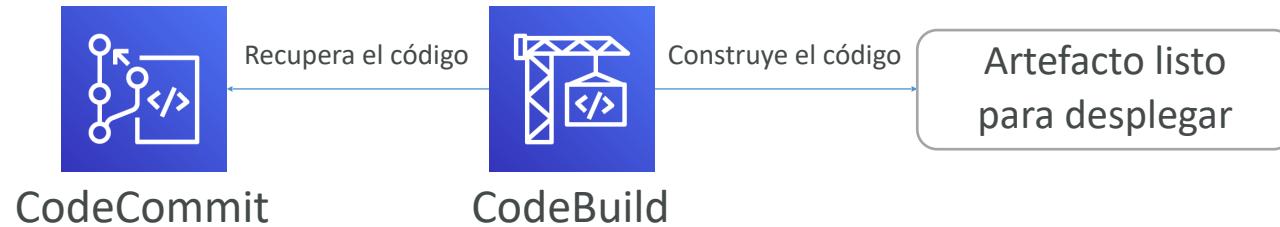
- Antes de enviar el código de la aplicación a los servidores, es necesario almacenarlo en algún lugar
- Los desarrolladores suelen almacenar el **código en un repositorio, utilizando la tecnología Git**
- Una oferta pública famosa es GitHub, el producto competidor de AWS es **CodeCommit**
- CodeCommit:
 - Servicio de control de fuentes que **aloja repositorios basados en Git**
 - Facilita la **colaboración con otros en el código**
 - Los cambios en el código se **versionan** automáticamente
- Ventajas:
 - Totalmente gestionado
 - Escalable y de alta disponibilidad
 - Privado, seguro, integrado con AWS



AWS CodeBuild



- Servicio de construcción de código en el Cloud (el nombre es obvio)
- **Compila el código fuente, ejecuta las pruebas y produce paquetes que están listos para ser desplegados (por CodeDeploy, por ejemplo)**

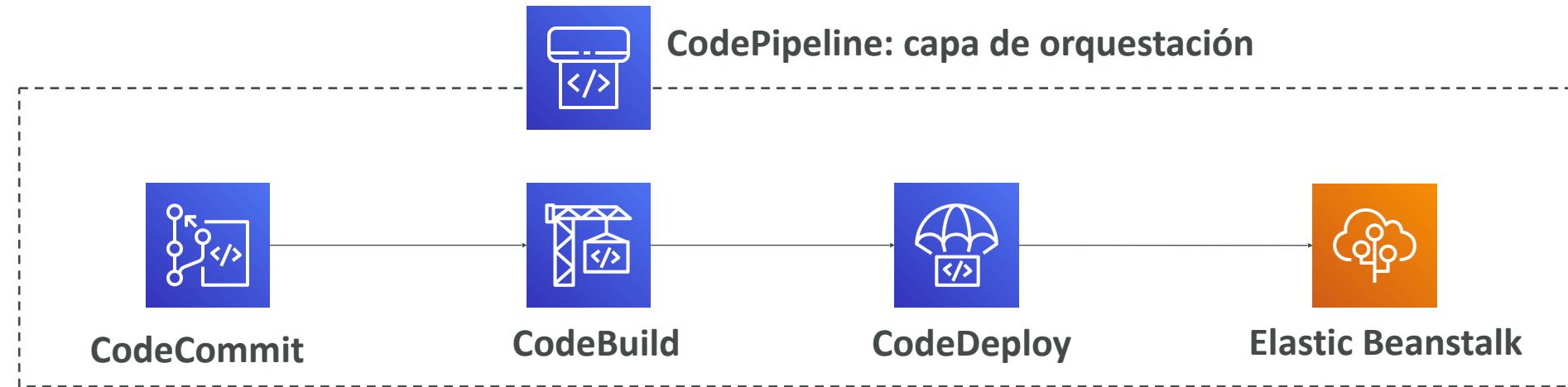


- Ventajas:
 - Totalmente gestionado, sin servidor
 - Continuamente escalable y altamente disponible
 - Seguro
 - Precio de pago por uso: sólo pagas por el tiempo de compilación

AWS CodePipeline



- **Orquestar los diferentes pasos para que el código sea empujado automáticamente a producción**
 - Código => Construir => Probar => Aprovisionar => Desplegar
 - Base de CICD (Integración continua y entrega continua)
- Ventajas:
 - Totalmente gestionado, compatible con CodeCommit, CodeBuild, CodeDeploy, Elastic Beanstalk, CloudFormation, GitHub, servicios de terceros (GitHub...) y plugins personalizados...
 - Entrega rápida y actualizaciones rápidas

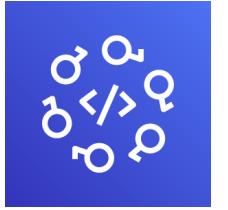


AWS CodeArtifact



- Los paquetes de software dependen unos de otros para ser construidos (también llamados dependencias de código), y se crean otros nuevos
- Almacenar y recuperar estas dependencias se llama **gestión de artefactos**
- Tradicionalmente tienes que configurar tu propio sistema de gestión de artefactos
- **CodeArtifact** es una **gestión de artefactos** segura, escalable y rentable para el desarrollo de software
- Funciona con herramientas comunes de gestión de dependencias como Maven, Gradle, npm, yarn, twine, pip y NuGet
- **Los desarrolladores y CodeBuild pueden recuperar las dependencias directamente desde CodeArtifact**

AWS CodeStar



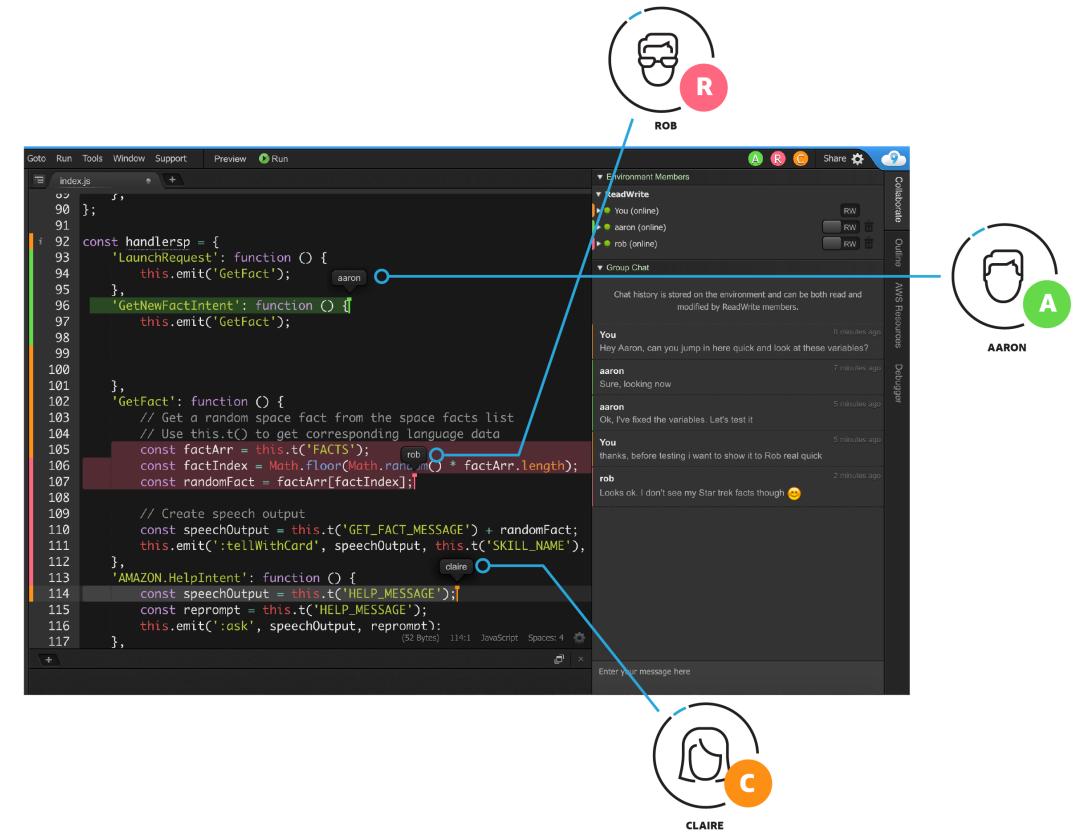
- **Interfaz de usuario unificada** para gestionar fácilmente las actividades de desarrollo de software **en un solo lugar**
- "Forma rápida" de empezar a configurar correctamente CodeCommit, CodePipeline, CodeBuild, CodeDeploy, Elastic Beanstalk, EC2, etc.
- Puedes editar el código "en la nube" utilizando **AWS Cloud9**

The screenshot shows the AWS CodeStar interface for an 'EC2 Web Application'. On the left, a sidebar lists navigation options: Dashboard, Code, Build, Deploy, Pipelines, Team, and Extensions. The main area has two main sections: 'Application activity' showing CPU Utilization over time (with a sharp peak around 21:00) and 'Continuous deployment' showing the flow from Source (CodeCommit) through Build (CodeBuild) to Application (CodeDeploy). The 'Commit history' section on the left lists recent commits by users like JD, HH, TO, T, and J, each with a commit ID and timestamp. A 'Team wiki tile' at the bottom allows for sharing project links and notes.

AWS Cloud9



- AWS Cloud9 es un IDE (Entorno de Desarrollo Integrado) en el Cloud para escribir, ejecutar y depurar código
- Los IDE "clásicos" (como IntelliJ, Visual Studio Code...) se descargan en un ordenador antes de ser utilizados
- Un IDE en el Cloud se puede utilizar dentro de un navegador web, lo que significa que puedes trabajar en tus proyectos desde tu oficina, casa o cualquier lugar con Internet sin necesidad de configuración
- AWS Cloud9 también permite la colaboración de código en tiempo real (pair programming)



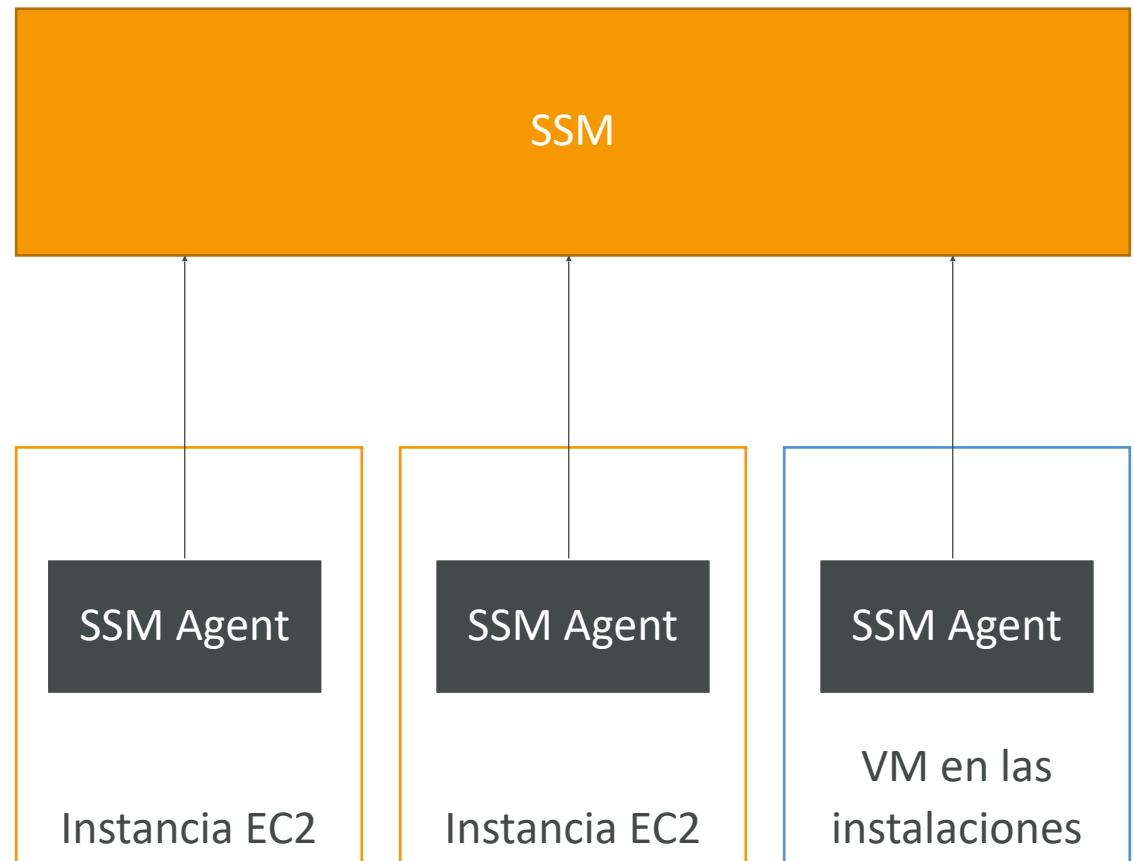
AWS Systems Manager (SSM)



- Te ayuda a gestionar tus sistemas **EC2 y On-Premises** a escala
- Otro servicio **híbrido** de AWS
- Obtén información operativa sobre el estado de tu infraestructura
- Conjunto de más de 10 productos
- Las características más importantes son:
 - **Automatización de parches para mejorar la normativa**
 - **Ejecuta comandos en toda una flota de servidores**
 - Almacena la configuración de los parámetros con el almacén de parámetros SSM
 - Funciona para Linux, Windows, MacOs y Raspberry Pi OS (Raspbian)

Cómo funciona Systems Manager

- Necesitamos instalar el agente SSM en los sistemas que controlamos
- Se instala por defecto en las AMI de Amazon Linux y en algunas AMI de Ubuntu
- Si una instancia no puede ser controlada con SSM, probablemente se trate de un problema con el agente SSM
- Gracias al agente SSM, podemos **ejecutar comandos, parchear y configurar** nuestros servidores

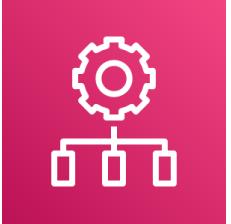


Systems Manager – SSM Session Manager

- Te permite iniciar un shell seguro en tus servidores EC2 y locales
- **No se necesita acceso SSH ni claves SSH**
- **No se necesita el puerto 22 (mayor seguridad)**
- Envía los datos de registro de la sesión a S3 o a CloudWatch Logs



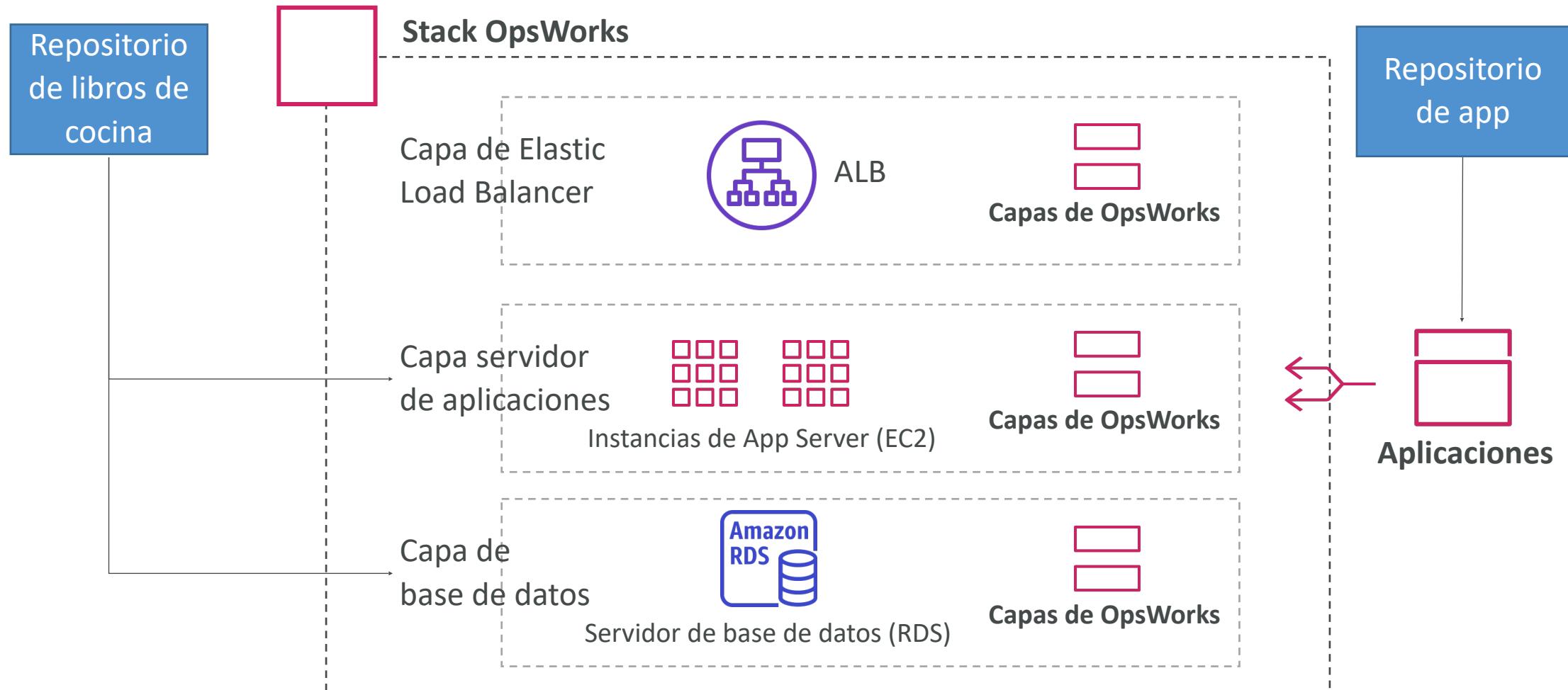
AWS OpsWorks



- Chef y Puppet te ayudan a realizar la configuración del servidor de forma automática, o acciones repetitivas
- Funcionan muy bien con EC2 y VM On-Premises
- AWS OpsWorks = Chef y Puppet gestionados
- Es una alternativa a AWS SSM
- Sólo aprovisiona **recursos estándar de AWS**:
 - Instancias EC2, bases de datos, balanceadores de carga, volúmenes EBS...
- **En el examen: Se necesita Chef o Puppet => AWS OpsWorks**



Arquitectura de OpsWorks



Resumen - Despliegue

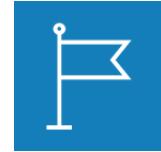
- **CloudFormation:** (sólo AWS)
 - Infraestructura como código, funciona con casi todos los recursos de AWS
 - Se repite en todas las regiones y cuentas
- **Beanstalk:** (sólo AWS)
 - Plataforma como servicio (PaaS), limitada a ciertos lenguajes de programación o Docker
 - Implementa el código de forma coherente con una arquitectura conocida: por ejemplo, ALB + EC2 + RDS
- **CodeDeploy** (híbrido): despliega y actualiza cualquier aplicación en los servidores
- **Systems Manager** (híbrido): parchea, configura y ejecuta comandos a escala
- **OpsWorks** (híbrido): gestiona Chef y Puppet en AWS

Resumen - Servicios para desarrolladores

- **CodeCommit:** Almacena el código en un repositorio git privado (versión controlada)
- **CodeBuild:** Construye y prueba el código en AWS
- **CodeDeploy:** Implementa el código en los servidores
- **CodePipeline:** Orquestación del pipeline (desde el código hasta la construcción y el despliegue)
- **CodeArtifact:** Almacena paquetes de software / dependencias en AWS
- **CodeStar:** Vista unificada para permitir a los desarrolladores hacer CI/CD y código
- **Cloud9:** IDE (Entorno de Desarrollo Integrado) en el Cloud con collab
- **AWS CDK:** Define tu infraestructura en el Cloud utilizando un lenguaje de programación

Infraestructura Global

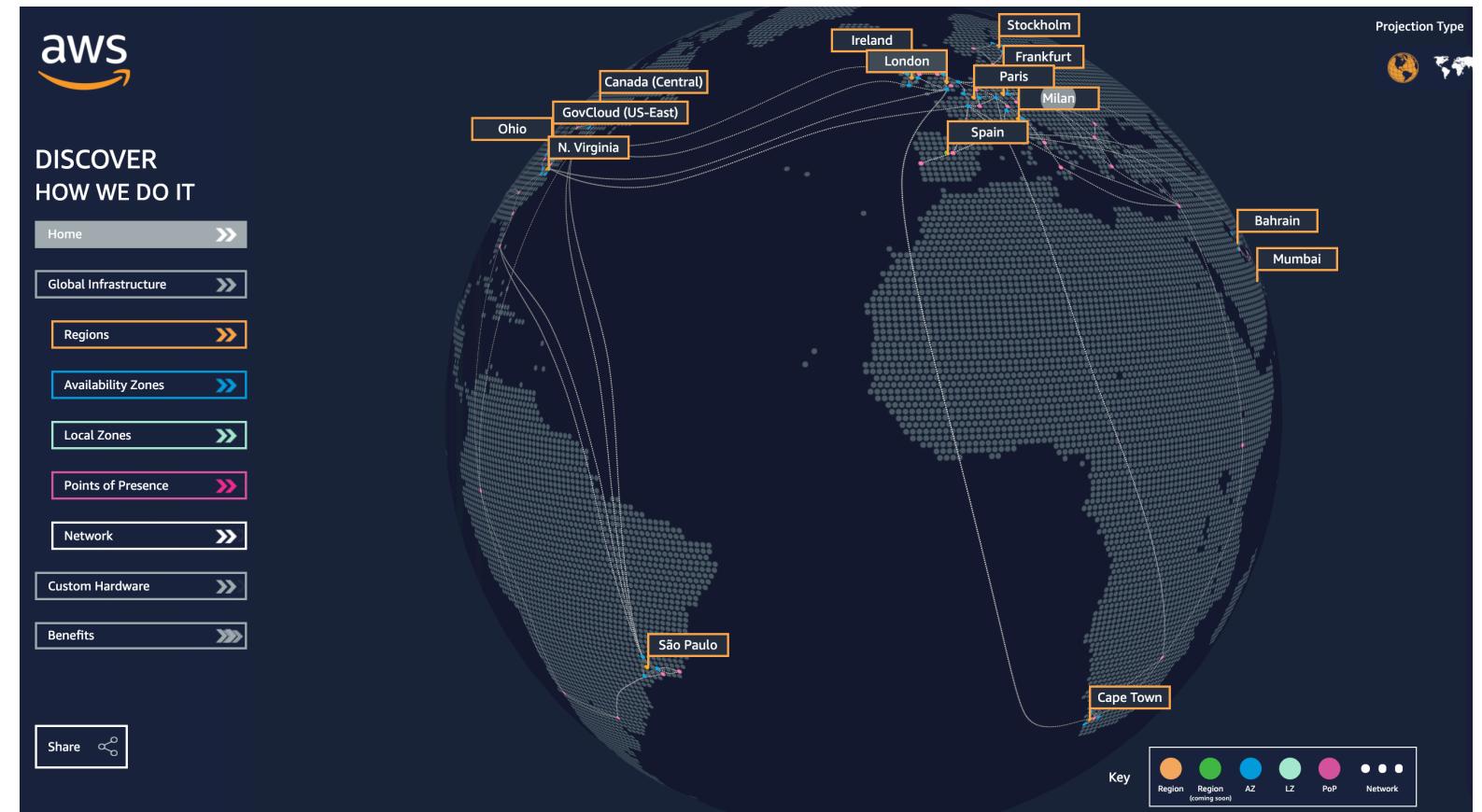
¿Por qué hacer una solicitud global?



- Una **aplicación global** es una aplicación desplegada en **múltiples geografías**
- En AWS: pueden ser **regiones** y/o **edge locations**
- **Disminución de la latencia**
 - La latencia es el tiempo que tarda un paquete de red en llegar a un servidor
 - Un paquete de Asia tarda en llegar a Estados Unidos
 - Implementa tus aplicaciones más cerca de tus usuarios para disminuir la latencia y mejorar la experiencia
- **Recuperación de desastres (Disaster Recovery - DR)**
 - Si una región de AWS se cae (terremoto, tormentas, corte de energía, política)...
 - Puedes comutar por error a otra región y que tu aplicación siga funcionando
 - Un plan de RD es importante para aumentar la disponibilidad de tu aplicación
- **Protección contra ataques:** la infraestructura global distribuida es más difícil de atacar

Infraestructura global de AWS

- **Regiones:** Para desplegar aplicaciones e infraestructura
- **Zonas de disponibilidad:** Formadas por múltiples centros de datos
- **Edge Location (puntos de presencia):** para la entrega de contenidos lo más cerca posible de los usuarios
- Más en: <https://infrastructure.aws/>



Aplicaciones globales en AWS

- **DNS global: Route 53**

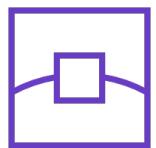


- Genial para encaminar a los usuarios al despliegue más cercano con la menor latencia
- Excelente para las estrategias de recuperación de desastres



- **Red global de entrega de contenidos (CDN): CloudFront**

- Replica parte de tu aplicación a las ubicaciones edge de AWS - disminuye la latencia
- Almacena las solicitudes comunes - mejora la experiencia del usuario y disminuye la latencia



- **S3 Transfer Acceleration:**

- Acelera las cargas y descargas globales en Amazon S3



- **AWS Global Accelerator:**

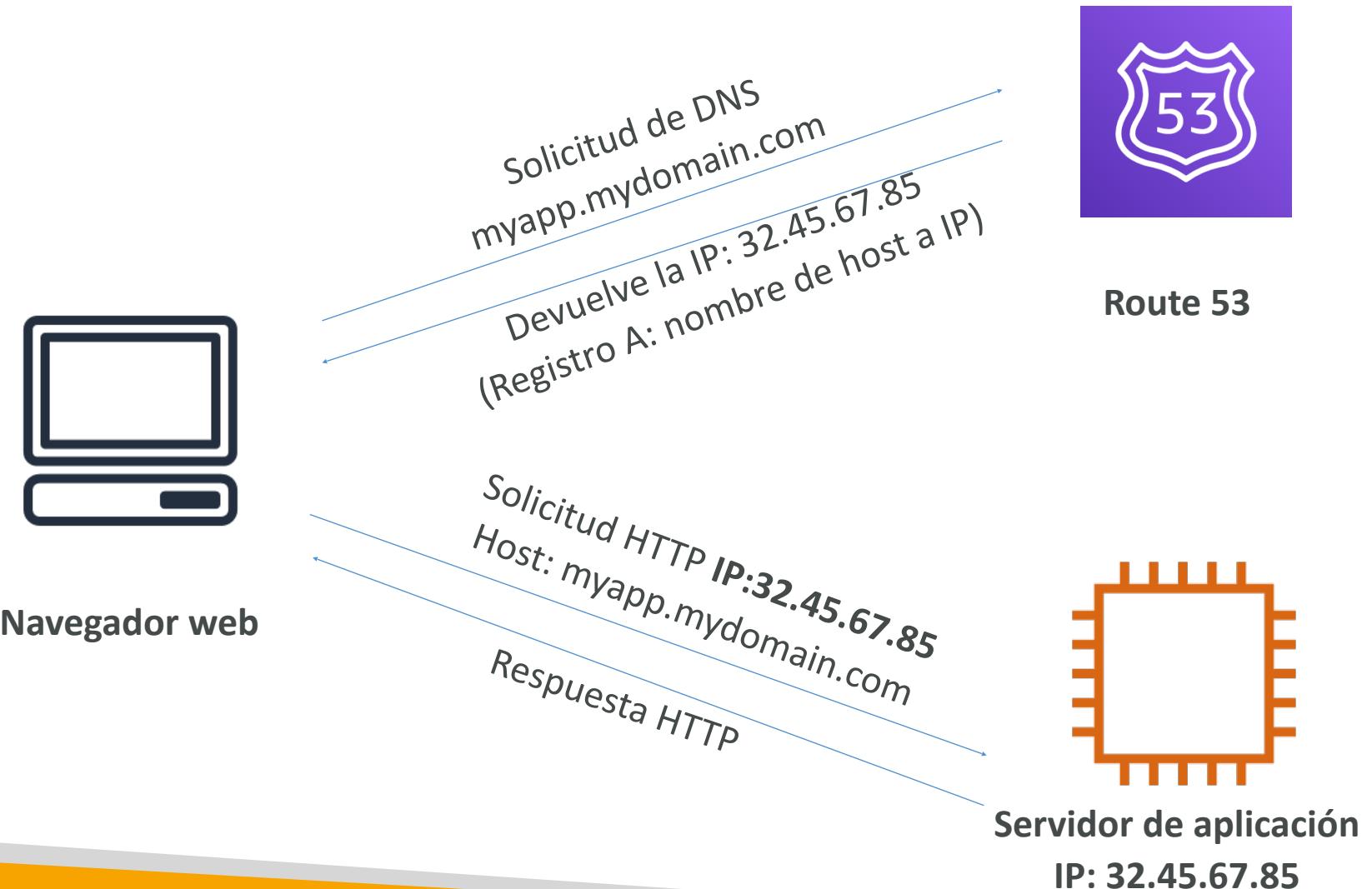
- Mejora la disponibilidad y el rendimiento de las aplicaciones globales utilizando la red global de AWS

Visión general de Amazon Route 53



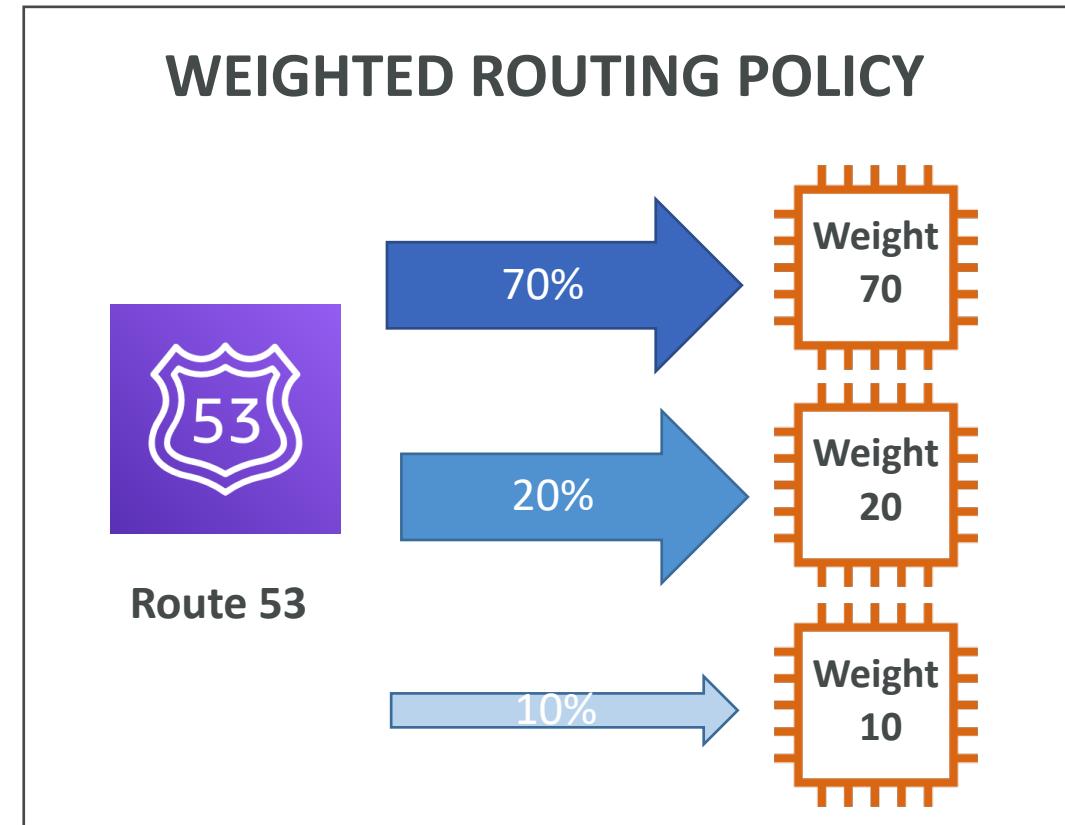
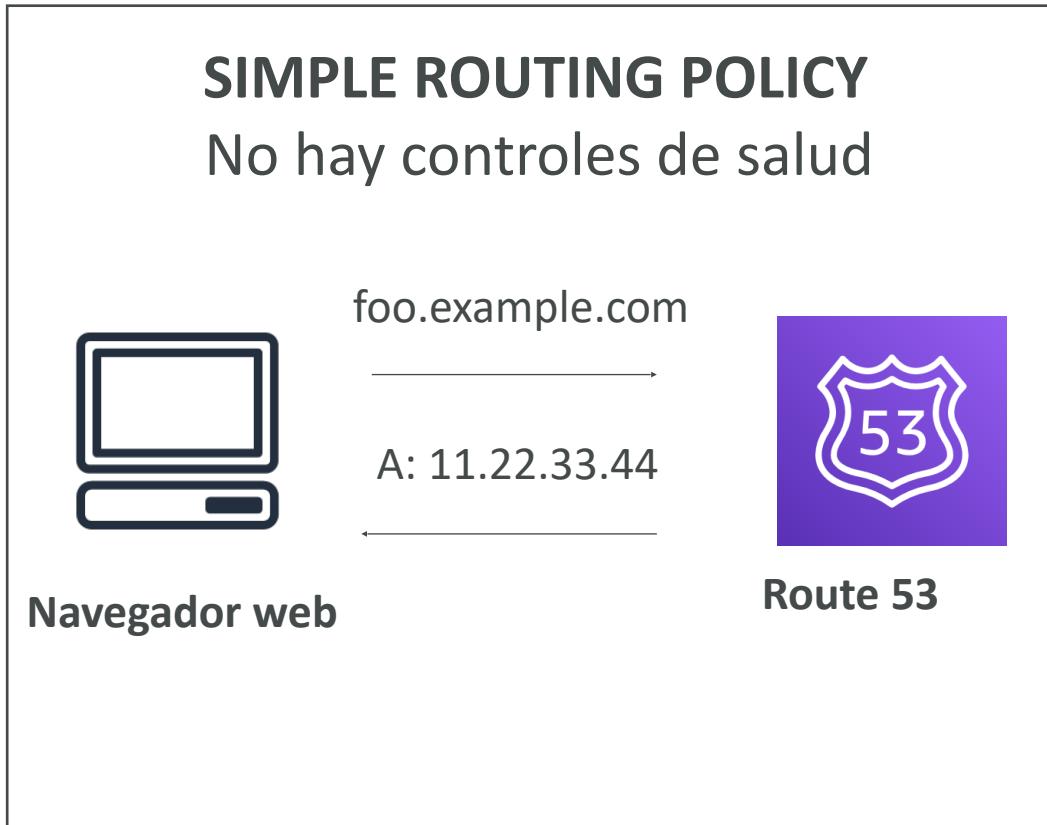
- Route53 es un DNS gestionado (Sistema de Nombres de Dominio)
- El DNS es una colección de reglas y registros que ayuda a los clientes a entender cómo llegar a un servidor a través de las URL
- En AWS, los registros más comunes son
 - www.google.com => 12.34.56.78 == **Registro A (IPv4)**
 - www.google.com => 2001:0db8:85a3:0000:0000:8a2e:0370:7334 == **AAAAA IPv6**
 - search.google.com => www.google.com == **CNAME: nombre de host a nombre de host**
 - ejemplo.com => recurso AWS == **Alias (ej: ELB, CloudFront, S3, RDS, etc...)**

Route 53 - Diagrama para un registro



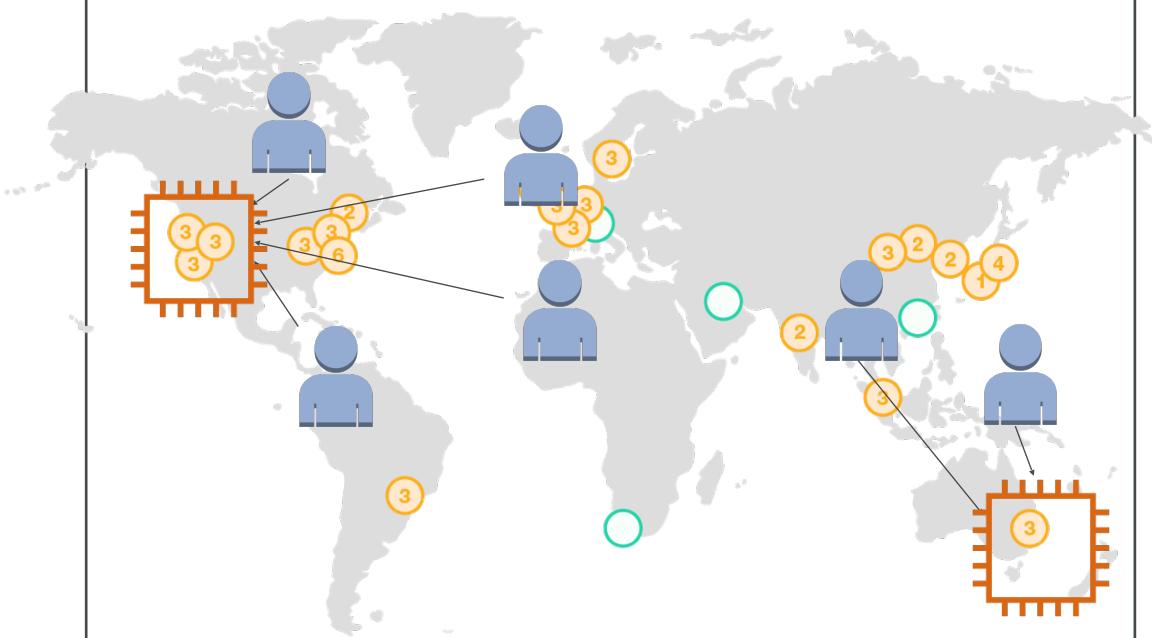
Políticas de enrutamiento de Amazon Route 53

- Necesidad de conocerlas a alto nivel para el examen Cloud Practitioner



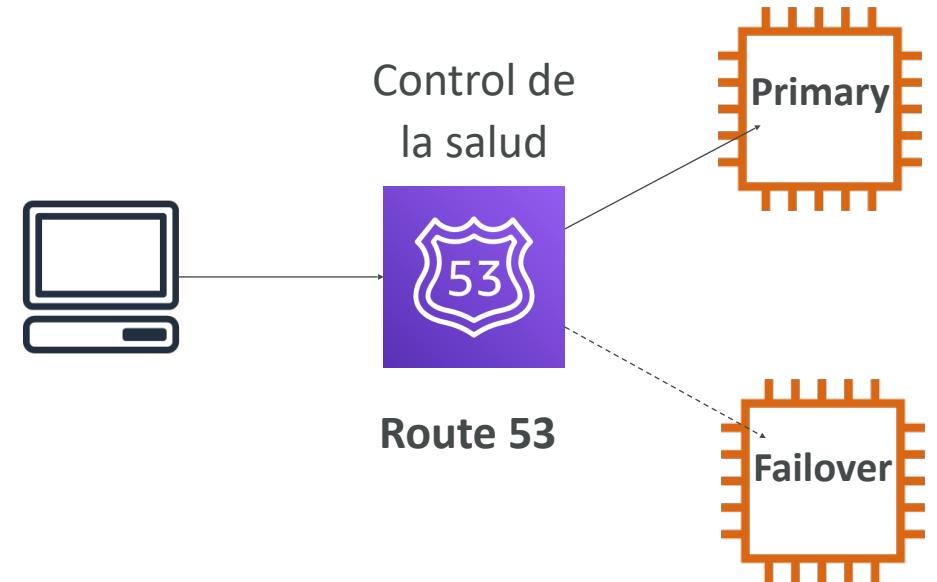
Políticas de enrutamiento de Route 53

LATENCY ROUTING POLICY

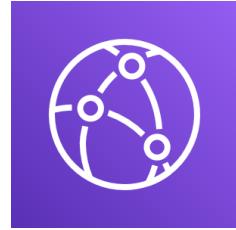


FAILOVER ROUTING POLICY

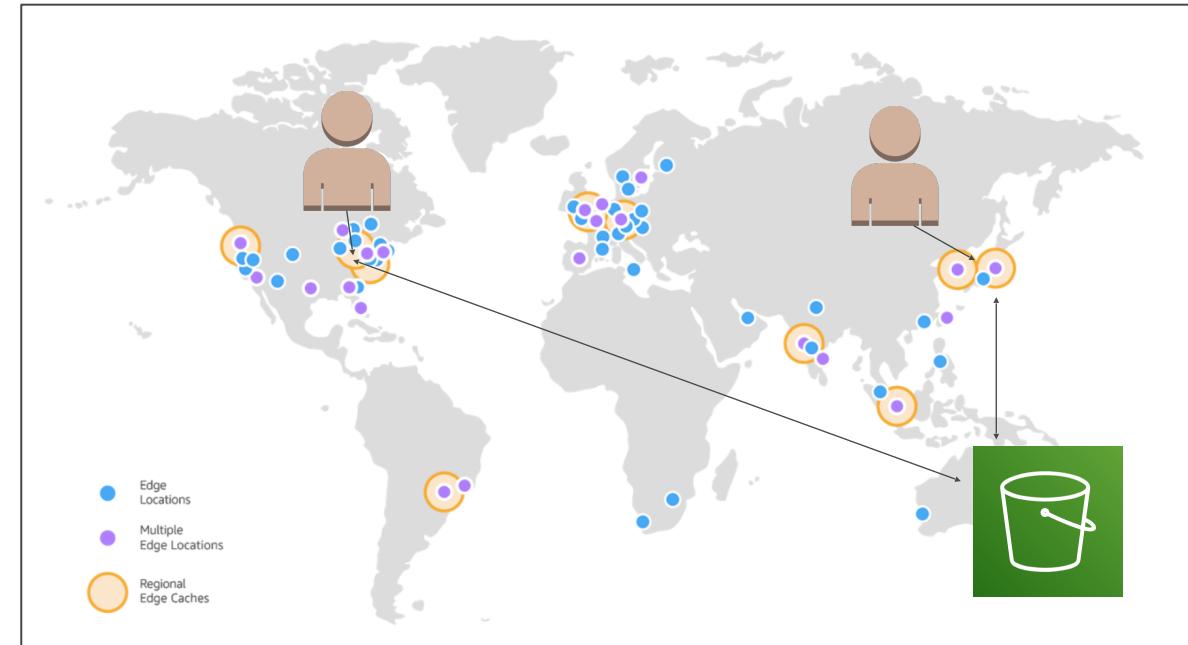
Recuperación de desastres



AWS CloudFront



- Red de entrega de contenidos (CDN)
- **Mejora el rendimiento de lectura, el contenido se almacena en caché en edge location**
- Mejora la experiencia de los usuarios
- +400 puntos de presencia a nivel mundial (ubicaciones edge)
- **Protección DDoS, integración con Shield, AWS Web Application Firewall**



Fuente: <https://aws.amazon.com/cloudfront/features/?nc=sn&loc=2>

CloudFront - Orígenes

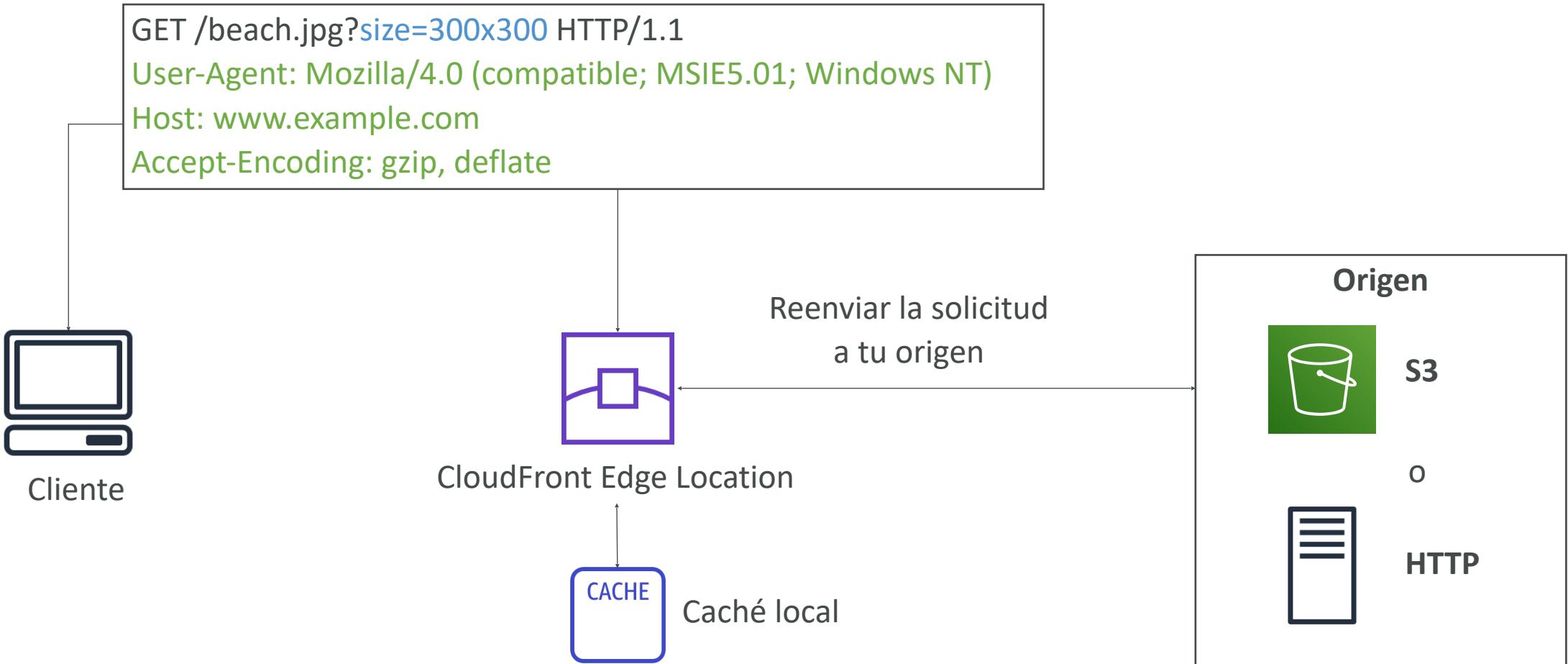
- **Bucket S3**

- Para distribuir archivos y almacenarlos en caché en el borde
- Seguridad mejorada con CloudFront **Origin Access Control (OAC)**
- OAC sustituye a Origin Access Identity (OAI)
- CloudFront puede utilizarse como entrada (para subir archivos a S3)

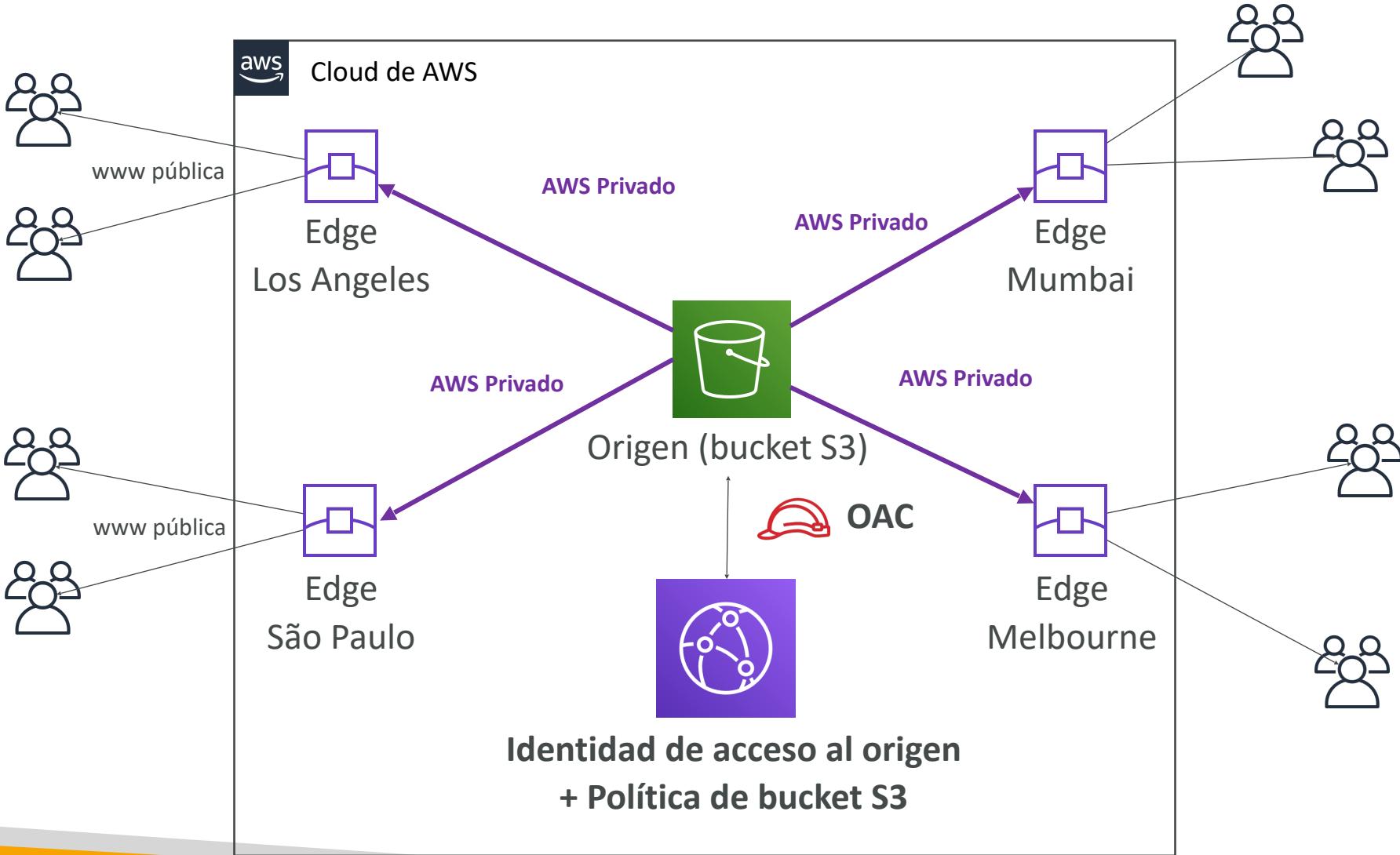
- **Origen personalizado (HTTP)**

- Application Load Balancer
- Instancia EC2
- Sitio web S3 (primero debes habilitar el bucket como sitio web S3 estático)
- Cualquier backend HTTP que deseas

CloudFront a alto nivel



CloudFront - S3 como origen

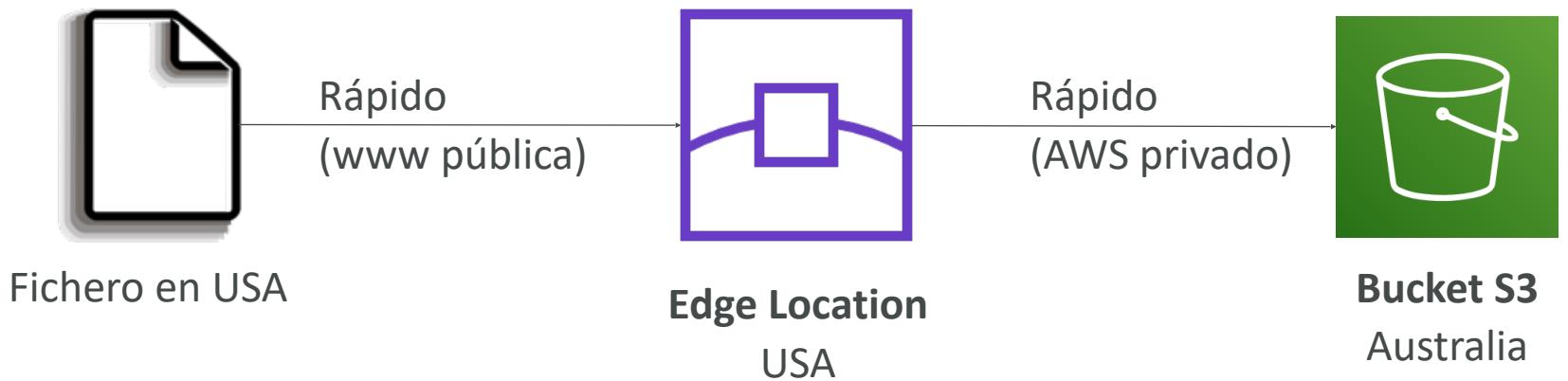


CloudFront vs S3 Cross Region Replication (CRR)

- CloudFront:
 - Red Global Edge
 - Los archivos se almacenan en caché durante un TTL (quizás un día)
 - **Es ideal para contenidos estáticos que deben estar disponibles en todas partes**
- S3 Cross Region Replication (CRR):
 - Debe configurarse para cada región en la que quieras que se produzca la replicación
 - Los archivos se actualizan casi en tiempo real
 - Sólo lectura
 - **Ideal para contenidos dinámicos que deben estar disponibles con baja latencia en pocas regiones**

S3 Transfer Acceleration

- Aumenta la velocidad de transferencia transfiriendo el archivo a una ubicación edge de AWS que reenviará los datos al bucket de S3 en la región de destino

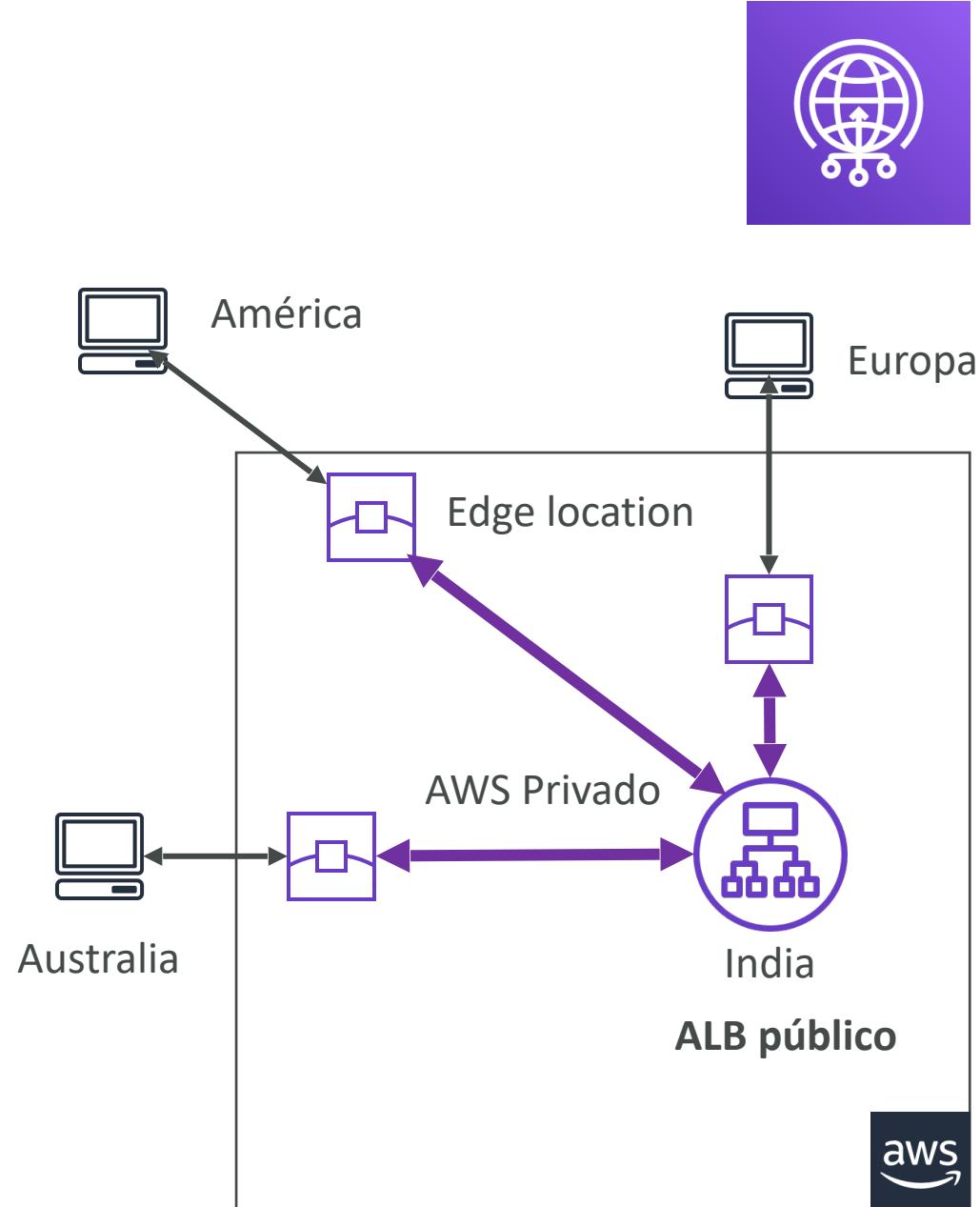


Prueba la herramienta en:

<https://s3-accelerate-speedtest.s3-accelerate.amazonaws.com/en/accelerate-speed-comparison.html>

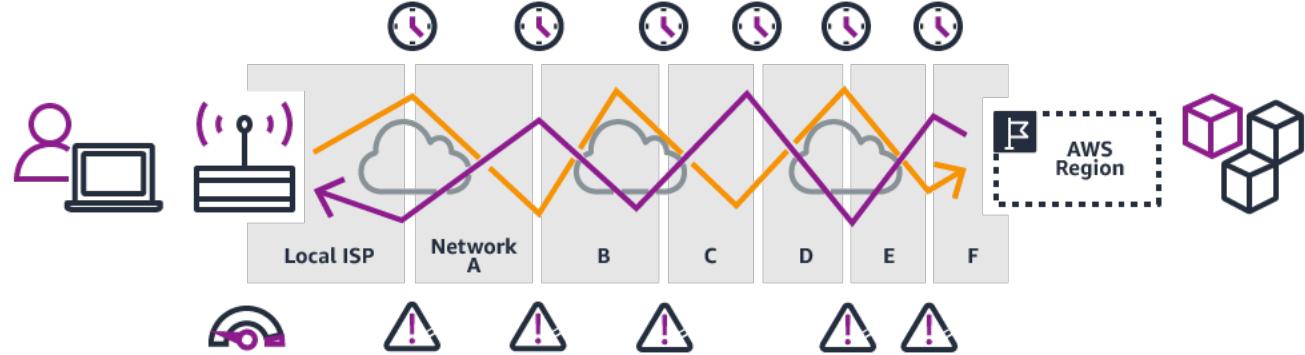
AWS Global Accelerator

- Mejora la disponibilidad y el rendimiento global de la aplicación utilizando la red global de AWS
- Aprovecha la red interna de AWS para optimizar la ruta hacia tu aplicación (60% de mejora)
- Se crean **2 IP Anycast** para tu aplicación y el tráfico se envía a través de los **puntos de presencia (Edge Locations)**
- Las Edge Locations envían el tráfico a tu aplicación

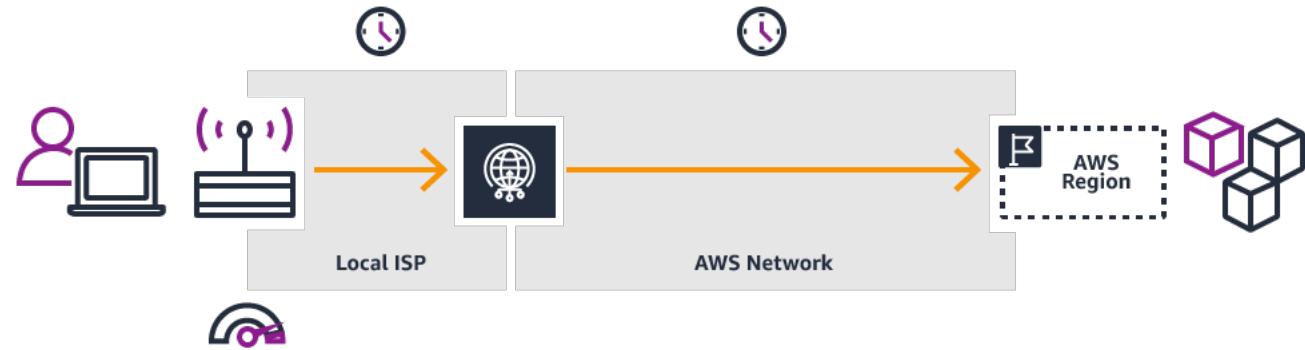


AWS Global Accelerator

Sin Global Accelerator



Con Global Accelerator

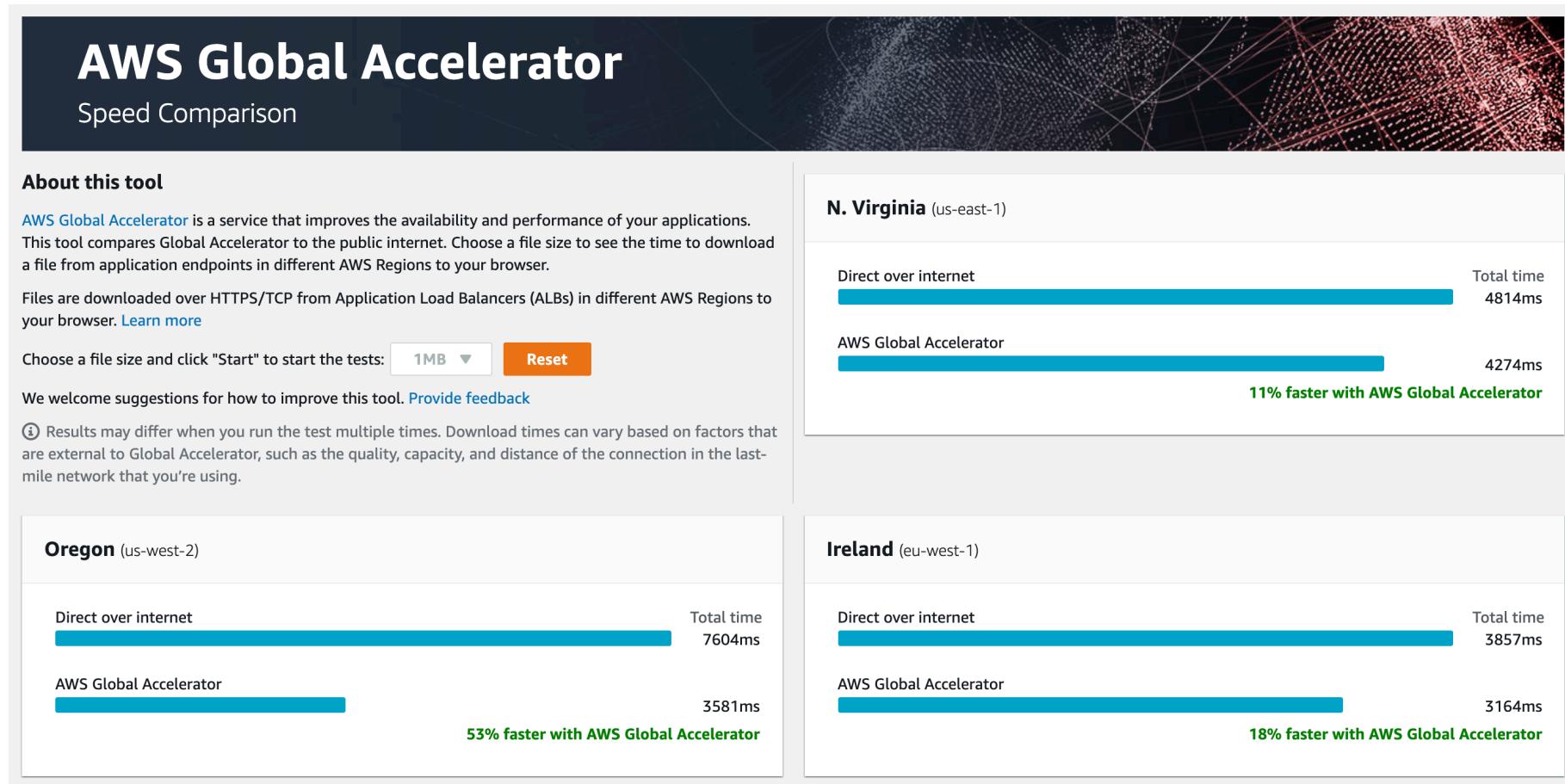


<https://aws.amazon.com/global-accelerator>

AWS Global Accelerator vs CloudFront

- Ambos utilizan la red global de AWS y sus ubicaciones de borde en todo el mundo
- Ambos servicios se integran con AWS Shield para la protección DDoS
- **CloudFront - Red de entrega de contenidos (CDN)**
 - Mejora el rendimiento de tu contenido almacenable en caché (como imágenes y videos)
 - El contenido se entrega en edge location
- **Global Accelerator**
 - Sin almacenamiento en caché, proxy de paquetes en el borde a las aplicaciones que se ejecutan en una o más regiones de AWS.
 - Mejora el rendimiento de una amplia gama de aplicaciones sobre TCP o UDP
 - Bueno para casos de uso de HTTP que requieren direcciones IP estáticas
 - Bueno para casos de uso de HTTP que requieran una comutación por error regional determinista y rápida

<https://speedtest.globalaccelerator.aws/#/>



AWS Outposts



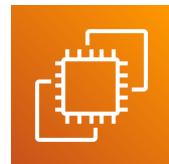
- **Cloud híbrido:** empresas que mantienen una infraestructura local junto a una infraestructura en la nube
- Por lo tanto, hay dos formas de tratar con los sistemas de IT:
 - Una para el Cloud de AWS (utilizando la consola de AWS, la CLI y las API de AWS)
 - Una para su infraestructura on-premise
- **Los AWS Outposts son "racks de servidores"** que ofrecen la misma infraestructura, servicios, API y herramientas de AWS para crear tus propias aplicaciones en las instalaciones al igual que en el Cloud
- **AWS configurará y administrará los "racks Outposts"** dentro de tu infraestructura local y podrás empezar a aprovechar los servicios de AWS en las instalaciones
- Eres responsable de la seguridad física del rack de Outposts



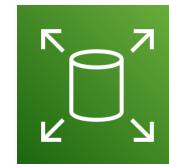
AWS Outposts



- Ventajas:
 - Acceso de baja latencia a los sistemas locales
 - Procesamiento local de datos
 - Residencia de datos
 - Migración más fácil de las instalaciones a el Cloud
 - Servicio totalmente gestionado
- Algunos servicios que funcionan en Outposts:



Amazon EC2



Amazon EBS



Amazon S3



Amazon EKS



Amazon ECS



Amazon RDS

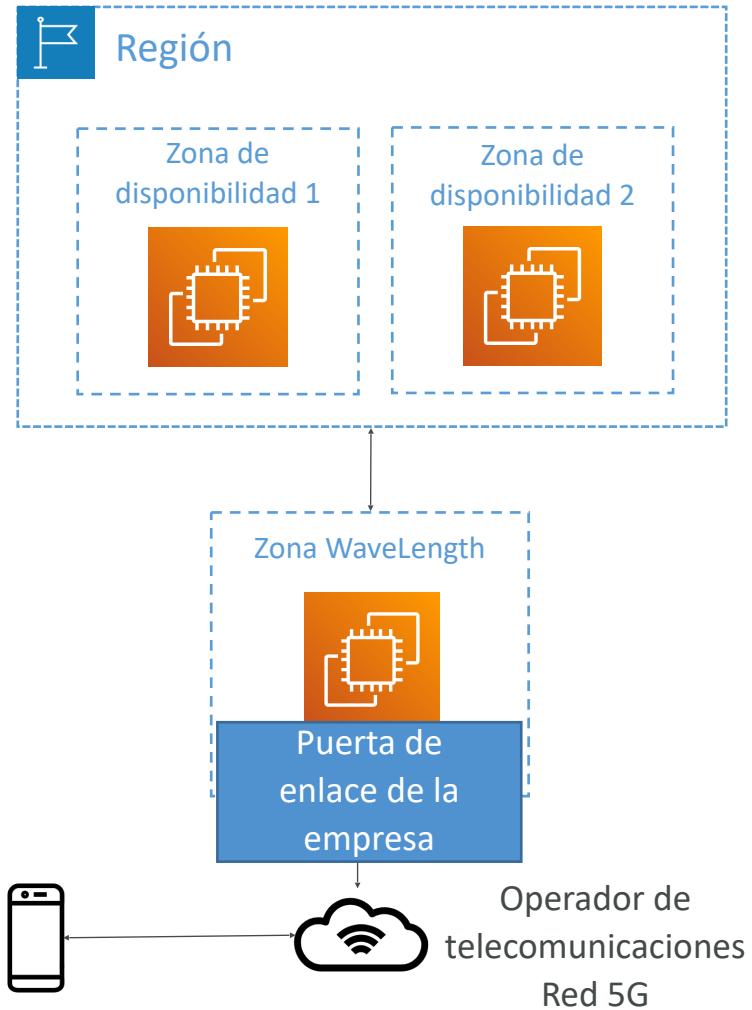


Amazon EMR

AWS WaveLength



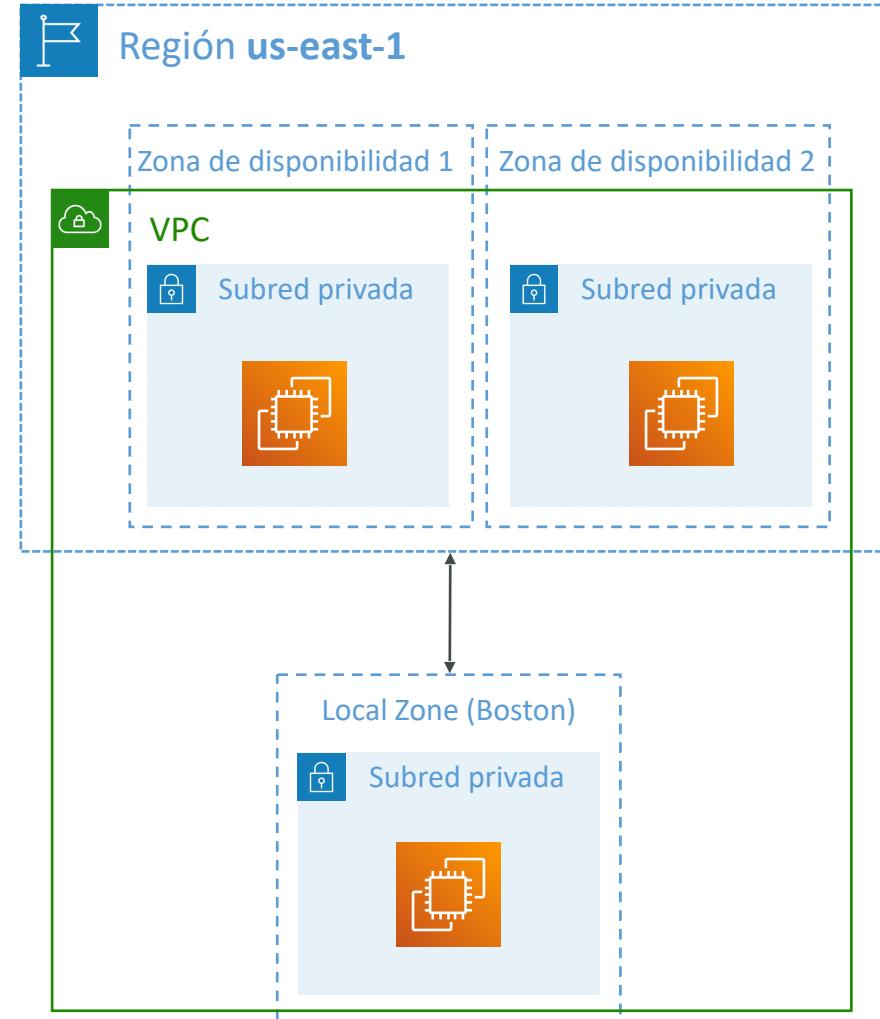
- Las **WaveLength Zones** son despliegues de infraestructura incrustados en los centros de datos de los proveedores de telecomunicaciones de las redes 5G
- Lleva los servicios de AWS al límite de las redes 5G
- Ejemplo: EC2, EBS, VPC...
- Aplicaciones de latencia ultrabaja a través de las redes 5G
- El tráfico no sale de la red del proveedor de servicios de comunicación (CSP)
- Conexión segura y de gran ancho de banda con la región AWS matriz
- Sin cargos adicionales ni acuerdos de servicio
- Casos de uso: Ciudades inteligentes, diagnósticos asistidos por ML, vehículos conectados, flujos de vídeo en directo interactivos, AR/VR, juegos en tiempo real, ...



AWS Local Zones



- Coloca la informática, el almacenamiento, la base de datos y otros servicios de AWS seleccionados más cerca de los **usuarios finales para ejecutar aplicaciones sensibles a la latencia**
- Amplía tu VPC a más ubicaciones - "**Extensión de una región de AWS**"
- Compatible con EC2, RDS, ECS, EBS, ElastiCache, Direct Connect ...
- Ejemplo:
 - **Región de AWS:** N.Virginia (us-east-1)
 - **AWS Local Zones:** Boston, Chicago, Dallas, Houston, Miami, ...



Arquitectura global de aplicaciones

Región única, AZ única

✗ Alta disponibilidad

✗ Latencia global

⚡ Dificultad



Región única, AZ múltiple

✓ Alta disponibilidad

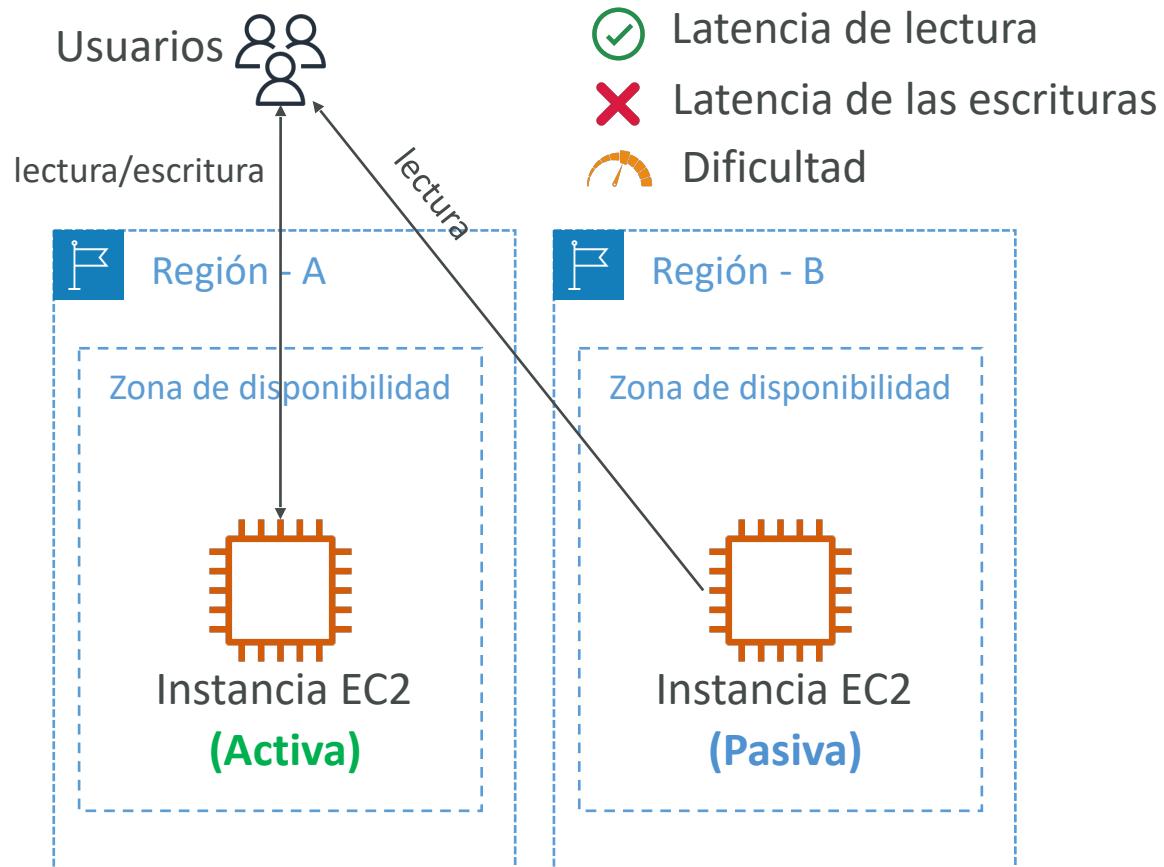
✗ Latencia global

⚡ Dificultad

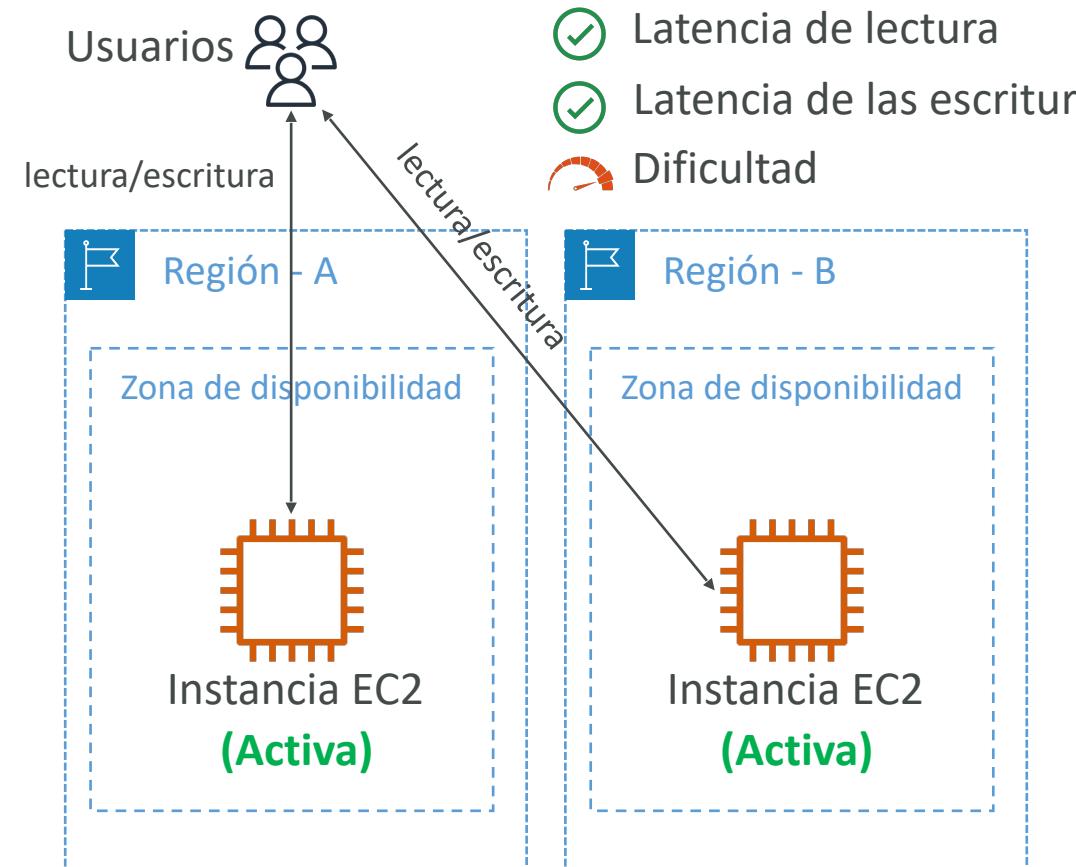


Arquitectura global de aplicaciones

Multi Región, Activa-Pasiva



Multi Región, Activa-Activa



Resumen - Aplicaciones globales en AWS



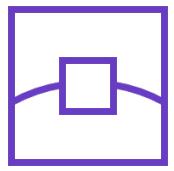
- **DNS global: Route 53**

- Genial para dirigir a los usuarios a la implementación más cercana con la menor latencia
- Excelente para las estrategias de recuperación de desastres



- **Red global de entrega de contenidos (CDN): CloudFront**

- Replica parte de tu aplicación a las ubicaciones de borde de AWS - disminuye la latencia
- Almacena las solicitudes comunes - mejora la experiencia del usuario y disminuye la latencia



- **S3 Transfer Acceleration**

- Acelera las cargas y descargas globales en Amazon S3



- **AWS Global Accelerator**

- Mejora la disponibilidad y el rendimiento de la aplicación global utilizando la red global de AWS

Resumen - Aplicaciones globales en AWS



- **AWS Outposts**

- Implementa racks Outposts en tus propios centros de datos para ampliar los servicios de AWS



- **AWS WaveLength**

- Lleva los servicios de AWS a edge location de las redes 5G
- Aplicaciones de latencia ultrabaja



- **AWS Local Zones**

- Acerca los recursos de AWS (computación, base de datos, almacenamiento, ...) a tus usuarios
- Buenas para aplicaciones sensibles a la latencia

Integración en el Cloud

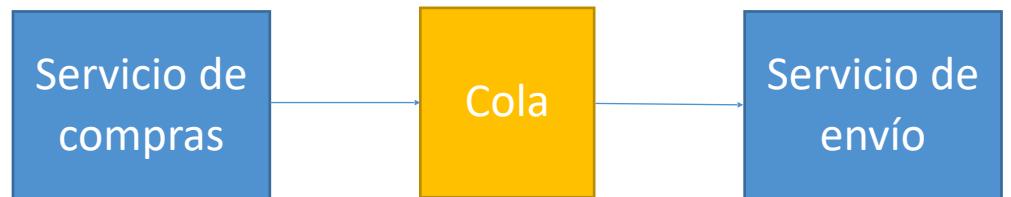
Introducción a la sección

- Cuando empezamos a desplegar varias aplicaciones, es inevitable que tengan que comunicarse entre sí
- Hay dos patrones de comunicación entre aplicaciones

**1) Comunicaciones sincrónicas
(de aplicación a aplicación)**



**2) Asíncrona / basada en eventos
(de la aplicación a la cola a la aplicación)**

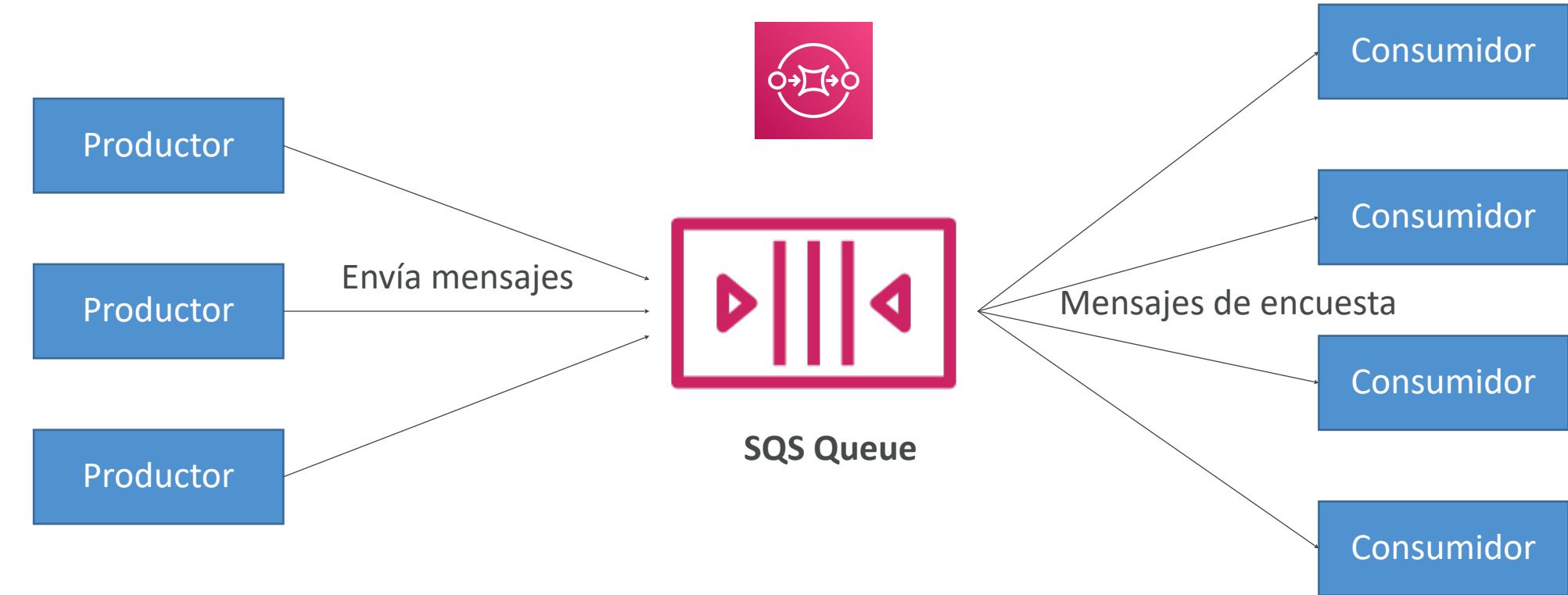


Introducción a la sección

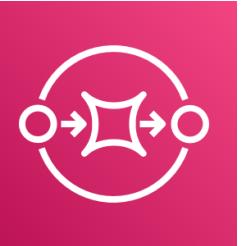
- La sincronización entre aplicaciones puede ser problemática si hay picos repentinos de tráfico
- ¿Qué pasa si de repente necesitas codificar 1000 vídeos, pero normalmente son 10?
- En ese caso, es mejor **desacoplar** tus aplicaciones:
 - usando SQS: modelo de cola
 - usando SNS: modelo pub/sub
 - utilizando Kinesis: modelo de flujo de datos en tiempo real
- ¡Estos servicios pueden escalar independientemente de nuestra aplicación!

Amazon SQS – Simple Queue Service

¿Qué es una cola?



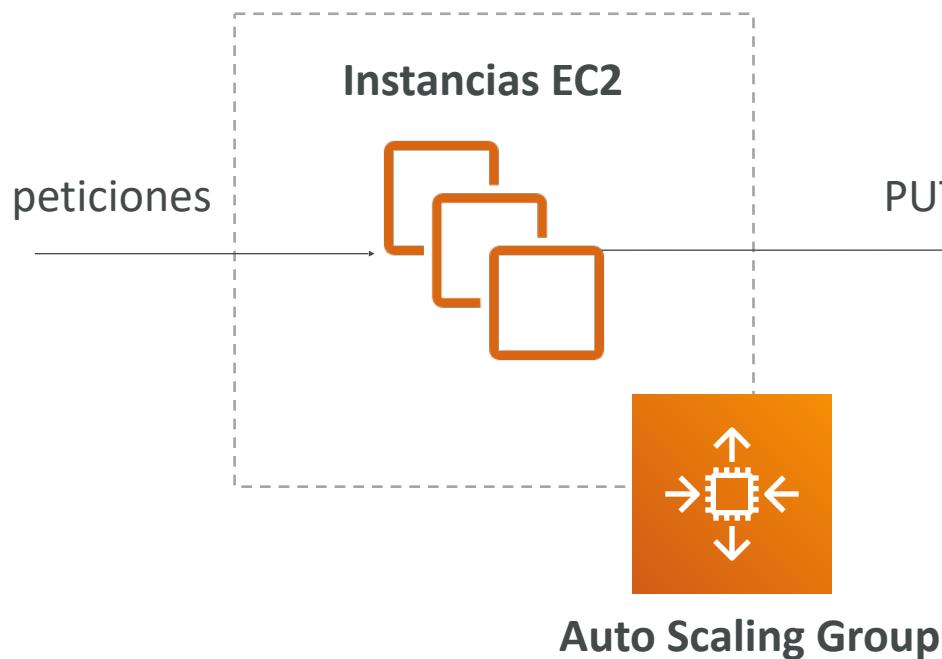
Amazon SQS – Cola estándar



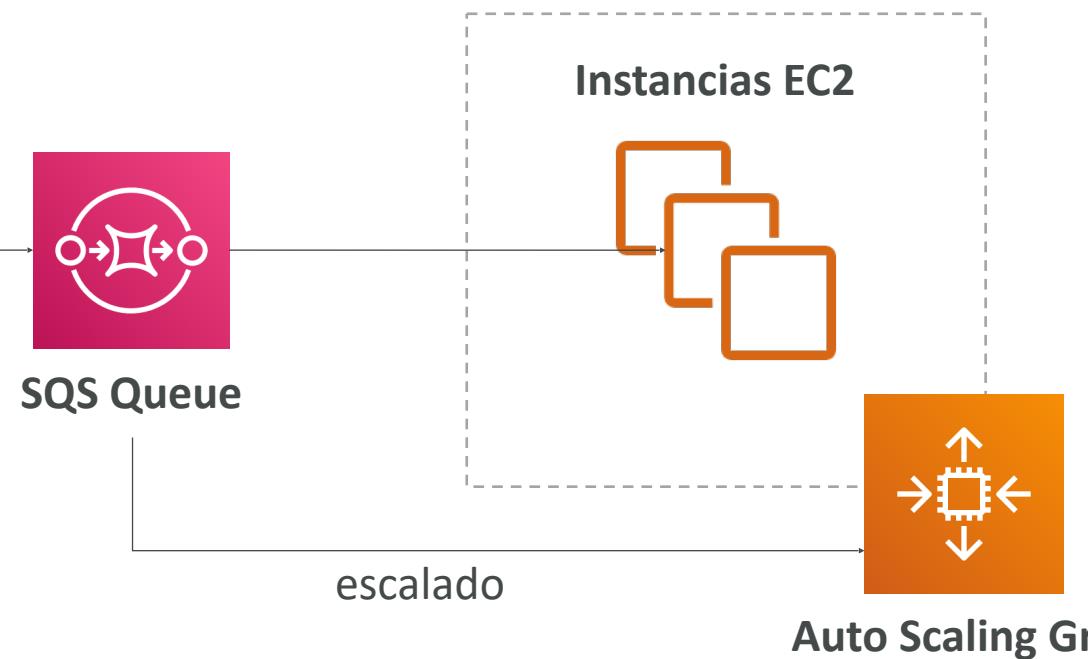
- La oferta más antigua de AWS (más de 10 años)
- Servicio totalmente gestionado (~serverless), utilizado para **desacoplar** aplicaciones
- Escala desde 1 mensaje por segundo hasta 10.000 por segundo
- Retención de mensajes por defecto 4 días, máximo de 14 días
- No hay límite en el número de mensajes que puede haber en la cola
- **Los mensajes se eliminan después de ser leídos por los consumidores**
- Baja latencia (<10 ms en publicación y recepción)
- **Los consumidores comparten el trabajo de leer los mensajes y escalan horizontalmente**

SQS para desvincular los niveles de aplicación

SERVIDORES WEB

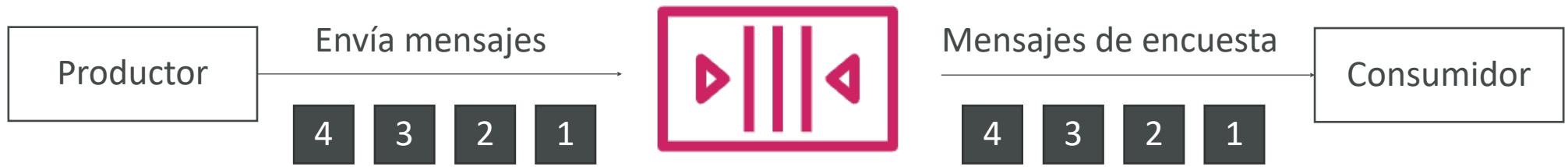


PROCESAMIENTO DE VÍDEO



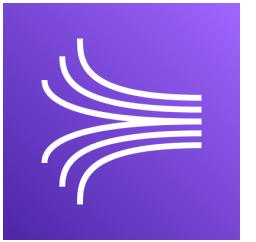
Amazon SQS – Cola FIFO

- FIFO = First In First Out (ordenación de los mensajes en la cola)



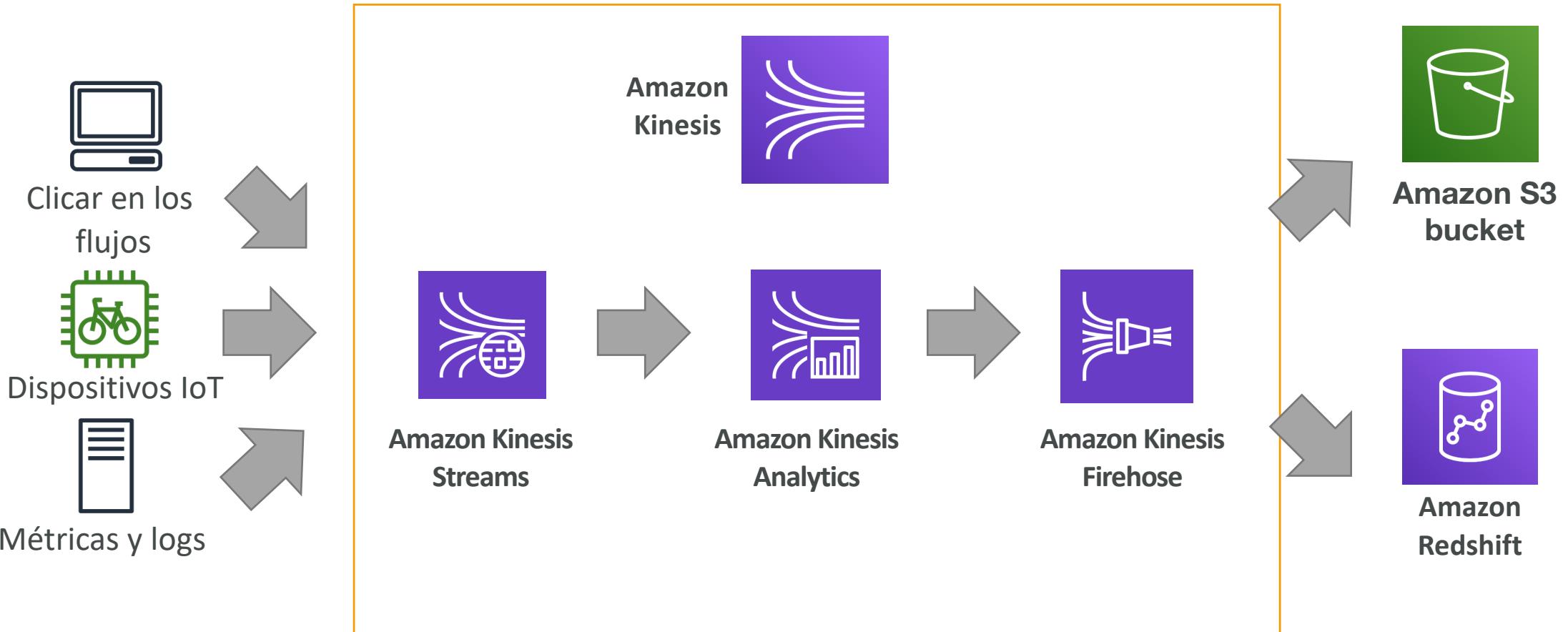
- Los mensajes son procesados en orden por el consumidor

Amazon Kinesis



- Para el examen: **Kinesis = streaming de big data en tiempo real**
- **Servicio gestionado para recopilar, procesar y analizar datos de streaming en tiempo real a cualquier escala**
- Demasiado detallado para el examen Cloud Practitioner, pero es bueno saberlo:
 - **Kinesis Data Streams**: streaming de baja latencia para ingerir datos a escala desde cientos de miles de fuentes
 - **Kinesis Data Firehose**: carga streams en S3, Redshift, ElasticSearch, etc...
 - **Kinesis Data Analytics**: realiza análisis en tiempo real de streams mediante SQL
 - **Kinesis Video Streams**: Monitorización de streams de vídeo en tiempo real para analítica o ML

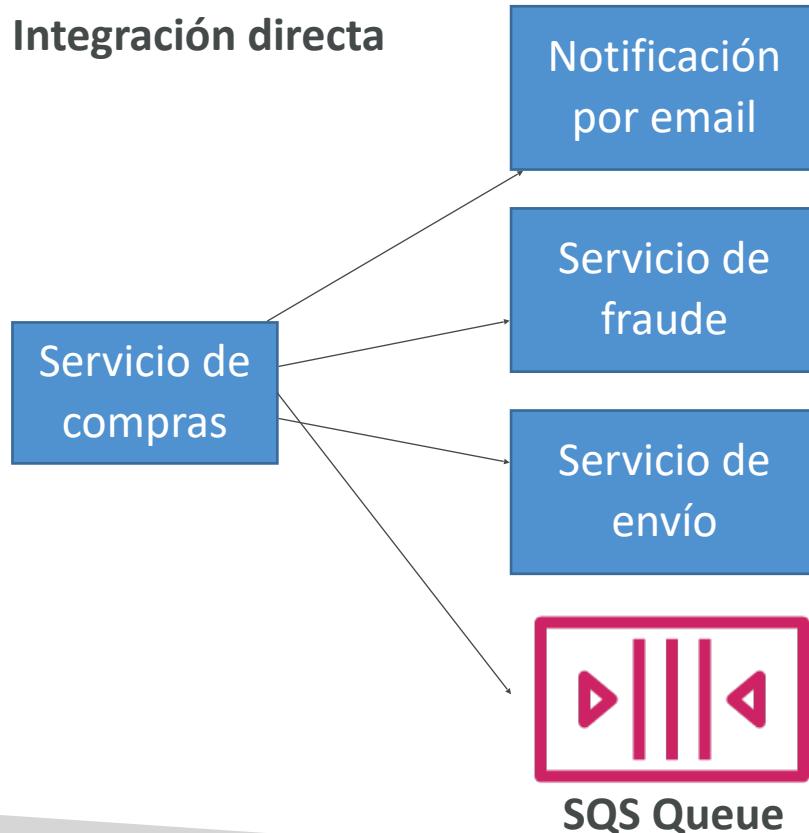
Kinesis (visión general de alto nivel)



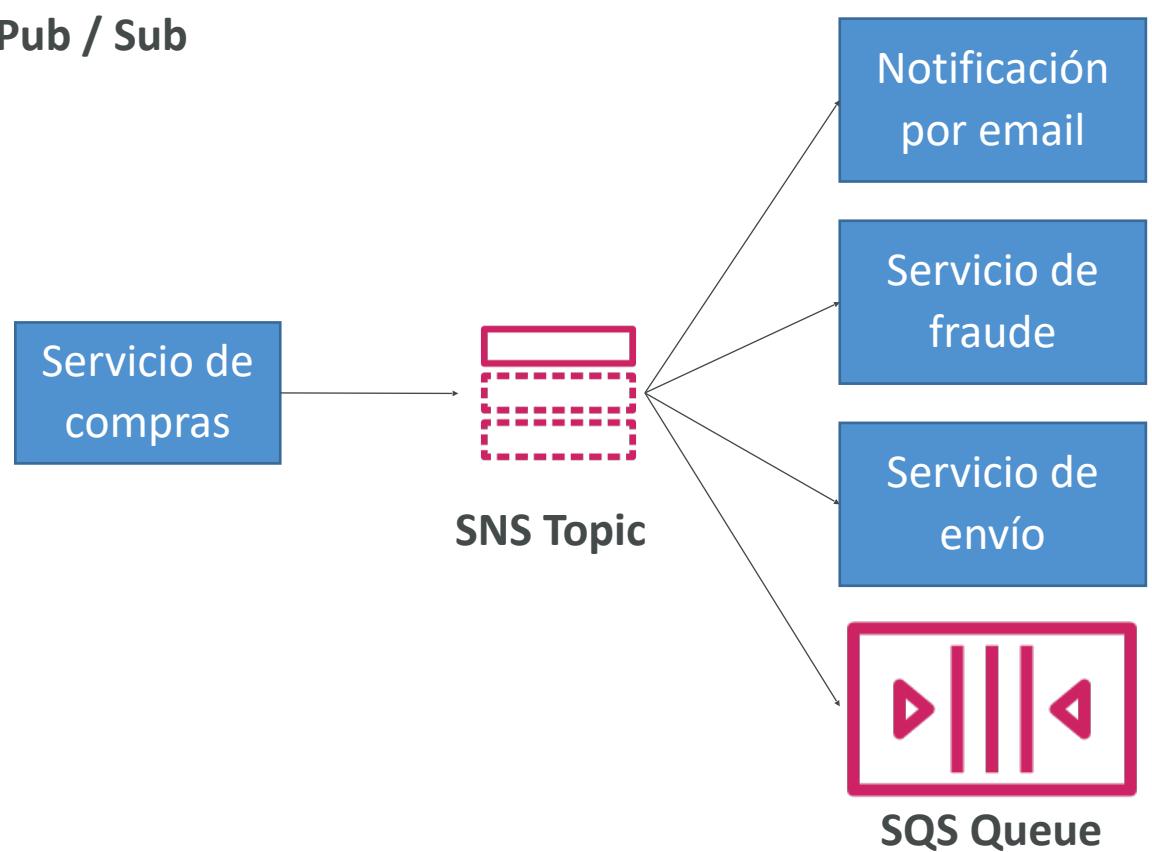
Amazon SNS

- ¿Y si quieres enviar un mensaje a muchos receptores?

Integración directa



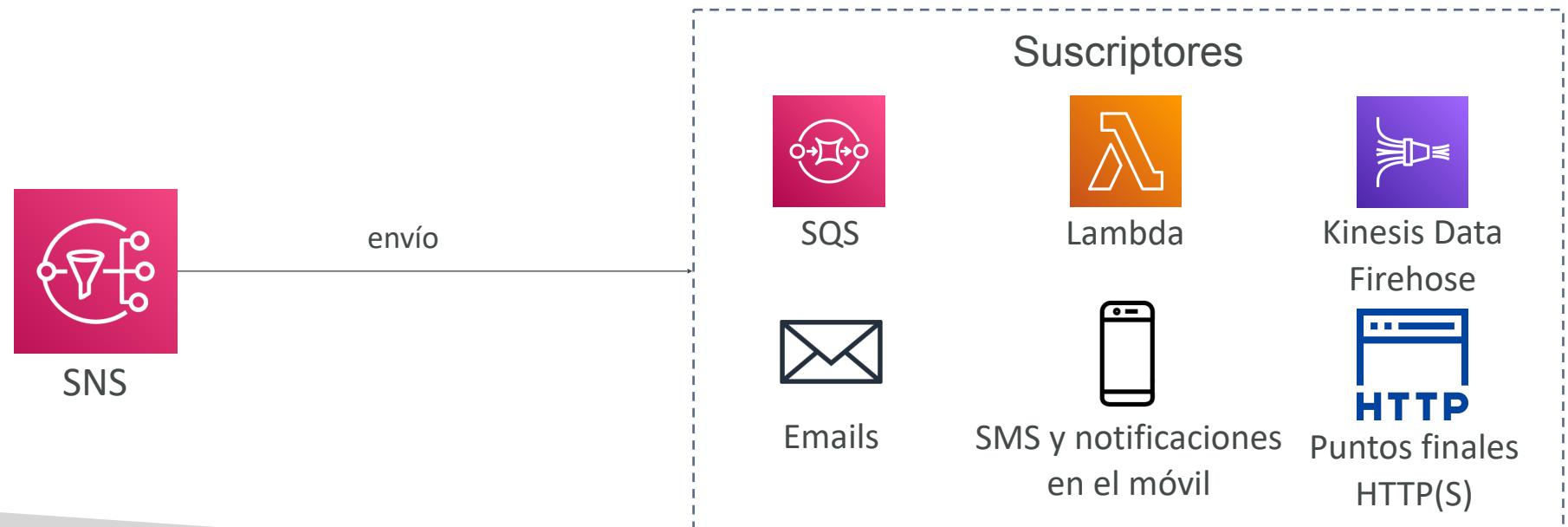
Pub / Sub



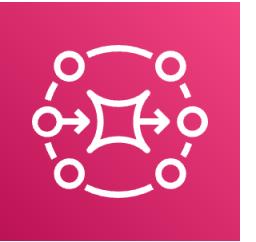
Amazon SNS



- Los "**publicadores**" de eventos sólo envían mensajes a un SNS Topic
- Tantos "**suscriptores**" de eventos como queramos escuchar las notificaciones del SNS Topic
- Cada suscriptor del Topic **recibirá todos los mensajes**
- Hasta 12.500.000 suscriptores por SNS Topic, límite de 100.000 Topics



Amazon MQ



- SQS, SNS son servicios "nativos del Cloud": protocolos propietarios de AWS
- Las aplicaciones tradicionales que se ejecutan desde las instalaciones pueden utilizar protocolos abiertos como: MQTT, AMQP, STOMP, Openwire, WSS
- Al migrar al Cloud, en lugar de rediseñar la aplicación para utilizar SQS y SNS, podemos utilizar Amazon MQ
- **Amazon MQ es un servicio gestionado de intermediación / broker** de mensajes para



- Amazon MQ no "escala" tanto como SQS / SNS
- Amazon MQ se ejecuta en servidores, puede ejecutarse en Multi-AZ con comutación por error
- Amazon MQ tiene tanto la función de cola (~SQS) como la de tema (~SNS)

Resumen - Integración

- **SQS:**
 - Servicio de colas en AWS
 - Múltiples productores, los mensajes se conservan hasta 14 días
 - Múltiples consumidores comparten la lectura y borran los mensajes cuando han terminado
 - Se utiliza para **desacoplar** aplicaciones en AWS
- **SNS:**
 - Servicio de notificaciones en AWS
 - Suscriptores: Correo electrónico, Lambda, SQS, HTTP, Móvil...
 - Múltiples suscriptores, envía todos los mensajes a todos ellos
 - Sin retención de mensajes
- **Kinesis:** streaming de datos en tiempo real, persistencia y análisis
- **Amazon MQ:** broker de mensajes gestionados para ActiveMQ y RabbitMQ en el Cloud (protocolos MQTT, AMQP..)

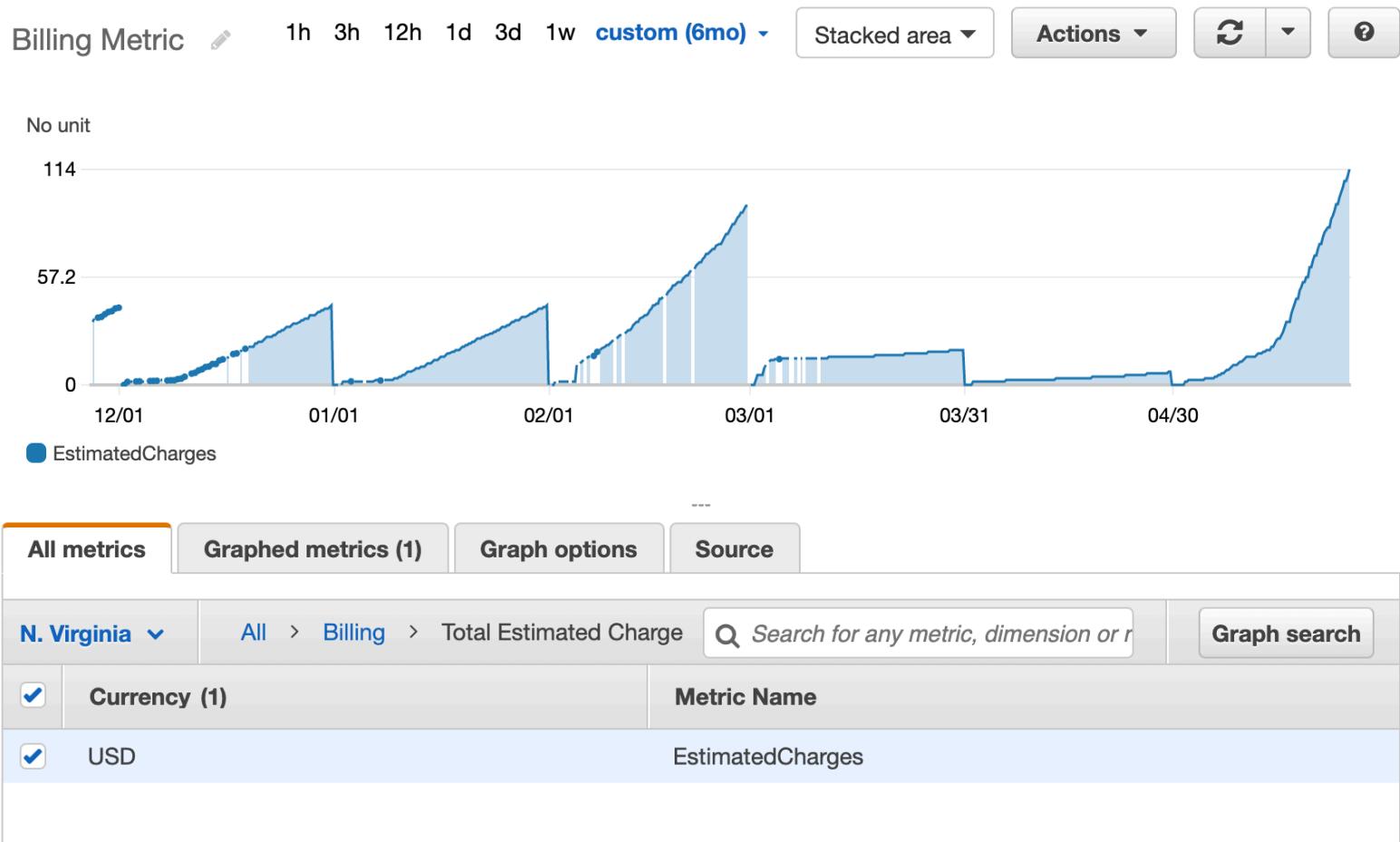
Monitorización del Cloud

Amazon CloudWatch Metrics



- CloudWatch proporciona métricas para todos los servicios de AWS
- La **métrica** es una variable a monitorizar (CPUUtilization, NetworkIn...)
- Las métricas tienen **marcas de tiempo**
- Puedes crear **dashboards de CloudWatch** con las métricas

Ejemplo: Métrica de facturación de CloudWatch (us east-1)



Métricas importantes

- **Instancias EC2:** Utilización de la CPU, Comprobaciones de estado, Red (no RAM)
 - Métricas por defecto cada 5 minutos
 - Opción de monitorización detallada (\$\$\$): métricas cada 1 minuto
- **Volúmenes EBS:** Lecturas/escrituras de disco
- **Buckets S3:** BucketSizeBytes, NumberOfObjects, AllRequests
- **Facturación:** Cargo total estimado (sólo en us-east-1)
- **Límites de servicio:** cuánto has estado utilizando una API de servicio
- **Métricas personalizadas:** introduce tus propias métricas

Amazon CloudWatch Alarms



- Las alarmas se utilizan para activar las notificaciones de cualquier métrica
- Acciones de las alarmas...
 - **Autoescalado**: aumentar o disminuir el número de instancias EC2 "deseadas"
 - **Acciones de EC2**: detener, terminar, reiniciar o **recuperar una instancia de EC2**
 - **Notificaciones SNS**: enviar una notificación a un tema SNS
- Varias opciones (muestreo, %, máximo, mínimo, etc...)
- Puedes elegir el periodo sobre el que evaluar una alarma
- Ejemplo: crear **una alarma de facturación** en la métrica de facturación de CloudWatch
- Estados de la alarma: OK, INSUFFICIENT_DATA, ALARM

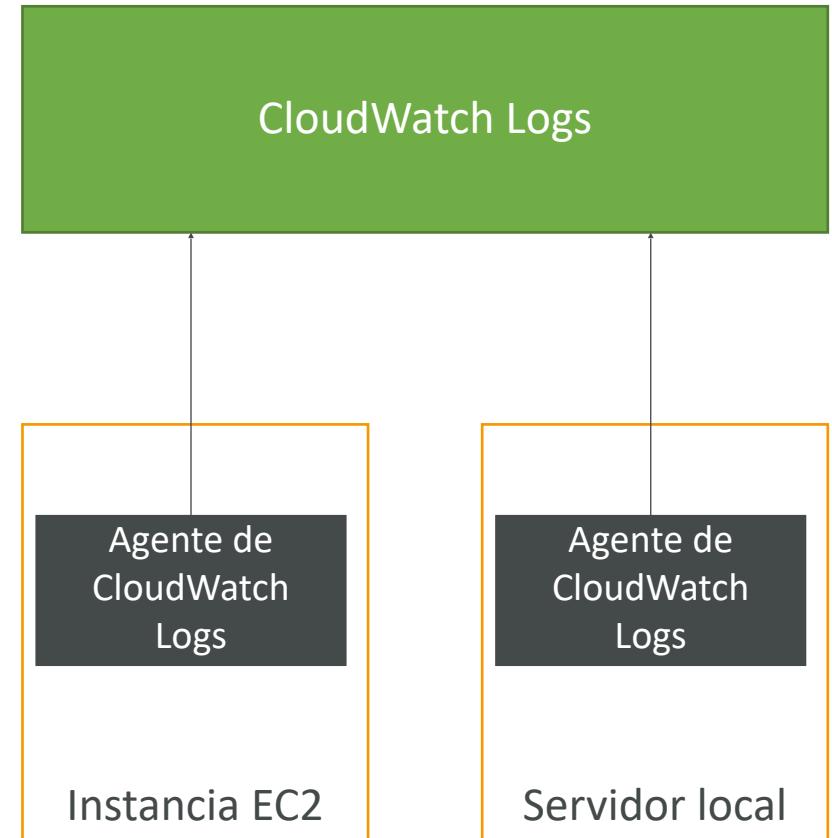


Amazon CloudWatch Logs

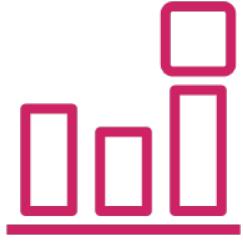
- CloudWatch Logs puede recoger logs de:
 - Elastic Beanstalk: recogida de logs desde la aplicación
 - ECS: recopilación desde los contenedores
 - AWS Lambda: recogida de logs de funciones
 - CloudTrail basado en un filtro
 - **Agentes de logs de CloudWatch: en máquinas EC2 o en servidores locales**
 - Route53: registro de consultas DNS
- Permite la **monitorización de logs en tiempo real**
- Retención de logs de CloudWatch ajustable

CloudWatch Logs para EC2

- Por defecto, ningún logs de tu instancia EC2 irá a CloudWatch
- Tienes que ejecutar un agente de CloudWatch en EC2 para enviar los archivos de logs que quieras
- Asegúrate de que los permisos IAM son correctos
- **El agente de logs de CloudWatch también se puede configurar en las instalaciones**



Amazon EventBridge (previamente CloudWatch Events)



- Programar: Trabajos Cron (scripts programados)

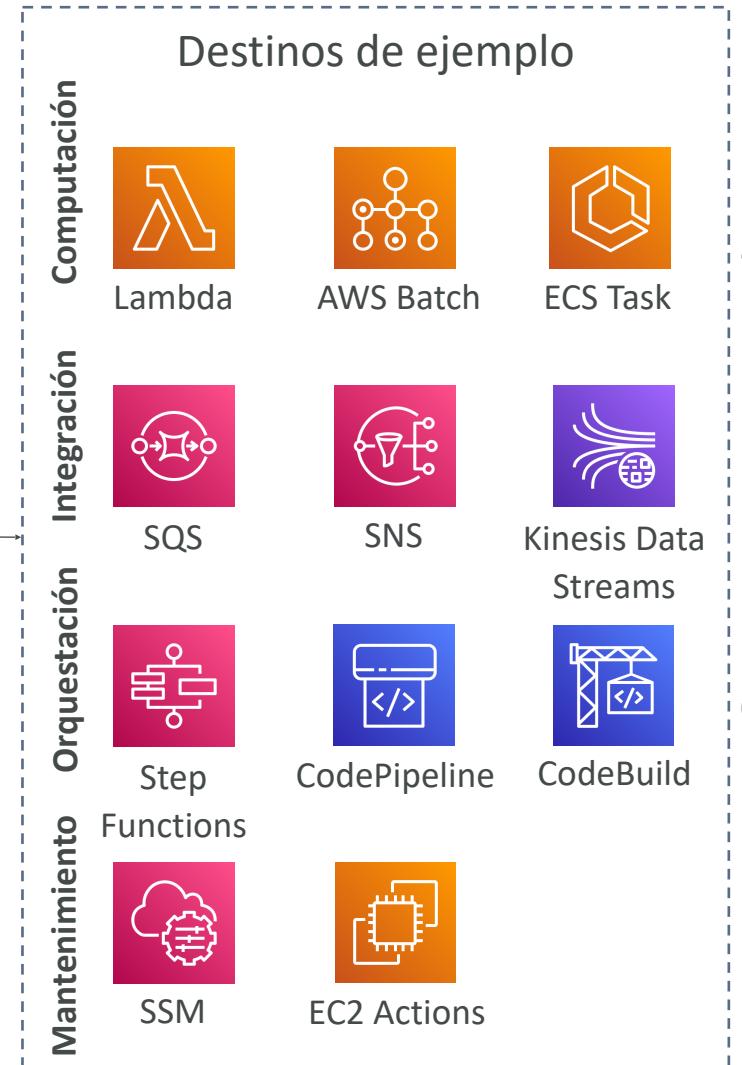
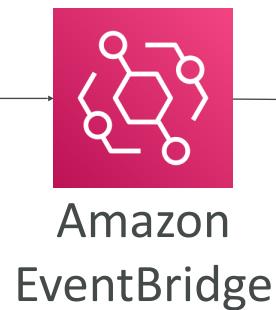


- Patrón de eventos: Reglas de eventos para reaccionar ante un servicio que hace algo

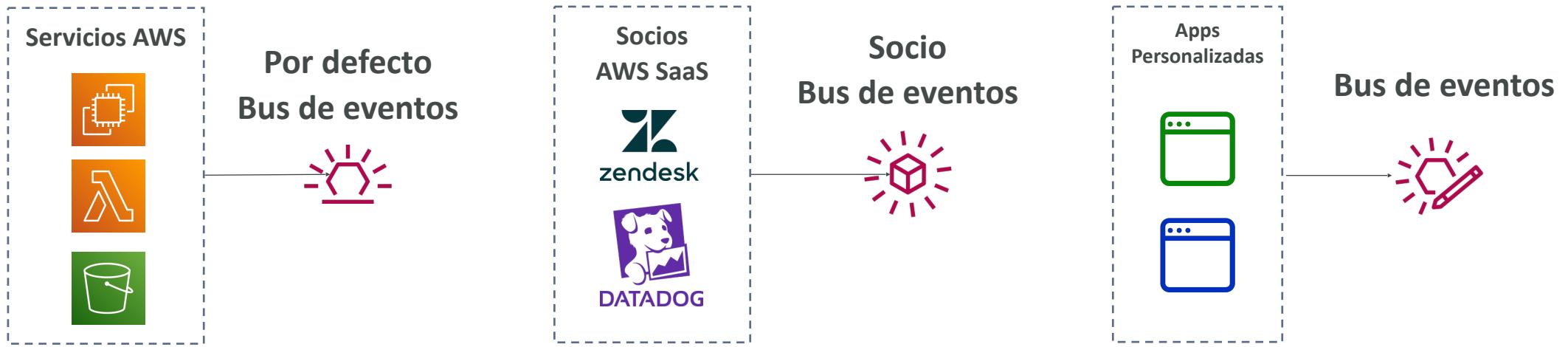


- Activar funciones Lambda, enviar mensajes SQS/SNS...

Reglas de Amazon EventBridge



Amazon EventBridge



- **Registro de esquemas**: esquema de eventos del modelo
- Puedes **archivar los eventos** (todos/filtro) enviados a un bus de eventos (indefinidamente o por un periodo determinado)
- Posibilidad de **reproducir los eventos archivados**

AWS CloudTrail



- Proporciona gobernanza, normativa y auditoría para tu cuenta de AWS
- CloudTrail está activado por defecto
- Obtén **un historial de eventos / llamadas a la API realizadas en tu cuenta de AWS** por:
 - Consola
 - SDK
 - CLI
 - Servicios de AWS
- Puedes poner logs de CloudTrail en CloudWatch Logs o en S3
- **Un rastro puede aplicarse a todas las Regiones (por defecto) o a una sola región.**
- Si se elimina un recurso en AWS, ¡investiga primero CloudTrail!

CloudTrail Diagram



AWS X-Ray



- Depuración en producción, a la vieja usanza:
 - Prueba localmente
 - Añade declaraciones de logs en todas partes
 - Vuelve a desplegar en producción
- Los formatos de logs difieren entre aplicaciones y el análisis de logs es difícil.
- Depuración: un gran monolito "fácil", servicios distribuidos "difícil"
- No hay vistas comunes de toda tu arquitectura
- Entra... ¡AWS X-Ray!

AWS X-Ray

Análisis visual de nuestras aplicaciones



Ventajas de AWS X-Ray

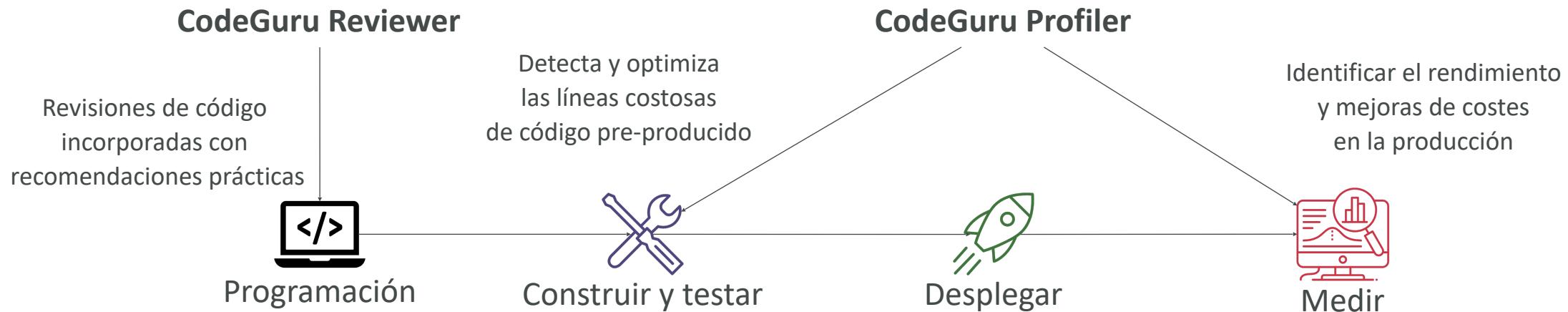


- Resolución de problemas de rendimiento (cuellos de botella)
- Comprender las dependencias en una arquitectura de microservicios
- Identificar los problemas del servicio
- Revisar el comportamiento de las solicitudes
- Encontrar errores y excepciones
- ¿Cumplimos el Acuerdo de nivel de servicio (SLA) de tiempo?
- ¿Dónde estoy limitado?
- Identificar los usuarios que se ven afectados

Amazon CodeGuru



- Un servicio con tecnología ML para **revisiones de código automatizadas y recomendaciones sobre el rendimiento de las aplicaciones**
- Ofrece dos funcionalidades
 - **CodeGuru Reviewer**: revisiones de código automatizadas para el análisis estático del código (desarrollo)
 - **CodeGuru Profiler**: visibilidad/recomendaciones sobre el rendimiento de la aplicación durante el tiempo de ejecución (producción)



Amazon CodeGuru Reviewer

- Identifica problemas críticos, vulnerabilidades de seguridad y fallos difíciles de encontrar
- Ejemplo: mejores prácticas de codificación comunes, fugas de recursos, detección de seguridad, validación de entradas
- Utiliza el Machine Learning y el razonamiento automatizado
- Lecciones aprendidas a través de millones de revisiones de código en miles de repositorios de código abierto y de Amazon
- Soporta Java y Python
- Se integra con GitHub, Bitbucket y AWS CodeCommit

The screenshot shows the Amazon CodeGuru Reviewer interface. At the top, there's a navigation bar with 'CodeGuru' and 'Code reviews'. Below it, the repository name 'RepositoryAnalysis-amazon-codeguru-reviewer-sample-app-master-mw2tsa56o0000000' is displayed. The main section is titled 'Details' and includes information such as:

- Status: Completed
- Recommendations: 4
- Metered lines of code: 80
- Time created: 10 Nov 2020 08:08:47 AM GMT-0800
- Last updated: 10 Nov 2020 08:11:44 AM GMT-0800
- Type: RepositoryAnalysis
- Provider: GitHub
- Repository: amazon-codeguru-reviewer-sample-app
- Branch name: master

Below the details, there's a section for 'Recommendations (4)'. The first recommendation is for 'EventHandler.java Line: 79' with a note: 'This code appears to be waiting for a resource before it runs. You could use the waiters feature to help improve efficiency. Consider using ObjectExists or ObjectNotExists. For more information, see <https://aws.amazon.com/blogs/developer/waiters-in-the-aws-sdk-for-java/>'. There are 'Was this helpful?' upvote and downvote buttons.

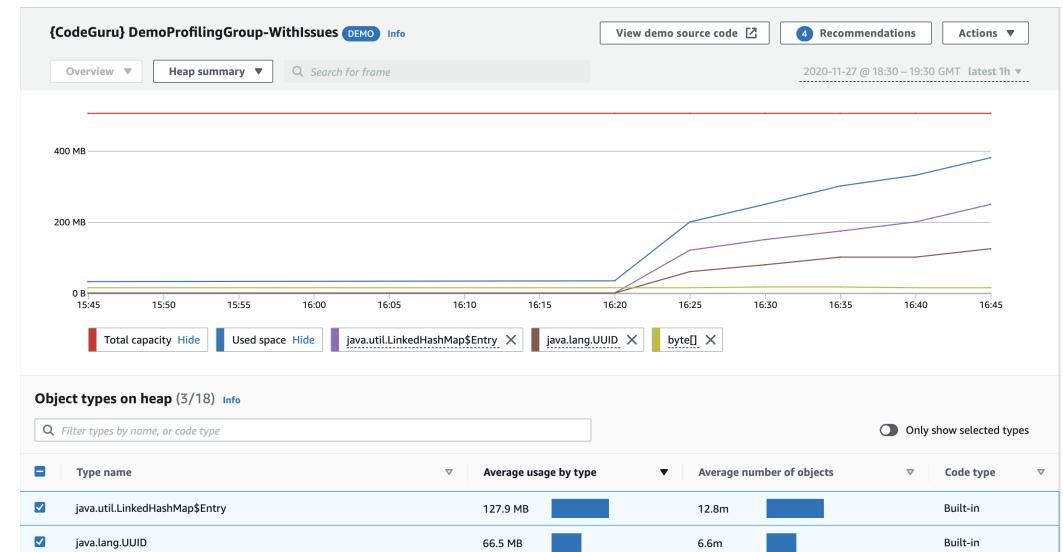
The second recommendation is for 'EventHandler.java Line: 100' with a note: 'This code might not produce accurate results if the operation returns paginated results instead of all results. Consider adding another call to check for additional results.' There are also 'Was this helpful?' upvote and downvote buttons.

The third recommendation is for 'EventHandler.java Line: 100' with a note: 'This code uses an outdated API. ListObjectsV2 is the revised List Objects API, and we recommend you use this revised API for new application developments.' There are 'Was this helpful?' upvote and downvote buttons.

<https://aws.amazon.com/codeguru/features/>

Amazon CodeGuru Profiler

- Ayuda a comprender el comportamiento en tiempo de ejecución de tu aplicación
- Ejemplo: identificar si tu aplicación está consumiendo una capacidad de CPU excesiva en una rutina de logs
- Funciones:
 - Identificar y eliminar las ineficiencias del código
 - Mejorar el rendimiento de la aplicación (por ejemplo, reducir la utilización de la CPU)
 - Disminuye los costes de computación
 - Proporciona un resumen de la pila (identifica los objetos que consumen memoria)
 - Detección de anomalías
- Soporta aplicaciones que se ejecutan en AWS o en las instalaciones
- Mínima sobrecarga en la aplicación



<https://aws.amazon.com/codeguru/features/>

AWS Health Dashboard - Historial de servicios



- Muestra todas las regiones, todos los servicios y su salud
- Muestra información histórica de cada día
- Tiene un canal RSS al que puedes suscribirte
- Antes se llamaba AWS Service Health Dashboard

Service history

The following table is a running log of AWS service interruptions for the past 12 months. Choose a status icon to see status updates for that service. All dates and times are reported in UTC. To update your time zone, see [Time zone settings](#).

Service	RSS	Today	9 Jan	8 Jan	7 Jan	6 Jan
Alexa for Business (N. Virginia)	RSS	OK	OK	OK	OK	OK
Amazon EventBridge Scheduler (N. Virginia)	RSS	OK	OK	OK	OK	OK
Amazon EventBridge Scheduler (Ohio)	RSS	OK	OK	OK	OK	OK
Amazon EventBridge Scheduler (Oregon)	RSS	OK	OK	OK	OK	OK
Amazon API Gateway (Montreal)	RSS	OK	OK	OK	OK	OK
Amazon API Gateway (N. California)	RSS	OK	OK	OK	OK	OK
Amazon API Gateway (N. Virginia)	RSS	OK	OK	OK	OK	OK
Amazon API Gateway (Ohio)	RSS	OK	OK	OK	OK	OK



AWS Health Dashboard – Estado de su cuenta

- Anteriormente llamado AWS Personal Health Dashboard (PHD)
- El AWS Account Health Dashboard proporciona **alertas y orientación** para solucionar problemas cuando AWS experimenta **eventos que pueden afectarte**.
- Mientras que el Service Health Dashboard muestra el estado general de los servicios de AWS, el Account Health Dashboard te ofrece una **visión personalizada del rendimiento y la disponibilidad de los servicios de AWS subyacentes a tus recursos de AWS**.
- El dashboard muestra **información relevante y oportuna** para ayudarte a gestionar los eventos en curso y proporciona **notificaciones proactivas** para ayudarte a planificar las **actividades programadas**.
- **Puede agregar datos de toda una AWS Organizations**



AWS Health Dashboard – Estado de su cuenta

- Servicio global
- Muestra cómo las caídas de AWS te afectan directamente a ti y a tus recursos de AWS
- Alertas, remedios, actividades proactivas y programadas

Open issues	0
Scheduled changes	0
Other notifications	0
Event log	

Open and recent issues (0)		Scheduled changes (0)		Other notifications (0)		Event log							
Event log													
<input type="text"/> Add filter													
Event	Status	Event category	Region / Zone	Start time	Last update time	Affected resources							
Operational issue - EC2 (Ohio)	Closed	Issue	us-east-2	December 24, 2022 at 2:25:00 AM UTC	December 24, 2022 at 2:38:53 AM UTC	-							
Operational issue - Codecatalyst (Oregon)	Closed	Issue	us-west-2	December 21, 2022 at 3:03:57 PM UTC	December 21, 2022 at 4:50:47 PM UTC	-							
Operational issue - Amplify (N. Virginia)	Closed	Issue	us-east-1	December 17, 2022 at 2:24:17 PM UTC	December 17, 2022 at 2:43:21 PM UTC	-							
Operational issue - Multiple services (Singapore)	Closed	Issue	ap-southeast-1	December 13, 2022 at 10:00:55 PM UTC	December 14, 2022 at 1:01:16 AM UTC	-							

Resumen - Monitorización

- **CloudWatch:**
 - **Métricas:** monitorización del rendimiento de los servicios AWS y métricas de facturación
 - **Alarms:** automatiza la notificación, realiza acciones EC2, notifica a SNS en función de la métrica
 - **Logs:** recopila logs de instancias EC2, servidores, funciones Lambda...
 - **Eventos (o EventBridge):** reacciona a eventos en AWS, o activa una regla según un programa
- **CloudTrail:** audita las llamadas a la API realizadas en tu cuenta de AWS
- **CloudTrail Insights:** análisis automatizado de tus Eventos CloudTrail
- **X-Ray:** rastrea las peticiones realizadas a través de tus aplicaciones distribuidas
- **AWS Health Dashboard:** estado de todos los servicios de AWS en todas las regiones
- **AWS Health Dashboard – Estado de su cuenta:** Eventos de AWS que afectan a tu infraestructura
- **Amazon CodeGuru:** revisiones de código automatizadas y recomendaciones sobre el rendimiento de las aplicaciones

Virtual Private Cloud (VPC)

VPC - Definición rápida

- La VPC es algo que debes conocer en profundidad para el AWS Certified Solutions Architect Associate y el AWS Certified SysOps Administrator
- **En el nivel AWS Certified Cloud Practitioner, debes conocer:**
 - VPC, subredes, puertas de enlace de Internet y puertas de enlace NAT
 - Grupos de seguridad, ACL de red (NACL), logs de flujo de la VPC
 - VPC Peering, VPC Endpoints
 - Site to Site VPN y Direct Connect
 - Transit Gateway
- Sólo te daré una visión general, menos de 1 ó 2 preguntas en tu examen.
- Vamos a echar un vistazo a la "VPC por defecto" (creada por defecto por AWS para ti)
- Hay una clase resumen al final. No pasa nada si no lo entiendes todo

Direcciones IP en AWS

- IPv4 - Protocolo de Internet versión 4 (4.300 millones de direcciones)
 - **IPv4 pública** - puede utilizarse en Internet
 - La instancia EC2 obtiene una nueva dirección IP pública cada vez que se detiene y se inicia (por defecto)
 - **IPv4 privada** - se puede utilizar en redes privadas (LAN) como la red interna de AWS (por ejemplo, 192.168.1.1)
 - La IPv4 privada es fija para las Instancias EC2 aunque las inicies/detengas
 - **IP elástica** - te permite adjuntar una dirección IPv4 pública fija a la instancia EC2
- • **Nota: tiene un coste continuo si no se adjunta a la instancia EC2 o si se detiene la instancia EC2**
- **IPv6 - Protocolo de Internet versión 6** (3.4×10^{38} direcciones)
 - Cada dirección IP es pública (no hay rango privado)
 - Ejemplo: 2001:db8:3333:4444:cccc:dddd:eeee:ffff

Manual de VPC y subredes

- **VPC - Virtual Private Cloud:** red privada para desplegar tus recursos (recurso regional)
- Las **subredes** te permiten particionar tu red dentro de tu VPC (recurso de zona de disponibilidad)
- Una **subred pública** es una subred accesible desde Internet
- Una **subred privada** es una subred a la que no se puede acceder desde Internet
- Para definir el acceso a internet y entre subredes, utilizamos las **tablas de rutas (tablas de enrutamiento)**.

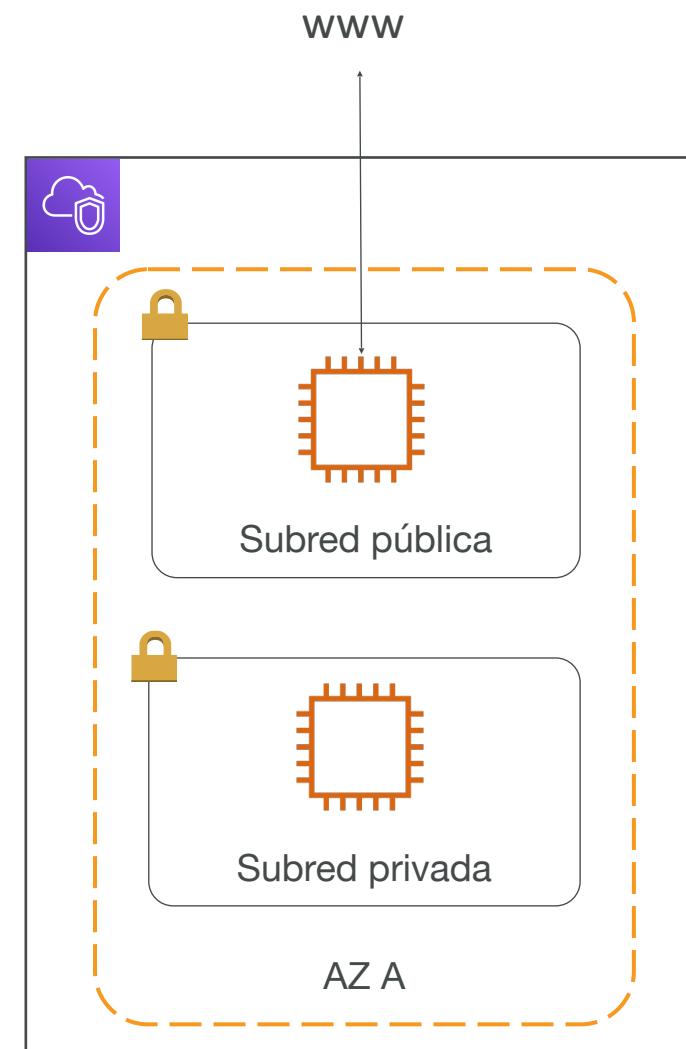
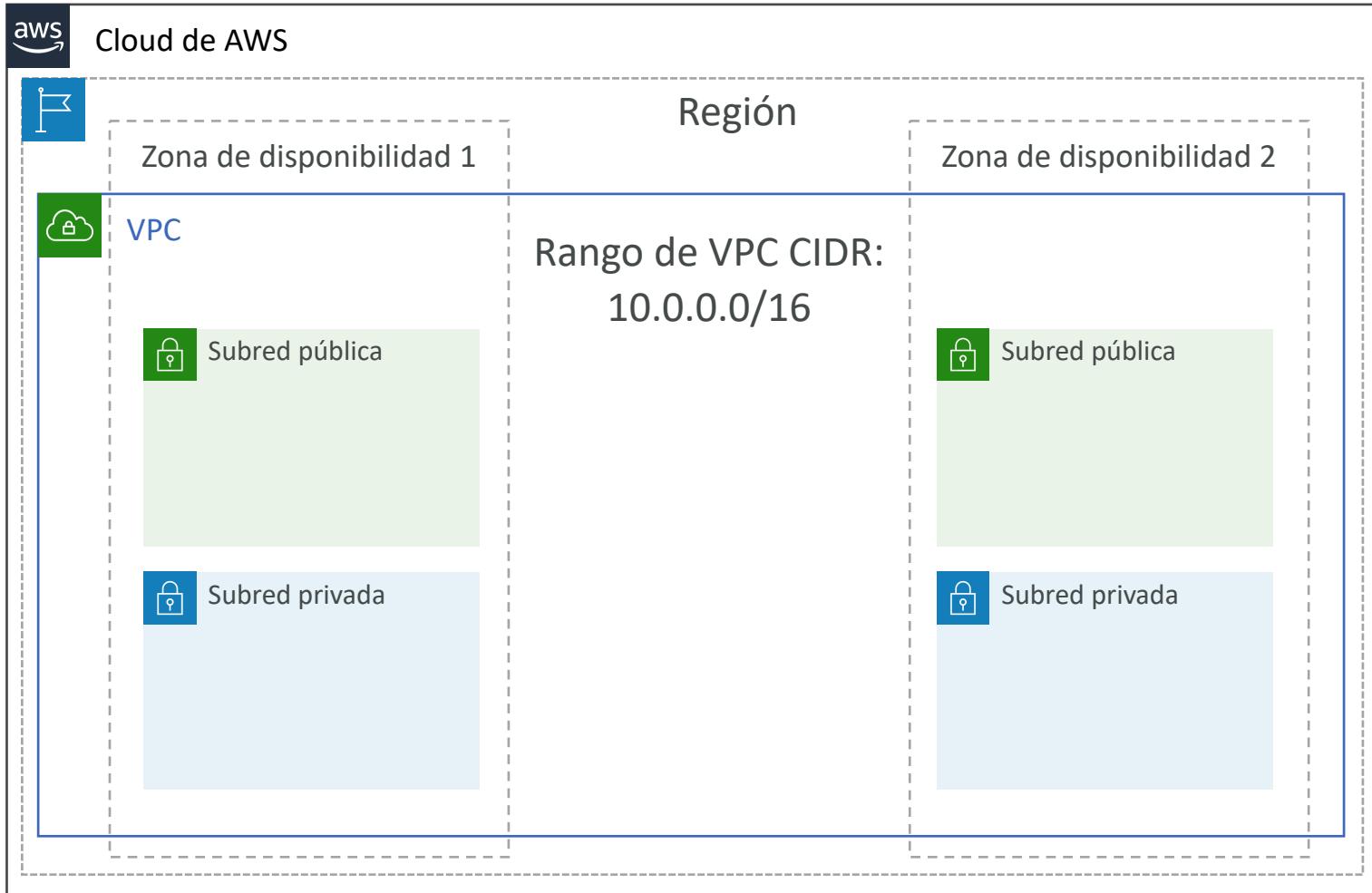
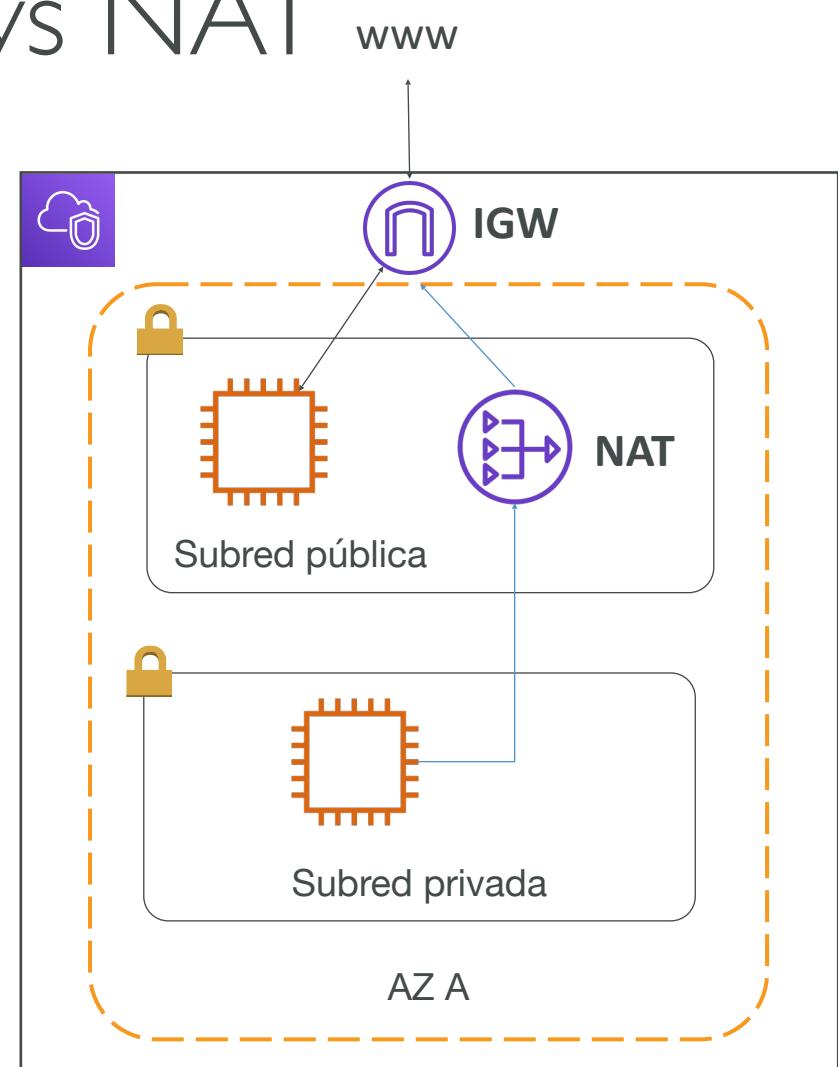


Diagrama de VPC



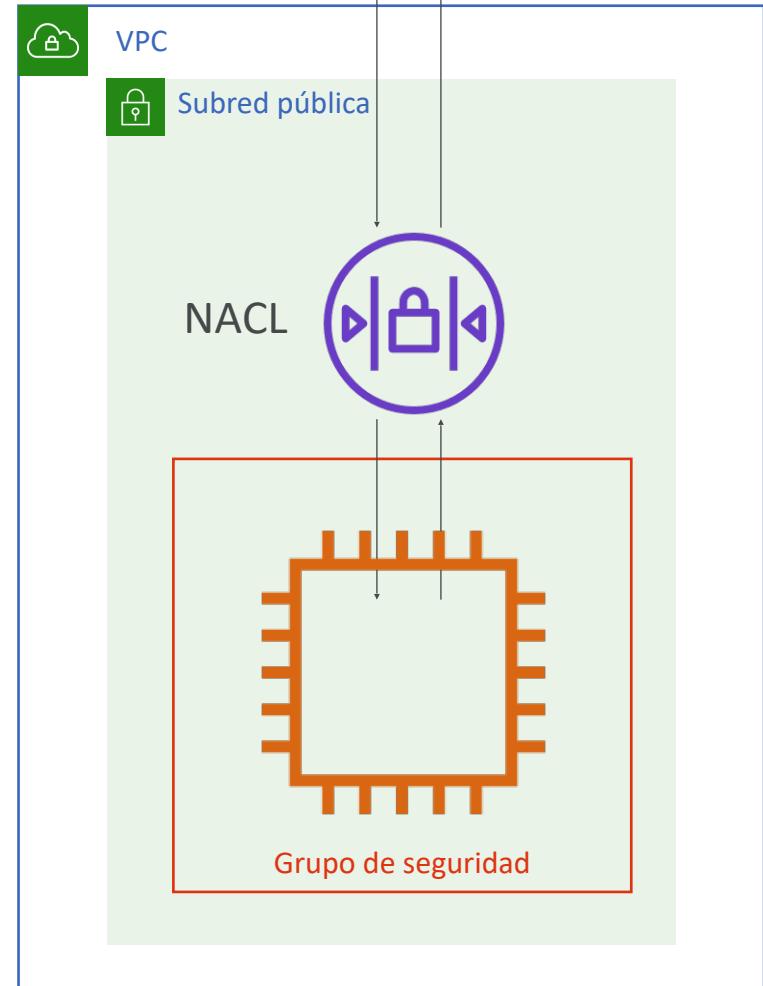
Gateway de Internet y Gateways NAT

- Los **Gateways de Internet** ayudan a nuestras instancias de la VPC a conectarse con Internet
- Las subredes públicas tienen una ruta hacia el gateway de Internet.
- Los **Gateways NAT** (gestionados por AWS) y las **Instancias NAT** (autogestionadas) permiten que tus instancias en tus **subredes privadas** accedan a internet sin dejar de ser privadas



ACL de red (NACL) y grupos de seguridad

- **NACL** (ACL de red)
 - Un firewall que controla el tráfico desde y hacia la subred
 - Puede tener reglas ALLOW y DENY
 - Se adjuntan a nivel de **subred**
 - Las reglas sólo incluyen direcciones IP
- **Grupos de seguridad**
 - Un firewall que controla el tráfico hacia y desde **una ENI / Instancia EC2**
 - Puede tener sólo reglas ALLOW
 - Las reglas incluyen direcciones IP y otros grupos de seguridad



Grupo de seguridad vs ACL de red (NACL)

Security group (Grupo de seguridad)	ACL de red
Opera en el nivel de la instancia	Opera en el nivel de la subred
Solo admite reglas de permiso	Admite reglas de permiso y de denegación
Es con estado: el tráfico de retorno se admite automáticamente, independientemente de las reglas	Es sin estado: las reglas deben permitir de forma explícita el tráfico de retorno
Evaluamos todas las normas antes de decidir si permitir el tráfico	Procesamos las reglas en orden, empezando por la regla numerada más baja, al decidir si permitir el tráfico
Se aplica a una instancia únicamente si alguien especifica el grupo de seguridad al lanzar la instancia, o asocia el grupo de seguridad a la instancia más adelante	Se aplica automáticamente a todas las instancias de las subredes con las que se ha asociado (por lo tanto, proporciona una capa de defensa adicional si las reglas del grupo de seguridad son demasiado permisivas)

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Security.html#VPC_Security_Comparison

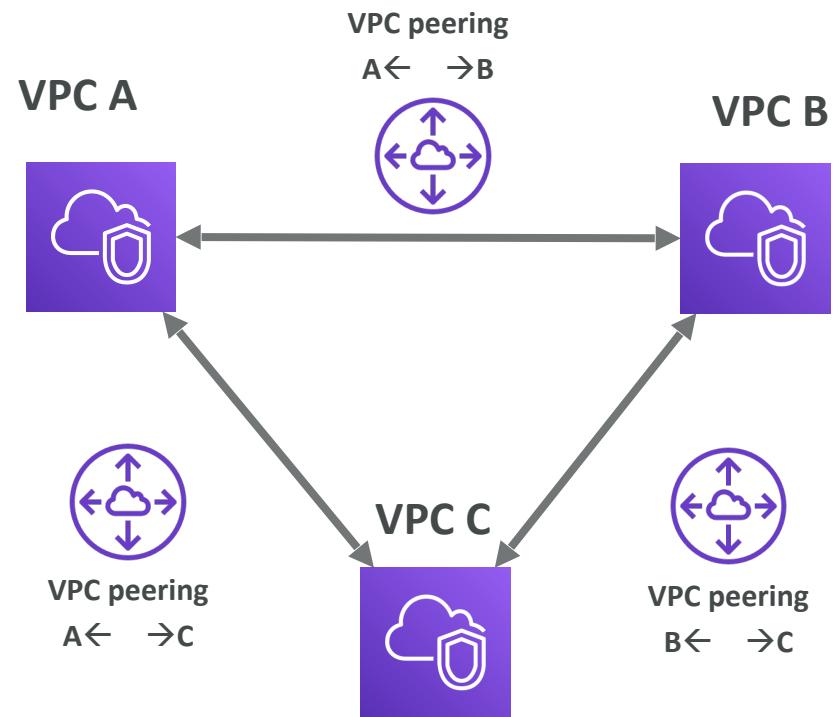


Logs de flujo de la VPC

- Captura información sobre el tráfico IP que entra en tus interfaces:
 - Logs de flujo de **VPC**
 - Logs de flujo de la **subred**
 - Logs de flujo de la **Interfaz de Red Elástica (ENI)**
- Ayuda a supervisar y solucionar problemas de conectividad. Ejemplo:
 - Subredes a Internet
 - Subredes a subredes
 - Internet a subredes
- Captura también la información de red de las interfaces gestionadas por AWS: Elastic Load Balancers, ElastiCache, RDS, Aurora, etc.
- Los datos de logs de flujo de VPC pueden ir a S3, CloudWatch Logs y Kinesis Data Firehose

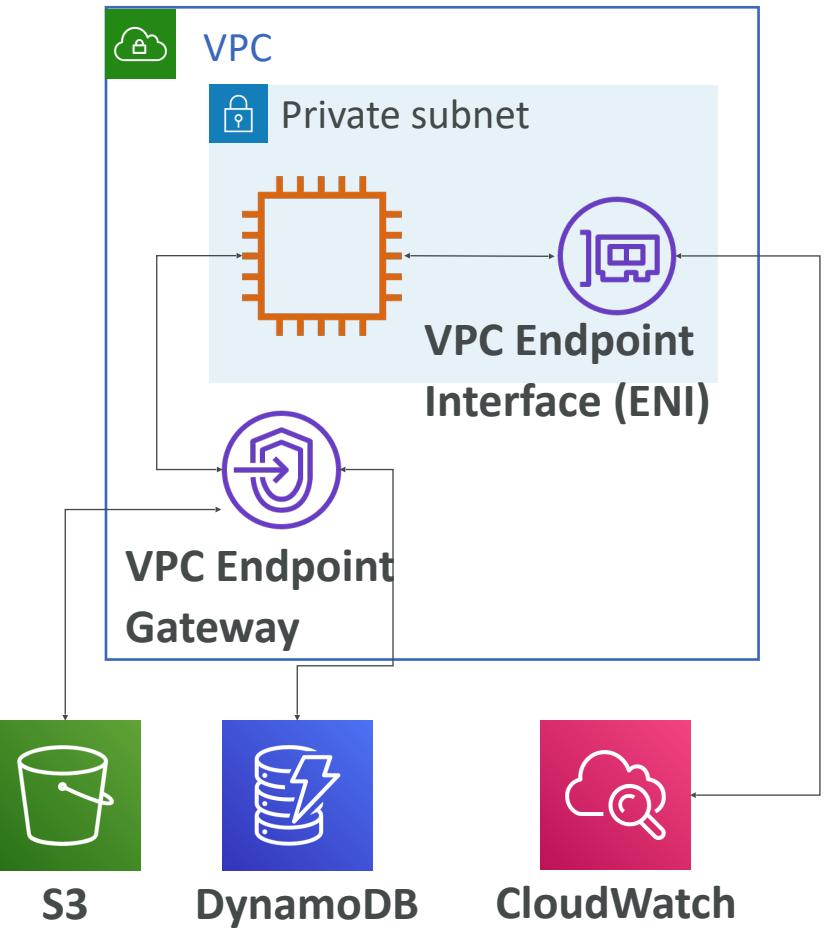
VPC Peering

- Conectar dos VPC, de forma privada, utilizando la red de AWS
- Haz que se comporten como si estuvieran en la misma red
- No deben tener un CIDR (rango de direcciones IP) superpuesto
- La conexión VPC Peering **no es transitiva** (debe establecerse para cada VPC que necesite comunicarse entre sí)



VPC Endpoints

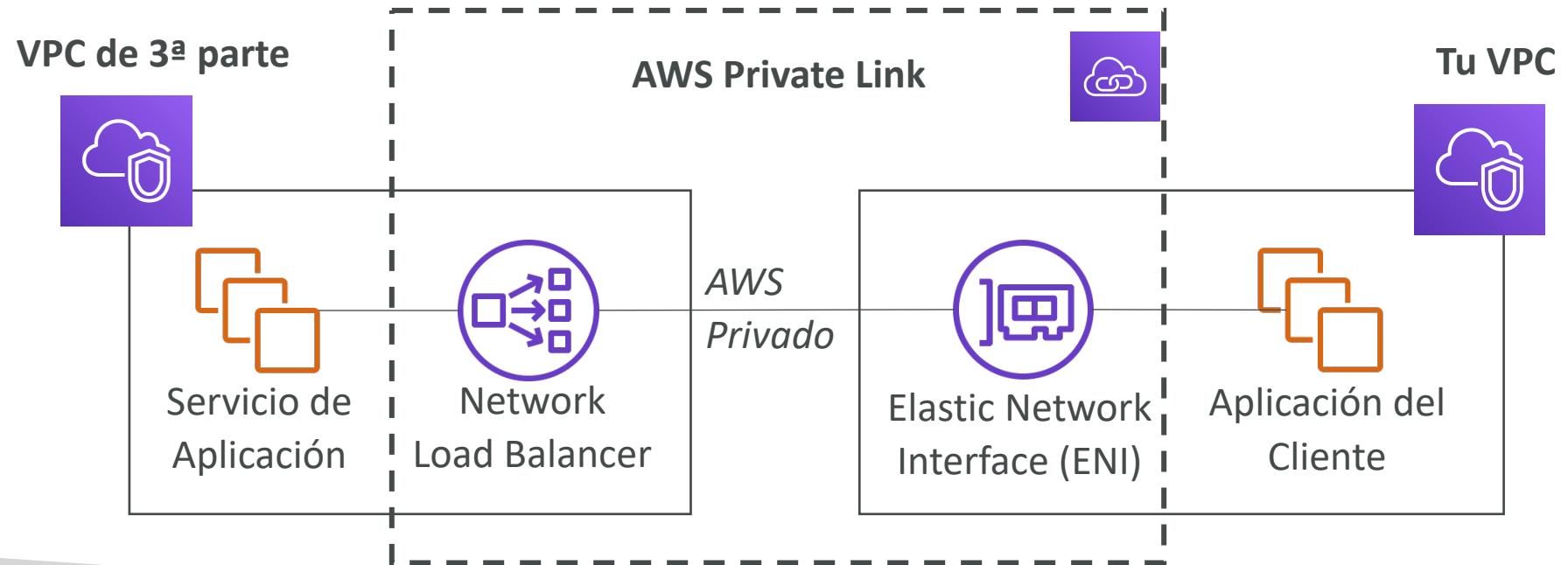
- Los endpoints te permiten conectarte a los servicios de AWS **utilizando una red privada** en lugar de la red www pública
- Esto te proporciona mayor seguridad y menor latencia para acceder a los servicios de AWS
- VPC Endpoint **Gateway**: S3 y DynamoDB
- VPC Endpoint **Interface**: el resto



AWS PrivateLink (Servicios VPC Endpoint)



- La forma más segura y escalable de exponer un servicio a miles de VPCs
- No requiere peering de VPC, gateway de Internet, NAT, tablas de rutas...
- Requiere un Network Load Balancer (VPC de servicio) y un ENI (VPC de cliente)



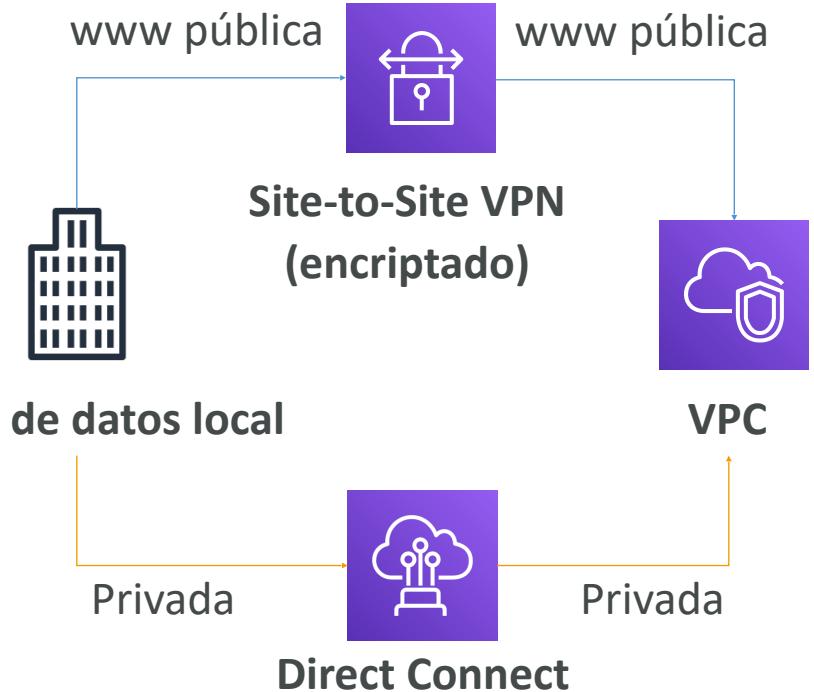
Site to Site VPN y Direct Connect

- **Site to Site VPN**

- Conecta una VPN local a AWS
- La conexión se encripta automáticamente
- Pasa por el Internet público

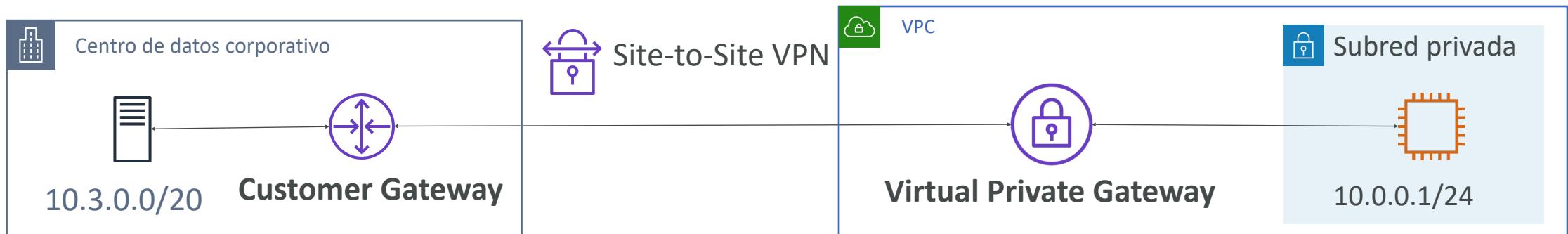
- **Direct Connect (DX)**

- Establece una conexión física entre las instalaciones y AWS
- La conexión es privada, segura y rápida
- Pasa por una red privada
- Tarda al menos un mes en establecerse



Site to Site VPN

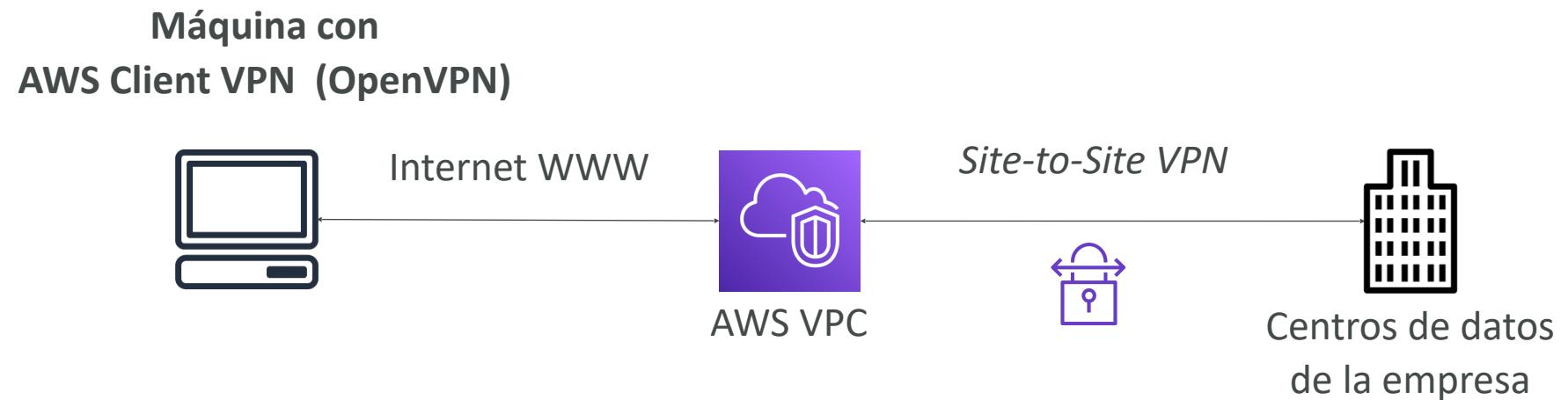
- En las instalaciones: debes utilizar un **Customer Gateway (CGW)**
- AWS: debe utilizar un **Virtual Private Gateway (VGW)**



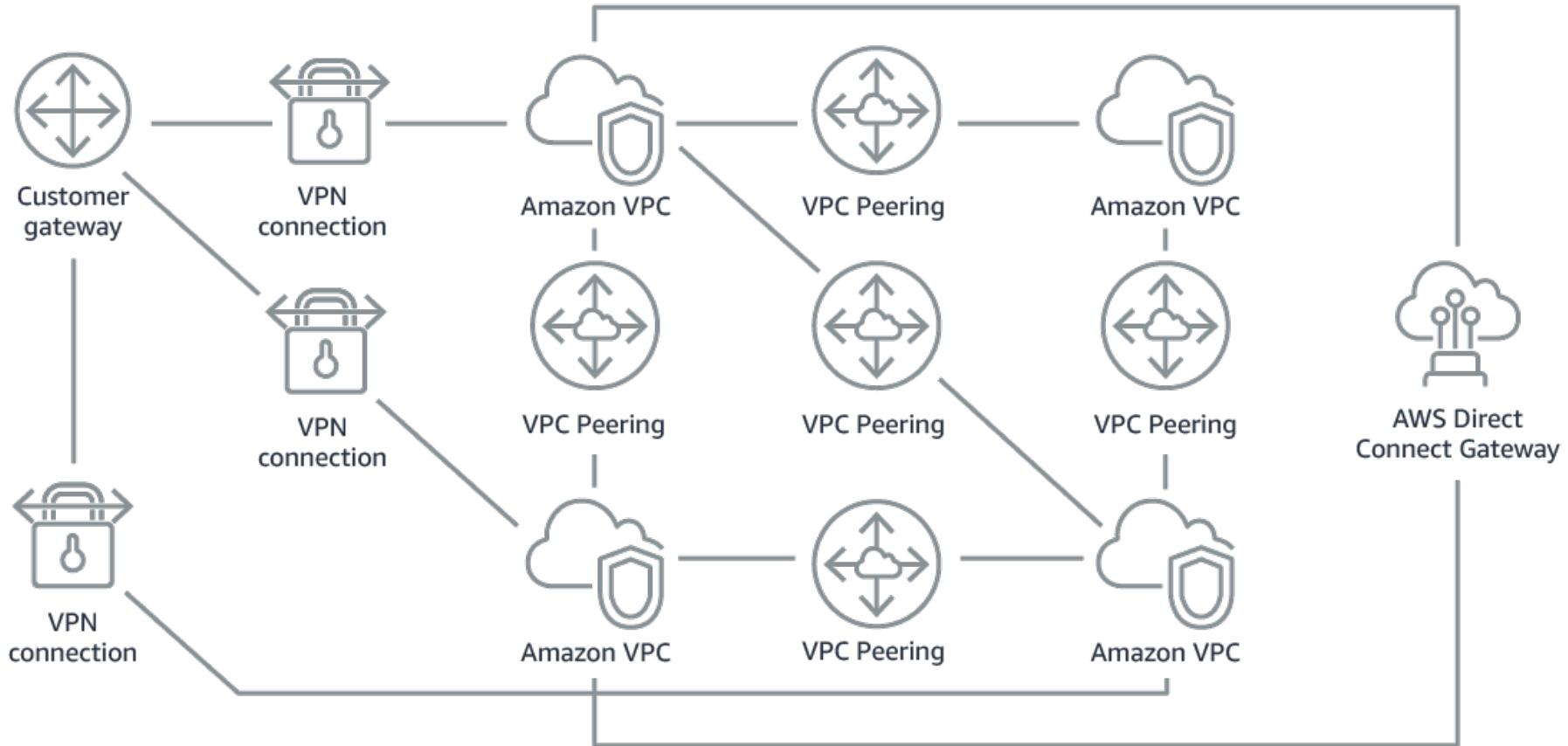
Cliente VPN



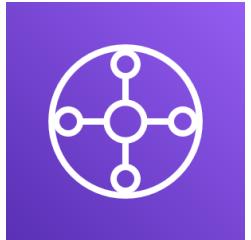
- Conectar desde tu ordenador mediante OpenVPN a tu red privada en AWS y en las instalaciones
- Te permite conectarte a tus instancias EC2 a través de una IP privada (como si estuvieras en la red VPC privada)
- Pasa por el **Internet público**



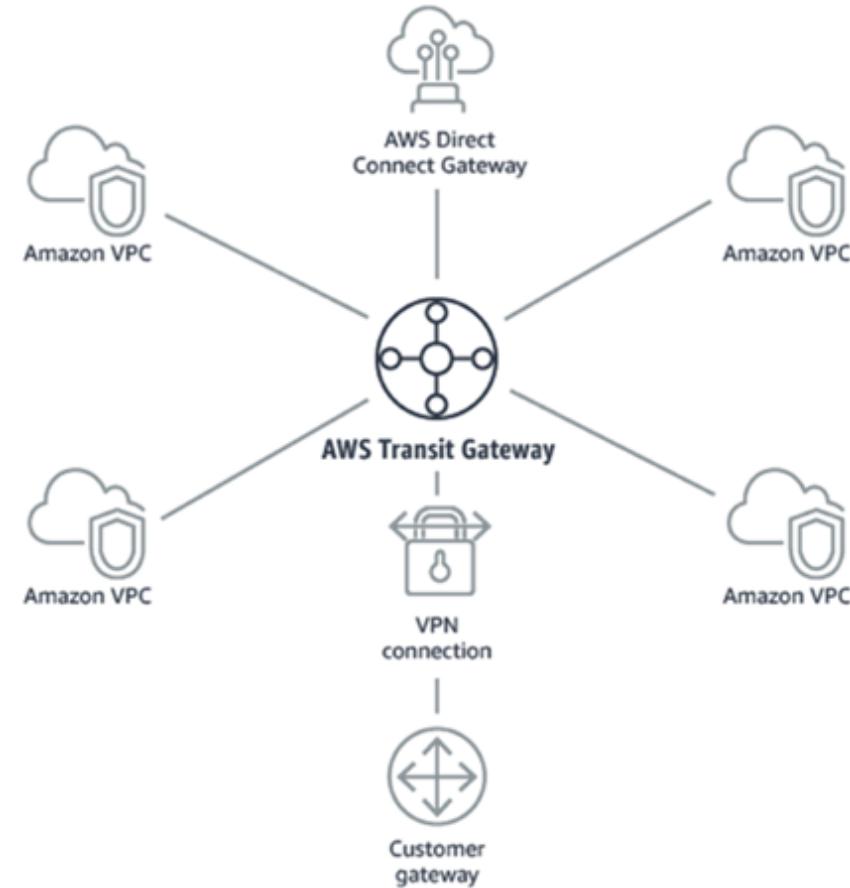
Las topologías de red pueden complicarse



Transit Gateway



- Para tener peering transitivo entre miles de VPC y locales, conexión hub-and-spoke (estrella)
- Un único Gateway para proporcionar esta funcionalidad
- Funciona con el Gateway de Direct Connect y las conexiones VPN



Resumen - Virtual Private Cloud (VPC)

- **VPC** - Virtual Private Cloud (nube privada virtual)
- **Subredes** - Vinculadas a una AZ, partición de red de la VPC
- **Gateway de Internet** - A nivel de la VPC, proporcionan acceso a Internet
- **Los Gateways NAT / Instancias** - Dan acceso a Internet a las subredes privadas
- **NACL** - Sin estado, reglas de subred para entrada y salida
- **Grupos de seguridad** - Con estado, operan a nivel de instancia EC2 o ENI
- **VPC Peering** - Conecta dos VPC con rangos de IP no solapados, no transitivos
- **IP elástica** - IPv4 pública fija, coste continuo si no se utiliza

Resumen - Virtual Private Cloud (VPC)

- **VPC Endpoints** - Proporcionan acceso privado a los servicios de AWS dentro de la VPC
- **PrivateLink** - Conecta de forma privada a un servicio en una VPC de terceros
- **Logs de flujo de la VPC** - Registros de tráfico de red
- **Site to Site VPN** - VPN a través de la Internet pública entre el DC local y AWS
- **VPN de cliente** - Conexión OpenVPN desde tu ordenador a tu VPC
- **Direct Connect** - Conexión privada directa a AWS
- **Transit Gateway** - Conecta miles de redes VPC y locales entre sí

Seguridad y normativa

Modelo de responsabilidad compartida de AWS

- Responsabilidad de AWS - Seguridad **del** Cloud
 - Proteger la infraestructura (hardware, software, instalaciones y redes) que ejecuta todos los servicios de AWS
 - Servicios gestionados como S3, DynamoDB, RDS, etc.
- Responsabilidad del cliente - Seguridad **dentro del** Cloud
 - En el caso de la instancia EC2, el cliente es responsable de la gestión del sistema operativo invitado (incluidos los parches y actualizaciones de seguridad), la configuración del firewall y la red, el IAM
 - Encriptación de los datos de la aplicación
- Controles compartidos:
 - Gestión de parches, gestión de la configuración, concienciación y formación

Ejemplo para RDS



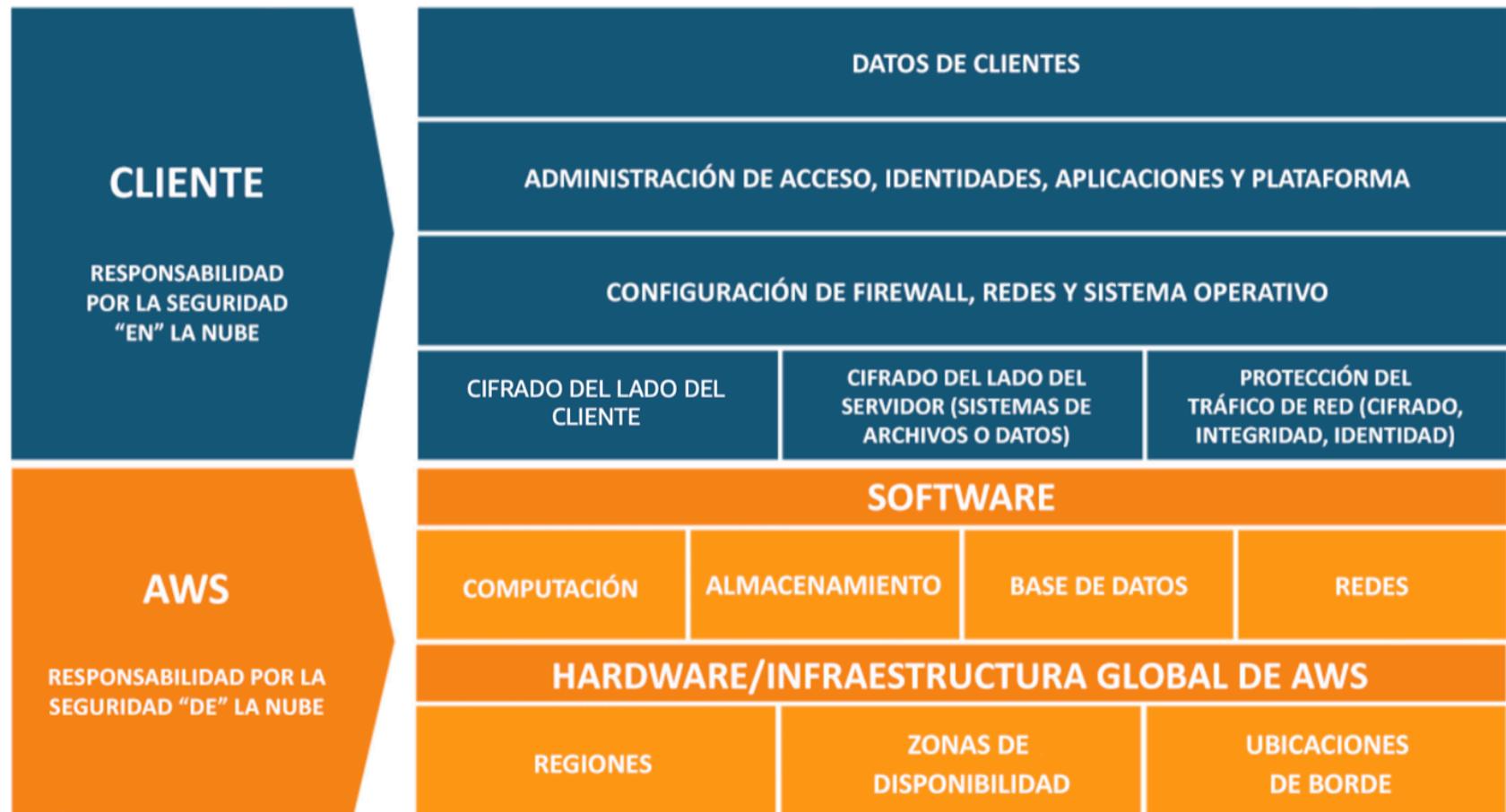
- Responsabilidad de AWS:
 - Gestionar la instancia EC2 subyacente, desactivar el acceso SSH
 - Parcheo automatizado de la BD
 - Parcheo automatizado del SO
 - Auditar la instancia subyacente y los discos y garantizar su funcionamiento
- Tu responsabilidad:
 - Comprobar las reglas de entrada de puertos / IP / grupo de seguridad en el SG de la BD
 - Creación de usuarios en la base de datos y permisos
 - Crear una base de datos con o sin acceso público
 - Asegúrate de que los grupos de parámetros o la BD están configurados para permitir sólo conexiones SSL
 - Configuración del cifrado de la base de datos



Ejemplo para S3

- Responsabilidad de AWS:
 - Garantizarte que obtienes almacenamiento ilimitado
 - Garantizarte la encriptación
 - Garantizar la separación de los datos entre diferentes clientes
 - Garantizar que los empleados de AWS no puedan acceder a tus datos
- Tu responsabilidad:
 - Configuración del bucket
 - Política de bucket / configuración pública
 - Usuario y roles IAM
 - Habilitar el cifrado

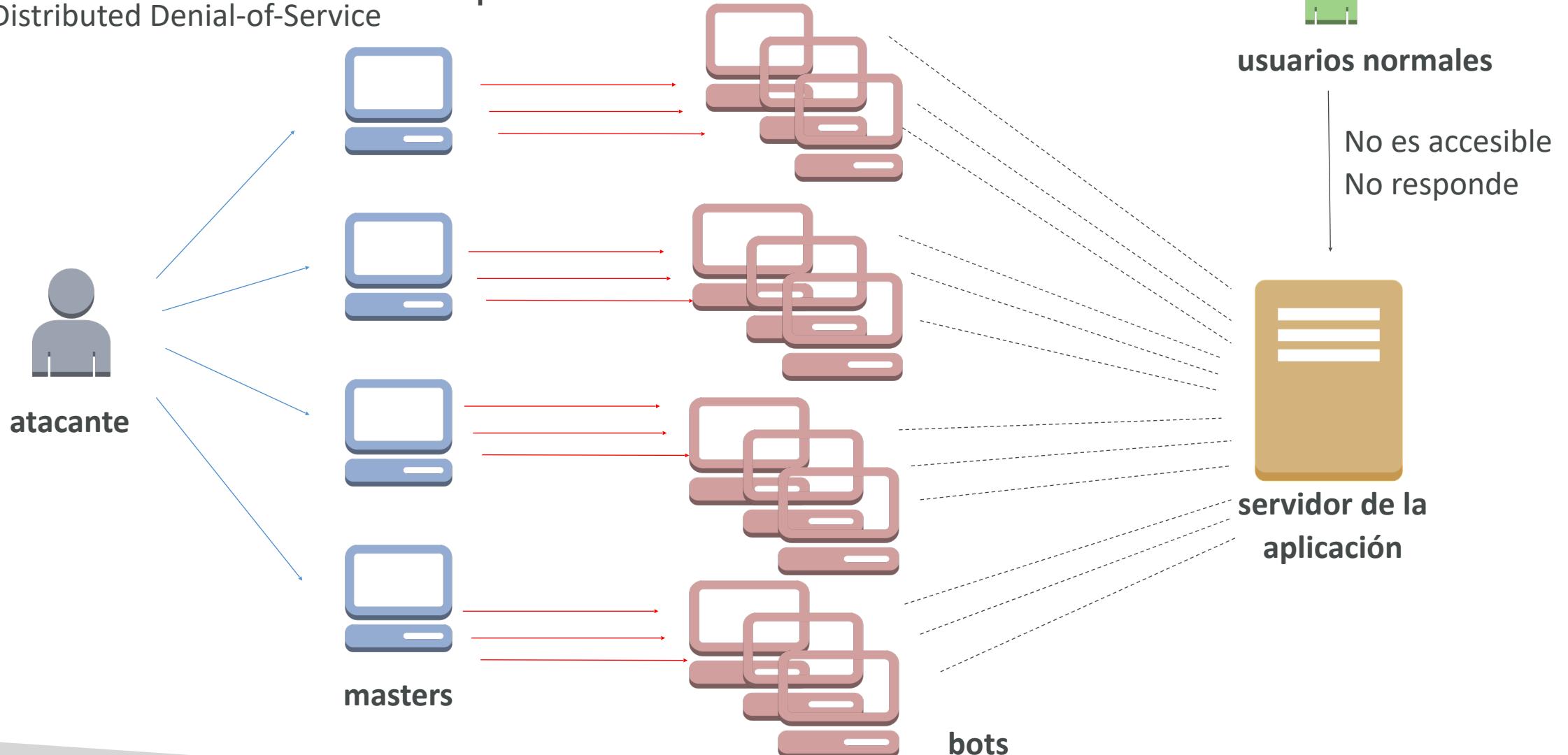
Diagrama del modelo de responsabilidad compartida



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

¿Qué es un ataque DDoS?

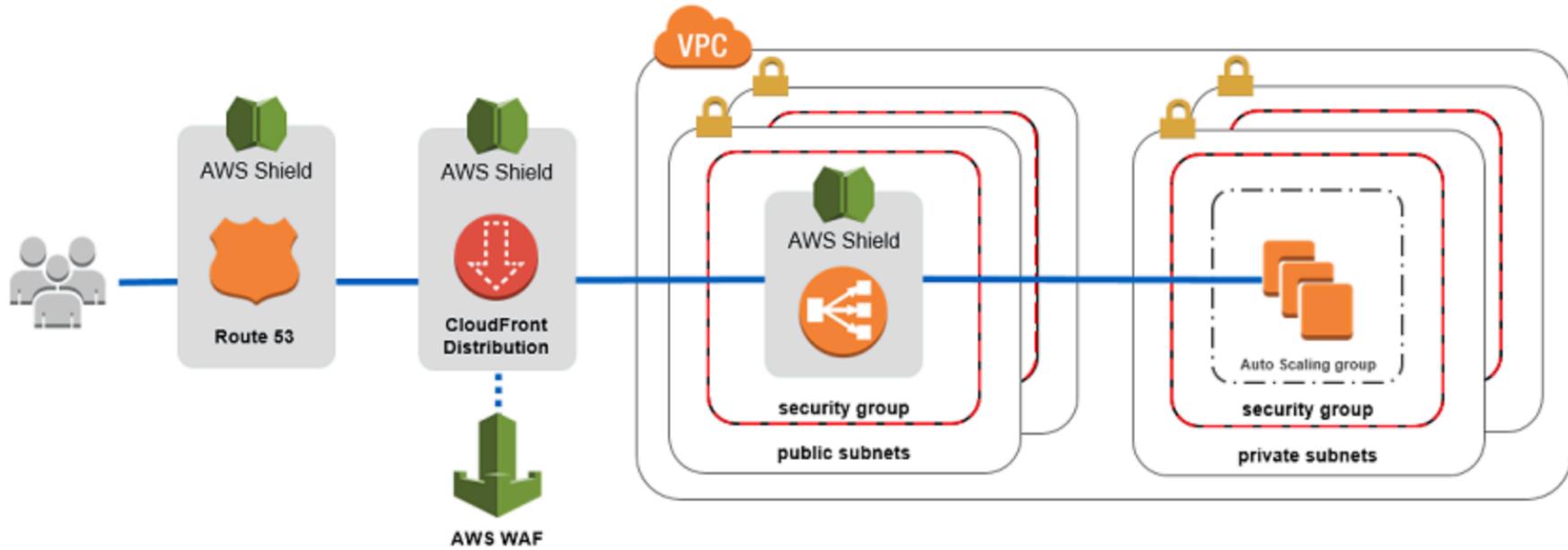
*Distributed Denial-of-Service



Protección DDoS en AWS

- **AWS Shield Standard:** protege contra ataques DDOS a tu sitio web y aplicaciones, para todos los clientes sin coste adicional
- **AWS Shield Advanced:** protección DDoS premium 24/7
- **AWS WAF:** Filtra solicitudes específicas basadas en reglas
- **CloudFront y Route 53:**
 - Protección de la disponibilidad mediante una red de borde global
 - Combinado con AWS Shield, proporciona mitigación de ataques en el borde
- Prepárate para escalar: aprovecha **AWS Auto Scaling**

Ejemplo de arquitectura de referencia para la protección DDoS



<https://aws.amazon.com/answers/networking/aws-ddos-attack-mitigation/>

AWS Shield



- **AWS Shield Standard:**
 - Servicio gratuito que se activa para cada cliente de AWS
 - Proporciona protección contra ataques como SYN/UDP Floods, ataques de reflexión y otros ataques de capa 3/capa 4
- **AWS Shield Advanced:**
 - Servicio opcional de mitigación de DDoS (3.000 dólares al mes por organización)
 - Protege contra ataques más sofisticados en [Amazon EC2](#), [Elastic Load Balancing \(ELB\)](#), [Amazon CloudFront](#), [AWS Global Accelerator](#) y [Route 53](#)
 - Acceso 24 horas al día, 7 días a la semana, al equipo de respuesta DDoS de AWS (DRP)
 - Protege contra las tarifas más altas durante los picos de uso debidos a los DDoS

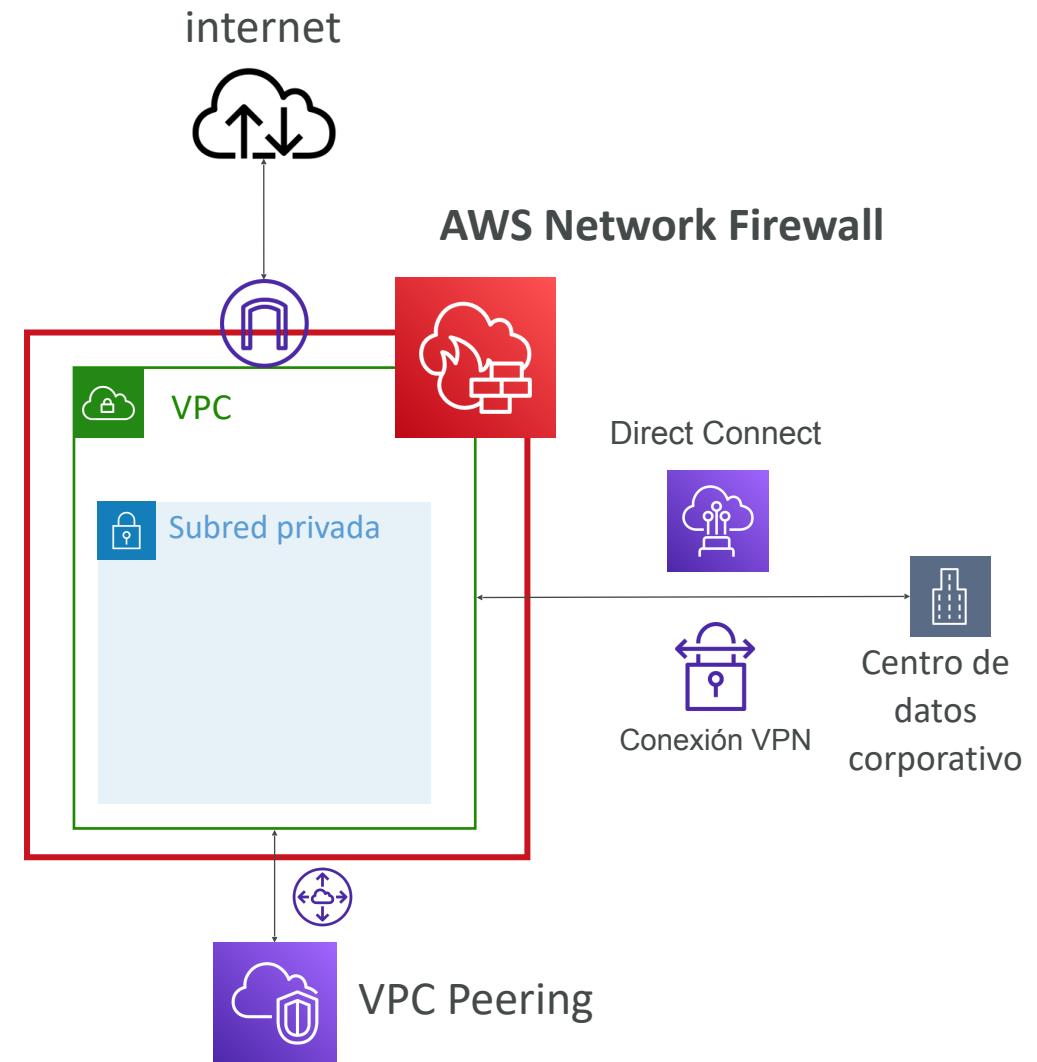
AWS WAF – Web Application Firewall



- Protege tus aplicaciones web de las vulnerabilidades web más comunes (Capa 7)
- La **Capa 7 es HTTP** (frente a la Capa 4 que es TCP)
- Despliega en el **Application Load Balancer, API Gateway, CloudFront**
- Define la ACL (Lista de Control de Acceso a la Web):
 - Las reglas pueden incluir **direcciones IP**, cabeceras HTTP, cuerpo HTTP o cadenas URI
 - Protege de los ataques más comunes: **inyección SQL** y **Cross-Site Scripting (XSS)**
 - Restricciones de tamaño, **geo-match (bloquear países)**
 - **Reglas basadas en la tasa** (para contar las ocurrencias de los eventos) - **para la protección DDoS**

AWS Network Firewall

- Protege toda tu Amazon VPC
- Protección de capa 3 a capa 7
- En cualquier dirección, puedes inspeccionar
 - Tráfico de VPC a VPC
 - Saliente a Internet
 - Entrante desde Internet
 - Hacia / desde Direct Connect y VPN Site-to-Site





Pruebas de penetración en el Cloud de AWS

- Los clientes de AWS pueden llevar a cabo evaluaciones de seguridad o pruebas de penetración en su infraestructura de AWS **sin la aprobación previa de 8 servicios:**
 - Instancias de Amazon EC2, NAT Gateways y Elastic Load Balancers
 - Amazon RDS
 - Amazon CloudFront
 - Amazon Aurora
 - Amazon API Gateway
 - Funciones AWS Lambda y Lambda Edge
 - Recursos de Amazon Lightsail
 - Entornos de Amazon Elastic Beanstalk
- La lista puede aumentar con el tiempo (no se te hará la pregunta en el examen)

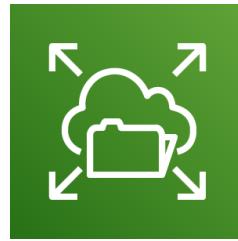


Pruebas de penetración en el Cloud de AWS

- **Actividades prohibidas**

- Caminar por la zona DNS a través de las Zonas Alojadas de Amazon Route 53
- Denial of Service (DoS), Distributed Denial of Service (DDoS), DoS simulado, DDoS simulado
- Inundación de puertos
- Inundación de protocolos
- Inundación de solicitudes (inundación de solicitudes de inicio de sesión, inundación de solicitudes de API)
- Para cualquier otro evento simulado, contacta con aws-security-simulated-event@amazon.com
- Leer más: <https://aws.amazon.com/security/penetration-testing/>

Datos en reposo vs. Datos en tránsito



Cifrado en reposo en EFS

Cifrado en tránsito durante la carga



Cifrado en reposo en S3

- **En reposo:** datos almacenados o archivados en un dispositivo
 - En un disco duro, en una instancia RDS, en S3 Glacier Deep Archive, etc.
- **En tránsito (en movimiento):** datos que se trasladan de un lugar a otro
 - Transferencia de las instalaciones a AWS, de EC2 a DynamoDB, etc.
 - **Significa que los datos se transfieren en la red**
- Queremos cifrar los datos en ambos estados para protegerlos.
- Para ello aprovechamos las **claves de cifrado**

AWS KMS (Key Management Service)



- Cada vez que escuches "encriptación" para un servicio de AWS, lo más probable es que se trate de KMS
- KMS = **AWS gestiona las claves de cifrado por nosotros**
- **Opción de cifrado:**
 - Volúmenes EBS: cifrar volúmenes
 - Buckets S3: Encriptación de objetos en el lado del servidor
 - Base de datos Redshift: cifrado de datos
 - Base de datos RDS: cifrado de datos
 - Unidades EFS: cifrado de datos
- **Cifrado activado automáticamente:**
 - Logs de CloudTrail
 - S3 Glacier
 - Storage Gateway

CloudHSM



- KMS => AWS gestiona el software de encriptación
- CloudHSM => AWS proporciona el **hardware** de encriptación
- Hardware dedicado (HSM = Módulo de Seguridad de Hardware)
- Gestionas por completo tus propias claves de cifrado (no AWS)
- El dispositivo HSM es resistente a la manipulación, cumple la normativa FIPS 140-2 Nivel 3



Ejemplo de dispositivo HSM

Diagrama CloudHSM



Tipos de Customer Master Keys: CMK

- **CMK gestionado por el cliente:**

- Creada, gestionada y utilizada por el cliente, puede ser activada o desactivada
- Posibilidad de política de rotación (se genera una nueva clave cada año, se conserva la antigua)
- Posibilidad de traer tu propia clave

- **CMK gestionada por AWS:**

- Creada, gestionada y utilizada en nombre del cliente por AWS
- Utilizada por los servicios de AWS (aws/s3, aws/ebs, aws/redshift)

- **CMK propiedad de AWS:**

- Colección de CMKs que un servicio de AWS posee y gestiona para utilizarlas en múltiples cuentas
- AWS puede utilizarlas para proteger los recursos de tu cuenta (pero no puedes ver las claves)

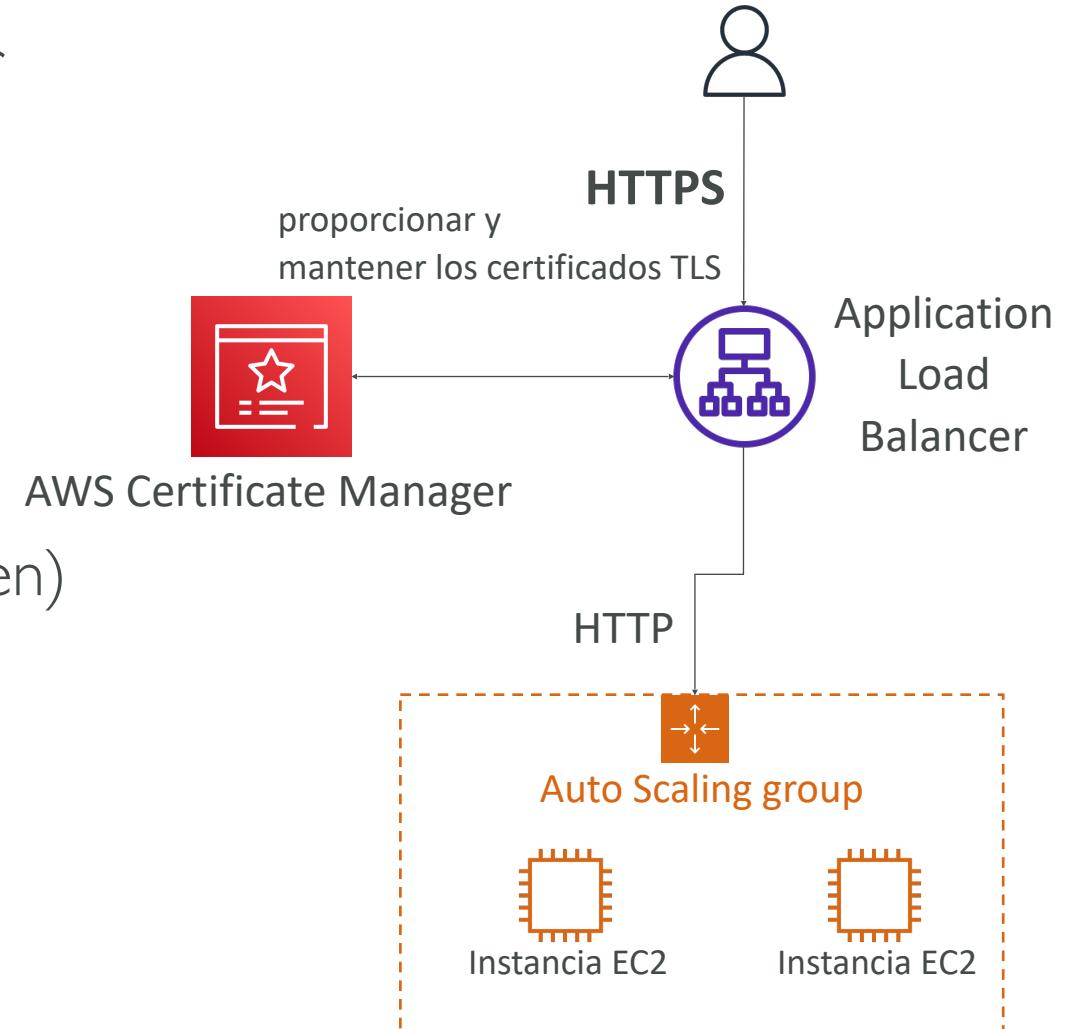
- **Claves CloudHSM (almacén de claves personalizado):**

- Claves generadas desde tu propio dispositivo de hardware CloudHSM
- Las operaciones criptográficas se realizan dentro del cluster CloudHSM

AWS Certificate Manager (ACM)



- Te permite aprovisionar, gestionar y desplegar fácilmente los **certificados SSL/TLS**
- Se utilizan para proporcionar encriptación en vuelo para los sitios web (HTTPS)
- Admite certificados TLS públicos y privados
- Gratuito para los certificados TLS públicos
- Renovación automática de certificados TLS
- Integraciones con (carga de certificados TLS en)
 - Elastic Load Balancers
 - Distribuciones de CloudFront
 - APIs en API Gateway



AWS Secrets Manager



- Servicio más nuevo, destinado a almacenar secretos
- Capacidad para forzar la **rotación de secretos** cada X días
- Automatizar la generación de secretos en la rotación (utiliza Lambda)
- Integración con **Amazon RDS** (MySQL, PostgreSQL, Aurora)
- Los secretos se encriptan mediante KMS
- Principalmente pensado para la integración con RDS



AWS Artifact (no es realmente un servicio)

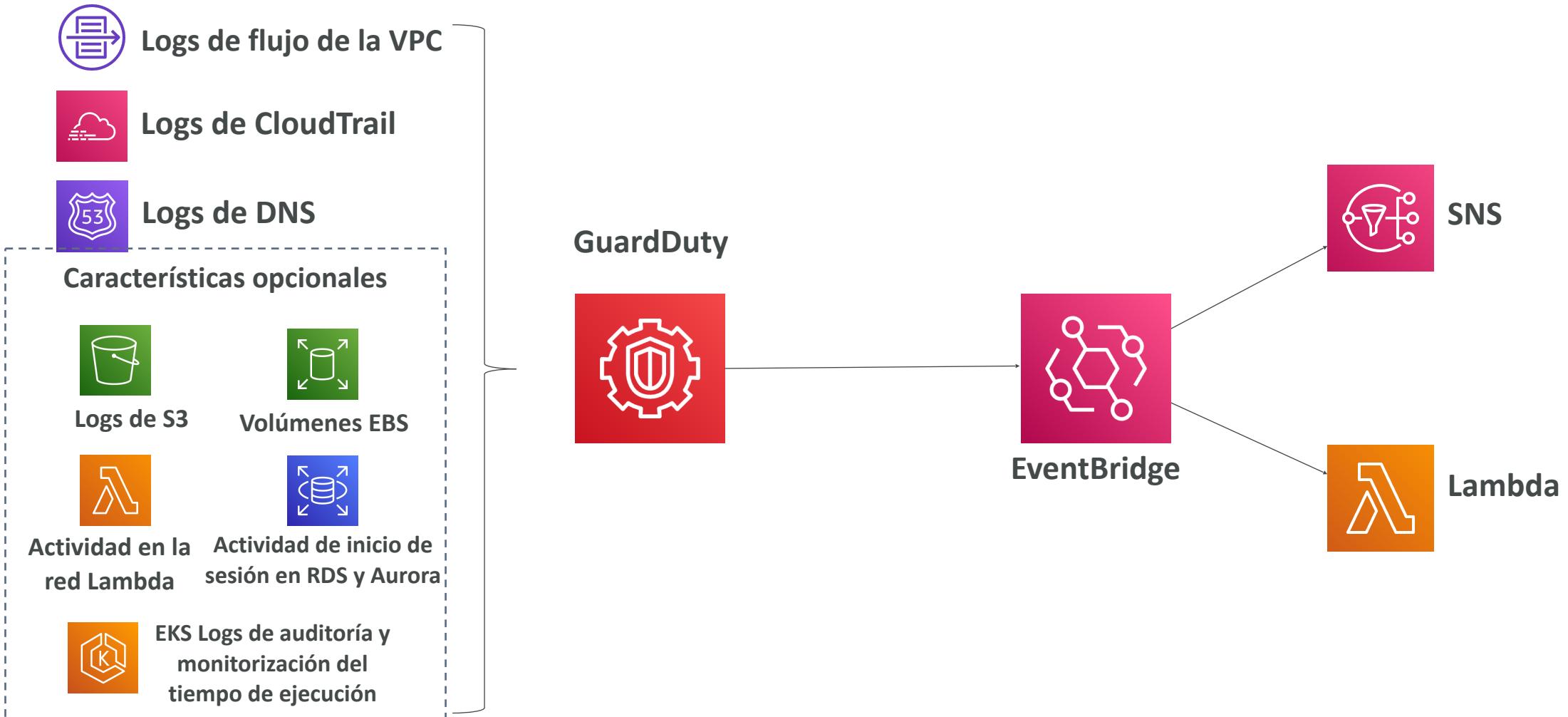
- **Portal que proporciona a los clientes acceso bajo demanda a la documentación de conformidad de AWS y a los acuerdos de AWS**
- **Artifact Reports** - Te permite descargar los documentos de seguridad y conformidad de AWS de auditores externos, como las certificaciones ISO de AWS, los informes del sector de las tarjetas de pago (PCI) y los informes de control de sistemas y organizaciones (SOC)
- **Artifact Agreements** - Te permite revisar, aceptar y hacer un seguimiento del estado de los acuerdos de AWS, como el Business Associate Addendum (BAA) o la Health Insurance Portability and Accountability Act (HIPAA) para una cuenta individual o en tu organización
- Puede utilizarse para **apoyar la auditoría interna o la normativa**



Amazon GuardDuty

- Descubrimiento inteligente de amenazas para proteger la cuenta de AWS
- Utiliza algoritmos de Machine Learning, detección de anomalías y datos de terceros
- Se activa con un clic (30 días de prueba), sin necesidad de instalar software
- Los datos de entrada incluyen:
 - **Logs de eventos de CloudTrail** - llamadas inusuales a la API, despliegues no autorizados
 - **Eventos de gestión de CloudTrail** - crear subred VPC, crear rastro, ...
 - **Eventos de datos S3 de CloudTrail** - obtener objeto, listar objetos, eliminar objeto, ...
 - **Logs de flujo de la VPC** - tráfico interno inusual, dirección IP inusual
 - **Logs de DNS** - instancias EC2 comprometidas que envían datos codificados dentro de las consultas DNS
 - **Características opcionales** - EKS Audit Logs, RDS & Aurora, EBS, Lambda, S3 Data Events...
- Puedes configurar **reglas de EventBridge de CloudWatch** para ser notificado en caso de hallazgos
- Las reglas de EventBridge pueden dirigirse a AWS Lambda o SNS
- **Puede proteger contra ataques de criptomonedas (tiene un "hallazgo" dedicado a ello)**

Amazon GuardDuty



Amazon Inspector

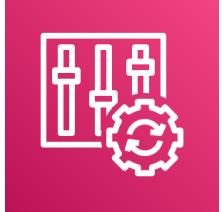
- **Evaluaciones de seguridad automatizadas**
- **Para instancias EC2**
 - Aprovechando el agente **AWS System Manager (SSM)**
 - Analiza contra **accesibilidad no intencionada a la red**
 - Analizar el **SO en ejecución** frente a vulnerabilidades conocidas
- **Para imágenes de contenedor enviadas a Amazon ECR**
 - Evaluación de las imágenes de contenedor a medida que se envían
- **Para Funciones Lambda**
 - Identifica vulnerabilidades de software en el código de las funciones y en las dependencias de los paquetes
 - Evaluación de funciones a medida que se despliegan
- Informes e integración con AWS Security Hub
- Envío de hallazgos a Amazon Event Bridge



¿Qué evalúa Amazon Inspector?

- **Recuerda: sólo para instancias EC2, imágenes de contenedor y funciones Lambda**
- Escaneo continuo de la infraestructura, sólo cuando sea necesario
- Vulnerabilidades de paquetes (EC2, ECR & Lambda) - base de datos de CVE
- Accesibilidad de la red (EC2)
- Se asocia una puntuación de riesgo a todas las vulnerabilidades para priorizarlas

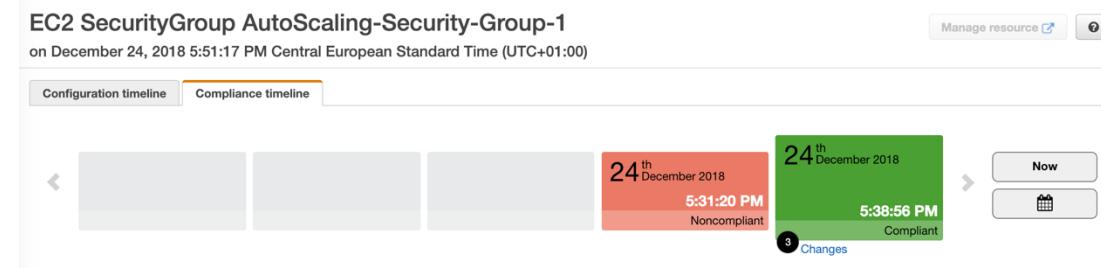
AWS Config



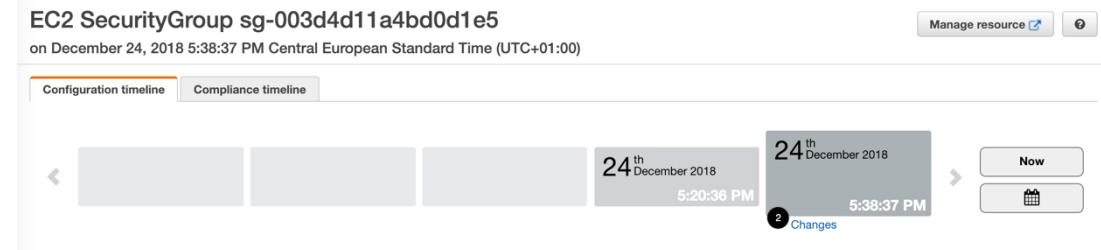
- Ayuda a **auditar y registrar la normativa de tus recursos de AWS**
- Ayuda a **registrar las configuraciones y los cambios a lo largo del tiempo**
- Posibilidad de almacenar los datos de configuración en S3 (analizados por Athena)
- Preguntas que se pueden resolver con AWS Config:
 - ¿Hay acceso SSH sin restricciones a mis grupos de seguridad?
 - ¿Mis buckets tienen acceso público?
 - ¿Cómo ha cambiado la configuración de mi ALB con el tiempo?
- Puedes recibir alertas (notificaciones SNS) de cualquier cambio
- AWS Config es un servicio por región
- Puede agregarse entre regiones y cuentas

Recurso de AWS Config

- Ver la normativa de un recurso a lo largo del tiempo



- Ver la configuración de un recurso a lo largo del tiempo

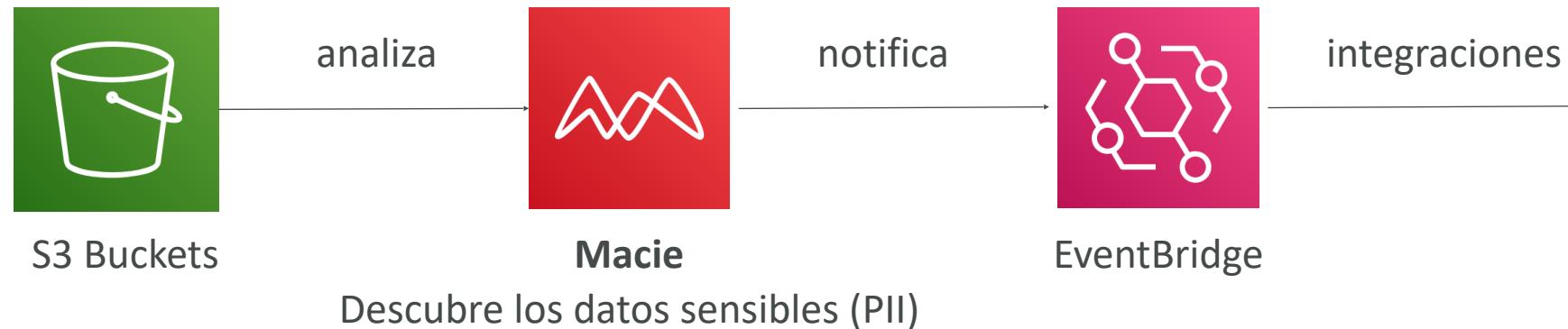


- Ver las llamadas a la API de CloudTrail si están activadas

Amazon Macie



- Amazon Macie es un servicio de seguridad y privacidad de datos totalmente gestionado que utiliza el **machine learning y la concordancia de patrones para descubrir y proteger tus datos sensibles en AWS**.
- Macie te ayuda a identificar y alertar sobre los **datos sensibles, como la información personal identifiable (PII)**

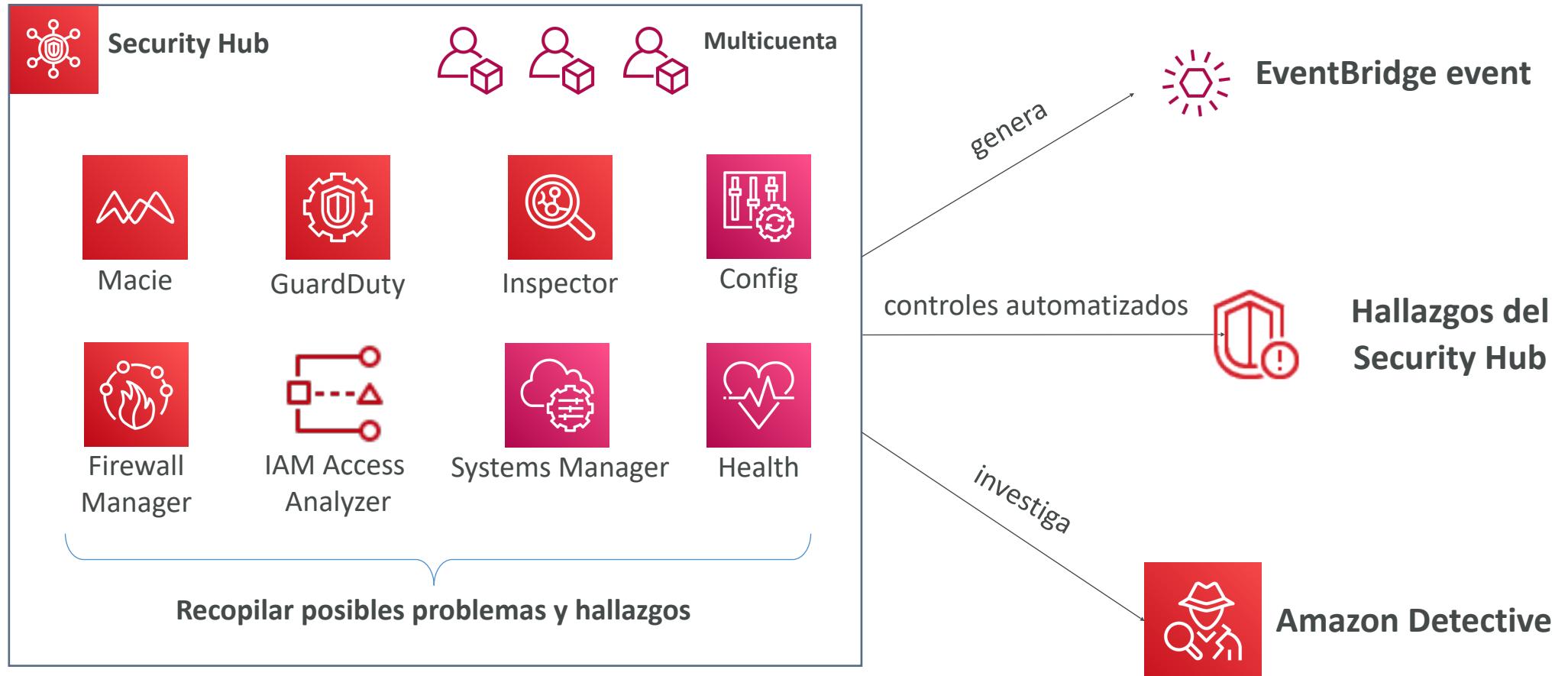




AWS Security Hub

- **Herramienta de seguridad central** para gestionar la **seguridad en varias cuentas de AWS y automatizar las comprobaciones de seguridad**
- Dashboards integrados que muestran el estado actual de la seguridad y la normativa para tomar medidas rápidamente
- Agrega automáticamente alertas en formatos predefinidos o de hallazgos personales de varios servicios de AWS y herramientas de socios de AWS:
 - Config
 - GuardDuty
 - Inspector
 - Macie
 - IAM Access Analyzer
 - AWS Systems Manager
 - AWS Firewall Manager
 - AWS Health
 - AWS Partner Network Solutions
- Primero debes habilitar el servicio de configuración de AWS

AWS Security Hub



Amazon Detective



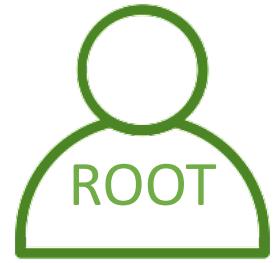
- GuardDuty, Macie y Security Hub se utilizan para identificar posibles problemas de seguridad, o hallazgos
- A veces los hallazgos de seguridad requieren un análisis más profundo para aislar la causa raíz y tomar medidas: es un proceso complejo
- Amazon Detective **analiza, investiga e identifica rápidamente la causa raíz de los problemas de seguridad o las actividades sospechosas (mediante ML y grafos)**
- **Recoge y procesa automáticamente los eventos** de Logs de flujo de la VPC, CloudTrail, GuardDuty y crea una vista unificada
- Produce visualizaciones con detalles y contexto para llegar a la causa raíz

AWS Abuse



- **Informar de la sospecha de que los recursos de AWS se utilizan con fines abusivos o ilegales**
- Los comportamientos abusivos y prohibidos son:
 - **Spam** - recibir correos electrónicos no deseados desde una dirección IP propiedad de AWS, sitios web y foros con spam de los recursos de AWS
 - **Escaneo de puertos** - envío de paquetes a sus puertos para descubrir los no seguros
 - **Ataques DoS o DDoS** - direcciones IP propiedad de AWS que intentan sobrecargar o colapsar tus servidores/software
 - **Intentos de intrusión** - logs en tus recursos
 - **Alojar contenido censurable o con derechos de autor** - distribuir contenido ilegal o con derechos de autor sin consentimiento
 - **Distribución de malware** - recursos de AWS que distribuyen software para dañar ordenadores o máquinas
- Ponte en contacto con el equipo de abusos de AWS: [AWS abuse form](#), o abuse@amazonaws.com

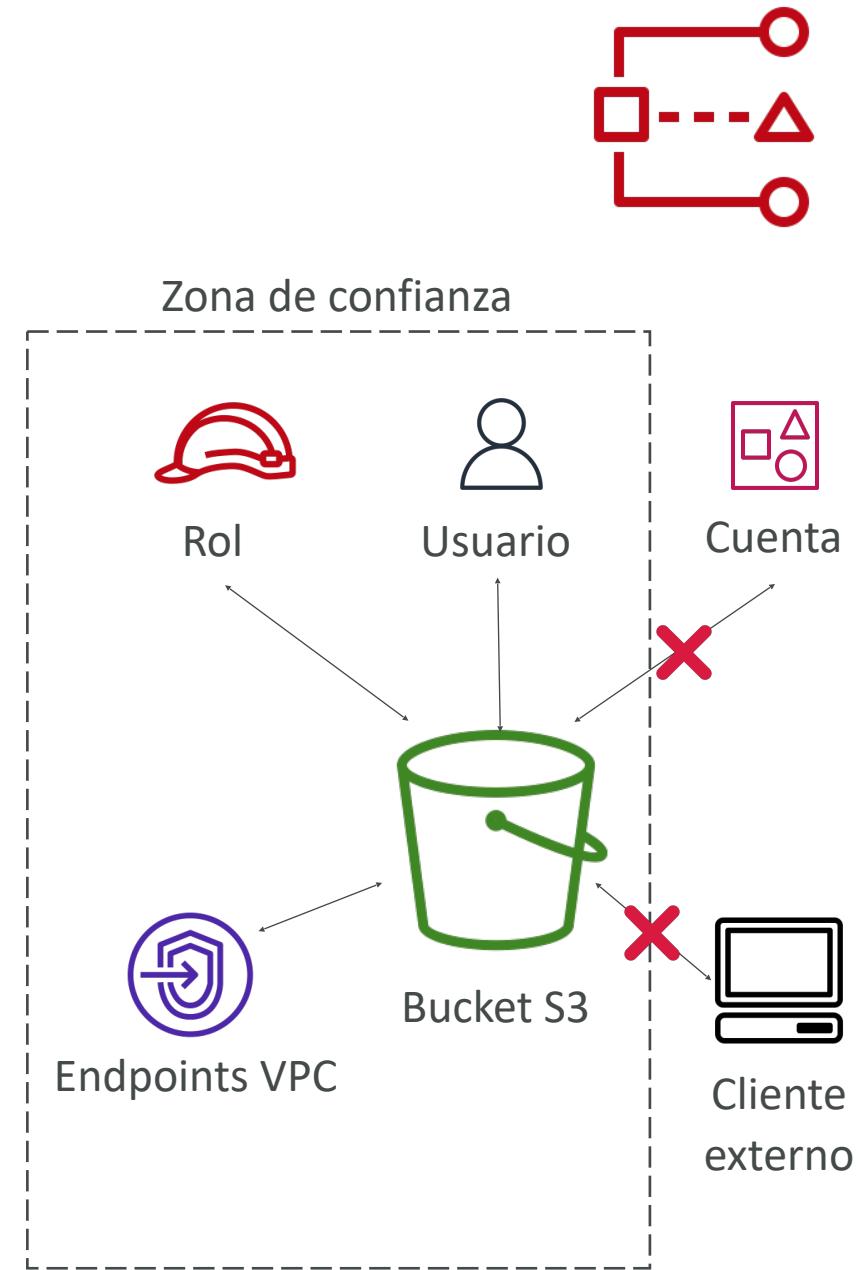
Privilegios de usuario root



- Usuario root = Propietario de la cuenta (creado cuando se crea la cuenta)
- Tiene acceso completo a todos los servicios y recursos de AWS
- **Bloquea las claves de acceso del usuario root de tu cuenta de AWS**
- No utilices la cuenta root para las tareas cotidianas, ni siquiera para las administrativas
- Acciones que sólo puede realizar el usuario root:
 - **Cambiar la configuración de la cuenta** (nombre de la cuenta, dirección de correo electrónico, contraseña del usuario root, claves de acceso del usuario root)
 - Ver ciertas facturas de impuestos
 - **Cerrar la cuenta de AWS**
 - Restaurar los permisos del usuario IAM
 - **Cambiar o cancelar el plan de AWS Support**
 - **Registrarse como vendedor en el Marketplace de instancias reservadas**
 - Configurar un bucket de Amazon S3 para habilitar la MFA
 - Editar o eliminar una política de bucket de Amazon S3 que incluya un ID de VPC o un ID de endpoints de VPC no válido
 - Registrarse en GovCloud

IAM Access Analyzer

- Averigua qué recursos se comparten externamente
 - Buckets S3
 - Roles IAM
 - Claves KMS
 - Funciones Lambda y capas
 - Colas SQS
 - Secrets Manager
- Definir **zona de confianza** = Cuenta de AWS o AWS Organization
- Acceso fuera de zona de confianza => hallazgos



Resumen - Seguridad y normativa

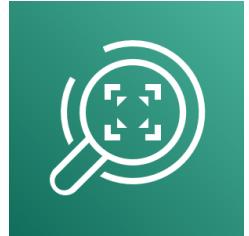
- **Responsabilidad compartida en AWS**
- **Shield:** Protección DDoS automática + soporte 24/7 avanzado
- **WAF:** Firewall para filtrar las peticiones entrantes basado en reglas
- **KMS:** Claves de cifrado gestionadas por AWS
- **CloudHSM:** Cifrado por hardware, gestionamos las claves de cifrado
- **AWS Certificate Manager:** Aprovisiona, administra e implementa certificados SSL/TLS
- **Artifact:** Accede a informes de normativa como PCI, ISO, etc...
- **GuardDuty:** Encuentra comportamientos maliciosos con los logs de VPC, DNS y CloudTrail
- **Inspector:** Encuentra vulnerabilidades de software en EC2, Imágenes ECR y funciones Lambda
- **Network Firewall:** Protege la VPC contra ataques de red

Resumen - Seguridad y normativa

- **Config:** Rastrea los cambios de configuración y el cumplimiento de la normativa
- **Macie:** Encuentra datos sensibles (por ejemplo, datos PII) en buckets de Amazon S3
- **CloudTrail:** Rastrea las llamadas a la API realizadas por los usuarios dentro de la cuenta
- **AWS Security Hub:** reúne los resultados de seguridad de varias cuentas de AWS
- **Amazon Detective:** encuentra la causa raíz de los problemas de seguridad o las actividades sospechosas
- **AWS Abuse:** Informa de los recursos de AWS utilizados con fines abusivos o ilegales
- **Privilegios del usuario root:**
 - Cambia la configuración de la cuenta
 - Cierra tu cuenta de AWS
 - Cambia o cancela tu plan de AWS Support
 - Registrarte como vendedor en el Marketplace de instancias reservadas
- **IAM Access Analyzer:** identifica qué recursos se comparten externamente

Machine Learning

Amazon Rekognition



- Encuentra **objetos, personas, textos, escenas en imágenes** y **vídeos** mediante ML
- **Análisis facial** y **búsqueda facial** para hacer verificación de usuarios, recuento de personas
- Crear una base de datos de "caras conocidas" o comparar con famosos
- Casos de uso:
 - Etiquetado
 - Moderación de contenidos
 - Detección de textos
 - Detección y análisis de rostros (género, rango de edad, emociones...)
 - Búsqueda y verificación de rostros
 - Reconocimiento de famosos
 - Trayectoria (por ejemplo, para el análisis de juegos deportivos)

<https://aws.amazon.com/rekognition/>

Amazon Transcribe



- **Convierte** automáticamente el **habla en texto**
- Utiliza un **proceso de deep learning** llamado **reconocimiento automático del habla** (ASR) para convertir el habla en texto de forma rápida y precisa
- **Elimina automáticamente la Información de Identificación Personal (PII)**
- **Soporta identificación automática de idioma para audio multilingüe**
- Casos de uso:
 - transcribir llamadas de atención al cliente
 - automatizar el subtulado y los subtítulos
 - generar metadatos para los activos de los medios de comunicación para crear un archivo con todas las posibilidades de búsqueda



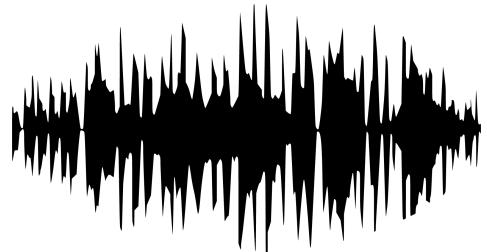
*"Hola mi nombre es Joan.
¡Espero que disfrutes del curso!"*

Amazon Polly



- Convierte el texto en voz real utilizando el aprendizaje profundo
- Permitiendo crear aplicaciones que hablan

*Hi! My name is Stéphane
and this is a demo of Amazon Polly*



Amazon Translate



- **Traducción** natural y precisa de **idiomas**
- Amazon Translate te permite **localizar contenidos** -como sitios web y aplicaciones- para **usuarios internacionales**, y traducir fácilmente grandes volúmenes de texto de forma eficiente.

Source language

Auto (auto) ▾

Hi my name is Stéphane

Target language

French (fr) ▾

Bonjour, je m'appelle Stéphane.

Portuguese (pt) ▾

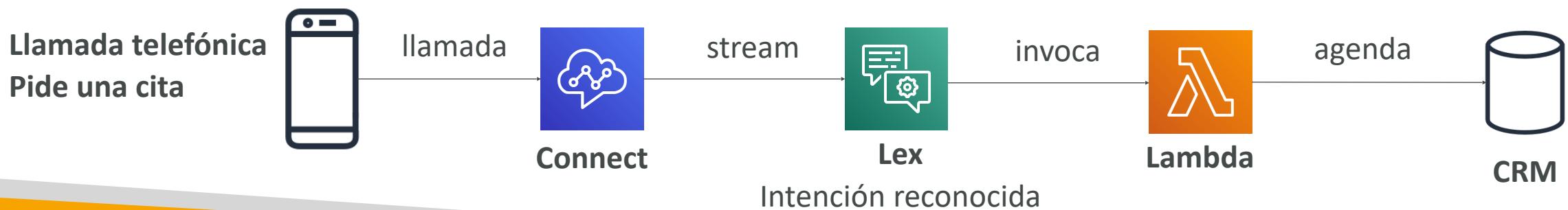
Oi, meu nome é Stéphane.

Hindi (hi) ▾

हाय मेरा नाम स्टीफन है

Amazon Lex & Connect

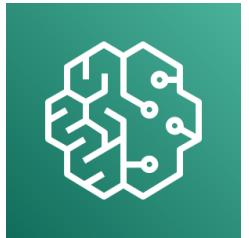
- **Amazon Lex:** (la misma tecnología que impulsa a Alexa)
 - Reconocimiento automático del habla (ASR) para convertir el habla en texto
 - Comprensión del Lenguaje Natural (NLU) para reconocer la intención del texto, de las personas que llaman
 - Ayuda a crear chatbots, bots de centros de llamadas
- **Amazon Connect:**
 - Recibe llamadas, crea flujos de contacto, **centro de contacto virtual** basado en la nube
 - Puede integrarse con otros sistemas CRM o AWS
 - Sin pagos iniciales, un 80% más barato que las soluciones tradicionales de centro de contacto



Amazon Comprehend

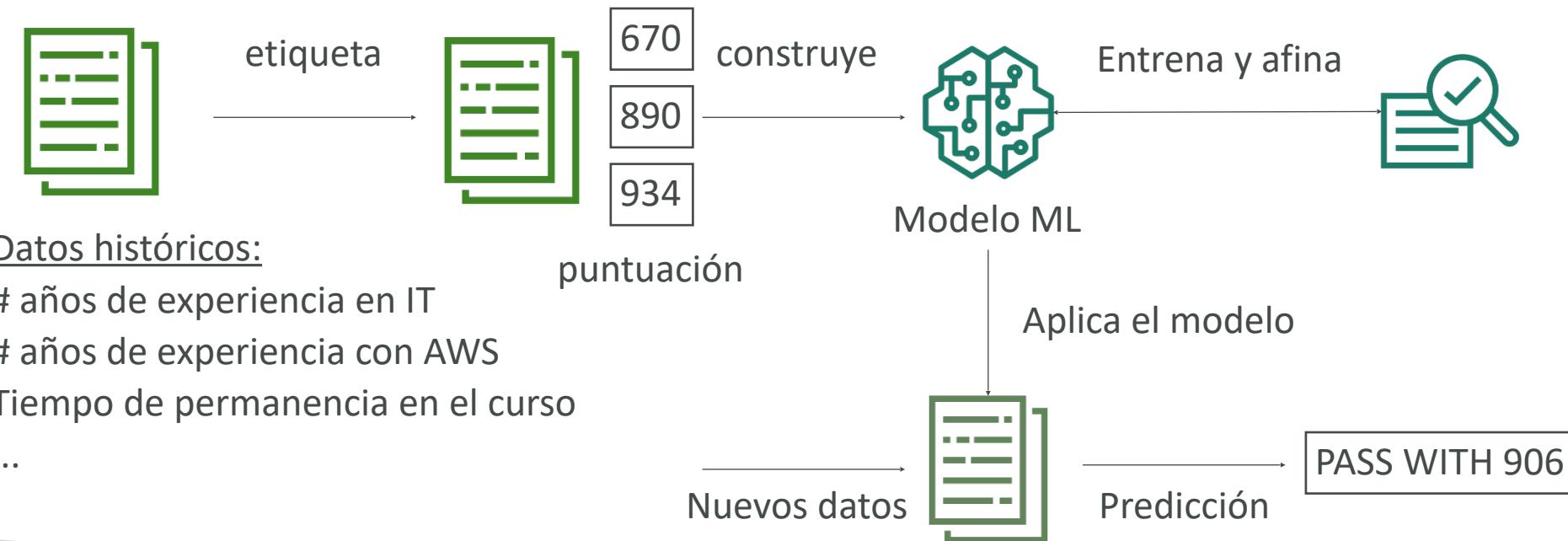


- Para el **Natural Language Processing – NLP (Procesamiento del Lenguaje Natural - PNL)**
- Servicio totalmente gestionado y sin servidor
- Utiliza el Machine Learning para encontrar ideas y relaciones en el texto
 - Lenguaje del texto
 - Extrae frases clave, lugares, personas, marcas o eventos
 - Comprende lo positivo o negativo del texto
 - Analiza el texto utilizando la tokenización y las partes del discurso
 - Organiza automáticamente una colección de archivos de texto por temas
- Ejemplos de casos de uso:
 - Analiza las interacciones con los clientes (correos electrónicos) para encontrar lo que conduce a una experiencia positiva o negativa
 - Crea y agrupa artículos por temas que Comprehend descubrirá



Amazon SageMaker

- Servicio totalmente gestionado para que los desarrolladores/científicos de datos construyan modelos ML
- Normalmente, es difícil hacer todos los procesos en un solo lugar + aprovisionar servidores
- Proceso de Machine Learning (simplificado): predecir la nota de tu examen



Amazon Forecast



- Servicio totalmente gestionado que utiliza el ML para ofrecer previsiones muy precisas
- Ejemplo: predecir las futuras ventas de un chubasquero
- Un 50% más de precisión que mirando los datos por sí mismos
- Reduce el tiempo de previsión de meses a horas
- Casos de uso: Planificación de la demanda de productos, planificación financiera, planificación de recursos, ...

Datos históricos de series temporales:

Características del producto

Precios

Descuentos

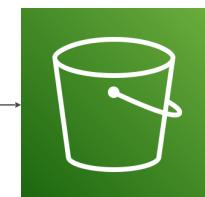
Tráfico del sitio web

Ubicación de las tiendas

...



carga



Amazon S3



Amazon Forecast

produce



Forecasting Model

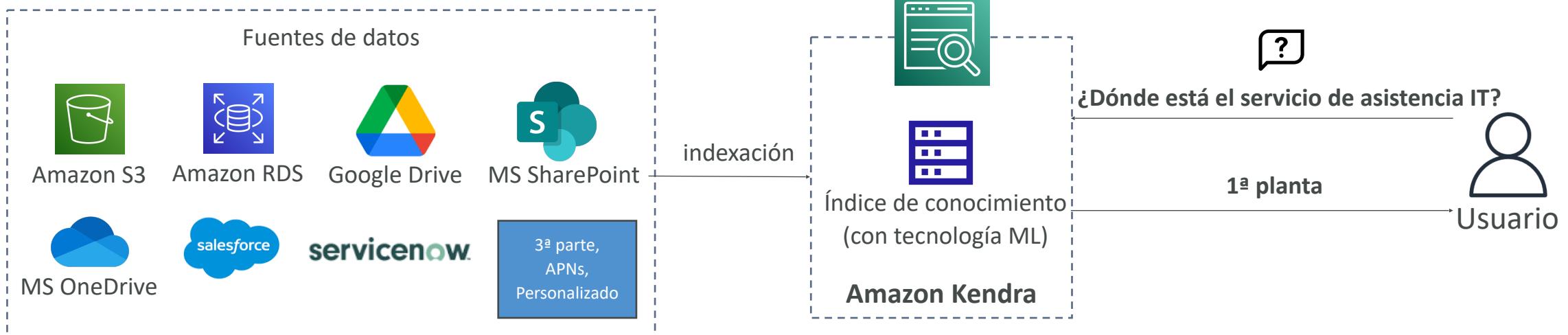


Ventas futuras
del impermeable:
500.000 dólares

Amazon Kendra



- **Servicio de búsqueda de documentos** totalmente gestionado y potenciado por Machine Learning
- Extrae respuestas de un documento (texto, pdf, HTML, PowerPoint, MS Word, preguntas frecuentes...)
- Capacidades de búsqueda en lenguaje natural
- Aprende de las interacciones/retroalimentación de los usuarios para promover los resultados preferidos (aprendizaje incremental)
- Capacidad de afinar manualmente los resultados de la búsqueda (importancia de los datos, frescura, personalización, ...)





Amazon Personalize

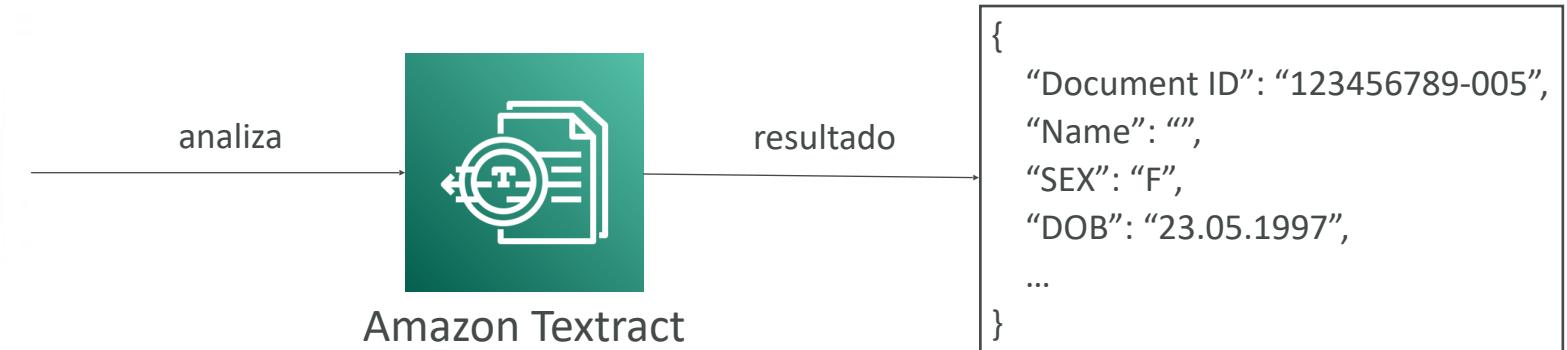
- Servicio de ML totalmente gestionado para crear aplicaciones con recomendaciones personalizadas en tiempo real
- Ejemplo: recomendaciones/reclasificación de productos personalizados, marketing directo personalizado
 - Ejemplo: El usuario compró herramientas de jardinería, proporciona recomendaciones sobre la próxima que debe comprar
- La misma tecnología utilizada por Amazon.com
- Se integra en sitios web existentes, aplicaciones, SMS, sistemas de marketing por correo electrónico, ...
- Se implementa en días, no en meses (no es necesario construir, formar y desplegar soluciones de ML)
- Casos de uso: tiendas minoristas, medios de comunicación y entretenimiento...



Amazon Textract



- Extrae automáticamente el texto, la escritura y los datos de cualquier documento escaneado utilizando IA y ML



- Extrae datos de formularios y tablas
- Leer y procesar cualquier tipo de documento (PDFs, imágenes, ...)
- Casos de uso:
 - Servicios financieros (por ejemplo, facturas, informes financieros)
 - Sanidad (por ejemplo, historiales médicos, reclamaciones de seguros)
 - Sector público (por ejemplo, formularios fiscales, documentos de identidad, pasaportes)

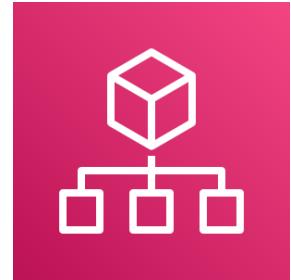
Resumen - Machine Learning

- **Rekognition:** detección de caras, etiquetado, reconocimiento de famosos
- **Transcribe:** de audio a texto (por ejemplo, subtítulos)
- **Polly:** de texto a audio
- **Translate:** traducciones
- **Lex:** construir bots conversacionales - chatbots
- **Connect:** centro de contacto en el Cloud
- **Comprehend:** procesamiento del lenguaje natural
- **SageMaker:** Machine Learning para todos los desarrolladores y científicos de datos
- **Forecast:** construye previsiones muy precisas
- **Kendra:** motor de búsqueda con ML
- **Personalize:** recomendaciones personalizadas en tiempo real
- **Textract:** detecta texto y datos en los documentos

Gestión de cuentas, facturación y asistencia

AWS Organizations

- Servicio global
- Permite gestionar **varias cuentas de AWS**
- La cuenta principal es la master account (cuenta maestra)
- Beneficios de costes:
 - **Facturación consolidada** en todas las cuentas: método de pago único
 - Beneficios de precios por **uso agregado** (descuento por volumen para EC2, S3...)
 - **Agrupación de instancias EC2 reservadas** para un ahorro óptimo
- La API está disponible para **automatizar la creación de cuentas de AWS**
- **Restringe los privilegios de las cuentas mediante Políticas de Control de Servicios (SCP)**

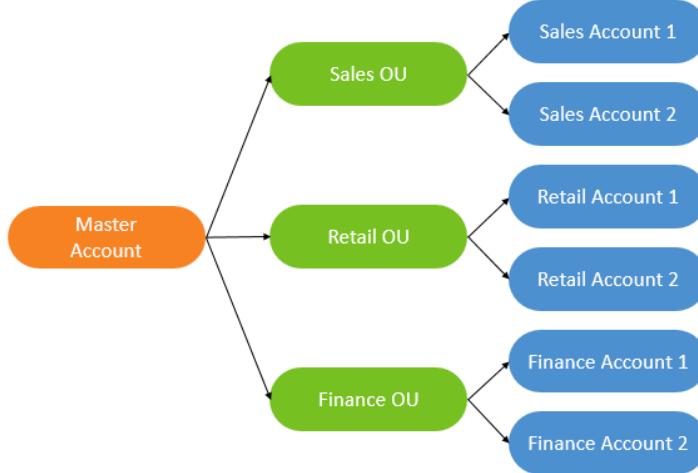


Estrategias multicuenta

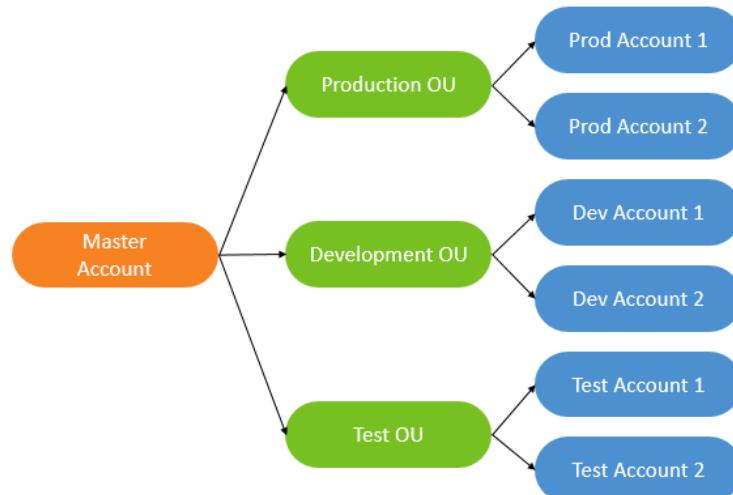
- Crear cuentas por **departamento**, por **centro de costes**, por **dev / test / prod**, en función de las **restricciones normativas** (usando SCP), para un **mejor aislamiento de los recursos** (ej.:VPC), para tener **límites de servicio separados por cuenta**, cuenta aislada para **logs**
- Cuenta múltiple vs. Cuenta única VPC múltiple
- Utilizar normas de etiquetado para la facturación
- Activa CloudTrail en todas las cuentas, envía los logs a la cuenta S3 central
- Enviar los logs de CloudWatch a la cuenta central de logs

Unidades Organizativas (UO) - Ejemplos

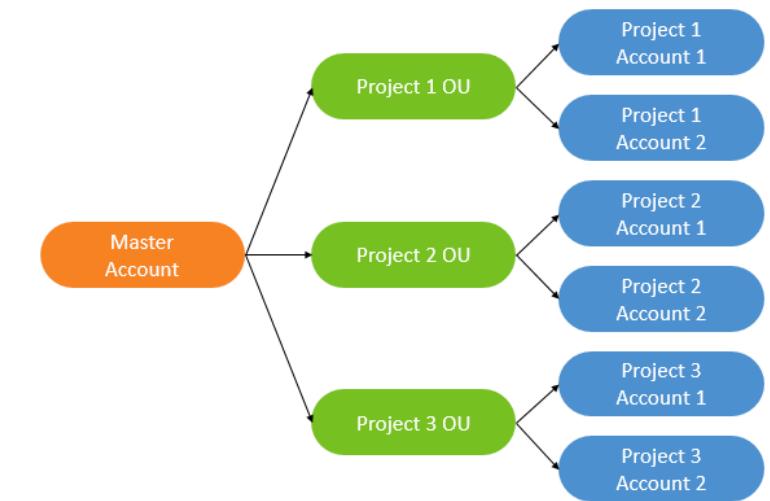
Unidad de negocio



Ciclo de vida medioambiental

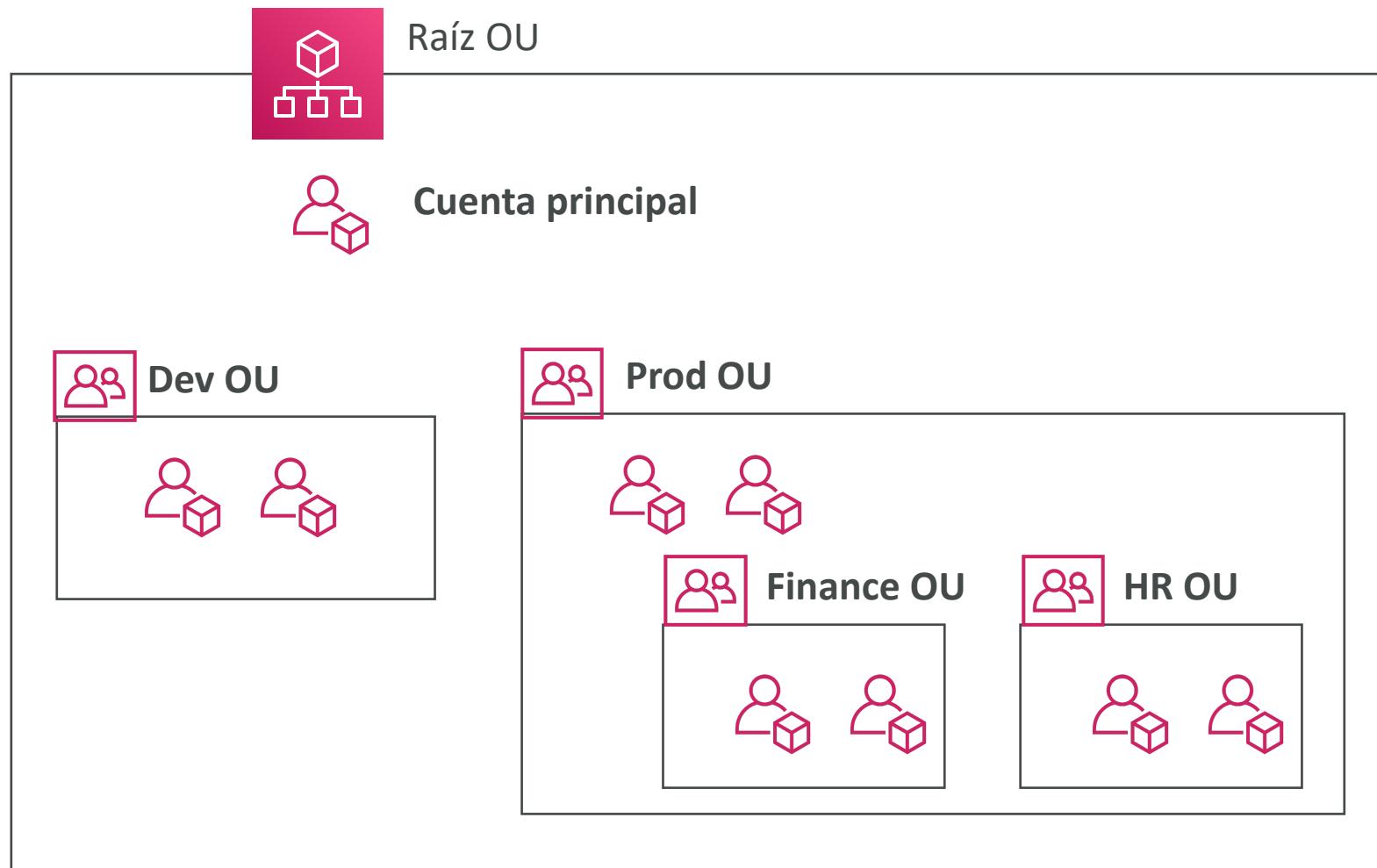


Basado en proyectos



<https://aws.amazon.com/answers/account-management/aws-multi-account-billing-strategy/>

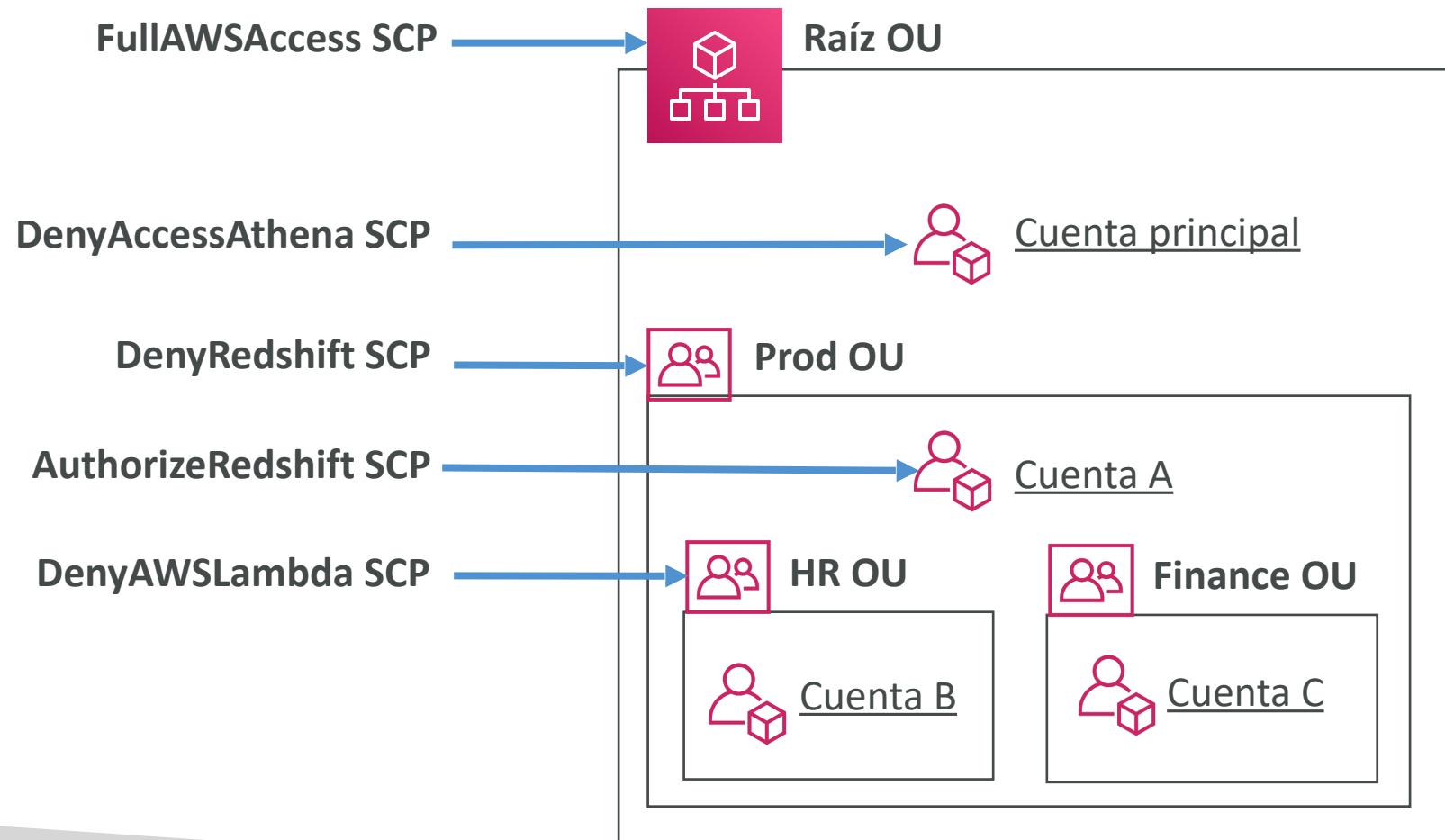
AWS Organization



Políticas de Control de Servicios (SCP)

- Lista blanca o negra de acciones IAM
- Se aplican a nivel de **OU** o de **Cuenta**
- No se aplica a la Cuenta Maestra
- El SCP se aplica a todos los **usuarios y roles** de la cuenta, incluido el usuario root
- El SCP no afecta a los roles vinculados al servicio
 - Los roles vinculados a servicios permiten que otros servicios de AWS se integren con las AWS Organizations y no pueden ser restringidos por SCP.
- El SCP debe tener un ALLOW explícito (no permite nada por defecto)
- Casos de uso:
 - Restringir el acceso a determinados servicios (por ejemplo: no se puede utilizar EMR)
 - Aplicar la normativa PCI deshabilitando explícitamente los servicios

Jerarquía SCP



- **Cuenta maestra**
 - Puede hacer cualquier cosa
 - (no se aplica el SCP)
- **Cuenta A**
 - Puede hacer cualquier cosa
 - EXCEPTO acceder a Redshift (denegación explícita desde Prod OU)
- **Cuenta B**
 - Puede hacer cualquier cosa
 - EXCEPTO acceder a Redshift (denegación explícita de la OU de Producción)
 - EXCEPTO acceder a Lambda (denegación explícita de la OU de Recursos Humanos)
- **Cuenta C**
 - Puede hacer cualquier cosa
 - EXCEPTO acceder a Redshift (denegación explícita de la OU de producción)

Ejemplos de SCP

Estrategias de lista negra y lista blanca

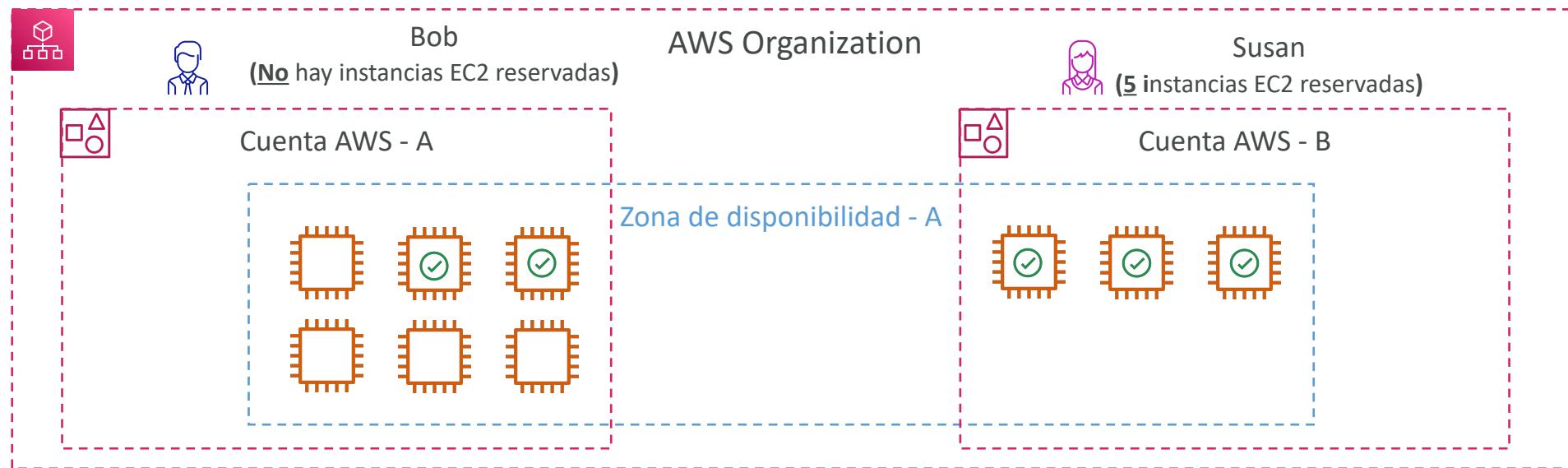
```
Version": "2012-10-17",
"Statement": [
    {
        "Sid": "AllowsAllActions",
        "Effect": "Allow",
        "Action": "*",
        "Resource": "*"
    },
    {
        "Sid": "DenyDynamoDB",
        "Effect": "Deny",
        "Action": "dynamodb:*",
        "Resource": "*"
    }
]
```

```
Version": "2012-10-17",
"Statement": [
    {
        "Effect": "Allow",
        "Action": [
            "ec2:*",
            "cloudwatch:*
```

Más ejemplos: https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_example-scps.html

AWS Organization – Facturación consolidada

- Cuando se activa, te proporciona:
 - **Uso combinado** - combina el uso en todas las cuentas de AWS en la Organización de AWS para **compartir los precios por volumen, las Instancias Reservadas y los descuentos de los Planes de Ahorro**
 - **Una factura** - obtener una factura para todas las cuentas de AWS en la Organización de AWS
- La cuenta de administración puede desactivar el uso compartido de los descuentos de las instancias reservadas para cualquier cuenta de la organización de AWS, incluida ella misma



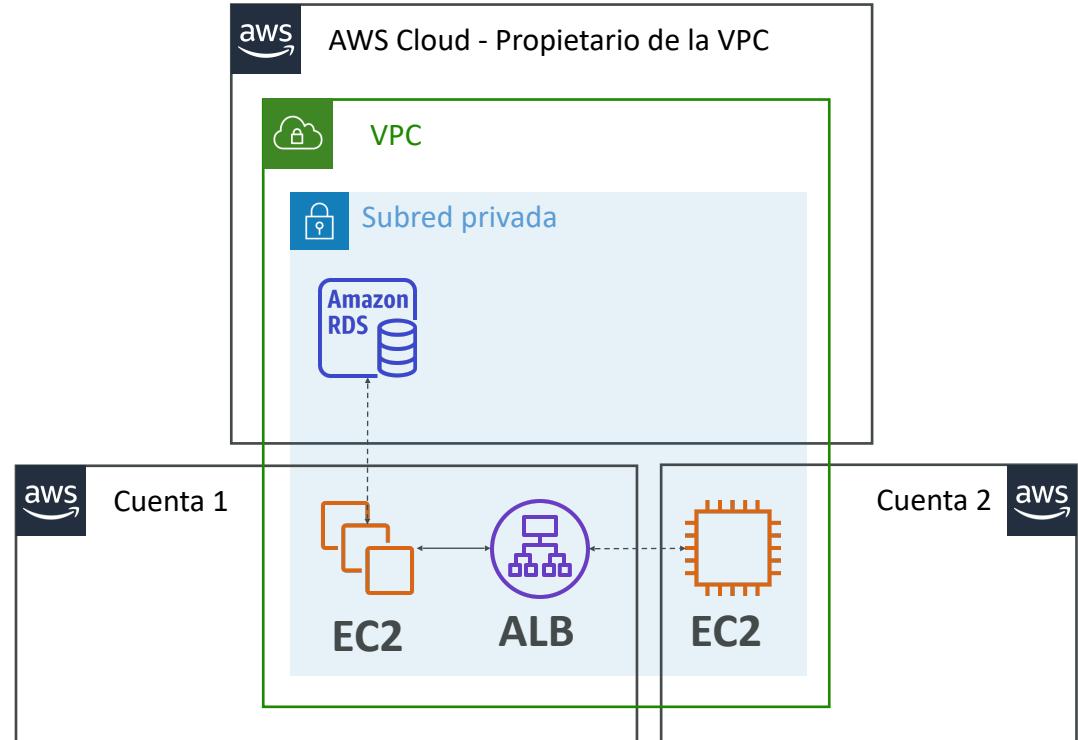
AWS Control Tower



- Una forma fácil de **configurar y gobernar un entorno AWS multicuenta seguro** y conforme a las mejores prácticas
- Ventajas:
 - Automatiza la configuración de tu entorno en unos pocos clics
 - Automatiza la gestión continua de las políticas
 - Detecta las infracciones de las políticas y corrígelas
 - Supervisa la normativa a través de un dashboards interactivo
- La AWS Control Tower se ejecuta sobre las Organizaciones de AWS:
 - Configura automáticamente las AWS Organizations para organizar las cuentas e implementar las SCP (Políticas de Control de Servicios)

AWS Resource Access Manager (AWS RAM)

- Comparte los recursos de AWS que poseas con otras cuentas de AWS
- Comparte con cualquier cuenta o dentro de tu organización
- ¡Evita la duplicación de recursos!
- Los recursos soportados incluyen Aurora, Subredes de VPC, Transit Gateway, Route 53, EC2 Hosts dedicados...



AWS Service Catalog



- Los usuarios que son nuevos en AWS tienen demasiadas opciones, y pueden crear stacks que no sean conformes / estén en línea con el resto de la organización
- Algunos usuarios sólo quieren un **portal rápido de autoservicio** para lanzar un conjunto de **productos autorizados** predefinidos **por los administradores**
- Incluye: máquinas virtuales, bases de datos, opciones de almacenamiento, etc.
- ¡Entra en AWS Service Catalog!

Diagrama AWS Service Catalog

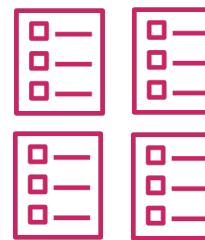
TAREAS ADMINISTRATIVAS

Producto



Plantillas de
CloudFormation

Portafolio



Colección de productos

Control



Permisos IAM para acceder
a portafolios

TAREAS DEL
USUARIO

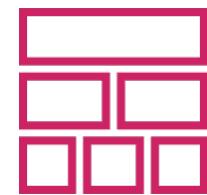
Lista de productos



Autorizado por IAM

Lanzamiento

Productos aprovisionados



Listo para usar
Correctamente configurado
Etiquetado correctamente

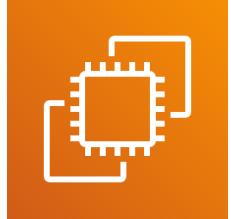
Modelos de precios en AWS

- AWS tiene 4 modelos de precios:
- **Paga por lo que usas:** paga por lo que usas, sigue siendo ágil, responde, cumple con las demandas de escala
- **Ahorra cuando reserves:** minimiza los riesgos, gestiona de forma predecible los presupuestos, cumple con los requisitos a largo plazo
 - Las reservas están disponibles para instancias reservadas de EC2, capacidad reservada de DynamoDB, nodos reservados de ElastiCache, instancias reservadas de RDS y nodos reservados de Redshift
- **Paga menos usando más:** descuentos por volumen
- **Paga menos al crecer AWS**

Servicios y niveles gratuitos en AWS

- IAM
 - VPC
 - Facturación consolidada
 - Elastic Beanstalk
 - CloudFormation
 - Auto Scaling Groups
 - Nivel gratis: <https://aws.amazon.com/free/>
 - Instancia EC2 t2.micro por un año
 - S3, EBS, ELB, AWS Data transfer
- 
- ⚠️ Sí pagas por los recursos creados**

Precios de computación - EC2



- Sólo se cobra por lo que usas
- Número de instancias
- Configuración de las instancias:
 - Capacidad física
 - Región
 - Sistema operativo y software
 - Tipo de instancia
 - Tamaño de la instancia
- Tiempo de funcionamiento del ELB y cantidad de datos procesados
- Monitorización detallada

Precios de computación - EC2

- **Instancias bajo demanda :**
 - Mínimo de 60s
 - Paga por segundo (Linux/Windows) o por hora (otros)
- **Instancias reservadas:**
 - Hasta un 75% de descuento en comparación con las instancias bajo demanda en la tarifa por hora
 - Compromiso de 1 o 3 años
 - Todo por adelantado, parcialmente por adelantado, sin adelantado
- **Instancias spot:**
 - Hasta un 90% de descuento en comparación con la tarifa horaria bajo demanda
 - Puja por la capacidad no utilizada
- **Host dedicado:**
 - Bajo demanda
 - Reserva para un compromiso de 1 o 3 años
- **Planes de ahorro** como alternativa para ahorrar en el uso sostenido

Precio de computación – Lambda y ECS

- Lambda:

- Pago por llamada
- Pago por duración



- ECS:

- Modelo de tipo de lanzamiento de EC2: No hay tarifas adicionales, pagas por los recursos de AWS almacenados y creados en tu aplicación



- Fargate:

- Modelo de tipo de lanzamiento Fargate: Pagas por los recursos de vCPU y memoria asignados a tus aplicaciones en tus contenedores



Precios de almacenamiento - S3



- **Clase de almacenamiento:** S3 Standard, S3 Infrequent Access, S3 One-Zone IA, S3 Intelligent Tiering, S3 Glacier and S3 Glacier Deep Archive
- Número y tamaño de los objetos: El precio puede ser escalonado (en función del volumen)
- Número y tipo de solicitudes
- Transferencia de datos FUERA de la región S3
- Aceleración de la transferencia en S3
- Transiciones del ciclo de vida
- Servicio similar: EFS (pago por uso, tiene reglas de acceso y ciclo de vida poco frecuentes)

Precios de almacenamiento - EBS



- Tipo de volumen (en función del rendimiento)
- Volumen de almacenamiento en GB por mes **provisionado**
- IOPS:
 - SSD de propósito general: Incluido
 - IOPS provisionadas SSD: Cantidad provisionada en IOPS
 - Magnético Número de peticiones
- Snapshots:
 - Coste de datos añadidos por GB al mes
- Transferencia de datos:
 - La transferencia de datos salientes está escalonada para descuentos por volumen
 - La entrada es gratis

Precios de las bases de datos - RDS



- Facturación por horas
- Características de la base de datos:
 - Motor
 - Tamaño
 - Clase de memoria
- Tipo de compra:
 - Bajo demanda
 - Instancias reservadas (1 o 3 años) con pago inicial requerido
- Almacenamiento de copias de seguridad: No hay cargo adicional por el almacenamiento de copias de seguridad hasta el 100% del almacenamiento total de tu base de datos para una región.

Precios de las bases de datos - RDS



- Almacenamiento adicional (por GB al mes)
- Número de peticiones de entrada y salida al mes
- Tipo de despliegue (el almacenamiento y la E/S son variables):
 - Una única AZ
 - Varias AZ
- Transferencia de datos:
 - La transferencia de datos salientes está escalonada por descuentos por volumen
 - La entrante es gratis

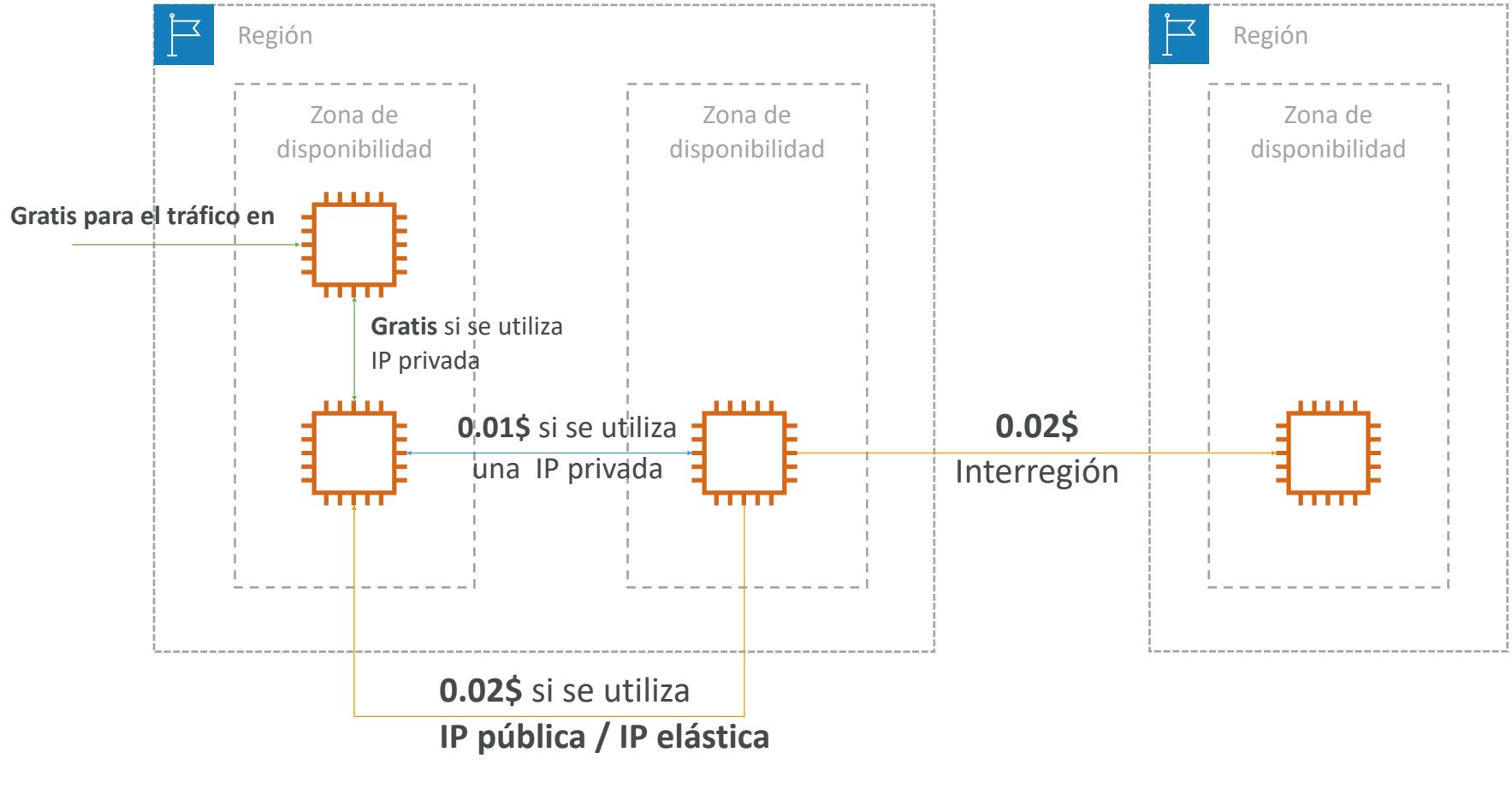


Entrega de contenidos – CloudFront

- Los precios son diferentes en las distintas regiones geográficas
- Agregado para cada ubicación de borde, luego se aplica a tu factura
- Transferencia de datos a domicilio (descuento por volumen)
- Número de peticiones HTTP/HTTPS

Per Month	United States & Canada	Europe & Israel	South Africa, Kenya, & Middle East	South America	Japan	Australia	Singapore, South Korea, Taiwan, Hong Kong, & Philippines	India
First 10TB	\$0.085	\$0.085	\$0.110	\$0.110	\$0.114	\$0.114	\$0.140	\$0.170
Next 40TB	\$0.080	\$0.080	\$0.105	\$0.105	\$0.089	\$0.098	\$0.135	\$0.130
Next 100TB	\$0.060	\$0.060	\$0.090	\$0.090	\$0.086	\$0.094	\$0.120	\$0.110

Costes de red en AWS por GB - Simplificado



- Utiliza la IP privada en lugar de la IP pública para obtener un buen ahorro y un mejor rendimiento de la red
- Utiliza la misma AZ para obtener el máximo ahorro (a costa de la alta disponibilidad)

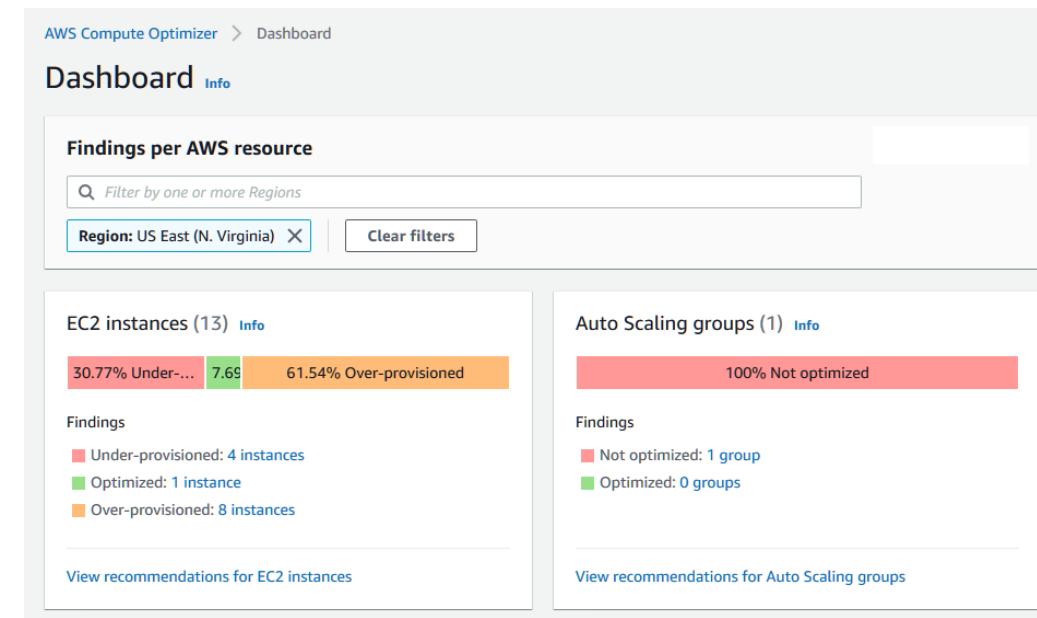


Planes de ahorro (Saving Plans)

- Comprométete a pagar una determinada cantidad de dólares por hora durante 1 o 3 años
- La forma más fácil de establecer compromisos a largo plazo en AWS
- **Plan de ahorro EC2**
 - Hasta un 72% de descuento en comparación con el plan bajo demanda
 - **Comprométete al uso de familias de instancias individuales en una región (por ejemplo, C5 o M5)**
 - Independientemente de la AZ, el tamaño (m5.xl a m5.4xl), el SO (Linux/Windows) o la tenencia
 - Todo por adelantado, parcialmente por adelantado, sin adelantado
- **Plan de ahorro de computación**
 - Hasta un 66% de descuento en comparación con el plan bajo demanda
 - Independientemente de la familia, la región, el tamaño, el sistema operativo, la tenencia y las opciones de computación
 - Opciones de computación: EC2, Fargate, Lambda
- **Plan de ahorro de Machine Learning:** SageMaker...
- Configuración desde la consola AWS Cost Explorer
- Calcula el precio en <https://aws.amazon.com/savingsplans/pricing/>

AWS Compute Optimizer

- **Reduce los costes y mejora el rendimiento**
recomendando los recursos de AWS óptimos para tus cargas de trabajo
- Te ayuda a elegir las configuraciones óptimas y a dimensionar correctamente tus cargas de trabajo (sobre/subprovisionamiento)
- Utiliza Machine Learning para analizar las **configuraciones de tus recursos** y sus **métricas de utilización CloudWatch**
- Recursos soportados
 - Instancias EC2
 - Grupos de autoescalamiento de EC2
 - Volúmenes EBS
 - Funciones Lambda
- Reduce tus costes hasta un 25%
- Las recomendaciones se pueden exportar a S3





Herramientas de facturación y cálculo de costes

- **Estimación de costes en el Cloud:**
 - Calculadora de precios
- **Seguimiento de los costes en el Cloud:**
 - Dashboards de facturación
 - Etiquetas de asignación de costes
 - Cost and Usage Reports (AWS CUR)
 - Cost Explorer
- **Seguimiento de los planes de costes:**
 - Alarmas de facturación
 - Presupuestos

AWS Pricing Calculator

- Disponible en <https://calculator.aws/>
- Calcula el coste de la arquitectura de tu solución

The screenshot shows the AWS Pricing Calculator interface. At the top, it displays the total estimate: First 12 months total **62,191.68 USD**, Total upfront **0.00 USD**, and Total monthly **5,182.64 USD**. Below this, under the heading "Services (2)", there are two service items:

- Amazon Aurora MySQL-Compatible**
Region: US East (Ohio)
Monthly: 5,110.80 USD
- Aurora MySQL-Compatible**
Change records per statement (0.38), (1 instances) db.r5.12xlarge Memory optimized OnDemand, Storage amount (300 GB)
Monthly: 5,110.80 USD

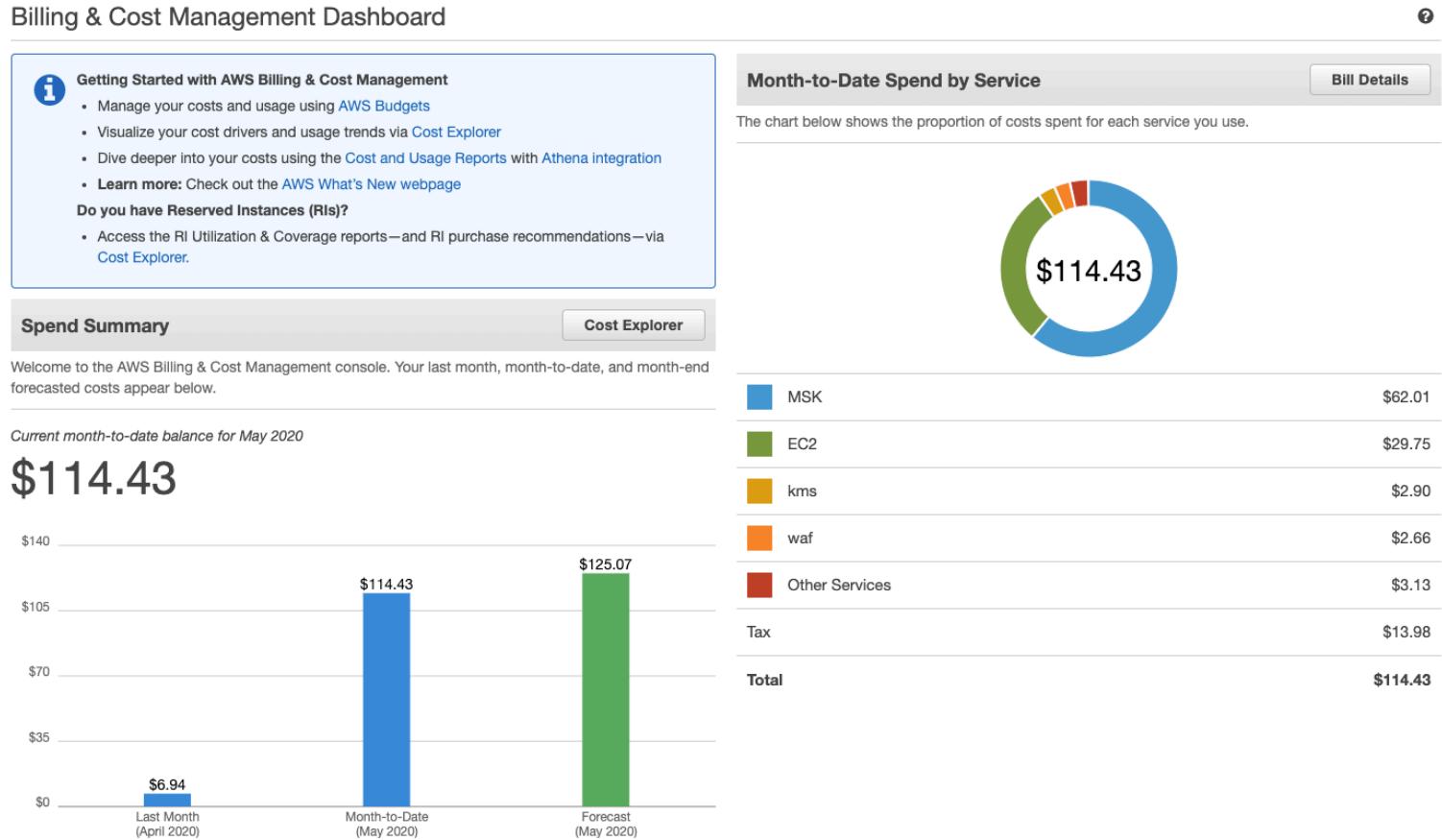
Below these, under the heading "Amazon EC2", there is one service item:

- Amazon EC2**
Region: US East (Ohio)
Monthly: 71.84 USD

At the bottom, there is a section titled "Quick estimate" with the following details:

Operating system (Linux), Quantity (1), Storage for each EC2 instance (General Purpose SSD (gp2)), Storage amount (30 GB), Instance type (t3a.xlarge)

Dashboards de facturación de AWS



Dashboard de la capa gratuita de AWS

All Free Tier services by usage

Service	Free Tier usage limit	Current usage	Forecasted usage	Month-to-date actual usage	Month-end forecasted usage
AWS Lambda	1,000,000 free requests per month for AWS Lambda	585,089 Requests	697,606 Requests	<div style="width: 58.51%;">58.51%</div>	<div style="width: 69.76%;">69.76%</div>
Amazon Simple Notification Service	1,000,000 Requests for Amazon Simple Notification Service (APS2)	575,640 Requests	686,340 Requests	<div style="width: 57.56%;">57.56%</div>	<div style="width: 68.63%;">68.63%</div>
AWS Lambda	400,000 seconds of compute time per month for AWS Lambda	61,973 seconds	73,891 seconds	<div style="width: 15.49%;">15.49%</div>	<div style="width: 18.47%;">18.47%</div>
AWS Key Management Service	20,000 free requests per month for AWS Key Management Service	1,533 Requests	1,828 Requests	<div style="width: 7.66%;">7.66%</div>	<div style="width: 9.14%;">9.14%</div>
AmazonCloudWatch	5 GB of Log Data Ingestion for Amazon Cloudwatch	0 GB	0 GB	<div style="width: 5.81%;">5.81%</div>	<div style="width: 6.92%;">6.92%</div>
AmazonCloudWatch	5 GB of Log Data Archive for Amazon Cloudwatch	0 GB-Mo	0 GB-Mo	<div style="width: 4.78%;">4.78%</div>	<div style="width: 5.70%;">5.70%</div>
Amazon Simple Notification Service	1,000 email notifications for Amazon Simple Notification Service (USE1)	25 Notifications	30 Notifications	<div style="width: 2.50%;">2.50%</div>	<div style="width: 2.98%;">2.98%</div>
Amazon Simple Queue Service	1,000,000 Requests of Amazon Simple Queue Service	11,323 Requests	13,501 Requests	<div style="width: 1.13%;">1.13%</div>	<div style="width: 1.35%;">1.35%</div>
CodeBuild	100 build minutes per month of build.general1.small compute type usage for AWS CodeBuild	1 minutes	1 minutes	<div style="width: 1.00%;">1.00%</div>	<div style="width: 1.19%;">1.19%</div>
AWS Step Functions	4,000 state transitions per month for AWS Step Functions	15 StateTransitions	18 StateTransitions	<div style="width: 0.38%;">0.38%</div>	<div style="width: 0.45%;">0.45%</div>

Etiquetas (tags) de asignación de costes

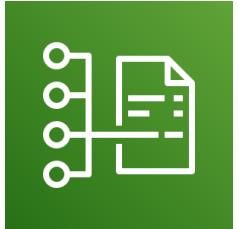
- Utiliza las **etiquetas de asignación** de costes para hacer un seguimiento detallado de tus costes de AWS
- **Etiquetas generadas por AWS**
 - Se aplican automáticamente al recurso que creas
 - Comienza con el prefijo **aws:** (por ejemplo, **aws: createdBy**)
- **Etiquetas definidas por el usuario**
 - Definidas por el usuario
 - Comienza con el prefijo **user:**

Total Cost	user:Owner	user:Stack	user:Cost Center	user:Application
0.95	DbAdmin	Test	80432	Widget2
0.01	DbAdmin	Test	80432	Widget2
3.84	DbAdmin	Prod	80432	Widget2
6.00	DbAdmin	Test	78925	Widget1
234.63	SysEng	Prod	78925	Widget1
0.73	DbAdmin	Test	78925	Widget1
0.00	DbAdmin	Prod	80432	Portal
2.47	DbAdmin	Prod	78925	Portal

Etiquetado y grupos de recursos

- Los **Tags** o **etiquetas** se utilizan para organizar los recursos:
 - EC2: instancias, imágenes, load balancers, grupos de seguridad...
 - RDS, recursos VPC, Route 53, usuarios IAM, etc.
 - Los recursos creados por CloudFormation se etiquetan todos de la misma manera
- Nomenclatura libre, las etiquetas más comunes son: Nombre, Entorno, Equipo...
- Las etiquetas pueden utilizarse para crear **grupos de recursos**
 - Crear, mantener y ver una colección de recursos que comparten etiquetas comunes
 - Gestionar estas etiquetas utilizando el Tag Editor (editor de etiquetas)

Cost and Usage Reports (AWS CUR)



- Profundiza en tus costes y uso de AWS
- El Informe de Costes y Uso de AWS contiene el **conjunto más completo de datos de costes y uso de AWS disponible**, incluyendo metadatos adicionales sobre los servicios de AWS, los precios y las reservas (**por ejemplo, las instancias reservadas (RIs) de Amazon EC2**).
- El AWS Cost & Usage Report (AWS CUR) enumera el uso de AWS para cada categoría de servicio utilizada por una cuenta y sus usuarios de IAM en partidas horarias o diarias, así como cualquier etiqueta que hayas activado con fines de asignación de costes.
- Puede integrarse con Athena, Redshift o QuickSight

Cost and Usage Reports (AWS CUR)

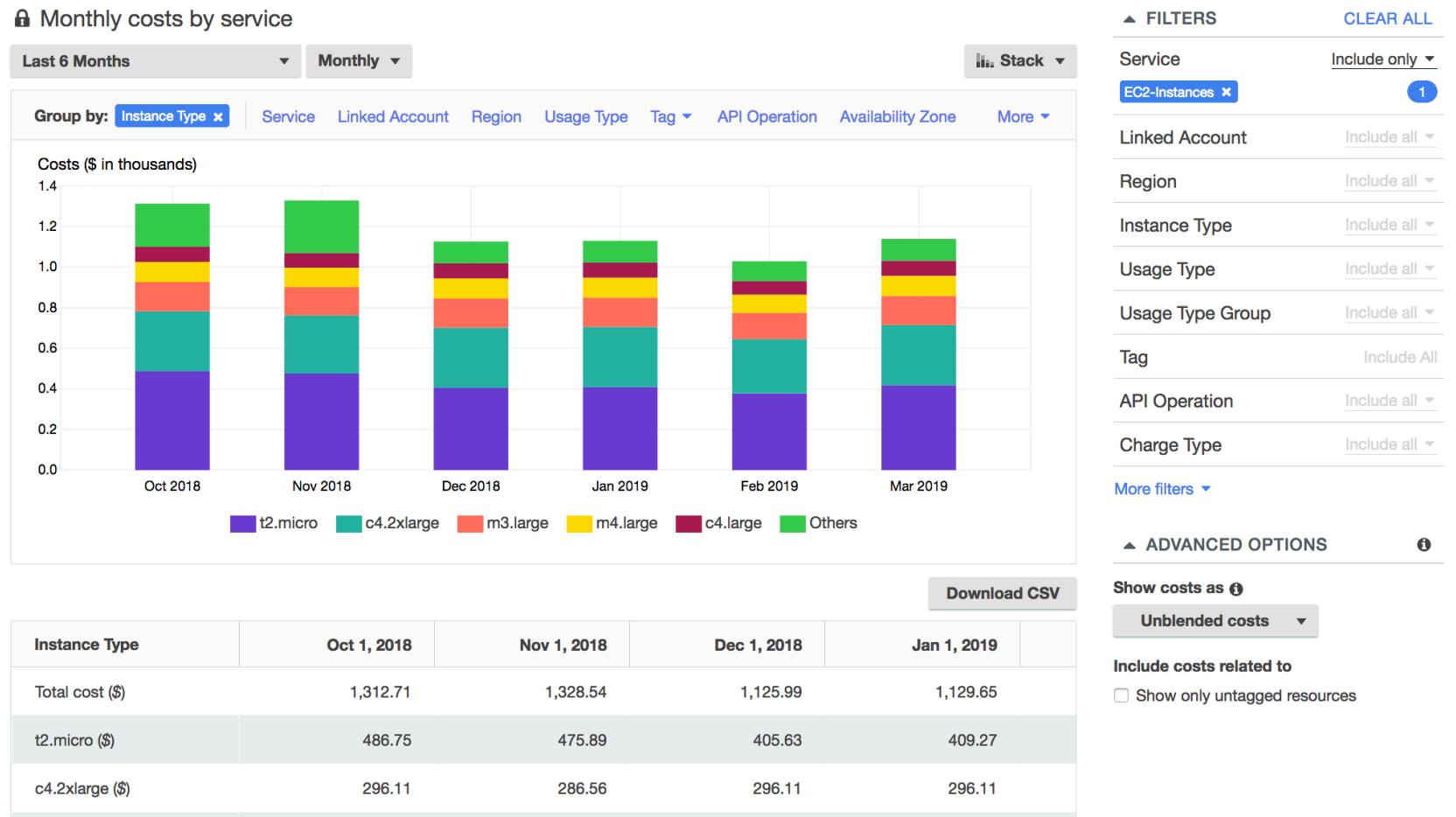
M	N	O	P	R	S	T
lineItem/ProductCode	lineItem/UsageType	lineItem/Operation	lineItem/AvailabilityZone	lineItem/UsageAmount	lineItem/CurrencyCode	lineItem/LineItemDescription
1 AmazonEC2	CW:AlarmMonitorUsage	Unknown		0.00134409	USD	\$0.00 per alarm-month - first 10 alarms
2 AmazonS3	Requests-Tier1	ListAllMyBuckets		2	USD	\$0.00 per request - PUT, COPY, POST, or LIST requests under the monthly global free tier
3 AmazonEC2	CW:AlarmMonitorUsage	Unknown		0.00134409	USD	\$0.00 per alarm-month - first 10 alarms
4 AmazonEC2	APS2-EBS:VolumeUsage.gp2	CreateVolume-Gp2		0.01344086	USD	\$0.00 per GB-month of General Purpose (SSD) provisioned storage under monthly free tier
5 AmazonEC2	APS2-EBS:VolumeUsage.gp2	CreateVolume-Gp2		0.01344086	USD	\$0.00 per GB-month of General Purpose (SSD) provisioned storage under monthly free tier
6 AmazonEC2	USW2-BoxUsage:t2.micro	RunInstances:0002	us-west-2a	1	USD	\$0.00 per Windows t2.micro instance-hour (or partial hour) under monthly free tier
7 AmazonEC2	USW2-USE1-AWS-Out-Bytes	PublicIP-Out		0.00000174	USD	\$0.000 per GB - data transfer out under the monthly global free tier
8 AmazonEC2	USW2-USE1-AWS-In-Bytes	PublicIP-In		0.00000138	USD	\$0.00 per GB - US West (Oregon) data transfer from US East (Northern Virginia)
9 AmazonEC2	USW2-USW1-AWS-In-Bytes	PublicIP-In		0.00000149	USD	\$0.00 per GB - US West (Oregon) data transfer from US West (Northern California)
10 AmazonS3	Requests-Tier1	ListAllMyBuckets		2	USD	\$0.00 per request - PUT, COPY, POST, or LIST requests under the monthly global free tier
11 AmazonEC2	USW2-DataTransfer-Out-Bytes	RunInstances		0.00038144	USD	\$0.00 per GB - data transfer out under the monthly global free tier
12 AmazonEC2	USW2-USE1-AWS-Out-Bytes	PublicIP-Out		0.00000174	USD	\$0.000 per GB - data transfer out under the monthly global free tier
13 AmazonEC2	USW2-DataTransfer-In-Bytes	RunInstances		0.00030951	USD	\$0.00 per GB - data transfer in per month
14 AmazonEC2	USW2-BoxUsage:t2.micro	RunInstances:0002	us-west-2a	1	USD	\$0.00 per Windows t2.micro instance-hour (or partial hour) under monthly free tier
15 AmazonEC2	USW2-USW1-AWS-Out-Bytes	PublicIP-Out		0.00000349	USD	\$0.000 per GB - data transfer out under the monthly global free tier
16 AmazonEC2	USW2-USW1-AWS-In-Bytes	PublicIP-In		0.00000276	USD	\$0.00 per GB - US West (Oregon) data transfer from US West (Northern California)
17 AmazonEC2	APS2-EBS:VolumeUsage.gp2	CreateVolume-Gp2		0.01344086	USD	\$0.00 per GB-month of General Purpose (SSD) provisioned storage under monthly free tier
18 AmazonEC2	CW:AlarmMonitorUsage	Unknown		0.00134409	USD	\$0.00 per alarm-month - first 10 alarms
19 AmazonEC2	USW2-BoxUsage:t2.micro	RunInstances:0002	us-west-2a	1	USD	\$0.00 per Windows t2.micro instance-hour (or partial hour) under monthly free tier
20 AmazonEC2	USW2-DataTransfer-Regional-Bytes	PublicIP-Out		0.00000349	USD	\$0.000 per GB - regional data transfer under the monthly global free tier
21 AmazonEC2	USW2-DataTransfer-In-Bytes	RunInstances		0.00032071	USD	\$0.000 per GB - data transfer in per month
22 AmazonEC2	USW2-DataTransfer-Regional-Bytes	PublicIP-In		0.00000302	USD	\$0.000 per GB - regional data transfer under the monthly global free tier
23 AmazonEC2	USW2-USE1-AWS-Out-Bytes	PublicIP-Out		0.00000174	USD	\$0.000 per GB - data transfer out under the monthly global free tier
24 AmazonEC2	USW2-DataTransfer-Out-Bytes	RunInstances		0.00045736	USD	\$0.000 per GB - data transfer out under the monthly global free tier
25 AmazonEC2	USW2-DataTransfer-In-Bytes	RunInstances		0.00036737	USD	\$0.000 per GB - data transfer in per month
26 AmazonEC2	USW2-APN2-AWS-In-Bytes	PublicIP-In		0.00000005	USD	\$0.00 per GB - US West (Oregon) data transfer from Asia Pacific (Seoul)
27 AmazonEC2	USW2-APN2-AWS-Out-Bytes	PublicIP-Out		0.00000018	USD	\$0.000 per GB - data transfer out under the monthly global free tier
28 AmazonEC2	USW2-USE1-AWS-In-Bytes	PublicIP-In		0.00000153	USD	\$0.00 per GB - US West (Oregon) data transfer from US East (Northern Virginia)
29 AmazonEC2	USW2-DataTransfer-Out-Bytes	RunInstances		0.00039945	USD	\$0.000 per GB - data transfer out under the monthly global free tier
30 AmazonEC2	CW:AlarmMonitorUsage	Unknown		0.00134409	USD	\$0.00 per alarm-month - first 10 alarms

Cost Explorer

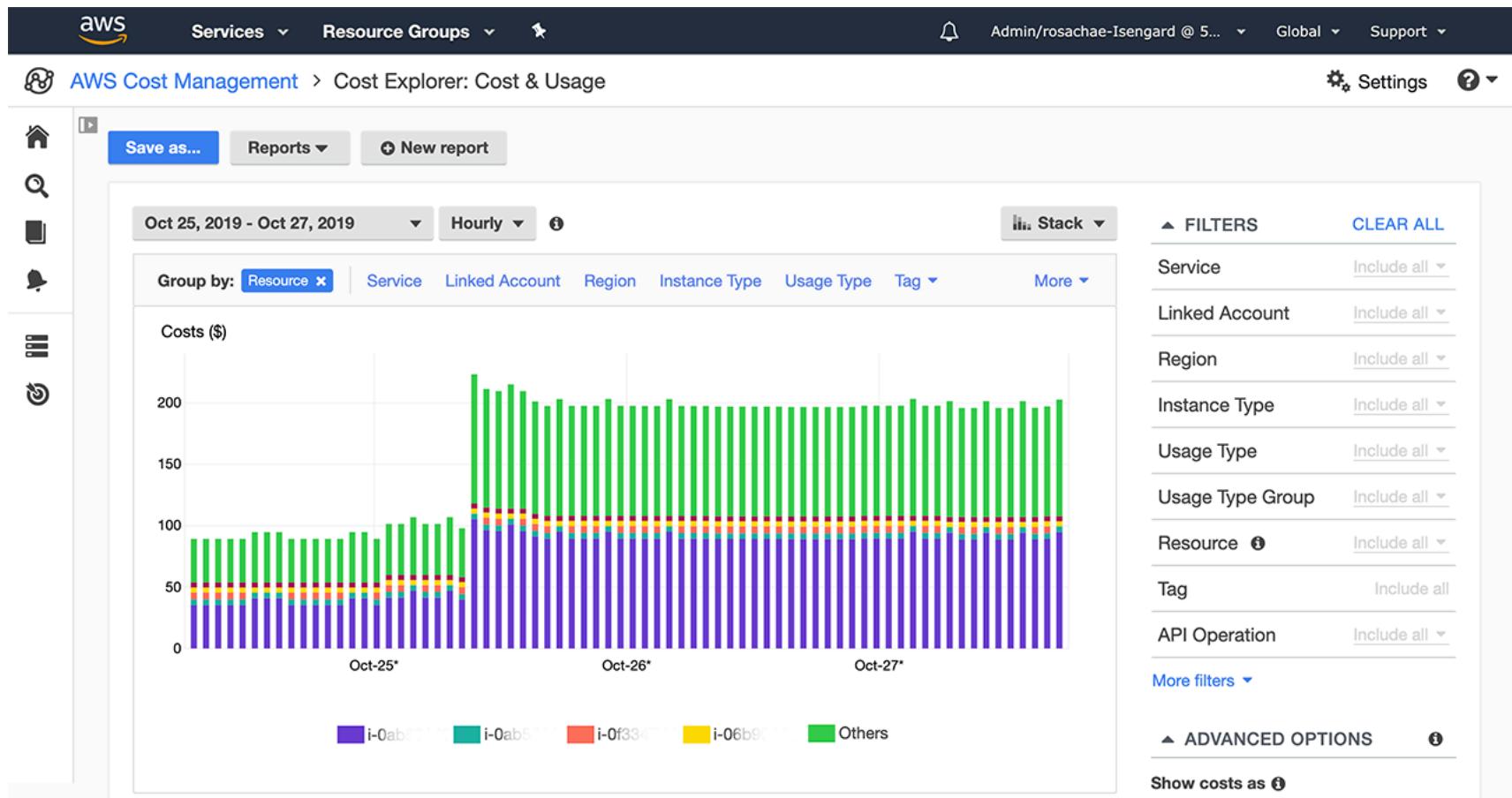


- Visualiza, entiende y gestiona tus costes y uso de AWS a lo largo del tiempo
- Crea informes personalizados que analicen los datos de costes y uso.
- Analiza tus datos a alto nivel: costes totales y uso en todas las cuentas
- O con granularidad mensual, por horas, a nivel de recursos
- Elige un **plan de ahorro** óptimo (para reducir los precios de tu factura)
- **Prevé el uso hasta 12 meses basándote en el uso anterior**

Cost Explorer – Coste mensual por servicio de AWS



Cost Explorer– Nivel de horas y recursos



Cost Explorer - Plan de ahorro

Alternativa a las instancias reservadas

Recommendation options

Savings Plans type <input checked="" type="radio"/> Compute <input type="radio"/> EC2 Instance	Savings Plans term <input type="radio"/> 1-year <input checked="" type="radio"/> 3-year	Payment option <input checked="" type="radio"/> All upfront <input type="radio"/> Partial upfront <input type="radio"/> No upfront	Based on the past <input type="radio"/> 7 days <input type="radio"/> 30 days <input checked="" type="radio"/> 60 days
--	---	---	--

Recommendation: Purchase a Compute Savings Plan at a commitment of \$2.40/hour

You could save an estimated **\$1,173** monthly by purchasing the recommended Compute Savings Plan.

Based on your past **60 days** of usage, we recommend purchasing a Savings Plan with a commitment of **\$2.40/hour** for a **3-year term**. With this commitment, we project that you could save an average of **\$1.61/hour** - representing a **40%** savings compared to On-Demand. To account for variable usage patterns, this recommendation maximizes your savings by leaving an average **\$0.04/hour** of On-Demand spend.

Before recommended purchase	After recommended purchase (based on your past 60 days of usage)
Monthly On-Demand spend <small> ⓘ</small> \$2,955 (\$4.05/hour) Based on your On-Demand spend over the past 60 days	Estimated monthly spend <small> ⓘ</small> \$1,782 (\$2.44/hour) Your recommended \$2.40/hour Savings Plans commitment + an average \$0.04/hour of On-Demand spend Estimated monthly savings <small> ⓘ</small> \$1,173 (\$1.61/hour) 40% monthly savings over On-Demand \$2,955 - \$1,782 = \$1,173

This recommendation examines your usage over the past 60 days (including your existing Savings Plans and EC2 Reserved Instances) and calculates what your costs would have been had you purchased the recommended Savings Plans. See applicable rates for Savings Plans [here](#). To generate this recommendation, AWS simulates your bill for different commitment amounts and recommends the commitment amount that provides the greatest estimated savings. [Learn more](#)

Recommended Compute Savings Plans

x	Term	Payment option	Recommended commitment	Estimated hourly savings
<input checked="" type="checkbox"/>	3-year	All upfront	\$2.40/hour	\$1.61 (40%)

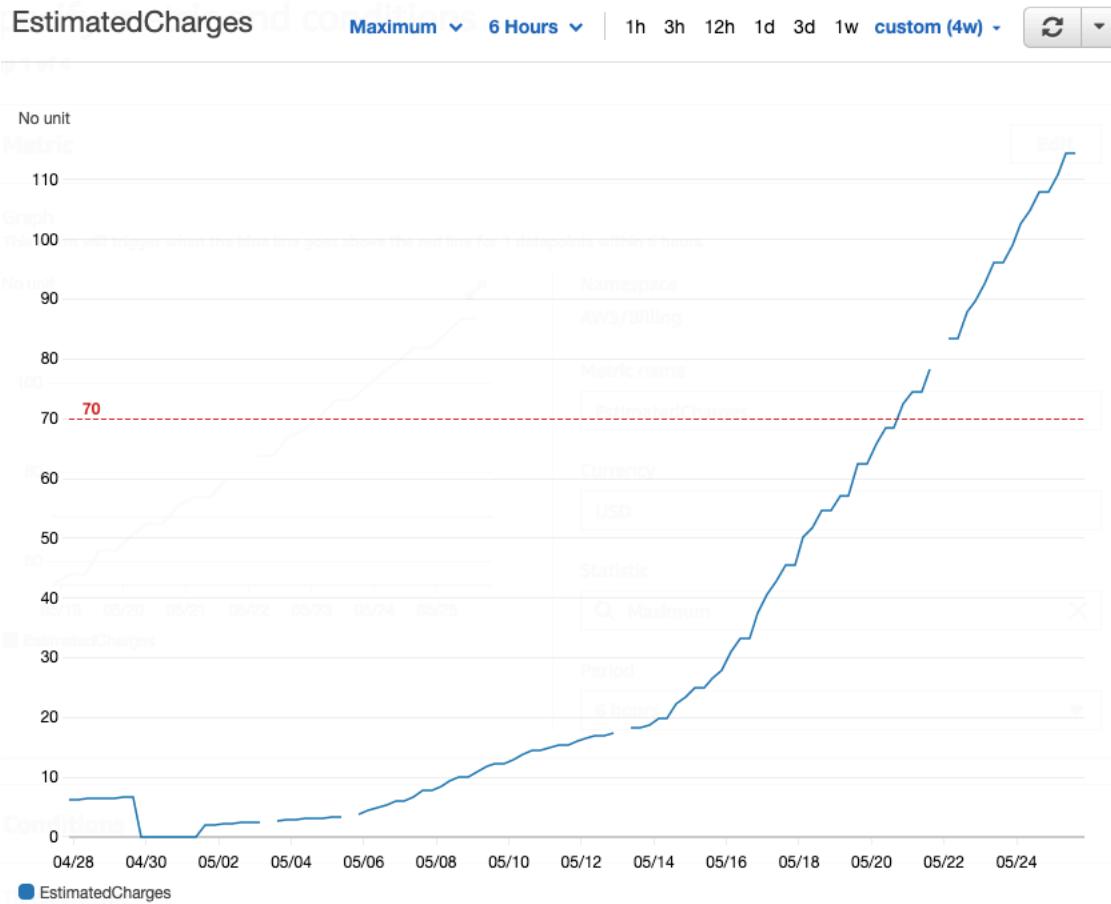
*Average hourly spend and minimum hourly spend based on your current on-demand spend for the given instance family.

Cost Explorer – Previsión de uso



Alarmas de facturación en CloudWatch

- La métrica de los datos de facturación se almacena en CloudWatch us-east-1
- Los datos de facturación son para los costes **globales** de AWS en todo el mundo
- Es para el coste real, no para los costes proyectados
- Pretende ser una simple alarma (no tan potente como AWS Budgets)



AWS Budgets



- Crea un presupuesto y **envía alarmas cuando los costes superen el presupuesto**
- 4 tipos de presupuestos: Uso, Coste, Reserva, Planes de ahorro
- Para las instancias reservadas (RI)
 - Haz un seguimiento de la utilización
 - Soporta EC2, ElastiCache, RDS, Redshift
- Hasta 5 notificaciones SNS por presupuesto
- Puedes filtrar por: servicio, cuenta vinculada, etiqueta, opción de compra, tipo de instancia, región, zona de disponibilidad, operación API, etc.
- Las mismas opciones que el AWS Cost Explorer
- 2 presupuestos son gratuitos, luego 0,02\$/día/presupuesto

AWS Cost Anomaly Detection

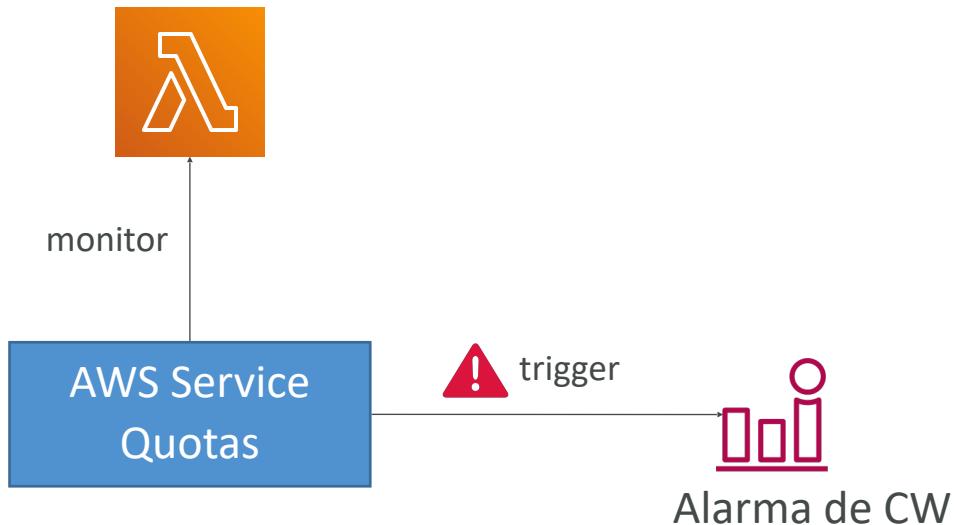
- **Monitorización continua de tus costes y uso mediante ML para detectar gastos inusuales**
- Aprende tus patrones de gasto únicos e históricos para detectar picos de costes puntuales y/o aumentos continuos de costes (no necesitas definir umbrales)
- Monitoriza servicios de AWS, cuentas asociadas, etiquetas de asignación de costes o categorías de costes
- Te envía el informe de detección de anomalías con el análisis de la causa raíz
- Recibe notificaciones con alertas individuales o un resumen diario/semanal (mediante SNS)



AWS Service Quotas

- Avisarte cuando estés cerca de un umbral de valor de cuota de servicio
- Crear alarmas CloudWatch en la consola cuotas de servicio
- Ejemplo: Ejecuciones concurrentes de Lambda
- Solicita un aumento de cuota a AWS Service Quotas o apaga los recursos antes de que se alcance el límite

Cuotas de AWS Lambda



Create a CloudWatch alarm: Concurrent executions X

Description
The maximum number of events that functions can process simultaneously in the current Region.

Alarm threshold
This alarm will notify you based on the threshold you choose.

Alarm name

Required. Alarm names must be unique within an AWS account.

Region
US East (N. Virginia) us-east-1

Pricing
Using CloudWatch can incur costs. [CloudWatch pricing](#)

[Cancel](#) [Create](#)



Trusted Advisor

- Sin necesidad de instalar nada - evaluación de alto nivel de la cuenta de AWS
- Analiza tus cuentas de AWS y proporciona recomendaciones en 5 categorías
 - **Optimización de costes**
 - **Rendimiento**
 - **Seguridad**
 - **Tolerancia a los fallos**
 - **Límites del servicio**

Checks

- ▶ ✓ **Amazon EBS Public Snapshots**

Checks the permission settings for your Amazon Elastic Block Store snapshots. 0 EBS snapshots are marked as public.
- ▶ ✓ **Amazon RDS Public Snapshots**

Checks the permission settings for your Amazon Relational Database Service snapshots. 0 RDS snapshots are marked as public.
- ▶ ✓ **IAM Use**

This check is intended to discourage the use of root access keys. At least one IAM user has been created for this account.

Trusted Advisor – Planes de soporte

7 CORE CHECKS (7 CONTROLES BÁSICOS)

Plan de soporte: Basic y Developer

- Permisos de buckets S3
- Grupos de seguridad – Puertos específicos sin restricciones
- Uso de IAM (un usuario IAM como mínimo)
- MFA en la cuenta root
- Snapshots de EBS públicos
- Snapshots públicos de RDS
- Service Quotas

FULL CHECKS (CONTROLES COMPLETOS)

Plan de soporte: Business y Enterprise

- Comprobaciones completas disponibles en las 5 categorías
- Posibilidad de establecer alarmas de CloudWatch cuando se alcanzan los límites
- **Acceso programado mediante la AWS Support API**



Precios de los planes de soporte de AWS

El plan de soporte Basic está incluido

Developer	Business	Enterprise On-Ramp	Enterprise
Lo que sea mayor entre 29,00 USD o El 3 % de los cargos mensuales de AWS	Lo que sea mayor entre 100,00 USD o El 10 % de los cargos mensuales de AWS para los primeros 0 USD hasta 10 000 USD El 7 % de los cargos mensuales de AWS desde 10 000 USD hasta 80 000 USD El 5 % de los cargos mensuales de AWS desde 80 000 USD hasta 250 000 USD El 3 % de los cargos mensuales de AWS superiores a 250 000 USD	Lo que sea mayor entre 5500,00 USD o El 10 % de los cargos mensuales de AWS	Lo que sea mayor entre 15 000,00 USD o El 10 % de los cargos mensuales de AWS para los primeros 0 USD hasta 150 000 USD El 7 % de los cargos mensuales de AWS desde 150 000 USD hasta 500 000 USD El 5 % de los cargos mensuales de AWS desde 500 000 USD hasta 1 000 000 USD El 3 % de los cargos mensuales de AWS superiores a 1 000 000 USD

Planes de soporte de AWS - Basic

- **Servicio de atención al cliente y comunidades** - Acceso 24x7 al servicio de atención al cliente, documentación, libros blancos y foros de soporte.
- **AWS Trusted Advisor** - Acceso a las 7 comprobaciones principales de Trusted Advisor y orientación para aprovisionar tus recursos siguiendo las mejores prácticas para aumentar el rendimiento y mejorar la seguridad.
- **AWS Personal Health Dashboard** - Una visión personalizada de la salud de los servicios de AWS, y alertas cuando tus recursos se ven afectados.

Planes de soporte de AWS - Developer

- Todo el plan de soporte basic+
- **Acceso por correo electrónico en horario laboral** a los asociados de soporte de Cloud
- Casos ilimitados / 1 contacto principal
- Gravedad de los casos / tiempos de respuesta:
 - Orientación general: < 24 horas laborables
 - Sistema deteriorado: < 12 horas laborables

Planes de soporte de AWS - Business (24/7)

- Destinado a ser utilizado si tienes cargas de **trabajo de producción**
- **Trusted Advisor** - Conjunto completo de comprobaciones + acceso a la API
- **Acceso telefónico, por correo electrónico y por chat 24x7** a los ingenieros de soporte de Cloud
- Casos ilimitados / contactos ilimitados
- Acceso a la Gestión de Eventos de Infraestructura **por una tarifa adicional.**
- Gravedad de los casos / tiempos de respuesta:
 - Orientación general: < 24 horas laborables
 - Sistema deteriorado: < 12 horas laborables
 - **Sistema de producción deteriorado: < 4 horas**
 - **Sistema de producción averiado: < 1 hora**

Planes de soporte de AWS - Enterprise On-Ramp

- Destinado a ser utilizado si tienes **cargas de trabajo de producción o críticas para el negocio**
- Todo el Plan de Soporte Business +
- Acceso a un grupo de **Gestores Técnicos de Cuentas (TAM)**
- **Equipo de soporte de atención** (para la facturación y las mejores prácticas de la cuenta)
- **Gestión de eventos de infraestructura, revisiones de operaciones y bien diseñadas**
- Gravedad de los casos / tiempos de respuesta:
 - ...
 - Sistema de producción deteriorado: < 4 horas
 - Sistema de producción averiado: < 1 hora
 - **Sistema crítico de negocio caído: < 30 minutos**

Planes de soporte de AWS - Enterprise

- Destinado a ser utilizado si tienes **cargas de trabajo de misión crítica**
- Todo el Plan de Soporte Business +
- Acceso a un **Gestor Técnico de Cuentas (TAM)** designado
- **Equipo de soporte de atención** (para la facturación y las mejores prácticas de la cuenta)
- **Gestión de eventos de la infraestructura, revisiones de operaciones y de la arquitectura**
- Gravedad de los casos / tiempos de respuesta:
 - ...
 - Sistema de producción deteriorado: < 4 horas
 - Sistema de producción averiado: < 1 hora
 - **Sistema crítico de negocio caído:** < 15 minutos

Resumen - Mejores prácticas para las cuentas

- Operar múltiples cuentas utilizando **organizaciones**
- Utiliza **SCP** (políticas de control de servicios) para restringir el poder de las cuentas
- Configura fácilmente varias cuentas con las mejores prácticas con **AWS Control Tower**
- **Utiliza etiquetas y etiquetas de asignación** de costes para facilitar la gestión y la facturación
- **Pautas de IAM**: MFA, mínimo privilegio, política de contraseñas, rotación de contraseñas
- **Config** para registrar todas las configuraciones de recursos y la normativa a lo largo del tiempo
- **CloudFormation** para desplegar pilas entre cuentas y regiones
- **Trusted Advisor** para obtener información, plan de soporte adaptado a tus necesidades
- Envía logs de servicio y de acceso a **S3 o a CloudWatch Logs**
- **CloudTrail** para registrar las llamadas a la API realizadas en tu cuenta
- **Si tu cuenta se ve comprometida**: cambia la contraseña root, borra y rota todas las contraseñas/claves, contacta con el soporte de AWS
- Permitir a los usuarios crear stacks predefinidos definidos por los administradores mediante **AWS Service Catalog**

Resumen - Herramientas de facturación y cálculo de costes

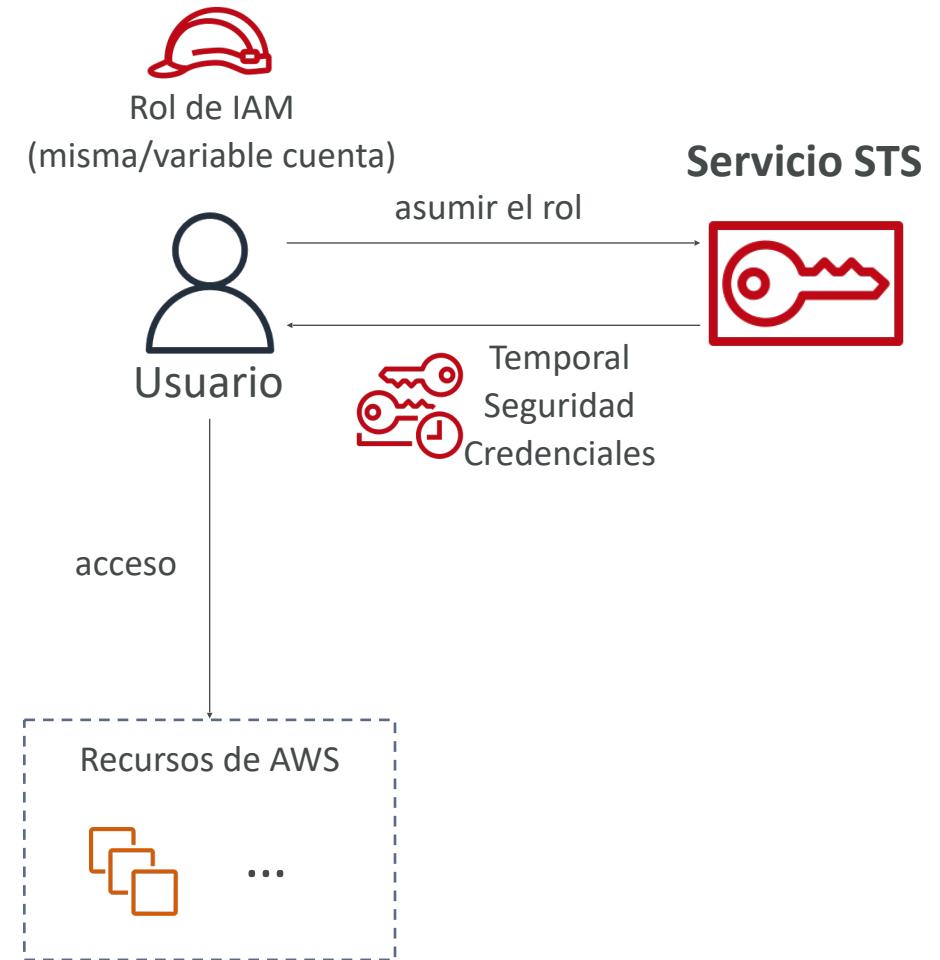


- **Compute Optimizer:** recomienda configuraciones de recursos para reducir el coste
- **Pricing Calculator:** coste de los servicios en AWS
- **Dashboard de facturación:** visión general de alto nivel + dashboards de niveles gratuitos
- **Etiquetas de asignación de costes:** etiqueta los recursos para crear informes detallados
- **Cost & Usage Reports:** el conjunto de datos de facturación más completo
- **Cost Explorer:** Visualiza el uso actual (detallado) y el uso previsto
- **Alarmas de facturación:** en us-east-1 - haz un seguimiento de la facturación global y por servicio
- **Budgets:** más avanzados - rastrea el uso, los costes y recibe alertas
- **Planes de ahorro:** forma sencilla de ahorrar según el uso a largo plazo de AWS
- **Cost Anomaly Detection:** detecta gastos inusuales utilizando Machine Learning
- **Service Quotas:** te avisa cuando estás cerca del umbral de cuota de servicio

Identidad Avanzada

AWS STS (Security Token Service)

- Te permite crear credenciales **temporales con privilegios limitados** para acceder a tus recursos de AWS
- Credenciales de corta duración: configuras el periodo de caducidad
- Casos de uso
 - **Federación de identidades:** gestionar las identidades de los usuarios en sistemas externos, y proporcionarles tokens STS para acceder a los recursos de AWS
 - **Roles IAM para el acceso cruzado/de la misma cuenta**
 - **Roles IAM para Amazon EC2:** proporciona credenciales temporales para que las instancias EC2 accedan a los recursos de AWS



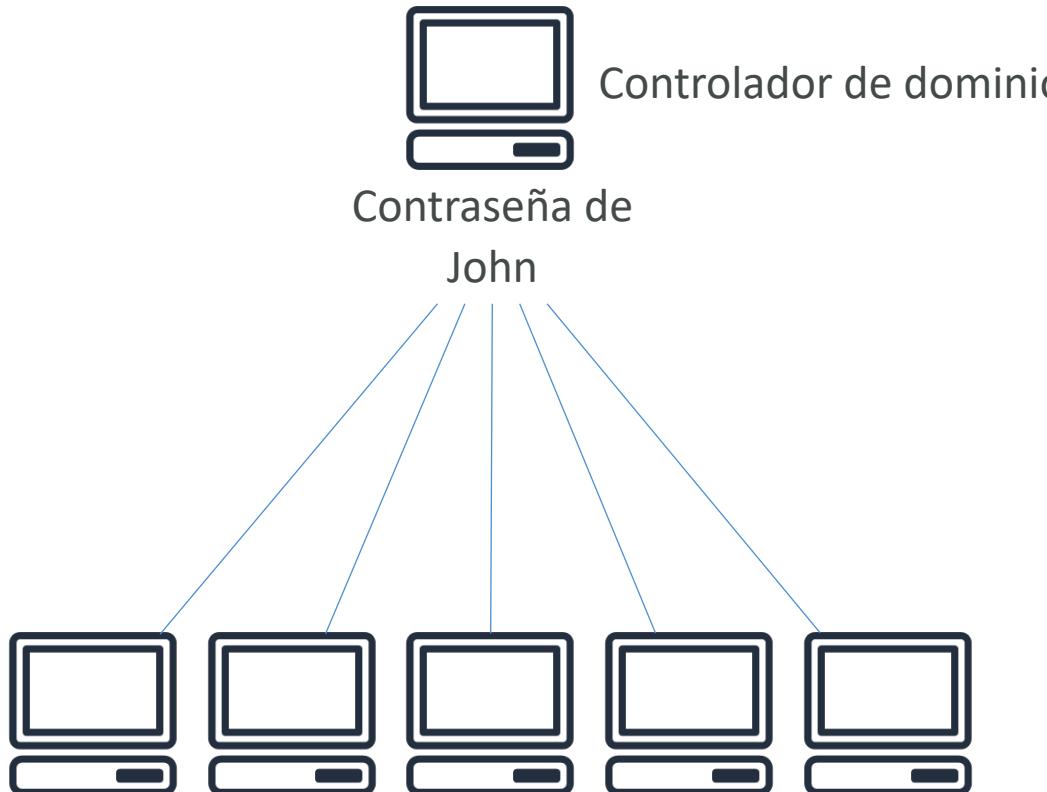
Amazon Cognito (simplificado)

- **Identidad para tus usuarios de aplicaciones web y móviles (potencialmente millones)**
- En lugar de crearles un usuario IAM, crea un usuario en Cognito



¿Qué es Microsoft Active Directory (AD)?

- Se encuentra en cualquier servidor Windows con servicios de dominio AD
- Base de datos de **objetos**: Cuentas de usuario, ordenadores, impresoras, archivos compartidos, grupos de seguridad
- Gestión centralizada de la seguridad, creación de cuentas, asignación de permisos



AWS Directory Services

- **AWS Managed Microsoft AD**

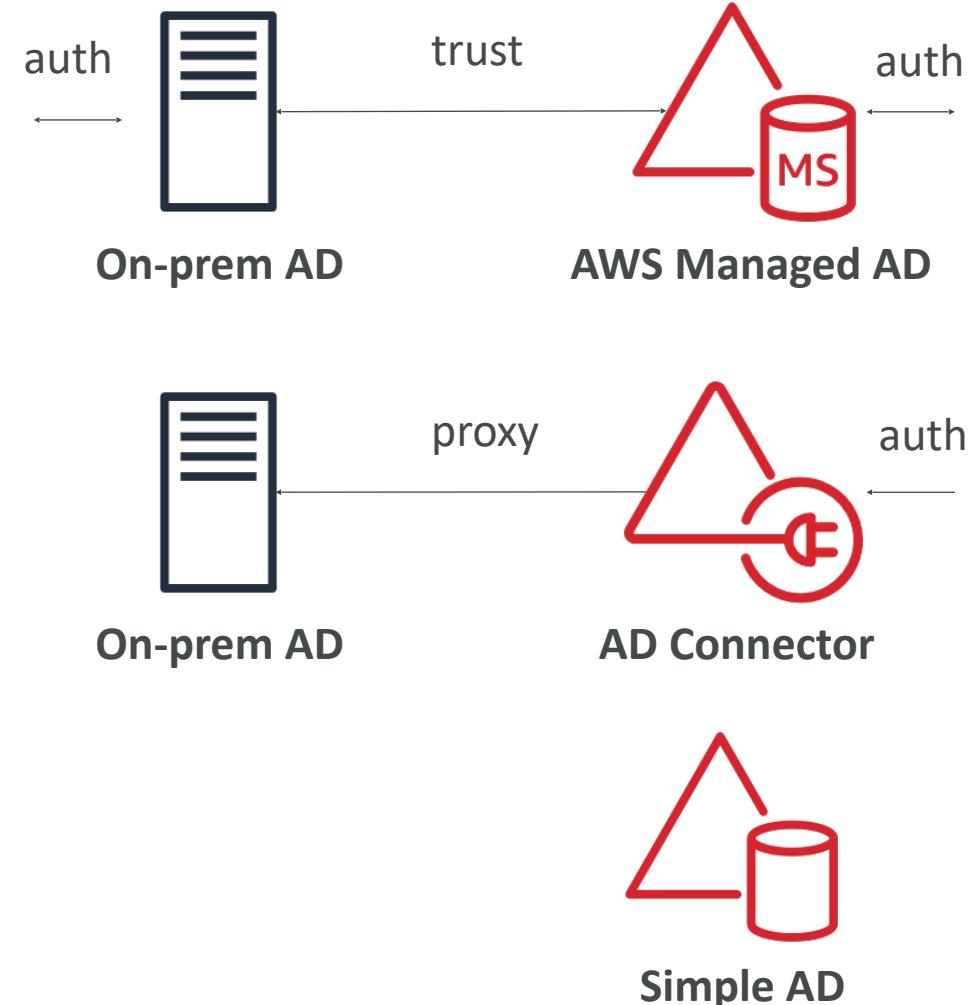
- Crea tu propio AD en AWS, administra los usuarios localmente, soporta MFA
- Establece conexiones de "confianza" con tu AD local

- **AD Conector**

- Directory Gateway (proxy) para redirigir al AD local, soporta MFA
- Los usuarios se gestionan en el AD local

- **Simple AD**

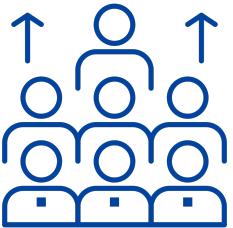
- Directorio gestionado compatible con AD en AWS
- No se puede unir con el AD local



AWS IAM Identity Center (sucesor de AWS Single Sign-On)



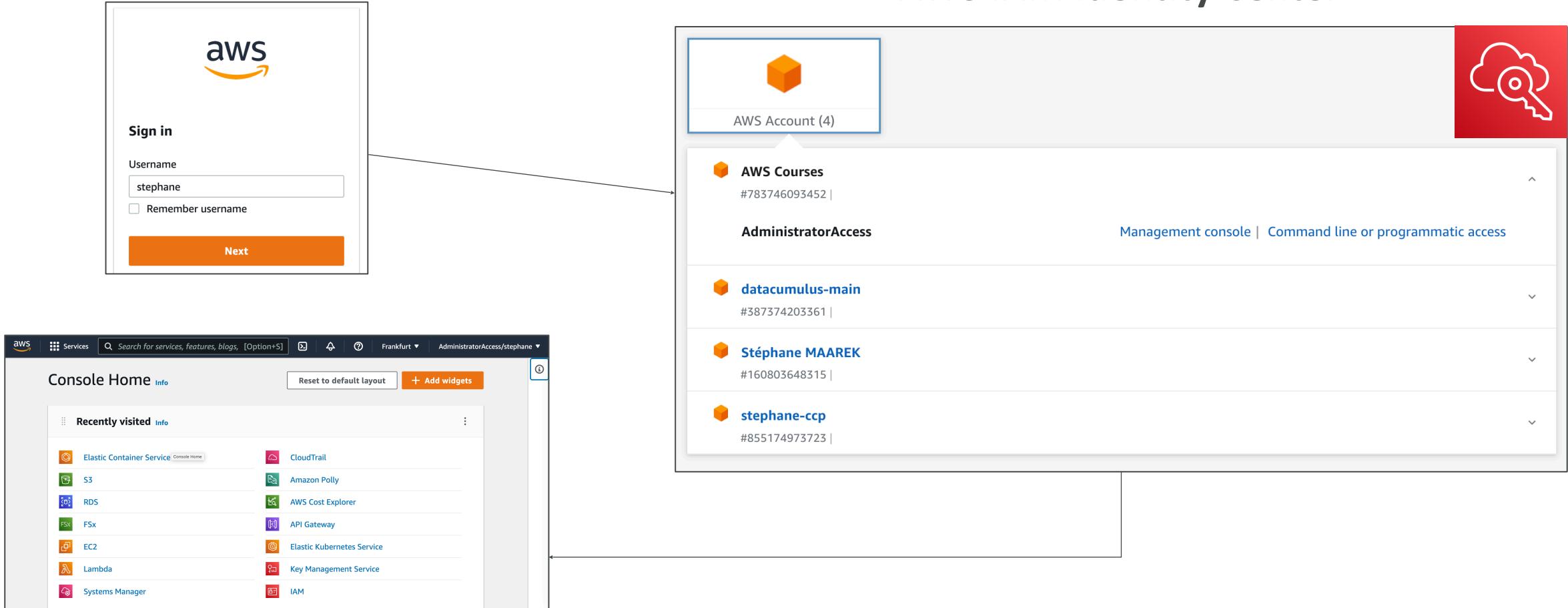
- Un inicio de sesión (inicio de sesión único) para todas tus
 - **Cuentas de AWS en AWS Organizations**
 - Aplicaciones empresariales en el Cloud (por ejemplo, Salesforce, Box, Microsoft 365, ...)
 - Aplicaciones habilitadas para SAML2.0
 - Instancias de Windows EC2
- Proveedores de identidad
 - Almacén de identidades incorporado en IAM Identity Center
 - De terceros: Active Directory (AD), OneLogin, Okta...



AWS IAM Identity Center

Flujo de inicio de sesión

AWS IAM Identity Center



Resumen - Identidad avanzada

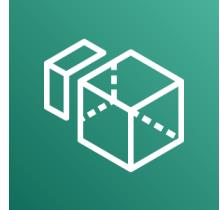
- **IAM**
 - Gestión de la identidad y el acceso dentro de tu cuenta de AWS
 - Para usuarios de confianza y pertenecientes a tu empresa
- **Organizations**: gestionar varias cuentas de AWS
- **Security Token Service (STS)**: credenciales temporales con privilegios limitados para acceder a los recursos de AWS
- **Cognito**: crea una base de datos de usuarios para tus aplicaciones móviles y web
- **Directory Services**: integra Microsoft Active Directory en AWS
- **IAM Identity Center**: un inicio de sesión para varias cuentas y aplicaciones de AWS

Otros servicios de AWS

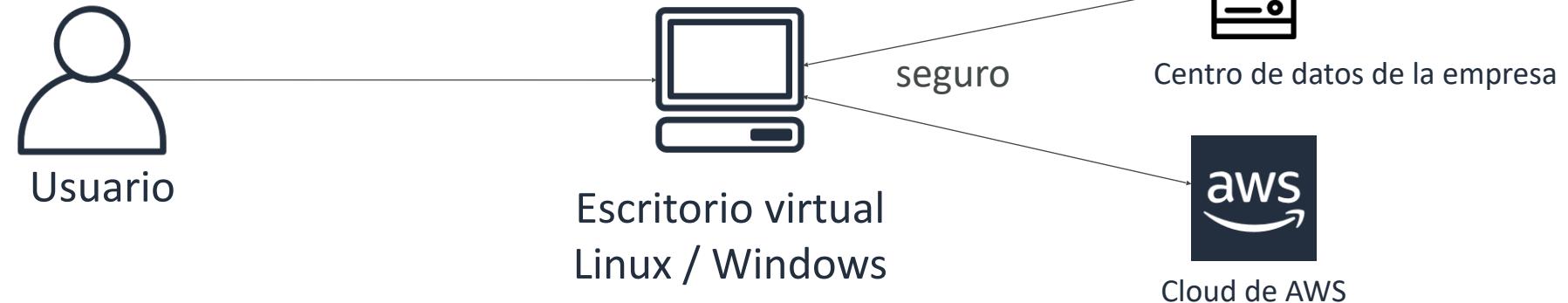
Sección de otros servicios de AWS

- Los otros servicios representan servicios que no pude agrupar con los otros
- Son servicios que, según los estudiantes, aparecen **a veces, pero raramente**, en el examen de AWS
- Las clases son cortas y breves y, probablemente, sin prácticas
- *No hay clase de resumen al final de la sección para mantener la flexibilidad*

Amazon WorkSpaces



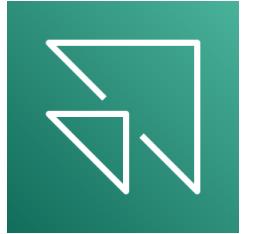
- Solución de escritorio gestionado como servicio (DaaS) para **aprovisionar** fácilmente **escritorios Windows o Linux**
- **Genial para eliminar la gestión de la VDI (Infraestructura de Escritorio Virtual) local**
- Rápidamente escalable a miles de usuarios
- Datos seguros: se integra con KMS
- Servicio de pago por uso con tarifas mensuales o por hora



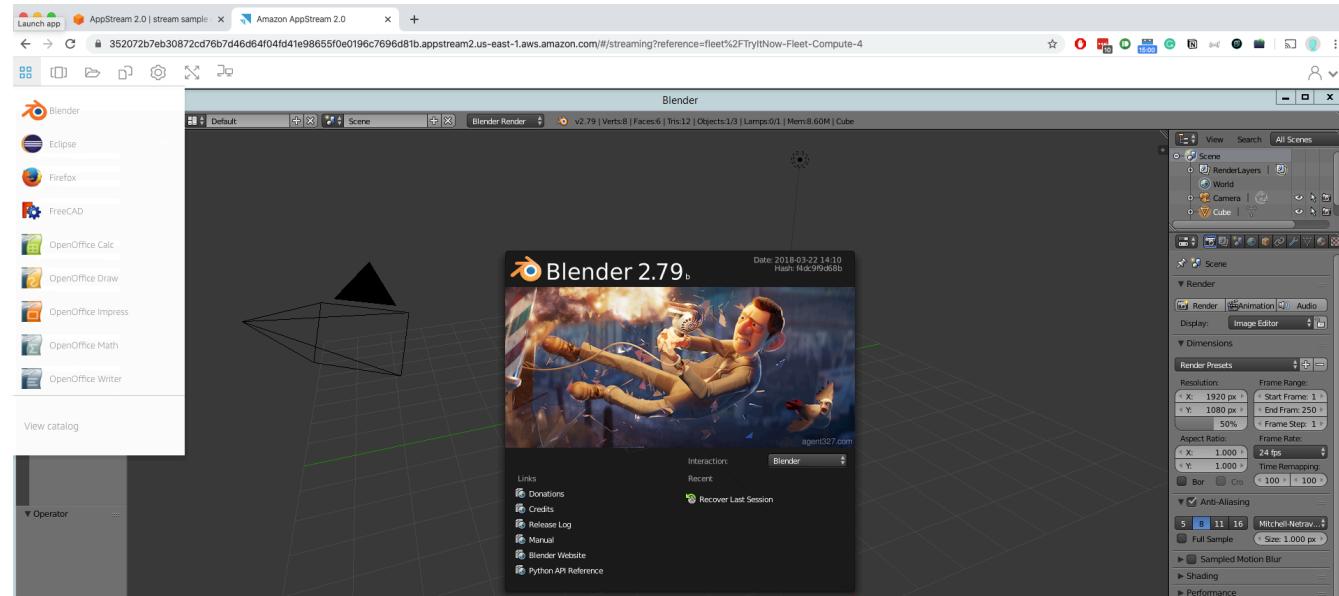
Amazon WorkSpaces - Varias regiones



Amazon AppStream 2.0



- Servicio de streaming de aplicaciones de escritorio para usuarios
- Entrega a cualquier ordenador, sin adquirir, infraestructura de aprovisionamiento
- **La aplicación se entrega desde un navegador web**



Amazon AppStream 2.0 vs WorkSpaces

- **Workspaces**

- Dispones de una VDI y un escritorio totalmente gestionados
- Los usuarios se conectan a la VDI y abren aplicaciones nativas o WAM
- Los espacios de trabajo están bajo demanda o siempre encendidos

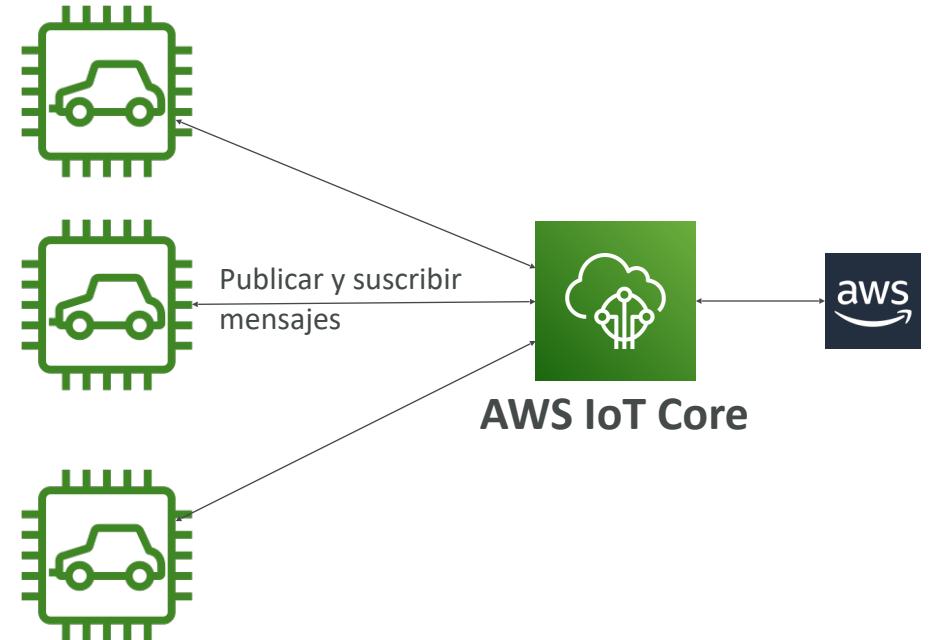
- **AppStream 2.0**

- Transmite una aplicación de escritorio a los navegadores web (sin necesidad de conectarse a una VDI)
- Funciona con cualquier dispositivo (que tenga un navegador web)
- Permite configurar un tipo de instancia por tipo de aplicación (CPU, RAM, GPU)

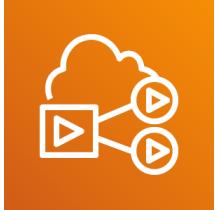
AWS IoT Core



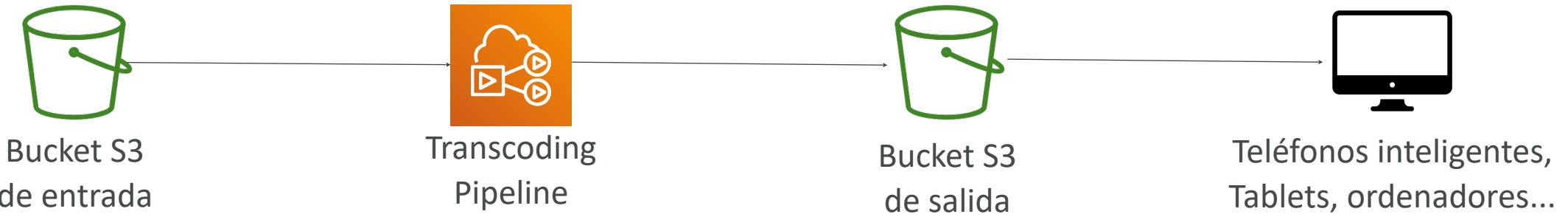
- IoT son las siglas de "Internet de las Cosas", la red de dispositivos conectados a Internet capaces de recopilar y transferir datos.
- El núcleo de IoT de AWS te permite **conectar fácilmente dispositivos IoT al Cloud de AWS**
- **Sin servidor, seguro y escalable** a miles de millones de dispositivos y billones de mensajes
- Tus aplicaciones pueden comunicarse con tus dispositivos aunque no estén conectados
- Se integra con muchos servicios de AWS (Lambda, S3, SageMaker, etc.)
- Construye aplicaciones IoT que recopilen, procesen, analicen y actúen sobre los datos



Amazon Elastic Transcoder



- Elastic Transcoder se utiliza para **convertir los archivos multimedia almacenados en S3 en archivos multimedia en los formatos requeridos por los dispositivos de reproducción de los consumidores (teléfonos, etc.)**
- Ventajas:
 - Fácil de usar
 - Altamente escalable - puede manejar grandes volúmenes de archivos multimedia y archivos de gran tamaño
 - Rentable: modelo de precios basado en la duración
 - Totalmente gestionado y seguro, paga por lo que usas



AWS AppSync



- Almacena y sincroniza los datos entre las aplicaciones móviles y web en tiempo real
- **Utiliza GraphQL (tecnología móvil de Facebook)**
- El código del cliente se puede generar automáticamente
- Integraciones con DynamoDB / Lambda
- Suscripciones en tiempo real
- Sincronización de datos sin conexión (sustituye a Cognito Sync)
- AWS Amplify puede aprovechar AWS AppSync en segundo plano



AWS Amplify

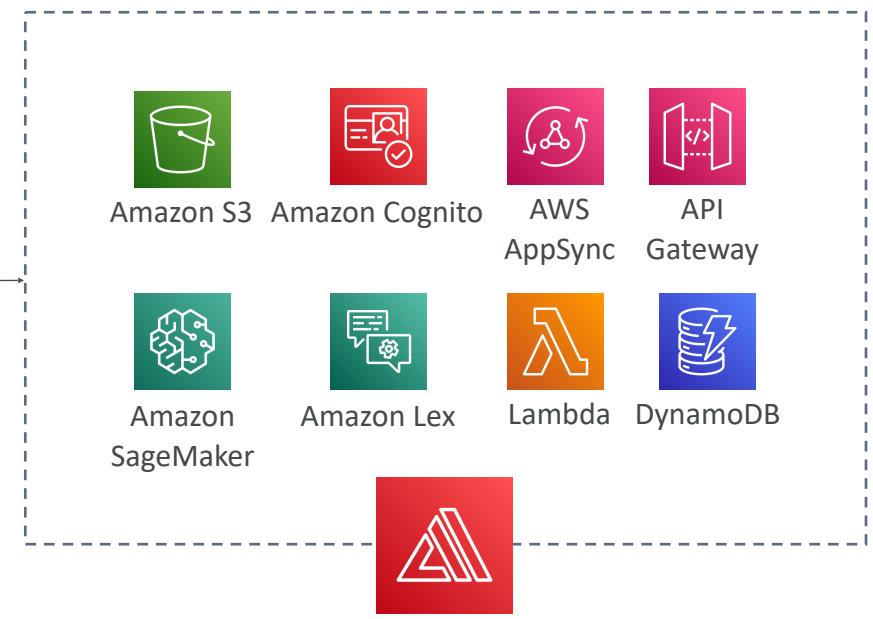


- **Un conjunto de herramientas y servicios que te ayudan a desarrollar y desplegar aplicaciones web y móviles escalables**
- Autenticación, almacenamiento, API (REST, GraphQL), CI/CD, PubSub, análisis, predicciones de IA/ML, monitorización, código fuente de AWS, GitHub, etc.

Set up

- Data
- Authentication
- Storage NEW
- Functions
- GraphQL API
- REST API
- Analytics

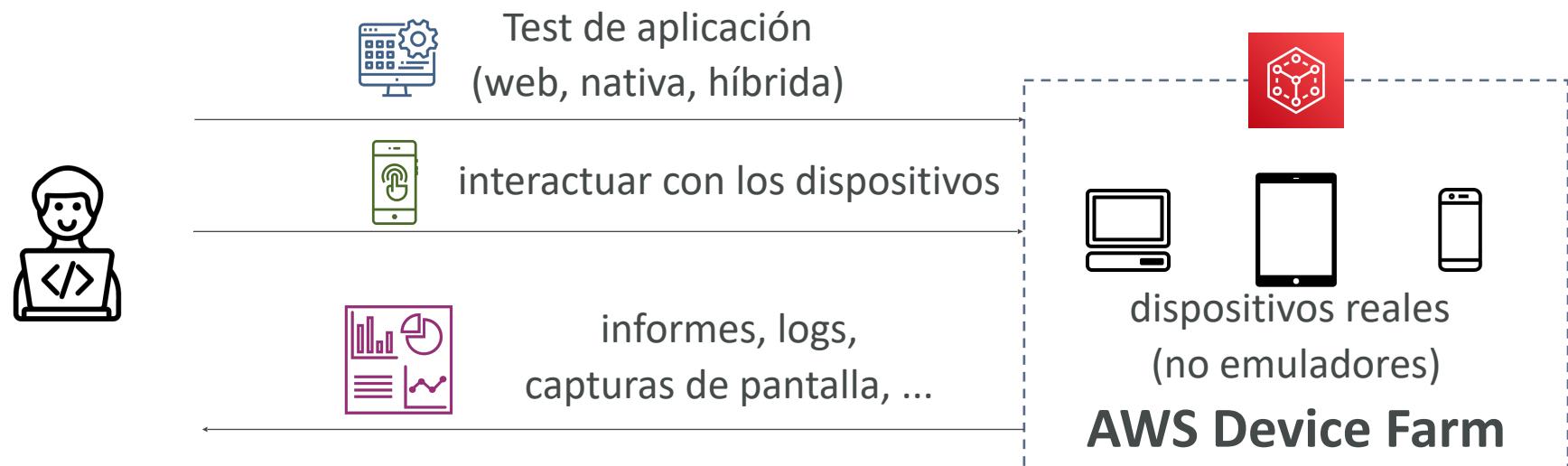
Amplify Studio



AWS Device Farm



- Servicio totalmente gestionado que prueba tus aplicaciones web y móviles en navegadores de escritorio, dispositivos móviles reales y tabletas
- Ejecuta pruebas simultáneamente en varios dispositivos (acelera la ejecución)
- Posibilidad de configurar los ajustes del dispositivo (GPS, idioma, Wi-Fi, Bluetooth, ...)

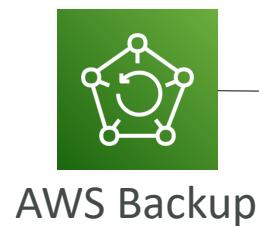


AWS Backup



- Servicio totalmente gestionado para administrar y automatizar centralmente las copias de seguridad en todos los servicios de AWS
- Copias de seguridad bajo demanda y programadas
- Soporta PITR (Point-in-time Recovery)
- Períodos de retención, gestión del ciclo de vida, políticas de copia de seguridad, ...
- Copia de seguridad entre regiones
- Copia de seguridad entre cuentas (usando AWS Organizations)

AWS Backup



AWS Backup

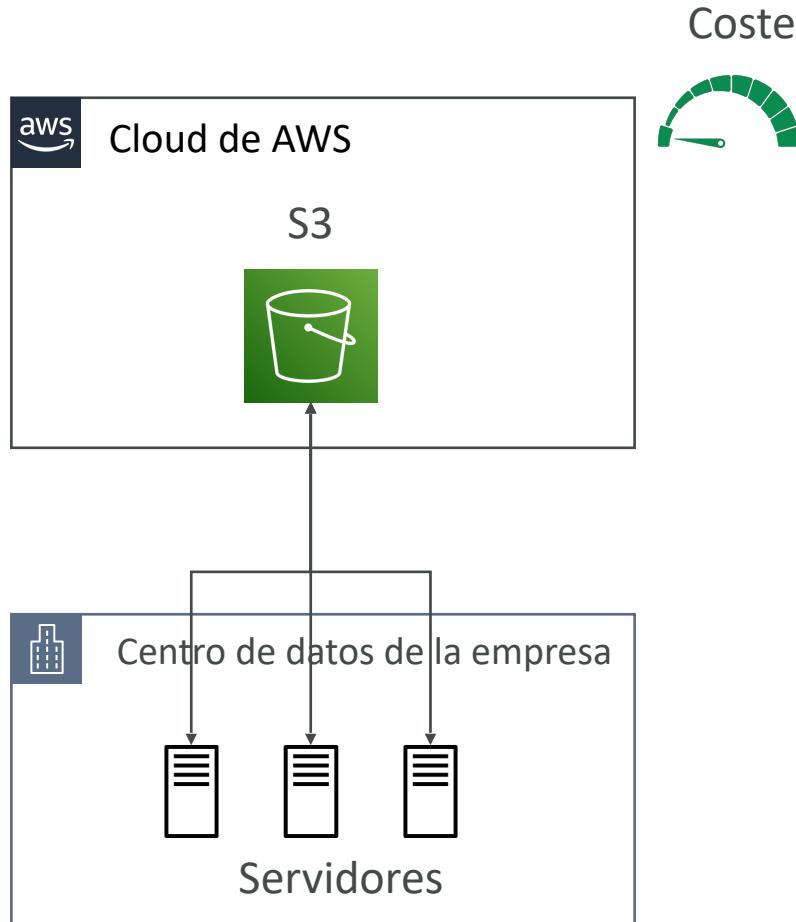
Crear un plan de copias
de seguridad
(frecuencia, política de
retención)



Amazon S3

Estrategias de recuperación de desastres

Copia de seguridad y restauración



Luz piloto

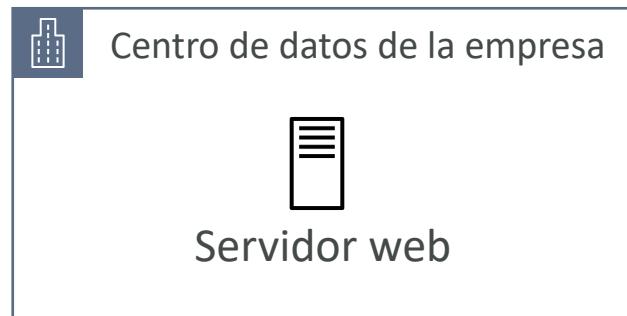
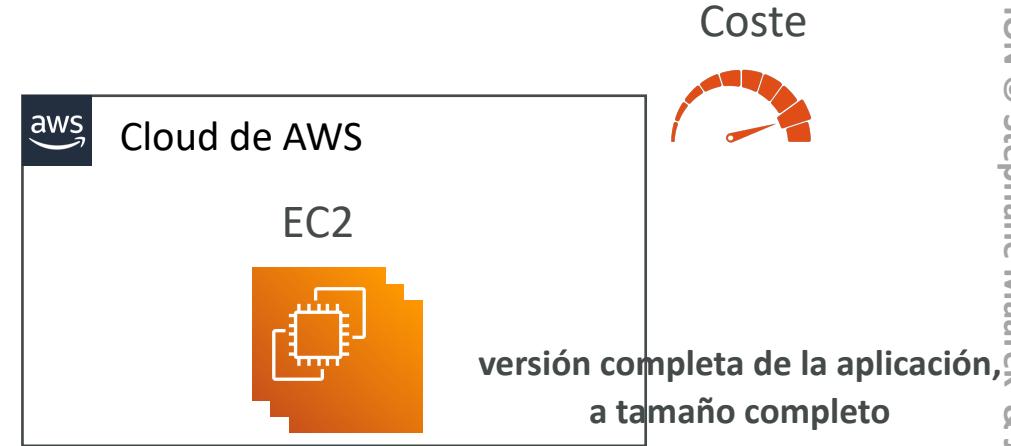


Estrategias de recuperación de desastres

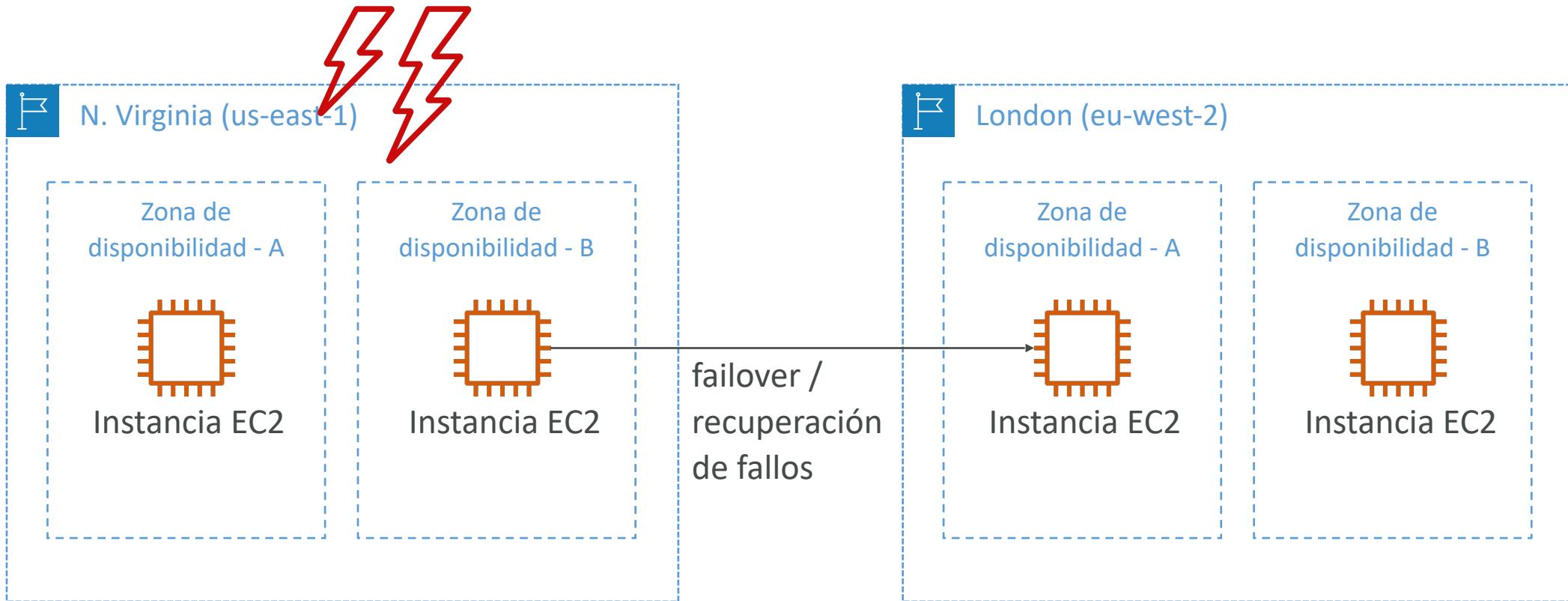
Warm Standby / Espera en caliente



Multisitio / Hot-Site



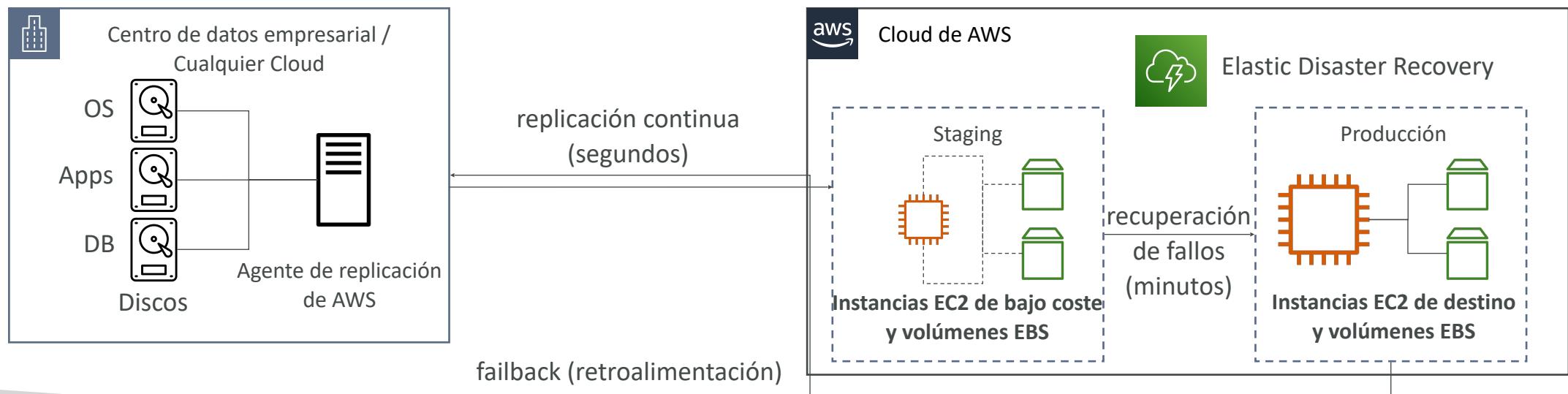
Configuración típica de RD para implementaciones en el Cloud



AWS Elastic Disaster Recovery (DRS)



- Antes se llamaba “CloudEndure Disaster Recovery”
- **Recupera** rápida y fácilmente tus servidores físicos, virtuales y en la nube en AWS
- Ejemplo: protege tus bases de datos más críticas (incluyendo Oracle, MySQL y SQL Server), aplicaciones empresariales (SAP)...
- Replicación continua a nivel de bloque para tus servidores

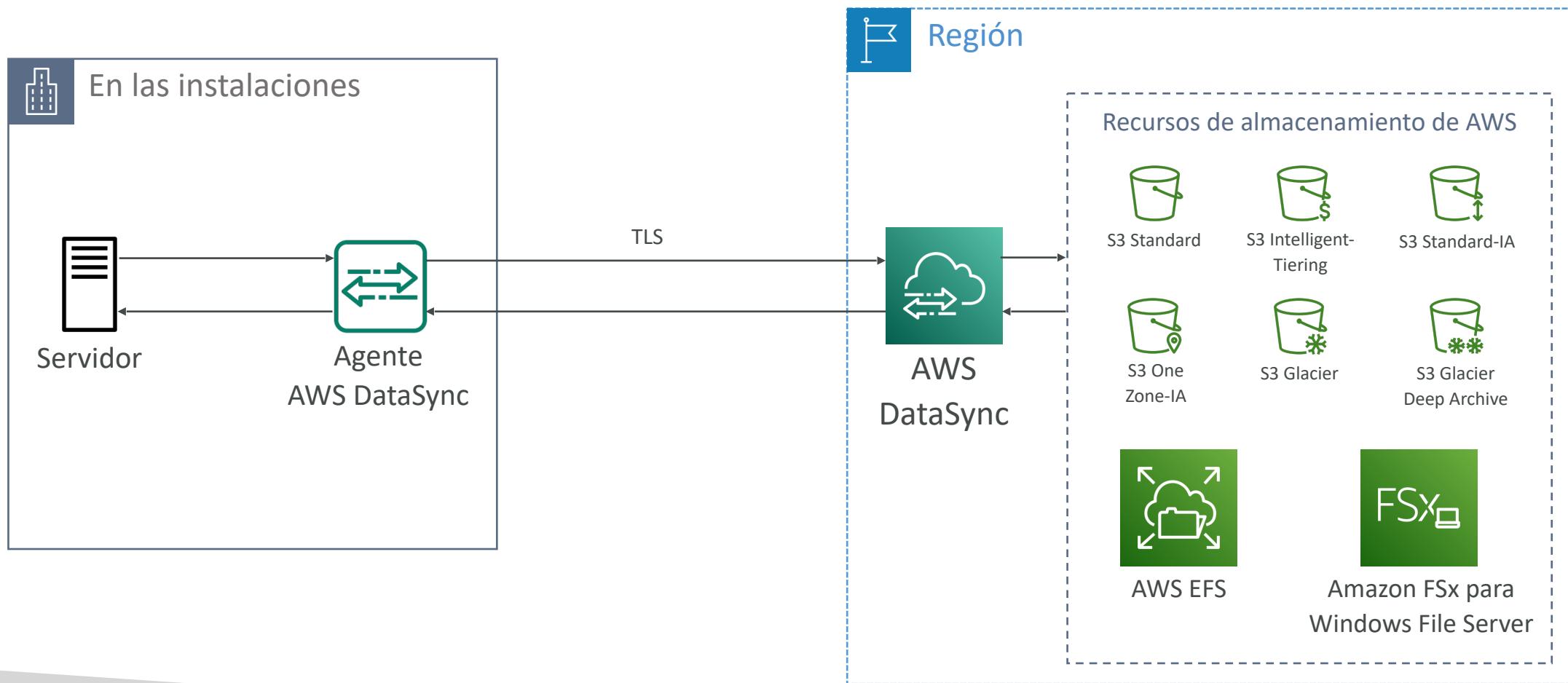


AWS DataSync



- Mueve una gran cantidad de datos de las instalaciones a AWS
- Puedes sincronizar a: Amazon S3 (cualquier clase de almacenamiento - incluyendo Glacier), Amazon EFS, Amazon FSx para Windows
- Las tareas de replicación se pueden programar cada hora, cada día, cada semana
- Las tareas de replicación son **incrementales** después de la primera carga completa

AWS DataSync

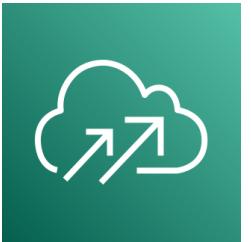


AWS Application Discovery Service



- Planificar los proyectos de migración recopilando información sobre los centros de datos locales
- Los datos de utilización de los servidores y la asignación de dependencias son importantes para las migraciones
- **Descubrimiento sin agente (AWS Agentless Discovery Connector)**
 - Inventario de máquinas virtuales, configuración e historial de rendimiento, como el uso de la CPU, la memoria y el disco
- **Descubrimiento basado en agentes (AWS Application Discovery Agent)**
 - Configuración del sistema, rendimiento del sistema, procesos en ejecución y detalles de las conexiones de red entre sistemas
- Los datos resultantes pueden verse en el AWS Migration Hub

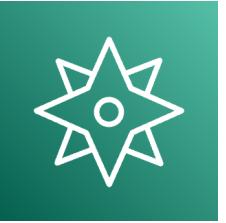
AWS Application Migration Service (MGN)



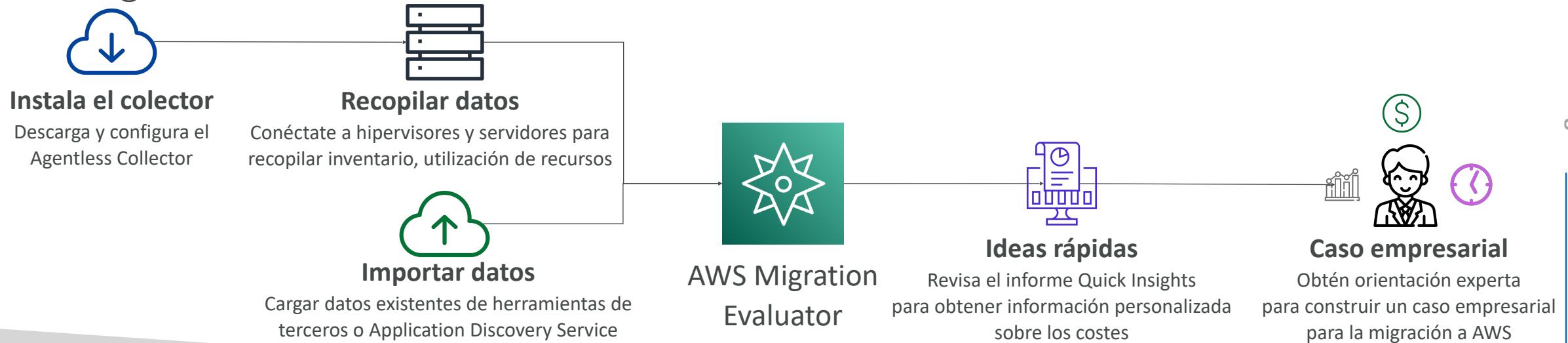
- La "evolución AWS" de CloudEndure Migration, que sustituye al AWS Server Migration Service (SMS)
- Solución Lift-and-shift que simplifica la migración de aplicaciones a AWS
- Convierte tus servidores físicos, virtuales y basados en la nube para que se ejecuten de forma nativa en AWS
- Soporta una amplia gama de plataformas, sistemas operativos y bases de datos



AWS Migration Evaluator



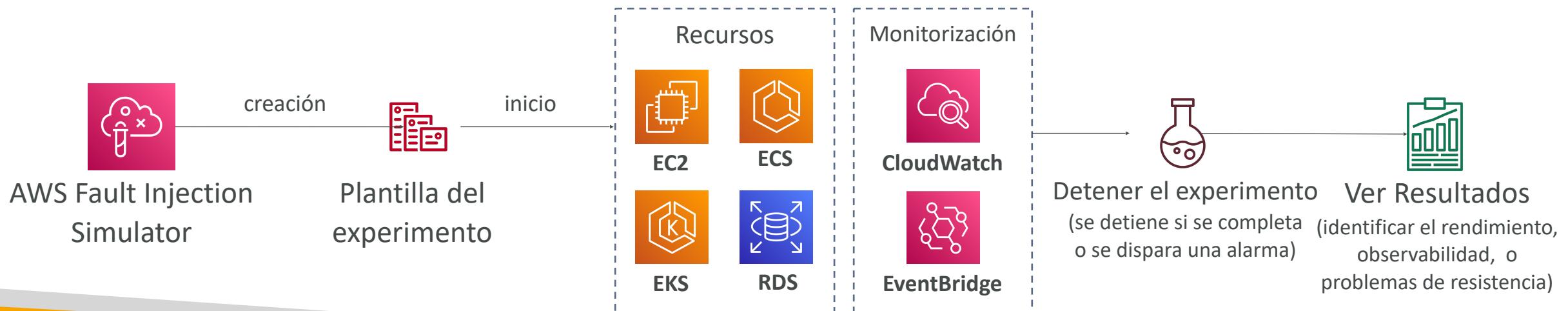
- Te ayuda a crear un caso empresarial basado en datos para la migración a AWS
- Proporciona una línea de base clara de lo que tu organización está ejecutando actualmente
- Instala el Agentless Collector para llevar a cabo una amplia detección
- Toma una snapshot de la huella local, dependencias de servidores, ...
- Analiza el estado actual, define el estado objetivo y desarrolla un plan de migración



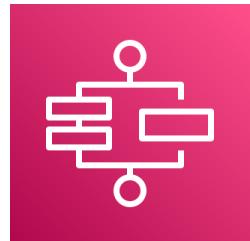
AWS Fault Injection Simulator (FIS)



- Un servicio totalmente gestionado para ejecutar experimentos de inyección de fallos en las cargas de trabajo de AWS
- Basado en la **ingeniería del caos**: estresar una aplicación creando eventos perturbadores (por ejemplo, un aumento repentino de la CPU o la memoria), observar cómo responde el sistema e implementar mejoras
- Te ayuda a descubrir fallos ocultos y cuellos de botella en el rendimiento
- Soporta los siguientes servicios de AWS: EC2, ECS, EKS, RDS...
- Utiliza plantillas preconstruidas que generan las interrupciones deseadas

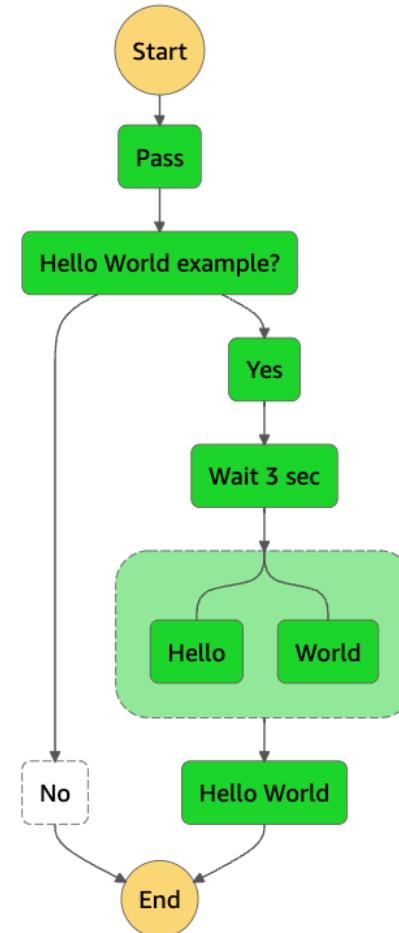


AWS Step Functions



- Construye un flujo de trabajo visual sin servidor para orquestar tus funciones Lambda
- **Características:** secuencia, paralelo, condiciones, tiempos de espera, manejo de errores, ...
- Puede integrarse con EC2, ECS, servidores locales, API Gateway, colas SQS, etc.
- Posibilidad de implementar la función de aprobación humana
- **Casos de uso:** cumplimiento de pedidos, procesamiento de datos, aplicaciones web, cualquier flujo de trabajo

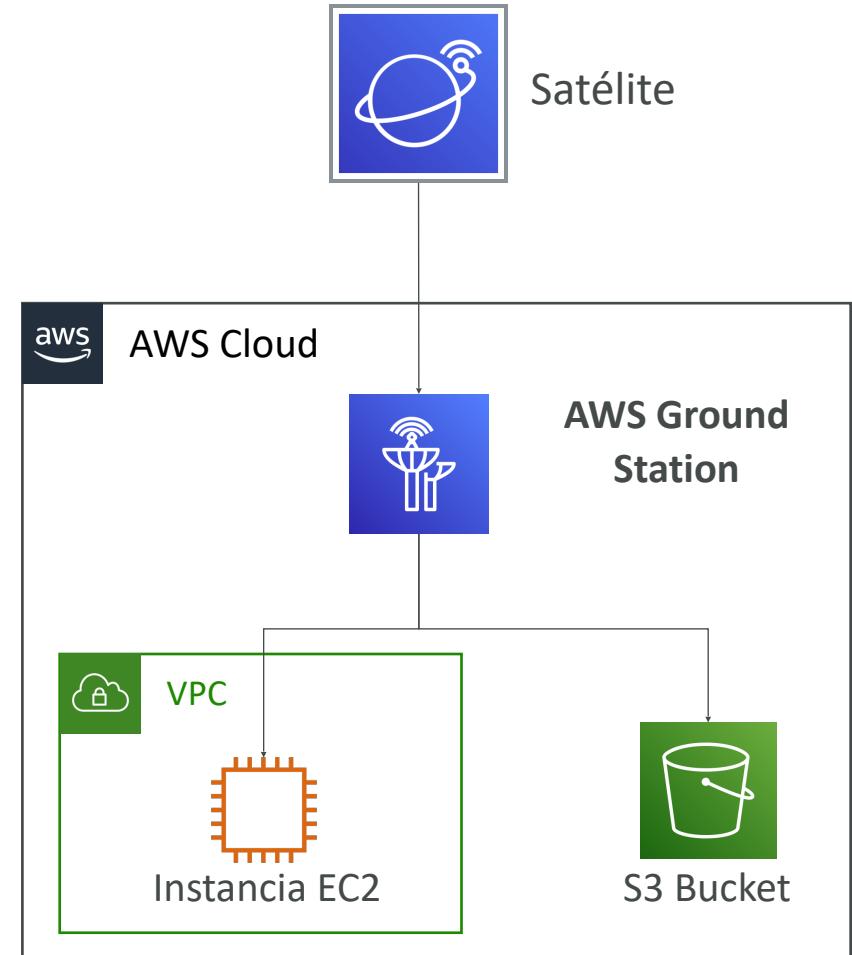
■ In Progress ■ Succeeded ■ Failed ■ Cancelled ■ Caught Error



AWS Ground Station

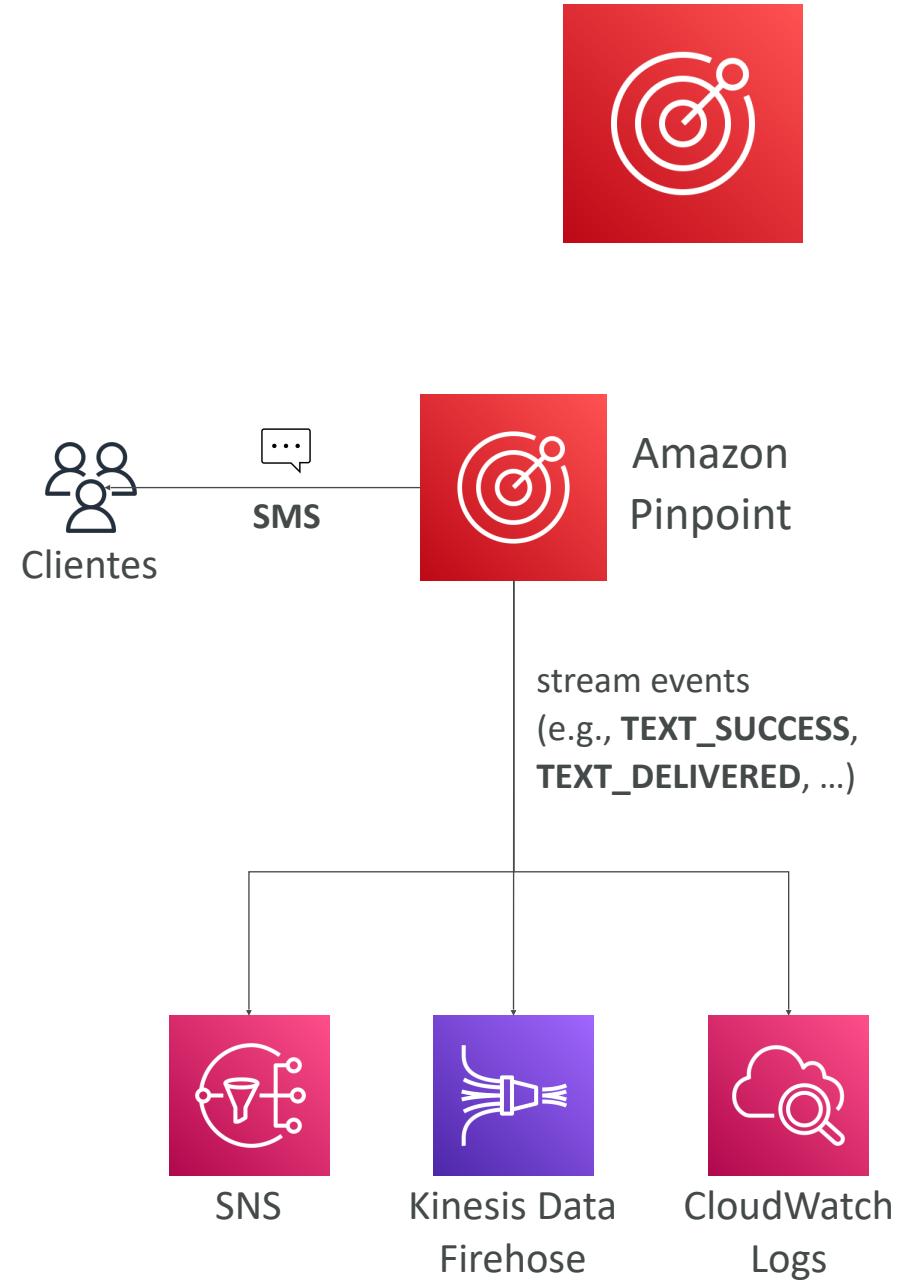


- Servicio totalmente gestionado que te permite controlar las comunicaciones por satélite, procesar los datos y escalar tus operaciones por satélite
- Proporciona una red global de estaciones terrestres de satélites cerca de las regiones de AWS
- Te permite descargar los datos de los satélites a tu VPC de AWS en cuestión de segundos
- Envía los datos de los satélites a una instancia S3 o EC2
- Casos de uso: previsión meteorológica, imágenes de superficie, comunicaciones, emisiones de vídeo



Amazon Pinpoint

- Servicio escalable de comunicaciones de marketing **bidireccional (saliente/entrante)**
- Soporta correo electrónico, SMS, push, voz y mensajería in-app
- Posibilidad de segmentar y personalizar los mensajes con el contenido adecuado para los clientes
- Posibilidad de recibir respuestas
- Escala a miles de millones de mensajes al día
- Casos de uso: realiza campañas enviando mensajes SMS de marketing, masivos y transaccionales
- **Frente a Amazon SNS o Amazon SES**
 - En SNS y SES gestionas la audiencia, el contenido y el calendario de entrega de cada mensaje
 - En Amazon Pinpoint, creas plantillas de mensajes, horarios de entrega, segmentos altamente segmentados y campañas completas



Arquitectura y ecosistema de AWS

Well Architected Framework

Principios generales de orientación

- Deja de adivinar tus necesidades de capacidad
- Testea sistemas a escala de producción
- Automatiza para facilitar la experimentación arquitectónica
- Permite arquitecturas evolutivas
 - Diseña en función de los requisitos cambiantes
- Impulsa las arquitecturas utilizando datos
- Mejorar mediante días de juego
 - Simular aplicaciones para días de venta flash

Mejores prácticas en el Cloud de AWS

Principios de diseño

- **Escalabilidad:** vertical y horizontal
- **Recursos desechables:** los servidores deben ser desechables y fácilmente configurables
- **Automatización:** Sin servidor, infraestructura como servicio, autoescalado...
- **Acoplamiento:**
 - Los monolitos son aplicaciones que hacen más y más con el tiempo, se hacen más grandes
 - Divídela en componentes más pequeños y débilmente acoplados
 - Un cambio o un fallo en un componente no debería afectar en cascada a otros componentes
- **Servicios, no servidores:**
 - No utilices sólo EC2
 - Utiliza servicios gestionados, bases de datos, serverless, etc.

Well Architected Framework - 6 Pilares

- 1) Excelencia operativa
 - 2) Seguridad
 - 3) Fiabilidad
 - 4) Eficiencia del rendimiento
 - 5) Optimización de costes
 - 6) Sostenibilidad
-
- **No son algo a equilibrar, ni a compensar, son una sinergia**

I) Excelencia operativa

- Incluye la capacidad de ejecutar y supervisar los sistemas para aportar valor al negocio y mejorar continuamente los procesos y procedimientos de soporte
- Principios de diseño
 - **Realiza operaciones como código** - Infraestructura como código
 - **Anotar la documentación** - Automatizar la creación de documentación anotada después de cada construcción
 - **Realiza cambios frecuentes, pequeños y reversibles** - Para que en caso de cualquier fallo, puedas revertirlo
 - **Perfecciona los procedimientos de las operaciones con frecuencia** - Y asegúrate de que los miembros del equipo están familiarizados con ellos
 - **Anticipa los fallos**
 - **Aprende de todos los fallos operativos**

Servicios AWS - Excelencia operativa

- Preparar



AWS CloudFormation



AWS Config

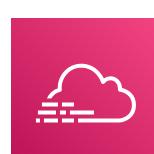
- Operar



AWS CloudFormation



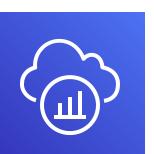
AWS Config



AWS CloudTrail

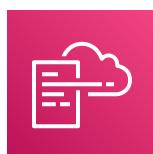


Amazon CloudWatch



AWS X-Ray

- Evolucionar



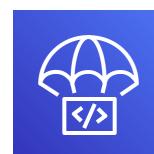
AWS CloudFormation



AWS CodeBuild



AWS CodeCommit



AWS CodeDeploy



AWS CodePipeline

2) Seguridad

- Incluye la capacidad de proteger la información, los sistemas y los activos a la vez que se proporciona valor empresarial mediante evaluaciones de riesgo y estrategias de mitigación
- Principios de diseño
 - **Implementar una base sólida de identidad** - Centralizar la gestión de privilegios y reducir (o incluso eliminar) la dependencia de las credenciales a largo plazo - Principio de mínimo privilegio - IAM
 - **Habilitar la trazabilidad** - Integrar logs y métricas con los sistemas para responder y actuar automáticamente
 - **Aplicar la seguridad en todas las capas** - Como red de borde, VPC, subred, equilibrador de carga, cada instancia, sistema operativo y aplicación
 - **Automatizar las mejores prácticas de seguridad**
 - **Protege los datos en tránsito y en reposo** - Cifrado, tokenización y control de acceso
 - **Mantén a las personas alejadas de los datos** - Reduce o elimina la necesidad de acceso directo o procesamiento manual de los datos
 - **Prepárate para los eventos de seguridad** - Realiza simulaciones de respuesta a incidentes y utiliza herramientas con automatización para aumentar la velocidad de detección, investigación y recuperación
 - **Modelo de responsabilidad compartida**

Servicios AWS - Seguridad

- Gestión de identidades y accesos



IAM



AWS STS



MFA token

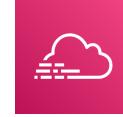


AWS Organizations

- Controles de detección



AWS Config



AWS CloudTrail



Amazon CloudWatch

- Protección de la infraestructura



Amazon CloudFront



Amazon VPC



AWS Shield



AWS WAF



Amazon Inspector

- Protección de datos



KMS



S3



Elastic Load Balancing (ELB)



Amazon EBS

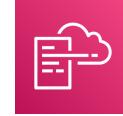


Amazon RDS

- Respuesta a incidentes



IAM



AWS CloudFormation



Amazon EventBridge

3) Fiabilidad

- Capacidad de un sistema para recuperarse de las interrupciones de la infraestructura o del servicio, adquirir dinámicamente recursos informáticos para satisfacer la demanda y mitigar las interrupciones, como las desconfiguraciones o los problemas transitorios de la red
- Principios de diseño
 - **Prueba los procedimientos de recuperación** - Utiliza la automatización para simular diferentes fallos o para recrear escenarios que hayan provocado fallos anteriormente
 - **Recupérate automáticamente de los fallos** - Anticipa y remedia los fallos antes de que se produzcan
 - **Escala horizontalmente para aumentar la disponibilidad agregada del sistema** - Distribuye las peticiones entre múltiples recursos más pequeños para asegurar que no comparten un punto de fallo común
 - **Deja de adivinar la capacidad** - Mantén el nivel óptimo para satisfacer la demanda sin aprovisionamiento excesivo o insuficiente - Utiliza el escalado automático
 - **Gestiona el cambio en la automatización** - Utiliza la automatización para realizar cambios en la infraestructura

Servicios AWS - Fiabilidad

- Fundamentos



IAM



Amazon VPC

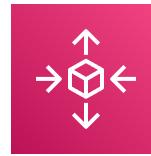


Service Quotas



AWS Trusted Advisor

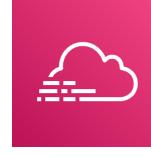
- Gestión del cambio



AWS Auto Scaling



Amazon CloudWatch



AWS CloudTrail



AWS Config

- Gestión del fracaso



Backups



AWS CloudFormation



Amazon S3



Amazon S3 Glacier



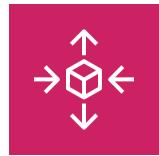
Amazon Route 53

4) Eficiencia del rendimiento

- Incluye la capacidad de utilizar los recursos informáticos de forma eficiente para satisfacer los requisitos del sistema, y de mantener esa eficiencia a medida que cambia la demanda y evolucionan las tecnologías
- Principios de diseño
 - **Democratizar las tecnologías avanzadas** - Las tecnologías avanzadas se convierten en servicios y, por tanto, puedes centrarte más en el desarrollo de productos
 - **Hazte global en minutos** - Despliegue fácil en múltiples regiones
 - Utiliza arquitecturas sin servidor - Evita la carga de gestionar servidores
 - **Experimenta más a menudo** - Es fácil realizar pruebas comparativas
 - **Símpatía mecánica** - Conoce todos los servicios de AWS

Servicios AWS - Eficiencia del rendimiento

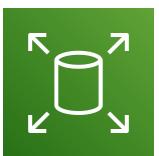
- Selección



AWS Auto Scaling



AWS Lambda

Amazon Elastic Block Store
(EBS)Amazon Simple Storage
Service (S3)

Amazon RDS

- Revisar

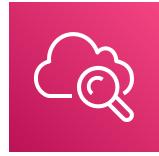


AWS CloudFormation



AWS Lambda

- Monitorización



Amazon CloudWatch

- Ventajas / Desventajas



Amazon RDS



Amazon ElastiCache



AWS Snowball



Amazon CloudFront

5) Optimización de costes

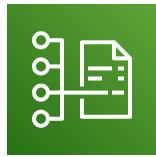
- Incluye la capacidad de ejecutar sistemas para ofrecer valor empresarial al precio más bajo
- Principios de diseño
 - **Adopta un modo de consumo** - Paga sólo por lo que usas
 - **Medir la eficiencia global** - Utilizar CloudWatch
 - **Deja de gastar dinero en las operaciones del centro de datos** - AWS se encarga de la parte de la infraestructura y permite al cliente centrarse en los proyectos de la organización
 - **Analiza y atribuye el gasto** - La identificación precisa del uso y los costes del sistema, ayuda a medir el retorno de la inversión (ROI) - Asegúrate de utilizar etiquetas
 - **Utiliza servicios gestionados y a nivel de aplicación para reducir el coste de propiedad** - Como los servicios gestionados operan a escala de el Cloud, pueden ofrecer un menor coste por transacción o servicio

Servicios AWS - Optimización de costes

- Conciencia del gasto
- Recursos rentables
- Adecuación de la oferta y la demanda
- Optimización en el tiempo



AWS Budgets



AWS Cost and Usage Report



AWS Cost Explorer



Reserved Instance Reporting



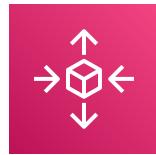
Instancia spot



Instancia reservada



Amazon S3 Glacier



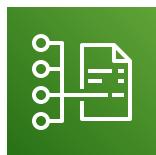
AWS Auto Scaling



AWS Lambda



AWS Trusted Advisor



AWS Cost and Usage Report

AWS News Blog

6) Sostenibilidad

- El pilar de la sostenibilidad se centra en minimizar el impacto medioambiental de la ejecución de cargas de trabajo en el Cloud.
- Principios de diseño
 - **Comprende tu impacto** - establece indicadores de rendimiento, evalúa las mejoras
 - **Establece objetivos de sostenibilidad** - Establece objetivos a largo plazo para cada carga de trabajo, modela el retorno de la inversión (ROI)
 - **Maximizar la utilización** - Dimensionar correctamente cada carga de trabajo para maximizar la eficiencia energética del hardware subyacente y minimizar los recursos ociosos.
 - **Anticipa y adopta nuevas ofertas de hardware y software más eficientes** - y diseña la flexibilidad para adoptar nuevas tecnologías con el tiempo.
 - **Utiliza servicios gestionados** - los servicios compartidos reducen la cantidad de infraestructura; los servicios gestionados ayudan a automatizar las mejores prácticas de sostenibilidad, como mover los datos a los que se accede con poca frecuencia al almacenamiento en frío y ajustar la capacidad de computación.
 - **Reduce el impacto descendente de tus cargas de trabajo en el Cloud** - Reduce la cantidad de energía o recursos necesarios para utilizar tus servicios y reduce la necesidad de que tus clientes actualicen sus dispositivos

Servicios AWS - Sostenibilidad

- Autoescalado EC2, oferta sin servidor (Lambda, Fargate)
- AWS Cost Explorer, AWS Graviton 2, Instancias EC2 T, Instancias @Spot
- EFS-IA, Amazon S3 Glacier, volúmenes EBS Cold HDD
- Configuraciones del ciclo de vida de S3, S3 Intelligent Tiering
- Gestor del ciclo de vida de los datos de Amazon
- Lectura local, escritura global RDS Réplicas de lectura, Aurora Global DB, DynamoDB Global Table, CloudFront

EC2 Auto Scaling



Cost Explorer



EFS-IA



S3 Intelligent Tiering



RDS



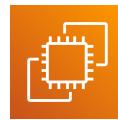
Aurora



Lambda



EC2



S3 Glacier



Data Lifecycle Manager



DynamoDB



Fargate



Instancias Spot



EBS





Herramienta AWS Well-Architected

- Herramienta gratuita para **revisar tus arquitecturas** con respecto al Marco de los 6 pilares de la buena arquitectura y **adoptar las mejores prácticas de arquitectura**
- ¿Cómo funciona?
 - Selecciona tu carga de trabajo y responde a las preguntas
 - Revisa tus respuestas con respecto a los 6 pilares
 - Obtén asesoramiento: obtén vídeos y documentación, genera un informe, ve los resultados en un dashboards
- Echemos un vistazo: <https://console.aws.amazon.com/wellarchitected>

A screenshot of the AWS Well-Architected Tool interface. The top navigation bar shows 'Well-Architected Tool > Workloads'. Below the navigation is a search bar labeled 'Search by workload name'. A toolbar with buttons for 'Generate report', 'View details', 'Edit', 'Delete', and 'Define workload' is visible. To the right of the toolbar are navigation icons for back, forward, and refresh. A table lists five workloads with columns: Name, Overall status, High risks, Medium risks, Improvement status, and Last updated. The workloads listed are: Internal Employee Portal (Answered, 13 High, 2 Medium, None, Nov 24, 2018), Mobile app - Android (Answered, 9 High, 1 Medium, None, Nov 24, 2018), Mobile app - iOS (Answered, 0 High, 1 Medium, None, Nov 24, 2018), Retail Website- EU (Unanswered, 0 High, 0 Medium, None, Nov 24, 2018), and Retail Website- North America (Unanswered, 0 High, 0 Medium, None, Nov 24, 2018).

Name	Overall status	High risks	Medium risks	Improvement status	Last updated
Internal Employee Portal	Answered	13	2	None	Nov 24, 2018 3:40 PM UTC-8
Mobile app - Android	Answered	9	1	None	Nov 24, 2018 3:43 PM UTC-8
Mobile app - iOS	Answered	0	1	None	Nov 24, 2018 3:49 PM UTC-8
Retail Website- EU	Unanswered	0	0	None	Nov 24, 2018 3:52 PM UTC-8
Retail Website- North America	Unanswered	0	0	None	Nov 24, 2018 3:19 PM UTC-8

© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#)

<https://aws.amazon.com/blogs/aws/new-aws-well-architected-tool-review-workloads-against-best-practices/>

AWS Cloud Adoption Framework (AWS CAF)

- Te ayuda a construir y luego ejecutar un plan integral para tu transformación digital mediante el uso innovador de AWS
- Creado por profesionales de AWS aprovechando las mejores prácticas de AWS y las lecciones aprendidas de miles de clientes
- AWS CAF identifica las capacidades organizativas específicas que apuntalan el éxito de las transformaciones en el Cloud
- AWS CAF agrupa sus capacidades en seis perspectivas:
Negocio, Personas, Gobierno, Plataforma, Seguridad y Operaciones



Perspectivas y capacidades fundamentales del CAF

Capacidades empresariales



- Perspectiva empresarial ayuda a garantizar que tus inversiones en el Cloud aceleran tus ambiciones de transformación digital y los resultados empresariales.
- Perspectiva de las personas sirve **como puente entre la tecnología y la empresa**, acelerando el viaje en el Cloud para ayudar a las organizaciones a evolucionar más rápidamente hacia una cultura de crecimiento continuo, aprendizaje y en la que el cambio se convierte en algo normal, centrándose en la cultura, la estructura organizativa, el liderazgo y el personal.
- Perspectiva de gobierno te ayuda a orquestar tus iniciativas en el Cloud maximizando los beneficios organizativos y minimizando los riesgos relacionados con la transformación.

Perspectivas y capacidades fundamentales del CAF

Capacidades empresariales



Perspectivas y capacidades fundamentales del CAF

Capacidades técnicas

- Perspectiva de la plataforma te ayuda a crear una plataforma de Cloud híbrida, escalable y de calidad empresarial, a modernizar las cargas de trabajo existentes y a implantar nuevas soluciones nativas de Cloud.

- Perspectiva de seguridad te ayuda a conseguir la confidencialidad, integridad y disponibilidad de tus datos y cargas de trabajo en el Cloud.

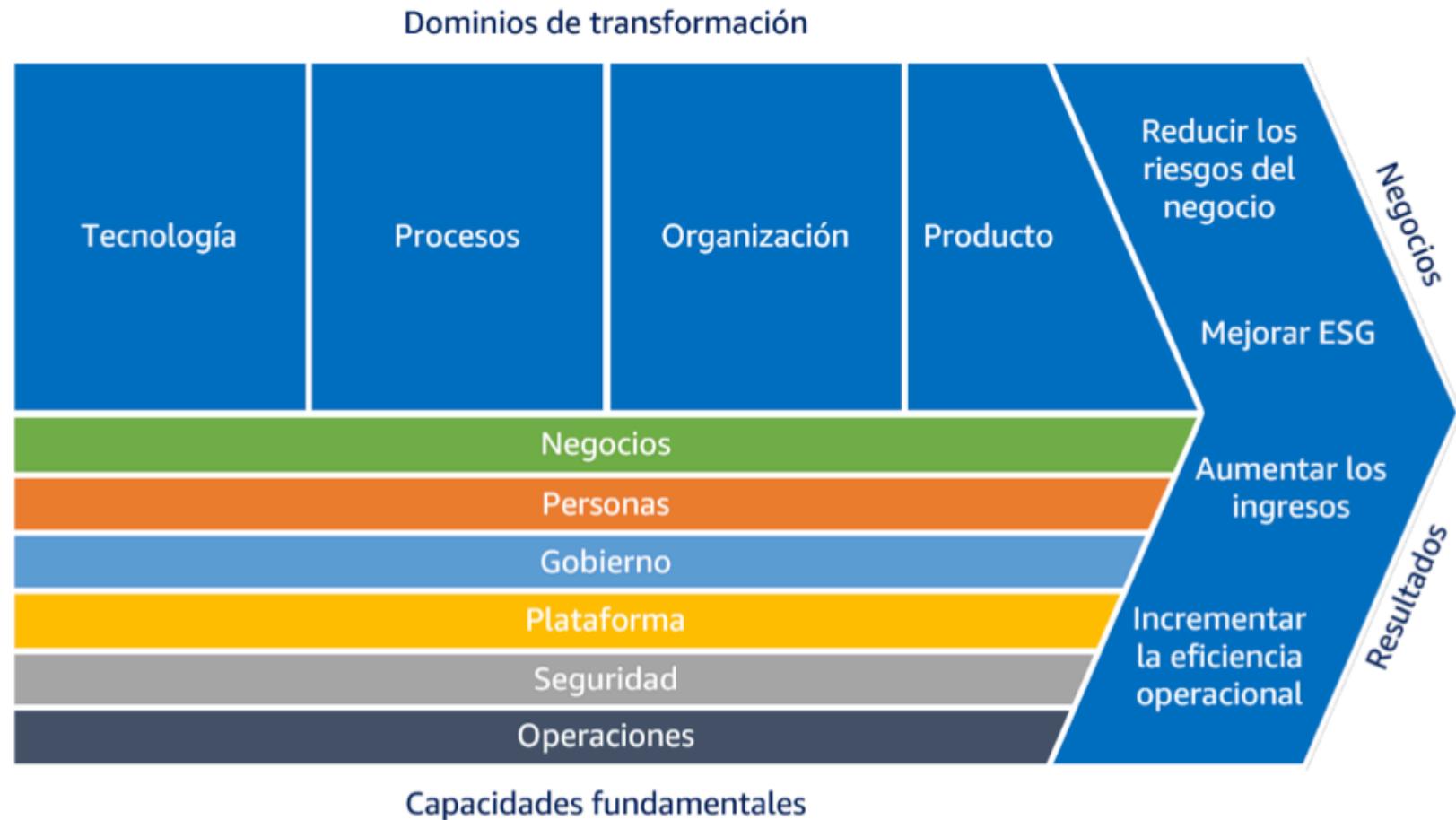
- Perspectiva de las operaciones ayuda a garantizar que tus servicios en el Cloud se prestan a un nivel que satisface las necesidades de tu empresa.


Perspectivas y capacidades fundamentales del CAF

Capacidades técnicas

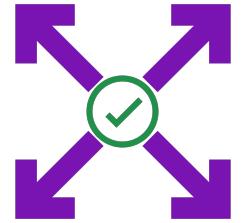


Cadena de valor de la transformación Cloud



AWS CAF - Dominios de transformación

- **Tecnología** - utilizar el Cloud para migrar y modernizar la infraestructura heredada, las aplicaciones, los datos y las plataformas de análisis...
- **Proceso** - digitalizando, automatizando y optimizando tus operaciones empresariales
 - aprovechar las nuevas plataformas de datos y análisis para crear perspectivas procesables
 - utilizando Machine Learning (ML) para mejorar tu experiencia de servicio al cliente...
- **Organización** - Reimaginando tu modelo operativo
 - organizar tus equipos en torno a productos y flujos de valor
 - aprovechando métodos ágiles para iterar y evolucionar rápidamente
- **Producto** - Reimaginar tu modelo de negocio creando nuevas propuestas de valor (productos y servicios) y modelos de ingresos



Dimensionamiento correcto de AWS

- EC2 tiene muchos tipos de instancia, pero elegir el tipo de instancia más potente no es la mejor opción, porque el Cloud es **elástico**
- El dimensionamiento correcto es el proceso de adecuar los tipos y tamaños de instancia a los requisitos de rendimiento y capacidad de tu carga de trabajo al menor coste posible
- **Aumentar la escala es fácil, así que empieza siempre con algo pequeño**
- También es el proceso de examinar las instancias desplegadas e identificar las oportunidades de eliminar o reducir su tamaño sin comprometer la capacidad u otros requisitos, lo que da lugar a una reducción de los costes
- Es importante dimensionar correctamente...
 - **antes de una migración al Cloud**
 - **continuamente después del proceso de incorporación al Cloud (los requisitos cambian con el tiempo)**
- CloudWatch, Cost Explorer, Trusted Advisor y herramientas de terceros pueden ayudar

Ecosistema AWS - Recursos gratuitos

- **Blogs de AWS:** <https://aws.amazon.com/blogs/aws/>
- **Foros (comunidad) de AWS:** <https://forums.aws.amazon.com/index.jspa>
- **Whitepapers y guías de AWS:** <https://aws.amazon.com/whitepapers>
- **Inicio rápido de AWS:** <https://aws.amazon.com/quickstart/>
 - Despliegues automatizados y de calidad en el Cloud de AWS
 - Construye tu entorno de producción rápidamente con plantillas
 - Ejemplo: WordPress en AWS https://fwd.aws/P3yyv?did=qs_card&trk=qs_card
 - Aprovecha CloudFormation
- **Soluciones AWS:** <https://aws.amazon.com/solutions/>
 - Soluciones tecnológicas vetadas para el Cloud de AWS
 - Ejemplo - AWS Landing Zone: entorno AWS seguro y multicuenta
 - <https://aws.amazon.com/solutions/implementations/aws-landing-zone/>
 - “Sustituido” por AWS Control Tower

Ecosistema AWS - AWS Support

DEVELOPER

- Acceso por correo electrónico en horario laboral a los asociados de soporte de Cloud
- Orientación general: < 24 horas laborables
- Sistema deteriorado: < 12 horas laborables

BUSINESS

- Acceso telefónico, por correo electrónico y por chat 24x7 a los ingenieros de soporte de Cloud
- Sistema de producción deteriorado: < 4 horas
- Sistema de producción averiado: < 1 hora

ENTERPRISE

- Acceso a un Gestor Técnico de Cuentas (TAM)
- Equipo de soporte de atención (para la facturación y las mejores prácticas de la cuenta)
- Caída del sistema crítico para el negocio < 15 minutos

AWS Marketplace



- Catálogo digital con miles de listados de software de **proveedores de software independientes** (3^a parte)
- Ejemplo:
 - AMI personalizada (SO personalizado, firewalls, soluciones técnicas...)
 - Plantillas de CloudFormation
 - Software como servicio
 - Contenedores
- Si compras a través de AWS Marketplace, se incluye en tu factura de AWS
- Puedes **vender tus propias soluciones** en AWS Marketplace

AWS Training

- Formación digital (online) y presencial de AWS (presencial o virtual)
- Formación privada de AWS (para tu organización)
- Formación y certificación para el Gobierno de EE.UU.
- Formación y certificación para la empresa
- Academia AWS: ayuda a las universidades a enseñar AWS
- Y tu profesor online favorito... ¡enseñándote todo sobre las Certificaciones de AWS y mucho más!

AWS Professional Services y Partner Network

- La organización de servicios profesionales de AWS es un equipo global de expertos
- Trabajan junto a tu equipo y a un miembro elegido de la APN
- APN = AWS Partner Network (Red de Socios de AWS)
- **Socios tecnológicos de APN:** proporcionan hardware, conectividad y software
- **Socios de consultoría de APN:** empresa de servicios profesionales para ayudar a construir en AWS
- **Socios de formación de APN:** encuentra quién puede ayudarte a aprender AWS
- **Programa de competencias de AWS:** las competencias de AWS se conceden a los socios de APN que han demostrado su competencia técnica y el éxito probado de sus clientes en áreas de soluciones especializadas

Centro de conocimiento de AWS

- Contiene las preguntas y peticiones más frecuentes y comunes

The screenshot shows the AWS re:Post knowledge center interface. At the top, there's a navigation bar with the AWS logo, the text "re:Post", a search bar, language selection ("Español"), resource links, and a "Iniciar sesión" button. Below the navigation is a secondary navigation bar with links for "Inicio", "Preguntas", "Centro de conocimiento" (which is highlighted), "Artículos", "Etiquetas", "Temas", and "Grupos comunitarios". A prominent orange "Hacer una pregunta" button is located on the right. The main content area has a breadcrumb trail: "Centro de conocimiento / Todos". The title "Todo el contenido del Centro de conocimiento" is displayed, along with the language setting "Idioma del contenido: Español". There are search and filter fields, and a pagination section showing "12 / página". The main content area displays six knowledge base articles in a grid:

- ¿Cómo puedo resolver errores HTTP 5xx en Amazon Keyspaces? (Oficial de AWS, Actualizada hace un mes)
- ¿Cómo puedo convertir un clúster de base de datos Multi-AZ sin cifrar en un clúster de base d... (Oficial de AWS, Actualizada hace un mes)
- ¿Cómo soluciono problemas de escalamiento automático en Amazon Keyspaces? (Oficial de AWS, Actualizada hace un mes)
- ¿Cómo puedo desplegar mi aplicación de forma segura y enrutar el tráfico a la URL de mi entorn... (Oficial de AWS, Actualizada hace un mes)
- ¿Cómo puedo usar un runbook de SAW para solucionar problemas de mi nombre de dominio... (Oficial de AWS, Actualizada hace un mes)
- ¿Por qué falló mi función de rotación Lambda de Secrets Manager con el error «El motor de base ... (Oficial de AWS, Actualizada hace un mes)

A vertical "COMENTARIOS" button is located on the right side of the article grid.

<https://repost.aws/es/knowledge-center/all>

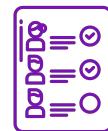
AWS IQ



- Encuentra rápidamente ayuda profesional para tus proyectos de AWS
- Contrata y paga a expertos de terceros certificados por AWS para trabajar en proyectos bajo demanda
- Videoconferencia, gestión de contratos, colaboración segura, facturación integrada
- **Para los clientes**



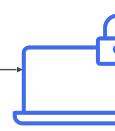
Enviar solicitud
describe tu proyecto



Revisar las respuestas
Conectar con los expertos
(requisitos y plazos)



Selecciona un experto
en función de las tarifas,
experiencia, ...



Trabaja con seguridad
Da a los expertos el acceso
adequado a tu cuenta de AWS



Cargos de pago por objetivos
añadidos en tu
factura de AWS

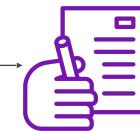
• Para los expertos



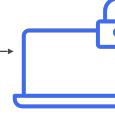
Crear foto de perfil,
biografía, certificados, ...



Conecta con los clientes



Iniciar una propuesta
descripción del trabajo, precio,
hitos, ...



Trabaja con seguridad
Consigue el acceso
adequado a la
cuenta de AWS de los clientes



Obtener el pago
Solicitar el pago después
de cumplir los objetivos

AWS re:Post



- **Servicio de preguntas y respuestas gestionado por AWS** que ofrece respuestas a tus preguntas técnicas sobre AWS, revisadas por expertos y que sustituye a los foros originales de AWS
- Forma parte de la capa gratuita de AWS
- Los miembros de la comunidad pueden ganar puntos de reputación para aumentar su estatus de experto de la comunidad proporcionando respuestas aceptadas y revisando las respuestas de otros usuarios
- **Las preguntas de los clientes de AWS Premium Support que no reciben respuesta de la comunidad se transmiten a los ingenieros de AWS Support**
- AWS re:Post no está destinado a ser utilizado para preguntas que son sensibles al tiempo o que implican cualquier información de propiedad

The screenshot shows a question titled "Import a self-signed Root CA in ACM PCA" with one accepted answer. The question asks for an example on how to import a self-signed root CA into ACM-PCA. The accepted answer provides three scenarios: 1. Installing a certificate for a root CA hosted by ACM Private CA; 2. Installing a subordinate CA certificate whose parent authority is hosted by ACM Private CA; and 3. Installing a subordinate CA certificate whose parent authority is externally hosted. The user who answered the question has a badge indicating they are an "EXPERT".

Import a self-signed Root CA in ACM PCA

I am looking for an example on how to import a self signed root CA into ACM-PCA, possibly using openssl to generate the external CA.

The documentation hasn't helped me and seems to only work for subordinate CAs.

<https://docs.aws.amazon.com/acm-pca/latest/userguide/PcaImportCaCert.html>

<https://docs.aws.amazon.com/cli/latest/reference/acm-pca/import-certificate-authority-certificate.html>

Follow Comment

1 Answers

Newest Most votes Most comments

ACCEPTED ANSWER

1 ACM Private CA supports three scenarios for installing a CA certificate : Scenario 1. Installing a certificate for a root CA hosted by ACM Private CA. Scenario 2. Installing a subordinate CA certificate whose parent authority is hosted by ACM Private CA. Scenario 3. Installing a subordinate CA certificate whose parent authority is externally hosted. It is not possible to import an external ROOT CA in ACM-PCA.

Comment

EXPERT answered a year ago EXPERT reviewed 7 days ago

AWS Managed Services (AMS)



- Proporciona soporte de infraestructuras y aplicaciones en AWS.
- **AMS ofrece un equipo de expertos en AWS** que gestionan y operan tu infraestructura para garantizar la seguridad, fiabilidad y disponibilidad.
- Ayuda a las organizaciones a descargar las tareas rutinarias de gestión y centrarse en sus objetivos empresariales.
- Servicio totalmente gestionado, por lo que AWS se encarga de actividades comunes como peticiones de cambios, monitorización, gestión de parches, seguridad y servicios de backup
- Implementa las mejores prácticas y mantiene tu infraestructura de AWS para reducir tu sobrecarga operativa y el riesgo
- El horario comercial de AMS es 24/365

AWS Managed Services (AMS)



- Seguridad mejorada
- Centrarse en la automatización
- Una normativa más estricta
- Costes de explotación reducidos
- Gestión simplificada
- Innovación sin fricciones

Preparación del examen

Nota rápida sobre los distractores

- Hay muchos servicios que encontrarás en las preguntas que son **distractores**
- Hay **más de 200 servicios de AWS**, y no podemos abarcarlos todos
 - Quicksight, Cognito, AppStreams, Server Migration Service, etc.
- He cubierto todos los servicios por los que, según mi investigación y experiencia, la gente recibe preguntas en el examen.
- Si ves un servicio que no está cubierto por mi curso, pero que aparece en el examen práctico de otra persona, no te asustes, lo habré dejado fuera intencionadamente
- Si ves un servicio que es una respuesta en el examen pero que no está cubierto en mi curso, ¡házmelo saber!

Punto de control del estado de aprendizaje

- Veamos hasta dónde hemos llegado en nuestro viaje de aprendizaje
- <https://aws.amazon.com/certification/certified-cloud-practitioner/>

La práctica hace la perfección

- Si eres nuevo en AWS, practica un poco gracias a este curso antes de lanzarte al examen
 - El examen recomienda que tengas 6 meses o más de experiencia práctica en AWS
 - ¡La práctica hace la perfección!
-
- Si te sientes abrumado por la cantidad de conocimientos que acabas de aprender, repásalos una vez más

Contenido del examen

- Dos tipos de preguntas:
 - **De opción múltiple:** tiene una respuesta correcta y tres incorrectas
 - **Respuesta múltiple:** tiene dos o más respuestas correctas de entre cinco o más opciones - ATENCIÓN: el software del examen no te dice si has seleccionado el número correcto de respuestas (pero se menciona el número requerido)
- **Intenta siempre responder a la pregunta**
 - Las preguntas no contestadas se consideran incorrectas
 - No hay penalización por una respuesta incorrecta → ¡Adivina!
- Si necesitas revisar una pregunta para más tarde (cuando hayas terminado de responder a todas las preguntas), puedes **marcarla**

PREGUNTA DE OPCIÓN MÚLTIPLE

¿Qué servicio de AWS hace...?

- Opción 1
- Opción 2
- Opción 3
- Opción 4

PREGUNTA DE RESPUESTA MÚLTIPLE

¿Pregunta blabla...? (SELECCIONA DOS)

- Opción 1
- Opción 2
- Opción 3
- Opción 4
- Opción 5

Proceder por eliminación

- La mayoría de las preguntas van a ser preguntas de alto nivel de "selección de servicios"
 - Para todas las preguntas, descarta las respuestas que sabes con seguridad que son incorrectas
 - Para las respuestas restantes, entiende cuál es la que tiene más sentido
-
- Hay muy pocas preguntas trampa
 - No lo pienses demasiado
 - Si una solución parece factible pero muy complicada, probablemente sea incorrecta

Lee la descripción general de cada servicio

- Ejemplo: <https://aws.amazon.com/s3/>
- Los resúmenes cubren muchas de las preguntas que se hacen en el examen
- Ayudan a confirmar tu comprensión de un servicio

Entra en la Comunidad AWS

- Ayudar y debatir con otras personas en las preguntas y respuestas del curso
- Revisa las preguntas formuladas por otras personas en las Preguntas y Respuestas
- Haz el test de práctica de esta sección
- Haz exámenes prácticos adicionales (por ejemplo, de mi curso de exámenes prácticos)

- Lee foros en línea
- Lee blogs en línea
- Asiste a reuniones locales y discute con otros ingenieros de AWS
- Mira vídeos en YouTube (AWS Conference)

¿Cómo funcionará el examen?

- Tendrás que inscribirte en línea en <https://www.aws.training/>
- La tasa del examen es de 100 USD
- Presenta dos documentos de identidad (DNI, tarjeta de crédito, los detalles están en los correos electrónicos que te enviamos)
- No se permiten notas, ni bolígrafo, ni hablar
- Se harán 65 preguntas en 90 minutos
- Al final puedes revisar opcionalmente todas las preguntas/respuestas

- Sabrás de inmediato si has aprobado / suspendido los exámenes
- No sabrás qué respuestas eran correctas / incorrectas
- Conocerás la puntuación global unos días después (notificación por correo electrónico)
- Para aprobar necesitas una puntuación de **al menos 700 sobre 1000**
- Si suspendes, puedes volver a hacer el examen 14 días después

Rutas de certificación de AWS - Arquitectura

Arquitectura

Arquitecto de soluciones

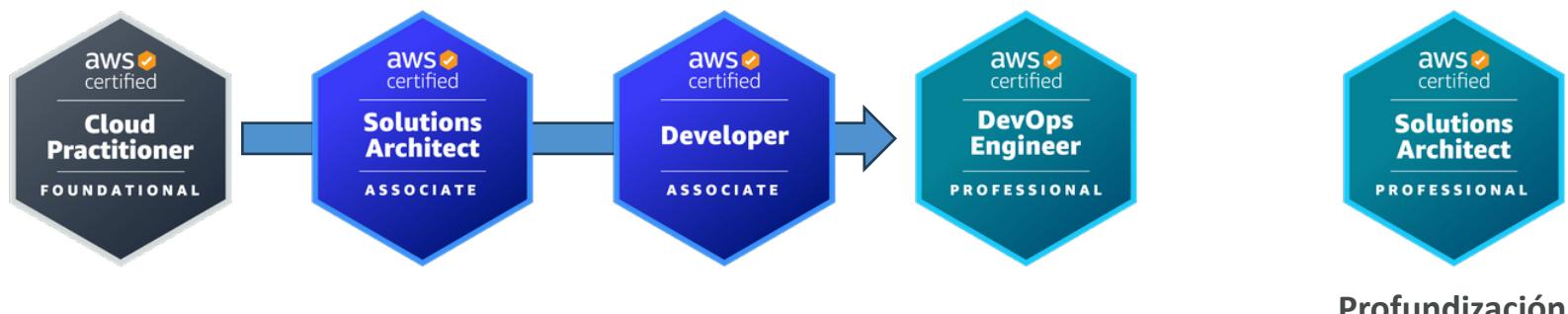
Diseña, desarrolla y gestiona infraestructura y activos en el Cloud, trabaja con DevOps para migrar aplicaciones al Cloud



Arquitectura

Arquitecto de aplicaciones

Diseñar aspectos significativos de la arquitectura de la aplicación, incluidos la interfaz de usuario, el middleware y la infraestructura, y garantizar sistemas escalables, fiables y gestionables en toda la empresa



https://d1.awsstatic.com/training-and-certification/docs/AWS_certification_paths.pdf

Rutas de certificación de AWS – Operaciones

Operaciones

Administrador de sistemas

Instalar, actualizar y mantener componentes informáticos y software, e integrar procesos de automatización



Profundización

Operaciones

Ingeniero en el Cloud

Implantar y utilizar la infraestructura informática en red de una organización e implantar sistemas de seguridad para mantener la seguridad de los datos



Profundización

Rutas de certificación AWS - DevOps

DevOps

Ingeniero de testing

Integrar las mejores prácticas de test y calidad en el desarrollo de software, desde el diseño hasta la publicación, a lo largo de todo el ciclo de vida del producto



DevOps

Ingeniero en Cloud DevOps

Diseño, despliegue y operaciones de un entorno global de Cloud Computing híbrido a gran escala, abogando por Pipelines automatizados CI/CD DevOps de extremo a extremo



Opcional

Profundización

DevOps

Ingeniero DevSecOps

Acelerar la adopción del Cloud por parte de las empresas al tiempo que permite una entrega rápida y estable de capacidades utilizando principios, metodologías y tecnologías CI/CD



Rutas de certificación AWS - Seguridad

Seguridad

Ingeniero de seguridad en el Cloud

Diseñar la arquitectura de seguridad informática y elaborar diseños detallados de ciberseguridad. Desarrollar, ejecutar y realizar un seguimiento del rendimiento de las medidas de seguridad para proteger la información



Profundización

Seguridad

Arquitecto de seguridad en el Cloud

Diseñar e implantar soluciones empresariales en el Cloud aplicando la gobernanza para identificar, comunicar y minimizar los riesgos empresariales y técnicos



Profundización

Rutas de certificación AWS - Análisis de datos y desarrollo

Análisis de datos

Ingeniero de datos en el Cloud

Automatiza la recogida y el procesamiento de datos estructurados/semiestructurados y monitoriza el rendimiento del Pipeline de datos



Profundización

Desarrollo

Ingeniero de desarrollo de software

Desarrollar, construir y mantener software en distintas plataformas y dispositivos

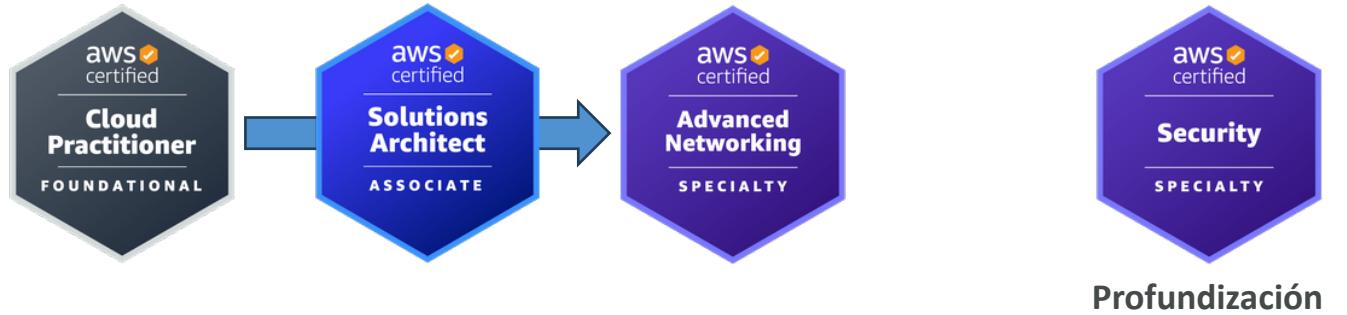


Rutas de certificación AWS - Redes y AI/ML

Redes

Ingeniero de redes

Diseñar e implantar redes informáticas y de información, como redes de área local (LAN), redes de área extensa (WAN), intranets, extranets, etc



Profundización

AI/ML

Ingeniero de Machine Learning

Investiga, construye y diseña sistemas de inteligencia artificial (IA) para automatizar modelos predictivos, y diseña sistemas, modelos y esquemas de Machine Learning



¡Enhорабуена!

Enhorabuena!

- ¡Enhorabuena por haber terminado el curso!
- Espero que apruebes el examen sin problemas ☺
- Si aún no lo has hecho, ¡nos encantaría que nos dieras una opinión!
- Si has aprobado, estaré más que contento de saber que te he ayudado
- Publícalo en las preguntas y respuestas para ayudar y motivar a otros estudiantes. ¡Comparte tus consejos!
- ¡Publícalo en LinkedIn y etiquétanos!
- ¡Espero que hayas aprendido a utilizar AWS!

Tu viaje de certificación de AWS

FOUNDATIONAL

Seis meses de conocimiento básico sobre la nube de AWS y el sector



PROFESSIONAL

Dos años de experiencia en el diseño, la operación y la solución de problemas con la nube de AWS



ASSOCIATE

Un año de experiencia solucionando problemas e implementando soluciones con la nube de AWS



SPECIALTY

Experiencia técnica en la nube de AWS de nivel Specialty según lo especificado en la guía del examen

