

# APUNTES AWS

Manuel Vergara  
2022

## Índice

TEMA 1 - Introducción a Cloud Computing.....	7
TEMA 2 - Introducción a AWS.....	10
TEMA 3 - Networking. VPC.....	12
3.1. - Objetos de una VPC.....	12
3.2. - Propiedades de VPC.....	17
3.3. - Asistente para VPC.....	17
3.4. - Borrar VPC.....	17
TEMA 4 - Máquinas virtuales y entornos de procesamiento.....	18
4.1. - Tipos de instancias.....	18
4.2. - Nitro System.....	18
4.3. - Consola EC2.....	19
4.4. - Limites en EC2 y VPC.....	20
4.5. - Lanzar una instancia.....	21
4.6. - NAT Gateway. Conectar una red privada a Internet.....	25
4.7. - Elastic IP.....	27
4.8. - Network interface.....	27
TEMA 5 - EC2 Plantillas.....	29
TEMA 6 - EC2 Instancias de tipo SPOT.....	29
TEMA 7 - EC2 Otros tipos de compras de instancias.....	31
7.1. - Saving Plans.....	31
7.2. - Instancias Reservadas.....	31
7.3. - Hosts dedicados.....	32
7.4. - Programar instancias.....	32
7.5. - Capacity Reservations.....	32
TEMA 8 - AWS CLI Cliente en modo comando de Amazon.....	34
8.1. - Instalación Linux.....	34
8.2. - Autenticación.....	34
8.3. - Ejemplo de comandos concretos.....	35
8.4. - Filtros de las filas.....	35
8.5. - Filtros de columnas. Opción Query.....	36
8.6. - Creando objetos.....	36
8.7. - Parar, arrancar y terminar una instancia.....	39
8.8. - CloudShell.....	39
TEMA 9 - EC2 Amazon Machine Image AMIs.....	40
9.1. - Crear una AMI personalizada.....	40
9.2. - Línea de comandos.....	40
9.3. - MarketPlace.....	42

TEMA 10 - EC2 Trabajar con volúmenes EBS (Elastic Bloc Store).....	43
10.1. - Particionar, formatear y montar volumen en Linux.....	44
10.2. - Particionar, formatear y montar volumen en Windows.....	47
10.3. - Snapshot de volumen.....	48
10.4. - Línea de comandos con volúmenes.....	51
TEMA 11 - EC2 Trabajar con EFS y FSX. Sistemas de ficheros compartidos.....	55
11.1. - EFS (Linux).....	55
11.2. - FSx (Windows y otros SO).....	60
11.3. - Línea de comandos.....	65
TEMA 12 - EC2 Load Balancers. Balanceadores de carga.....	69
12.1. - Target groups.....	72
12.2. - Crear el balanceador de carga ALB.....	75
12.3. - Línea de comandos ALBs.....	79
12.4. - Crear el balanceador de carga NLB.....	82
12.5. - Línea de comandos NLB.....	89
TEMA 13 - EC2 Grupos de Autoescalada. AutoScaling Groups.....	91
13.1. - Diferencias entre Launch Templates y Launch Configuration.....	91
13.2. - Crear una Launch Configuration.....	92
13.3. - Crear una Launch Template.....	93
13.4. - Crear un grupo de autoescalada.....	94
13.5. - Propiedades grupo de autoescalada.....	97
13.6. - Comportamiento del autoescalado. Prueba.....	99
13.7. - Opciones adicionales.....	102
13.8. - Política de escalado. Simple y Step.....	106
TEMA 14 - S3 Almacenamiento escalable en la nube.....	110
14.1. - Buckets.....	110
14.2. - Objetos.....	112
14.3. - Clases de almacenamiento.....	114
14.4. - Versionado.....	115
14.5. - Management – Gestión.....	117
14.6. - Acceso público.....	120
14.7. - Bloqueo objetos.....	124
14.8. - S3Browser.....	125
14.9. - Web estática en S3.....	125
14.10. - Inventario de los objetos.....	126
14.11. - Línea de comandos para S3.....	127
TEMA 15 - RDS Bases de Datos Relacionales.....	135
15.1. - Crear BBDD en RDS Standard.....	137
15.2. - Crear BBDD en RDS Easy.....	139
15.3. - Gestionar, modificar y borrar BBDD en RDS.....	139
15.4. - Opciones subnet group, parameter groups y option groups.....	140
15.5. - Propiedades y parámetros concretos según la BBDD.....	141
15.6. - Read replica.....	143
15.7. - RDS Reservadas.....	146
15.8. - CLI RDS.....	146
TEMA 16 - RDS Aurora.....	148
16.1. - Crear BBDD tipo Aurora.....	148
TEMA 17 - RDS Backup y Mantenimiento.....	157

TEMA 18 - RDS Migración de Bases de Datos.....	159
18.1. - Hacer migración.....	160
18.2. - SCT (Schema Conversion Tool).....	165
TEMA 19 - Calculadora de Precios.....	168
TEMA 20 - SNS Simple Notification Service.....	169
20.1. - Crear un servicio SNS.....	170
20.2. - Ejemplo CLI RDS.....	175
TEMA 21 - Grupo de Recursos y editor de Tags.....	177
TEMA 22 - CloudWatch. DashBoards y Métricas.....	179
22.1. - Conceptos.....	179
22.2. - Consola de CloudWatch.....	181
TEMA 23 - CloudWatch Alarmas.....	197
23.1. - Crear una alarma.....	197
TEMA 24 - CloudWatch Logs.....	202
TEMA 25 - IAM Identify Access Management. Gestión de identidades en AWS.....	210
25.1. - Consola IAM.....	212
25.2. - CLI IAM.....	220
TEMA 26 - CloudTrail: Monitorización accesos de usuarios.....	227
26.1. - AWS CLI.....	230
TEMA 27 - Cloud9 y las SDK – Entorno de desarrollo y pruebas.....	231
27.1. - Ejemplo de código python.....	233
TEMA 28 - Bases de Datos: DocumentDB.....	236
28.1. - Arquitectura.....	237
28.2. - Consola DocumentDB.....	238
28.3. - Conectar con la BBDD Mondo.....	241
28.4. - Gestión de instancias y cluster.....	245
TEMA 29 - CloudFormation. Plantillas para nuestra infraestructura.....	246
29.1. - Crear un stack.....	247
29.2. - Designer para crear una plantilla.....	250
TEMA 30 - Compute – Lightsail.....	254
TEMA 31 - Compute – Elastic Beanstalk.....	257
TEMA 32 - Compute AWS Lambda.....	261
32.1. - Conceptos.....	264
32.2. - Probando blueprint.....	265
32.3. - Ejemplo de trigger.....	266
32.4. - Ejemplo de destino.....	266
32.5. - Ejemplo con todos los pasos para crear una función, trigger y destino.....	267
32.6. - AWS Step Functions.....	268
TEMA 33 - SQS – Servicio de mensajes de Amazon.....	270
33.1. - Diferencia SNS vs SQS.....	270
33.2. - Tipos de colas de mensajes.....	270
33.3. - Crear cola standard.....	271
33.4. - Crear cola FIFO.....	273
33.5. - Cola de mensajes muertos.....	274
33.6. - Enviar y recibir desde python.....	274
TEMA 34 - EKS Elastic Kubernetes Service.....	277
34.1. - Crear un cluster.....	278
34.2. - Crear workers.....	279

34.3. - AWS CLI con EKS.....	280
34.4. - kubectl.....	282
34.5. - Borrar cluster.....	284
TEMA 35 - ECS Elastic Container Service.....	286
35.1. - Crear un cluster.....	286
35.2. - Crear una tarea.....	286
35.3. - Crear un servicio.....	288
TEMA 36 - ECR Elastic Container Registry.....	289
36.1. - Crear repositorio público.....	289
36.2. - Crear una imagen de Docker.....	290
36.3. - Probar un despliegue con LightSail.....	292
36.4. - Crear repositorio privado.....	292
36.5. - Asignar permisos de acceso.....	293
36.6. - AWS CLI.....	294
TEMA 37 - Route 53.....	297
37.1. - Dominio.....	298
37.2. - Hosted zone.....	298
37.3. - Probar zona host con una instancia.....	299
37.4. - Probar zona host con un bucket S3.....	299
37.5. - Probando subdominio.....	301
37.6. - Apuntando a un load balancer.....	302
37.7. - Health Check.....	302
37.8. - Políticas de enrutamiento.....	303
37.9. - Traffic Flow.....	305
TEMA 38 - Resumen de todos los servicios.....	307
38.1. - Administración de costes.....	307
38.2. - Computación (máquina).....	307
38.3. - Almacenamiento.....	308
38.4. - Bases de datos.....	308
38.5. - Red y contenido.....	309
38.6. - Migración.....	310
38.7. - Herramientas de desarrollo.....	310
38.8. - Herramientas de Administración.....	311
38.9. - Servicios Multimedia.....	312
38.10. - Identidad, Seguridad y Conformidad.....	312
38.11. - Analítica.....	313
38.12. - Inteligencia Artificial - Machine Learning.....	314
38.13. - Internet de las cosas (IoT).....	315
38.14. - Centro de contacto / Atención al cliente.....	315
38.15. - Desarrollo de juegos.....	315
38.16. - Servicios móviles.....	316
38.17. - AR / VR Realidad Aumentada / Realidad Virtual.....	316
38.18. - Integración de aplicaciones.....	316
38.19. - Productividad Empresarial.....	316
38.20. - Escritorio y transmisión de aplicaciones.....	317
38.21. - Blockchain.....	317
38.22. - Robótica.....	317
38.23. - Licenciamiento.....	317

38.24. - Enlaces de interés:.....317

Este documento contiene los apuntes tomados en el curso «[Amazon AWS al completo](#)» impartido por [Apasoft Training](#) en agosto y septiembre de 2022. El curso udemy consta de 46 horas aproximadamente de vídeo-tutoriales. Las prácticas aquí contenidas tuvieron una duración de alrededor de unas 220 horas.

Los apuntes no fueron pensados para compartirlos, por ello pueden tener lagunas de información o contenido adicional respecto al curso, ya que se redactaron para recordar procedimientos y conceptos que el autor creyó relevantes. Teniendo un documento, a mi parecer, tan completo y entendiendo que el conocimiento debe ser libre se decidió compartirlo.

Si te parece útil este documento puedes agradecerlo a través de las vías de contacto de la web <https://vergaracarmona.es>

Recuerda,

*"Quien se corta su propia leña se calienta dos veces"*

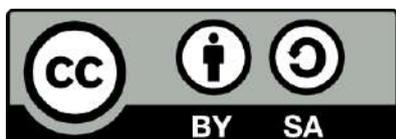


Esta obra está bajo una [Licencia Creative Commons Atribución-CompartirIgual 4.0 Internacional](#). Para ver una copia de esta licencia, visite <https://creativecommons.org/licenses/by-sa/4.0/legalcode.es>.

Usted es libre de:

- **Compartir** — copiar y redistribuir el material en cualquier medio o formato
  - **Adaptar** — remezclar, transformar y crear a partir del material para cualquier finalidad, incluso comercial.
- Bajo las condiciones siguientes:

- **Reconocimiento** — Debe reconocer adecuadamente la autoría, proporcionar un enlace a la licencia e indicar si se han realizado cambios. Puede hacerlo de cualquier manera razonable, pero no de una manera que sugiera que tiene el apoyo del licenciador o lo recibe por el uso que hace.
- **Compartir Igual** — Si remezcla, transforma o crea a partir del material, deberá difundir sus contribuciones bajo la misma licencia que el original.



- **No hay restricciones adicionales** — No puede aplicar términos legales o medidas tecnológicas que legalmente restrinjan realizar aquello que la licencia permite.



Esta licencia está aceptada para Obras Culturales Libres.  
El licenciador no puede revocar estas libertades mientras cumpla con los términos de la licencia.

# TEMA 1 - Introducción a Cloud Computing

**Cloud Computing** (nube) entrega de recursos tecnológicos bajo demanda.

NIST dice que es un modelo que permite un acceso a través de la red a un conjunto de recursos informáticos que son configurables, con aprovisamiento rápido y con la posibilidad de liberar con un mínimo esfuerzo.

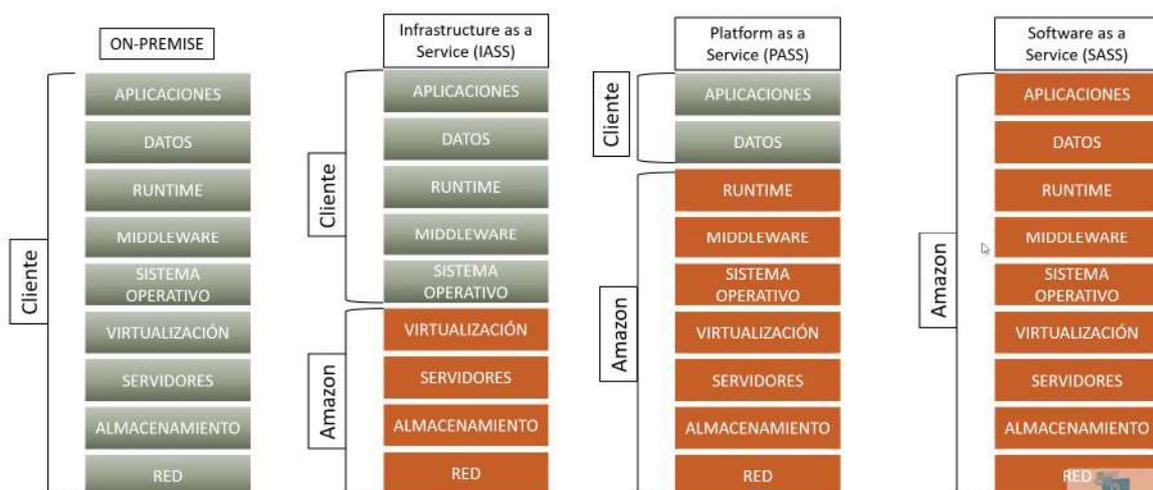
**Recursos:** Networks, Servidores, Almacenamiento, Aplicaciones, Servicios, Seguridad, Redes....

## Características:

- On-demand Self Service. Se puede solicitar los servicios bajo demanda.
- Acceso a través de internet.
- Recursos compartidos
  - Modelo multi inquilino.
  - Se asignan y reasignan dinámicamente
  - Los clientes no se preocupan por la ubicación física
- Gran escalabilidad.
- Control total sobre los gastos en servicios. Facturación al milímetro, si no se usa un servicio no se paga.

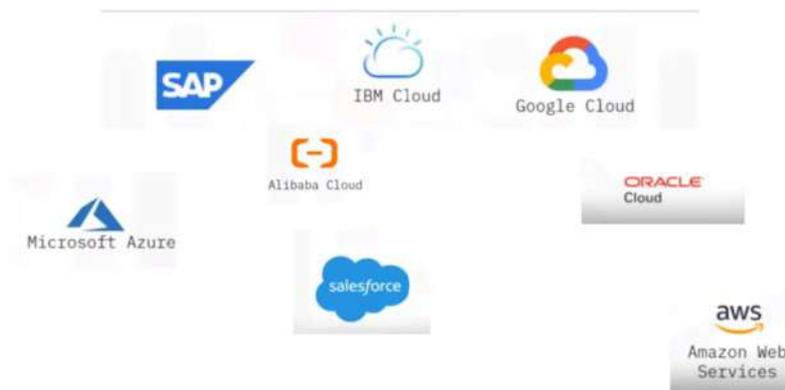
**CCaS** – Cloud Computing as a Service.

**Modos de despliegue** en los Cloud. Redes públicas, redes privadas (pueden ser on-premise) y las híbridas.



Incremento en gasto en Cloud: El mercado mundial de servicios en la nube pública crecerá.

Líderes en Cloud Computing:



Salesforce y SAP – Ofrece productos de RRHH, Gestión de ventas, gestión empresarial...

Alibaba se conoce también por Aliyun, tiene su propio nicho de mercado.

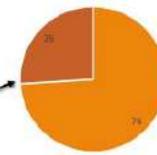
Pasar a la nube (Se han democratizado los recursos):

- Pequeñas empresas tienen a su disposición recursos antes inviables.
- Ya no es necesario una gran inversión inicial.
- Se puede mantener la competitividad
- Permite incluir tecnologías de vanguardia: Workflows, IA, Automatización, IoT, Blockchain, infraestructura híbridas/seguras, aplicaciones nuevas o heredadas, etc

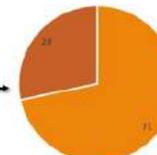
- Es una estrategia, no es la solución para todo.

- ❑ Según IBM, más de las tres cuartas partes de las empresas hoy utilizan Cloud Computing de alguna manera, permitiendo expandirse a nuevas industrias.
- ❑ El 74% ha adoptado algún servicio en Cloud nube para mejorar la experiencia del cliente
- ❑ El 71% utiliza la nube para crear productos y servicios mejorados, al tiempo que reduce simultáneamente los sistemas legacy y reduce los costos

Inversión en la nube



Mejorar sus Recursos



## TEMA 2 - Introducción a AWS

La capa gratuita de Amazon: Ofrecen al menos para un año algunos productos gratis para probar.

<https://aws.amazon.com/es/free>

Existen pruebas temporales, de 12 meses gratuitos y gratis siempre.

Regiones amazon:



Regiones google:



Una región de AWS está compuesta de **AZ** (Availability Zones. Zonas de disponibilidad) que son CPD. Aun estando separados no estarán a más de 100 millas.

También están las **localizaciones de borde** que contienen una infraestructura menos compleja que una AZ y acercan servicios a los usuarios. Cloud Front es una aplicaciones para llegar a los usuarios locales.

Las **zonas locales** están solo en EEUyU. Para la sensibilidad en latencia con servicios de BBDD, aplicaciones, etc

**Wavelength** - permite a los desarrolladores crear aplicaciones que ofrecen latencias de milisegundos de un solo dígito a dispositivos móviles y usuarios finales.

**Outposts** – Para tener HW amazon en un CPD propio y usarlo de manera híbrida, utilizando CPD propio y la nube de AWS

Motivos para seleccionar una región:

- Legales
- Precio
- Latencia. Distancia con el usuario final
- Disponibilidad de servicios.

**AWS Billing Dashboard** es la consola para controlar la facturación.

Con CloudWatch puedes crear alarmas de facturación.

Trucos para no gastar dinero en AWS:

- Utilizar la capa gratuita
- Borrar o parar los componentes una vez se haya terminado la prueba
- Utilizar instancias de tipo Spot (No se pueden utilizar en producción)

**Personal AWS Health** se utiliza para ver el estado de los servicios.

Se supone que hay una visión general de amazon pero el enlace no funciona:

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

**Trusted Advisor** da recomendaciones para posibles problemas de la infraestructura. Tiene una parte gratuita y otra de pago (El más barato unos 30USD).

Tipos de soportes: Básico, desarrollador, Empresa, Empresas con sistemas críticos y entornos críticos. <https://aws.amazon.com/es/premiumsupport/plans/>

## TEMA 3 - Networking. VPC.

Una **VPC (Virtual Private Cloud)** es un concepto virtual aislado para desplegar componentes. Es una zona de la red.

Cada VPC tiene un bloque CIDR (IPv4 o IPv6 o de ambas. Classes Inter-Domain Routing (Enrutamiento Entre Dominios Sin Clases, en castellano)). Son el conjunto de direcciones IP que se asignan a la VPC. Son direcciones privadas. Ejemplo: 10.0.0.0/16



Cada Región pueden tener distintas zonas de disponibilidad (AZ), de 2 a n zonas. Dentro de las zonas se crean las subredes que pueden ser públicas o privadas. En las subredes se distribuyen las direcciones IP de la CIDR.

### 3.1. - Objetos de una VPC

Tablas de rutas, ACLs, Subred y Gateway

#### 3.1.1. - Tablas de rutas

Nos permite indicar como será el tráfico de entrada y salida con unas reglas. La *Main route table* es la tabla por defecto, será la tabla de rutas que heredarán las subredes (Asociación implícita. Si se asigna manualmente es explícita). Las propiedades son:

- Routes.
  - Destination. Es el ámbito donde se podrá acceder.
  - Target. Es el tipo de acceso.
    - Core Network
    - Egress Only Internet Gateway
    - Instance

- Internet Gateway
- Network Interface
- Outpost Local Gateway
- Peering Connection
- Transit Gateway
- Virtual Private Gateway
- Gateway Load Balancer Endpoint
- Local
  - Propagated.
- Subnet associations
- Edge association
- Route propagation
- Tags

### 3.1.2. - ACLs

Access Control List. Reglas de entrada y salida para una VPC. La *Main Network ACL* se crea implícita con el VPC.

- Details
- Inbound rules. Permisos del tráfico que entra
  - Rule number. De inferior a superior. La primera regla es la que se aplica. \* significa cualquier entrada.
  - Type
  - Protocol
  - Port range
  - Source
  - Allow/deny
- Outbound rules. Permisos del tráfico que sale.
- Subnet associations
- Tags

### 3.1.3. - Subred

Las subredes se necesitan para trabajar dentro de una VPC y con una ACL. Cuando se crea un objeto en AWS siempre suele pedir una subnet. El VPC es el envoltorio donde se construyen las subredes y es dentro de las subredes donde se construyen las MV, BBDD, etc Con lo que no tiene sentido tener una VPC sin subredes.

Al crearla se asociará al CIDR de la VPC seleccionada. Se debe seleccionar una AZ de la región. Se debe dividir cada subnet con un rango adecuado.

Se puede calcular con las calculadoras online como <https://mxtoolbox.com/SubnetCalculator.aspx>

📊

## Subnet Calculator

/24 ▾
Calculate

Input <b>10.0.0.0/24</b>	Input IP <b>10.0.0.0</b>	Input Long <b>167772160</b>	Input Hex <b>0A.00.00.00</b>
CIDR <b>10.0.0.0/24</b>	CIDR IP Range <b>10.0.0.0 - 10.0.0.255</b>	CIDR Long Range <b>167772160 - 167772415</b>	CIDR Hex Range <b>0A.00.00.00 - 0A.00.00.FF</b>
IPs in Range <b>256</b>	Mask Bits <b>24</b>	Subnet Mask <b>255.255.255.0</b>	Hex Subnet Mask <b>FF.FF.FF.00</b>

Propiedades de una subred:

- Details
- Flow logs. Registros
- Route table. Asigna la main por defecto, de manera implícita
- Network ACL. Asigna la main por defecto, de manera implícita
- CIDR reservations. Reserva de IPs
- Sharing
- Tags

Las subredes **por defecto son privadas**, sin acceso a internet, tan solo pueden acceder a las subredes del mismo VPC.

Para que tenga acceso (sea **pública**) se deben hacer distintas cosas, como añadir el componente IG (Internet Gateway) – Elastic IP.



Además, se debe configurar la tabla de rutas (En el diagrama la AZ B). Con esto estará habilitado el tráfico tanto de entrada como de salida.

La **Elastic IP** es una IP estática pública para que nunca cambie la IP de entrada de tráfico.

### 3.1.4. - Gateway

Será la puerta de entrada con la subred que seleccionemos como pública.

Las gateway se asocian a posteriori de su creación. (Attach to VPC) Entonces se podrá asociar a cualquier subred de ese VPC, esto se hará creando una tabla de rutas.

The screenshot shows the AWS console interface for a route table named 'ruta-internet' with ID 'rtb-032416a09bf9e029a'. At the top, there is a notification banner: 'You can now check network connectivity with Reachability Analyzer' with a 'Run Reachability Analyzer' button. Below this is the 'Details' section with the following information:

Route table ID rtb-032416a09bf9e029a	Main No	Explicit subnet associations -	Edge associations -
VPC vpc-06efefd12f7a7228f   ml-vpc-prueba	Owner ID 992365247711		

Below the details are tabs for 'Routes', 'Subnet associations', 'Edge associations', 'Route propagation', and 'Tags'. The 'Routes' tab is active, showing a table with 2 routes:

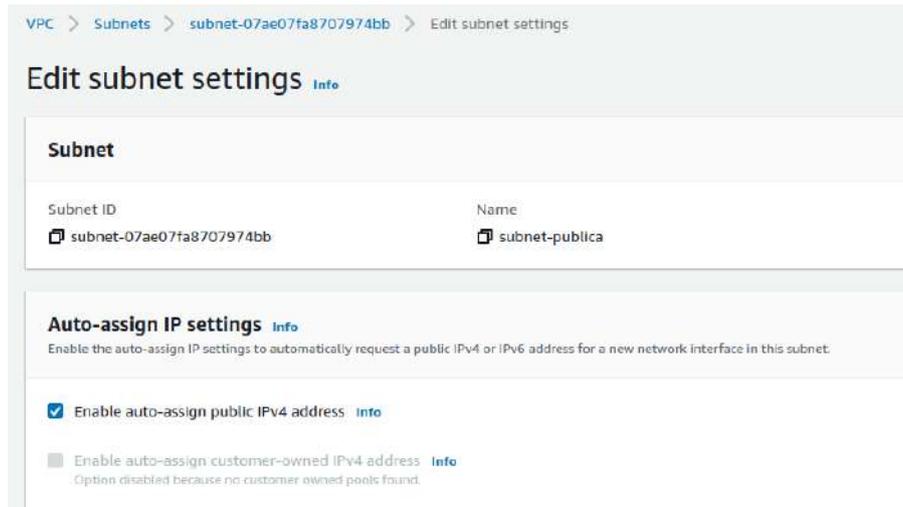
Destination	Target	Status	Propagated
0.0.0.0/0	igw-0c1d71ff63ae2143e	Active	No
10.0.0.0/24	local	Active	No

Luego se asigna la tabla de rutas a la subred pública

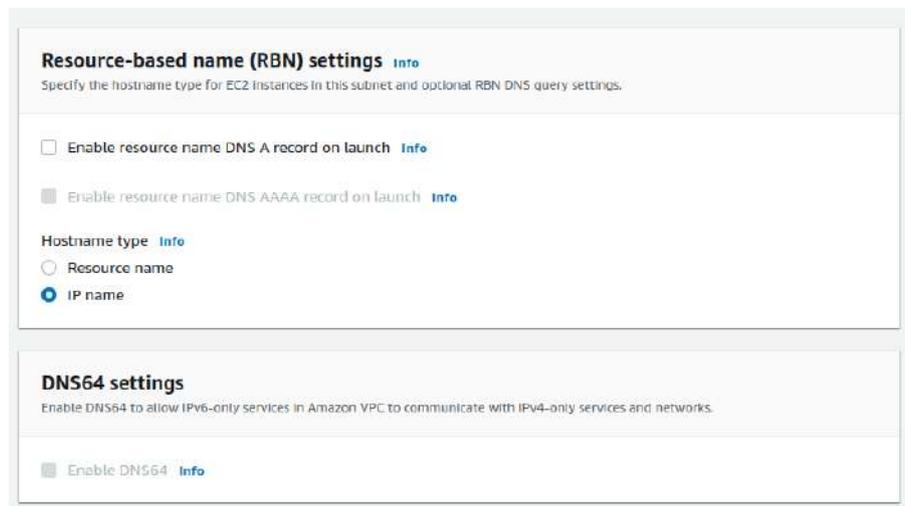
The screenshot shows the 'Subnet associations' tab in the AWS console. It displays 'Explicit subnet associations (1)'. There is a search bar and a table with the following data:

Subnet ID	IPv4 CIDR	IPv6 CIDR
subnet-07ae07fa8707974bb / subnet-publica	10.0.0.16/28	-

Además, editando las propiedades de la subnet pública podemos hacer que todas las instancias que se creen dentro de la subnet se le va a asociar una IP pública



Y se puede editar el tipo de hostname:



### 3.2. - Propiedades de VPC

CIDR, DNS hostname (debería estar activo), DNS resolution (debería estar activo), Middlebox route y tags

### 3.3. - Asistente para VPC

Se puede clicar «VPC and more» cuando creas una VPC donde tendremos una preview de la creación. Antes, con «Launch VPC Wizard», daba opciones predeterminadas de VPCs.

### 3.4. - Borrar VPC

En principio, siempre pide la confirmación del borrado con el nombre del objeto que se vaya a borrar.

Cuando borras una VPC intentará borrar todos los objetos asociados, a no ser que estén asociados a otros recursos. En algunas ocasiones, no permite borrar por alguna asociación.

## TEMA 4 - Máquinas virtuales y entornos de procesamiento

EC2 es el servicio de MV. Es una de los servicios más conocidos de AWS porque dispone de las instancias y MV necesarias para afrontar cualquier tipo de trabajo en la infraestructura de AWS.

Se ofrecen bajo distintos tipos de alquiler y de instancias.

EC2 está por debajo de muchos servicios de AWS como los de BBDD, IA, etc.

### 4.1. - Tipos de instancias

Hay muchos tipos de instancias, con lo que al principio cuesta elegir una. Soporte AWS: <https://aws.amazon.com/es/ec2/instance-types/> En la ayuda divide las instancias en grupos y estos en familias de instancias:

- De uso general, Optimizadas para informática, Optimizadas para memoria, Informática acelerada, Optimizadas para almacenamiento

También se puede ver las Características de las instancias y la Medición del rendimiento de las instancias.

El explorador va muy bien para filtrar instancias: <https://aws.amazon.com/es/ec2/instance-explorer/>

En «EC2 Dashboard» también tenemos una manera de filtrar las instancias. Em esta tabla informativa se puede ver el precio aproximado. Si marcamos una instancia veremos más detalles:

- Details, Compute, Networking, Storage, Accelators, Pricing

### 4.2. - Nitro System

Es la infraestructura con una combinación de hardware dedicado y software para que funcionen correctamente los servidores. Se usa como el motor para hacer funcionar las virtualizaciones con distintos componentes (Tarjetas, chip de seguridad, hipervisor, enclaves, TPM, ...). La plataforma subyacente para la última generación de instancias de EC2 que permite a AWS innovar con mayor rapidez, reducir aún más los costos para nuestros clientes y ofrecer más beneficios, como nuevos tipos de instancias y un nivel de seguridad superior.

Recursos del soporte de AWS (Vídeos):

- [Video: Beneficios de seguridad de la arquitectura Nitro EC2 \(pantalla de inicio\)](#)
- [Video: Beneficios de seguridad de la arquitectura Nitro EC2 \(presentación\)](#)
- [Video: Análisis profundo de Nitro \(presentación\)](#)

- [Video: Evolución de Nitro System \(presentación\)](#)
- [Blog de Jeff Barr](#)
- [Perspectives - AWS Nitro System Support for Previous Generation Instances - James Hamilton](#)

## 4.3. - Consola EC2

Recursos:

- Instancias corriendo
- Servidores dedicados
- IPs elásticas
- Instancias generales
- Pares de llaves
- Balanceadores de carga
- Placement groups
- Grupos de seguridad
- Capturas de instancias
- Volúmenes

Atributos de la cuenta:

- Documentación
- Consola de la VPC
- Encriptación EBS
- Zonas
- Numero de serie de la consola EC2
- Especificaciones por defecto
- Experimentos en consola.

Se puede lanzar una instancia o efectuar una migración.

Aparece la información de eventos programados.

Aparece un resumen del servicio en Service health

También existe una consola global de todas las regiones dentro de la cuenta: «EC2 Global view»

## 4.4. - Límites en EC2 y VPC

En limits podemos ver los límites actuales del EC2 y el VPC. Si se necesita aumentar algún límite se debe solicitar a AWS con «Request limit increase», que es un servicio de tickets. AES deberá aprobar el nuevo límite.

Se puede calcular los posibles límites con Calculate vCPU limit.

## 4.5. - Lanzar una instancia

Se puede **etiquetar** cada instancia. Con name será el nombre del objeto. Luego podemos darle un key relacionado con un value. Cada etiqueta se puede extender a otros tipos de recursos.

Una **AMI** es como una imagen ISO que se utilizan para crear las MV.

**Application and OS Images (Amazon Machine Image)** [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

**Quick Start**

Amazon Linux | Ubuntu | Windows | Red Hat | SUSE Linux

[Browse more AMIs](#)  
Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

**Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type** Free tier eligible

ami-090fa75af13c156b4 (64-bit (x86)) / ami-020ef1e2f6c2cc6d6 (64-bit (Arm))  
Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Amazon Linux 2 Kernel 5.10 AMI 2.0.20220719.0 x86\_64 HVM gp2

Architecture	AMI ID	Provider
64-bit (x86)	ami-090fa75af13c156b4	Verified provider

En principio ofrece las más habituales, pero en Browse more AMIs podemos encontrar más, con filtros de búsqueda.

Search for an AMI by entering a search term e.g. "Windows"

Quickstart AMIs (45) My AMIs (0) AWS Marketplace AMIs (6008) Community AMIs (500)

Refine results

- Clear all filters
- Free tier only info
- OS category
  - All Linux/Unix
  - All Windows
- Architecture
  - 64-bit (Arm)
  - 32-bit (x86)
  - 64-bit (x86)
  - 64-bit (Mac)
  - 64-bit (Mac-Arm)

All products (45 filtered, 45 unfiltered)

- Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type**  
ami-090fa75af13c156b4 (64-bit (x86)) / ami-020ef1e2f6c2cc6d6 (64-bit (Arm))  
Amazon Linux 2 comes with five years support. It provides Linux kernel 5.10 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras. This AMI is the successor of the Amazon Linux AMI that is now under maintenance only mode and has been removed from this wizard.  
Platform: amazon Root device type: ebs Virtualization: hvm ENA enabled: Yes
- Amazon Linux 2 AMI (HVM) - Kernel 4.14, SSD Volume Type**  
ami-0cabc39acf991f4f1 (64-bit (x86)) / ami-0201c8df31f1b7ead (64-bit (Arm))  
Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras. This AMI is the successor of the Amazon Linux AMI that is now under maintenance only mode and has been removed from this wizard.  
Platform: amazon Root device type: ebs Virtualization: hvm ENA enabled: Yes
- macOS Monterey**  
ami-07a0f396eeb97c9f (64-bit (Mac)) / ami-01a9da8de3d589094 (64-bit (Mac-Arm))

Podemos escoger entre las de inicio rápido, AMIs propias personalizadas, la del mercado de AWS y las de la comunidad.

Después se selecciona el **tipo de MV**:

Q

<b>t1.micro</b> Family: t1 1 vCPU 0.612 GiB Memory On-Demand Linux pricing: 0.02 USD per Hour On-Demand Windows pricing: 0.02 USD per Hour	Free tier eligible
<b>t2.nano</b> Family: t2 1 vCPU 0.5 GiB Memory On-Demand Linux pricing: 0.0058 USD per Hour On-Demand Windows pricing: 0.0081 USD per Hour	
<b>t2.micro</b> Family: t2 1 vCPU 1 GiB Memory On-Demand Linux pricing: 0.0116 USD per Hour On-Demand Windows pricing: 0.0162 USD per Hour	Free tier eligible
<b>t2.small</b> Family: t2 1 vCPU 2 GiB Memory On-Demand Linux pricing: 0.023 USD per Hour On-Demand Windows pricing: 0.032 USD per Hour	
<b>t2.medium</b> Family: t2 2 vCPU 4 GiB Memory On-Demand Linux pricing: 0.0464 USD per Hour On-Demand Windows pricing: 0.0644 USD per Hour	
<b>t2.large</b> Family: t2 2 vCPU 8 GiB Memory On-Demand Linux pricing: 0.0928 USD per Hour On-Demand Windows pricing: 0.1208 USD per Hour	
<b>t2.micro</b> Family: t2 1 vCPU 1 GiB Memory On-Demand Linux pricing: 0.0116 USD per Hour On-Demand Windows pricing: 0.0162 USD per Hour	Free tier eligible

Se pueden comparar el tipo de MV.

Después deberemos crear unos **pares de llaves** para poder conectarnos mediante ssh.

**Create key pair**
✕

Key pairs allow you to connect to your Instance securely.

Enter the name of the key pair below. When prompted, store the private key in a secure and accessible location on your computer. **You will need it later to connect to your instance.** [Learn more](#)

Key pair name

The name can include upto 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type

**RSA**  
RSA encrypted private and public key pair

**ED25519**  
ED25519 encrypted private and public key pair (Not supported for Windows instances)

Private key file format

**.pem**  
For use with OpenSSH

**.ppk**  
For use with PuTTY

Cancel
Create key pair

Después parametramos la **red**. Elegimos el VPC, la subnet, si asigna IP pública y grupos de seguridad.

Los **grupos de seguridad** sirven para parametrar el firewall. Lo normal es utilizar el mismo grupo a servidores con el mismo rol.

Ahora el **almacenamiento**, donde podemos escoger la capacidad y el tipo de disco.

Select

General purpose SSD (gp3)

General purpose SSD (gp2)

Provisioned IOPS SSD (io1)

Provisioned IOPS SSD (io2)

Cold HDD (sc1)

Throughput Optimized HDD (st1)

Magnetic (standard)

gp es gama media con un precio razonable.

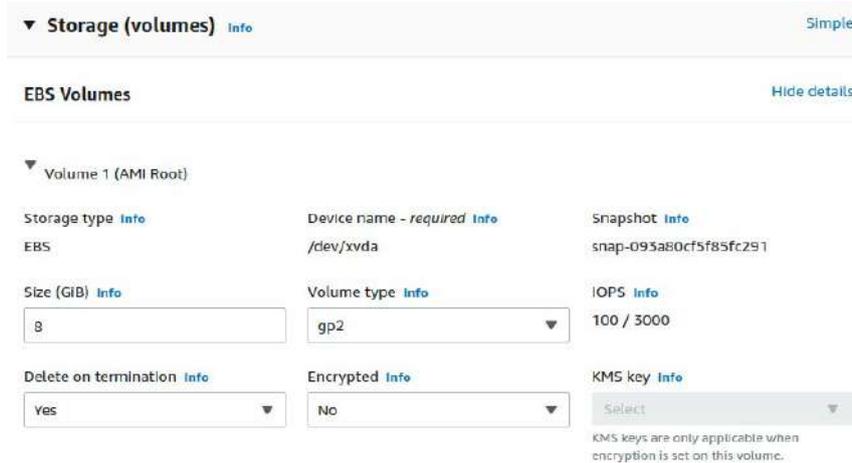
io se usa cuando necesitas un procesamiento de entrada y salida rápido.

sc es el viejo HDD

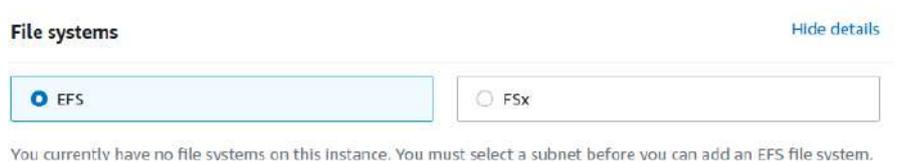
st es un HDD optimizado

Magnetic es un tipo de disco antiguo.

En avanzado vemos más datos:



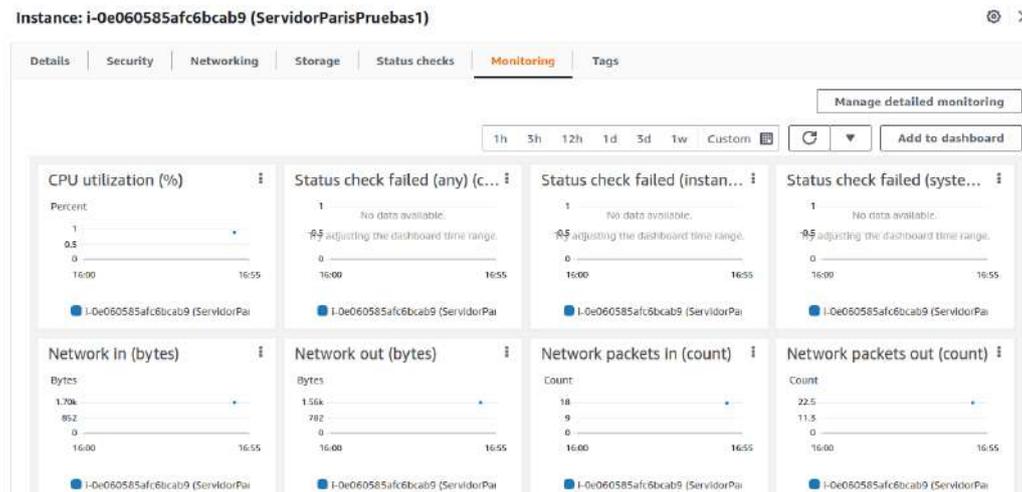
También se puede escoger el **sistema de ficheros**



Por último, en detalles avanzados se puede escoger algunos elementos y parámetros más.

En los **atributos** de la instancia creada encontraremos:

- Detalles, Seguridad, la red, el almacenamiento, el estado, monitorización y sus etiquetas.



Las **monitorizaciones** se pueden añadir en un panel general que se crea en CloudWatch.

Los **Estados** de las instancias pueden ser: Parado, encendida, reiniciando, hibernación y terminada.

Hay una diferencia entre parar/arrancar y reboot. Si paras y arrancas se cambia la IP y el nombre por defecto de la máquina.

Para una **IP estática** se necesita pagar una Elastic IP.

Para conectarse a las instancias desde internet necesitamos la IP pública. Podemos ir en la parte superior a Conect para ver las opciones que tenemos. Las opciones en MV Linux son:

- EC2 Instance Connect – A través de un navegador. No todas las instancias lo permiten.
- Session Manager – Con un agente de conexión
- SSH client – La tradicional
- EC2 serial console -

En las MV de Amazon Linux el usuario suele ser ec2-user. En Debian root. En Centos Centos.

Las opciones en MV Windows son:

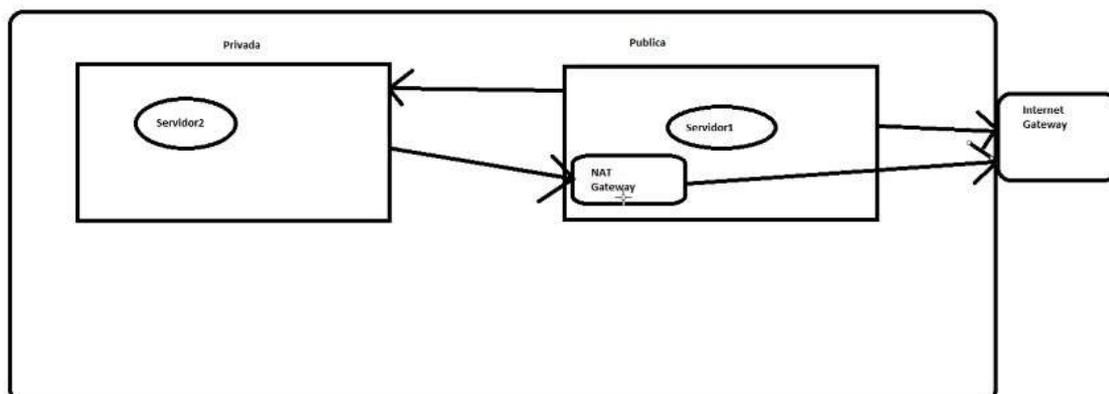
- Session Manager – Con un agente de conexión
- RDP client – La tradicional. Se deberá descargar el archivo rdp.
- EC2 serial console -

Ejemplo de instalación de Apache en Amazon Linux 2:

```
sudo yum update
sudo yum install httpd
sudo systemctl start httpd
sudo systemctl enable httpd
sudo systemctl status httpd
```

## 4.6. - NAT Gateway. Conectar una red privada a Internet

NAT Gateway es un componente para poder conseguir que una red privada llegue a Internet conectándose de manera segura a Internet Gateway. Hace de pasarela habilitando o deshabilitando el tráfico. De esta manera no se exponen todos los componentes de la red privada.



Deberemos generar una Elastic IP. Cuidado que son de pago.

Tendremos una instancia en la subnet pública y otra en la privada. Podremos conectarnos desde la instancia de la subnet pública a la instancia de la subnet privada.

Ahora activamos el NAT Gateway en la instancia de la subnet pública. Para crearla debemos estar en la VPC. La NAT deberá estar en la red pública. Podrá ser pública o privada. Las privadas pueden ser para conectarse entre las VPC.

La crearemos en la red pública.

**Create NAT gateway** [Info](#)

A highly available, managed Network Address Translation (NAT) service that instances in private subnets can use to connect to services in other VPCs, on-premises networks, or the Internet.

**NAT gateway settings**

**Name - optional**  
Create a tag with a key of 'Name' and a value that you specify.

gateway1

The name can be up to 255 characters long.

**Subnet**  
Select a subnet in which to create the NAT gateway.

subnet-07ae07fa8707974bb (subnet-publica)

**Connectivity type**  
Select a connectivity type for the NAT gateway.

Public  
 Private

**Elastic IP allocation ID** [Info](#)  
Assign an Elastic IP address to the NAT gateway.

eipalloc-0f91fcdf589f7551f [Allocate Elastic IP](#)

Para asociarla se debe hacer en la tabla de rutas de la subnet privada.

VPC > Route tables > rtb-0011f9d7df9a87433 > Edit routes

**Edit routes**

Destination	Target	Status	Propagated
10.0.0.0/24	local	Active	No
0.0.0.0/0	-	-	No

[Add route](#)

Q |

- Core Network
- Egress Only Internet Gateway
- Gateway Load Balancer Endpoint
- Instance
- Internet Gateway
- local
- NAT Gateway
- Network Interface
- Outpost Local Gateway
- Peering Connection
- Transit Gateway
- Virtual Private Gateway

Cancel [Preview](#) [Save changes](#)

Ahora ya podremos conectarnos como antes y actualizar la instancia de la subnet privada porque ya tendremos internet.

## 4.7. - Elastic IP

Creamos una en “Allocate Elastic IP address”. Una vez creada la debemos asociar, lo podemos hacer a una Instancia en concreto o a una Network Interfaces. En ambos casos hay que decir la IP privada a la que estará asociada.

**Associate Elastic IP address**

Choose the Instance or network Interface to associate to this Elastic IP address (13.36.101.155)

**Elastic IP address: 13.36.101.155**

**Resource type**  
Choose the type of resource with which to associate the Elastic IP address.

Instance

Network interface

**Warning:** If you associate an Elastic IP address to an instance that already has an Elastic IP address associated, this previously associated Elastic IP address will be disassociated but still allocated to your account. [Learn more](#)

**Instance**

**Private IP address**  
The private IP address with which to associate the Elastic IP address.

**Reassociation**  
Specify whether the Elastic IP address can be reassociated with a different resource if it already associated with a resource.

Allow this Elastic IP address to be reassociated

Cuando accederemos a la Elastic IP estará directamente conectada con la IP privada.

La Elastic IP se puede desasociar. Después se le puede dar un release.

## 4.8. - Network interface

Suelen empezar por eni (Elastic Network Interfaces). Son tarjetas de red. Se pueden tener varias tarjetas de red, pero según la AMI se pueden tener más o menos. También hay un límite global de las tarjetas que se pueden tener.

Instance type	Maximum network interfaces	Private IPv4 addresses per interface	IPv6 addresses per interface
t2.nano	2	2	2
t2.micro	2	2	2
t2.small	3	4	4
t2.medium	3	6	6
t2.large	3	12	12
t2.xlarge	3	15	15
t2.2xlarge	3	15	15

Para crear una tarjeta de red se crean en Network Interfaces. Crear una nueva, se pondrá el nombre, se escogerá la subnet y se puede escoger la IP o que la asigne automáticamente.

**Description - optional**

A descriptive name for the network interface.

**Subnet**

The subnet in which to create the network interface.

**Private IPv4 address**

The private IPv4 address to assign to the network interface.

Auto-assign

Custom

IPv4 address

También escogeremos el grupo de seguridad.

Después la seleccionaremos y asociamos con Attach a cualquier instancia de la subnet.

Para desasociar la Tarjeta de red es con Detach.

Una misma interfaces puede asignar más de una IP.

Las Elastic IP se pueden asociar con la interfaz que creamos.

## TEMA 5 - EC2 Plantillas

Se pueden crear plantillas para lanzar las mismas instancias.

Se pueden anidar las plantillas, basarse en una plantilla para crear una segunda.

El tipo de instancia se puede seleccionar dando unos mínimos y máximos de CPU y memoria, siempre y cuando se use Spot Fleet, Auto Scale o EC2 Fleet.

Para lanzar una instancia con la plantilla tan solo hay que seleccionarlo.

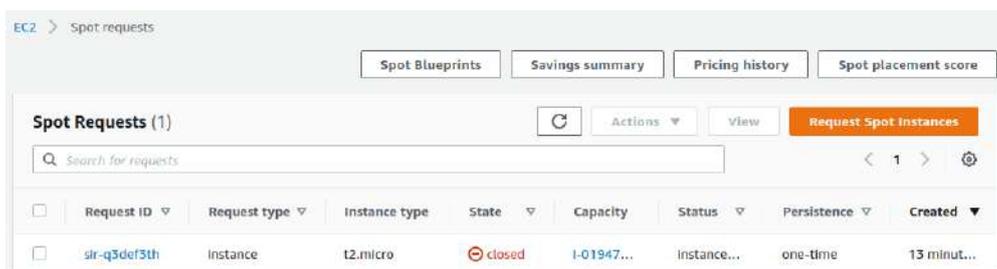
Las plantillas pueden tener versiones modificando la plantilla. Se puede seleccionar una versión como predeterminada. Estas versiones también se pueden eliminar.

Se puede crear un Spot Fleet y un Auto Scaling group

## TEMA 6 - EC2 Instancias de tipo SPOT

Hasta ahora se ha visto instancias bajo demanda. Las de tipos SPOT son MV que no se pueden parar, se pueden directamente eliminar pero no detener. Son MV más baratas que las normales.

Tiene una sección de Spot Request donde se pueden pedir una Spot. Puede que no la concedan si no hay recursos para ellos.

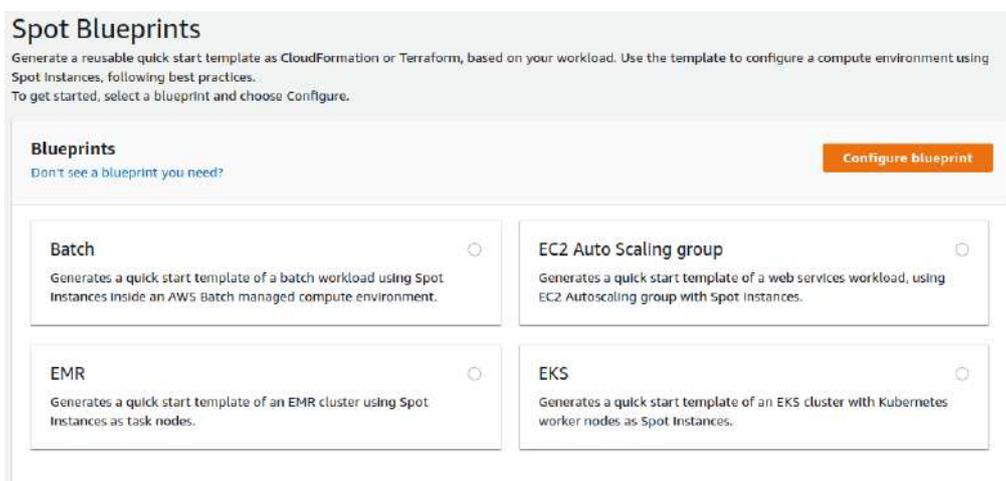


The screenshot shows the AWS Spot Requests console. At the top, there are tabs for 'Spot Blueprints', 'Savings summary', 'Pricing history', and 'Spot placement score'. Below the tabs, there's a section for 'Spot Requests (1)' with a search bar and a 'Request Spot Instances' button. A table below shows the details of the request:

Request ID	Request type	Instance type	State	Capacity	Status	Persistence	Created
sir-q3def3th	Instance	t2.micro	closed	1-01947...	Instance...	one-time	13 minut...

Si Amazon en un momento dado necesita estos recursos te puede tumbar la máquina.

Con Spot Blueprints son plantilla CloudFormation o Terraform:



The screenshot shows the AWS Spot Blueprints console. It features a 'Configure blueprint' button and a list of available blueprints:

- Batch**: Generates a quick start template of a batch workload using Spot Instances inside an AWS Batch managed compute environment.
- EC2 Auto Scaling group**: Generates a quick start template of a web services workload, using EC2 Autoscaling group with Spot Instances.
- EMR**: Generates a quick start template of an EMR cluster using Spot Instances as task nodes.
- EKS**: Generates a quick start template of an EKS cluster with Kubernetes worker nodes as Spot Instances.

Cuando se solicita un Spot se pueden pedir EBS optimizado para mejorar el rendimiento de los discos, se puede añadir la monitorización de CloudWatch.

El Tenancy es para escoger si la queremos en una máquina compartida o dedicada.

Se puede especificar comandos Linux para que se ejecuten en el momento que se arranque

Un Fleet es una flota de instancias, se pueden crear varias instancias al mismo tiempo.

En la capacidad podemos parametrizar algunas características

**Target capacity**

**Total target capacity**  
Set your total target capacity (number of instances or vCPUs) to launch. If you specified a launch template, you can allocate part of the target capacity as On-Demand. The number of On-Demand instances always persists, while Spot instances can be scaled.

1 Instances

Include On-Demand base capacity  
Allocate part of target capacity as On-Demand instances

Maintain target capacity  
Automatically replace interrupted Spot instances

**Interruption behavior**  
Terminate

Capacity rebalance  
When a rebalance notification is sent to a Spot instance, Spot Fleet automatically attempts to replace the instance before it is interrupted. [Learn More](#)

**Instance replacement strategy**  
Launch only  
Fleet only launches a replacement instance and will not terminate the instance that receives the rebalance recommendation. You ca...

Set maximum cost for Spot instances  
Set the maximum amount per hour that you're willing to pay for all the Spot instances in your fleet

Set your max cost (per hour)  
\$

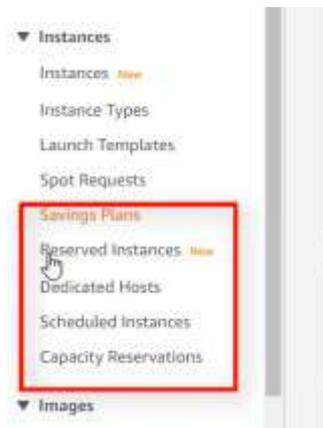
Se puede interrumpir un SPOT

- si los recursos de esas instancias AWS lo necesita para otro servicio que no sea SPOT o que considere prioritario.
- si supera el precio que se ha estimado.

Además de terminate, se puede parar o hibernar. Pero será Amazon quien la reinicie cuando tenga la capacidad de recursos o del precio que hemos dicho. Se conservará el disco y demás pero todo lo temporal se pierde.

También existe la opción para la capacidad de balanceo, con la que AWS buscará un sustituto para el disco que se termine. Dos opciones: Launch only o Launch before terminate.

## TEMA 7 - EC2 Otros tipos de compras de instancias



### 7.1. - Saving Plans

Se contrata un plan para ahorrar respecto a las máquinas on-demand. Es un servicio que se llama AWS Cost Management. En la primera visita al servicio no te permite ver las opciones hasta que no pasen 24 horas. Ofrece tres tipos:

- **Compute:** Los que tienen que ver con el procesamiento. Mayor flexibilidad en EC2, Aws Fargate y AWS Lambda. Este plan es independiente de la familia de la instancia, la región, la AZ o tenancy...
- **EC2 Instance:** Solo con EC2 e indicando la máquina y la región.
- **SageMaker:** Son los productos que se utilizan para machine learning.

Los pagos pueden ser por adelantado, parciales o sin adelantar, cada opción tiene sus ventajas.

Se puede hacer estimaciones con «recomendaciones». Estos planos son para entornos estáticos, monolíticos, donde la estructura a penas cambie. Así se hacen cálculos aproximados.

### 7.2. - Instancias Reservadas

Van bien cuando se necesita un servidor 24 horas los 7 días de la semana.

Seller	Term	Effective rate	Upfront price	Hourly rate	Payment option	Offering class	Quantity available	Desired quantity	Normalized units per hour
AWS	12 months	\$0.007	\$61.00	\$0.000	All upfront	Standard	Unlimited	1	0.5
AWS	12 months	\$0.009	\$78.00	\$0.000	All upfront	Convertible	Unlimited	1	0.5
AWS	12 months	\$0.007	\$0.00	\$0.007	No upfront	Standard	Unlimited	1	0.5
AWS	12 months	\$0.010	\$0.00	\$0.010	No upfront	Convertible	Unlimited	1	0.5
AWS	12 months	\$0.007	\$31.00	\$0.004	Partial upfront	Standard	Unlimited	1	0.5
AWS	12 months	\$0.009	\$40.00	\$0.005	Partial upfront	Convertible	Unlimited	1	0.5

Se pueden hacer convertible para poder cambiar la máquina, pero solo aumentando. Reservando la instancia AWS te cobra igual si la tienes encendida o apagada.

### 7.3. - Hosts dedicados

Es lo mismo que las instancias pero en este caso es un host específico en donde solo estarán las instancias de la misma familia que se creen, sin espacio para otros usuarios.

Se pueden marcar autoemplazamiento. Sirve para alojar aquí cada vez que se lance una instancia de la familia escogida en el host dedicado.

Precios: <https://aws.amazon.com/es/ec2/dedicated-hosts/pricing/> Se pueden calcular los precios por hora de cada tipo de host dedicada.

La cuota de los límites en las cuentas, por defecto, es 0. Con lo cual, para crear un host dedicado se debe pedir a AWS que cambie los límites. Se hace en Limits.

Con “Config recording” se guarda un registro del uso de las máquinas y todos sus cambios de configuración. Así se puede tener un registro de las licencias.

### 7.4. - Programar instancias

Ya no están activas. Es una opción que ha quitado AWS. Eran similares a las instancias reservadas pero se podía configurar un horario concreto de uso.

### 7.5. - Capacity Reservations

Es una manera de reservar las capacidad de tener un cierto tipo de máquinas dedicadas para contratar. Te cobran como si tuvieras una máquina encendida.

Precios: [https://docs.aws.amazon.com/es es/AWSEC2/latest/UserGuide/capacity-reservations-pricing-billing.html](https://docs.aws.amazon.com/es_es/AWSEC2/latest/UserGuide/capacity-reservations-pricing-billing.html)

Esta opción es lógico cuando se planea tener una máquina muy grande, ya que así te aseguras tener esa máquina disponible en el momento que se necesite. Sin necesidad de esperar que AWS la pueda ofrecer.

Las reservas se pueden programar para que terminen en un momento concreto.

Una vez se tiene una reserva de capacidad, se debe indicar al crear la instancia que se va a utilizar dicha reserva, empezando por indicar la subred donde se encuentra y el tipo de máquina. La reserva debe tener configurado autoemplazar cualquier instancia.

O bien, crear la instancia desde la misma reserva.

## TEMA 8 - AWS CLI Cliente en modo comando de Amazon

Ayuda: <https://aws.amazon.com/es/cli/>

Documentación: <https://docs.aws.amazon.com/cli/index.html>

Referencia de comandos: <https://awscli.amazonaws.com/v2/documentation/api/latest/reference/index.html>

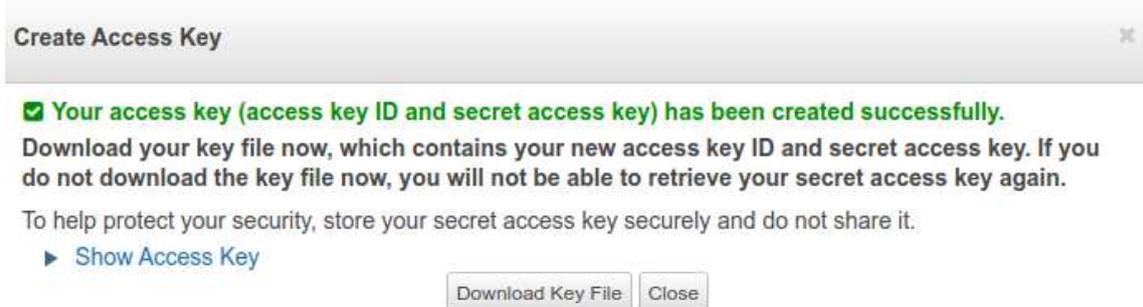
### 8.1. - Instalación Linux

```
curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"
unzip awscliv2.zip
sudo ./aws/install
```

Para ver la versión: `aws --version`

### 8.2. - Autenticación

Para autenticarse, en la barra superior, clicando en el nombre de usuario aparece una opción de credenciales: "Security Credentials". Hay varios tipos de credenciales. Para CLI podemos usar Access Keys que contienen un Access Key ID y la clave. Esta clave es personal e intransferible, se pueden tener 2.



Access Key ID: AKIA6ODMT7TPSMXRMNYK  
Secret Access Key: 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

Ahora, en la línea de comandos:

```
aws configure
```

Pedirá 4 datos: El ID de la clave, la clave, la region por defecto y el formato de salida por defecto (text, table, json, etc Por defecto es texto.)

```
administrador@ubuntudocker:~$ aws configure
AWS Access Key ID [None]: AKIA60DMT7TPSMXRMNYK
AWS Secret Access Key [None]: D1aUP7g+OX9IHZ1IU4nB+00YdZNu9VnAbpswjm/
Default region name [None]: eu-west-3
Default output format [None]:
administrador@ubuntudocker:~$
```

Para probar que funciona podemos ver las instancias:

```
aws ec2 describe-instances
```

En la carpeta de usuario se crea la carpeta .aws con dos documentos: config y credentials

```
administrador@ubuntudocker:~$ cat .aws/c
config      credentials
administrador@ubuntudocker:~$ cat .aws/config
[default]
region = eu-west-3
administrador@ubuntudocker:~$ cat .aws/credentials
[default]
aws_access_key_id = AKIA60DMT7TPSMXRMNYK
aws_secret_access_key = D1aUP7g+OX9IHZ1IU4nB+00YdZNu9VnAbpswjm/
administrador@ubuntudocker:~$
```

### 8.3. - Ejemplo de comandos concretos

Poniendo help detrás de la opción deseada nos aparecerá ayuda concreta del comando o el subcomando.

Ver la vpc:

```
aws ec2 describe-vpcs
```

Formatos con --output:

yaml	Los guiones significan listas.
text	Texto plano
table	En una tabla (En Windows no saca los colores y se debe añadir --color off)

Ver las subnets:

```
aws describe-subnets
```

### 8.4. - Filtros de las filas

Filtrar según los datos que queremos mostrar.

Ejemplo de opciones del subcomando describe-subnets:

[--filters <value>] Filtrar elementos (ver opciones:

<https://awscli.amazonaws.com/v2/documentation/api/latest/reference/ec2/describe-subnets.html#options>) Se debe seguir las opciones de la doc. Ejemplo sintaxis general:

```
aws ec2 describe-subnets --filters "Name=state, Values=available" "Name=vpc-id, Values=vpc-06efefd12f7a7228f"
```

`[--subnet-ids <value>]`                   Mostrar una subnet o varias por Ids  
`[--dry-run | --no-dry-run]`  
`[--cli-input-json | --cli-input-yaml]`  
`[--starting-token <value>]`               A partir de qué elemento se empieza a listar  
`[--page-size <value>]`                    Determinar el tamaño de la página  
`[--max-items <value>]`                    Máximo de elementos a visualizar  
`[--generate-cli-skeleton <value>]`

## 8.5. -        **Filtros de columnas. Opción Query**

Filtrar según los metadatos que queremos mostrar.

El comando es `--query`

Ejemplos para filtrar subnets:

Filtrar subnets por array (Empieza en 0)

```
aws ec2 describe-subnets --query 'Subnets[1]'
```

Filtrar por rango del array

```
aws ec2 describe-subnets --query 'Subnets[1:3]'
```

Filtrar por key del array. El punto concatena el query

```
aws ec2 describe-subnets --query 'Subnets[*].AvailabilityZone'
```

Filtrar dos campos de dentro del array

```
aws ec2 describe-subnets --query 'Subnets[][SubnetId, CidrBlock]'
```

En VPC. Filtrar con tres columnas

```
aws ec2 describe-vpcs --query 'Vpcs[][VpcId,State,IsDefault]' --output table
```

Poner labels para identificar los campos

```
aws ec2 describe-vpcs --query 'Vpcs[][{"Id de VPC":VpcId},{Estado:State},IsDefault]'
```

Si se pone labels en todos los campos se puede mostrar como tabla:

```
aws ec2 describe-vpcs --query 'Vpcs[][{"Id de VPC":VpcId},{Estado:State},{"VPC por defecto":IsDefault}]' --output table
```

## 8.6. -        **Creando objetos**

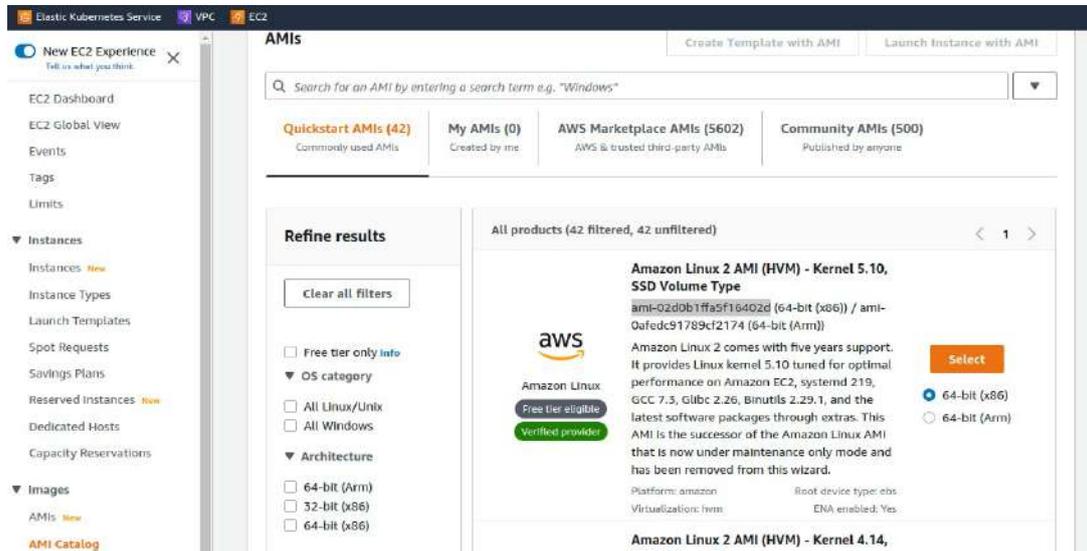
Ayuda: <https://awscli.amazonaws.com/v2/documentation/api/latest/reference/ec2/run-instances.html>

Para crear una instancia se utiliza el subcomando `run-instances` que tiene las siguientes opciones:

`[--block-device-mappings <value>]`  
`[--image-id <value>]`

[--instance-type <value>] Tipo de instancia, familia, que se va a utilizar  
 [--ipv6-address-count <value>]  
 [--ipv6-addresses <value>]  
 [--kernel-id <value>]  
 [--key-name <value>] Este es el Key Pair que se desea  
 [--monitoring <value>]  
 [--placement <value>]  
 [--ramdisk-id <value>]  
 [--security-group-ids <value>]  
 [--security-groups <value>] Grupo de seguridad  
 [--subnet-id <value>]  
 [--user-data <value>]  
 [--additional-info <value>]  
 [--client-token <value>]  
 [--disable-api-termination | --enable-api-termination]  
 [--dry-run | --no-dry-run]  
 [--ebs-optimized | --no-ebs-optimized]  
 [--iam-instance-profile <value>]  
 [--instance-initiated-shutdown-behavior <value>]  
 [--network-interfaces <value>]  
 [--private-ip-address <value>]  
 [--elastic-gpu-specification <value>]  
 [--elastic-inference-accelerators <value>]  
 [--tag-specifications <value>]  
 [--launch-template <value>]  
 [--instance-market-options <value>]  
 [--credit-specification <value>]  
 [--cpu-options <value>]  
 [--capacity-reservation-specification <value>]  
 [--hibernation-options <value>]  
 [--license-specifications <value>]  
 [--metadata-options <value>]  
 [--enclave-options <value>]  
 [--private-dns-name-options <value>]  
 [--maintenance-options <value>]  
 [--disable-api-stop | --no-disable-api-stop]  
 [--count <value>] Se indica el número de instancia que se desea  
 [--secondary-private-ip-addresses <value>]  
 [--secondary-private-ip-address-count <value>]  
 [--associate-public-ip-address | --no-associate-public-ip-address]  
 [--cli-input-json | --cli-input-yaml]  
 [--generate-cli-skeleton <value>]

Para crear una instancia se necesita la ID de un AMI (Imágenes de máquina de Amazon).



Copio la ID del AMI que quiera usar: ami-02d0b1ffa5f16402d

Luego se debe indicar el tipo de instancia, la Key Pair y el grupo de seguridad. Además indicamos cuantas instancias queremos. Ejemplo:

```
aws ec2 run-instances --image-id ami-02d0b1ffa5f16402d --instance-type t3.micro --key-name ServidorPruebasAWS2 --security-groups ServidoresWEB --count 1
```

Se comprueba en la consola web que se ha creado la instancia. En la consola se puede comprobar con el subcomando describe-instances. Por ejemplo, puede ver el Id, el estado y la fecha de lanzamiento.

```
aws ec2 describe-instances --query 'Reservations[].Instances[].[{"Id de la instancia":InstanceId},{Estado:State.Name},{"Fecha de lanzamiento":LaunchTime}]' --output table
```

DescribeInstances		
Estado	Fecha de lanzamiento	Id de la instancia
stopped	2022-08-16T23:49:22+00:00	i-0e060585afc6bcab9
shutting-down	2022-08-17T14:43:31+00:00	i-00a3750814c5340e9
stopped	2022-08-12T18:38:37+00:00	i-0cee5531268123695

Para saber el nombre de una instancia:

```
aws ec2 describe-instances --query 'Reservations[].Instances[].[{Nombre:Tags[?Key==`Name`]][0].Value},{ID:InstanceId},{Estado:State.Name}]' --output table
```

## 8.7. - Parar, arrancar y terminar una instancia

Ejemplo de Stop

```
aws ec2 stop-instances --instance-ids i-00a3750814c5340e9
```

Ejemplo de start con query

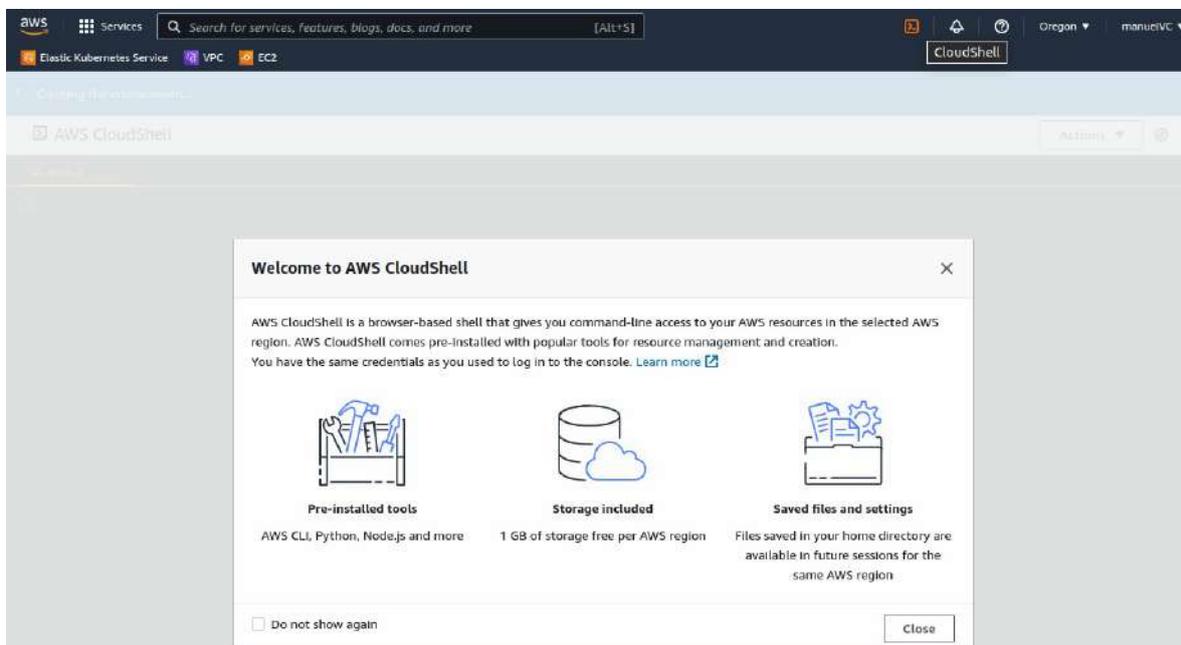
```
aws ec2 start-instances --instance-ids i-00a3750814c5340e9
```

Ejemplo de Terminar

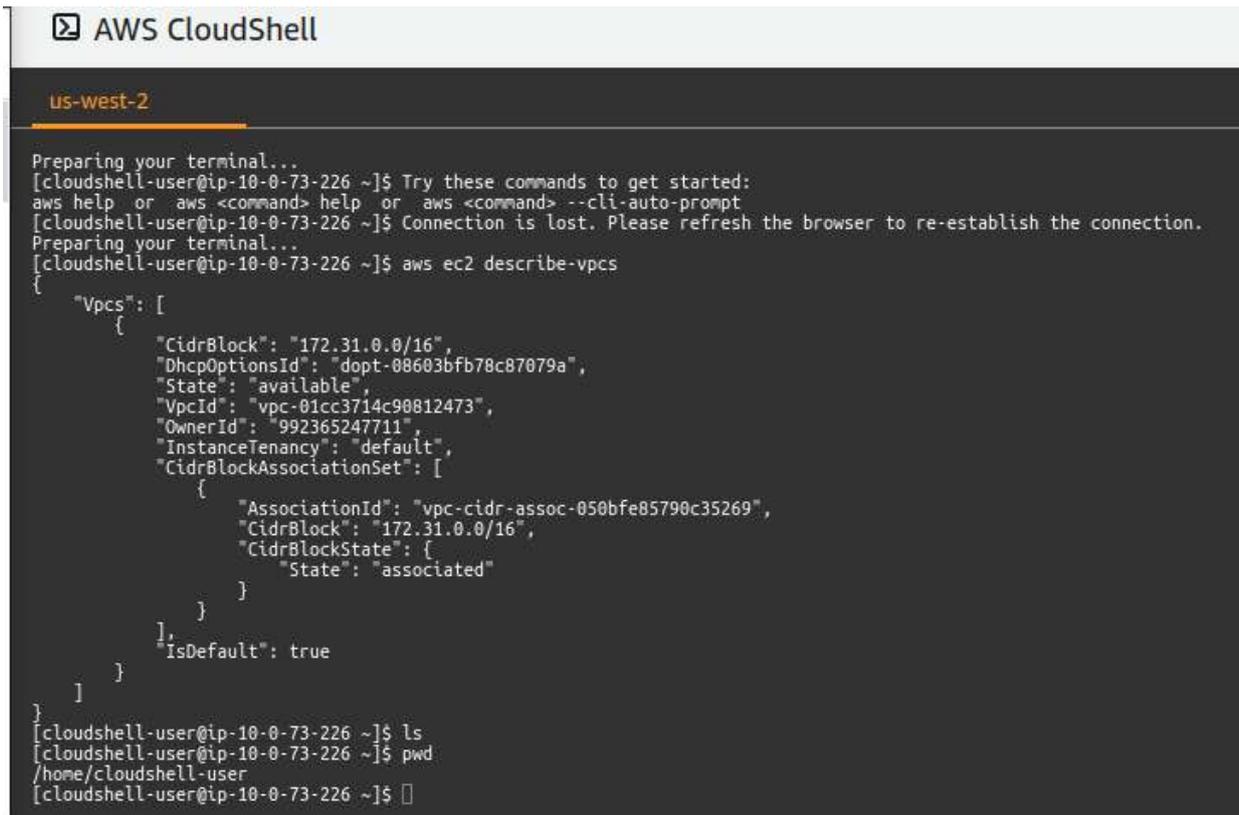
```
aws ec2 terminate-instances --instance-ids i-00a3750814c5340e9
```

## 8.8. - CloudShell

Es un entorno preparado para lanzar comandos, una shel en entorno navegador. No todas las AZ tienen esta opción. Aparece en la barra superior, al lado de las notificaciones



Es útil porque te guarda hasta un 1 GB de información por usuario, con lo cuál se puede abrir en cualquier navegador



```

AWS CloudShell

us-west-2

Preparing your terminal...
[cloudshell-user@ip-10-0-73-226 ~]$ Try these commands to get started:
aws help or aws <command> help or aws <command> --cli-auto-prompt
[cloudshell-user@ip-10-0-73-226 ~]$ Connection is lost. Please refresh the browser to re-establish the connection.
Preparing your terminal...
[cloudshell-user@ip-10-0-73-226 ~]$ aws ec2 describe-vpcs
{
  "Vpcs": [
    {
      "CidrBlock": "172.31.0.0/16",
      "DhcpOptionsId": "dopt-08603bfb78c87079a",
      "State": "available",
      "VpcId": "vpc-01cc3714c90812473",
      "OwnerId": "992365247711",
      "InstanceTenancy": "default",
      "CidrBlockAssociationSet": [
        {
          "AssociationId": "vpc-cidr-assoc-050bfe85790c35269",
          "CidrBlock": "172.31.0.0/16",
          "CidrBlockState": {
            "State": "associated"
          }
        }
      ]
    }
  ],
  "IsDefault": true
}
[cloudshell-user@ip-10-0-73-226 ~]$ ls
[cloudshell-user@ip-10-0-73-226 ~]$ pwd
/home/cloudshell-user
[cloudshell-user@ip-10-0-73-226 ~]$ █

```

## TEMA 9 - EC2 Amazon Machine Image AMIs

En el catalogo salen divididas por 4 grupos: Quickstart, my AMIs, Marketplace y Community.

Los filtros son muy extensos.

Una vez seleccionada se puede crear una instancia o una plantilla.

### 9.1. - Crear una AMI personalizada

Se puede crear una AMI como si fuera una ISO, con unos programas concretos que se necesiten desplegar en todas las instancias.

Una vez instaladas las necesidades se selecciona la instancia y en Action/image and templates/create image podemos crear nuestra imagen. Lo que hará es crear un snapshot de la imagen.

Entonces estará en nuestras AMIs. En esta sección se pueden encontrar las imágenes propias, las que se han compartido conmigo y las públicas.

### 9.2. - Línea de comandos

Para ver las AMIs es con el siguiente comando

```
aws ec2 describe-images --owner self
```

La opción --owner self se debe poner para que tan solo salga las AMIs propias y no todas a las que se tiene acceso, que son todas las públicas.

Ejemplo con una query compleja

```
aws ec2 describe-images --owner self --query 'Images[].[{"ID imagen":ImageId}, {"Nombre":Name}, {"ID SnapShot":BlockDeviceMappings[.Ebs.SnapshotId}]'
```

```
administrador@ubuntu:~$ aws ec2 describe-images --owner self --query 'Images[].[{"ID
imagen":ImageId}, {"Nombre":Name}, {"ID SnapShot":BlockDeviceMappings[.Ebs.SnapshotId}]'
[
  [
    {
      "ID imagen": "ami-06a2ad98d6849aa2f"
    },
    {
      "Nombre": "EntornoLinuxDesarrolloWeb"
    },
    {
      "ID SnapShot": [
        "snap-0789fa5d444a32b64"
      ]
    }
  ]
]
```

Crear una AMI desde una instancia que este corriendo. Primero hay que examinar la ID de la instancia de la que se quiere crear el AMI.

```
aws ec2 describe-instances
```

Se podrá filtrar con --query o --filter para localizar la instancia concreta. Luego hacemos el comando:

```
aws ec2 create-image --instance-id i-0e060585afc6bcab9 --name AMIpersonalizadaConWeb
```

Para comprobar si es correcto con query

```
aws ec2 describe-images --owner self --query "Images[].[Name,ImageId,BlockDeviceMappings[.Ebs.SnapshotId,State]"
```

```
administrador@ubuntu:~$ aws ec2 describe-images --owner self --query "Images[].[Name,ImageId,BlockDeviceMappings[.Ebs.SnapshotId,State]"
[
  [
    "AMIpersonalizadaConWeb",
    "ami-05c1cbc05794e8801",
    [
      "snap-022a0c4ecbac3a1eb"
    ],
    "available"
  ],
  [
    "EntornoLinuxDesarrolloWeb",
    "ami-06a2ad98d6849aa2f",
    [
      "snap-0789fa5d444a32b64"
    ],
    "available"
  ]
]
```

### **9.3. - MarketPlace**

En el buscador de servicios podemos encontrar “AWS Marketplace Subscriptions” para gestionar las suscripciones a las AMIs en la que nos hemos suscrito, encontrar AMIs,

Cada producto tiene su página de suscripción con los detalles del producto. Hay curiosidades como bitname que ofrece Wordpress de manera gratuita pero en la suscripción te avisa que AWS te va a cobrar por la infraestructura, la instancia.

## TEMA 10 - EC2 Trabajar con volúmenes EBS (Elastic Bloc Store)

Un tipo de almacenamiento, un disco virtual que se asocia a una instancia para poder trabajar con él. Para crear un disco en una MV tan solo hay que añadir un volumen EBS. Hay que tener en cuenta cuando se crea una instancia si queremos que el volumen se llame igual tenemos que extender el tag al volumen.

En los volúmenes se pueden ver los detalles, el Status Check, la monitorización de algunos parámetros y los tags.

Para añadir un volumen a una instancia primero iremos a “Volumes” y lo crearemos.

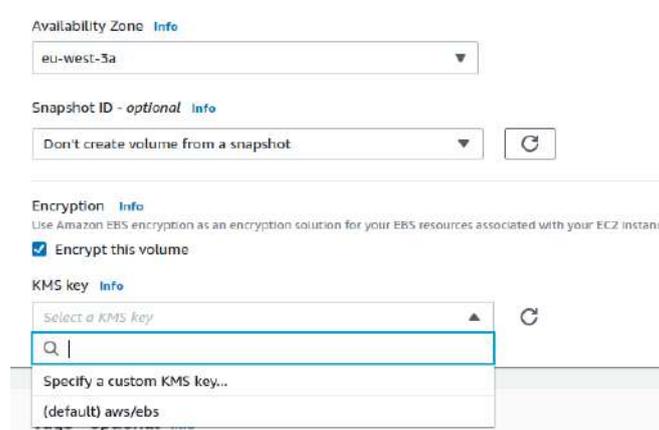
Tipos de discos:

- General purpose SSD. (gp) Los más habituales.
- Provisioned IOPS SSD (io) – Con latencia baja, es para trabajos de mucho tráfico de entrada y salida.
- Throughput Optimized HDD (st) – Disco magnetico de bajo coste. Para procesos secuenciales.
- Cold HDD (sc) – Disco magnetico de bajo coste. Para datos cold, que no tenga consultas. Como para backups o datos que se quieran guardar a largo plazo.
- Magnetic - Disco magnetico de bajo coste

AWS da el dato IOPS, que es el número solicitado de operaciones de E/S por segundo que el volumen puede soportar.

Hay que asegurarse que el volumen está en la misma AZ que la instancia a la que le queremos asociar.

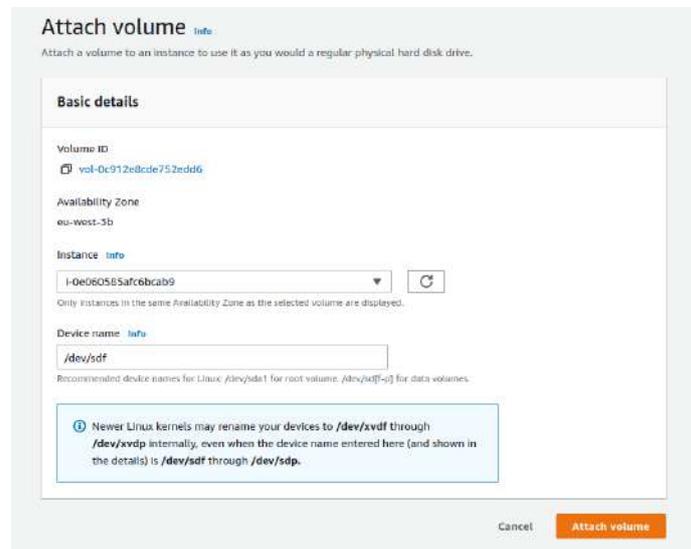
Se puede crear un volumen haciendo una copia de un snapshot. Además, también se puede encriptar.



The screenshot shows the AWS console interface for creating an EBS volume. It includes the following elements:

- Availability Zone:** A dropdown menu set to "eu-west-3a".
- Snapshot ID:** A dropdown menu set to "Don't create volume from a snapshot", with a refresh button to its right.
- Encryption:** A section with the heading "Encryption" and a sub-heading "Use Amazon EBS encryption as an encryption solution for your EBS resources associated with your EC2 instance". A checkbox labeled "Encrypt this volume" is checked.
- KMS key:** A dropdown menu set to "Select a KMS key", with a refresh button to its right. A search bar is visible below the dropdown, and a list of options is shown, including "Specify a custom KMS key..." and "(default) aws/ebs".

Para asociar el disco se debe hacer un “Attach volume” en el menú de Actions con el disco seleccionado. Seleccionamos la instancia y nos dará un nombre por defecto.



Una vez asociado el disco habrá que particionarlo, formatearlo y montarlo en el SO.

## 10.1. - Particionar, formatear y montar volumen en Linux

Entramos por ssh en la terminal y vemos los disco montados con

```
df -h
```

Y podemos ver los discos SSD disponibles con

```
ls -l /dev/sd*
```

Primero debemos particionarlo usando fdisk

```
sudo fdisk /dev/sdf
```

Entrará en un prompt de fdisk del disco y podemos ver los posibles comandos con la ayuda con m:

DOS (MBR)

- a toggle a bootable flag
- b edit nested BSD disklabel
- c toggle the dos compatibility flag

Generic

- d delete a partition
- F list free unpartitioned space
- l list known partition types
- n add a new partition
- p print the partition table
- t change a partition type

- v verify the partition table
- i print information about a partition

#### Misc

- m print this menu
- u change display/entry units
- x extra functionality (experts only)

#### Script

- I load disk layout from sfdisk script file
- O dump disk layout to sfdisk script file

#### Save & Exit

- w write table to disk and exit
- q quit without saving changes

#### Create a new label

- g create a new empty GPT partition table
- G create a new empty SGI (IRIX) partition table
- o create a new empty DOS partition table
- s create a new empty Sun partition table

Con p veremos particiones pero en este caso no tiene

```
Command (m for help): p
Disk /dev/sdf: 5 GiB, 5368709120 bytes, 10485760 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xffa7e4eb

Command (m for help):
```

Con n crearemos una nueva partición y le decimos que es Primary, la partición 1, que empiece al principio y acabe al final (Los parámetros que vienen por defecto)

```
Command (m for help): n
Partition type
  p primary (0 primary, 0 extended, 4 free)
  e extended (container for logical partitions)
Select (default p): p
Partition number (1-4, default 1): q
Value out of range.
Partition number (1-4, default 1): 1
First sector (2048-10485759, default 2048):
Last sector, +sectors or +size{K,M,G,T,P} (2048-10485759, default 10485759):

Created a new partition 1 of type 'Linux' and of size 5 GiB.

Command (m for help):
```

Ahora, dándole a la p para que enseñe las particiones se verá la creada

```

Command (m for help): p
Disk /dev/sdf: 5 GiB, 5368709120 bytes, 10485760 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xffa7e4eb

Device      Boot Start      End  Sectors  Size Id Type
/dev/sdf1   2048 10485759 10483712   5G 83 Linux
Command (m for help): █

```

Con `w` guardaremos la tabla de particiones y sale del prompt. Podemos ver la partición con `ls -l /dev/sd*`

```

Command (m for help): w
The partition table has been altered.
Calling ioctl() to re-read partition table.
Syncing disks.

[ec2-user@ip-10-0-0-29 ~]$ ls -l /dev/sd*
lrwxrwxrwx 1 root root 4 Aug 19 16:26 /dev/sda -> xvda
lrwxrwxrwx 1 root root 5 Aug 19 16:26 /dev/sda1 -> xvda1
lrwxrwxrwx 1 root root 4 Aug 19 16:55 /dev/sdf -> xvdf
lrwxrwxrwx 1 root root 5 Aug 19 16:55 /dev/sdf1 -> xvdf1

```

Ahora hay que formatearlo con `mkfs`.

```

[ec2-user@ip-10-0-0-29 ~]$ mkfs
mkfs      mkfs.ext2  mkfs.ext4  mkfs.minix  mkfs.vfat
mkfs.cramfs  mkfs.ext3  mkfs.fat   mkfs.msdos  mkfs.xfs
[ec2-user@ip-10-0-0-29 ~]$ █

```

Usaremos el formato `xfs`, que dice que es el más moderno ¿? Es el sistema de ficheros que suele usar RHEL <https://es.wikipedia.org/wiki/XFS> No parece tener mucha diferencia con Ext.

`mkfs.xfs /dev/sdf1`

```

[ec2-user@ip-10-0-0-29 ~]$ sudo mkfs.xfs /dev/sdf1
meta-data=/dev/sdf1             isize=512    agcount=4, agsize=327616 blks
=                               sectsz=512   attr=2, projid32bit=1
=                               crc=1       finobt=1, sparse=0
data      =                       bsize=4096  blocks=1310464, imaxpct=25
=                               sunit=0    swidth=0 blks
naming    =version 2              bsize=4096  ascii-ci=0 ftype=1
log       =internal log         bsize=4096  blocks=2560, version=2
=                               sectsz=512  sunit=0 blks, lazy-count=1
realtime  =none                 extsz=4096  blocks=0, rtextents=0
[ec2-user@ip-10-0-0-29 ~]$ █

```

Ahora tenemos que montar el disco con

`mkdir /mnt/disco2`

`mount /dev/sdf1 /mnt/disco2`

Y con `df` veremos el disco montado

```
[ec2-user@ip-10-0-0-29 ~]$ sudo mkdir /mnt/disco2
[ec2-user@ip-10-0-0-29 ~]$ sudo mount /dev/sdf1 /mnt/disco2
[ec2-user@ip-10-0-0-29 ~]$ df -h
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        474M   0  474M   0% /dev
tmpfs           483M   0  483M   0% /dev/shm
tmpfs           483M  476K  483M   1% /run
tmpfs           483M   0  483M   0% /sys/fs/cgroup
/dev/xvda1      8.0G  1.9G  6.2G  24% /
tmpfs           97M   0   97M   0% /run/user/1000
tmpfs           97M   0   97M   0% /run/user/0
/dev/xvdf1      5.0G   38M  5.0G   1% /mnt/disco2
```

Ahora ya podremos trabajar con el disco.

## 10.2. - Particionar, formatear y montar volumen en Windows

Cuando se asocia se puede poner la etiqueta en Device name, que es diferente a la de Linux

**Attach volume** [info](#)

Attach a volume to an instance to use it as you would a regular physical hard disk drive.

**Basic details**

Volume ID  
vol-052f901090e1ef31f (Windows1-a)

Availability Zone  
us-west-2b

Instance [info](#)  
i-03e1ac410e394f2ba

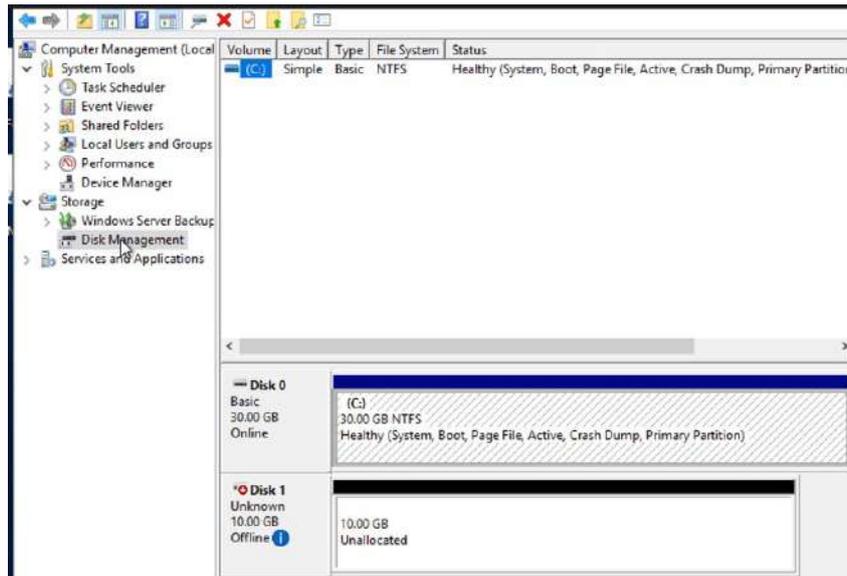
Only instances in the same Availability Zone as the selected volume are displayed.

Device name [info](#)  
xvdf

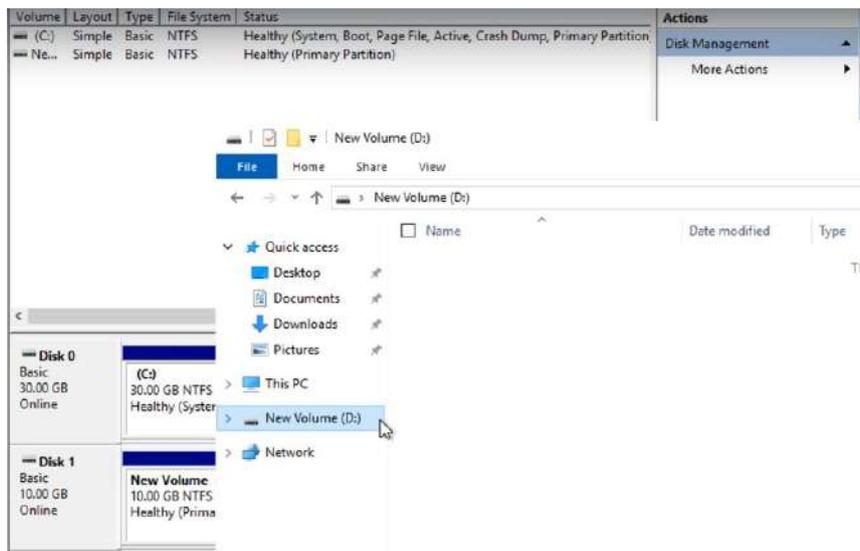
Windows device names: xvdf through xvdp.

Cancel **Attach volume**

Entramos en Computer Management (Administrador del servidor), en Disk Managememt (Administrador de disco) y veremos el disco como desconocido.

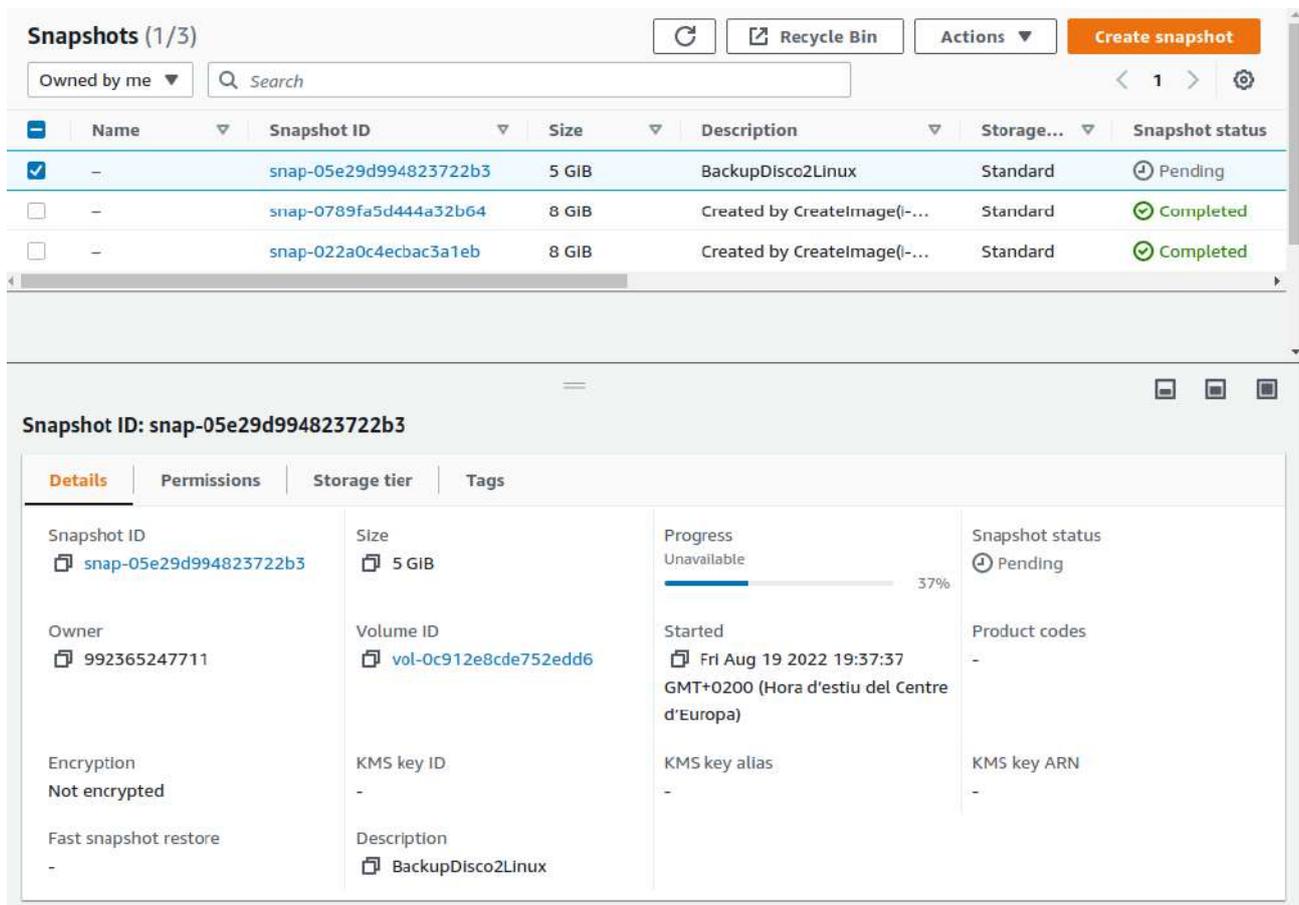
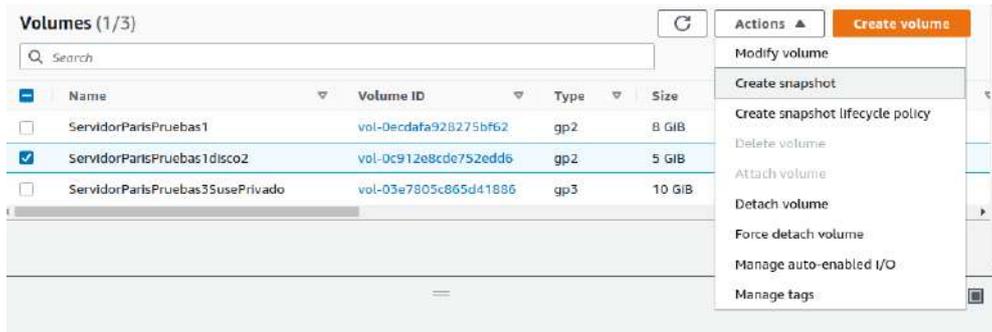


Clicamos con el secundario, lo ponemos online. Secundario de nuevo y se inicializa con MBR. Y luego creamos un volumen simple con el tamaño por defecto completo, con la letra que queramos y formato NTFS y la etiqueta que queramos.

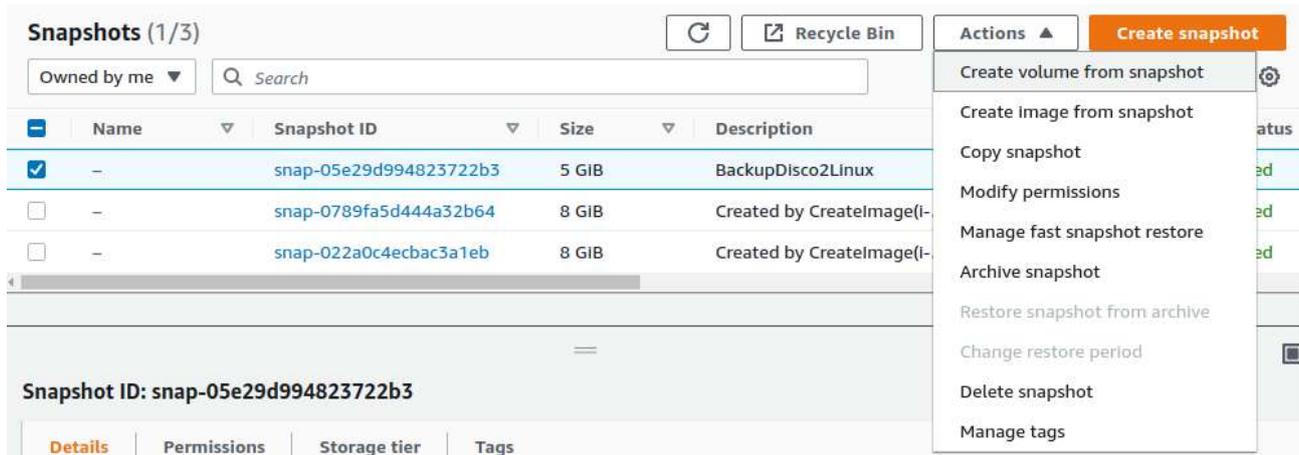


### 10.3. - Snapshot de volumen

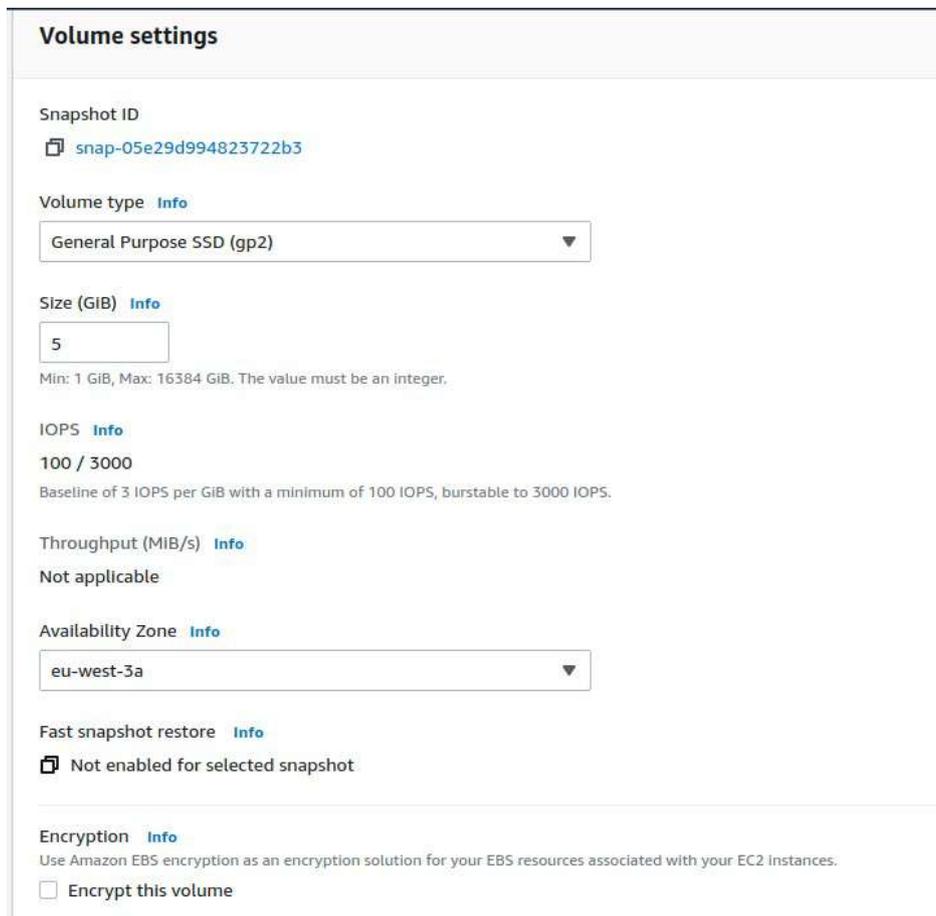
Guardará el disco tal y como lo tengamos en ese momento, con toda la información. Se crea así:



Ahora se puede crear un volumen a través de este snapshot.



Se podrá crear un disco más grande. Hay que seleccionar la zona correcta donde este la instancia a donde lo queremos asociar.



Cuando lo asociemos el SO detectará el formato del volumen.

Después, para borrar el volumen hay que borrar la instancia o desasociar y borrar el volumen.

Las snapshot se pueden borrar con facilidad. Si tenemos AMIs propias habrán Snapshot asociadas a esas AMIs, porque AWS las guarda así. Estas no se pueden borrar desde snapshot

## 10.4. - Línea de comandos con volúmenes

Podemos ver los volúmenes con

```
aws ec2 describe-volumes
```

Para ver solo los ids de los volúmenes

```
aws ec2 describe-volumes --query 'Volumes[].VolumeId'
```

Y para ver a donde están asociadas

```
aws ec2 describe-volumes --query 'Volumes[].[{"Id del Volumen":VolumeId},{ "ID instancia asociada":Attachments[].InstanceId}]'
```



```
administrador@ubuntudocker:~$ aws ec2 describe-volumes --query 'Volumes[].[{"Id del Volumen":VolumeId}, {"ID instancia asociada":Attachments[].InstanceId}]'
[
  [
    {
      "Id del Volumen": "vol-0ecdafa928275bf62"
    },
    {
      "ID instancia asociada": [
        "i-0e060585afc6bcab9"
      ]
    }
  ],
  [
    {
      "Id del Volumen": "vol-03e7805c865d41886"
    },
    {
      "ID instancia asociada": [
        "i-0cee5531268123695"
      ]
    }
  ]
]
```

Para crear un volumen es con el sub-comando create-volume que tiene estas opciones:

```
--availability-zone <value>
[--encrypted | --no-encrypted]
[--iops <value>]
[--kms-key-id <value>]
[--outpost-arn <value>]
[--size <value>]
[--snapshot-id <value>]
[--volume-type <value>]
[--dry-run | --no-dry-run]
[--tag-specifications <value>]
[--multi-attach-enabled | --no-multi-attach-enabled]
[--throughput <value>]
```

```
[--client-token <value>]
[--cli-input-json | --cli-input-yaml]
[--generate-cli-skeleton <value>]
```

Tendremos que poner la AZ que debe ser la misma de la instancia a la que queremos asociarla.

Ejemplo:

```
aws ec2 create-volume --availability-zone eu-west-3b --size 5 --volume-type gp2
```

```
administrador@ubuntudocker:~$ aws ec2 create-volume --availability-zone eu-west-3b --size 5 --volume-type gp2
{
  "AvailabilityZone": "eu-west-3b",
  "CreateTime": "2022-08-19T18:13:12+00:00",
  "Encrypted": false,
  "Size": 5,
  "SnapshotId": "",
  "State": "creating",
  "VolumeId": "vol-0c956f9595c594bb9",
  "Iops": 100,
  "Tags": [],
  "VolumeType": "gp2",
  "MultiAttachEnabled": false
}
```

Ahora ya aparece en el listado de volúmenes, pero sin instancia asociada

```
aws ec2 describe-volumes --query 'Volumes[. [{"Id del Volumen":VolumeId}, {"Estado asociación a Instancia":Attachments[].State}, {"ID instancia asociada":Attachments[].InstanceId}]' --output yaml
```

```
administrador@ubuntudocker:~$ aws ec2 describe-volumes --query 'Volumes[. [{"Id del Volumen":VolumeId}, {"Estado asociación a Instancia":Attachments[].State}, {"ID instancia asociada":Attachments[].InstanceId}]' --output yaml
- - Id del Volumen: vol-0ecdafa928275bf62
  - Estado asociación a Instancia:
    - attached
    - ID instancia asociada:
      - i-0e060585afc6bcab9
- - Id del Volumen: vol-0c956f9595c594bb9
  - Estado asociación a Instancia: []
  - ID instancia asociada: []
- - Id del Volumen: vol-03e7805c865d41886
  - Estado asociación a Instancia:
    - attached
    - ID instancia asociada:
      - i-0cee5531268123695
```

Para asociarlo es con el sub-comando attach-volume que tiene estas opciones:

```
--device <value>
--instance-id <value>
--volume-id <value>
[--dry-run | --no-dry-run]
[--cli-input-json | --cli-input-yaml]
[--generate-cli-skeleton <value>]
```

El comando queda así:

```
aws ec2 attach-volume --device /dev/sdf --instance-id i-0e060585afc6bcab9 --volume-id vol-0c956f9595c594bb9
```

Y ahora ya podemos ver la asociación

```

administrador@ubuntu:~$ aws ec2 attach-volume --device /dev/sdf --instance-id i-0e060585afc6bcab9 --volume-id vol-0c956f9595c594bb9
{
  "AttachTime": "2022-08-19T18:26:18.050000+00:00",
  "Device": "/dev/sdf",
  "InstanceId": "i-0e060585afc6bcab9",
  "State": "attaching",
  "VolumeId": "vol-0c956f9595c594bb9"
}
administrador@ubuntu:~$ aws ec2 describe-volumes --query 'Volumes[][{"Id del Volumen":VolumeId}, {"Estado asociación a Instancia":Attachments[].State}, {"ID instancia asociada":Attachments[].InstanceId}]' --output yaml
- Id del Volumen: vol-0ecdaf928275bf62
- Estado asociación a Instancia:
  - attached
- ID instancia asociada:
  - i-0e060585afc6bcab9
- Id del Volumen: vol-0c956f9595c594bb9
- Estado asociación a Instancia:
  - attached
- ID instancia asociada:
  - i-0e060585afc6bcab9
- Id del Volumen: vol-03e7805c865d41886
- Estado asociación a Instancia:
  - attached
- ID instancia asociada:
  - i-0cee5531268123695
administrador@ubuntu:~$

```

Para dettach

```

[--device <value>]
[--force | --no-force]
[--instance-id <value>]
--volume-id <value>
[--dry-run | --no-dry-run]
[--cli-input-json | --cli-input-yaml]
[--generate-cli-skeleton <value>]

```

aws ec2 detach-volume --volume-id vol-0c956f9595c594bb9

```

administrador@ubuntu:~$ aws ec2 detach-volume --volume-id vol-0c956f9595c594bb9
{
  "AttachTime": "2022-08-19T18:26:17+00:00",
  "Device": "/dev/sdf",
  "InstanceId": "i-0e060585afc6bcab9",
  "State": "detaching",
  "VolumeId": "vol-0c956f9595c594bb9"
}
administrador@ubuntu:~$ aws ec2 describe-volumes --query 'Volumes[][{"Id del Volumen":VolumeId}, {"Estado asociación a Instancia":Attachments[].State}, {"ID instancia asociada":Attachments[].InstanceId}]' --output yaml
- Id del Volumen: vol-0ecdaf928275bf62
- Estado asociación a Instancia:
  - attached
- ID instancia asociada:
  - i-0e060585afc6bcab9
- Id del Volumen: vol-0c956f9595c594bb9
- Estado asociación a Instancia:
  - detaching
- ID instancia asociada:
  - i-0e060585afc6bcab9
- Id del Volumen: vol-03e7805c865d41886
- Estado asociación a Instancia:
  - attached
- ID instancia asociada:
  - i-0cee5531268123695
administrador@ubuntu:~$

```

Para borrar es delete-volume

```
--volume-id <value>  
[--dry-run | --no-dry-run]  
[--cli-input-json | --cli-input-yaml]  
[--generate-cli-skeleton <value>]
```

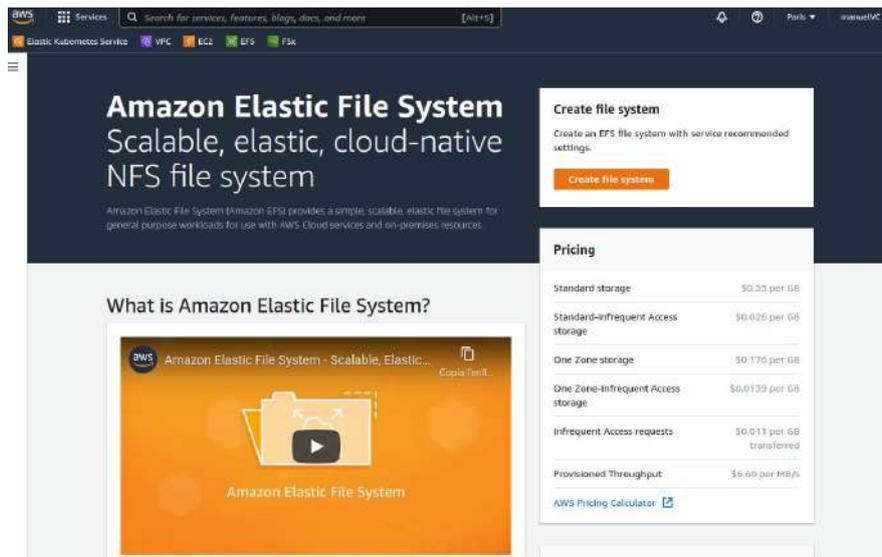
```
aws ec2 delete-volume --volume-id vol-0c956f9595c594bb9
```

```
administrador@buntudocker:~$ aws ec2 delete-volume --volume-id vol-0c956f9595c594bb9  
administrador@buntudocker:~$ aws ec2 describe-volumes --query 'Volumes[].[{"Id del Volumen":VolumeId},{  
"Estado asociación a Instancia":Attachments[].State},{ "ID instancia asociada":Attachments[].InstanceId}]  
' --output yaml  
- - Id del Volumen: vol-0ecda928275bf62  
- Estado asociación a Instancia:  
  - attached  
- ID instancia asociada:  
  - i-0e060585afc6bcab9  
- Id del Volumen: vol-03e7805c865d41886  
- Estado asociación a Instancia:  
  - attached  
- ID instancia asociada:  
  - i-0cee5531268123695
```

# TEMA 11 - EC2 Trabajar con EFS y FSX. Sistemas de ficheros compartidos

## 11.1. - EFS (Linux)

EFS (Amazon Elastic File System) es un Sistema de ficheros parecido a NFS (Network File System). Se utiliza para tener acceso en red entre los Linux.



Standard almacena el fichero en dos AZ para tener backup.

Standard-infrequent es lo mismo que estandar pero para documentos que no se consulten mucho. Con esta opción cobran por acceder a los datos.

One Zone es que se almacenan los datos en una AZ. También tiene su opción por infrequent.

Se puede utilizar para hacer backup, para sincronizar datos y para transferir datos con un servicio ftp/sftp.

[AWS Backup](#)

[AWS DataSync](#)

[AWS Transfer](#)

Antes de continuar tenemos que tener un grupo de seguridad que admita el acceso a través del puerto NFS (2049). El acceso al EFS es a través de un acces point al servidor, por eso lo necesita.

### Create security group Info

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

#### Basic details

Security group name Info  
  
Name cannot be edited after creation.

Description Info

VPC Info

#### Inbound rules Info

Type <small>Info</small>	Protocol <small>Info</small>	Port range <small>Info</small>	Source <small>Info</small>	Description - optional <small>Info</small>	
NFS	TCP	2049	Anywh... <input type="text" value="0.0.0.0/0"/>	Acceso al puerto NFS	Del etc

#### Outbound rules Info

Type <small>Info</small>	Protocol <small>Info</small>	Port range <small>Info</small>	Destination <small>Info</small>	Description - optional <small>Info</small>	
All traffic	ALL	All	Custom <input type="text"/>		Del ...

Para crearlo se puede hacer en modo sencillo o con más detalles en el modo avanzado clicando en Customize. Hay que asegurarse tanto el VPC correcto como la AZ.

### Create file system

Create an EFS file system with service recommended settings. [Learn more](#)

**Name - optional**  
Name your file system.  
  
Name can include letters, numbers, and +-=\_./ symbols, up to 256 characters.

**Virtual Private Cloud (VPC)**  
Choose the VPC where you want EC2 instances to connect to your file system. [Learn more](#)  
  
mi-vpc-prueba

**Storage class** [Learn more](#)

Standard  
Stores data redundantly across multiple AZs

One Zone  
Stores data redundantly within a single AZ

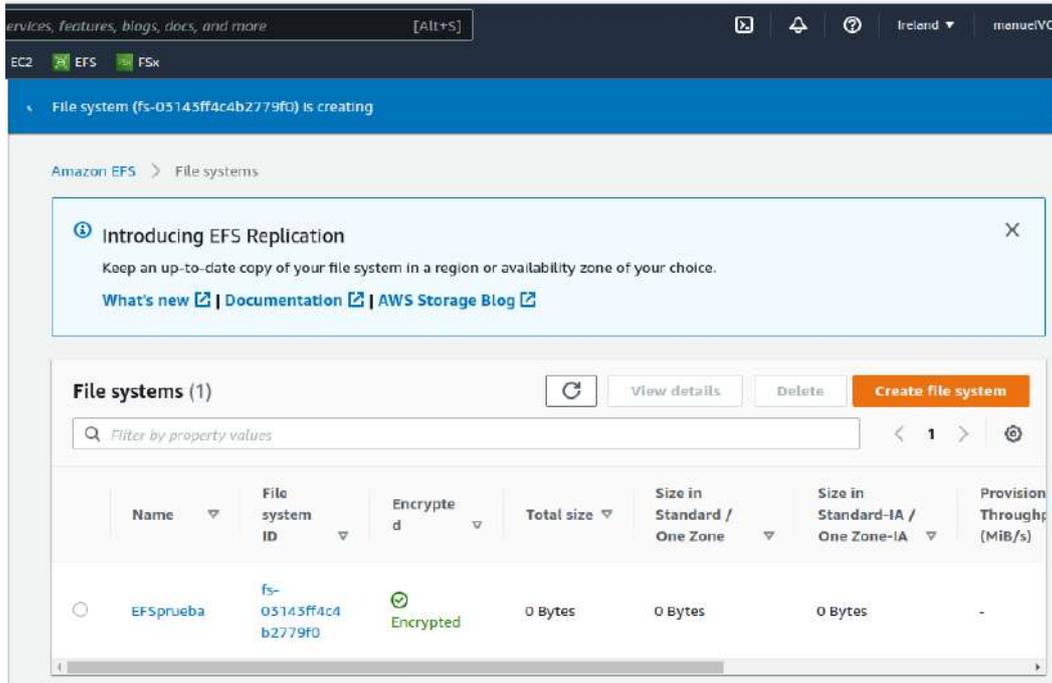
**Availability Zone**  
Choose the Availability Zone where you want to create your file system

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

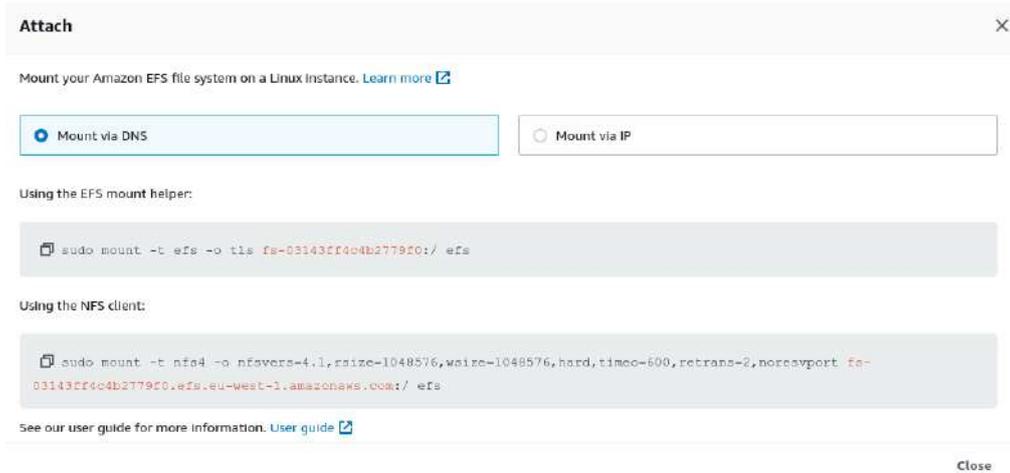
En la AZ Paris no permite crear EFS



En Irlanda sí que lo permite



Para asociarlo existen varias formas



Los ajustes avanzados permiten hacer backup, gestión del ciclo de vida

### File system settings

#### General

**Name - optional**  
Name your file system.  
  
Name can include letters, numbers, and +-=\_./ symbols, up to 256 characters.

**Storage class** [Learn more](#)

Standard  
Stores data redundantly across multiple AZs

One Zone  
Stores data redundantly within a single AZ

**Availability Zone**  
Choose the Availability Zone where you want to create your file system

**Automatic backups**  
Automatically backup your file system data with AWS Backup using recommended settings. Additional pricing applies. [Learn more](#)

Enable automatic backups

**Lifecycle management**  
EFS Intelligent-Tiering uses Lifecycle Management to automatically achieve the right price and performance blend for your application by moving your files between the One Zone and One Zone-Infrequent Access.

**Transition into IA**  
Transition files from One Zone to One Zone-Infrequent Access.

**Transition out of IA**  
Transition files from One Zone-Infrequent Access to One Zone.

**Performance mode**  
Set your file system's performance mode based on IOPS required. File systems using One Zone Storage classes only support General Purpose performance mode. [Learn more](#)

General Purpose  
Ideal for latency-sensitive use cases, like web serving environments and content management systems

Max I/O  
Scale to higher levels of aggregate throughput and operations per second.

**Throughput mode**  
Set how your file system's throughput limits are determined. [Learn more](#)

Bursting  
Throughput scales with file system size

Provisioned  
Throughput fixed at specified amount

**Encryption**  
Choose to enable encryption of your file system's data at rest. Uses the AWS KMS service key (aws/elasticfilesystem) by default. [Learn more](#)

Enable encryption of data at rest

[Customize encryption settings](#)

Podemos especificar opciones de red. Importante escogerlo correctamente respecto las instancias que queremos que se conecten. Y el grupo de seguridad debe permitir el acceso NFS

#### Network

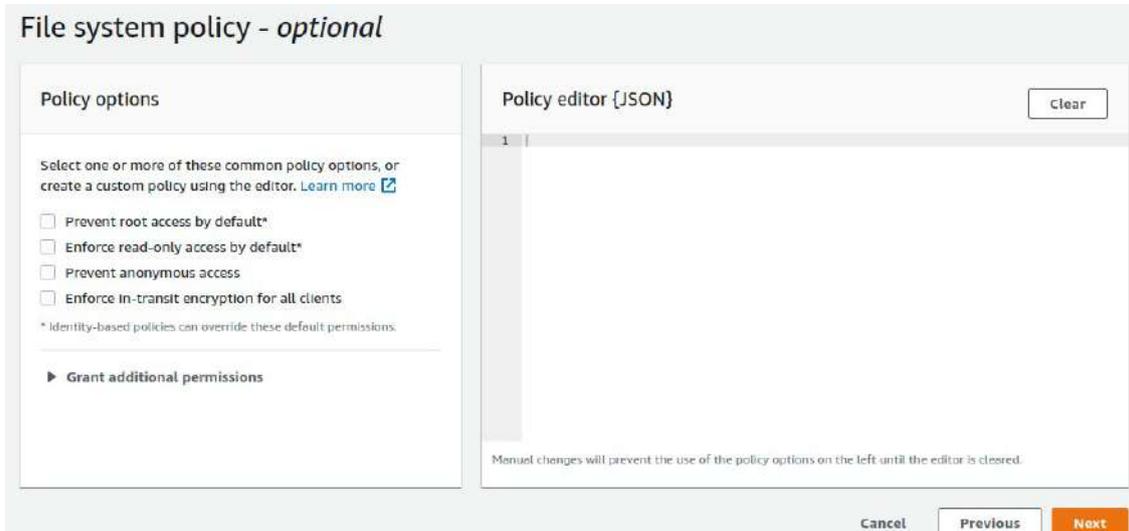
**Virtual Private Cloud (VPC)**  
Choose the VPC where you want EC2 instances to connect to your file system. [Learn more](#)

default

**Mount targets**  
A mount target provides an NFSv4 endpoint at which you can mount an Amazon EFS file system. We recommend creating one mount target per Availability Zone. [Learn more](#)

Availability zone	Subnet ID	IP address	Security groups	
<input type="text" value="eu-west-1a"/>	<input type="text" value="subnet-046b32ca9e77439f9"/>	<input type="text" value="Automatic"/>	<input type="text" value="sg-05b2de69cbbf7c0c0"/> default	<input type="button" value="Remove"/>

Podemos especificar con JSON una política de sistema de ficheros. Se puede editar en Policy editor. Tenemos las opciones: Impedir el acceso de root por defecto, Imponer el acceso de sólo lectura por defecto, Impedir el acceso anónimo y Imponer el cifrado en tránsito para todos los clientes.



Y ya tendríamos creado el Fyle System.

ATENCIÓN que la red del EFS tarda en crearse

Metered size	Monitoring	Tags	File system policy	Access points	Network	Replication
<b>Network</b>						
						Manage
Availability zone ▲	Mount target ID ▼	Subnet ID ▼	Mount target state ▼	IP address ▼	Network interface ID ▼	Security groups ▼
eu-west-1a	fsmt-063f9fd3cda364780	subnet-046b32ca9e77439f9	Creating	172.31.41.160	eni-01a59d8fde7c32fa0	-

## 11.2. - FSx (Windows y otros SO)

Es el remplazo de NFS para Windows. Se puede utilizar con 4 sistemas de ficheros:

- NetApp
- OpenZFS
- Windows File Server
- Lustre – Es open source <https://www.lustre.org/>



### 11.2.1. - Prueba con Lustre para Linux

Select file system type

File system options

- Amazon FSx for NetApp ONTAP
- Amazon FSx for OpenZFS
- Amazon FSx for Windows File Server
- Amazon FSx for Lustre

**Amazon FSx for Lustre**

Amazon FSx for Lustre provides cost-effective, high-performance, scalable file storage for compute workloads such as machine learning, high performance computing (HPC), video processing, and financial modeling.

- Accessible from Linux compute instances and containers (running on AWS or on-premises) over a POSIX-compliant protocol.
- Integrates seamlessly with Amazon S3 (connect your S3 data sets to your FSx for Lustre file system, run your analyses, write results back to S3, and delete your file system), Amazon SageMaker, Amazon Elastic Kubernetes Service (EKS), AWS Batch, and AWS ParallelCluster.
- Delivers consistent sub-millisecond latencies, up to hundreds of gigabytes per second of throughput, and up to millions of IOPS.
- Provides multiple deployment options for short-term and long-term data processing, with built-in, fully managed backups.
- Supports data compression to reduce storage consumption of both your file system storage and backups.

Cancel Next

Tenemos diversas opciones como clase de disco, velocidad de I/O, capacidad, etc

### Create file system

**File system details**

File system name - optional [Info](#)  
  
Maximum of 256 Unicode letters, whitespace, and numbers, plus + - = \_ : /

Deployment and storage type [Info](#)  
 Select a deployment type and storage type to fit your workload requirements

- Persistent, SSD
- Persistent, HDD
  - with SSD cache
- Scratch, SSD

Throughput per unit of storage [Info](#)  
Throughput (MB/s) per unit of storage (TiB)

- 125 MB/s/TiB
- 250 MB/s/TiB
- 500 MB/s/TiB
- 1000 MB/s/TiB

Storage capacity [Info](#)  
 TiB  
Supported sizes: 1,2 TiB or increments of 2,4 TiB

Throughput capacity [Info](#)  
Throughput capacity = Storage capacity (TiB) \* Per unit storage throughput (MB/s)  
 0 MB/s

Data compression type [Info](#)  
Data compression reduces the physical disk space needed to store file data. Select LZ4 to enable data compression

Lustre version  
 2.12

Los tipos de almacenamiento Scratch es para datos que no importan si se pierden.

Si queremos crear el grupo de seguridad a mano necesitaremos varios rangos de puertos: 988 y 1021-1023

Type	Protocol	Port Range	Source	Description
Custom TCP rule	TCP	988	Choose <b>Custom</b> and enter the security group ID of the security group that you just created	Allows Lustre traffic between FSx for Lustre file servers
Custom TCP rule	TCP	988	Choose <b>Custom</b> and enter the security group IDs of the security groups associated with your Lustre clients	Allows Lustre traffic between FSx for Lustre file servers and Lustre clients
Custom TCP rule	TCP	1021-1023	Choose <b>Custom</b> and enter the security group ID of the security group that you just created	Allows Lustre traffic between FSx for Lustre file servers
Custom TCP rule	TCP	1021-1023	Choose <b>Custom</b> and enter the security group IDs of the security groups associated with your Lustre clients	Allows Lustre traffic between FSx for Lustre file servers and Lustre clients

Por defecto ya crear un grupo de seguridad correcto.

También aparece la encriptación, si queremos exportar datos a S3, configurar el logging (Los logs se podrán leer en CloudWatch), Backup (Se harán periodicos pero también se pueden hacer manuales) y Tags

Tardar un rato en crearse. Cuidado que es un producto caro, si es una prueba no hay que dejarlo creado.

Podremos ver detalles del componente

### FSxLustre (fs-07cd80032bc627225)

#### Summary

File system ID fs-07cd80032bc627225	Storage type SSD	Lustre version 2.12
Lifecycle state Creating	Storage capacity 1.2 TiB <span>Update</span>	Availability Zones eu-west-1a
File system type Lustre	Throughput per unit of storage 125 MB/s/TiB	Creation time 2022-08-20T16:36:07+02:00
Deployment type Persistent 2	Total throughput 150 MB/s	Mount name h3xzxbmv
Data compression type NONE <span>Update</span>		

**Network & security** | Monitoring | Administration | Data repository | Backups | Updates | Tags

Para asociarlo es parecido a NFS, hay que clicar en Attach y dar  los comandos para hacerlo

#### Attach file system

**From Linux instances (Amazon EC2, Amazon WorkSpaces, VMware Cloud on AWS)**

▼ Prerequisites

1. Create or select your Linux EC2 Instance in the same AWS VPC as your file system.
2. Open an SSH client and connect to your EC2 Instance. ([Find out how to connect.](#))
3. Install the open-source Lustre client, which is supported on most Linux distributions.

▼ Attach instruction - using the default DNS name

1. Open a terminal
2. Create a new directory on your EC2 Instance, for example `/fsx`

```
sudo mkdir /fsx
```
3. sudo mount -t lustre -o noatime,flock fs-07cd80032bc627225.fsx.eu-west-1.amazonaws.com@tcp:/h3xzxbmv /fsx

**From Amazon Elastic Kubernetes Service (EKS) use the Amazon FSx for Lustre CSI Driver**

▼ Attach instruction - using the default DNS name

Instructions on accessing Persistent Volumes (PVs) backed by Amazon FSx for Lustre based filesystems from Amazon EKS clusters can be found [here](#).

Close

En este caso debemos instalar el cliente de Lustre. Para hacerlo en Amazon Linux 2 es:

```
sudo amazon-linux-extras install -y lustre2.10
```

```
sudo yum -y update kernel && sudo reboot
```

Luego ya podemos montar el volumen

```
Last login: Sat Aug 20 14:37:15 2022 from 37.120.199.237
┌───┴───┐
┌─┴─┐ Amazon Linux 2 AMI
└─┬─┘
└─┬─┘
└─┬─┘

https://aws.amazon.com/amazon-linux-2/
4 package(s) needed for security, out of 18 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-37-56 ~]$ ls
efs fsx
[ec2-user@ip-172-31-37-56 ~]$ sudo mount -t lustre -o noatime,flock fs-07cd80032bc627225.fsx.eu-west-1.amazonaws.com@tcp:/h3xzbmv fsx
[ec2-user@ip-172-31-37-56 ~]$ df -h
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        474M   0  474M   0% /dev
tmpfs           483M   0  483M   0% /dev/shm
tmpfs           483M 404K  483M   1% /run
tmpfs           483M   0  483M   0% /sys/fs/cgroup
/dev/xvda1      8.0G  1.7G  6.4G  21% /
tmpfs           97M   0   97M   0% /run/user/1000
172.31.45.7@tcp:/h3xzbmv 1.2T  7.8M  1.2T   1% /home/ec2-user/fsx
[ec2-user@ip-172-31-37-56 ~]$
```

### 11.3. - Línea de comandos

Para acceder a efs o fsx hay que entrar en sus subcomandos, sus subcomandos son:

aws efs

```
create-access-point
create-file-system
create-mount-target
create-replication-configuration
delete-access-point
delete-file-system
delete-file-system-policy
delete-mount-target
delete-replication-configuration
describe-access-points
describe-account-preferences
describe-backup-policy
describe-file-system-policy
describe-file-systems
describe-lifecycle-configuration
describe-access-points
describe-account-preferences
describe-backup-policy
describe-file-system-policy
describe-file-systems
describe-lifecycle-configuration
describe-mount-target-security-groups
describe-mount-targets
describe-replication-configurations
```

Para ver los sistemas de ficheros creados

- list-tags-for-resource
- modify-mount-target-security-groups
- put-account-preferences
- put-backup-policy
- put-file-system-policy
- put-lifecycle-configuration
- tag-resource
- untag-resource
- update-file-system

#### aws fsx

- associate-file-system-aliases
- cancel-data-repository-task
- copy-backup
- create-backup
- create-data-repository-association
- create-data-repository-task
- create-file-system
- create-file-system-from-backup
- create-snapshot
- create-storage-virtual-machine
- create-volume
- create-volume-from-backup
- delete-backup
- delete-data-repository-association
- delete-file-system
- delete-snapshot
- delete-storage-virtual-machine
- delete-volume
- describe-backups
- describe-data-repository-associations
- describe-data-repository-tasks
- describe-file-system-aliases
- describe-file-systems
- describe-snapshots
- describe-storage-virtual-machines
- describe-volumes
- disassociate-file-system-aliases
- help
- list-tags-for-resource
- release-file-system-nfs-v3-locks
- restore-volume-from-snapshot
- tag-resource

Para ver los sistemas de ficheros creados

untag-resource  
 update-data-repository-association  
 update-file-system  
 update-snapshot  
 update-storage-virtual-machine  
 update-volume

```

[root@curso ~]# aws fsx describe-file-systems
{
  "FileSystems": [
    {
      "OwnerId": "264297788131",
      "CreationTime": "2022-01-12T09:32:51.075000+01:00",
      "FileSystemId": "fs-09c7b3bd2f8bb1fac",
      "FileSystemType": "LUSTRE",
      "Lifecycle": "AVAILABLE",
      "StorageCapacity": 1200,
      "StorageType": "SSD",
      "VpcId": "vpc-0bb143acbd251ad96",
      "SubnetIds": [
        "subnet-07e47c4661a3bec50"
      ],
      "NetworkInterfaceIds": [
        "eni-034b16c3456471681",
        "eni-0cd8f284d5b68ba85"
      ],
      "DNSName": "fs-09c7b3bd2f8bb1fac.fsx.us-west-2.amazonaws.com",
      "KmsKeyId": "arn:aws:kms:us-west-2:264297788131:key/fff684a2-2573-4970-b37a-3378787a52d1",
      "ResourceARN": "arn:aws:fsx:us-west-2:264297788131:file-system/fs-09c7b3bd2f8bb1fac",
      "Tags": [
        {
          "Key": "Name",
          "Value": "fsx1"
        }
      ],
      "LustreConfiguration": {
        "WeeklyMaintenanceStartTime": "5:06:30",
        "DeploymentType": "PERSISTENT_2",
        "PerUnitStorageThroughput": 125,
        "MountName": "zeqz2bmv",
        "DailyAutomaticBackupStartTime": "06:30",
        "AutomaticBackupRetentionDays": 7,
        "CopyTagsToBackups": false,
        "DataCompressionType": "NONE",
        "LogConfiguration": {
          "Level": "DISABLED"
        }
      },
      "FileSystemTypeVersion": "2.12"
    }
  ]
}

```

Ejemplo backup:

```
aws fsx create-backup --file-system-id xxxxxxxxxxxxxxxx
```

```
[root@curso ~]# aws fsx create-backup --file-system-id fs-09c7b3bd2f8bb1fac
{
  "Backup": {
    "BackupId": "backup-019487af822374b4c",
    "Lifecycle": "PENDING",
    "Type": "USER_INITIATED",
    "CreationTime": "2022-01-12T10:51:09.081000+01:00",
    "KmsKeyId": "arn:aws:kms:us-west-2:264297788131:key/fff684a2-2573-4970-b37a-3378787a52d1",
    "ResourceARN": "arn:aws:fsx:us-west-2:264297788131:backup/backup-019487af822374b4c",
    "Tags": [],
    "FileSystem": {
      "FileSystemId": "fs-09c7b3bd2f8bb1fac",
      "FileSystemType": "LUSTRE",
      "StorageCapacity": 1200,
      "StorageType": "SSD",
      "ResourceARN": "arn:aws:fsx:us-west-2:264297788131:file-system/fs-09c7b3bd2f8bb1fac",
      "LustreConfiguration": {
        "WeeklyMaintenanceStartTime": "5:06:30",
        "DeploymentType": "PERSISTENT_2",
        "PerUnitStorageThroughput": 125,
        "DailyAutomaticBackupStartTime": "06:30",
        "AutomaticBackupRetentionDays": 7,
        "DataCompressionType": "NONE"
      },
      "FileSystemTypeVersion": "2.12"
    },
    "OwnerId": "264297788131"
  }
}
```

Se pueden ver los backups con:

`aws fsx describe-backups`

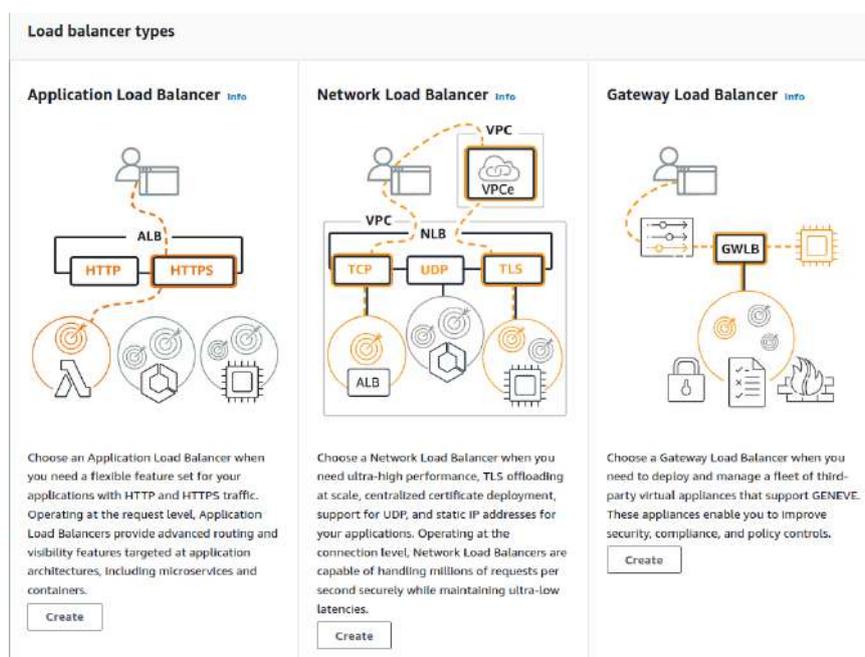
```
[root@curso ~]# aws fsx describe-backups
{
  "Backups": [
    {
      "BackupId": "backup-019487af822374b4c",
      "Lifecycle": "CREATING",
      "Type": "USER_INITIATED",
      "CreationTime": "2022-01-12T10:51:09.081000+01:00",
      "KmsKeyId": "arn:aws:kms:us-west-2:264297788131:key/fff684a2-2573-4970-b37a-3378787a52d1",
      "ResourceARN": "arn:aws:fsx:us-west-2:264297788131:backup/backup-019487af822374b4c",
      "Tags": [],
      "FileSystem": {
        "FileSystemId": "fs-09c7b3bd2f8bb1fac",
        "FileSystemType": "LUSTRE",
        "StorageCapacity": 1200,
        "StorageType": "SSD",
        "ResourceARN": "arn:aws:fsx:us-west-2:264297788131:file-system/fs-09c7b3bd2f8bb1fac",
        "LustreConfiguration": {
          "WeeklyMaintenanceStartTime": "5:06:30",
          "DeploymentType": "PERSISTENT_2",
          "PerUnitStorageThroughput": 125,
          "DailyAutomaticBackupStartTime": "06:30",
          "AutomaticBackupRetentionDays": 7,
          "DataCompressionType": "NONE"
        },
        "FileSystemTypeVersion": "2.12"
      },
      "OwnerId": "264297788131"
    }
  ]
}
```

## TEMA 12 - EC2 Load Balancers. Balanceadores de carga

Mediante un failover se repartirá el tráfico entre las instancias que hayamos preparado con la misma app.

Se pueden crear 3 tipos de balanceadores de carga según en la capa OSI que trabajen:

- **Balanceador de aplicación.** Trabajan en la capa de aplicación, en entornos web (http o https) pueden ir a instancias, a firegates o a Lambda.
- **Balanceador de red.** Trabajan en la capa 4 de transporte. TCP, UDP y TLS. Para instancias y otros productos de Amazon. También a los ALB (Application Load Balancer)
- **Balanceador de Gateway.** Trabajan con adplayers¿? de terceros que soportan GENEVE.



Por otra parte se puede acceder al balanceador de carga antiguo de Amazon, pero de manera temporal. Se supone que el 15 de agosto pasado dejaba de funcionar. Estaba pensado para las grandes plataformas que usaban el antiguo balanceador.

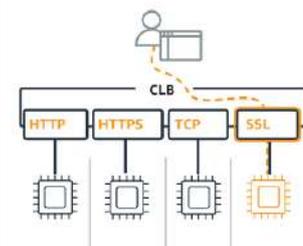
▼ Classic Load Balancer - *previous generation*

### Classic Load Balancer Info

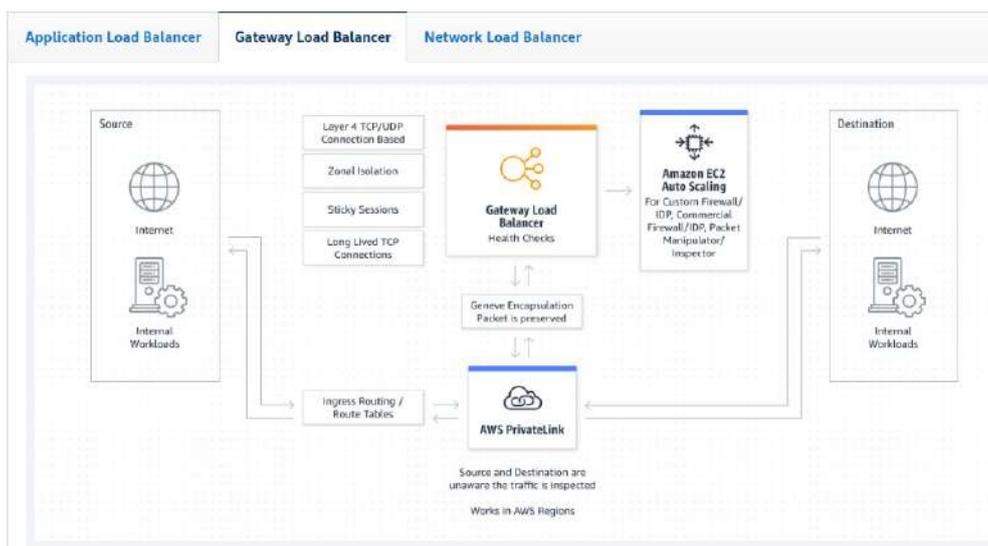
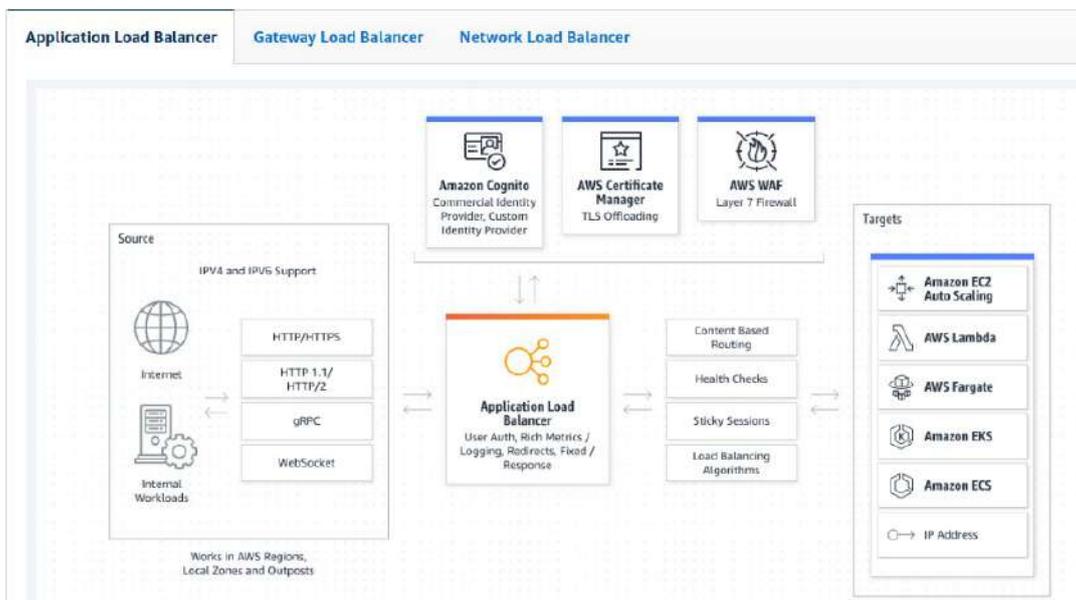
Choose a Classic Load Balancer when you have an existing application running in the EC2-Classic network.

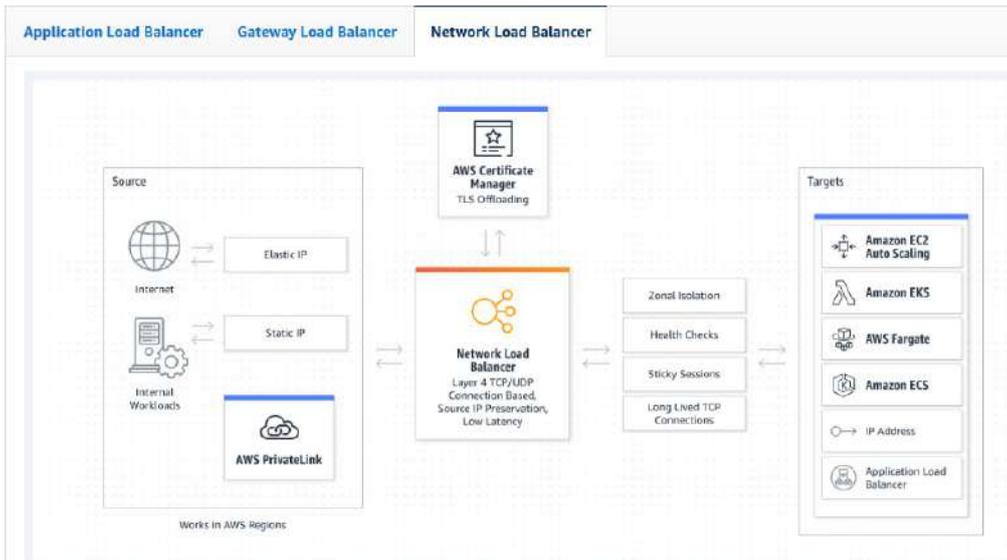
**Info** AWS will be retiring the EC2-Classic network on August 15, 2022. [Learn more](#)

Create

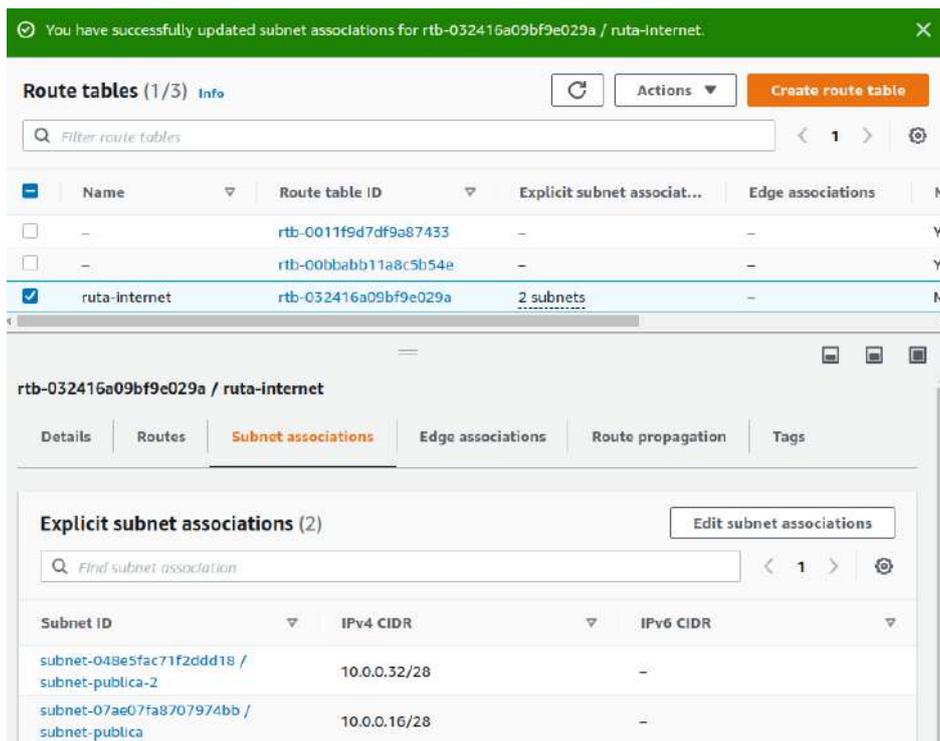


Documentación de los balanceadores: <https://aws.amazon.com/elasticloadbalancing/?nc=sn&loc=1>

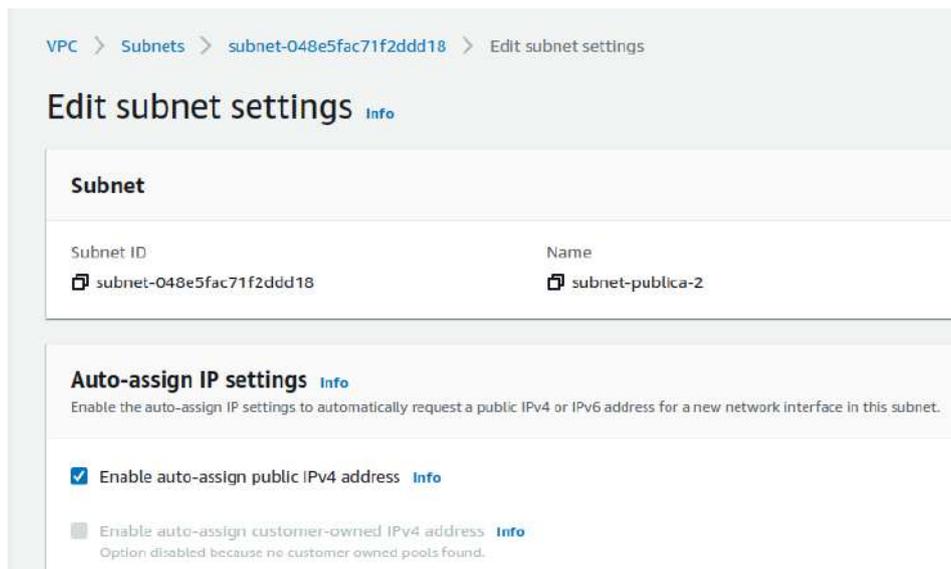




Necesitamos al menos dos subredes donde balancear, cada una debe estar en un AZ distinta. Para hacerla pública se debe tener el gateway en la tabla de rutas tener asociada la subred.



En la subred se debe habilitar la asignación de Ipv4 pública



La VPC tendrá que tener las DNS hostnames y las DNS resolution habilitadas.

Las instancias nuevas tienen que tener habilitada la Ipv\$ pública.

Ahora tendremos que crear el **Target Group**. Son los componentes que se balancearán, en este caso añadimos las 3 instancias.

Para el Gateway Load Balancer se necesitan más recursos para poder hacerlo, por eso se hará la práctica. Se hará del ALB y del NLB.

## 12.1. - Target groups

### Specify group details

Your load balancer routes requests to the targets in a target group and performs health checks on the targets.

**Basic configuration**  
Settings in this section cannot be changed after the target group is created.

Choose a target type

- Instances**
  - Supports load balancing to instances within a specific VPC.
  - Facilitates the use of [Amazon EC2 Auto Scaling](#) to manage and scale your EC2 capacity.
- IP addresses**
  - Supports load balancing to VPC and on-premises resources.
  - Facilitates routing to multiple IP addresses and network interfaces on the same instance.
  - Offers flexibility with microservice based architectures, simplifying inter-application communication.
  - Supports IPv6 targets, enabling end-to-end IPv6 communication, and IPv4-to-IPv6 NAT.
- Lambda function**
  - Facilitates routing to a single Lambda function.
  - Accessible to Application Load Balancers only.
- Application Load Balancer**
  - Offers the flexibility for a Network Load Balancer to accept and route TCP requests within a specific VPC.
  - Facilitates using static IP addresses and PrivateLink with an Application Load Balancer.

Target group name

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

Se puede balancear:

- Instancias
- Direcciones IPs. Una instancia podría tener varias IPs
- Funciones Lambda. Es para ejecutar procedimientos y funciones en entornos serverless.
- Aplicaciones

Se puede indicar el nombre, el protocolo, la VPC, la versión de protocolo,

Target group name

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

Protocol      Port

HTTP      :      80

VPC

Select the VPC with the instances that you want to include in the target group.

mi-vpc-prueba  
vpc-06efef12f7a7228f  
IPv4: 10.0.0.0/24

Protocol version

- HTTP1**  
Send requests to targets using HTTP/1.1. Supported when the request protocol is HTTP/1.1 or HTTP/2.
- HTTP2**  
Send requests to targets using HTTP/2. Supported when the request protocol is HTTP/2 or gRPC, but gRPC-specific features are not available.
- gRPC**  
Send requests to targets using gRPC. Supported when the request protocol is gRPC.

Puede hacer un chequeo para comprobar si funciona el protocolo. Lo que hará es lanzar ping y esperar su respuesta. Se pueden configurar detalles como poner una página concreta a comprobar.

### Health checks

The associated load balancer periodically sends requests, per the settings below, to the registered targets to test their status.

Health check protocol

HTTP

Health check path

Use the default path of "/" to ping the root, or specify a custom path if preferred.

/

Up to 1024 characters allowed.

---

▼ Advanced health check settings Restore defaults

**Port**

The port the load balancer uses when performing health checks on targets. The default is the port on which each target receives traffic from the load balancer, but you can specify a different port.

Traffic port

Override

**Healthy threshold**

The number of consecutive health checks successes required before considering an unhealthy target healthy.

5

2-10

**Unhealthy threshold**

The number of consecutive health check failures required before considering a target unhealthy.

2

2-10

**Timeout**

The amount of time, in seconds, during which no response means a failed health check.

5

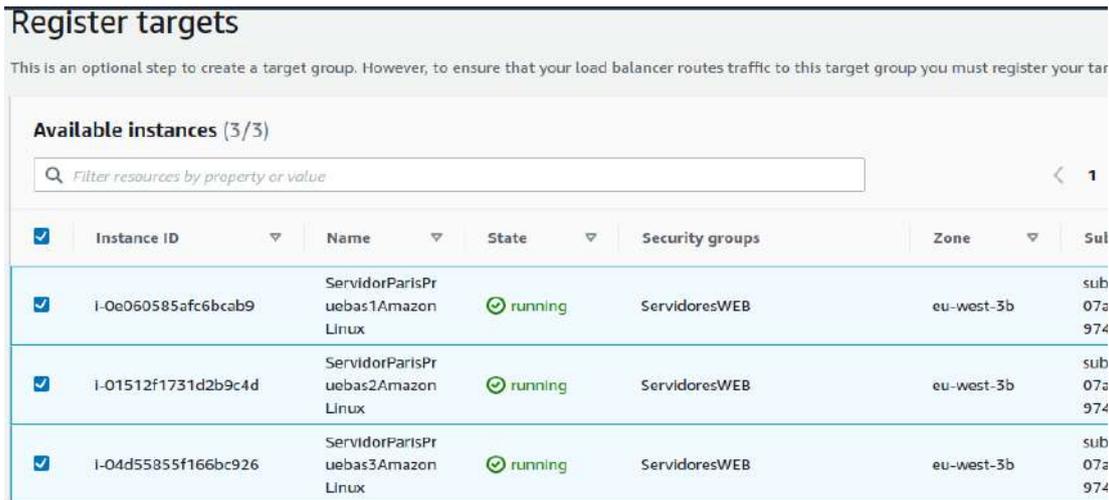
seconds

2-120

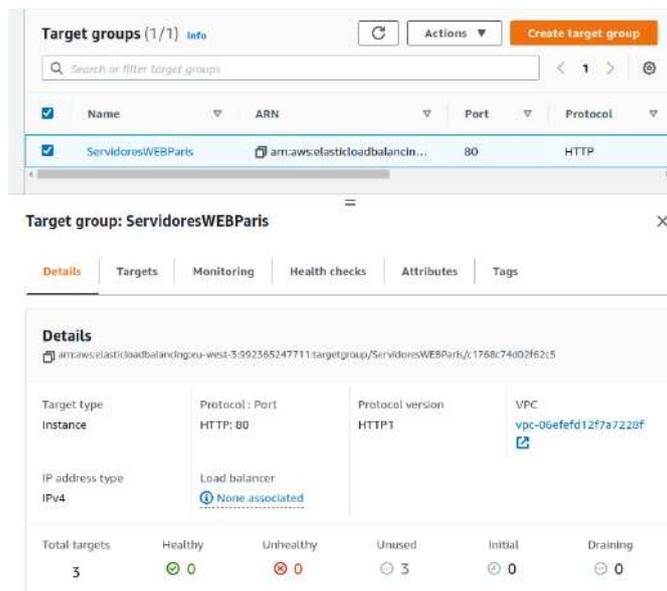
**Interval**

The approximate amount of time between health checks of an individual target.

Luego indica las instancias (o los elementos) que queremos seleccionar para balancear.



Aquí también se puede indicar el puerto. Después de incluir los elementos ya se crea el target group.

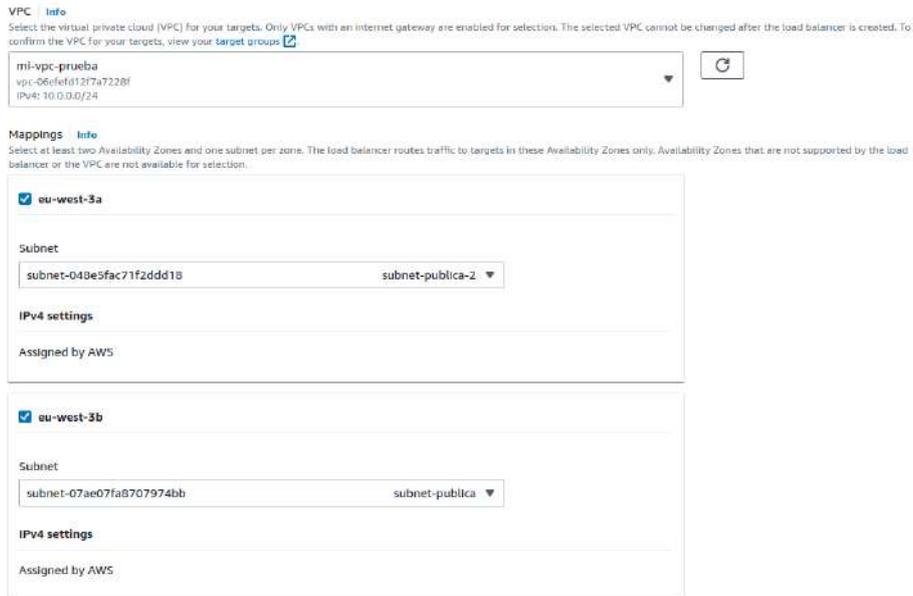


## 12.2. - Crear el balanceador de carga ALB

Para las 3 instancias anteriores usaremos el ALB para balancear en capa de aplicación.

En el esquema puede ser Internet-facing o Internal. La interna puede ser para SQL u otros servidores que estén dentro de la red privada.

El Network Mapping se debe configurar con cuidado para tener el acceso a los targets.

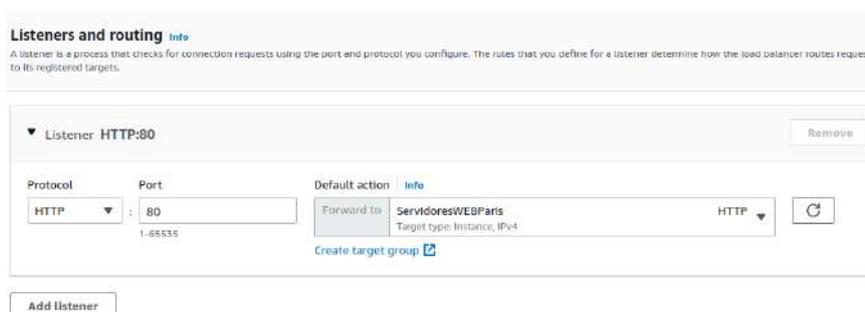


Aquí se ve que es obligatorio tener al menos dos AZ.

Ahora mismo no ofrece otros AZ porque solo ofrece los que tiene subnet.

En el grupo de seguridad debe tener habilitado el puerto 80.

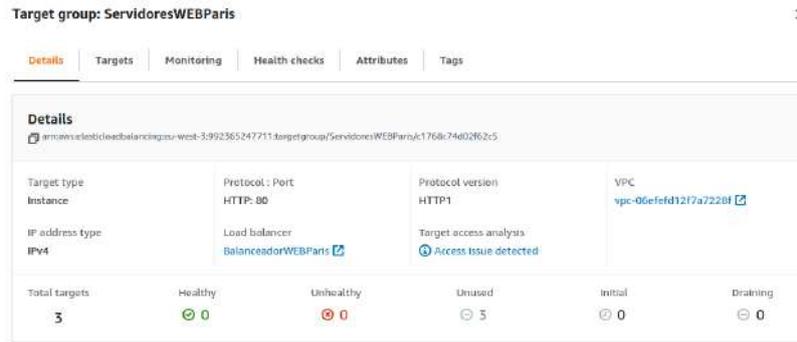
En el Listener es importante que este el puerto que necesite la aplicación. En este momento también se puede crear el Target Group.



Como se pueden poner varios puertos se pueden destinar para aplicaciones distintas.

El AWS Global Accelerator sirve para utilizar direcciones IP fijas usando la red global de Amazon para optimizar el tráfico.

Una vez creado podemos comprobar en el target group que tenemos con Healthy todas las instancias añadidas:



Para acceder al balanceador nos da un nombre DNS. Como el algoritmo es Round Robin, cada vez que entremos a la dirección nos aparecerá el siguiente servidor web, por orden.



Podemos definir en Listeners distintos puertos. En cada puerto podemos editar las reglas



Por ejemplo, puede especificar que si se intenta entrar en /datos se redirecciones a otra página.

RULE ID	IF (all match)	THEN
1	+ Add condition Host header... Path... Http header... Http request method... Query string... Source IP...	+ Add action
last	<b>HTTP 80: default action</b> This rule cannot be moved or deleted	<b>THEN</b> Forward to ServidoresWEBParis: 1 (100%) Group-level stickiness: Off

RULE ID	IF (all match)	THEN
1	Path is /datos + Add condition	+ Add action Forward to... Redirect to... Return fixed response... Note: Additional actions are available for HTTPS listeners.
last	<b>HTTP 80: default action</b> This rule cannot be moved or deleted	<b>THEN</b> Forward to ServidoresWEBParis: 1 (100%) Group-level stickiness: Off

RULE ID	IF (all match)	THEN
1	Path is /datos + Add condition	1. Redirect to http://vergaracarmona.es:80/? Status code: HTTP_301 + Add action
last	<b>HTTP 80: default action</b> This rule cannot be moved or deleted	<b>THEN</b> Forward to ServidoresWEBParis: 1 (100%) Group-level stickiness: Off

Con lo que si intento entrar en la url con /datos se redirecciona a la web indicada.

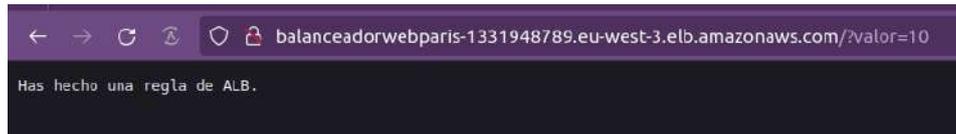
Las reglas se van consultando de arriba a abajo, si la primera se cumple no revisará las siguientes. Por eso aparece Insert Rule cuando le damos a añadir entre cada regla:

1	am_ad721 IF ✓ Path is /datos	<b>THEN</b> Redirect to http://vergaracarmona.es:80/? Status code: HTTP_301
last	<b>HTTP 80: default action</b> This rule cannot be moved or deleted	<b>THEN</b> Forward to ServidoresWEBParis: 1 (100%) Group-level stickiness: Off

Por ejemplo, también se pueden insertar query. En este caso la respuesta es un error con un texto

RULE ID	IF (all match)	THEN
1	Query string is valor:10 + Add condition	1. Return fixed response 503 (more...) + Add action

Y si cumple la regla lo redirige al error



## 12.3. - Linea de comandos ALBs

Opciones de aws elbv2

add-listener-certificates

add-tags

create-listener

create-load-balancer

create-rule

create-target-group

delete-listener

delete-load-balancer

delete-rule

delete-target-group

deregister-targets

describe-account-limits

describe-listener-certificates

describe-listeners

describe-load-balancer-attributes

describe-load-balancers

describe-rules

describe-ssl-policies

describe-tags

describe-target-group-attributes

describe-target-groups

describe-target-health

help

modify-listener

modify-load-balancer-attributes

modify-rule

modify-target-group

modify-target-group-attributes

register-targets

remove-listener-certificates

remove-tags

set-ip-address-type

```
set-rule-priorities
set-security-groups
set-subnets
wait
```

Por ejemplo:

aws elbv2 describe-load-balancers

```
administrador@ubuntu:~$ aws elbv2 describe-load-balancers
{
  "LoadBalancers": [
    {
      "LoadBalancerArn": "arn:aws:elasticloadbalancing:eu-west-3:992365247711:loadbalancer/app/BalanceadorWEBParis/55c6c9cc8aefe3dc",
      "DNSName": "BalanceadorWEBParis-1331948709.eu-west-3.elb.amazonaws.com",
      "CanonicalHostedZoneId": "Z3Q77PNBQ571R4",
      "CreatedTime": "2022-08-22T19:15:37.340000+00:00",
      "LoadBalancerName": "BalanceadorWEBParis",
      "Scheme": "internet-facing",
      "VpcId": "vpc-06efefd12f7a7228f",
      "State": {
        "Code": "active"
      },
      "Type": "application",
      "AvailabilityZones": [
        {
          "ZoneName": "eu-west-3a",
          "SubnetId": "subnet-048e5fac71f2ddd18",
          "LoadBalancerAddresses": []
        },
        {
          "ZoneName": "eu-west-3b",
          "SubnetId": "subnet-07ae07fa8707974bb",
          "LoadBalancerAddresses": []
        }
      ],
      "SecurityGroups": [
        "sg-0527f1d0d8d4ff0e",
        "sg-08b19fde393e9cdb3"
      ],
      "IpAddressType": "ipv4"
    }
  ]
}
```

aws elbv2 describe-target-groups

```
administrador@ubuntu:~$ aws elbv2 describe-target-groups
{
  "TargetGroups": [
    {
      "TargetGroupArn": "arn:aws:elasticloadbalancing:eu-west-3:992365247711:targetgroup/ServidoresWEBParis/c1768c74d02f62c5",
      "TargetGroupName": "ServidoresWEBParis",
      "Protocol": "HTTP",
      "Port": 80,
      "VpcId": "vpc-06efefd12f7a7228f",
      "HealthCheckProtocol": "HTTP",
      "HealthCheckPort": "traffic-port",
      "HealthCheckEnabled": true,
      "HealthCheckIntervalSeconds": 30,
      "HealthCheckTimeoutSeconds": 5,
      "HealthyThresholdCount": 5,
      "UnhealthyThresholdCount": 2,
      "HealthCheckPath": "/",
      "Matcher": {
        "HttpCode": "200"
      },
      "LoadBalancerArns": [
        "arn:aws:elasticloadbalancing:eu-west-3:992365247711:loadbalancer/app/BalanceadorWEBParis/55c6c9cc8aefe3dc"
      ],
      "TargetType": "instance",
      "ProtocolVersion": "HTTP1",
      "IpAddressType": "ipv4"
    }
  ]
}
```

O también se puede preguntar como está un target group. Este comando necesitará que se indique la url que utiliza Amazon para identificar objetos, que es la arn:

```
aws elbv2 describe-target-health --target-group-arn arn:aws:elasticloadbalancing:eu-west-3:992365247711:targetgroup/ServidoresWEBParis/c1768c74d02f62c5
```

```

administrador@ubuntu:~$ aws elbv2 describe-target-health --target-group-arn arn:aws:elasticloadbalancing:eu-west-3:992365247711:targetgroup/ServidoresWEBParis/c1768c74d02f62c5
{
  "TargetHealthDescriptions": [
    {
      "Target": {
        "Id": "i-01512f1731d2b9c4d",
        "Port": 80
      },
      "HealthCheckPort": "80",
      "TargetHealth": {
        "State": "healthy"
      }
    },
    {
      "Target": {
        "Id": "i-04d55855f166bc926",
        "Port": 80
      },
      "HealthCheckPort": "80",
      "TargetHealth": {
        "State": "healthy"
      }
    },
    {
      "Target": {
        "Id": "i-0e060585afc6bcab9",
        "Port": 80
      },
      "HealthCheckPort": "80",
      "TargetHealth": {
        "State": "healthy"
      }
    }
  ]
}

```

aws elbv2 describe-listeners --load-balancer-arn arn:aws:elasticloadbalancing:eu-west-3:992365247711:loadbalancer/app/BalanceadorWEBParis/55c6c9cc0afe3dc

```

administrador@ubuntu:~$ aws elbv2 describe-listeners --load-balancer-arn arn:aws:elasticloadbalancing:eu-west-3:992365247711:loadbalancer/app/BalanceadorWEBParis/55c6c9cc0afe3dc
{
  "Listeners": [
    {
      "ListenerArn": "arn:aws:elasticloadbalancing:eu-west-3:992365247711:listener/app/BalanceadorWEBParis/55c6c9cc0afe3dc/12aa82e9221fed60",
      "LoadBalancerArn": "arn:aws:elasticloadbalancing:eu-west-3:992365247711:loadbalancer/app/BalanceadorWEBParis/55c6c9cc0afe3dc",
      "Port": 80,
      "Protocol": "HTTP",
      "DefaultActions": [
        {
          "Type": "Forward",
          "TargetGroupArn": "arn:aws:elasticloadbalancing:eu-west-3:992365247711:targetgroup/ServidoresWEBParis/c1768c74d02f62c5",
          "ForwardConfig": {
            "TargetGroups": [
              {
                "TargetGroupArn": "arn:aws:elasticloadbalancing:eu-west-3:992365247711:targetgroup/ServidoresWEBParis/c1768c74d02f62c5",
                "Weight": 1
              }
            ],
            "TargetGroupStickinessConfig": {
              "Enabled": false
            }
          }
        }
      ]
    }
  ]
}
administrador@ubuntu:~$

```

aws elbv2 describe-rules --listener-arn arn:aws:elasticloadbalancing:eu-west-3:992365247711:listener/app/BalanceadorWEBParis/55c6c9cc0afe3dc/12aa82e9221fed60

```

"Rules": [
  {
    "RuleArn": "arn:aws:elasticloadbalancing:eu-west-3:992365247711:listener-rule/app/BalancedorWEBParis/55c6c9cc0aefe3dc/12aa82e9221fed60/76519d748f2250a1",
    "Priority": "1",
    "Conditions": [
      {
        "Field": "query-string",
        "QueryStringConfig": {
          "Values": [
            {
              "Key": "valor",
              "Value": "10"
            }
          ]
        }
      }
    ],
    "Actions": [
      {
        "Type": "fixed-response",
        "Order": 1,
        "FixedResponseConfig": {
          "MessageBody": "Has hecho una regla de ALB.",
          "StatusCode": "303",
          "ContentType": "text/plain"
        }
      }
    ],
    "IsDefault": false
  },
  {
    "RuleArn": "arn:aws:elasticloadbalancing:eu-west-3:992365247711:listener-rule/app/BalancedorWEBParis/55c6c9cc0aefe3dc/12aa82e9221fed60/4b0ca4ad78aad721",
    "Priority": "2",
    "Conditions": [
      {
        "Field": "path-pattern",
        "Values": [
          "/datos"
        ],
        "PathPatternConfig": {
          "Values": [
            "/datos"
          ]
        }
      }
    ],
    "Actions": [

```

Cuando tengo identificada una regla concreta de listener puedo borrarla

```
aws elbv2 delete-rule --rule-arn arn:aws:elasticloadbalancing:eu-west-3:992365247711:listener-rule/app/BalancedorWEBParis/55c6c9cc0aefe3dc/12aa82e9221fed60/76519d748f2250a1
```

Y lo podemos comprobar

```

administrador@ubuntu:~$ aws elbv2 delete-rule --rule-arn arn:aws:elasticloadbalancing:eu-west-3:992365247711:listener-rule/app/BalancedorWEBParis/55c6c9cc0aefe3dc/12aa82e9221fed60/76519d748f2250a1
administrador@ubuntu:~$ aws elbv2 describe-rules --listener-arn arn:aws:elasticloadbalancing:eu-west-3:992365247711:listener/app/BalancedorWEBParis/55c6c9cc0aefe3dc/12aa82e9221fed60
{
  "Rules": [
    {
      "RuleArn": "arn:aws:elasticloadbalancing:eu-west-3:992365247711:listener-rule/app/BalancedorWEBParis/55c6c9cc0aefe3dc/12aa82e9221fed60/4b0ca4ad78aad721",
      "Priority": "2",
      "Conditions": [
        {
          "Field": "path-pattern",
          "Values": [
            "/datos"
          ],
          "PathPatternConfig": {
            "Values": [
              "/datos"
            ]
          }
        }
      ],
      "Actions": [
        {
          "Type": "redirect",
          "Order": 1,
          "RedirectConfig": {
            "Protocol": "HTTP",
            "Port": "80",
            "Host": "vergaracarmona.es",
            "Path": "/",
            "Query": "",
            "StatusCode": "HTTP_301"
          }
        }
      ],
      "IsDefault": false
    },
    {
      "RuleArn": "arn:aws:elasticloadbalancing:eu-west-3:992365247711:listener-rule/app/BalancedorWEBParis/55c6c9cc0aefe3dc/12aa82e9221fed60/4ef223e947be6a12",
      "Priority": "default",
      "Conditions": [],
      "Actions": [
        {
          "Type": "forward",
          "TargetGroupArn": "arn:aws:elasticloadbalancing:eu-west-3:992365247711:targetgroup/ServidoresWEBParis/c1768c74d02f62c5",
          "ForwardConfig": {

```

## 12.4. - Crear el balanceador de carga NLB

El Network Load Balancer va por la capa 4 de transporte.

Para el ejemplo creamos dos instancias en dos subredes distintas

ServidorParisPruebas1AmazonLinux	i-0e060585afc6bcab9	 Running		t2.micro	 2/2 checks passed	No alarms		eu-west-3b
ServidorParisPruebas2AmazonLinux	i-0465e6b3a4a57e53d	 Stopped		t2.micro	-	No alarms		eu-west-3b
ServidorParisPruebas3AmazonLinux	i-06b3474f683bbc51e	 Stopped		t2.micro	-	No alarms		eu-west-3b
ServidorParisPruebas4AmazonLinux	i-0779d13421d6908af	 Running		t2.micro	 2/2 checks passed	No alarms		eu-west-5a

Y en ambas se instala mariadb y mariadb-server y se abre el puerto 3306 en el grupo de seguridad.

Se crea un usuario a cada BBDD y se le da privilegios.

Ahora ya creamos el target group, basándonos en Instancias y con el puerto 3306

### Basic configuration

Settings in this section cannot be changed after the target group is created.

Choose a target type

**Instances**

- Supports load balancing to instances within a specific VPC.
- Facilitates the use of [Amazon EC2 Auto Scaling](#) to manage and scale your EC2 capacity.

**IP addresses**

- Supports load balancing to VPC and on-premises resources.
- Facilitates routing to multiple IP addresses and network interfaces on the same instance.
- Offers flexibility with microservice based architectures, simplifying inter-application communication.
- Supports IPv6 targets, enabling end-to-end IPv6 communication, and IPv4-to-IPv6 NAT.

**Lambda function**

- Facilitates routing to a single Lambda function.
- Accessible to Application Load Balancers only.

**Application Load Balancer**

- Offers the flexibility for a Network Load Balancer to accept and route TCP requests within a specific VPC.
- Facilitates using static IP addresses and PrivateLink with an Application Load Balancer.

Target group name

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

Protocol

TCP ▼

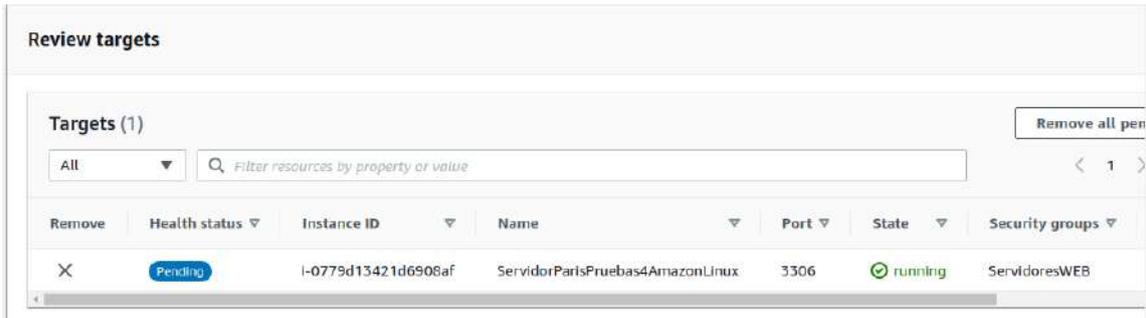
Port

: 3306 ▲▼

En esta ocasión solo pondremos una instancia por target group. El primero:

Remove	Health status	Instance ID	Name	Port	State	Security groups
	Pending	i-0e060585afce6bcab9	ServidorParisPruebas1AmazonLinux	3306	running	ServidoresWEB

Y el segundo Target Group:



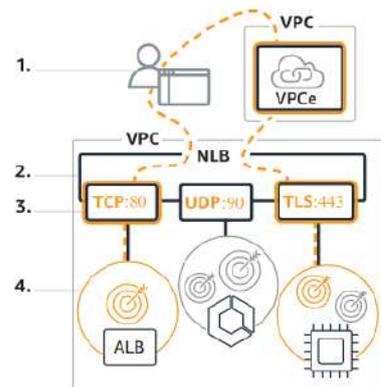
Ahora creamos el NLB

### Create Network Load Balancer [Info](#)

The Network Load Balancer distributes incoming TCP and UDP traffic across multiple targets such as Amazon EC2 instances, microservices, and containers. When the load balancer receives a connection request, it selects a target based on the protocol and port that are specified in the listener configuration, and the routing rule specified as the default action.

#### How Network Load Balancers work

1. Your client makes a request to your application.
2. The load balancer receives the request either directly or through an endpoint for private connectivity (via AWS PrivateLink).
3. The listeners in your load balancer receive requests of matching protocol and port, and route these requests based on the default action that you specify. You can use a TLS listener to offload the work of encryption and decryption to your load balancer.
4. Healthy targets in one or more target groups receive traffic according to the flow hash algorithm.



Tengo que escoger la VPC y las subnets involucradas

### Network mapping [Info](#)

The load balancer routes traffic to targets in the selected subnets, and in accordance with your IP address settings.

#### VPC

Select the virtual private cloud (VPC) for your targets. Only VPCs with an internet gateway are enabled for selection. The selected VPC cannot be changed after the load balancer is created. To confirm the VPC for your targets, view your [target groups](#).

mi-vpc-prueba  
vpc-06efcfd12f7a7228f  
IPv4: 10.0.0.0/24

[Refresh](#)

#### Mappings

Select at least one Availability Zone and one subnet for each zone. We recommend selecting at least two Availability Zones. The load balancer will route traffic only to targets in the selected Availability Zones. Zones that are not supported by the load balancer or VPC cannot be selected. Subnets can be added, but not removed, once a load balancer is created.

eu-west-3a

Subnet  
subnet-048e5fac71f2ddd18      subnet-publica-2

IPv4 settings

IPv4 address  
Assigned by AWS

---

eu-west-3b

Subnet  
subnet-07ae07fa8707974bb      subnet-publica

IPv4 settings

IPv4 address  
Assigned by AWS

En el listener ponemos 2 puertos, 3306 y 3307. Los puertos de entrada es indiferente, pero iremos a los puertos 3306 de cada uno de los targets, que tienen una instancia distinta.

### Listeners and routing [Info](#)

A listener is a process that checks for connection requests using the port and protocol you configure. The rules that you define for a listener determine how the load balancer routes requests to its registered targets.

▼ Listener TCP:3306 [Remove](#)

Protocol: TCP    Port: 3306  
1-65535

Default action [Info](#)  
Forward to: GruposMariadb  
Target type: Instance, IPv4

[Create target group](#)

---

▼ Listener TCP:3307 [Remove](#)

Protocol: TCP    Port: 3307  
1-65535

Default action [Info](#)  
Forward to: mysql2  
Target type: Instance, IPv4

[Create target group](#)

[Add listener](#)

El resumen:

**Summary**  
Review and confirm your configurations. [Estimate cost](#)

<b>Basic configuration</b> <a href="#">Edit</a> NLBproof <ul style="list-style-type: none"><li>Internet-facing</li><li>IPv4</li></ul>	<b>Network mapping</b> <a href="#">Edit</a> VPC <a href="#">vpc-06efefd12f7a7228f</a> mi-vpc-prueba <ul style="list-style-type: none"><li>eu-west-3a <a href="#">subnet-048e5fec71f2ddd18</a> subnet-publica-2</li><li>eu-west-3b <a href="#">subnet-07ae07fa8707974bb</a> subnet-publica</li></ul>	<b>Listeners and routing</b> <a href="#">Edit</a> <ul style="list-style-type: none"><li>TCP:3306 defaults to <a href="#">GruposMariadb</a></li><li>TCP:3307 defaults to <a href="#">mysql2</a></li></ul>	<b>Tags</b> <a href="#">Edit</a> None
--	---	--	--

**Attributes**

*i* Certain default attributes will be applied to your load balancer. You can view and edit them after creating the load balancer.

En estos listener no hay reglas como en el ALB

Load balancer: NLBproof

Description | **Listeners** | Monitoring | Integrated services | Tags

Listeners listen for connection requests using their protocol and port. You can add, remove, or update listeners and listener rules.

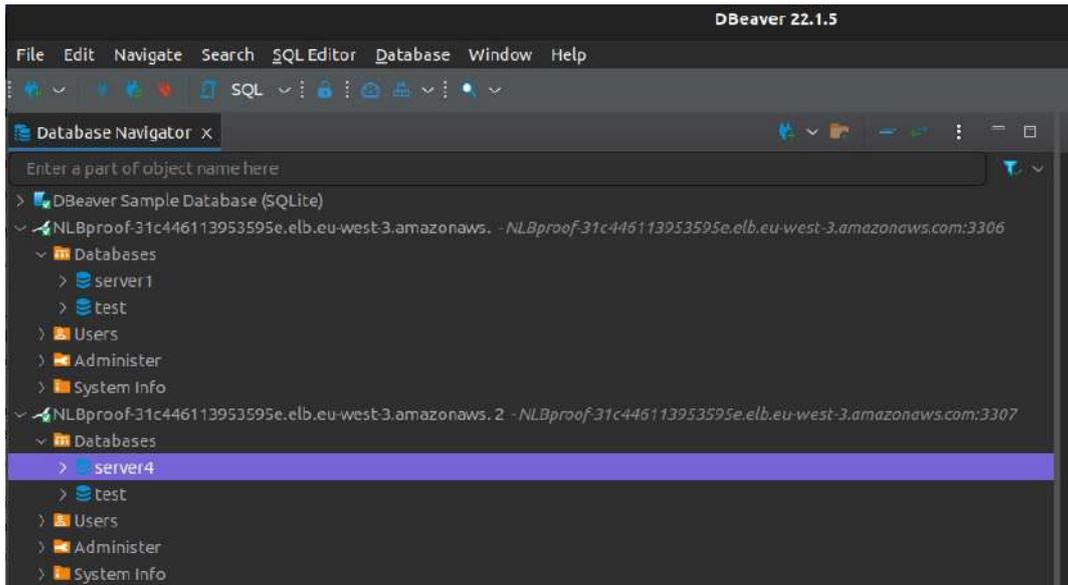
To view and edit listener attributes, select the listener and choose Edit.

[Add listener](#) [Edit](#) [Delete](#)

<input type="checkbox"/>	Listener ID	Security policy	SSL Certificate	ALPN policy	Default action
<input type="checkbox"/>	TCP : 3306 arn...4c9b699ebba360a8 ▾	N/A	N/A	N/A	forwarding to <a href="#">GruposMariadb</a>
<input type="checkbox"/>	TCP : 3307 arn...d70d12c53d1a0f6b ▾	N/A	N/A	N/A	forwarding to <a href="#">mysql2</a>

En los servicios integrados, además del Global Accelerator también tenemos el VPC Endpoint Services y el Traffic Mirroring..

Ahora para probar el balanceador tendremos que entrar en los servidores por los dos puertos en el mismo DNS del balanceador



## 12.5. - Línea de comandos NLB

También es con aws elbv2. Por ejemplo, describe-load-balancers

```
administrador@ubuntu:~$ aws elbv2 describe-load-balancers
{
  "LoadBalancers": [
    {
      "LoadBalancerArn": "arn:aws:elasticloadbalancing:eu-west-3:992365247711:loadbalancer/net/NLBproof/31c446113953595e",
      "DNSName": "NLBproof-31c446113953595e.elb.eu-west-3.amazonaws.com",
      "CanonicalHostedZoneId": "Z1CMS0P5QUZ6D5",
      "CreatedTime": "2022-08-23T21:07:44.789600+00:00",
      "LoadBalancerName": "NLBproof",
      "Scheme": "internet-facing",
      "VpcId": "vpc-06efefd12f7a7228f",
      "State": {
        "Code": "active"
      },
      "Type": "network",
      "AvailabilityZones": [
        {
          "ZoneName": "eu-west-3a",
          "SubnetId": "subnet-048e5fac71f2ddd18",
          "LoadBalancerAddresses": []
        },
        {
          "ZoneName": "eu-west-3b",
          "SubnetId": "subnet-07ae07fa8707974bb",
          "LoadBalancerAddresses": []
        }
      ],
      "IpAddressType": "ipv4"
    }
  ]
}
```

Para borrar es con delete-load-balancer con la opción para indicar el arn --load-balancer-arn

```
administrador@ubuntu:~$ aws elbv2 delete-load-balancer --load-balancer-arn arn:aws:elasticloadbalancing:eu-west-3:992365247711:loadbalancer/net/NLBproof/31c446113953595e
administrador@ubuntu:~$ aws elbv2 describe-load-balancers
{
  "LoadBalancers": []
}
```

Ahora pido información de los target groups

```

administrador@ubuntudocker:~$ aws elbv2 describe-target-groups
{
  "TargetGroups": [
    {
      "TargetGroupArn": "arn:aws:elasticloadbalancing:eu-west-3:992365247711:targetgroup/GruposMariadb/7061712c9cc52469",
      "TargetGroupName": "GruposMariadb",
      "Protocol": "TCP",
      "Port": 3306,
      "VpcId": "vpc-06efefd12f7a7228f",
      "HealthCheckProtocol": "TCP",
      "HealthCheckPort": "traffic-port",
      "HealthCheckEnabled": true,
      "HealthCheckIntervalSeconds": 30,
      "HealthCheckTimeoutSeconds": 10,
      "HealthyThresholdCount": 3,
      "UnhealthyThresholdCount": 3,
      "LoadBalancerArns": [],
      "TargetType": "instance",
      "IpAddressType": "ipv4"
    },
    {
      "TargetGroupArn": "arn:aws:elasticloadbalancing:eu-west-3:992365247711:targetgroup/mysql2/ee24752c9523dfeb",
      "TargetGroupName": "mysql2",
      "Protocol": "TCP",
      "Port": 3306,
      "VpcId": "vpc-06efefd12f7a7228f",
      "HealthCheckProtocol": "TCP",
      "HealthCheckPort": "traffic-port",
      "HealthCheckEnabled": true,
      "HealthCheckIntervalSeconds": 30,
      "HealthCheckTimeoutSeconds": 10,
      "HealthyThresholdCount": 3,
      "UnhealthyThresholdCount": 3,
      "LoadBalancerArns": [],
      "TargetType": "instance",
      "IpAddressType": "ipv4"
    }
  ]
}
administrador@ubuntudocker:~$ █

```

Y borro primero uno

```

administrador@ubuntudocker:~$ aws elbv2 delete-target-group --target-group-arn arn:aws:elasticloadbalancing:eu-west-3:992365247711:targetgroup/GruposMariadb/7061712c9cc52469
administrador@ubuntudocker:~$ aws elbv2 describe-target-groups
{
  "TargetGroups": [
    {
      "TargetGroupArn": "arn:aws:elasticloadbalancing:eu-west-3:992365247711:targetgroup/mysql2/ee24752c9523dfeb",
      "TargetGroupName": "mysql2",
      "Protocol": "TCP",
      "Port": 3306,
      "VpcId": "vpc-06efefd12f7a7228f",
      "HealthCheckProtocol": "TCP",
      "HealthCheckPort": "traffic-port",
      "HealthCheckEnabled": true,
      "HealthCheckIntervalSeconds": 30,
      "HealthCheckTimeoutSeconds": 10,
      "HealthyThresholdCount": 3,
      "UnhealthyThresholdCount": 3,
      "LoadBalancerArns": [],
      "TargetType": "instance",
      "IpAddressType": "ipv4"
    }
  ]
}
administrador@ubuntudocker:~$ █

```

Y luego el otro

```

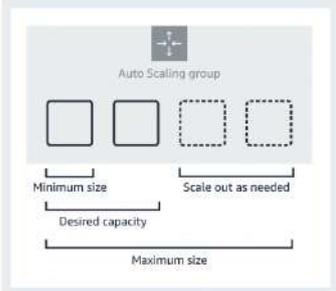
administrador@ubuntudocker:~$ aws elbv2 delete-target-group --target-group-arn arn:aws:elasticloadbalancing:eu-west-3:992365247711:targetgroup/mysql2/ee24752c9523dfeb
administrador@ubuntudocker:~$ aws elbv2 describe-target-groups
{
  "TargetGroups": []
}
administrador@ubuntudocker:~$ █

```

## TEMA 13 - EC2 Grupos de Autoescalada. AutoScaling Groups

Los grupos de autoescalada son un conjunto de instancias EC2 que van a poder escalar hacia arriba o hacia abajo dependiendo de ciertas características. Por ejemplo, cuando se dispare el consumo de CPU.

### How it works



An Auto Scaling group is a collection of Amazon EC2 instances that are treated as a logical unit. You configure settings for a group and its instances as well as define the group's minimum, maximum, and desired capacity. Setting different minimum and maximum capacity values forms the bounds of the group, which allows the group to scale as the load on your application spikes higher or lower, based on demand. To scale the Auto Scaling group, you can either make manual adjustments to the desired capacity or let Amazon EC2 Auto Scaling automatically add and remove capacity to meet changes in demand.

When launching fleets of instances, you can specify what percentage of your capacity should be fulfilled by On-Demand instances, and what percentage with Spot instances, to save up to 90% on EC2 costs. Amazon EC2 Auto Scaling lets you provision and balance capacity across Availability Zones to optimize availability. It also provides lifecycle hooks, instance health checks, and scheduled scaling to automate capacity management.

### Pricing

Amazon EC2 Auto Scaling features have no additional fees beyond the service fees for Amazon EC2, CloudWatch (for scaling policies), and the other AWS resources that you use. Visit the pricing page of each service to learn more.

### Getting started [↗](#)

- [What is Amazon EC2 Auto Scaling?](#)
- [Getting started with Amazon EC2 Auto Scaling](#)
- [Set up a scaled and load-balanced application](#)
- [FAQ](#)

Un grupo autoescalada tendrá un mínimo de instancias con un tamaño mínimo, un tamaño deseado y escalará cuando se necesite hasta el tamaño máximo que indiquemos.

Es muy útil cuando se tienen picos de tráfico temporal. Por ejemplo, una e-commerce que triplica las visitas los fines de semana, con el autoescalado se adaptaría al tráfico.

Las reglas del escalado se pueden crear basándose en la **CPU**, según las métricas del Amazon **CloudWatch** y/o usando un **Elastic Load Balancing**.

### 13.1. - Diferencias entre Launch Templates y Launch Configuration

Las configuraciones de lanzamientos sirven para indicar las características de las instancias que se usarán para el grupo de autoescalada.

Amazon recomienda que en vez de utilizar Launch Configuration se utilice las plantillas de Launch Templates.

Launch Configuration no tiene tantas características, es más simple. Además solo se pueden utilizar con grupos de autoescalada mientras Launch Templates se puede utilizar también para crear instancias.

Es muy posible que AWS acabe eliminando las Launch Configuration.

## 13.2. - Crear una Launch Configuration

Tendremos que indicar el nombre, escoger el AMI (Cojo la personalizada con Apache) y el Tipo de instancia (escojo t2.small que es gratuita).

Luego, da la opción de que sean Spot Instances para ser más barato, el precio máximo a gastar por hora, el Perfil IAM (Identity Access Management), si queremos que la monitorización en CloudWatch sea detallada y la optimización EBS.

**Additional configuration - optional**

Purchasing option [Info](#)

Request Spot instances

Current price

- eu-west-3a: \$0.007900
- eu-west-3b: \$0.007900
- eu-west-3c: \$0.007900

Maximum price (per instance/hour)

\$ 0.01

IAM instance profile [Info](#)

Select IAM role

Monitoring [Info](#)

Enable EC2 instance detailed monitoring within CloudWatch

EBS-optimized instance

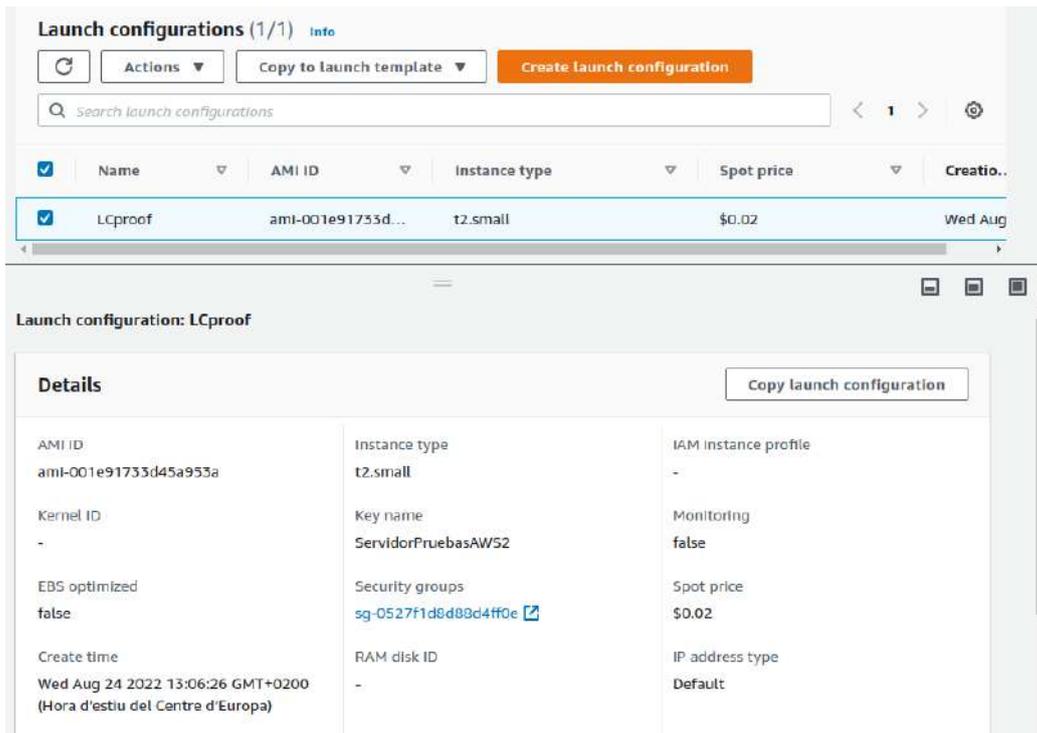
Launch as EBS-optimized instance

▶ Advanced details

ⓘ Later, if you want to use a different launch configuration, you can create a new one and apply it to any Auto Scaling group. Existing launch configurations cannot be edited.

Deberemos indicar los volúmenes, el grupo de seguridad y el archivo KeyPair para loguearse (Esto nos pide confirmación en un check). Y ya creamos,

Todas las instancias tendrán estos parámetros comunes.



### 13.3. - Crear una Launch Template

Ahora crearemos una plantilla basada en el AMIs para poder utilizarla también en los grupos de autoescalado.

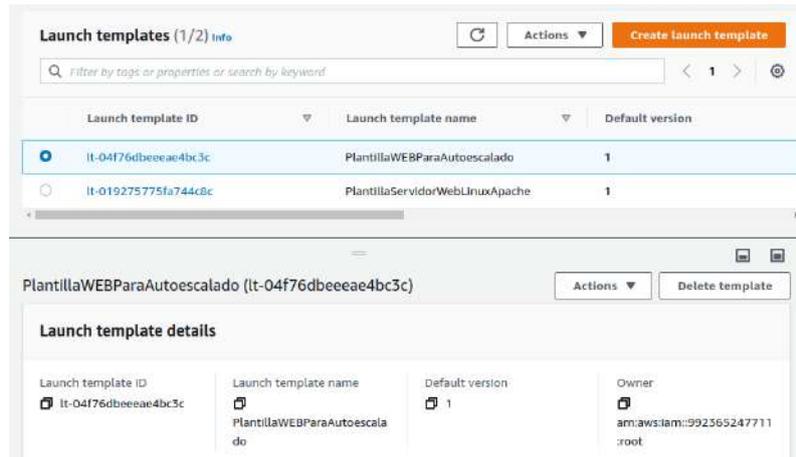
Al inicio hay un check para que la opciones se ajusten a una guía para el autoescalado



Selecciono la AMI que quiero para la plantilla, la AMIs con Linux y Apache.

Escogemos el tipo de instancia (t2.small), el key pair, la subred, el grupo de seguridad, el almacenamiento,

Si dejamos opciones vacías nos lo pedirá cuando lancemos el autoescalado.



### 13.4. - Crear un grupo de autoescalada

En Launch Template se puede cambiar a Launch configuration

The screenshot shows the 'Choose launch template or configuration' step in the AWS console. It features a title 'Choose launch template or configuration' with an 'Info' link. Below the title is a descriptive paragraph: 'Specify a launch template that contains settings common to all EC2 instances that are launched by this Auto Scaling group. If you currently use launch configurations, you might consider migrating to launch templates.' The form is divided into two main sections. The first section, titled 'Name', contains a sub-section 'Auto Scaling group name' with the instruction 'Enter a name to identify the group.' Below this is a text input field containing 'GrupoWEBautoescalada' and a note: 'Must be unique to this account in the current Region and no more than 255 characters.' The second section, titled 'Launch template' with an 'Info' link, has a 'Switch to launch configuration' link on the right. It contains a sub-section 'Launch template' with the instruction 'Choose a launch template that contains the instance-level settings, such as the Amazon Machine Image (AMI), instance type, key pair, and security groups.' Below this is a dropdown menu with the placeholder text 'Select a launch template' and a refresh icon. At the bottom left of this section is a link 'Create a launch template' with an external link icon. At the bottom right of the entire form are 'Cancel' and 'Next' buttons.

Por defecto aparece Launch template. En el **paso 1** seleccionamos la creada y hace un resumen de las características básicas.

Luego, en el **paso 2**, se pueden cambiar algunas opciones como la VPC y las Azs (Se pueden indicar varias, escojo las públicas). También podemos indicar los requisitos de la instancia.

En el **paso 3** es el balanceador de carga, podemos indicar sin, con uno que exista o con uno que creamos. En Health check se creará un grupo para tan solo comprobar si las instancias se autoescalán estresandoles cada x tiempo. Por último se podrán añadir métricas adicionales en CloudWatch.

El **paso 4** es el más importante, es la configuración del tamaño del grupo y las reglas de escalada.

**Group size - optional** [Info](#)

Specify the size of the Auto Scaling group by changing the desired capacity. You can also specify minimum and maximum capacity limits. Your desired capacity must be within the limit range.

**Desired capacity type**  
Choose the unit of measurement for the desired capacity value. By default, the desired capacity is measured in number of instances (units).

Units

**Desired capacity**

**Minimum capacity**

**Maximum capacity**

En las políticas se puede indicar el nombre, el tipo de métrica, el valor, el tiempo que espera para contabilizar el valor y si queremos no permitir que se autoescale hacia abajo.

**Scaling policies - optional**

Choose whether to use a scaling policy to dynamically resize your Auto Scaling group to meet changes in demand. [Info](#)

**Target tracking scaling policy**  
Choose a desired outcome and leave it to the scaling policy to add and remove capacity as needed to achieve that outcome.

None

**Scaling policy name**

**Metric type**

**Target value**

**Instances need**  
 seconds warm up before including in metric

Disable scale in to create only a scale-out policy

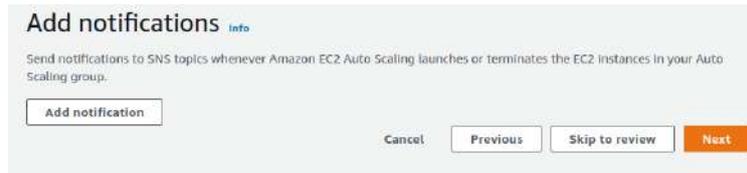
Además, podemos decir que no se tengan en cuenta los cierres cuando hagamos una política de scale-in, es decir, que no se elimine una instancia en el desescalado.

**Instance scale-in protection - optional**

**Instance scale-in protection**  
If protect from scale in is enabled, newly launched instances will be protected from scale in by default.

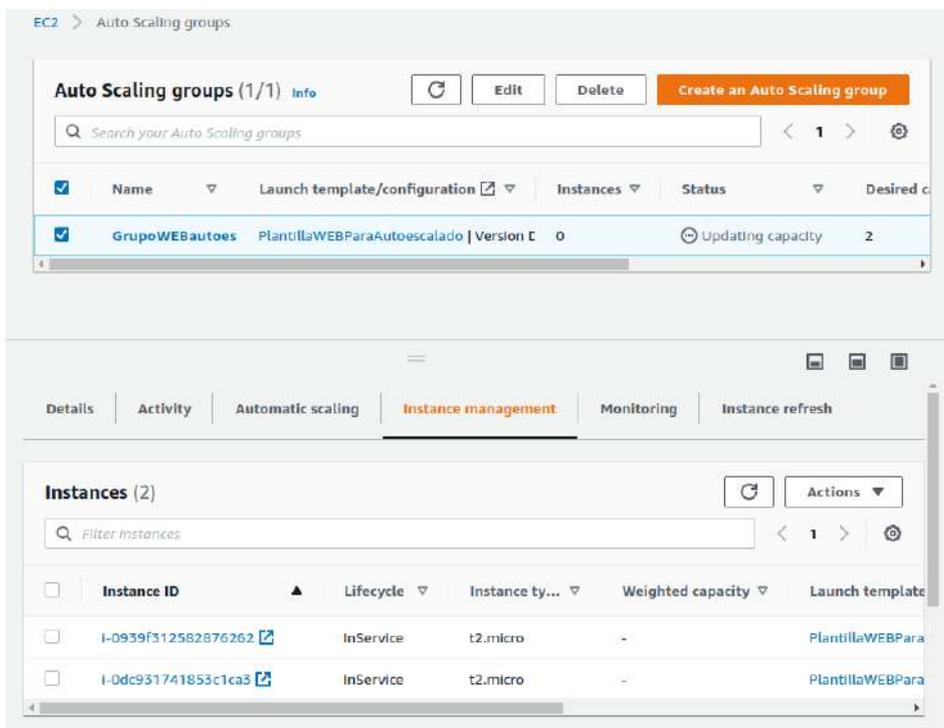
Enable instance scale-in protection

En el **paso 5** es que envíe notificaciones cuando efectúe autoescalado. Se envían por SNS (Simple Notification Service), se necesitan crear Topics.



Por último, **paso 6**, se pueden crear Tags específicas, como en todos los objetos y componentes de AWS. El **paso 7** es tan solo una revisión de las opciones seleccionadas.

Una vez creado el grupo de autoescalada empezará a crear las instancias. CUIDADO. Cuando inicie la creación de grupo de autoescalada tenía recién creada la AMIs y el Launch Template seleccionado. Me ha dado problemas para acabar de crear el grupo de autoescalada y he tenido que volver al paso 1 para sincronizar los datos.



### 13.5. - Propiedades grupo de autoescalada

**Detalles** – Con un resumen de las características del grupo. Se pueden editar en cada uno de los grupos.

**Activity** – Aparece un historial de los sucesos. Aquí se pueden activar notificaciones.

The screenshot shows the AWS console interface for an AutoScaling Group. The top navigation bar includes tabs for Details, Activity, Automatic scaling, Instance management, Monitoring, and Instance refresh. The 'Activity' tab is selected.

**Activity notifications (0)**

Filter notifications:

Send to:  On instance action

No notifications are currently specified

[Create notification](#)

**Activity history (2)**

Filter activity history:

Status	Description	Cause
Successful	Launching a new EC2 instance: i-Odc931741853c1ca5	At 2022-08-24T12:04:45Z a user request created an AutoScalingGroup changing the desired capacity from 0 to 2. At 2022-08-24T12:04:50Z an instance was started in response to a difference between the desired and actual capacity, increasing the capacity from 0 to 2.
Successful	Launching a new EC2 instance: i-O939f312582876262	At 2022-08-24T12:04:45Z a user request created an AutoScalingGroup changing the desired capacity from 0 to 2. At 2022-08-24T12:04:50Z an instance was started in response to a difference between the desired and actual capacity, increasing the capacity from 0 to 2.

**Automatic scaling** – Se puede indicar el autoescalado.

The screenshot shows the 'Automatic scaling' tab in the AWS console. It displays two sections: 'Dynamic scaling policies (1)' and 'Predictive scaling policies (0)'. The 'Dynamic scaling policies' section is expanded to show a policy named 'Demasiada CPU'.

**Dynamic scaling policies (1)**

[Create dynamic scaling policy](#)

**Demasiada CPU**

Policy type: Target tracking scaling

Enabled or disabled? Enabled

Execute policy when: As required to maintain Average CPU utilization at: 10

Take the action: Add or remove capacity units as required

Instances need: 300 seconds to warm up before including in metric

Scale in: Enabled

**Predictive scaling policies (0)**

[Create predictive scaling policy](#)

No predictive scaling policies have been created

Predictive scaling policies use historical data to scale out your group ahead of forecasted hourly load.

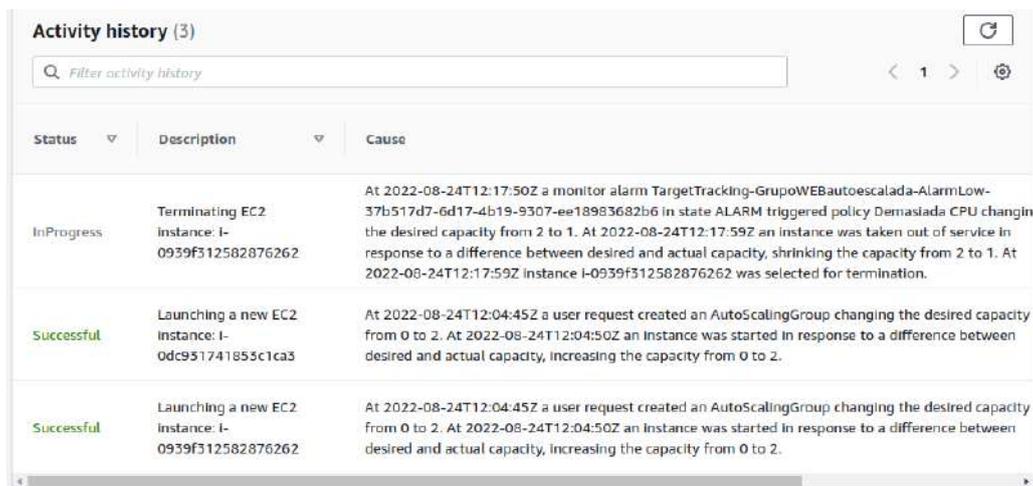
**Instance management** – Gestión de las instancias que conforman el grupo. Se puede añadir un Lifecycle Hooks, lanzando acciones concretas cuando se cambia el estado del objeto.

**Monitoring** – Monitorización de autoescalada y de las instancias EC2

**Instance refresh** – Apareceran las actualizaciones de las instancias. Por ejemplo, para poner actualizaciones de la aplicación que tengamos en las instancias.

## 13.6. - Comportamiento del autoescalado. Prueba

Al pasar un tiempo (300s), en activity se puede ver como ha terminado con una instancia



Status	Description	Cause
InProgress	Terminating EC2 instance: I-0939f312582876262	At 2022-08-24T12:17:50Z a monitor alarm TargetTracking-GrupoWEBautoescalada-AlarmLow-37b517d7-6d17-4b19-9307-ee18983682b6 in state ALARM triggered policy Demasiada CPU changing the desired capacity from 2 to 1. At 2022-08-24T12:17:59Z an instance was taken out of service in response to a difference between desired and actual capacity, shrinking the capacity from 2 to 1. At 2022-08-24T12:17:59Z instance I-0939f312582876262 was selected for termination.
Successful	Launching a new EC2 instance: I-0dc951741855c1ca3	At 2022-08-24T12:04:45Z a user request created an AutoScalingGroup changing the desired capacity from 0 to 2. At 2022-08-24T12:04:50Z an Instance was started in response to a difference between desired and actual capacity, increasing the capacity from 0 to 2.
Successful	Launching a new EC2 instance: I-0939f312582876262	At 2022-08-24T12:04:45Z a user request created an AutoScalingGroup changing the desired capacity from 0 to 2. At 2022-08-24T12:04:50Z an Instance was started in response to a difference between desired and actual capacity, increasing the capacity from 0 to 2.

Es debido a qué para mantener menos del 10% de CPU indicado en la política «Demasiada CPU» se puede con tan solo una instancia.

Vamos a la instancia que está corriendo y le lanzamos un proceso pesado. Nos conectamos a través de SSH y utilizaremos un programa para estresar la CPU. Stress de Epel (Es de Red Hat, allí se puede instalar directamente con yum install). En ubuntu, debian y demás es otra forma para instalarlo.

Como tenemos Amazon Linux 2 tendremos que instalar un programa que nos permitirá instalar repositorios externos, como EPEL:

```
sudo yum install -y amazon-linux-extras
```

Ya está instalado. Ahora instalamos el repositorio EPEL

```
sudo amazon-linux-extras install epel
```

Y ahora ya podemos instalar el programa en concreto, que se llama stress.

```
Sudo yum install -y stress
```

Opciones de stress

```
`stress' imposes certain types of compute stress on your system
```

Usage: stress [OPTION [ARG]] ...

-?, --help show this help statement  
--version show version statement  
-v, --verbose be verbose  
-q, --quiet be quiet  
-n, --dry-run show what would have been done  
-t, --timeout N timeout after N seconds  
--backoff N wait factor of N microseconds before work starts  
-c, --cpu N spawn N workers spinning on sqrt()  
-i, --io N spawn N workers spinning on sync()  
-m, --vm N spawn N workers spinning on malloc()/free()  
--vm-bytes B malloc B bytes per vm worker (default is 256MB)  
--vm-stride B touch a byte every B bytes (default is 4096)  
--vm-hang N sleep N secs before free (default none, 0 is inf)  
--vm-keep redirty memory instead of freeing and reallocating  
-d, --hdd N spawn N workers spinning on write()/unlink()  
--hdd-bytes B write B bytes per hdd worker (default is 1GB)

Example: stress --cpu 8 --io 4 --vm 2 --vm-bytes 128M --timeout 10s

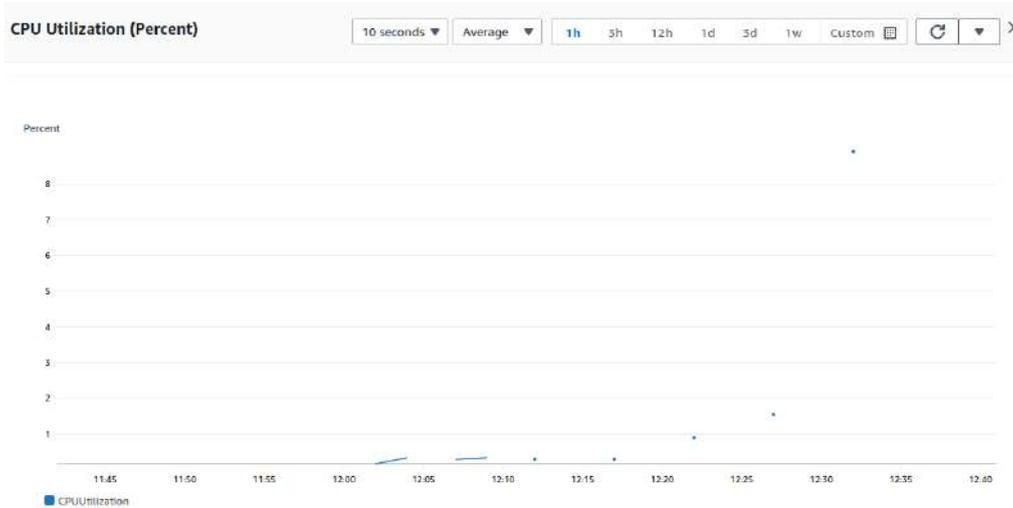
Note: Numbers may be suffixed with s,m,h,d,y (time) or B,K,M,G (size).

Vamos a estresar con más de 10 hooks de CPU

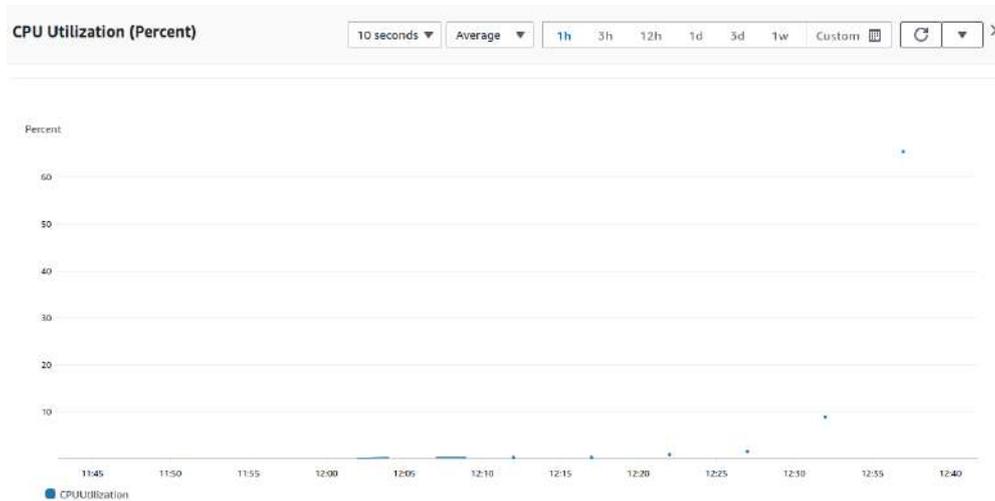
```
stress -c 10
```

```
[root@ip-10-0-0-30 ~]# stress -c 10  
stress: info: [4173] dispatching hogs: 10 cpu, 0 io, 0 vm, 0 hdd
```

En el grupo de autoescalada, podemos monitorizar el CPU de las instancias EC2



Cuando este 300 segundos usando más del 10% de CPU creará las instancias que considere necesario para adaptarse a los recursos.



En Activity se puede ver como crea 3 instancias más que considera necesarias, según los parámetros dados.

Status	Description	Cause
WaitingForInstanceWarmup	Launching a new EC2 Instance: I-0691327c70fba0ede	At 2022-08-24T12:42:34Z a monitor alarm TargetTracking-GrupoWEBautoescalada-AlarmHigh-6e6ef7c4-9950-45d1-9cb2-c7a569f24475 in state ALARM triggered policy Demasiada CPU changing the desired capacity from 1 to 4. At 2022-08-24T12:42:39Z an instance was started in response to a difference between desired and actual capacity, increasing the capacity from 1 to 4.
WaitingForInstanceWarmup	Launching a new EC2 Instance: I-025c183d18d3ba6a3	At 2022-08-24T12:42:34Z a monitor alarm TargetTracking-GrupoWEBautoescalada-AlarmHigh-6e6ef7c4-9950-45d1-9cb2-c7a569f24475 in state ALARM triggered policy Demasiada CPU changing the desired capacity from 1 to 4. At 2022-08-24T12:42:39Z an instance was started in response to a difference between desired and actual capacity, increasing the capacity from 1 to 4.
WaitingForInstanceWarmup	Launching a new EC2 Instance: I-06013478880496a77	At 2022-08-24T12:42:34Z a monitor alarm TargetTracking-GrupoWEBautoescalada-AlarmHigh-6e6ef7c4-9950-45d1-9cb2-c7a569f24475 in state ALARM triggered policy Demasiada CPU changing the desired capacity from 1 to 4. At 2022-08-24T12:42:39Z an instance was started in response to a difference between desired and actual capacity, increasing the capacity from 1 to 4.
Successful	Terminating EC2 Instance: I-0939f312582876262	At 2022-08-24T12:17:50Z a monitor alarm TargetTracking-GrupoWEBautoescalada-AlarmLow-37b517d7-6d17-4b19-9307-ee18983682b6 in state ALARM triggered policy Demasiada CPU changing the desired capacity from 2 to 1. At 2022-08-24T12:17:59Z an instance was taken out of service in response to a difference between desired and actual capacity, shrinking the capacity from 2 to 1. At 2022-08-24T12:17:59Z instance I-0939f312582876262 was selected for termination.
Successful	Launching a new EC2 Instance: I-0dc931741853c1ca3	At 2022-08-24T12:04:45Z a user request created an AutoScalingGroup changing the desired capacity from 0 to 2. At 2022-08-24T12:04:50Z an instance was started in response to a difference between desired and actual capacity, increasing the capacity from 0 to 2.
Successful	Launching a new EC2 Instance: I-0939f312582876262	At 2022-08-24T12:04:45Z a user request created an AutoScalingGroup changing the desired capacity from 0 to 2. At 2022-08-24T12:04:50Z an instance was started in response to a difference between desired and actual capacity, increasing the capacity from 0 to 2.

Ahora desactivo el stress con CTRL C y entonces volverá a la normalidad, terminando las 3 instancias. Ha tardado unos 30 minutos

### 13.7. - Opciones adicionales

Creamos un nuevo grupo para darle opciones.

Utilizaremos una plantilla sin spot para poder modificarlo.

En los tipos de requerimientos de las instancias seleccionaremos «Override launch template» para ver más opciones. Se puede seleccionar parámetros concretos de CPUs y memoria para que seleccione tipos concretos de instancias.

### Instance type requirements [Info](#)

You can keep the same instance attributes or instance type from your launch template, or you can choose to override the launch template by specifying different instance attributes or manually adding instance types.

[Reset to launch template](#)

**Specify instance attributes**  
Provide your compute requirements. We fulfill your desired capacity with matching instance types based on your allocation strategy selection.

**Manually add instance types**  
Add one or more instance types. Any of the instance types may be launched to fulfill your desired capacity based on your allocation strategy selection.

#### Required instance attributes

Enter your compute requirements in virtual CPUs (vCPUs) and memory.

**vCPUs**  
Enter the minimum and maximum number of vCPUs per instance.

<input type="text" value="0"/>	<input type="text" value="0"/>
minimum	maximum
<input type="checkbox"/> No minimum	<input type="checkbox"/> No maximum

**Memory (GiB)**  
Enter the minimum and maximum GiBs of memory per instance.

<input type="text" value="0"/>	<input type="text" value="0"/>
minimum	maximum
<input type="checkbox"/> No minimum	<input type="checkbox"/> No maximum

**Additional instance attributes - optional**  
Add instance attributes to further limit which instance types may be used to fulfill your desired capacity.

[Add attribute](#)

**► Preview matching instance types (0)**  
This list includes all the instance types that match your compute requirements. Amazon EC2 may provision from any of these instance types. The exact instance types that are used to fulfill your desired capacity depend on the allocation strategy you choose and available capacity.

Y se podrían añadir los tipos concretos. También se puede seleccionar manualmente, parametrando el porcentaje de uso del ancho total tendrá cada tipo de instancia

Specify instance attributes  
Provide your compute requirements. We fulfill your desired capacity with matching instance types based on your allocation strategy selection.

Manually add instance types  
Add one or more instance types. Any of the instance types may be launched to fulfill your desired capacity based on your allocation strategy selection.

Choose the instance types that best suit the needs of your application.

Primary instance type Weight [Info](#)

1.  1vCPU 1 Gib Memory

The above instance type is prepopulated from your launch template, but you can change it.

Additional instance types

Redo recommendations

2.  1vCPU 2 Gib Memory

3.  2vCPU 4 Gib Memory

También se puede escoger un porcentaje On-Demand y Spot

También se puede escoger si se tendrá en cuenta para In-Demand la prioridad anterior o el precio más bajo. Y en las Spot la capacidad optimizada o el precio más bajo.

**Allocation strategies** [Info](#)

**On-Demand allocation strategy**  
Choose the allocation strategy to apply to your On-Demand Instances when they are launched.

**Prioritized**  
Launch On-Demand Instances based on the priority order of Instance types you set above.

**Lowest price**  
Launch On-Demand Instances from the lowest priced Instance pools.

**Spot allocation strategy**  
Choose the allocation strategy to apply to your Spot Instances when they are launched.

**Capacity optimized (recommended)**  
Launch Spot Instances optimally based on the available Spot capacity.

**Lowest price**  
Launch Spot Instances from the lowest priced instance pools.

**Instance**  **Prioritize instance types** [Info](#)  
You set the priority order for your Instance types, and EC2 attempts to fulfill Spot capacity based on these priorities while still optimizing for capacity.

**Instance:**  **Capacity rebalance** [Info](#)  
When you enable capacity rebalancing, and a rebalance notification is sent to an Instance, EC2 Auto Scaling automatically attempts to replace the Instance before it is interrupted. Instances are

To run fault-tolerant applications, you should use Spot Instances with capacity rebalancing. Spot Instances are spare EC2 capacity that offer steep discounts compared to On-Demand prices that AWS can interrupt with a 2-minute notification.

% On-Demand

% Spot

**Include On-Demand base capacity**  
Specify how much On-Demand capacity the Auto Scaling group should have for its base portion before scaling by percentages. The maximum group size will be increased (but not decreased) to this value.

En el paso 3 podemos elegir un balanceador. Como ahora mismo no tenemos ninguno vamos a crearlo.

Como hemos escogido el esquema de internet-facing, necesitamos que las dos subredes para balancear sean públicas.

**Network mapping**  
Your new load balancer will be created using the same VPC and Availability Zone selections as your Auto Scaling group. You can select different subnets and add subnets from additional Availability Zones.

**VPC**  
vpc-06efefd12f7a7228f [mi-vpc-prueba](#)

**Availability Zones and subnets**  
You must select a single subnet for each Availability Zone enabled. Only public subnets are available for selection to support DNS resolution.

eu-west-3a

eu-west-3b

Use the options below to attach your Auto Scaling group to an existing load balancer, or to a new load balancer that you define.

**No load balancer**  
Traffic to your Auto Scaling group will not be fronted by a load balancer.

**Attach to an existing load balancer**  
Choose from your existing load balancers.

**Attach to a new load balancer**  
Quickly create a basic load balancer to attach to your Auto Scaling group.

**Attach to a new load balancer**  
Define a new load balancer to create for attachment to this Auto Scaling group.

**Load balancer type**  
Choose from the load balancer types offered below. Type selection cannot be changed after the load balancer is created. If you need a different type of load balancer than those offered here, [visit the Load Balancing console](#).

**Application Load Balancer**  
HTTP, HTTPS

**Network Load Balancer**  
TCP, UDP, TLS

**Load balancer name**  
Name cannot be changed after the load balancer is created.

**Load balancer scheme**  
Scheme cannot be changed after the load balancer is created.

**Internal**

**Internet-facing**

En Target Group tampoco tenemos ninguno así que lo creamos, pero en este caso las instancias serán añadidas tal y como las cree el grupo de autoescalado.

**Listeners and routing**

If you require secure listeners, or multiple listeners, you can configure them from the [Load Balancing console](#) after your load balancer is created.

<b>Protocol</b>	<b>Port</b>	<b>Default routing (forward to)</b>
HTTP	80	Create a target group ▼
<b>New target group name</b>		
An instance target group with default settings will be created.		
GrupoWEBautoescalada2-1		

Esta vez le damos más capacidad

**Configure group size and scaling policies** Info

Set the desired, minimum, and maximum capacity of your Auto Scaling group. You can optionally add a scaling policy to dynamically scale the number of instances in the group.

**Group size - optional** Info

Specify the size of the Auto Scaling group by changing the desired capacity. You can also specify minimum and maximum capacity limits. Your desired capacity must be within the limit range.

Desired capacity

Minimum capacity

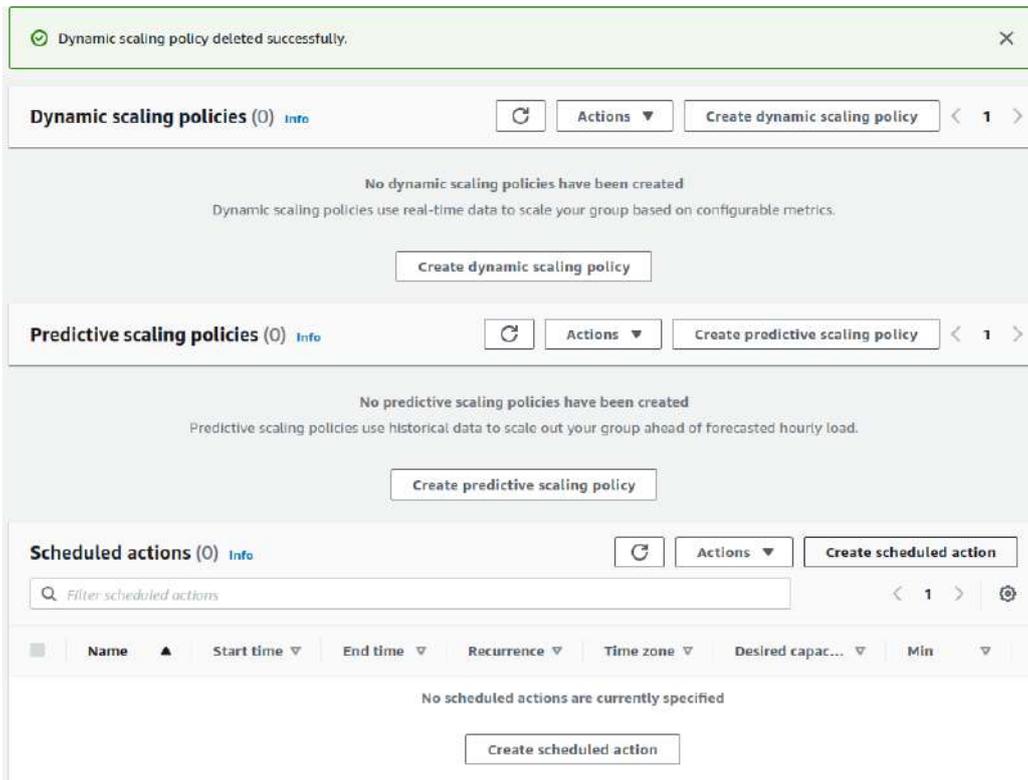
Maximum capacity

Ahora creará el conjunto de instancias que crea necesarias. Si nos vamos a Load Balancer podremos ver el Grupo creado y en Target Groups el grupo con las instancias que se van creando en el autoescalado.

Cuando eliminamos un grupo de autoescalada se elimina también las instancias, pero no el balanceador de carga y ni el target group del balanceador. CUIDADO QUE COBRAN

## 13.8. - Política de escalado. Simple y Step

En Automatic scaling del grupo 1 de autoescalada borramos la política de «Demasiada CPU» creada anteriormente.



Creamos una nueva política de escalada donde podemos seguir estos parámetros según el **tipo de política** que se escoge.

- **Target tracking scaling** – Por defecto
  - Nombre
  - Tipo de métrica
    - CPU
    - Tráfico entrante (bytes)
    - Tráfico saliente (bytes)
    - Load Balancer
  - Valor de la métrica
  - Tiempo que espera contabilizando el valor para realizar acción.
  - Si queremos no permitir que se autoescale hacia abajo.
- **Step scaling** – Permite poner rangos
  - Nombre
  - Alarma CloudWatch – Es obligatoria ponerla, no deja editar la acción si no la pones.
  - Acción

- Añadir, borrar o cargar
- Unidad
- Tipo de unidad (Unidad o porcentaje)
- RANGO - when (Cuando el valor está entre n y n)
- Tiempo que espera contabilizando el valor para realizar acción

**Create dynamic scaling policy**

Policy type: Step scaling

Scaling policy name: Subida de Maquina

CloudWatch alarm: prueba

Create = CloudWatch alarm [Create = CloudWatch alarm](#)  
 breaches the alarm threshold: DatabaseConnections > 2 for 1 consecutive periods of 300 seconds for the metric dimensions:  
 DBInstanceIdentifier = mariadb1

Take the action: Add

1 capacity units when 2 <= DatabaseConnections < 5

5 capacity units when 5 <= DatabaseConnections < +infinity

Instances need: 300 seconds warm up before including in metric

- **Simple scaling** – El simple. Lo normal es que sea la alarma quien dispare la acción.
  - Nombre
  - Alarma CloudWatch – Puede estar asociado además a una alarma.
  - Acción
    - Añadir, borrar o cargar
    - Unidad
    - Tipo de unidad (Unidad o porcentaje)
  - Tiempo que espera contabilizando el valor para realizar acción

**PoliticaSimpleEliminar**

Policy type:  
Simple scaling

Enabled or disabled?  
Enabled

Execute policy when:  
No alarm selected

Take the action:  
Remove 1 capacity units

And then wait:  
0 seconds before allowing another scaling activity

Se pueden ejecutar las políticas manualmente

**Dynamic scaling policies (1/1)** [Info](#)

**PoliticaSimpleEliminar**

Policy type:  
Simple scaling

Enabled or disabled?  
Enabled

Execute policy when:  
No alarm selected

Take the action:  
Remove 1 capacity units

And then wait:  
0 seconds before allowing another scaling activity

**Actions** ▲

- Enable
- Disable
- Execute
- Edit
- Delete

## TEMA 14 - S3 Almacenamiento escalable en la nube

S3 (Simple Storage Service.) es un servicio de almacenamiento del tipo objeto, guarda objetos. Backups, entornos web, guardar resultados de AWS, etc. Realmente se puede guardar cualquier cosa.



Funciona con un componente que se llama bucket, que es una zona de almacenamiento donde podemos guardar objetos.

- Nos permite un sistema de acceso muy granulado para decidir quien accede a nuestros datos.
- Se puede optimizar el coste con distintos tipos de almacenamiento.
- Se puede replicar en cualquier region.
- Acceso On-premises (Desde mi propio CPD) o VPC.
- Practicamente indestructible.

Se puede usar para IA, analítica avanzada, Machine Learning, etc...

Productos con conectores con S3: Tablo, Oracle, Pentahoo, etc

### 14.1. - Buckets

Un bucket es un contenedor que almacena datos. S3 es global, aunque cuando los creas eliges una region concreta.

Los **nombres** no se pueden repetir en todo AWS, así que tiene que ser un nombre personalizado.

Se pueden crear buckets basados en otros que tengamos con **choose bucket**.

El número máximo de bucket que se pueden tener son 100. Cada bucket tiene espacio ilimitado, por ello no es necesario tener muchos.

Se puede habilitar **ACLs** en Object Ownership. Aquí se controlará quien será el propietario del bucket.

**Object Ownership** Info

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

**ACLs disabled (recommended)**

All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

**ACLs enabled**

Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

**Object Ownership**

**Bucket owner preferred**

If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.

**Object writer**

The object writer remains the object owner.

**?** If you want to enforce object ownership for new objects only, your bucket policy must specify that the bucket-owner-full-control canned ACL is required for object uploads. [Learn more](#)

AWS recomienda que seas propietario la cuenta actual y ya luego puedes dar otra propiedad.

Luego se puede bloquear el acceso, es donde se dan los permisos. Por defecto está todo bloqueado

**Block all public access**

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another:

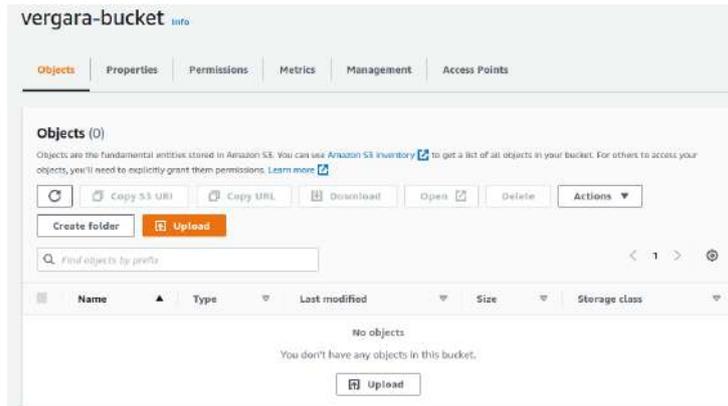
- Block public access to buckets and objects granted through new access control lists (ACLs)**  
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- Block public access to buckets and objects granted through any access control lists (ACLs)**  
S3 will ignore all ACLs that grant public access to buckets and objects.
- Block public access to buckets and objects granted through new public bucket or access point policies**  
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- Block public and cross-account access to buckets and objects through any public bucket or access point policies**  
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

Se puede habilitar el **versionado** del bucket.

Podemos **encriptar** los objetos del contenedor, el contenedor no se encripta.

También se pueden **bloquear** los objetos para que no se puedan cambiar.

Una vez creado podemos añadir los objetos que queramos.



El resto de pestañas son para ver/editar las propiedades, los permisos, la gestión y puentes de acceso. Además de una pestaña de métricas que se pueden personalizar.

Se puede crear una estructura de carpetas para ordenar los objetos. Dentro de cada carpeta puede tener propiedades diferentes.

Los niveles de almacenamiento son

Storage class

Amazon S3 offers a range of storage classes designed for different use cases. [Learn more](#) or see [Amazon S3 pricing](#)

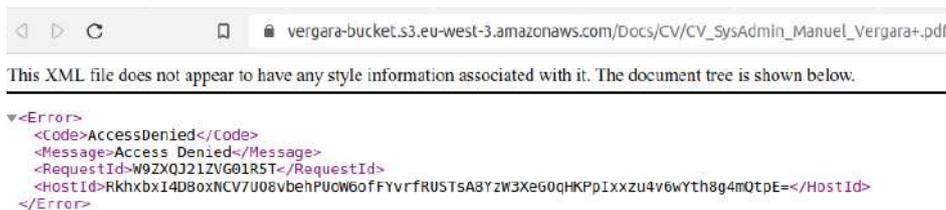
Storage class	Designed for	Availability Zones	Min storage duration	Min billable object size
Standard	Frequently accessed data (more than once a month) with milliseconds access	≥ 3	-	-
Intelligent-Tiering	Data with changing or unknown access patterns	≥ 3	-	-
Standard-IA	Infrequently accessed data (once a month) with milliseconds access	≥ 3	30 days	128 KB
One Zone-IA	Recreatable, infrequently accessed data (once a month) stored in a single Availability Zone with milliseconds access	1	30 days	128 KB
Glacier Instant Retrieval	Long-lived archive data accessed once a quarter with instant retrieval in milliseconds	≥ 3	90 days	128 KB
Glacier Flexible Retrieval (formerly Glacier)	Long-lived archive data accessed once a year with retrieval of minutes to hours	≥ 3	90 days	-
Glacier Deep Archive	Long-lived archive data accessed less than once a year with retrieval of hours	≥ 3	180 days	-
Reduced redundancy	Noncritical, frequently accessed data with milliseconds access (not recommended as S3 Standard is more cost effective)	≥ 3	-	-

## 14.2. - Objetos

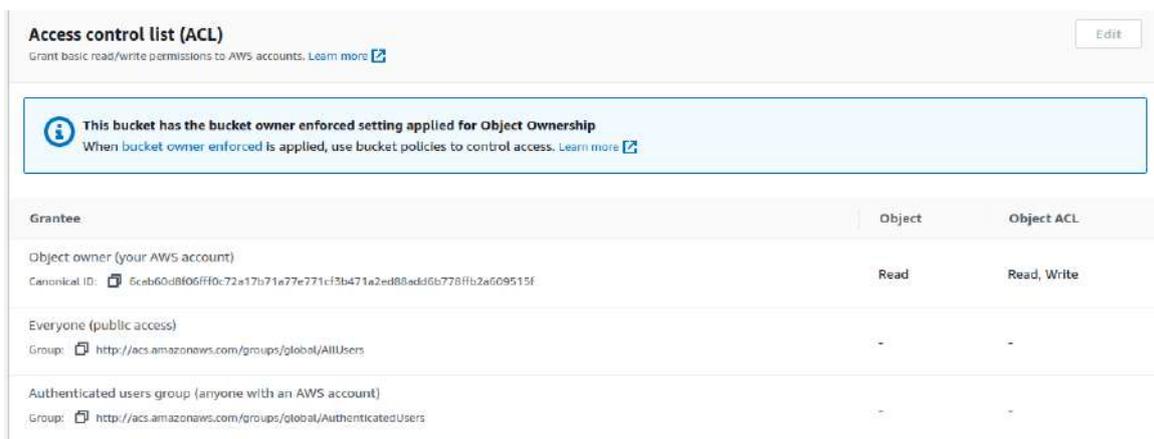
Un **objeto** tiene:

- **Propiedades**
  - **Key** – Un identificador único de cada objeto, que suele corresponder con el nombre y las estructura jerárquica. Una URI

- **Metadata** – Son las propiedades, definen y describen el objeto. Se pueden añadir más metadatos.
- **Uri S3** -
- **ARN** (Amazon Resource Name)
- **Etiqueta identitaria**
- **URL del objeto** - Sin permisos para acceder desde https aparece un error cuando entramos en el enlace



- **Permisos** – Si hemos dejado la propiedad a la cuenta actual hay que utilizar bucket policies para cambiar permisos. Nos indica quien es el propietario y qué permisos tiene. Por ejemplo, la cuenta propia, el acceso público y grupos de usuarios autenticados.



- **Versiones** – En versiones aparecerían los cambios si tuviésemos activado el versionado y con algún cambio efectuado.

En Objects actions existen varias opciones. Una de ella es «Share with a presigned URL» donde se puede compartir el objeto con un tiempo de expiración que determinamos.

### Share "CV\_SysAdmin\_Manuel\_Vergara .pdf" with a presigned URL ✕

Presigned URLs are used to grant access to an object for a limited time. [Learn more](#)

ⓘ Anyone can access the object with this presigned URL until it expires, even if the bucket, and object are private.

**Time interval until the presigned URL expires**  
 Using the S3 console, you can share an object with a presigned URL for up to 12 hours or until your session expires. To create a presigned URL with a longer time interval, use the AWS CLI or AWS SDK. Time intervals for presigned URLs can be restricted by your IAM policy.

Minutes  
 Hours

**Number of minutes**

30

Must be a whole number between 1 and 720.

After you create the presigned URL, it's automatically copied to your clipboard.

Cancel Create presigned URL



Además, se puede descargar, se puede calcular el tamaño total (Práctico para las carpetas), copiar, mover, renombrar, editar metadatos en forma valor-key (definidos por sistema o por propietario), etc

### 14.3. - Clases de almacenamiento

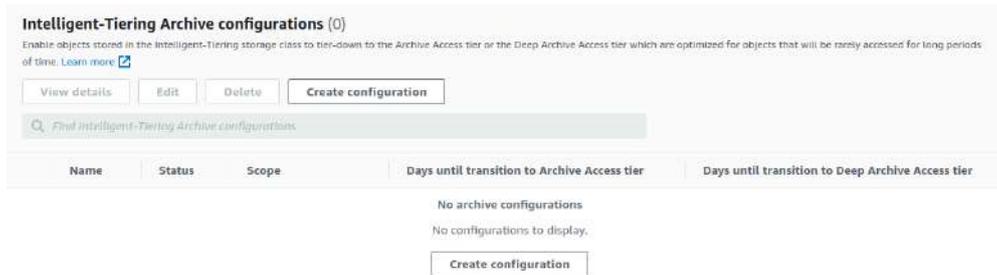
Dependiendo del uso que le demos al contenido tenemos varias clases de almacenamiento para economizar los costes. Cuando se sube objetos, AWS lo replica para tener acceso desde las distintas AZ.

Los niveles son:

- **Standard** – Documentos habituales. Una vez al mes. Es el más optimizado.
- **Intelligent-Tiering** – Cuando no se tiene claro el patrón de cambios, con esta opción es S3 quien determina la clase más adecuada. Lo determina a través de la monitorización de como se utiliza el objeto. Tiene un coste adicional pero si no se tiene claro como se va a usar el objeto es la mejor opción. Las capas por las que mueve el contenido son:
  - **Frequent Access tier** – Automática.
  - **Infrequent Access tier** – Automática. Si no es accedido en 30 días pasa aquí.

- **Archive Instant Access tier** – Automática. Si no es accedido en 90 días. (Se pueden personalizar)
- **Archive Access tier** – Opcional. Si no es accedido en 90 días. (Se pueden personalizar). Se tarda entre 3 y 5 horas en recuperar.
- **Deep Archive Access tier** - Opcional. Si no es accedido en 180 días. (Se pueden personalizar). Se tarda unas 12 horas en recuperar.

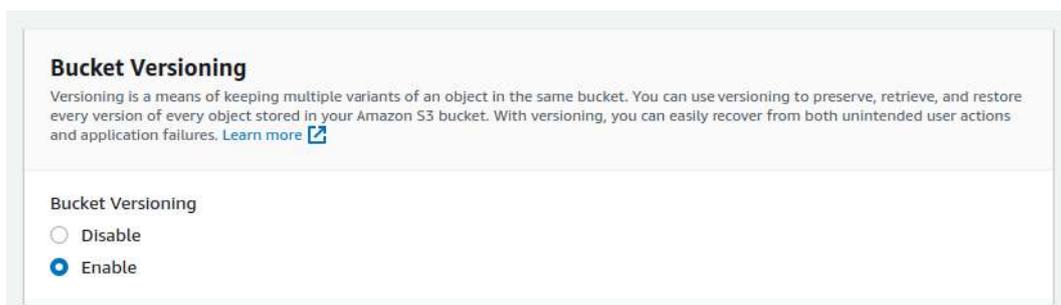
Las configuraciones Intelligent Tiering se configura en las propiedades del bucket



- **Standard-IA** – Esta pensado para datos que no se accede demasiado pero se necesita una acceso rápido.
- **One Zone-IA** – Este no tiene replica, solo se guarda en una AZ y en caso de perderla no hay forma de recuperarla.
- **Glacier Instant Retrieval** – Cuando no se va a usar el objeto. Pero es el más rápido de obtener cuando se requiere.
- **Glacier Flexible Retrieval** – No se utiliza el objeto y tarda minutos o horas en recuperarse.
- **Glacier Deep Archive** – Este es el archivado profundo que es costoso en recuperarse.
- **Reduced redundancy** – Es el más inmediato para acceder, pero no es recomendable, es para información no crítica.

Cada tipo de almacenamiento tiene un precio, al igual que la recuperación u operar con los objetos.

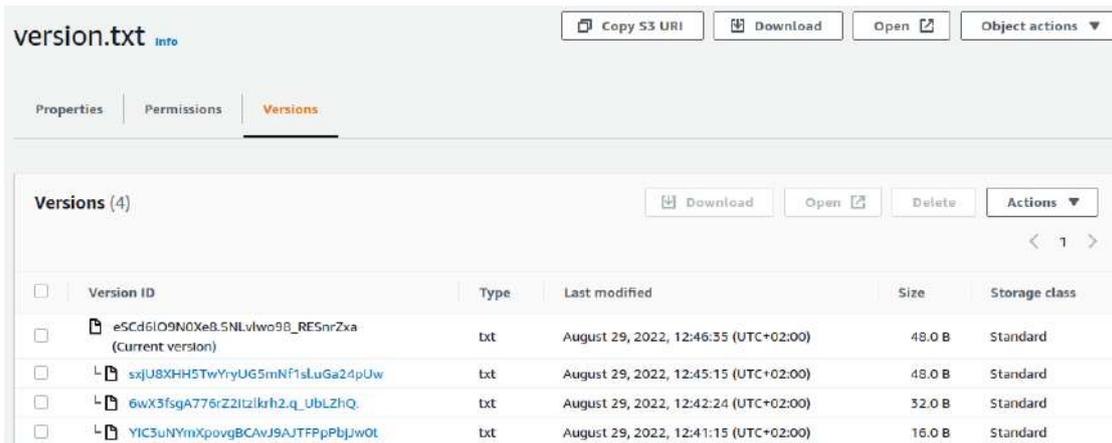
## 14.4. - Versionado



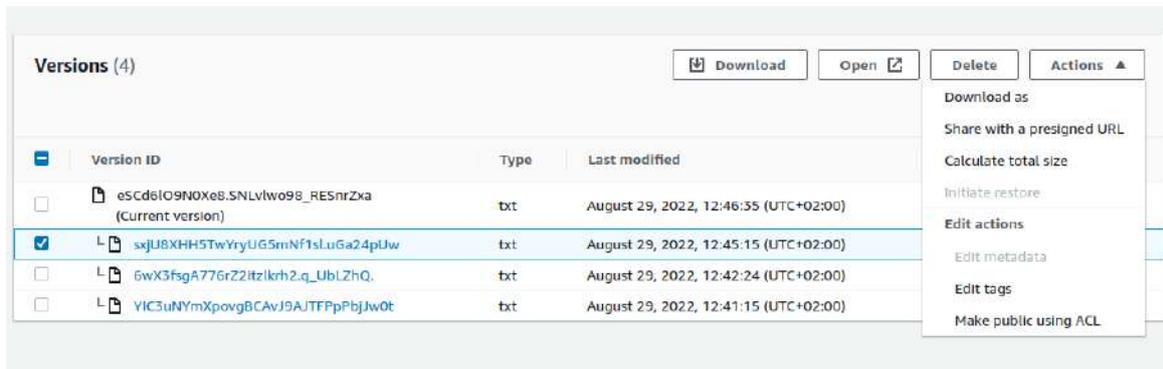
Con el versionado habilitado se pueden recuperar versiones anteriores de los objetos, tanto para guardarla en el mismo lugar como para recuperarla en otra parte como un backup.

Los versionados aparecen en cada uno de los objetos. Se crea la nueva versión cuando:

- Se sube un documento que resulta tener el mismo Key, con el mismo nombre.
- Se cambian los metadatos

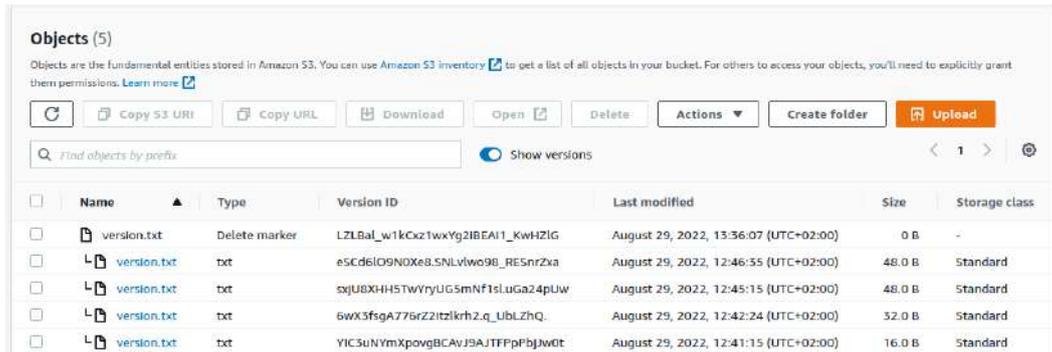


Para recuperar los objetos puede parecer que es en Initiate restore pero esto es para recuperar objetos archivados (Deep glacier)



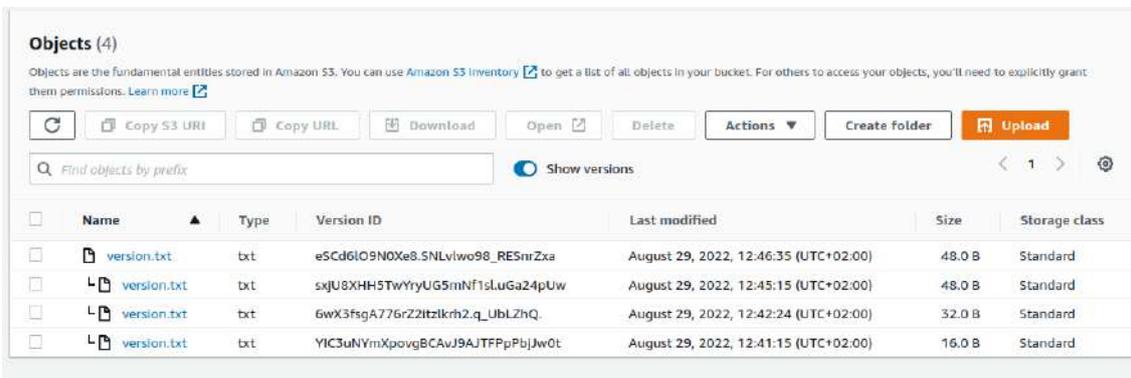
Para recuperar una versión antigua se debe descargar la versión concreta y volverla a subir.

También se puede borrar el objeto y ver en la carpeta concreta las versiones con «Show version»:



Cuando se borra lo que hace es borrar la versión actual y dejar el resto en una especie de marcador. Estos también ocupan espacio de almacenamiento por cada versión.

Cpn lo cual, debemos borrar permanentemente solo el Delete marker. Entonces, la última versión se convierte en la versión actual.



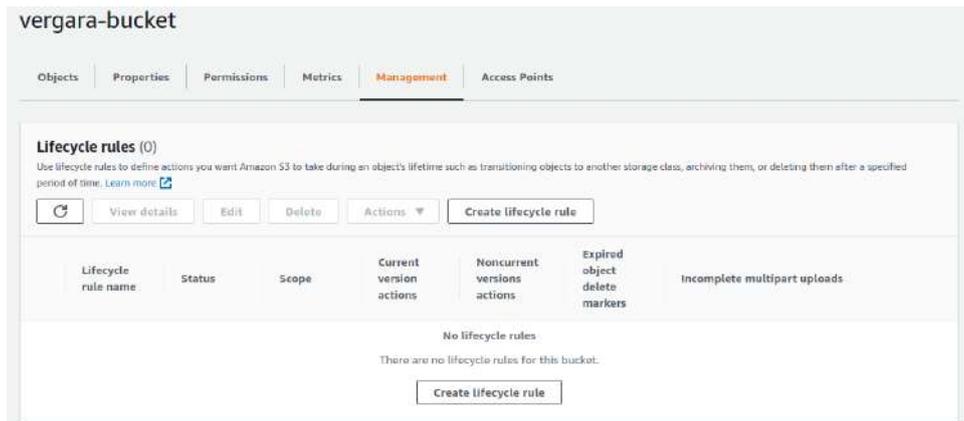
También, si se sube un objeto con el mismo nombre (misma key) se recuperan todas las versiones anteriores.

Seleccionando todo y seleccionando borrado permanente es la manera para que no quede rastro.

## 14.5. - Management – Gestión

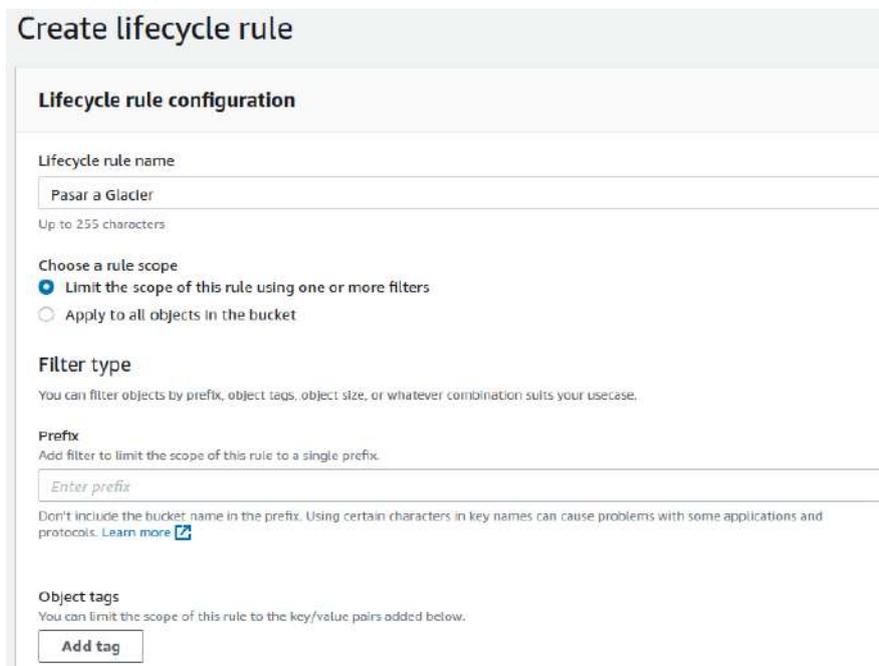
### 14.5.1. - Ciclo de vida

El ciclo de vida son las acciones que se toman dentro del contenido.



Se pueden hacer distintas acciones con el contenido. Se debe crear las reglas del ciclo de vida.

Se pueden limitar a uno o varios elementos o se aplicará a todos los objetos. Se puede filtrar por prefijos o a través de tags.



También se puede mover las versiones actuales entre distintas clases de almacenamientos, las no actuales. Se puede decir que expiren las versiones. Se puede borrar permanente los objetos no actuales. Y se puede eliminar versiones expiradas.

**Lifecycle rule actions**

Choose the actions you want this rule to perform. Per-request fees apply. [Learn more](#) or see [Amazon S3 pricing](#)

- Move current versions of objects between storage classes
- Move noncurrent versions of objects between storage classes
- Expire current versions of objects
- Permanently delete noncurrent versions of objects
- Delete expired object delete markers or incomplete multipart uploads

These actions are not supported when filtering by object tags or object size.

Por ejemplo, en una regla se puede manejar la transición del objeto filtrado.

**Transition current versions of objects between storage classes**

Choose transitions to move current versions of objects between storage classes based on your use case scenario and performance access requirements. These transitions start from when the objects are created and are consecutively applied. [Learn more](#)

Choose storage class transitions

Standard-IA
▼

Days after object creation

Number of days

Remove

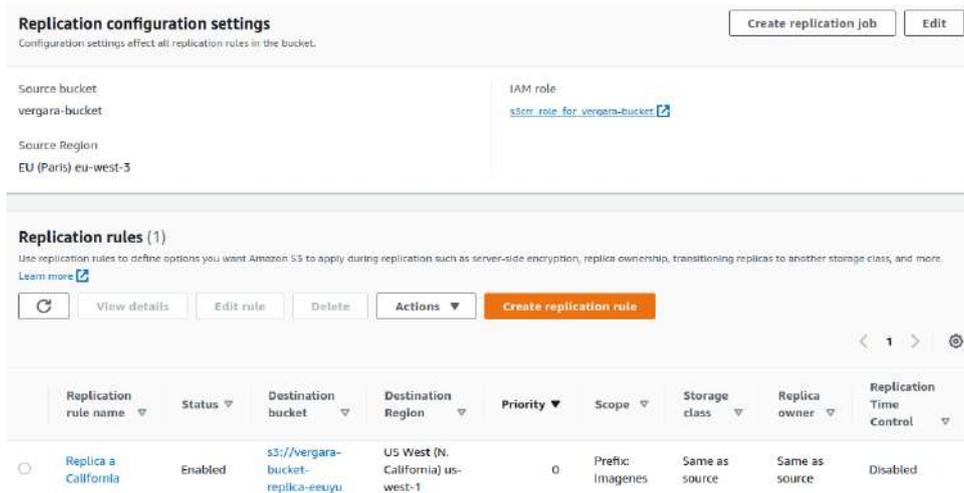
A valid integer value is required.

Add transition

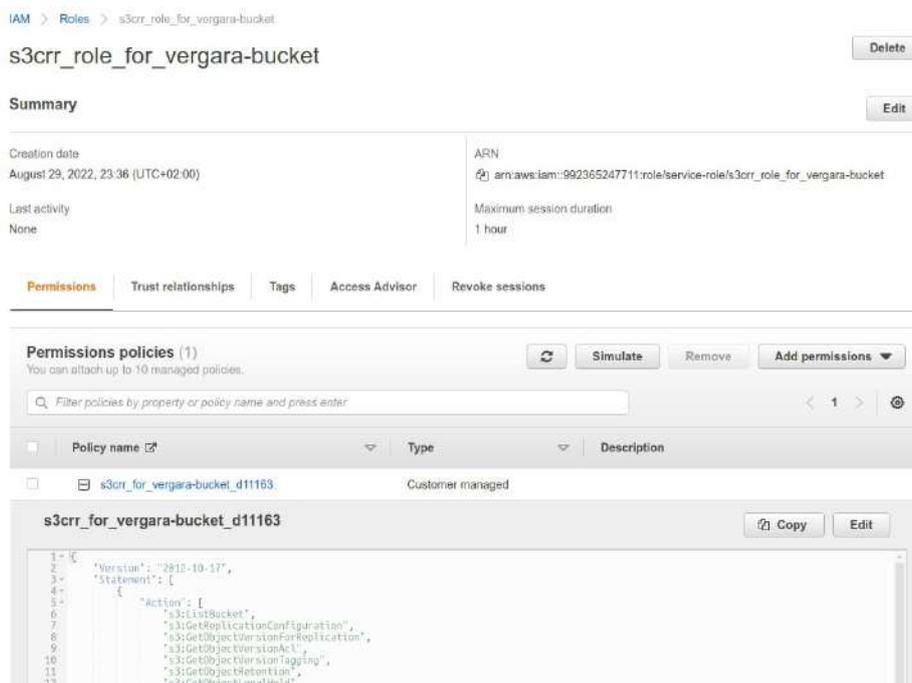
## 14.5.2. - Replicación

Sirve para llevar contenido de un bucket a otro o de una carpeta a otra, aunque tenga otra AZ. Puede servir para llevarlo a un bucket compartido o a una carpeta de backups.

- Se puede tener habilitado o no.
- Se selecciona el Source bucket y se utilizan filtros y tags para seleccionar los objetos a replicar.
- Se seleccionar el destino tanto de la cuenta propia como ajena.
- Se debe activar el versionado, indica para activarlo
- Se puede seleccionar el IAM o también se puede crear uno nuevo
- Se puede encriptar
- Se puede escoger la clase de almacenamiento en el destino.
- Con el RTC se puede obligar a que haga la replicación en menos de 15 minutos.
- Se pueden extraer métricas.
- Se puede eliminar las operaciones del objeto original.
- Se puede eliminar los metadatos añadidos.



Cuando lo creamos aparece un enlace al rol de replicado creado en el que se puede ver las acciones que puede hacer este rol



### 14.6. - Acceso público

En Permissions podemos cambiar varios parámetros:

- El bloqueo de acceso público – Editando aparece las mismas opciones que creando el bucket
  - Dos bloqueos por ACLs y otros dos por políticas

### Edit Block public access (bucket settings) Info

**Block public access (bucket settings)**

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

- Block all public access**  
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.
  - Block public access to buckets and objects granted through *new* access control lists (ACLs)**  
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
  - Block public access to buckets and objects granted through *any* access control lists (ACLs)**  
S3 will ignore all ACLs that grant public access to buckets and objects.
  - Block public access to buckets and objects granted through *new* public bucket or access point policies**  
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
  - Block public and cross-account access to buckets and objects through *any* public bucket or access point policies**  
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

- La política del bucket es del tipo recurso. Se puede utilizar para dar o quitar permisos a usuarios concretos. La parte de políticas de seguridad en AWS se suele manejar con las IAM. Se crea a través de JSON.
  - Ejemplo de permisos:

### Política de Seguridad

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Leers3",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:ListBucketVersions",
        "s3:ListBucket",
        "s3:GetObjectVersion"
      ],
      "Resource": "arn:aws:s3:::mi-bucket/*",
      "Condition": {
        "IpAddress": {
          "aws:SourceIp": "10.0.0.16"
        }
      },
      "Principal": {
        "AWS": "*"
      }
    }
  ]
}
```

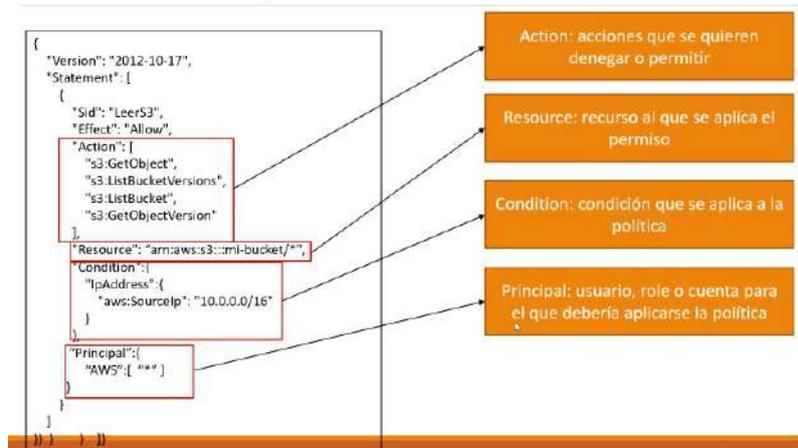
Versión: En estos momentos es 2012-10-17

Statement: Nombre del grupo completo de parámetros

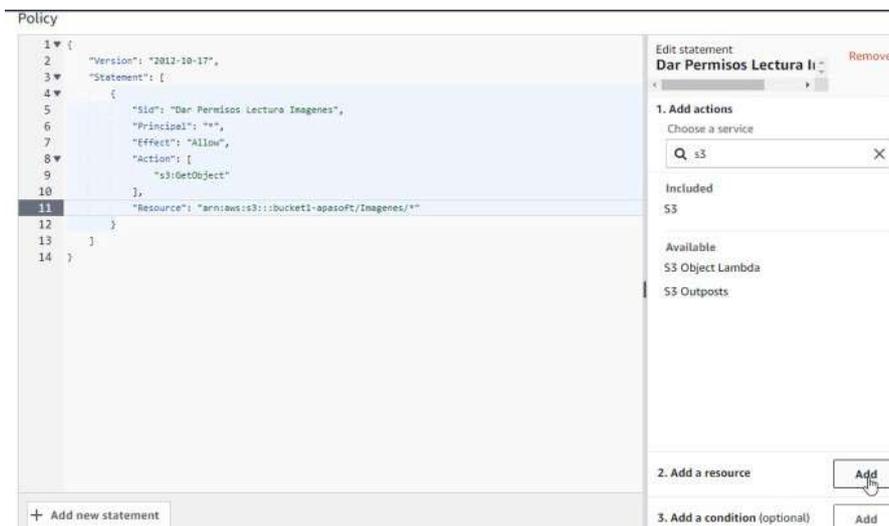
SID: Nombre que se aplica a la política

Effect: Permitir o denegar acceso. Puede ser Allow o Deny

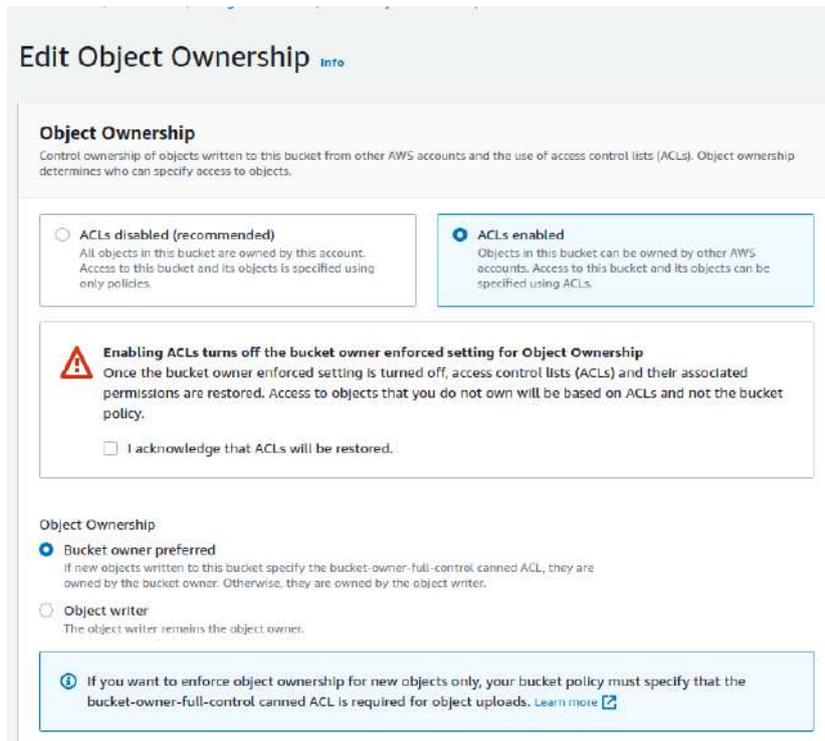
## Política de Seguridad



## Editor de políticas JSON



- La propiedad del bucket – Lo preferible es la recomendada, tenerlo deshabilitado. De esta manera son las Políticas del bucket quienes dan los permisos. Si se habilita son las ACLs quienes manejan permisos.



- Las listas de control de acceso (ACL) – Para que se active el botón de editar debemos tener habilitadas las ACLs en la propiedad.

Grantee	Objects	Bucket ACL
<b>Bucket owner (your AWS account)</b> Canonical ID:  b98f57abafb573f27dd86bcf85d4017a16fc2a0396d5f571919f5872768bec73	<input checked="" type="checkbox"/> List <input checked="" type="checkbox"/> Write	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write
<b>Everyone (public access)</b> Group:  http://acs.amazon-aws.com/groups/global/AllUsers	<input type="checkbox"/> List <input type="checkbox"/> Write	<input type="checkbox"/> Read <input type="checkbox"/> Write
<b>Authenticated users group (anyone with an AWS account)</b> Group:  http://acs.amazon-aws.com/groups/global/AuthenticatedUsers	<input type="checkbox"/> List <input type="checkbox"/> Write	<input type="checkbox"/> Read <input type="checkbox"/> Write
<b>S3 log delivery group</b> Group:  http://acs.amazon-aws.com/groups/s3/LogDelivery	<input type="checkbox"/> List <input type="checkbox"/> Write	<input type="checkbox"/> Read <input type="checkbox"/> Write

Lo interesante de esta opción es que se pueden editar las ACLs por objetos concretos sin afectar al resto. Pero si se hace a nivel de bucket se hará a todos los archivos.

- Cross-origin resource sharing (CORS)

## 14.7. - Bloqueo objetos

El bloqueo de objetos, si no lo hacemos cuando creamos el bucket no lo podremos hacer después. Se tendría que abrir una petición a AWS para que lo hicieran manualmente. Cuando se activa automáticamente también se activa el versionado.

**▼ Advanced settings**

**Object Lock**  
Store objects using a write-once-read-many (WORM) model to help you prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. [Learn more](#)

Disable

**Enable**  
Permanently allows objects in this bucket to be locked. Additional Object Lock configuration is required in bucket details after bucket creation to protect objects in this bucket from being deleted or overwritten.

 Object Lock works only in versioned buckets. Enabling Object Lock automatically enables Bucket Versioning.

 **Enabling Object Lock will permanently allow objects in this bucket to be locked**  
Enable Object Lock only if you need to prevent objects from being deleted to have data integrity and regulatory compliance. After you enable this feature, anyone with the appropriate permissions can put immutable objects in the bucket. You might be blocked from deleting the objects and the bucket. Additional Object Lock configuration is required in bucket details after bucket creation to protect objects in this bucket from being deleted or overwritten. [Learn more](#)

I acknowledge that enabling Object Lock will permanently allow objects in this bucket to be locked.

También avisa que si se crea un bloqueo a cierto objeto puede quedar de manera permanente hasta la fecha de expiración del bloqueo o con el parámetro indicado. Con lo cuál, no se podrá eliminar el bucket y la única forma de eliminarlo es eliminando la cuenta.

Mientras se sube un objeto no se puede bloquear, a no ser que se use AWS CLI, AWS SDK o S3 REST API.

**Object Lock**  
Store objects using a write-once-read-many (WORM) model to help you prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. [Learn more](#)

 **Object Lock settings can't be specified on upload using the S3 console**  
If your bucket policy requires new objects stored in this bucket to have specific Object Lock settings on upload, use the AWS CLI, AWS SDK or Amazon S3 REST API. [Learn more](#)

Una vez subido el objeto, dentro del mismo en propiedades, hay dos opciones de bloqueo:

- **Object Lock legal hold** – No tiene temporalidad, solo se habilita o deshabilita.
- **Object Lock retention** – CUIDAO! Puede bloquear completamente sin que se pueda desbloquear. El bloqueo tiene una fecha de expiración. Hay dos modos:
  - **Governance mode** – Se puede volver atrás y deshabilitar el bloqueo
  - **Compliance mode** – Nadie puede quitar el bloqueo antes de la fecha indicada

Si se intentan borrar, en principio parece que se puede pero quedará versionado. Esta versión no se puede borrar con el bloqueo habilitado.

El bloqueo puede servir legalmente para indicar que un objeto no ha sido modificado.

## 14.8. - S3Browser

Es una herramienta de un tercero para poder navegar por los buckets como si fuera un fichero en nuestro SO. <https://s3browser.com/> Como esta herramienta existen otras, AWS no tiene ninguna herramienta interna para esto, en cambio Azure si que la tiene.

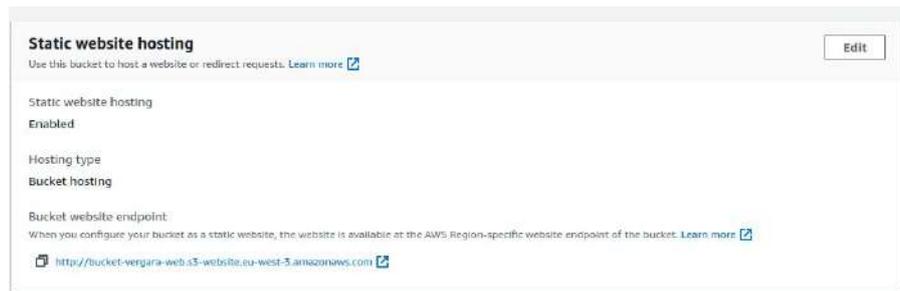
## 14.9. - Web estática en S3

Con las ACLs activadas (O haciendo políticas expresas para hacer accesible la carpeta donde este la web) y haciendo todo público. Vamos al final de las propiedades del bucket y está la opción «Static website hosting».

The screenshot shows the AWS console interface for editing static website hosting on a bucket. The breadcrumb trail is 'Amazon S3 > Buckets > bucket-vergara-web > Edit static website hosting'. The main heading is 'Edit static website hosting' with an 'Info' link. Below this, there's a section 'Static website hosting' with a sub-heading 'Use this bucket to host a website or redirect requests. Learn more'. The 'Static website hosting' section has two radio buttons: 'Disable' (unselected) and 'Enable' (selected). The 'Hosting type' section has two radio buttons: 'Host a static website' (selected) and 'Redirect requests for an object' (unselected). Below the 'Host a static website' option, there's a note: 'Use the bucket endpoint as the web address. Learn more'. Below the 'Redirect requests for an object' option, there's a note: 'Redirect requests to another bucket or domain. Learn more'. A blue information box contains a note: 'For your customers to access content at the website endpoint, you must make all your content publicly readable. To do so, you can edit the S3 Block Public Access settings for the bucket. For more information, see Using Amazon S3 Block Public Access'. Below this, there's an 'Index document' section with a text input field containing 'index.html'. Below that is an 'Error document - optional' section with a text input field containing 'error.html'. At the bottom, there's a 'Redirection rules - optional' section with a text area containing a single rule with a status of '1'.

Lo habilitamos e indicamos el host o la redirección. En el caso del host debemos indicar el documento que será el índice y el de error. Además, podemos añadir una reglas de redireccionamiento.

Luego tenemos que subir los documentos de la web dándole permiso de lectura pública. Si volvemos de nuevo a la propiedades a la parte de Static website hosting, veremos que nos ha generado un enlace.



## 14.10. - Inventario de los objetos

Recopilación de inventario se puede hacer en la pestaña management en el apartado configuración de inventarios.

Cuando creas un inventario puede tardar días en recopilar la información de los objetos y sus metadatos.

Creando una configuración de inventario se parámetro:

- el nombre
- Opción a filtrar por prefijos
- Listar por versión actual o por todas las versiones anteriores
- Destino del resultado. Path de la ubicación.
- Política para permisos en el bucket destino. Permite el servicio S3 en el bucket correspondiente indicando el origen y la cuenta para el control.
- Frecuencia del inventario. Diaria o semanal
- Formato de salida. CSV, Apache ORC o Apache Parquet
- Si la configuración queda activa o desactiva para publicar los inventarios
- Si se quiere encriptar
- Se le puede añadir campos extraer en los metadatos

**Additional metadata fields - optional**  
 Choose the metadata that should be included for each listed object in the report. [Learn more](#)

**Object**

Size

Last modified

Multipart upload

Replication status

Encryption

Bucket key status

**Storage class**

Storage class

Intelligent-Tiering: Access tier

**Data integrity**

ETag

Additional checksums function

**Object Lock**

All Object Lock configurations

- Object Lock: Retention mode
- Object Lock: Retain until date
- Object Lock: Legal hold status

Aparecen varias carpetas. Una con el report diario, otro con los datos y otro con hive (visualizar los datos en BBDD de entorno BigData <https://hive.apache.org/>). Dentro del report diario hay dos archivos: un manifest.json con un resumen de los datos y un checksum.

## 14.11. - Línea de comandos para S3

### 14.11.1. - Subcomando "aws s3"

Documentación: <https://awscli.amazonaws.com/v2/documentation/api/latest/reference/s3/index.html>

Opciones:

**cp** – Copiar. Tanto desde o hacia un bucket como desde o hacia local: <LocalPath> <S3Uri> or <S3Uri> <LocalPath> or <S3Uri> <S3Uri>

```
administrador@ubuntu:~$ aws s3 cp ficheroPruebaCopia.txt s3://bucket-vergara-desde-consola/ficheroCopiadoDesdeLocal.txt
upload: ./ficheroPruebaCopia.txt to s3://bucket-vergara-desde-consola/ficheroCopiadoDesdeLocal.txt
administrador@ubuntu:~$ aws s3 ls s3://bucket-vergara-desde-consola
2022-09-02 11:19:47          79 ficheroCopiadoDesdeLocal.txt
administrador@ubuntu:~$
```

Tiene opciones parecidas a cp de bash. Por ejemplo --recursive Para copiar directorios y su contenido.

Se puede mezclar con un script de Linux. Por ejemplo, para subir todos los ficheros del directorio local:

```
for i in *
do
```

aws s3 cp \$i s3://vergara-bucket/Docs/  
done

**ls** – Listar

```
administrador@ubuntudocker:~$ aws s3 ls
2022-09-01 21:52:42 bucket-vergara-web
2022-09-02 10:10:00 vergara-bucket
2022-08-30 01:01:10 vergara-bucket-bloqueo
```

**mv** - Mover

**rm** – Borrar objetos y buckets. Por ejemplo, usando un for de bash

```
administrador@ubuntudocker:~/pruebas_AWS$ for i in *; do aws s3 rm s3://bucket-vergara-desde-consola/$i; done
delete: s3://bucket-vergara-desde-consola/fichero01.txt
delete: s3://bucket-vergara-desde-consola/fichero02.txt
delete: s3://bucket-vergara-desde-consola/fichero03.txt
delete: s3://bucket-vergara-desde-consola/fichero04.txt
delete: s3://bucket-vergara-desde-consola/fichero05.txt
administrador@ubuntudocker:~/pruebas_AWS$ aws s3 ls s3://bucket-vergara-desde-consola
2022-09-02 11:19:47          79 ficheroCopiadoDesdeLocal.txt
```

**mb** – Crear un bucket. Sintaxis: `aws s3 mb s3://mybucket`

```
administrador@ubuntudocker:~$ aws s3 mb s3://bucket-vergara-desde-consola
make_bucket: bucket-vergara-desde-consola
administrador@ubuntudocker:~$ aws s3 ls
2022-09-02 11:12:44 bucket-vergara-desde-consola
2022-09-01 21:52:42 bucket-vergara-web
2022-09-02 10:10:00 vergara-bucket
2022-08-30 01:01:10 vergara-bucket-bloqueo
```

**presign** - Genera una URL pre-firmada para un objeto de Amazon S3. Esto permite que cualquiera que reciba la URL pre-firmada pueda recuperar el objeto de S3 con una solicitud HTTP GET. Todas las URL pre-firmadas utilizan ahora sigv4, por lo que la región debe configurarse explícitamente.

**rb** – Borrar un bucket

**sync** - Sincroniza directorios y prefijos de S3. Copia recursivamente los archivos nuevos y actualizados del directorio de origen al de destino. Solo crea carpetas en el destino si contienen uno o más archivos.

**website** - Establece la configuración del sitio web para un bucket.

### 14.11.2. - Subcomando "aws s3api"

Es más parecido a lo visto hasta ahora como CLI. Documentación:

<https://awscli.amazonaws.com/v2/documentation/api/latest/reference/s3api/index.html>

Por ejemplo, para listar los buckets:

```
aws s3api list-buckets
```

```

administrador@ubuntudocker:~/pruebas_AWS$ aws s3api list-buckets
{
  "Buckets": [
    {
      "Name": "bucket-vergara-desde-consola",
      "CreationDate": "2022-09-02T09:12:44+00:00"
    },
    {
      "Name": "bucket-vergara-web",
      "CreationDate": "2022-09-01T19:52:42+00:00"
    },
    {
      "Name": "vergara-bucket",
      "CreationDate": "2022-09-02T08:10:00+00:00"
    },
    {
      "Name": "vergara-bucket-bloqueo",
      "CreationDate": "2022-08-29T23:01:10+00:00"
    }
  ],
  "Owner": {
    "ID": "6cab60d8f06fff0c72a17b71a77e771cf3b471a2ed88add6b778ffb2a609515f"
  }
}

```

Para crear un bucket:

```
aws s3api create-bucket --bucket nombre-del-nuevo-bucket --region eu-west-3 --create-bucket-configuration LocationConstraint=eu-west-3
```

**CUIDADO:** Si no ponemos la region lo creará en us-east-1. Y si no ponemos la configuración del bucket no permite crearlo.

```

administrador@ubuntudocker:~/pruebas_AWS$ aws s3api create-bucket --bucket bucket-vergara-desde-consola2 --region eu-west-3
An error occurred (IllegalLocationConstraintException) when calling the CreateBucket operation: The unspecified location constraint is incompatible for the region specific endpoint this request was sent to.
administrador@ubuntudocker:~/pruebas_AWS$ aws s3api create-bucket --bucket bucket-vergara-desde-consola2 --region eu-west-3 --create-bucket-configuration LocationConstraint=eu-west-3
{
  "Location": "http://bucket-vergara-desde-consola2.s3.amazonaws.com/"
}
administrador@ubuntudocker:~/pruebas_AWS$ █

```

Para subir un objeto:

```
aws s3api put-object --bucket nombre-bucket --key nombre-fichero-en-destino --body nombre-fichero-actual
```

Para listar objetos:

```
aws s3api list-objects --bucket nombre-bucket
```

```

administrador@ubuntudocker:~/pruebas_AWS$ aws s3api put-object --bucket bucket-vergara-desde-consola2 --key ficheroPutObject.txt --body fichero03.txt
{
  "ETag": "\"d41d8cd98f00b204e9800998ecf8427e\""
}
administrador@ubuntudocker:~/pruebas_AWS$ aws s3api list-objects --bucket bucket-vergara-desde-consola2
{
  "Contents": [
    {
      "Key": "ficheroPutObject.txt",
      "LastModified": "2022-09-02T10:28:54+00:00",
      "ETag": "\"d41d8cd98f00b204e9800998ecf8427e\"",
      "Size": 0,
      "StorageClass": "STANDARD",
      "Owner": {
        "ID": "6cab60d8f06fff0c72a17b71a77e771cf3b471a2ed88add6b778ffb2a609515f"
      }
    }
  ]
}

```

Opciones del subcomando s3api:

abort-multipart-upload

complete-multipart-upload

copy-object  
create-bucket  
create-multipart-upload  
delete-bucket  
delete-bucket-analytics-configuration  
delete-bucket-cors  
delete-bucket-encryption  
delete-bucket-intelligent-tiering-configuration  
delete-bucket-inventory-configuration  
delete-bucket-lifecycle  
delete-bucket-metrics-configuration  
delete-bucket-ownership-controls  
delete-bucket-policy  
delete-bucket-replication  
delete-bucket-tagging  
delete-bucket-website  
delete-object  
delete-object-tagging  
delete-objects  
delete-public-access-block  
get-bucket-accelerate-configuration  
get-bucket-acl  
get-bucket-analytics-configuration  
get-bucket-cors  
get-bucket-encryption  
get-bucket-intelligent-tiering-configuration  
get-bucket-inventory-configuration  
get-bucket-lifecycle-configuration  
get-bucket-location  
get-bucket-logging  
get-bucket-metrics-configuration  
get-bucket-notification-configuration  
get-bucket-ownership-controls  
get-bucket-policy  
get-bucket-policy-status  
get-bucket-replication  
get-bucket-request-payment  
get-bucket-tagging  
get-bucket-versioning  
get-bucket-website  
get-object  
get-object-acl

get-object-attributes  
get-object-legal-hold  
get-object-lock-configuration  
get-object-retention  
get-object-tagging  
get-object-torrent  
get-public-access-block  
head-bucket  
head-object  
list-bucket-analytics-configurations  
list-bucket-intelligent-tiering-configurations  
list-bucket-inventory-configurations  
list-bucket-metrics-configurations  
list-buckets  
list-multipart-uploads  
list-object-versions  
list-objects  
list-objects-v2  
list-parts  
put-bucket-accelerate-configuration  
put-bucket-acl  
put-bucket-analytics-configuration  
put-bucket-cors  
put-bucket-encryption  
put-bucket-intelligent-tiering-configuration  
put-bucket-inventory-configuration  
put-bucket-lifecycle-configuration  
put-bucket-logging  
put-bucket-metrics-configuration  
put-bucket-notification-configuration  
put-bucket-ownership-controls  
put-bucket-policy  
put-bucket-replication  
put-bucket-request-payment  
put-bucket-tagging  
put-bucket-versioning  
put-bucket-website  
put-object  
put-object-acl  
put-object-legal-hold  
put-object-lock-configuration  
put-object-retention

put-object-tagging  
put-public-access-block  
restore-object  
select-object-content  
upload-part  
upload-part-copy  
wait  
write-get-object-response

### 14.11.3. - Subcomando "aws s3control"

Para el plano de control.

Documentación: <https://awscli.amazonaws.com/v2/documentation/api/latest/reference/s3control/index.html>

Opciones:

create-access-point  
create-access-point-for-object-lambda  
create-bucket  
create-job  
create-multi-region-access-point  
delete-access-point  
delete-access-point-for-object-lambda  
delete-access-point-policy  
delete-access-point-policy-for-object-lambda  
delete-bucket  
delete-bucket-lifecycle-configuration  
delete-bucket-policy  
delete-bucket-tagging  
delete-job-tagging  
delete-multi-region-access-point  
delete-public-access-block  
delete-storage-lens-configuration  
delete-storage-lens-configuration-tagging  
describe-job  
describe-multi-region-access-point-operation  
get-access-point  
get-access-point-configuration-for-object-lambda  
get-access-point-for-object-lambda  
get-access-point-policy  
get-access-point-policy-for-object-lambda

get-access-point-policy-status  
get-access-point-policy-status-for-object-lambda  
get-bucket  
get-bucket-lifecycle-configuration  
get-bucket-policy  
get-bucket-tagging  
get-job-tagging  
get-multi-region-access-point  
get-multi-region-access-point-policy  
get-multi-region-access-point-policy-status  
get-public-access-block  
get-storage-lens-configuration  
get-storage-lens-configuration-tagging  
list-access-points  
list-access-points-for-object-lambda  
list-jobs  
list-multi-region-access-points  
list-regional-buckets  
list-storage-lens-configurations  
put-access-point-configuration-for-object-lambda  
put-access-point-policy  
put-access-point-policy-for-object-lambda  
put-bucket-lifecycle-configuration  
put-bucket-policy  
put-bucket-tagging  
put-job-tagging  
put-multi-region-access-point-policy  
put-public-access-block  
put-storage-lens-configuration  
put-storage-lens-configuration-tagging  
update-job-priority  
update-job-status

#### **14.11.4. - Subcomando "s3outposts"**

Para las operaciones de S3 on Outposts.

Documentación: <https://awscli.amazonaws.com/v2/documentation/api/latest/reference/s3outposts/index.html>

Opciones:

create-endpoint  
delete-endpoint

list-endpoints

list-shared-endpoints

## TEMA 15 - RDS Bases de Datos Relacionales

Hay distintos tipos de BBDD en AWS.

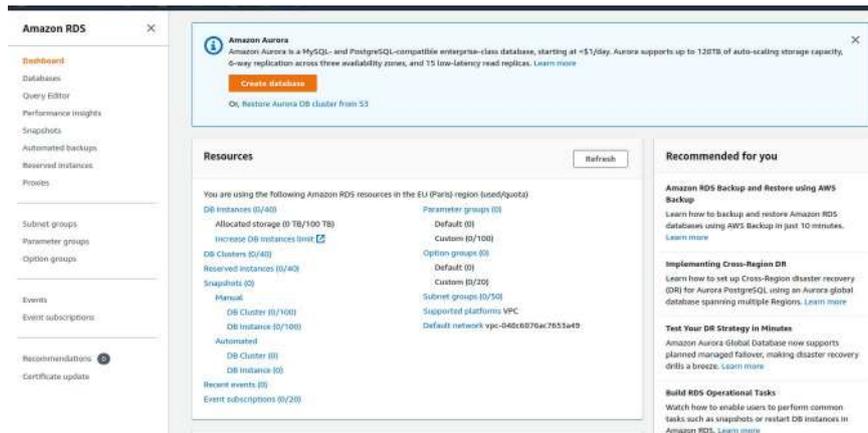


A rasgos generales:

- BBDD **relacionales** de terceros.
  - RDS – Oracle, SQL server, Mariadb, postgresSQL, mySQL..
    - Aurora es una BBDD enfocada para cloud. También forma parte de RDS pero es diferente al resto. Soporta serverless.
- **NoSQL** -
  - Key-Value
    - DynamoDB
  - In-Memory
    - Elastic Cache (Memcached y redis). Es un frontal para tener por detrás una BBDD tradicional.
    - MemoryDB for Redis. BBDD completa, con todas las características necesarias.
  - Document
    - DocumentDB compatibles con MongoDB
  - Graph
    - Neptune se parece a otras como NeoForJava
  - Columnar
    - Keyspaces como Apache Cassandra
  - Time series. Permite recorrer datos de tipo temporal masivos.
    - Timestream

- Ledger – Contable. Certifica de manera inequívoca los asientos que se hacen. Incluso, tienen validez judicial.
  - QLDB
- **Data warehouse**
  - Redshift – BBDD más popular

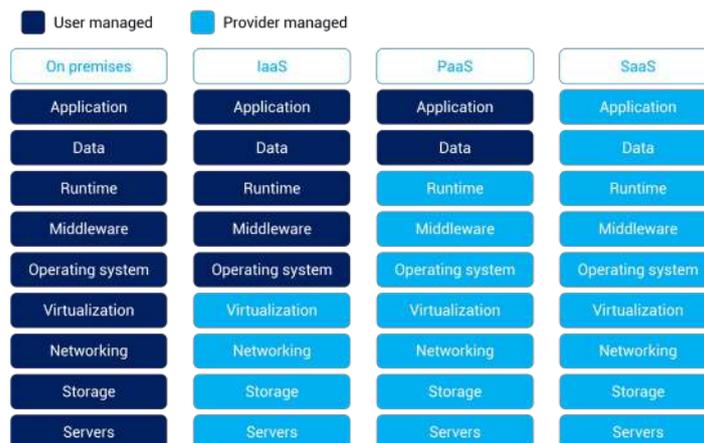
RDS



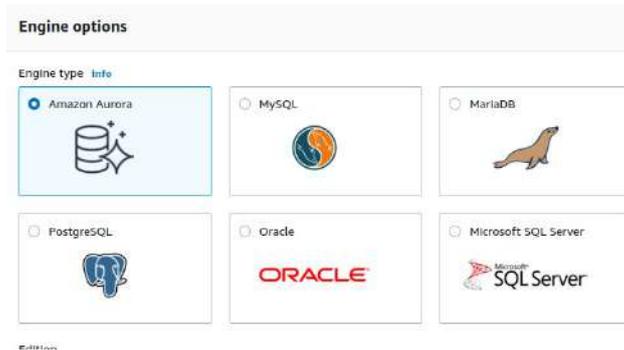
RDS es un PaSS (Plataforma como servicio). AWS se encargará de la gestión de la máquina y el cliente puede usar el software. Tampoco se puede configurar la BBDD o administrar su instalación, las actualizaciones...

Para controlarlo todo se debe crear una instancia y montar dentro la BBDD.

Recordatorio:



Si le damos a crear BBDD podemos ver las BBDD relacionales que podemos utilizar.



Aurora son BBDD parecidas a SQL pero no son lo mismo, es otra implementación.

## 15.1. - Crear BBDD en RDS Standard

- Tenemos dos **tipos de creación**:
  - **Standard** – Te pide algunas variables para su configuración.
  - **Easy** – Ofrece algunas configuraciones predefinidas por defecto
- **Tipo de BBDD**. Aurora, mysql, mariadb, etc
  - Podemos escoger la versión
- **Plantillas** – Según que escogemos nos dará unas opciones u otras.
  - Producción
  - Desarrollo
  - Free tier – Pruebas en una capa gratuita.
- **Opciones**
  - Nombre de la BBDD
  - Credenciales. Usuario admin y password
- **Configuración de la instancia**. Según el tipo de plantilla podremos seleccionar unas máquinas u otras, según la optimización que se requiera. Cada BBDD necesita unos recursos y según como sea conviene escoger una instancia u otra (ver documentación: <https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.DBInstanceClass.html>). El precio que cuesta la BBDD está basado en la instancia que se elija. Las instancias empiezan por db. porque están diseñadas orientadas a las BBDD.

<b>db.t2.micro</b>	1 vCPUs	1 GiB RAM	Not EBS Optimized
<b>db.t2.small</b>	1 vCPUs	2 GiB RAM	Not EBS Optimized
<b>db.t2.medium</b>	2 vCPUs	4 GiB RAM	Not EBS Optimized
<b>db.t2.large</b>	2 vCPUs	8 GiB RAM	Not EBS Optimized
<b>db.t2.xlarge</b>	4 vCPUs	16 GiB RAM	Not EBS Optimized
<b>db.t2.2xlarge</b>	8 vCPUs	32 GiB RAM	Not EBS Optimized
<b>db.t3.micro</b>	2 vCPUs	1 GiB RAM	Network: 2.085 Mbps
<b>db.t3.small</b>	2 vCPUs	2 GiB RAM	Network: 2.085 Mbps
<b>db.t3.medium</b>	2 vCPUs	4 GiB RAM	Network: 2.085 Mbps

- **Almacenamiento.** No tenemos todos los tipos de disco, con las instancias varían. Normalmente se activa la autoescalada para que puede crecer hasta cierto tamaño. Indica un mínimo de espacio.
- **Disponibilidad y durabilidad.** Para despliegue en distintas AZ. Lo que hace es crear Instancias Standby, de réplica. No es posible usarlo con la plantilla Free tier.
- **Conexión.** Aquí decidimos
  - si queremos conectarla con una instancia EC2 (Tiene que estar arrancada)
  - La VPC
  - El grupo de subred
  - Si queremos acceso público.
  - El grupo de seguridad. Lo seguro es un grupo que solo permita el puerto de la BBDD
  - AZ
  - También podemos cambiar el puerto de conexión en la configuración adicional.
- **Tipo de autenticación.**
- **Monitorización.** Habilitar o no la monitorización.
- **Configuración adicional.**
  - Una BBDD inicial, nos pide el nombre-bucket
  - El grupo de parámetros es para especificar el comportamiento de la BBDD
  - En el grupo de opciones se especifican opciones.
  - El backup. Por defecto está habilitado. Debe estar habilitado si no es una prueba. Se guarda como un snapshot.

- Nos pregunta si queremos encriptación
  - AWS KMS key
  - Performance Insights – permite detectar posibles problemas de rendimiento o de datos. Es gratuita la versión de 7 días. La de 2 años es de pago.
  - Exportación de Logs. (Cuidado, ocupan mucho espacio normalmente). Esto se exporta a CloudWatch
  - IAM role
  - Mantenimiento – Habilitar actualizaciones automáticas en pequeños cambios. Se pueden programar
  - Se puede habilitar la protección de borrado.
- **Estimación costes mensuales.**

En caso de Oracle u otras BBDD con licencia, AWS no se responsabiliza y tenemos que adquirirla. Es normal que tarde unos minutos en crearse.



## 15.2. - Crear BBDD en RDS Easy

Tan solo escoges el tipo de BBDD, el tipo de instancia (Desarrollo, producción o Free tier), el nombre de la bbdd y el usuario/pass. Luego un resumen y se crea la BBDD. easy

## 15.3. - Gestionar, modificar y borrar BBDD en RDS

La vista de una BBDD es parecida a una instancia

**maridb-proof-1** [Modify] [Actions]

**Summary**

DB identifier maridb-proof-1	CPU 1.63%	Status Available	Class db.t5.micro
Role Instance	Current activity 0 Connections	Engine MariaDB	Region & AZ eu-west-3a

Connectivity & security | Monitoring | Logs & events | Configuration | Maintenance & backups | Tags

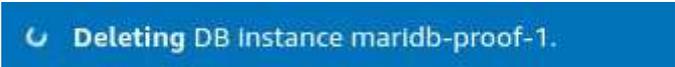
**Connectivity & security**

<b>Endpoint &amp; port</b> Endpoint maridb-proof-1.c129nxqgvsjlj.eu-west-3.rds.amazonaws.com Port 3306	<b>Networking</b> Availability Zone eu-west-3a VPC mi-vpc-prueba (vpc-06efefd12f7a7220f) Subnet group default-vpc-06efefd12f7a7220f Subnets subnet-07ae07fa8707974bb subnet-048e5fac71f2dd18 subnet-05a5290b719979d78 Network type IPv4	<b>Security</b> VPC security groups default (sg-08b19fde593e9c0b3) [Active] Publicly accessible Yes Certificate authority rds-ca-2019 Certificate authority date August 22, 2024, 19:08 (UTC+02:00)
--	---	---

- Connectivity & security
- Monitoring
- Logs & events - cabe la posibilidad de hacer un watch a un log en el mismo panel.
- Configuration
- Maintenance & backups – Aquí se pueden ver los snapshots que se van creando.
- Tags

Las modificaciones pueden tardar en aplicarse. En principio, cualquier modificación permite dejarlo para el momento del mantenimiento o realizarla inmediatamente.

Hay que tener en cuenta que el borrado también tardará.



Deleting DB Instance maridb-proof-1.

Existen opciones diferentes para borrar según el tipo de BBDD.

- Se puede crear un snapshot final para posibles errores.
- Se pueden guardar los snapshot creados automáticamente, de los últimos 7 días.

Si no se guarda ningún snapshot deberemos confirmar nuestro consentimiento.

## 15.4. - Opciones subnet group, parameter groups y option groups

**Subnet group** son un conjunto de subnet que se pueden asociar en grupo a una BBDD. Es obligatorio tener un grupo de subnet en cada BBDD. Si no la creamos lo hace automáticamente y le llama default. Puede ser que no sea lo mejor, porque puede conectarse por una subnet que no sea deseada. Es importante crearla personalizada según las necesidades que tengamos.

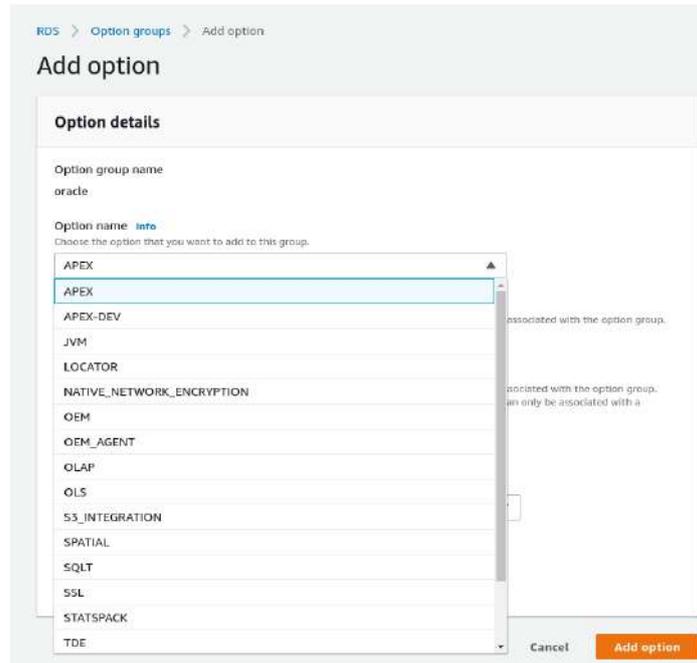
Tendremos que relacionar las subredes que tengamos publicas para poder conectarnos.

**Parameter groups** permiten crear una configuración para las BBDD. Como es un PaaS no se tiene acceso a los archivos de configuración del tipo de BBDD que escojamos. Entonces, esta opción permite cambiar algunos parámetros de la BBDD para poder cambiar esos archivos.

Se crean para tipo de BBDD concretas, para versiones concretas, y después de crearlo se puede entrar y modificar la mayoría de parámetros. Algunos parámetros no están permitido cambiar porque AWS considera que puede afectar al sistema.

**Option groups** es muy parecido al parameter groups pero está más orientado a las opciones. Creando un grupo deberemos escoger el motor, por ejemplo «oracle-ee».

Una vez creado podremos entrar dentro y comprobar las opciones (Conjunto de componentes) que nos permite añadir en el motor para cuando se arranque la BBDD.



Cuando cambiamos opciones de un grupo que se está usando desde una BBDD, nos da la opción de aplicar inmediatamente o esperar a la hora de mantenimiento.

## 15.5. - Propiedades y parámetros concretos según la BBDD

Según el tipo de BBDD tendremos unas propiedades distintas. Para verlas todas las posibilidades, tendremos que escoger la plantilla de producción.

### 15.5.1. - MariaDB

Licencia GPL. Gratuita.

- El tipo de almacenamiento permite
  - gp2 – Es la económica.
  - io1 - IOPS provisionadas puede subir bastante los costes. Estas BBDD tienen un rendimiento muy optimizado.
  - Magnetic – Esta pensado para entornos legacy o BBDD poco utilizadas.
- Se puede tener autoescalada
- Permite standby (Modo replica)
- En los grupos de parámetros y opciones, se tendría que tener previamente uno creado específico para Mariadb para que nos de la opción de escogerlo.

### 15.5.2. - MySQL

Licencia GPL. Gratuita. Desde que Oracle compró Sun Microsystem y adquirió mysql, entre la versión 5 y la 8 han habido muchos cambios, sobretodo de conectividad.

- En disponibilidad y durabilidad, además del multi-AZ y el mono-AZ, también se soporta el multi-AZ cluster. Se activo a partir de la versión 8.0.26. Es como crear una primaria con dos réplicas. Está en modo beta (preview). Aparece en el tutorial pero no en la creación actual de la BBDD.
- En la autenticación se puede autenticar también por kerberos.

El resto de propiedades son iguales que mariadb.

### 15.5.3. - PostgreSQL

Licencia GPL. Gratuita. Es exactamente igual que MySQL.

### 15.5.4. - Oracle

Es una versión comercial.

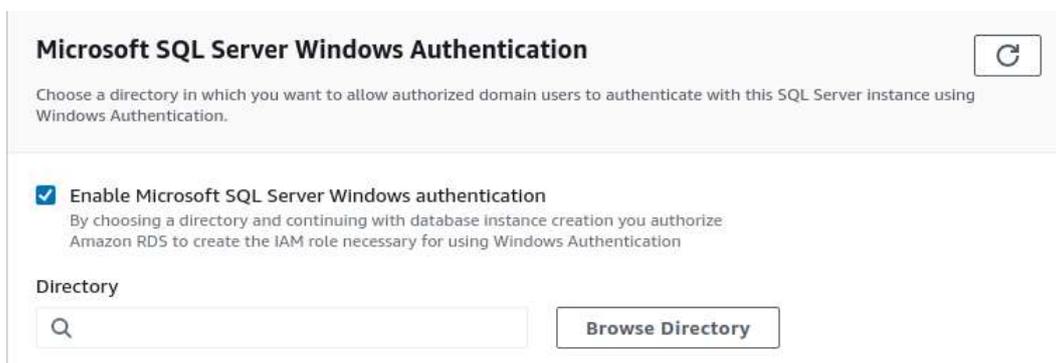
- En el vídeo-tutorial dice que existe dos posibilidades de gestión:
  - Amazon RDS normal – Será AWS quien gestione la BBDD. Un PaaS en toda regla.
  - Amazon RDS custom – Permite una personalización de BBDD, con cierto acceso.
- Se puede utilizar una arquitectura multitenant. Contiene una BBDD primaria (Contenedora. CDB) con otras secundarias (PDB)
- Permite dos clases de versiones (AWS no gestiona licencias, se debe comprar a parte):
  - Oracle Enterprise Edition. Hay que tener licencia
  - Oracle Standard Edition Two. Permite que AWS te ofrezca la licencia y te la cobra.
- No hay plantilla Free tier. Directamente es en producción o en desarrollo.
- En las instancias, lo mínimo que permite Oracle son máquinas de 2 GB de Ram. En Memory optimized y Standard Classes permite incluir los core e hilos. Además, se puede incluir memoria adicional.

### 15.5.5. - Microsoft SQL Server

Es una versión comercial.

- En el vídeo-tutorial dice que existe dos posibilidades de gestión:
  - Amazon RDS normal – Será AWS quien gestione la BBDD. Un PaaS en toda regla.
  - Amazon RDS custom – Permite una personalización de BBDD, con cierto acceso.
- Permite escoger entre 4 ediciones

- SQL Server Express Edition. Version gratuita hasta 10 GB. Solo se puede utilizar en la plantilla Free Tier. Exige 2 cpu y 2 GB de ram como mínimo, solo puedes escoger instancias pequeñas de t3.
  - SQL Server Web Edition. Es una versión limitada para web. Solo se puede utilizar en la plantilla de producción . Exige 2 cpu y 2 GB de ram como mínimo
  - SQL Server Standard Edition. Se puede escoger entre producción y desarrollo. Exige 2 cpu y 8 GB de ram como mínimo
  - SQL Server Enterprise Edition. Es la versión completa. Se puede escoger entre producción y desarrollo. Exige 4 cpu y 16 GB de ram como mínimo
- Tiene una sección especial de Microsoft SQL donde se puede incluir la autenticación de un Directorio Activo



**Microsoft SQL Server Windows Authentication** ⌂

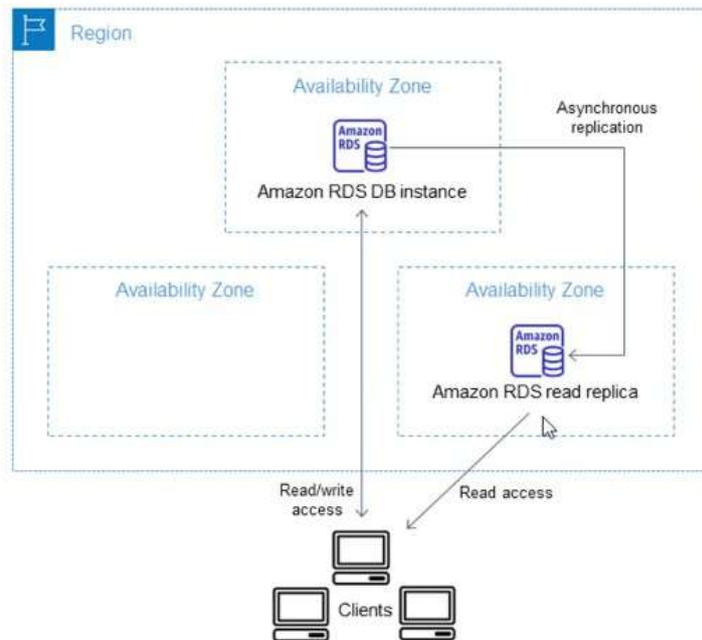
Choose a directory in which you want to allow authorized domain users to authenticate with this SQL Server instance using Windows Authentication.

**Enable Microsoft SQL Server Windows authentication**  
By choosing a directory and continuing with database instance creation you authorize Amazon RDS to create the IAM role necessary for using Windows Authentication

Directory

## 15.6. - Read replica

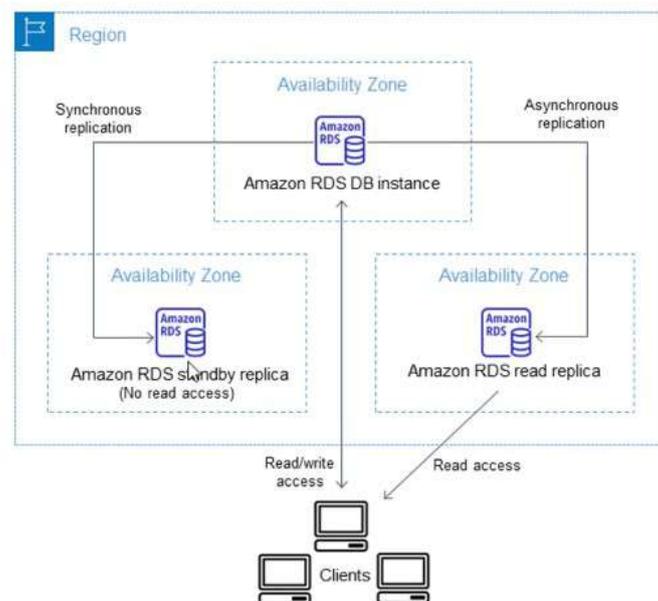
Se puede crear una Read Replica para que en una region, los clientes puedan acceder a la BBDD. Se replican de manera asincrona, con lo cual, se puede crear un acceso de escritura directo a la BBDD y otro acceso de solo lectura a la Read Replica.



De pendiendo del motor de BBDD se puede crear más de una Read Replica.

Utiliza la tecnología de las propias BBDD (mysql, oracle, etc) para crear estas replicas.

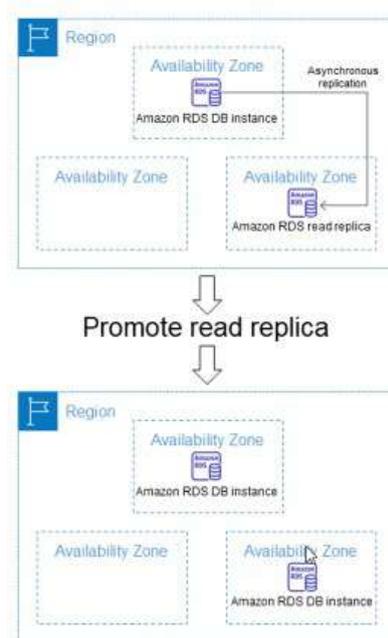
Si tenemos una Multi-AZ, también se puede crear una Read Replica.



La replicación en standby (multi-AZ) es sincrónica. Está más pensada para backup. Aunque la Read Replica también se puede usar para backup.

Se tiene que tener en cuenta que puede existir un desajuste de los datos con la Read Replica por ser asincrónica la replicación.

Podemos promover una replica de solo lectura a una instancia normal y corriente, para utilizarla como una BBDD normal. Para promover se debe parar la BBDD original.



Para mantener la arquitectura se debe crear otra Read Replica.

### 15.6.1. - Crear Replica de Lectura

Para la creación de una Replica de lectura es muy parecida en todas los tipos de BBDD menos en oracle y SQL Server, las Enterprise. El concepto es el mismo pero porque tiene componentes distintos.

Hay un límite de 5 replicas por BBDD. Tiene un coste por los recursos que utiliza. No podemos crear una replica de una BBDD si no tenemos activados los backups.

En «Actions» seleccionamos «Create read replica» y nos lleva a la configuración con los mismos parámetros que una BBDD original:

- Decimos la clase de instancia.
- Si queremos la replica en multi-AZ o no
- El tipo de instancia
- La region AWS – Podemos escoger una region distinta para la replica.
- Tipo de almacenamiento
- Availability & durability
- Conectividad
- Autenticación
- Configuración adicional

- Backups
- Encriptación
- Monitorización
- Logs
- Mantenimiento

Hereda muchos campos de la BBDD original. Realmente, la única diferencia es que no se puede escribir, es de solo lectura.

DB identifier	Role	Engine	Region & AZ	Size	Status	CPU
mariadb1	Primary	MariaDB	us-west-2a	db.t3.micro	Available	2.93%
masriadb1-replica	Replica	MariaDB	us-west-2a	db.t3.micro	Available	1.57%

### 15.6.2. - Promover Replica de Lectura

Marcando la replica, en «Actions» seleccionamos «Promote» y nos da la opción de Habilitar Backup y su periodo. Entonces pasará a ser una BBDD primaria.

DB identifier	Role	Engine	Region & AZ	Size	Status	CPU	Current activity
mariadb1	Instance	MariaDB	us-west-2a	db.t3.micro	Available	3.04%	3 Connections
masriadb1-replica	Instance	MariaDB	us-west-2a	db.t3.micro	Available	3.66%	0 Connections

Esto significa que dejará de replicarse con la primera, y la primera estará igual.

## 15.7. - RDS Reservadas

Es igual que las instancias reservadas. Consiste en alquilar una RDS para un largo periodo y así ahorrar costes respecto al on-demand. De la misma manera se puede pagar el total, parcial, etc.

Igual que pasa con las instancias, cuando se reserva aunque no se use te siguen cobrando.

## 15.8. - CLI RDS

Crear una base de datos RDS de tipo Mysql

```
aws rds create-db-instance --db-instance-identifier db-20 --db-instance-class db.t3.micro --engine mysql --master-username admin1 --master-user-password lepanto1 --allocated-storage 20
```

Comprobar que se ha creado, tanto en la consola como en modo comando

```
aws rds describe-db-instances --query DBInstances[.].DBInstanceIdentifier
```

Crear un snapshot de la Base de datos

```
aws rds create-db-snapshot --db-instance-identifier db-20 --db-snapshot-identifier snp-20
```

Comprobar en la consola y en línea de comandos que se ha creado

```
aws rds describe-db-snapshots
```

Visualizar solo el nombre del snapshot

```
aws rds describe-db-snapshots --query
```

También se puede poner sin nombre

```
aws rds describe-db-snapshots --query "DBSnapshots[*].DBSnapshotIdentifier"
```

Borrar el snapshot

```
aws rds delete-db-snapshot --db-snapshot-identifier snp-11
```

Borrar la Base de datos

```
aws rds delete-db-instance --db-instance-identifier db-02 --skip-final-snapshot
```

También se puede pedir el nombre de la snapshot, si sabemos concretarla, meterla en una variable bash y utilizarla para borrar:

```
snapshot=$(aws rds describe-db-snapshots --snapshot-type manual --query  
DBSnapshots[*].DBSnapshotIdentifier --output text)
```

```
aws rds delete-db-snapshot --db-snapshot-identifier $snapshot
```

Borrar la BBDD

```
aws rds delete-db-instance --db-instance-identifier db-02 --skip-final-snapshot
```

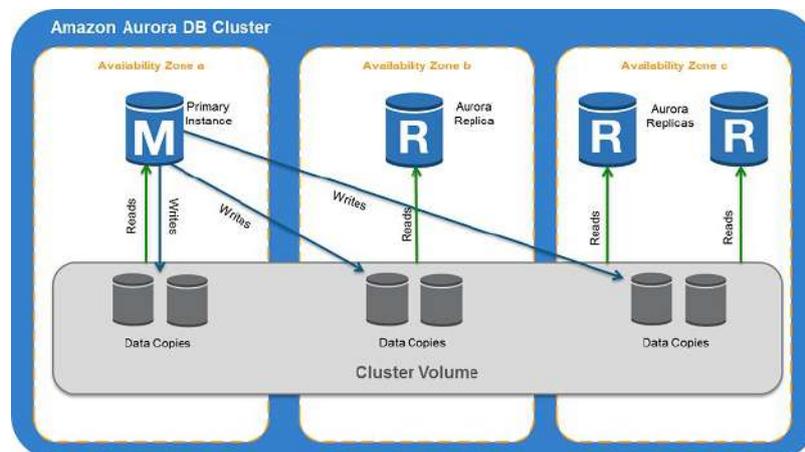
## TEMA 16 - RDS Aurora

Aurora DB clusters es una versión compatible con mysql y postgres.

Pueden trabajar como un servidor normal y en serverless.

Los **clusters** pueden ser:

- **single-master** (un solo master y réplicas) – Una instancia primaria y hasta 15 réplicas (solo lectura). A diferencia de las réplicas de las otras BBDD, estas comparten un cluster de almacenamiento. AWS recomienda que la arquitectura se reparta en distintas AZ.
- **multi-master** (todas las instancias de aurora serían de escritura y lectura) - Solo puede tener hasta 4 instancias



### 16.1. - Crear BBDD tipo Aurora

- Edición
  - mysql
  - postgresQL
- (No aparece single-master y multi-master)
- Permite mostrar
  - Versiones que soportan BBDD global
  - Versiones que soportan consultas paralelas. Traslada el procesamiento a la capa de almacenamiento. Habría que crear un «parameter group» con el parámetro `aurora_parallel_query` activado.

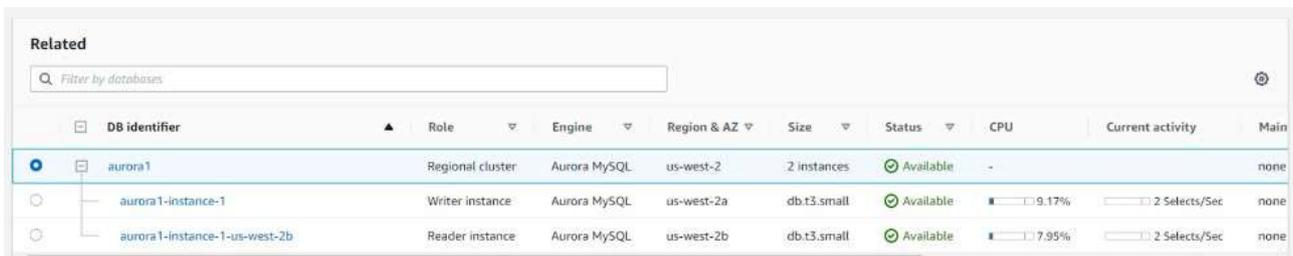
 Parallel query is off by default. To enable it, use a DB Instance parameter group with the `aurora_parallel_query` parameter enabled. [Learn more](#) 

- Versiones severless,
- Plantillas- No hay Free Tier, solo producción y desarrollo.
- Configuración Instancias según la versión que hemos escogido.
- En la configuración adicional hay una casilla de prioridad failover para escoger entre las 15 posibles replicas la preferente. En caso necesario, de forma automática, pasará la master a la escogida.

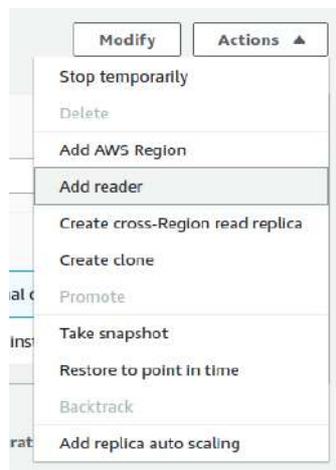


- El backup es obligatorio
- BackTrack – Permite volver a un tiempo de la BBDD si necesidad de recrear la instancia.

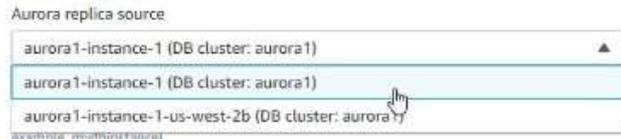
El resto de posibles configuraciones son similares al resto de BBDD.



Se puede añadir regiones, o réplicas de lectura en “actions”



Cuando se añade una réplica nueva se puede escoger de fuente la original u otra replica



Vuelve a dar la opción de escoger la prioridad del failover.

Instance ID	Role	Engine	Availability Zone	Instance Class	Status	Read IOPS	Writes/Sec
aurora1	Regional cluster	Aurora MySQL	us-west-2	3 instances	Available	-	-
aurora1-instance-1	Writer instance	Aurora MySQL	us-west-2a	db.t3.small	Available	9.01%	2 Selects/Sec
aurora1-instance-1-us-west-2b	Reader instance	Aurora MySQL	us-west-2b	db.t3.small	Available	7.48%	2 Selects/Sec
aurora1-replica2	Reader instance	Aurora MySQL	us-west-2a	db.t3.small	Creating	-	-

Los endpoints son globales para todas las réplicas, uno de escritura y otro de lectura (Con prefijo -ro-).

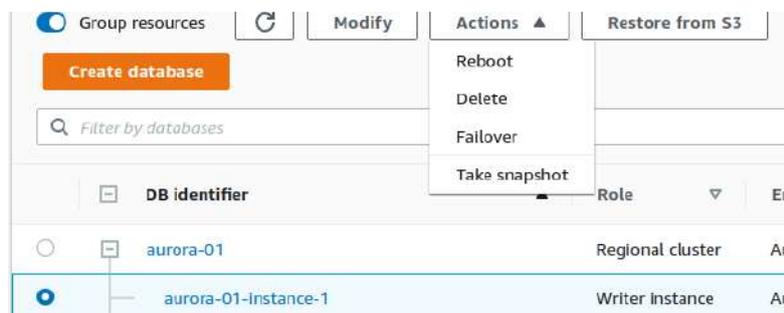
Endpoint name	Status	Type	Port
aurora1.cluster-ch1uvo38tkfx.us-west-2.rds.amazonaws.com	Available	Writer instance	3306
aurora1.cluster-ro-ch1uvo38tkfx.us-west-2.rds.amazonaws.com	Available	Reader instance	3306

Se puede **personalizar los endpoints**



Pueden servir para entrar a réplicas concretas configuradas con instancias más potentes por requerimientos de algún servicio o todo lo contrario, un endpoint a réplicas más ligeras para servicios con pocos requerimientos.

Se puede crear un **failover de una réplica** concreta de escritura con el botón “Actions”.



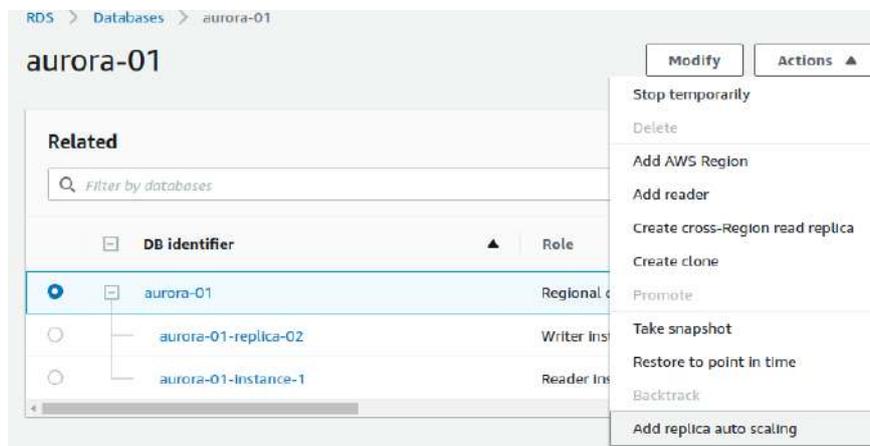
Para comprobarlo se puede ver en los logs del cluster

Recent events (5)

Filter by db events

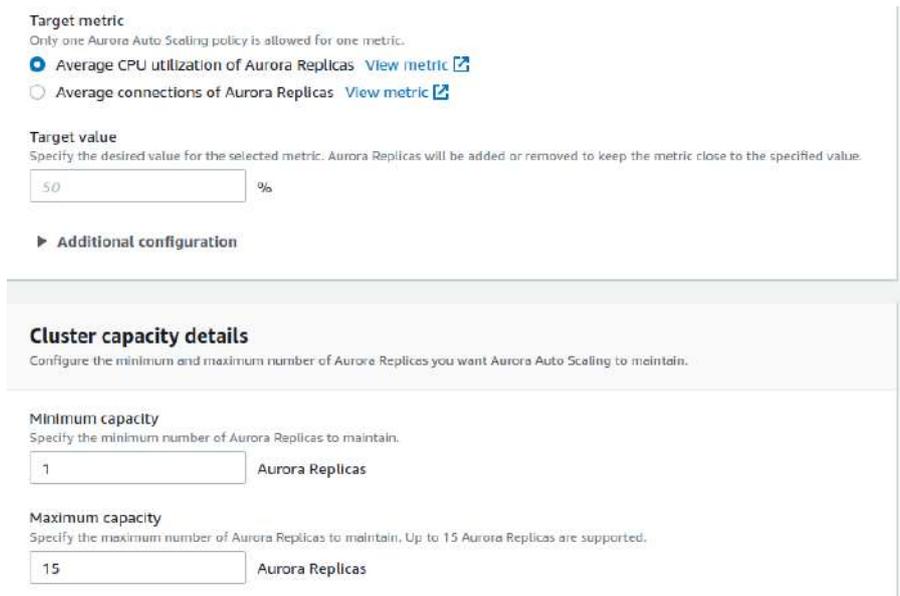
Time	System notes
January 16, 2022, 9:18:00 AM UTC	DB instance created
January 16, 2022, 9:19:25 AM UTC	Monitoring Interval changed to 60
January 16, 2022, 9:20:42 AM UTC	Finished updating DB parameter group
January 16, 2022, 10:27:32 AM UTC	A new writer was promoted. Restarting database as a reader.
January 16, 2022, 10:27:42 AM UTC	DB instance restarted

Se puede crear una **réplica de autoescalada** que pueden venir bien si se desconoce el ciclo de vida que pueden tener las réplicas. Se selecciona el clúster y en “actions” está la opción de “Add replica auto scaling”.

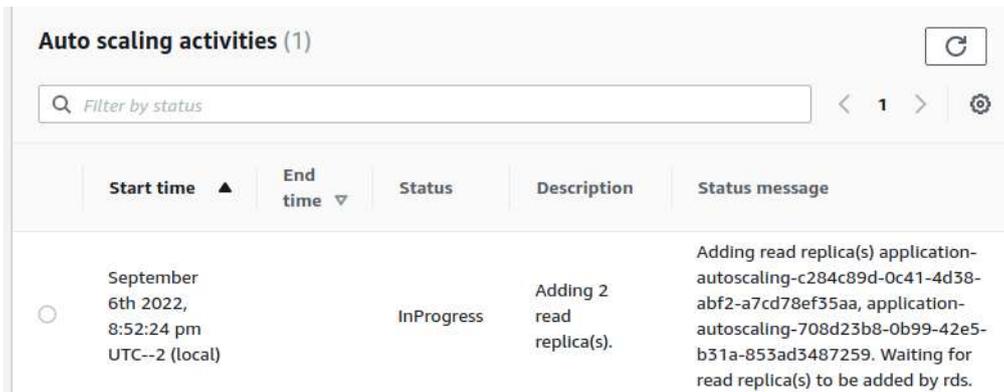


Se le nombra a la política. Se puede

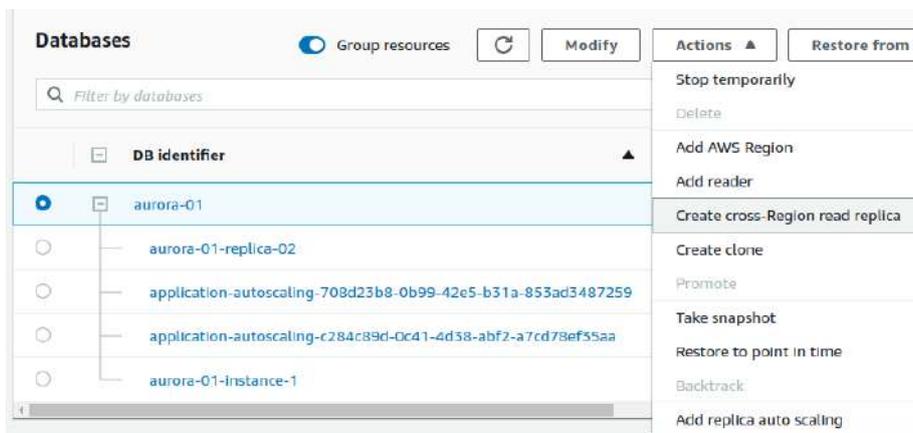
- basar en métricas de CPU o en las conexiones. También se puede determinar los segundos de espera para crear o reducir.
- Indicar el mínimo y el máximo de réplicas.



En el momento que necesita las replicas se pueden ver en los logs de autoescalada.

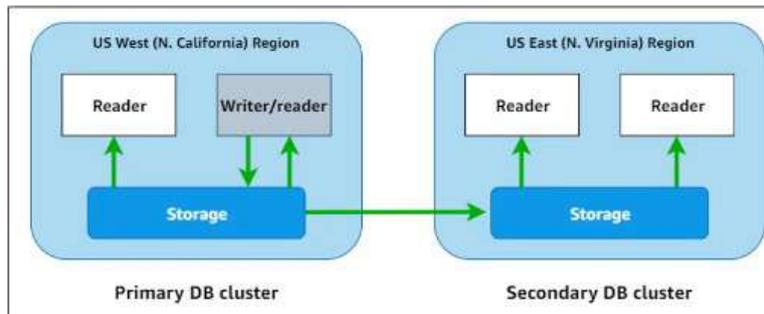


También se puede **replicar el cluster en otra region**. Se presiona “Actions” y “Create cross-Region Read replica”.



Es conveniente seleccionar multi-AZ porque si la replicación se interrumpe se deberá volver a empezar. Es importante antes crear en la region destino el grupo de subnets necesario.

También se puede **extender el cluster a otra región** para hacerlo más grande. Es en “Actions” y “Add AWS Region”. Es la manera de hacerlo global.



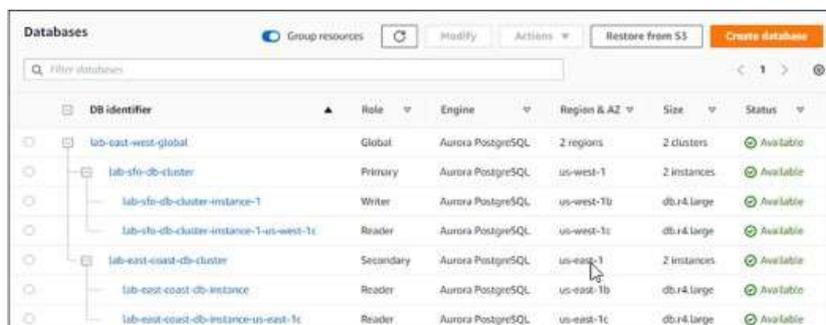
Aurora global databases tiene algunas limitaciones:

- No está en todas las regiones.
- Requiere algunos parámetros de configuración muy concretos.
- Hay unas versiones de mysql y de postgresQL que lo soporta.
- No soporta Multimaster (No está actualmente en RDS), Serverless, Backtrackin ni RDS Proxy.
- Necesitan instancias memory-intensive.

Resumen:

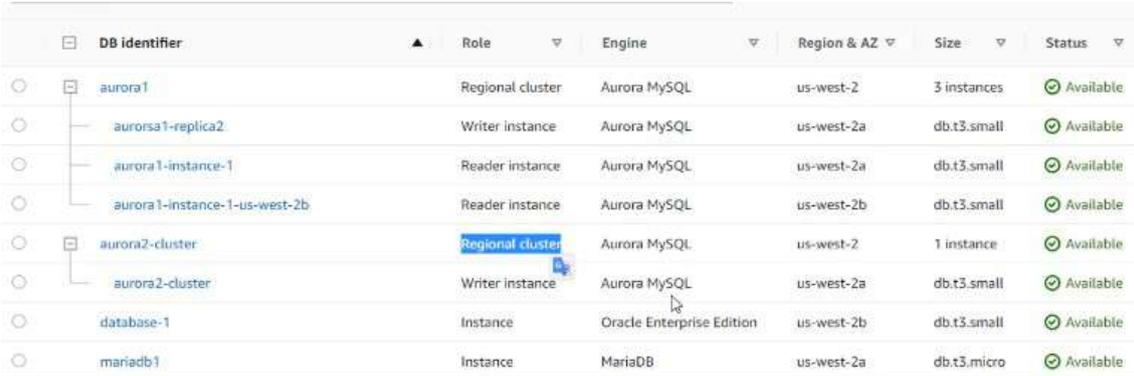
Description	Primary AWS Region	Secondary AWS Regions
Aurora DB clusters	1	5 (maximum)
Writer instances	1	0
Read-only instances (Aurora replicas), per Aurora DB cluster	15 (max)	16 (total)
Read-only instances (max allowed, given actual number of secondary Regions)	15 - s	s = total number of secondary AWS Regions

Aparecería así en las BBDD:



También se puede **clonar el cluster**. En “Action” y “Create clone”. Es la manera más rápida de crear una copia de las BBDD de Aurora.

Hereda el motor, la instancia y la conectividad entre otras cosas. De todas formas algunas propiedades se pueden modificar para que lo haga en la copia. Queda como un clúster independiente del primero:



DB identifier	Role	Engine	Region & AZ	Size	Status
aurora1	Regional cluster	Aurora MySQL	us-west-2	3 instances	Available
aurora1-replica2	Writer instance	Aurora MySQL	us-west-2a	db.t3.small	Available
aurora1-instance-1	Reader instance	Aurora MySQL	us-west-2a	db.t3.small	Available
aurora1-instance-1-us-west-2b	Reader instance	Aurora MySQL	us-west-2b	db.t3.small	Available
aurora2-cluster	Regional cluster	Aurora MySQL	us-west-2	1 instance	Available
aurora2-cluster	Writer instance	Aurora MySQL	us-west-2a	db.t3.small	Available
database-1	Instance	Oracle Enterprise Edition	us-west-2b	db.t3.small	Available
mariaadb1	Instance	MariaDB	us-west-2a	db.t3.micro	Available

Para borrar el cluster completo hay que ir borrando instancias hasta que no quede ninguna. Lo ideal es hacerlo desde CLI con un bucle que se ocupe de borrarlas todas. Las instancias en modo gráfico se borran en “Action” y “Delete”. En la última instancia nos pregunta si queremos guardar un snapshot.

Mientras borramos podemos comprobar que si borramos primero la réplica de escritura, igual que el failover, hará que cualquiera de las otras réplicas se hará de escritura para sustituirla.

No se puede parar réplicas individualmente, se debe parar el clúster completo.

Para **crear una multi-master** (No lo veo, lo explica en el curso, creo que AWS ya no permite multi-master) solo hay unas versiones concretas y en mysql-aurora. El resto de propiedades son idénticas. Pero necesita unas características concretas.

El modo **serverless** en Aurora tiene dos versiones de mysql y 3 de postgresSQL. En este modo tendremos la opción de escoger sin servidor (serverless) en la configuración de la instancia.

Nos permite escoger un rango de ACUs (Aurora Capacity Units. Más o menos un ACU equivale a 2 GB y se le asocia una cantidad de CPU y de red). Con serverless se hace un escalado de recursos para según las necesidades que se van teniendo.

**Instance configuration**  
The DB instance configuration options below are limited to those supported by the engine that you selected above.

DB Instance class [Info](#)

- Serverless
- Memory optimized classes (includes r classes)
- Burstable classes (includes t classes)

Serverless v2 - new  
Instant scaling for even the most demanding workloads.

Include previous generation classes

Capacity range [Info](#)  
Database capacity is measured in Aurora Capacity Units (ACUs). 1 ACU provides 2 GiB of memory and corresponding compute and networking.

Minimum ACUs	Maximum ACUs
<input type="text" value="8"/> (16 GiB)	<input type="text" value="64"/> (128 GiB)
0.5 to 128 in increments of 0.5	1 to 128 in increments of 0.5

Los cambios entre el rango de ACUs, AWS lo hace cuando menos queries tiene. Se recomienda no hacer queries muy largas para darle espacios a los posibles cambios.

En serverless no hay réplicas, es directamente la escala de capacities que hemos indicado.

El **Query editor** es una forma de conectarse a las BBDD serverless, pero necesita el Data API habilitado. Para habilitarlo se debe modificar la BBDD serverless y en conectividad se puede activar la opción.

**Connectivity**

VPC security group  
Choose a VPC security group to allow access to your database. Ensure that the security group rules allow the appropriate incoming traffic.

Choose VPC security groups

default X

Web Service Data API

- Data API [Info](#)  
Enable the SQL HTTP endpoint, a connectionless Web Service API for running SQL queries against this database. When the SQL HTTP endpoint is enabled, you can also query your database from inside the RDS console (these features are free to use).

Entonces ya nos podremos conectar a Query editor y ejecutar las queries online.



Es muy sencilla, para trabajar siempre es mejor un editor externo. Pero se pueden hacer pruebas.

## TEMA 17 - RDS Backup y Mantenimiento

Los backups indican:

- Tiempo que entre las copias
- El tiempo que puede retroceder entre los backups existentes
- El momento en que se hacen las copias.

Un backup es la creación de snapshot de un momento concreto. En los automáticos le da el nombre snapshot-nombrebdd-fecha. Modificando la BBDD se puede modificar algunos aspectos del Backup como el periodo de retención como el horario aproximado para realizarse.

En los Automated backups constan los backups definidos con un resumen de sus propiedades y las snapshots.

En Snapshots aparecen por tipos:

- Manuales – Se hacen eligiendo la BBDD y “Take snapshot”. También en snapshot, en “Take snapshot”
- Automáticas
- Compartidas por mi
- Públicas
- Del servicio de Backups – Es un servicio a parte para hacer backups, y aquí aparecerá los backups que se hagan desde este servicio y que estén relacionados con las BBDD.
- Exportadas en S3



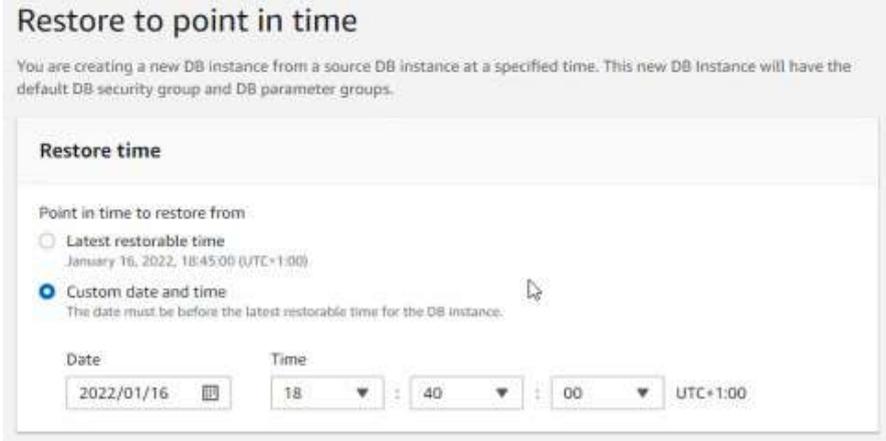
En “Actions” de los snapshots se puede **restaurar, copiar, compartir, migrar y borrar**.

**Copiar** es interesante porque te lo puedes llevar a otra región. Sería como un backup del backup.

Cuando se **comparte** puedes indicar la ID de la cuenta AWS o lo puedes hacer público. El inconveniente que tiene es que se debe compartir la clave por defecto del encriptado. Con lo cuál, tendrá que tener una clave de encriptación (KMS) concreta para esto, no puede ser la clave por defecto que indica AWS.

Para **restaurar**, tan solo hay que darle al botón en “Actions” y lo que hará es generar una nueva BBDD, a la cuál se le puede poner un nombre nuevo y modificar algunos de los parámetros. Es mejor no cambiar el tipo de almacenamiento porque puede tener problemas en la migración.

Una recuperación de un punto en el tiempo de un backup (En Actions/Restore to point in time), en la que vas una semana atrás, por ejemplo, hace perder todas las líneas que se hayan escrito en ese tiempo.



The screenshot shows the 'Restore to point in time' configuration page in the AWS console. At the top, it says 'Restore to point in time' and provides a brief explanation: 'You are creating a new DB Instance from a source DB instance at a specified time. This new DB Instance will have the default DB security group and DB parameter groups.' Below this is a section titled 'Restore time' with two radio button options: 'Latest restorable time' (with a subtext 'January 16, 2022, 18:45:00 (UTC+1:00)') and 'Custom date and time' (with a subtext 'The date must be before the latest restorable time for the DB instance.'). The 'Custom date and time' option is selected. Below the options, there are input fields for 'Date' (showing '2022/01/16' with a calendar icon) and 'Time' (showing '18:40:00' with dropdown menus for each component and 'UTC+1:00' as the time zone).

El tiempo que tarde en restaurar será equivalente al que se tardó en crear más el tiempo que le lleve recuperar todos los datos de la BBDD.

Si se escoge una versión de BBDD antigua, se puede simular como AWS te recomienda actualizar la versión a la actual. Cuando se deben hacer esta clase de actualizaciones, siempre es recomendable efectuar un backup antes de empezar. El **mantenimiento** aparecerá en la pestaña “Maintenance & backups” de la BBDD, en este lugar se pueden aplicar los mantenimientos/actualizaciones.

## TEMA 18 - RDS Migración de Bases de Datos

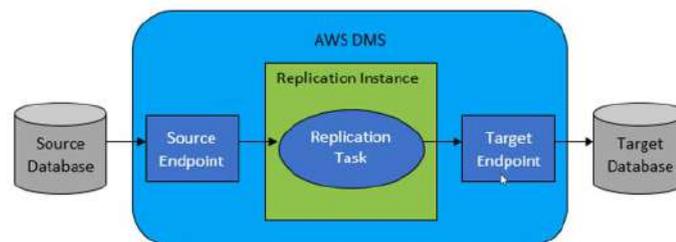
Hay un servicio en concreto para esto con su propio dashboard: Database migration service.

- Permite migrar muchos tipos de bases de datos, tanto en modo cloud como en modo on-premise.
- Se pueden realizar migraciones únicas y también los cambios que se puedan ir produciendo.
- Se pueden migrar entre distintos motores de BBDD
- Se pueden perfilar y mejorar la migraciones con la herramienta SCT (Schema Conversion Tool). Se descarga en local y permite definir los esquemas de entrada y salida.
- Se pueden hacer transformaciones y conversiones en el proceso.

Se necesita una instancia para efectuar la migración. En esta máquina se hará todo el trabajo pesado de replicación. Hay que tener en cuenta el costo de la instancia.

### Migración de Bases de Datos

#### □ Arquitectura General



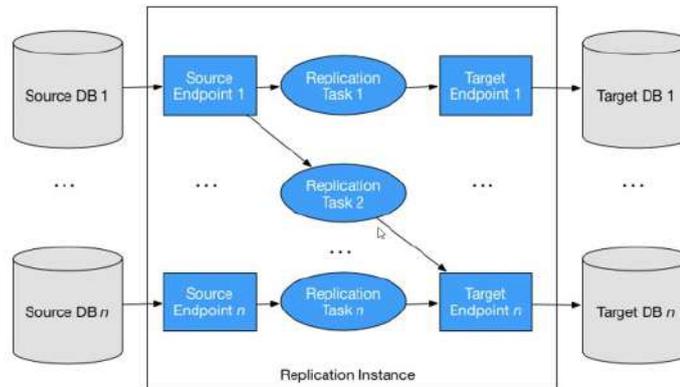
Tendremos un origen apuntando a un endpoint de entrada y un endpoint de salida apuntando al destino de la migración.

En la documentación podemos encontrar las BBDD origen y destino que se soportan en AWS.

Como trabaja es creando replication task que son independientes.

## Migración de Bases de Datos

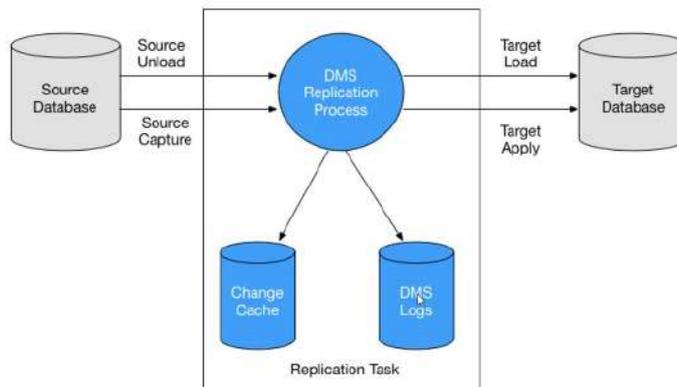
### Procesos



Crearé una cache de cambios y logs de cada proceso de replicación

## Migración de Bases de Datos

### Procesos



### 18.1. - Hacer migración

La migración se hace en AWS DMS (Database Migration Service).

Lo primero que debemos hacer es una replication instances. Hay instancias especializadas para esta cuestión. Dependiendo de las necesidades de la migración necesitaremos una instancia más grande o más pequeña, existen de todos los tamaños.

Las propiedades que le podemos dar son:

- Nombre
- Nombre descriptivo para el sufijo del ARN

- Descripción
- Clases de instancias
- Versión de la ingeniería. Se debe asegurar en la documentación que acepta el tipo y versión de BBDD. Se puede escoger una versión Beta
- Tamaño del almacenamiento. No es solo el tamaño de la BBDD, hay que contar que habrá archivos temporales, procesos, etc además del tamaño de la BBDD.
- VPC
- Opción Multi-AZ. Si se escoge tendremos una replicación primaria y el resto serán standby. Puede venir bien si creemos que puede dar errores un proceso de migración.
- Acceso público
- Grupos de subnet. Son igual que las de BBDD, pero no son las mismas. Hay que crearla antes de empezar a crear la instancia
- Zona habilitada
- Grupo de seguridad
- KMS key
- El modo mantenimiento
- Tags. Importante en desarrollo y producción tenerlos para poder filtrar búsquedas

Estas máquinas aparecerán en el servicio DMS, no en EC2 ni en otro lugar. La manera de gestionarla es en la consola correcta.

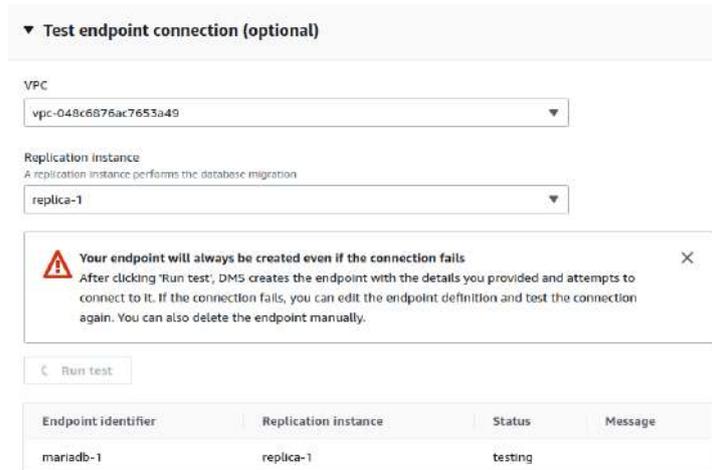
Ahora debemos **preparar el entorno** de la migración. **DMS tiene que poder conectarse a las BBDD** tanto de origen como de destino. O bien con acceso público o por VPN o con conexión interna....

Tenemos que **tener un usuario en la BBDD para la migración** con los permisos adecuados para los datos a migrar.

Ahora tendremos que **crear los endpoint** de tipo fuente y de tipo destino. Cuando escogemos una BBDD de RDS tendremos que marcarlo para que nos aparezca. Si la BBDD está en otra ubicación deberemos dejarlo desmarcado. Las propiedades de una BBDD en RDS son:

- Deberemos marcar el tipo de acceso, si es “AWS Secrets Manager” (Se verá más adelante, permite guardar contraseñas) o “Provide access information manually” (Introducimos la contraseña de manera manual)
- KMS key
- Tags

- Test conexión endpoint – para probar si se puede conectar.



Si todo va bien aparecerá successful

Endpoint identifier	Replication instance	Status	Message
mariadb-1	replica-1	successful	

Y creamos endpoint.

Las propiedades de una BBDD fuera de RDS son las mismas pero cambian algunas:

- En la conexión deberemos especificar:
  - Nombre de servidor
  - Puerto
  - Nombre usuario
  - Contraseña

Es **IMPORTANTE** efectuar los test de conexión para evitar problemas o confusiones.

Ahora tendremos que **crear una tarea de migración**. Se pueden definir los siguientes parámetros:

- identificado de tarea
- Prefijo ARN
- Indicar la instancia replica
- indicar las BBDD de origen y destino
- Tipo de migración. Puede ser:

- Migrar datos existentes
- Migrar datos existentes y replicar los cambios que vayan sucediendo.
- Replicar los cambios que vayan sucediendo
- En las opciones se pueden poner a través de un asistente Wizard o de un archivo JSON. El JSON tiene más posibles opciones pero normalmente no es necesario. Ejemplos de opciones:
  - Las tablas en destino se pueden borrar, truncar o no hacer nada.
  - Que se hace con las LOB (Large Objects. Que contienen objetos grandes. Suelen ser binarios con archivos adjuntos.). Se pueden no incluir, incluir todo o un modo limitado.
  - Podemos habilitar una validación al final que tardará equivalentemente a lo que tarde en migrar.
  - Podemos añadir logs a CloudWatch
  - Crear una control table.
- Mapeos de tabla que también tiene opción Wizard y por archivo JSON.
  - Añadir nueva regla schema
  - Decir el schema concreto
  - Las tablas
  - Y la acción.

▼ Selection rules

Choose the schema and/or tables you want to include with, or exclude from, your migration task. [Info](#) Add new selection rule

---

▼ where schema name is like 'curso\_aws' and Source table name is like '%', Include ✕

Schema

Source name  
 Use the % character as a wildcard

Source table name  
 Use the % character as a wildcard

Action  
 Choose "Include" to migrate your selected objects, or "Exclude" to ignore them during the migration.

Source filters [Info](#) Add column filter

- Reglas de transformación. No es una ETL (Extraer, transformar y cargar) que en AWS es el servicio GLUE, mucho más completo.
  - Escoger un origen de schema, tabla o Columna
  - Nombre del schema
  - Nombre de tabla
  - Y escoger la acción. (Mover a, renombrar, hacer mayúscula o minúsculas, añadir prefijo, etc)
- Premigration assessment. Sirve para hacer una serie de pruebas antes de empezar la migración para buscar posibles errores. El informe lo deja en un bucket S3 Se le da un nombre identificativo y se puede comprobar

Assessments to run

- Large objects (LOBs) are used but target LOB columns are not nullable**  
Checks for nullability of a LOB column in the target when full LOB mode or inline LOB mode is used. AWS DMS requires a target LOB column to be nullable when using these LOB modes.
- Source table with LOBs but without primary keys or unique constraints**  
Checks for the presence of source tables with LOBs but without a primary key or unique key. For AWS DMS to migrate LOBs, a source table must have a primary key or unique key.
- Source table without primary key for CDC or full load and CDC tasks only**  
Checks for the presence of a primary key or a unique key in source tables. The lack of a primary key or a unique key during change data capture (CDC) can cause performance issues during replication.
- Target table without primary keys for CDC tasks only**  
Checks for the presence of a primary key or a unique key in already created target tables for a database migration task performing a change data capture (CDC) replication. Lack of a primary key or unique key in a target table can cause full table scans on the target when AWS DMS applies updates or deletes. This can result in performance issues during replication.
- Unsupported data types**  
Checks for data types unsupported by AWS DMS in the source endpoint. Not all data types can be migrated between endpoint types.
- Unsupported source primary key types - composite primary keys**  
Checks for the presence of composite primary keys in source tables. This option is for migrating to either Amazon DynamoDB (applies to all DMS replication Instance versions) or Amazon Elasticsearch Service (applies only to DMS replication instances before 3.3.3). The source table's primary key must be a single column.

- Pregunta si comienza la migración solo crear la tarea o posteriormente.

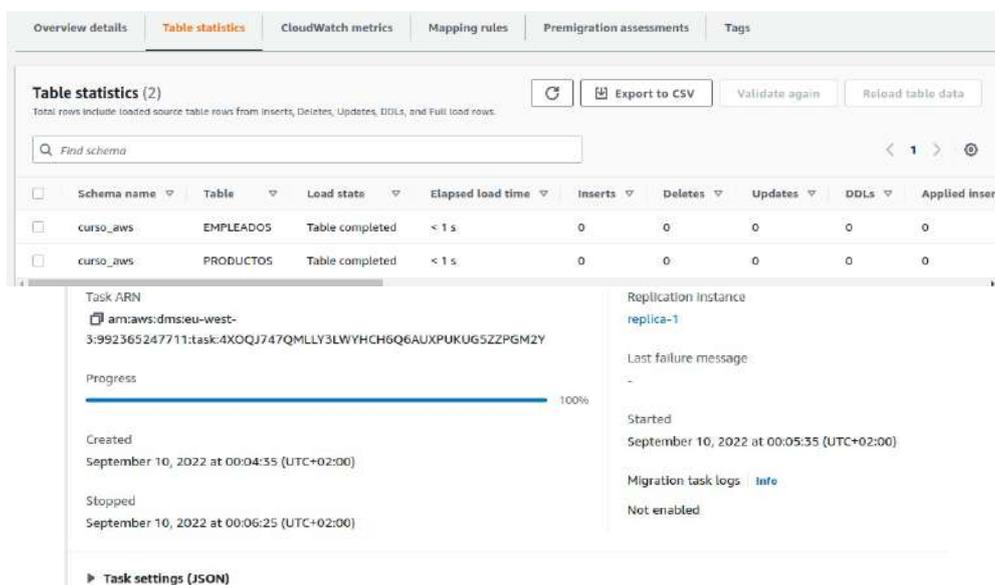
The screenshot shows the configuration for a transformation rule named 'convert-uppercase'. At the top, it specifies the source: 'where schema name is like 'curso\_aws' and table name is like 'EMPLEADOS''. Below this, the configuration is as follows:

- Target:** A dropdown menu set to 'Table'.
- Schema name:** A dropdown menu set to 'Enter a schema'.
- Schema name:** A text input field containing 'curso\_aws'. Below it, a note says 'Use the % character as a wildcard'.
- Table name:** A text input field containing 'EMPLEADOS'. Below it, a note says 'Use the % character as a wildcard'.
- Action:** A dropdown menu set to 'Make uppercase'.

Una vez se completa la tarea nos da bastante información:



- Detalles generales
- Estadísticas de tabla. Se pueden comprobar las filas y muchos otros datos



- Las métricas CloudWatch
- Mapping rules (Reglas de mapeo)
- La premigración.
- Etiquetas

Hay que prestar especial atención cuando la migración es en BBDD de origen y destino de diferentes tipos.

## 18.2. - SCT (Schema Conversion Tool)

La herramienta SCT (Schema Conversion Tool) nos puede ayudar a la conversión de datos concretos que den problemas. Nos permite algunas conversiones:

Source Database	Target Database on Amazon RDS
Oracle Database	Amazon Aurora MySQL-Compatible Edition (Aurora MySQL), Amazon Aurora PostgreSQL-Compatible Edition (Aurora PostgreSQL), MariaDB 10.5, MySQL, PostgreSQL
Oracle Data Warehouse	Amazon Redshift
Microsoft Azure SQL Database	Aurora MySQL, Aurora PostgreSQL, MySQL, PostgreSQL
Microsoft SQL Server	Amazon Redshift, Aurora MySQL, Aurora PostgreSQL, Babelfish for Aurora PostgreSQL (only for assessment reports), MariaDB, Microsoft SQL Server, MySQL, PostgreSQL
Teradata	Amazon Redshift
IBM Netezza	Amazon Redshift
Greenplum	Amazon Redshift
HPE Vertica	Amazon Redshift
MySQL	Aurora PostgreSQL, MySQL, PostgreSQL
PostgreSQL	Aurora MySQL, Aurora PostgreSQL, MySQL, PostgreSQL
IBM DB2 LUW	Aurora MySQL, Aurora PostgreSQL, MariaDB, MySQL, PostgreSQL
IBM Db2 for z/OS	Aurora MySQL, Aurora PostgreSQL, MySQL, PostgreSQL
Apache Cassandra	Amazon DynamoDB
SAP ASE	Aurora MySQL, Aurora PostgreSQL, MariaDB, MySQL, PostgreSQL
Amazon Redshift	Amazon Redshift
Azure Synapse Analytics	Amazon Redshift
Snowflake	Amazon Redshift
BigQuery	Amazon Redshift

Se debe descargar e instalar en Windows (exe), Fedora (rpm) y Ubuntu (deb).

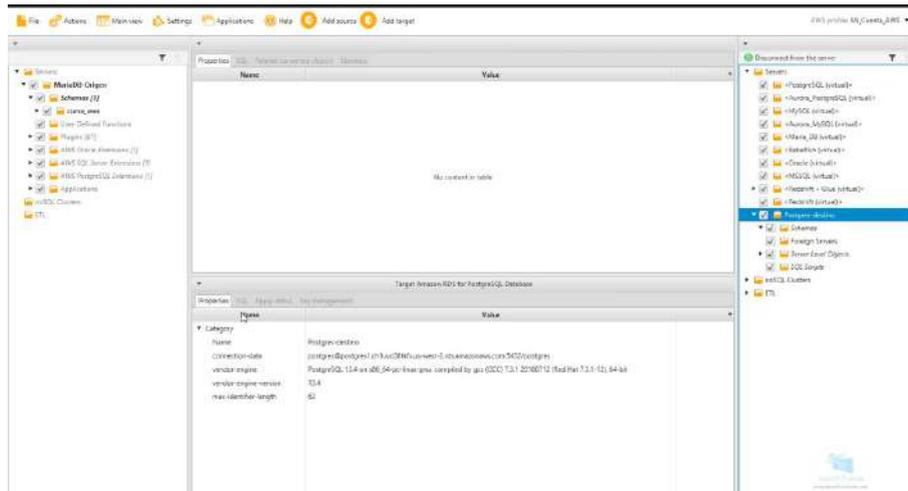
Dentro de la aplicación, antes de hacer nada tenemos que:

- Global Setting/AWS service profile/Añadir uno nuevo con las credenciales correctas. Se convierte en el perfil por defecto.
- Global Settings/Drivers/Descargar los drivers que se necesiten para el mapeo. Por ejemplo, el de mysql es el connecto/J, el de postgres se llama igual... Los dos son .jar.

Podremos comprobar en Data Migration view que podremos comprobar los proyectos de migración que tengamos en la cuenta conectada.

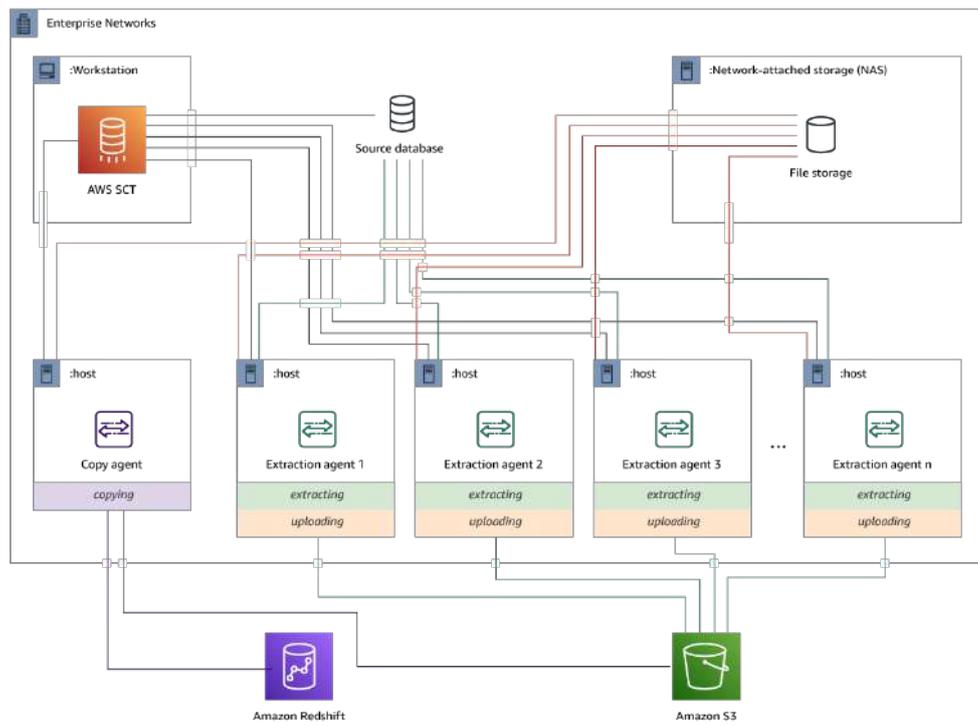
En el **mapping view** se crea el mapeo.

- Se añade la fuente con todos los datos y se efectua un test connection
- Se añade el destino con todos los datos y se efectua un test connection
- Ahora ya se puede crear el mapping
  - Nueva regla de migración y sus datos.
  - Nueva regla de transformación y sus datos.
- Después podemos revisar en main view los schemas de las BBDD



- Después creamos la tarea de migración

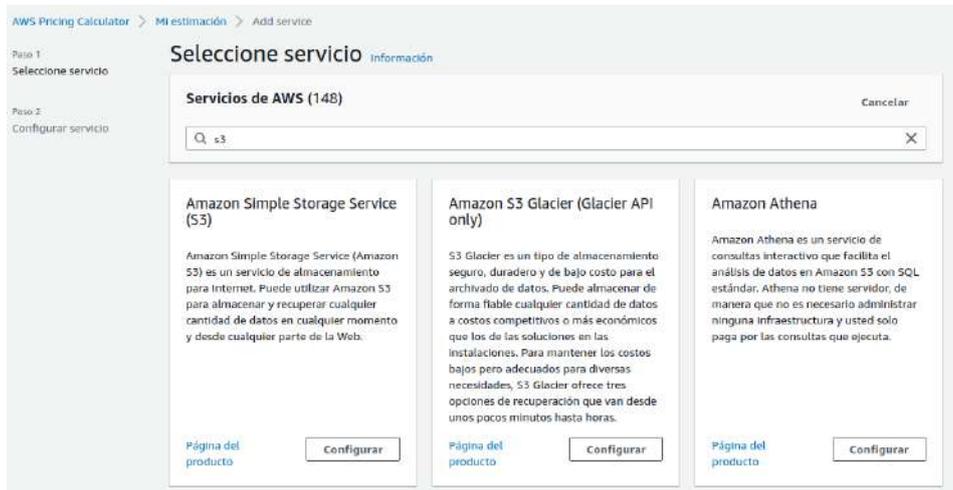
Ejemplo de mapeo:



# TEMA 19 - Calculadora de Precios

Con esta herramientas se pueden hacer estimaciones. Si se tiene claro los productos que se necesitan y el tiempo de uso, está herramienta es muy certera: <https://calculator.aws/#/>

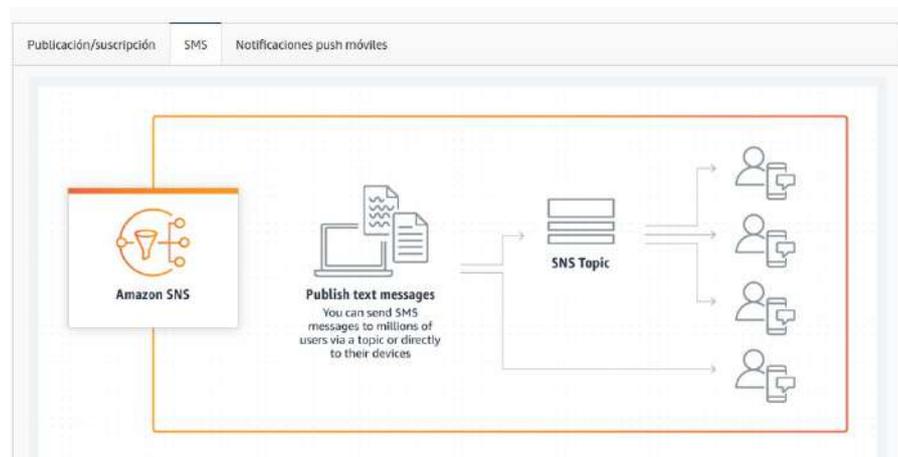
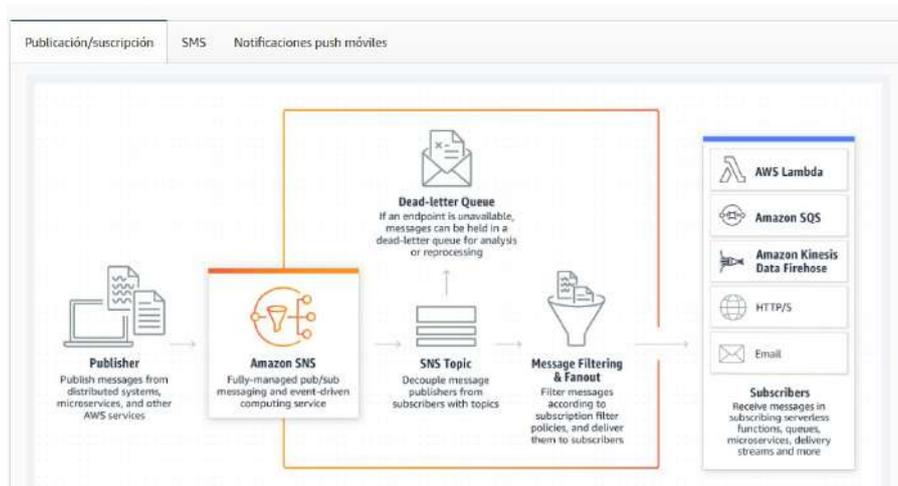
Se crea una estimación, se añaden servicios por tipo configurando al detalle los recursos.



# TEMA 20 - SNS Simple Notification Service

Es un servicio de notificaciones push móviles, correo electrónico, SMS y mensajería de suscripción que nos puede servir para cualquier notificación de AWS.

AWS SNS se ocupa de guardar los mensajes en un SNS Topic. Con lo cuál, las aplicaciones conectadas lo que hacen es consultar SNS Topic como si fuese un buzón





Con este servicio se pueden coger mensajes de cualquier servicio y redirigirlo a cualquier otro.

Los Topics sirven para conectar dos infraestructuras diferentes, es un servidor de mensajes como IBM-MQ de IBM y JMS de Java. Lo que hacen es preparar un mensaje origen para que lo pueda interpretar en destino.

A nivel de servidores de mensajes tenemos varios tipos:

- Point to point – Los que tienen un mensaje específico para un destinatario concreto.
- Topic – Son las suscripciones. Son mensajes que se recopilan para leer por 1 a n destinos.

Otro servicio de AWS es SQS que es un servidor de mensajes que tiene Point to point y Topics.

## 20.1. - Crear un servicio SNS

Lo primero es **crear un Topic**. Los parámetros configurables son:

- Tipo
  - FIFO Primero en llegar es el primero en salir
  - Standard
- Nombre
- Descripción
- Se puede definir una Política de protección de datos.
- Encriptación
- Definir la política de Acceso
- La política de devolución de mensajes
- Logging

- Etiquetas

Se puede hacer una prueba de mensajes, indicando:

- El mensaje
- TTL
- body - la estructura del mensaje. Se puede escoger una diferente según el destino
- Los atributos – estarán asociados al mensaje. Será el destino quien tenga que descifrarlos.

El siguiente paso es **crear una suscripción**. Que es indicar el tipo de destino a donde queremos enviar los mensajes. Tendremos que indicar:

- El topic que queremos utilizar
- El protocolo que queremos utilizar.

- Indicaremos el endpoint, por ejemplo, en email será la cuenta de correo electrónico en concreto.
- Se pueden filtrar suscripciones. Por ejemplo, algún tipo como error.
- dead-letter-queue – Es la cola de mensajes muertos, que no se han podido crear. Puede venir bien para manipular esos mensajes en un futuro.

Una vez se crea la suscripción, el mail destino tendrá que confirmar que quiere esta suscripción.

You have chosen to subscribe to the topic:  
**arn:aws:sns:eu-west-3:992365247711:Base-de-datos**

To confirm this subscription, click or visit the link below (If this was in error no action is necessary):  
[Confirm subscription](#)

Please do not reply directly to this email. If you wish to remove yourself from receiving all future SNS subscription confirmation requests please send an email to [sns-opt-out](#)

Deberemos confirmar en el mensaje y después podremos ver en suscripción que ya está confirmado.

ID	Endpoint	Status	Protocol	Topic
89a571d8-52c7-4efa-8caf-976e8609db05	manuel@vergaracarmona.es	Confirmed	EMAIL	Base-de-datos

Ahora ya tenemos el topic y el destino de la suscripción, deberemos **crear el origen**.

**En RDS** hay una opción en el sidebar que son los eventos. Vamos a «Event subscriptions» y creamos uno nuevo. Podemos escoger los siguientes parámetros:

- Nombre
- Destino. Aquí podemos escoger el topic o crear uno nuevo.
- Origen. En el caso de RDS se pueden indicar snapshots, Cluster snapshots, Instances, Parameter groups, Security Groups, Clusters y RDS proxies.
  - Se podrá especificar todos los objetos, varios o uno en concreto.
  - Se podrá especificar todos los eventos, varios o uno en concreto.

Una vez creado, tendremos un evento activo que producirá mensajes hacia el topic, y este, los remitirá al suscriptor.

**En S3** podemos ir a las propiedades de un bucket podremos ver “AWS CloudTrail data events”, que es un servicio parecido, y “Events notifications” donde podremos enviar una notificación a SNS con los eventos. Ahora bien, en el caso de S3 debemos dar permisos correctos porque el usuario es el de S3:

- Seleccionamos la ARN del topic SNS.
- Seleccionamos el ARN del bucket.
- Volvemos a SNS y creamos una política de seguridad en el topic que queramos usar:

```
{
  "Version": "2012-10-17",
  "Id": "example-ID",
  "Statement": [
    {
      "Sid": "Ejemplo SNS",
      "Effect": "Allow",
      "Principal": {
        "Service": "s3.amazonaws.com"
      },
      "Action": [
        "SNS:Publish"
      ],
      "Resource": "SNS-topic-ARN",

```

```

    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:s3:*:*:bucket-name"
      },
      "StringEquals": {
        "aws:SourceAccount": "bucket-owner-account-id"
      }
    }
  ]
}

```

Las políticas son idénticas a las de S3. En este ejemplo habilitamos que el servicio S3 publique en SNS utilizando el topic SNS desde el origen del bucket concreto y con el usuario indicado.

Ahora ya podemos volver a S3 y en las propiedades del bucket “Creamos un event notification” con los siguientes parámetros:

- Nombre
- Prefijo y/o Sufijo – para filtrar la ubicación y los objetos en sí.
- Tipos de eventos a notificar. Se pueden especificar en concreto o seleccionar todos.
- Destino. Podemos escoger entre varios. En todos ellos tendremos que escogerlos de una lista o especificar el ARN.
  - Función Lambda – Es una función que se ejecuta en un entorno Serverless.
  - SNS Topic
  - SQS queue

**En EC2**, en concreto en un grupo de autoescalada. Cuando se crea un grupo de autoescalada, en el paso de “Add notifications” donde elegimos el SNS Topic y los tipos de eventos que notifica.

## Add notifications Info

Send notifications to SNS topics whenever Amazon EC2 Auto Scaling launches or terminates the EC2 instances in your Auto Scaling group.

▼ **Notification 1** Remove

**SNS Topic**  
Choose an SNS topic to use to send notifications

Create a topic

**Event types**  
Notify subscribers whenever instances

- Launch
- Terminate
- Fail to launch
- Fail to terminate

Add notification

Cancel Previous Skip to review Next

Tal y como se vayan produciendo los eventos seleccionados los notificará al topic.

## 20.2. - Ejemplo CLI RDS

Documentación: <https://awscli.amazonaws.com/v2/documentation/api/latest/reference/sns/index.html>

aws sns

Subcomandos:

- add-permission
- check-if-phone-number-is-opted-out
- confirm-subscription
- create-platform-application
- create-platform-endpoint
- create-sms-sandbox-phone-number
- create-topic
- delete-endpoint
- delete-platform-application
- delete-sms-sandbox-phone-number
- delete-topic
- get-data-protection-policy
- get-endpoint-attributes
- get-platform-application-attributes
- get-sms-attributes
- get-sms-sandbox-account-status
- get-subscription-attributes
- get-topic-attributes
- list-endpoints-by-platform-application
- list-origination-numbers
- list-phone-numbers-opted-out
- list-platform-applications
- list-sms-sandbox-phone-numbers
- list-subscriptions
- list-subscriptions-by-topic
- list-tags-for-resource
- list-topics
- opt-in-phone-number
- publish
- publish-batch
- put-data-protection-policy
- remove-permission
- set-endpoint-attributes
- set-platform-application-attributes
- set-sms-attributes

- set-subscription-attributes
- set-topic-attributes
- subscribe
- tag-resource
- unsubscribe
- untag-resource
- verify-sms-sandbox-phone-number

#### Ver los topics

- aws sns list-topics

#### Ver las suscripciones

- aws sns list-subscriptions

#### Crear un topic

- aws sns create-topic --name Nombre-del-topic

#### Asociar suscripción con un topic

- aws sns subscribe --topic-arn ARN-del-topic --protocol [http | https | email | email-json | sms | sqs | application | lambda | firehose] --notification-endpoint Correo-electronico-o-telefono-o...

#### Desasociar suscripción de un topic

- aws sns unsubscribe -subscription-arn ARN-de-suscripción

#### Borrar Topic

- aws sns delete-topic --topic-arn Nombre-ARN-del-topic

#### Borrar endpoint

- aws sns delete-endpoint

## TEMA 21 - Grupo de Recursos y editor de Tags

Una buena política de etiquetas nos puede servir para poder tener categorizados con una jerarquía los objetos desplegados. De esta manera, desde la monitorización en CloudWatch o desde el control de costes en Billing, tendremos facilidad para informes, para aplicar métricas, para gestión y control de multitud de aspectos. Es **IMPORTANTE** la decisión de una política de etiquetado en la infraestructura entre los miembros de la organización.

Con “Resource Groups & Tag Editor” podemos tener un control de la gestión de las etiquetas. Además, podemos crear plantillas de infraestructura con CloudFormation.

En el **Editor de Tags** podemos etiquetar masivamente recursos concretos de forma que lo podamos agrupar en un grupo de recursos. Los parámetros que podemos usar para filtrar son por Regiones, por tipo de recursos y/o por etiquetas ya existentes.

Una vez le damos a buscar recursos nos aparece un listado desde donde podemos seleccionar para etiquetar con el key:valor que queramos clicando en “Manager tags”.

The screenshot shows the AWS Tag Editor interface. At the top, it says "Selected resources (4)" and "View the tags for the editable resources you selected." Below this is a search bar for resources. A table lists the selected resources:

Identifier	Tag Name	Service	Type	Region	Tags
i-0e060585af6bcbab9	ServidorParisPruebas1AmazonLinux	EC2	Instance	eu-west-3	2
subnet-05a5296b719979d78	subred-privada	EC2	Subnet	eu-west-3	1
subnet-048e5fac71f2ddd18	subnet-publica-2	EC2	Subnet	eu-west-3	1
subnet-07ae071a8707974bb	subnet-publica	EC2	Subnet	eu-west-3	1

Below the table is the "Edit tags of all selected resources" section. It contains a form with the following fields:

- Tag key: Entorno
- Tag value - optional: Desarrollo
- Name: Selected resources have different tag values
- Responsible: Manu

At the bottom, there are buttons for "Add tag", "Cancel", "Previous", and "Review and apply tag changes".

En “Tags Policies” es una opción que nos permite crear una política de etiquetado para añadirlas en los nuevos objetos.

En **crear un grupo de recursos** podemos basarlo en Tags o en CloudFormation stack. Basados en Tags tenemos la siguiente configuración:

- Se puede agrupar con unos criterios concretos, por ejemplo, buscando recursos directamente en un listado o añadiendo directamente las etiquetas key:valor. Hacemos una preview de los resultados de filtrado.
- Se puede agrupar otros grupos de recursos
- Nombre y descripción del grupo

- Etiquetas de grupo (Opcional)

Una vez se cree se pueden ver en “Saved Resource Groups”.

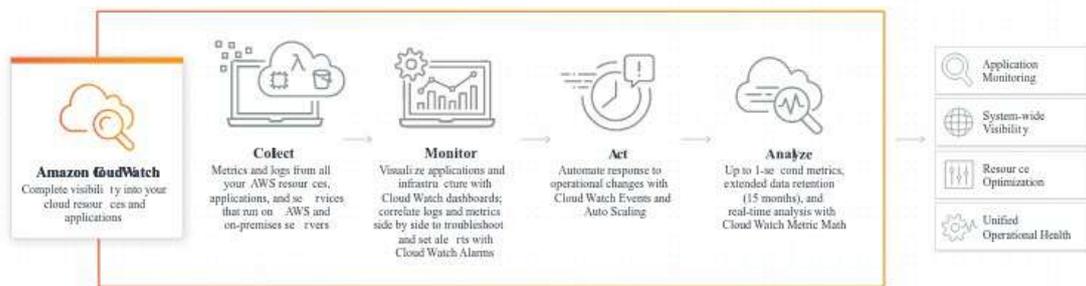
# TEMA 22 - CloudWatch. DashBoards y Métricas

Es el servicio que ofrece AWS para monitorizar y controlar logs. Agrupa un conjunto de funcionalidades para métricas, logs, alarmas, etc.

Existen servicios parecidos para este control, como “AWS EventBridge”.

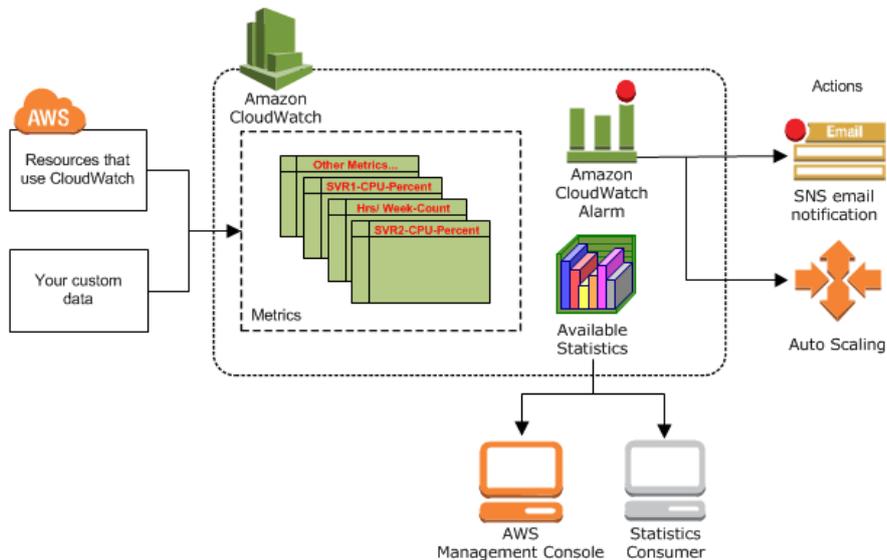
CloudWatch recolecta información para la monitorización. A través de los eventos puede proceder a acciones concretas destinadas a ayudar al análisis de la información para encontrar patrones, detectar posibles problemas o incluso incluirlos en machine Learning.

Este ciclo permite llevarlas a aplicaciones de monitorización, tendremos una visión amplia del sistema, podremos optimizar los recursos y unificar las operaciones de mantenimiento.



## 22.1. - Conceptos

Arquitectura del producto:



Es el lugar donde se almacenan las métricas de los recursos configurados.

AWS envía sus métricas y podemos configurarlas. Con las alarmas de CloudWatch se pueden hacer dos acciones: Notificación SNS o Auto escalar.

Las estadísticas que va guardando CloudWatch se pueden explotar desde la gestión de AWS o por terceros.

Unos **conceptos básicos** son:

- **namespaces** – Un contenedor para métricas de CloudWatch. Las métricas en distintos espacios de nombres están aisladas entre sí, de forma que las métricas de distintas aplicaciones no estén acumuladas por error en las mismas estadísticas. Los espacios de nombres de AWS utilizan la nomenclatura: AWS/service. Ejemplos: AWS/S3, AWS/EC2, etc
- **Métricas** – Representan una serie de DataPoints ordenados temporalmente que se publican en CloudWatch. Una métrica es una variable que hay que monitorizar y los **DataPoints** son los valores de esa variable a lo largo del tiempo. Por ejemplo, el uso de la CPU de una determinada instancia EC2 es una métrica que Amazon EC2 proporciona y se almacena como un DataPoint.
- AWS dispone de un **conjunto de métricas** para sus servicios de forma gratuita:
  - Monitorización básica: frecuencia de 5 minutos.
  - Monitorización detallada: frecuencia de 1 minuto. Se cobra a parte.
  - Métricas personalizadas: pueden llegar a una frecuencia de 1 segundo.

Las métricas son específicas de una región.

- **Retención de métricas:**
  - Los DataPoints con un período de menos de 60 segundos están disponibles durante 3 horas. Estos DataPoints son métricas personalizadas de alta resolución.
  - Los DataPoints con un período de 60 segundos están disponibles durante 15 días.
  - Los DataPoints con un período de 300 segundos (5 min.) están disponibles durante 63 días.
  - Los DataPoints con un período de 3600 segundos (1 hora) están disponibles durante 455 días. (15 meses).
  - Después de los 15 meses si no se usan se pierden.

Los DataPoints con un periodo más corto se acumulan para almacenarlos a largo plazo. Por ejemplo, si recopilamos datos con un período de 1 minuto, los datos están disponibles durante 15 días con una resolución de 1 minuto. Después de 15 días estos datos siguen estando disponibles, pero se acumulan y solo se pueden recuperar con una resolución de 5 minutos. Después de 63 días, los datos siguen acumulándose y están disponibles con una resolución de 1 hora.

- **Time stamp** – Cada DataPoint debe asociarse a una marca temporal o timestamp. La marca temporal puede ser de hasta dos semanas en el pasado y de hasta dos horas en el futuro. CloudWatch crea una en función de la hora a la que se recibió el punto de datos.
- **Dimensiones** – Es un par de nombre-valor que forma parte de la identidad de una métrica... Cada métrica tiene características específicas que la describen y puede considerar las dimensiones como categorías para las características.
- **Units** – Cada estadística tiene una unidad de medida. Entre las unidades de ejemplo se incluyen Bytes, Seconds, Count y Percent.
- **Aggregation** – Amazon CloudWatch acumula estadísticas de acuerdo con la duración del periodo que especifique al recuperar las estadísticas.
- **Percentiles** – Indica el peso relativo de un valor en un conjunto de datos. Por ejemplo, el percentil 95 significa que el 95% de los datos está por debajo de este valor y el 5 por ciento de los datos está por encima del mismo. Los percentiles ayudan a entender mejor la distribución de los datos de métricas. Los percentiles se suelen utilizar para aislar anomalías.
- **Alarms** – Vigila una única métrica durante el período especificado y realiza una o varias acciones especificadas según el valor de la métrica relativo a un determinado umbral durante un período de tiempo. La acción es una notificación que se envía a un tema de Amazon SNS o a una política de Auto Scaling.

## 22.2. - Consola de CloudWatch

- **Dashboards** – Son los cuadros de mando desde donde monitoriza. Se pueden personalizar con widgets o se pueden crear automáticos.
- **Alarms** – Gestión de las alarmas
- **Logs** – Se pueden agrupar o se pueden usar queries para buscar concretos con Logs Insights.
- **Metrics** – Es el componente básico donde se va recopilando la información para poder utilizarla en la monitorización y el rendimiento.
- **x-ray traces** - Ayuda a analizar y depurar las aplicaciones distribuidas, como las construidas con una arquitectura de microservicios. Se puede comprender el rendimiento de aplicaciones y servicios subyacentes, e identificar y solucionar la causa raíz de los problemas de rendimiento y los errores.
- **Events** – Los eventos se gestionan desde EventBridge. Antes estaba integrado aquí pero se separó el servicio.
- **Application monitoring** – Se puede construir aplicaciones para que envíen información a CloudWatch.
- **Insights** – Son descubrimientos que se hacen en algún entorno. Se pueden aplicar en Contenedores, Lambda, con colaboradores y en aplicaciones.

En las **Settings** se pueden configurar algunos comportamientos del producto.

### 22.2.1. - Dashboards

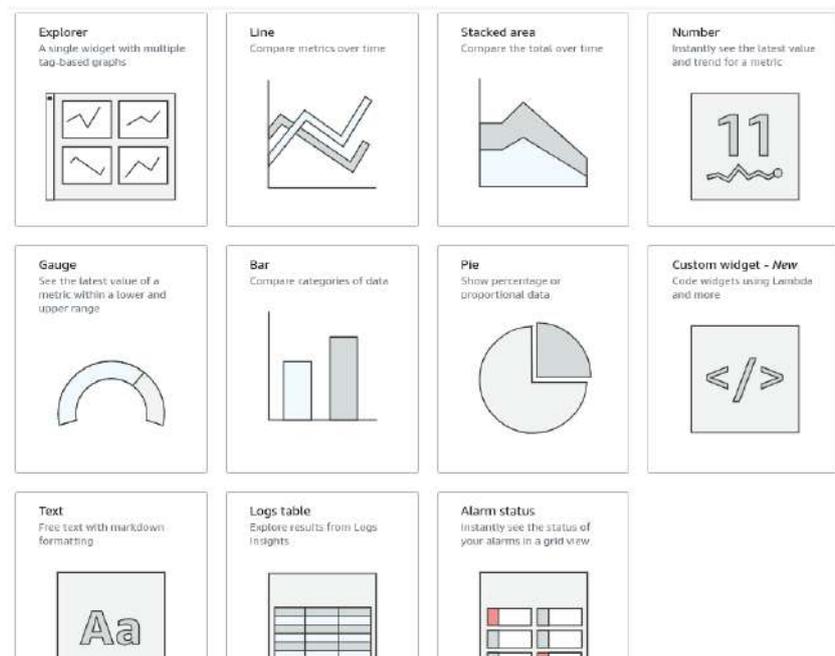
3 son gratuitos, con 50 widgets por panel. A partir del cuarto son 3 dolares mensuales, aunque solo se cree y se borre.

Los elementos que se pueden añadir en los dashboard se le llaman widgets.

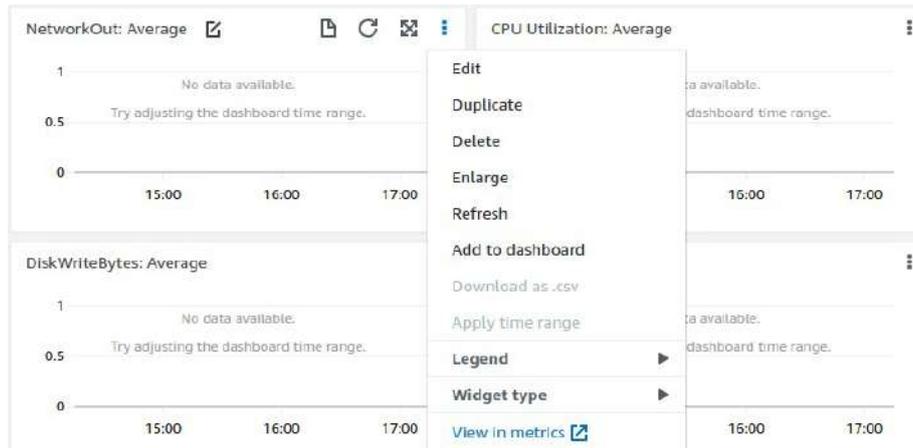
Cuando se crea uno nos pide el nombre y luego podemos añadir widgets de forma manual o de manera automática.

### 22.2.2. - Widgets y Métricas

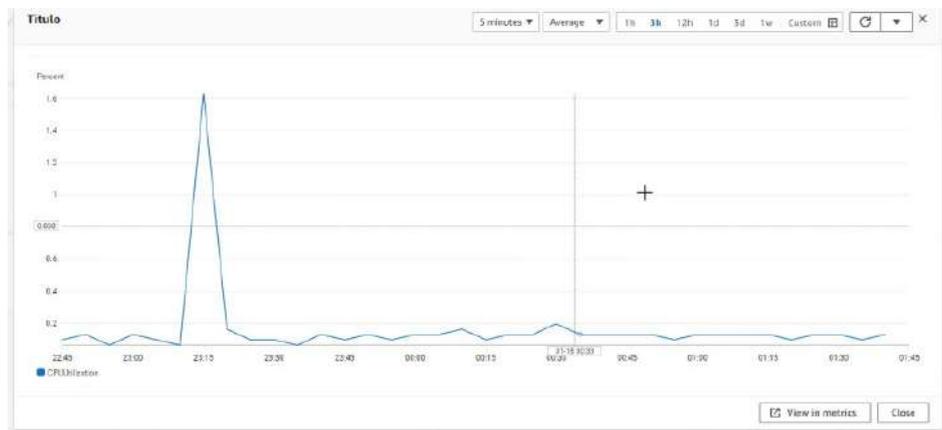
Los tipos de widgets son una forma de mostrar las métricas, podemos escoger entre distintos tipos.



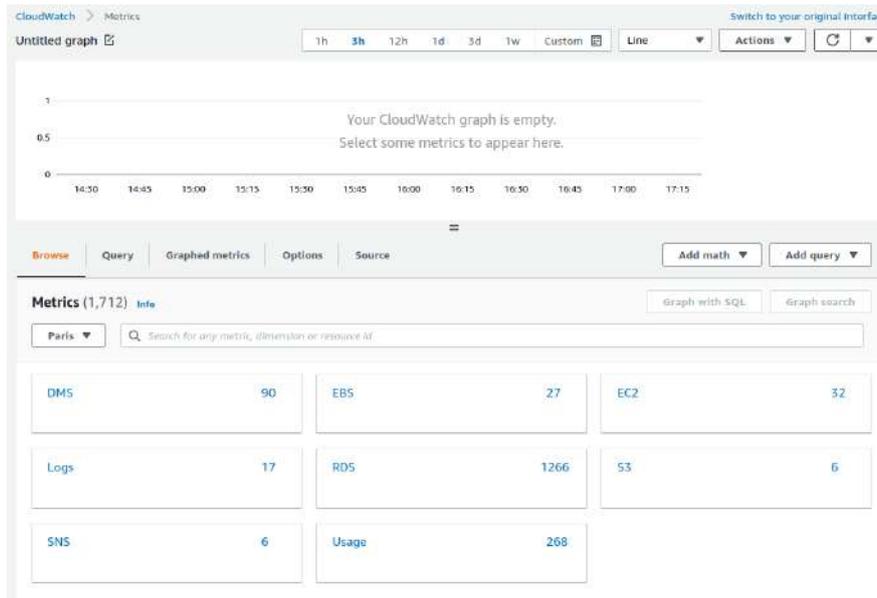
Podemos escoger la ubicación y el orden de los widgets en la consola. Tenemos opciones para cada uno de los widgets.



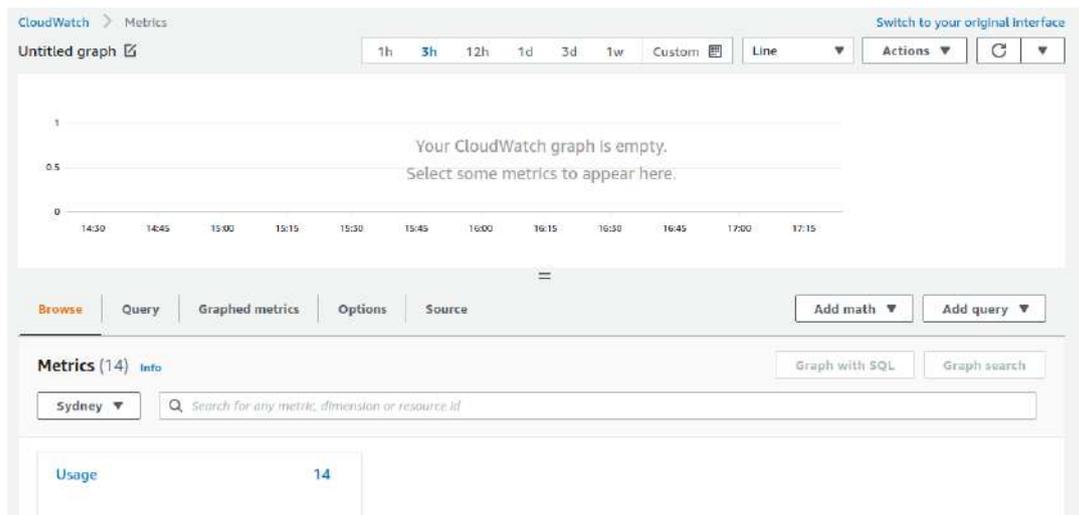
Podemos ampliarlo a pantalla completa para ver con más detalles y variar los parámetros de la gráfica.



Lo más interesante es configurar nuestras propias métricas para que sea lo más personalizado posible a nuestras necesidades. Dentro de las metrics aparecen solo las de los productos que hayamos utilizado.



Por ejemplo, si cambiamos a una region que no hayamos usado a penas aparecerá ninguna.



En este panel podemos escoger métricas para crear nuestro widget personalizado. Incluso podemos incluir las métricas de otras regiones.

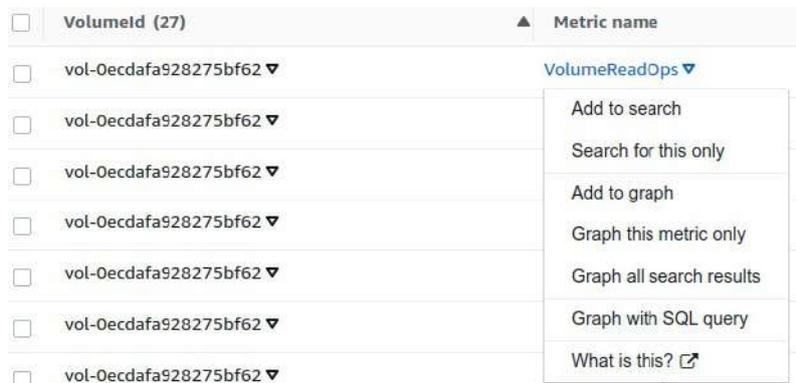
Podemos filtrar por búsquedas que pueden incluir métricas de distintas clases. Por ejemplo, si buscamos EBS nos saldrán las métricas que tengan que ver con este servicio aunque no estén dentro de la clase EBS. Podrían estar en RDS o EC2

Si añadimos varias búsquedas irá filtrando



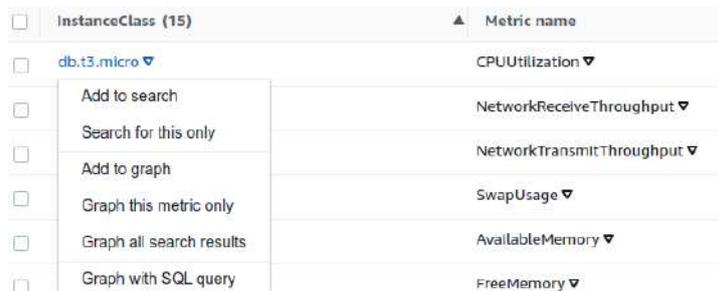
Cada métrica va a estar asociados a una ID de la clase de elemento y a un nombre de métrica.

Para entender que es cada nombre de métrica tendremos que acudir a la documentación. Podemos hacerlo directamente en el menú contextual de cada nombre. En «What is this?».



Añadir la búsqueda, buscar solo este, añadir al gráfico, gráfico de esta métrica solo, gráfico de toda la cerca del resultado, Gráfico con query SQL y What is this?.

Cada elemento también tiene una serie de opciones.



Añadir la búsqueda, buscar solo este, añadir al gráfico, gráfico de esta métrica solo, gráfico de toda la cerca del resultado y Gráfico con query SQL.

En algunos casos podemos añadir todos los elementos directamente



En un gráfico se pueden añadir varias métricas. Cuando las tenemos seleccionadas, en la pestaña «Graphed metrics», podemos cambiar el nombre de la métrica para la gráfica.



Se podrán seleccionar algunas acciones que queremos que recoja en la métrica. Por ejemplo, el color, statistic podemos seleccionar qué recoge, podemos decir el periodo, etc

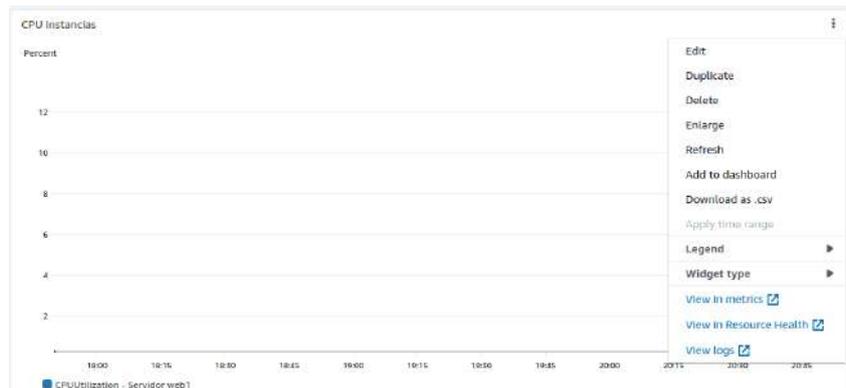
En Options podemos parametrizar algunos aspectos de cada tipo de gráfica.

En Source nos genera un fichero JSON que podría utilizar, por ejemplo, desde AWS CLI o AWS SDK.

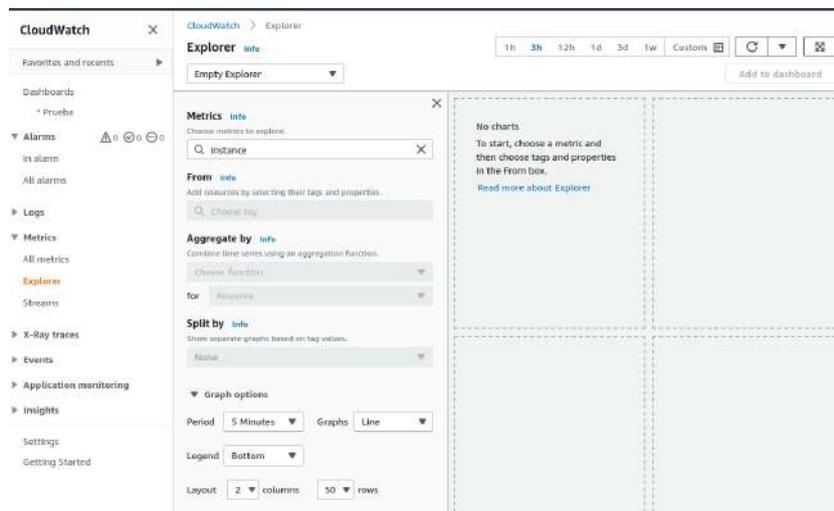
En la parte de arriba podemos cambiarle el nombre al gráfico.

En «Actions» podemos añadirlo a un dashboard, compartir o descargar en .csv.

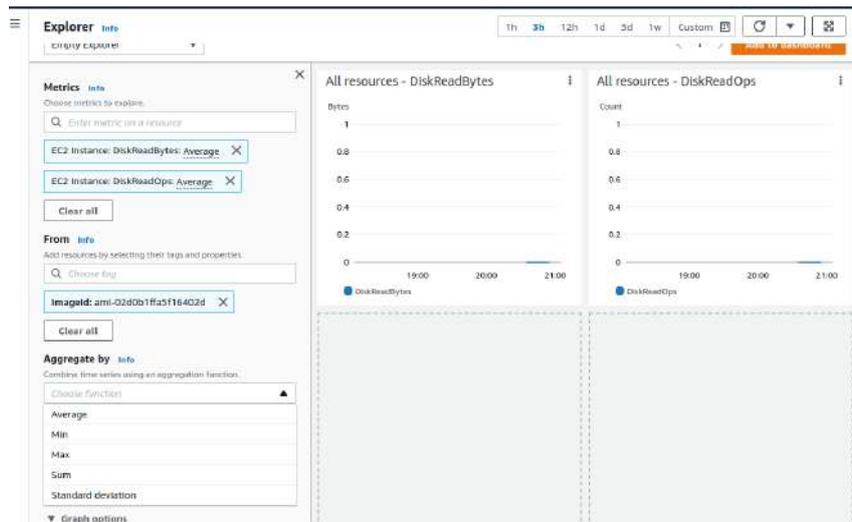
Una vez lo pasemos al dashboard tendremos también algunas acciones como editarlo, duplicarlo, borrarlo, etc



Dentro de las métricas, también tenemos el explorer. Sirve para agrupar métricas, dividir las, etc Se pueden seleccionar algunas plantillas para hacerlo rápido y en masa por servicio.



Se selecciona el tipo de métrico y desde donde recoge los datos (el recurso o tags). Tal y como vayamos parámetros va generando los gráficos. Luego se le puede indicar la agregación. Con split se pueden separar los gráficos por valores.



Por último se pueden configurar opciones y agregar al dashboard

### 22.2.3. - Agente CloudWatch

Se pueden configurar para que una instancia mande métricas especiales además de las que se mandan por defecto. Se instala dentro de la instancia y puede mandar métricas y logs (Por ejemplo, de los apache o tomcat o cualquier servicio interno de la instancia.).

En principio, se puede instalar en todas las instancias soportadas por AWS (RedHat, Suse, etc). En **cada SO tendrá un modo de instanci3n**. Documentaci3n:

[https://docs.aws.amazon.com/es\\_es/AmazonCloudWatch/latest/monitoring/install-CloudWatch-Agent-on-EC2-Instance.html](https://docs.aws.amazon.com/es_es/AmazonCloudWatch/latest/monitoring/install-CloudWatch-Agent-on-EC2-Instance.html)

En el **caso de Amazon Linux 2** es con el siguiente comando:

```
sudo yum install amazon-cloudwatch-agent
```

Ahora tendremos que parametrizar el archivo de configuraci3n del agente. Documentaci3n:

[https://docs.aws.amazon.com/es\\_es/AmazonCloudWatch/latest/monitoring/CloudWatch-Agent-Configuration-File-Details.html](https://docs.aws.amazon.com/es_es/AmazonCloudWatch/latest/monitoring/CloudWatch-Agent-Configuration-File-Details.html)

Los ficheros est3n en /opt/aws

```
[ec2-user@ip-10-0-0-29 ~]$ cd /opt/aws/
[ec2-user@ip-10-0-0-29 aws]$ ls
amazon-cloudwatch-agent  apitools  bin
[ec2-user@ip-10-0-0-29 aws]$ tree amazon-cloudwatch-agent/
amazon-cloudwatch-agent/
├── bin
│   ├── amazon-cloudwatch-agent
│   ├── amazon-cloudwatch-agent-config-wizard
│   ├── amazon-cloudwatch-agent-ctl
│   ├── config-downloader
│   ├── config-translator
│   ├── cwagent-otel-collector
│   ├── CWAGENT_VERSION
│   └── start-amazon-cloudwatch-agent
├── cwagent-otel-collector
│   ├── etc
│   │   └── cwagent-otel-collector.d
│   ├── logs
│   └── var
├── doc
│   └── amazon-cloudwatch-agent-schema.json
├── etc
│   ├── amazon-cloudwatch-agent.d
│   └── common-config.toml
├── LICENSE
├── logs
├── NOTICE
├── RELEASE_NOTES
├── THIRD-PARTY-LICENSES
└── var

11 directories, 14 files
```

En el archivo bin tenemos unos scripts por defecto para lanzar el agente, para configurarlo entre otras cosas.

```
[ec2-user@ip-10-0-0-29 amazon-cloudwatch-agent]$ ll bin/
total 207944
-rwxr-xr-x 1 root root 66556280 Jun  9 19:14 amazon-cloudwatch-agent
-rwxr-xr-x 1 root root  9261336 Jun  9 19:14 amazon-cloudwatch-agent-config-wizard
-rwxr-xr-x 1 root root   19318 Jun  9 19:14 amazon-cloudwatch-agent-ctl
-rwxr-xr-x 1 root root  8255864 Jun  9 19:14 config-downloader
-rwxr-xr-x 1 root root 18741720 Jun  9 19:14 config-translator
-rwxr-xr-x 1 root root  91570232 Jun  9 19:14 cwagent-otel-collector
-rw-r--r-- 1 root root    11 Jun  9 19:14 CWAGENT_VERSION
-rwxr-xr-x 1 root root 18508024 Jun  9 19:14 start-amazon-cloudwatch-agent
[ec2-user@ip-10-0-0-29 amazon-cloudwatch-agent]$
```

También tiene un controlador del agente que se llama amazon-cloudwatch-agent-ctl

El **fichero de configuración** para definir las características de lo que queremos enviar a CloudWatch es un JSON que se puede generar desde el script amazon-cloudwatch-agent-config-wizard

```

[ec2-user@ip-10-0-0-29 bin]$ sudo ./amazon-cloudwatch-agent-config-wizard
=====
- Welcome to the Amazon CloudWatch Agent Configuration Manager -
-
- CloudWatch Agent allows you to collect metrics and logs from -
- your host and send them to CloudWatch. Additional cloudWatch -
- charges may apply.
=====
On which OS are you planning to use the agent?
1. linux
2. windows
3. darwin
default choice: [1]:
1
Trying to fetch the default region based on ec2 metadata...
Are you using EC2 or On-Premises hosts?
1. EC2
2. On-Premises
default choice: [1]:
1
Which user are you planning to run the agent?
1. root
2. cwagent
3. others
default choice: [1]:
1
Do you want to turn on StatsD daemon?
1. yes
2. no
default choice: [1]:
1
Which port do you want StatsD daemon to listen to?
default choice: [8125]

What is the collect interval for StatsD daemon?
1. 10s
2. 30s
3. 60s
default choice: [1]:
1
What is the aggregation interval for metrics collected by StatsD daemon?
1. Do not aggregate
2. 10s
3. 30s
4. 60s
default choice: [4]:
4
Do you want to monitor metrics from CollectD? WARNING: CollectD must be installed or the Agent will fail to start
1. yes
2. no
default choice: [1]:
1
Do you want to monitor any host metrics? e.g. CPU, memory, etc.
1. yes

```

Nos hará una serie de preguntas básicas:

- Que SO estamos usando
- Donde está alojado. EC2 o On-Premises
- Que usuario será quien gestione el agente.
- Si queremos ejecutar el demonio StatsD
- Nos pregunta el puerto que utilizará el demonio.
- Cada cuanto tiempo recopila información el demonio.
- Cada cuanto tiempo agrega información el demonio.
- Luego pregunta si queremos recolectar información con el demonio CollectD, que monitoriza las métricas.
- Si se quiere monitorizar cualquier tipo de métrica
- Si quiero monitorizar por la cpu por core.
- Si queremos añadir las dimensiones EC2 (ImageId, InstanceId, InstanceType, etc). Nos permite que luego podamos configurar la métrica.
- Si queremos agregar InstanceId



Ahora ya tenemos el documento generado como config.json. En la documentación se puede ver los parámetros que podemos definir:

[https://docs.aws.amazon.com/es\\_es/AmazonCloudWatch/latest/monitoring/metrics-collected-by-CloudWatch-agent.html](https://docs.aws.amazon.com/es_es/AmazonCloudWatch/latest/monitoring/metrics-collected-by-CloudWatch-agent.html)

La **estructura de config.json** son los siguientes parámetros:

- agent - indica cada cuanto tiempo y el usuario.
- logs
- metrics
  - aggregation\_dimensions
  - append\_dimensions
  - metrics\_collected

```

GNU nano 2.9.8                                config.json
{
  "agent": {
    "metrics_collection_interval": 60,
    "run_as_user": "root"
  },
  "logs": {
    "logs_collected": {
      "files": {
        "collect_list": [
          {
            "file_path": "/var/log/httpd/*",
            "log_group_name": "mis_apaches",
            "log_stream_name": "servidorWEB",
            "retention_in_days": 1
          }
        ]
      }
    }
  },
  "metrics": {
    "aggregation_dimensions": [
      {
        "InstanceId"
      }
    ],
    "append_dimensions": {
      "AutoScalingGroupName": "${aws:AutoScalingGroupName}",
      "ImageId": "${aws:imageid}",
      "InstanceId": "${aws:InstanceId}",
      "InstanceType": "${aws:InstanceType}"
    },
    "metrics_collected": {
      "collectd": {
        "metrics_aggregation_interval": 60
      },
      "cpu": {
        "measurement": [
          "cpu_usage_idle",
          "cpu_usage_iowait",
          "cpu_usage_user",
          "cpu_usage_system"
        ],
        "metrics_collection_interval": 60,
        "resources": [
          ""
        ],
        "totalcpu": false
      },
      "disk": {
    
```

Para añadir por ejemplo la memoria libre, la memoria inactiva, la memoria total y la memoria usada, comprobamos como se llama cada componente en la documentación:

Métrica	Descripción
mem_free	La cantidad de memoria que no se está utilizando. Unidades: bytes
mem_inactive	La cantidad de memoria que no se ha utilizado de alguna manera durante el último período de muestreo. Unidades: bytes
mem_total	La cantidad total de memoria. Unidades: bytes
mem_used	La cantidad de memoria en uso actualmente. Unidades: bytes

Y lo añadimos al espacio de mem de metrics\_collected.

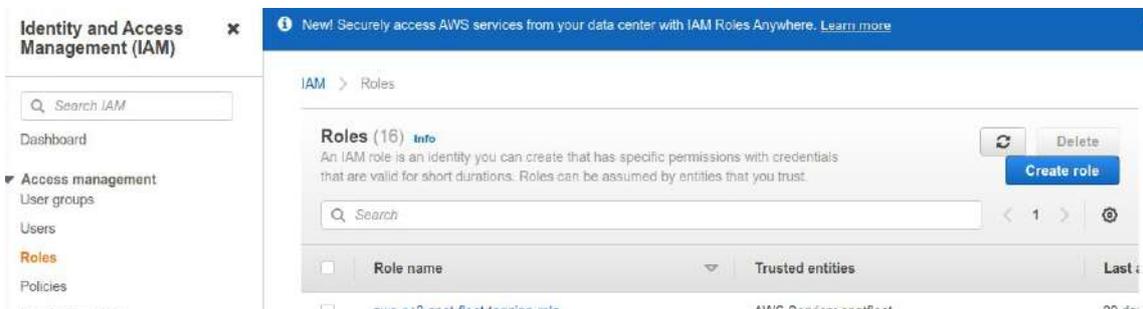
Antes:

```
"mem": {
  "measurement": [
    "mem_used_percent"
  ],
  "metrics_collection_interval": 60
},
"statsd": {
```

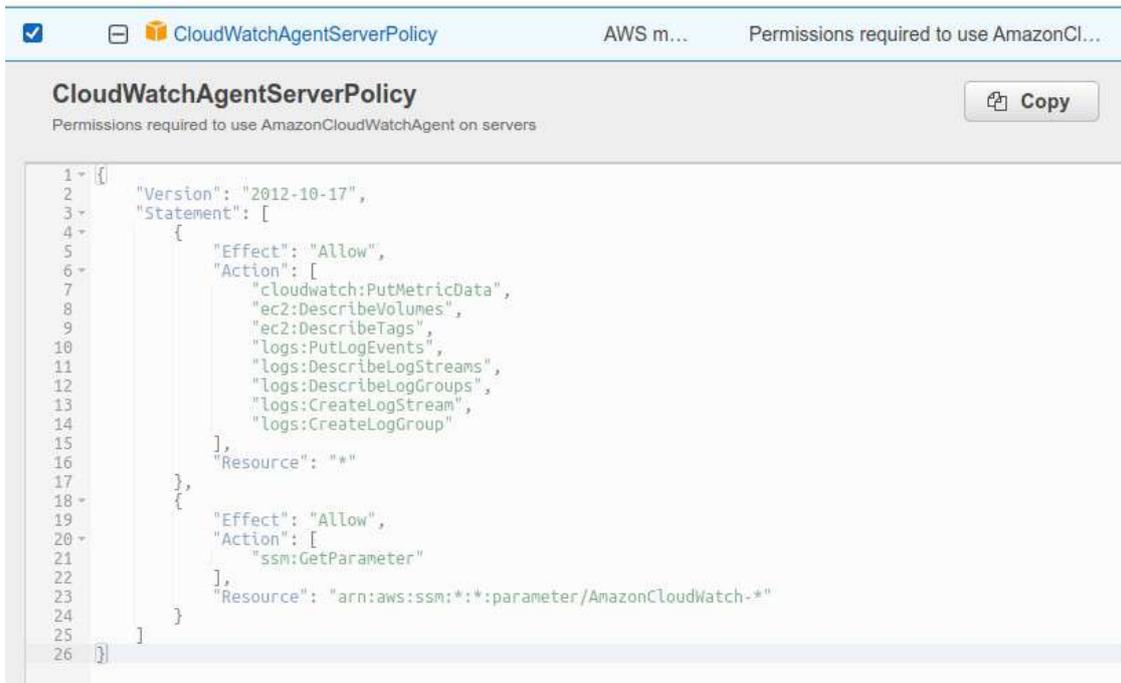
Después:

```
"mem": {
  "measurement": [
    "mem_used_percent",
    "mem_free",
    "mem_inactive",
    "mem_total",
    "mem_used"
  ],
  "metrics_collection_interval": 60
},
```

Antes de arrancar el agente **necesitamos un rol (IAM)** para darle los permisos necesarios, que son la de escribir en CloudWatch, y se lo asignaremos a la instancia. Así que buscamos el servicio IAM, el apartado roles y creamos uno nuevo. Esto será un grupo de permisos.



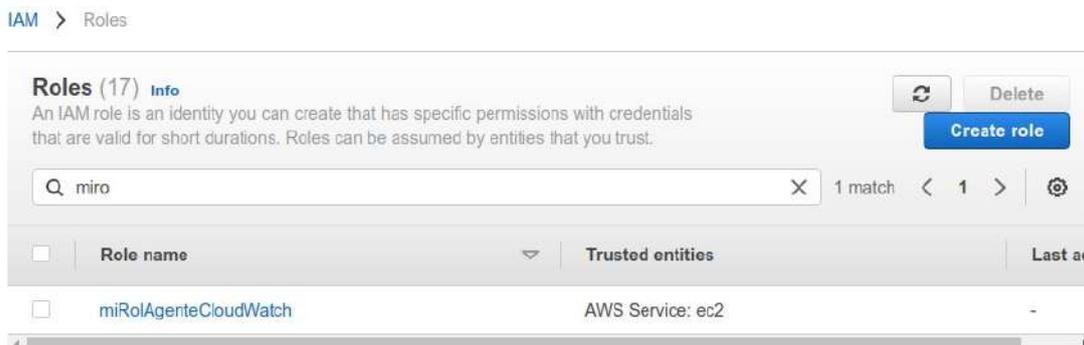
Creamos un AWS service, de tipo EC2 y le damos permisos. En este caso se llaman CloudWatchAgentServerPolicy, son políticas de permisos.



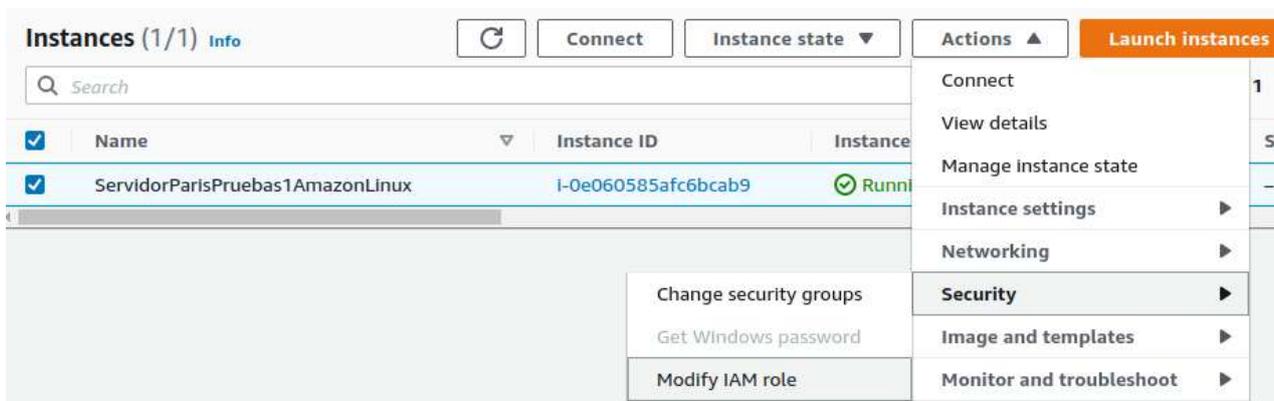
```
1- [{"  
2-   "Version": "2012-10-17",  
3-   "Statement": [  
4-     {  
5-       "Effect": "Allow",  
6-       "Action": [  
7-         "cloudwatch:PutMetricData",  
8-         "ec2:DescribeVolumes",  
9-         "ec2:DescribeTags",  
10-        "logs:PutLogEvents",  
11-        "logs:DescribeLogStreams",  
12-        "logs:DescribeLogGroups",  
13-        "logs:CreateLogStream",  
14-        "logs:CreateLogGroup"  
15-      ],  
16-      "Resource": "*"   
17-    },  
18-    {  
19-      "Effect": "Allow",  
20-      "Action": [  
21-        "ssm:GetParameter"  
22-      ],  
23-      "Resource": "arn:aws:ssm:*:*:parameter/AmazonCloudWatch-*"  
24-    }  
25-  ]  
26- }]
```

Después se le debe indicar el nombre del rol, la descripción y si queremos tags.

Una vez creado deberemos asignarle a la instancia este rol.



Entonces vamos a la instancia, la seleccionamos, botón «Actions», Security y Modify IAM role.



Seleccionamos el rol y ya lo tenemos. Lo podemos comprobar en la pestaña Security de la instancia.

Ahora tenemos que arrancar el agente. deberíamos ver en la documentación cuál es el mecanismo correcto según nuestro tipo de instancia y de SO:

<https://docs.aws.amazon.com/es-es/AmazonCloudWatch/latest/monitoring/install-CloudWatch-Agent-commandline-fleet.html> Es IMPORTANTE comprobar la documentación porque lo van cambiando.

En el caso de EC2 con Amazon Linux 2 es este:

```
sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -a fetch-config -m ec2 -s -c file:configuration-file-path
```

Lo lanza el binario controlador del agente amazon-cloudwatch-agent-ctl que tiene la siguiente sintaxis:

```
amazon-cloudwatch-agent-ctl -a
stop|start|status|fetch-config|append-config|remove-config|set-log-level
[-m ec2|onPremise|auto]
[-c default|all|ssm:<parameter-store-name>|file:<file-path>]
[-o default|all|ssm:<parameter-store-name>|file:<file-path>]
[-s]
[-l INFO|DEBUG|WARN|ERROR|OFF]
```

Nos da error

```
ip-10-0-0-29 bin]$ sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -a fetch-config -m ec2 -s
/opt/aws/amazon-cloudwatch-agent/bin/config.json
cessing amazon-cloudwatch-agent *****
amazon-cloudwatch-agent/bin/config-downloader --output-dir /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-ag
nload-source file:/opt/aws/amazon-cloudwatch-agent/bin/config.json --mode ec2 --config /opt/aws/amazon-cloudwatch-
common-config.toml --multi-config default
to detect region from ec2
22:26:45 D! [EC2] Found active network interface
ly fetched the config and saved in /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d/file_config.json.

figuration validation...
amazon-cloudwatch-agent/bin/config-translator --input /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.j
t-dir /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d --output /opt/aws/amazon-cloudwatch-agent/etc/
dwatch-agent.toml --mode ec2 --config /opt/aws/amazon-cloudwatch-agent/etc/common-config.toml --multi-config defau

22:26:45 Reading json config file path: /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d/file_config
...
22:26:45 I! Valid json input schema.
ng run as user...
to detect region from ec2
22:26:45 D! [EC2] Found active network interface
figuration found.
ion validation first phase succeeded
amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent -schematest -config /opt/aws/amazon-cloudwatch-agent/etc/amazon-
-agent.toml
ion validation second phase failed
rror Log =====
22:26:45Z E! [telegraf] Error running agent: Error parsing /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-
, open /usr/share/collectd/types.db: no such file or directory
ip-10-0-0-29 bin]$
```

No puede abrir /usr/share/collectd/types.db, que significa que no tiene el recolector CollectD, así que lo instalamos.

```
sudo yum install -y collectd
```

Si no funciona podemos utilizar el gestor de paquetes amazon-linux-extras.

Lanzamos de nuevo el arranque del agente, esta vez con éxito:

```

[ec2-user@ip-10-0-0-29 bin]$ sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -a fetch-config -m ec2 -s -c file:/opt/aws/amazon-cloudwatch-agent/bin/config.json
***** processing amazon-cloudwatch-agent *****
/opt/aws/amazon-cloudwatch-agent/bin/config-downloader --output-dir /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d --download-source file:/opt/aws/amazon-cloudwatch-agent/bin/config.json --mode ec2 --config /opt/aws/amazon-cloudwatch-agent/etc/common-config.toml --multi-config default
I! Trying to detect region from ec2
2022/09/11 22:31:27 D! [EC2] Found active network interface
Successfully fetched the config and saved in /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d/file_config.json.tmp
Start configuration validation...
/opt/aws/amazon-cloudwatch-agent/bin/config-translator --input /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.json --input-dir /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d --output /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.toml --mode ec2 --config /opt/aws/amazon-cloudwatch-agent/etc/common-config.toml --multi-config default
2022/09/11 22:31:27 Reading json config file path: /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d/file_config.json.tmp ...
2022/09/11 22:31:27 I! Valid json input schema.
I! Detecting run_as_user...
I! Trying to detect region from ec2
2022/09/11 22:31:27 D! [EC2] Found active network interface
No csm configuration found.
Configuration validation first phase succeeded
/opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent -schematest -config /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.toml
Configuration validation second phase succeeded
Configuration validation succeeded
amazon-cloudwatch-agent has already been stopped
Created symlink from /etc/systemd/system/multi-user.target.wants/amazon-cloudwatch-agent.service to /etc/systemd/system/amazon-cloudwatch-agent.service.
Redirecting to /bin/systemctl restart amazon-cloudwatch-agent.service
    
```

Si comprobamos el estado del demonio nos dice que está activo.

```

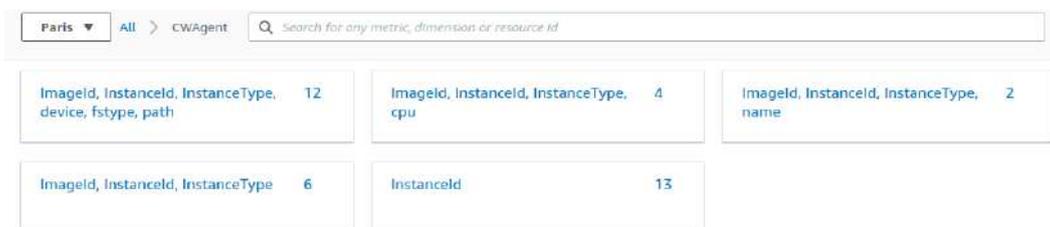
[ec2-user@ip-10-0-0-29 bin]$ systemctl status amazon-cloudwatch-agent.service
● amazon-cloudwatch-agent.service - Amazon CloudWatch Agent
   Loaded: loaded (/etc/systemd/system/amazon-cloudwatch-agent.service; enabled; vendor preset: disabled)
   Active: active (running) since Sun 2022-09-11 22:31:28 UTC; 1min 51s ago
   Main PID: 8255 (amazon-cloudwat)
   CGroup: /system.slice/amazon-cloudwatch-agent.service
           └─8255 /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent -config /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwat...

Sep 11 22:31:28 ip-10-0-0-29.eu-west-3.compute.internal systemd[1]: Started Amazon CloudWatch Agent.
Sep 11 22:31:28 ip-10-0-0-29.eu-west-3.compute.internal start-amazon-cloudwatch-agent[8255]: /opt/aws/amazon-cloudwatch-agent/etc/amazon-...t.
Sep 11 22:31:28 ip-10-0-0-29.eu-west-3.compute.internal start-amazon-cloudwatch-agent[8255]: I! Detecting run_as_user...
Hint: Some lines were ellipsized, use -l to show in full.
    
```

Ahora, si nos vamos a métricas de CloudWatch veremos un nuevo elemento, el CWAgent



Y dentro tendremos las métricas configuradas.



Por ejemplo podremos seleccionar los parámetros de memoria añadidos:



Además, en Log Groups que veremos luego, también guarda un fichero de logs de apache.

CloudWatch > Log groups > mis\_apaches > servidorWEB

### Log events

You can use the filter bar below to search for and match terms, phrases, or values in your log events. [Learn more about filter patterns](#)

View as text

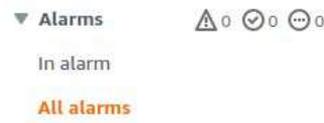
1m 30m 1h 12h Custom

▶	Timestamp	Message
		There are older events to load. <a href="#">Load more.</a>
▶	2022-09-12T17:45:49.751+02:00	83.54.93.176 - - [12/Sep/2022:15:45:48 +0000] "GET / HTTP/1.1" 200 10145 "-" "Moz...
▶	2022-09-12T17:45:49.751+02:00	83.54.93.176 - - [12/Sep/2022:15:45:48 +0000] "GET /default.css HTTP/1.1" 200 557...
▶	2022-09-12T17:45:49.751+02:00	83.54.93.176 - - [12/Sep/2022:15:45:48 +0000] "GET /img/star2.jpg HTTP/1.1" 200 7...

## TEMA 23 - CloudWatch Alarmas

En “**All alarms**” tenemos todas las alarmas configuradas.

En “**In alarms**” tenemos las alarmas que se han disparado.



Los símbolos, de izquierda a derecha:

- **Alarmas activas**
- **Alarmas ok**
- **Alarmas sin datos suficientes.** Suele ser provocado por estar recién creada o no tiene suficientes DataPoint para saber si está correcta.

Los **tres estados** de las alarmas son “que ha saltado”, “que está ok” o “sin datos suficientes”.

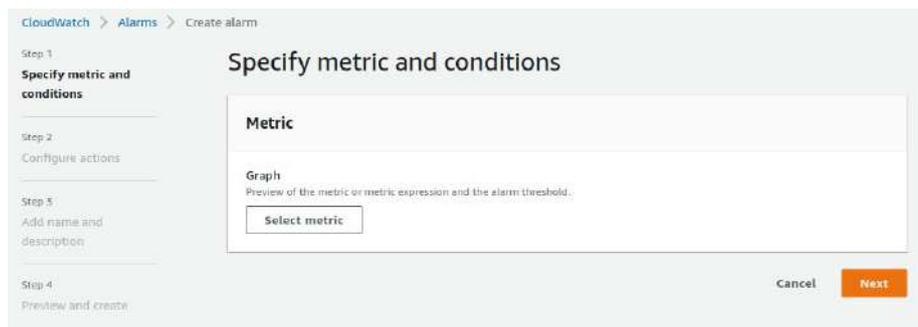
Los **tipos de alarmas** son “compuestas” o “alarmas métricas”.

Y las **acciones** que pueden hacer son “Habilitarlas”, “deshabilitarlas” o “sin acciones”.

Las alarmas se pueden basar en métricas y en condiciones. En base a esto se le indica las acciones.

### 23.1. - Crear una alarma

Se crea en 4 pasos.



Como ejemplo vamos a crear una alarma de CPU que se conecte al SNS y envíe un correo.

Primero seleccionamos la métrica. Es como el panel de metrics.

Ahora decidimos las condiciones con un valor estático o con una función de anomalía (un rango de comportamiento).

**Conditions**

Threshold type

**Static**  
Use a value as a threshold

**Anomaly detection**  
Use a band as a threshold

Whenever CPUUtilization is...  
Define the alarm condition.

**Greater**  
> threshold

**Greater/Equal**  
>= threshold

**Lower/Equal**  
<= threshold

**Lower**  
< threshold

than...  
Define the threshold value.

10000

Must be a number

**Conditions**

Threshold type

**Static**  
Use a value as a threshold

**Anomaly detection**  
Use a band as a threshold

Whenever CPUUtilization is...  
Define the alarm condition

**Outside of the band**  
> or < threshold

**Greater than the band**  
> threshold

**Lower than the band**  
< threshold

Anomaly detection threshold  
Based on a standard deviation. Higher number means thicker band, lower number means thinner band.

2

Must be a positive number

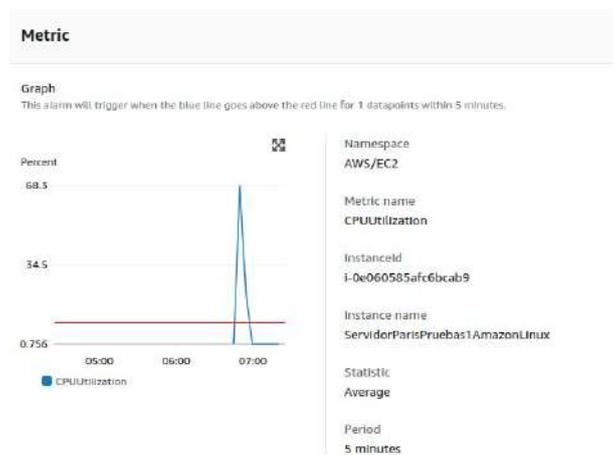
En las opciones adicionales podemos decidir que hacemos con la perdida de datos. Si se dan por perdidos, si se dan por datos correctos o si es algo malo que no haya datos.

- ▼ **Additional configuration**
- Treat missing data as missing
  - Treat missing data as good (not breaching threshold)
  - Treat missing data as ignore (maintain the alarm state)
  - Treat missing data as bad (breaching threshold)

Una vez tenemos la métrica y las condiciones ya podemos escoger la acción entre:

- Enviar una notificación. Se puede enviar una notificación si se dispara una alarma, si la alarma se quita y paso ok, o si no hay datos suficientes. Se selecciona o se crea el topic. Se puede enviar más de una notificación, se pueden añadir.
- Una acción de auto escalada – Se selecciona un grupo de autoescalada y se especifica la tarea.
- Una acción EC2 – Podemos hacer un recover (las instancias pequeñas no lo soportan), parar la instancia, Terminarla o reiniciarla.
- Una acción System Manager.

Una vez configurada la acción aparece un preview antes de crear.



Podemos revisar y volver a editar algún aspecto. Si todo es correcto se crea y podemos ver los detalles, las acciones, el histórico y alarmas parentales.

En este caso, después de estresar el CPU (stress -c 10 -t 600s) en el histórico vemos que se ha intentado la notificación pero SNS no tiene los suficientes permisos para enviar el correo

Date	Type	Description
2022-09-12 07:44:20	Configuration update	Alarm "CPU ServidorWEB" updated
2022-09-12 07:41:15	Action	Failed to execute action arn:aws:sns:eu-west-3:992365247711:Base-de-datos. Received error: "CloudWatch Alarms is not authorized to perform: SNS:Publish on resource:arn:aws:sns:eu-west-3:992365247711:Base-de-datos"
2022-09-12 07:41:15	State update	Alarm updated from <b>In alarm</b> to <b>OK</b> .
2022-09-12 07:36:15	Action	Failed to execute action arn:aws:sns:eu-west-3:992365247711:Base-de-datos. Received error: "CloudWatch Alarms is not authorized to perform: SNS:Publish on resource:arn:aws:sns:eu-west-3:992365247711:Base-de-datos"
2022-09-12 07:36:15	State update	Alarm updated from <b>OK</b> to <b>In alarm</b> .
2022-09-12 07:31:15	Action	Failed to execute action arn:aws:sns:eu-west-3:992365247711:Base-de-datos. Received error: "CloudWatch Alarms is not authorized to perform: SNS:Publish on resource:arn:aws:sns:eu-west-3:992365247711:Base-de-datos"
2022-09-12 07:31:15	State update	Alarm updated from <b>Insufficient data</b> to <b>OK</b> .
2022-09-12 07:29:44	Configuration update	Alarm "CPU ServidorWEB" created

Creamos la política de permisos en el topic.

```

{
  "Version": "2012-10-17",
  "Id": "example-ID",
  "Statement": [
    {
      "Sid": "Eventos de S3",
      "Effect": "Allow",
      "Principal": {
        "Service": "s3.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:us-west-2:264297788131:Base-de-Datos",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "264297788131"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:s3:::bucket1-apasoft"
        }
      }
    },
    {
      "Sid": "Cloudwatch",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudwatch.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:us-west-2:264297788131:Base-de-Datos",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:cloudwatch:us-west-2:264297788131:alarm:Cpu Servidor2"
        }
      }
    }
  ]
}

```



## TEMA 24 - CloudWatch Logs

CloudWatch Logs es el entorno que almacena archivos de logs.

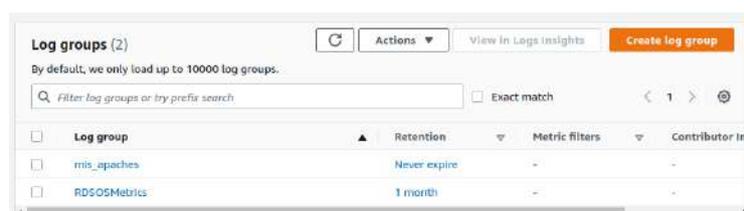
- Permite monitorizar, almacenar y acceder a los archivos de log generados por instancias de Amazon Elastic Compute Cloud (Amazon EC2), AWS CloudTrail, Route 53 y otras fuentes y servicios de AWS. Algunos entornos son automáticos y otros necesitan un agente que envíe los logs.
- Permite centralizar los logs de todos los sistemas, aplicaciones y servicios de AWS en un único punto central y de gran escalabilidad.
- Se puede buscar a través de patrones específicos, filtrarlos en función de campos específicos o archivarlos de forma segura para futuros análisis. CloudWatch inside.
- Se pueden implementar como un flujo único y consistente de eventos ordenados por tiempo.
- Se pueden consultar y ordenarlos según múltiples dimensiones, agruparlo por campos específicos, crear cálculos personalizados y visualizar datos en DashBoards y paneles personalizables.

Conceptos:

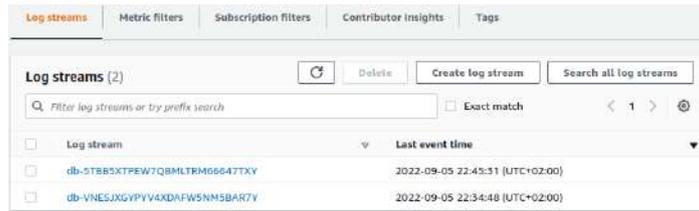
- **Log Events:** Son los eventos registrados en logs. Es un registro de alguna actividad que ha guardado una aplicación o el recurso que se está monitorizando. Contiene dos propiedades:
  - **Timestamp:** Cuando se produjo el evento.
  - **Mensaje** del evento sin procesar. Son otras herramientas las que procesan el mensaje.
- **Log Stream:** Es una secuencia de log events que comparten el mismo origen. Representar la secuencia de eventos procedente de una aplicación o recurso.
- **Log Groups:** Un grupo de Log Stream que comparten las mismas características. Cada Log Stream pertenece a un Log Group.
- **Metric Files:** Permiten extraer observaciones y datos.

En el panel de CloudWatch tenemos dos pestañas de Logs: Log Groups y Logs Insights.

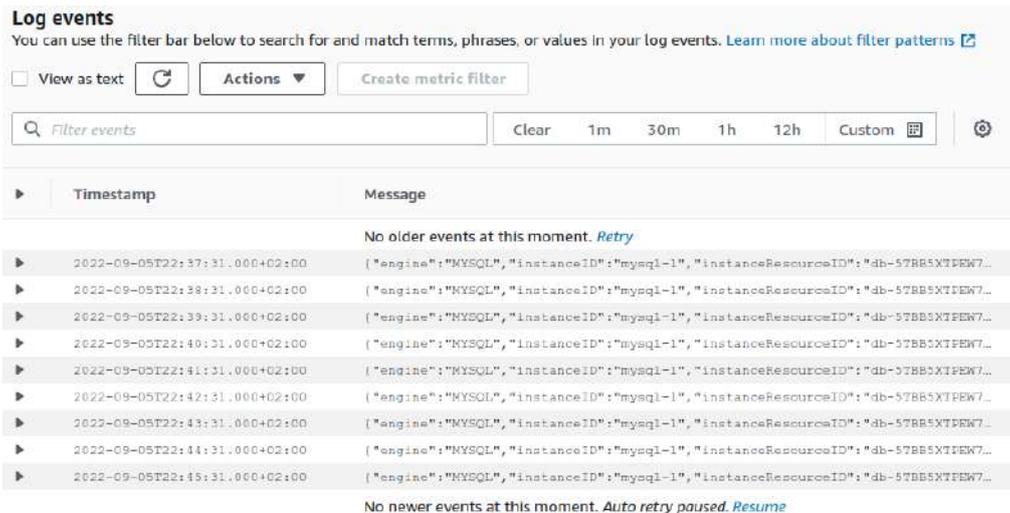
- **Log Groups** – Donde quedan los grupos configurados.



- Dentro está compuesto de **Logs Stream**



- Y dentro de cada log stream hay una serie de **eventos de logs**.

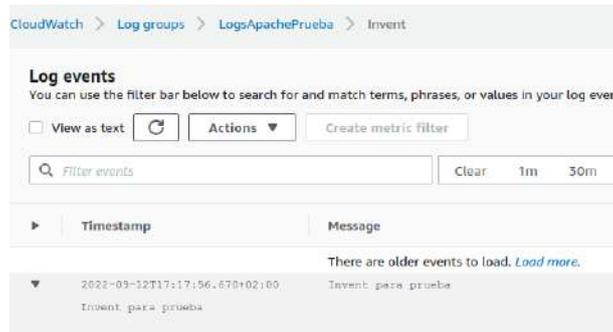


Cada **event log** es un **fichero sin procesar** con detalles del evento. En este caso un JSON.

```
2022-09-05T22:37:31.000+02:00 [{"engine": "MYSQL", "instanceID": "mysql-1", "instanceResourceID": "db-57BBSXTPEW7..."}]
{
  "engine": "MYSQL",
  "instanceID": "mysql-1",
  "instanceResourceID": "db-57BBSXTPEW7QBMLTRM66647TXV",
  "timestamp": "2022-09-05T22:37:31.000",
  "version": 1,
  "uptime": "00:02:25",
  "memUsed": 3,
  "cpuUtilization": {
    "user": 0,
    "sys": 0,
    "system": 0.3,
    "wait": 7.0,
    "idle": 92.4,
    "total": 26.7,
    "total": 41.4,
    "total": 2.2,
    "time": 0.5
  },
  "loadAverageMinute": {
    "one": 1.22,
    "five": 0.87,
    "fifteen": 0.26
  },
  "memory": {
    "writeback": 0,
    "suppPageFree": 0,
    "suppPageRead": 0,
    "suppPageReq": 0,
    "cached": 218028,
    "suppPageWrite": 2049,
    "free": 114520,
    "suppPageTotal": 0,
    "inactive": 319706,
    "pageTable": 1244,
    "dirty": 1186,
    "mapped": 66602,
    "active": 403228,
    "total": 779132,
    "slab": 42368,
    "buffers": 12868
  },
  "locks": {
    "locking": 101,

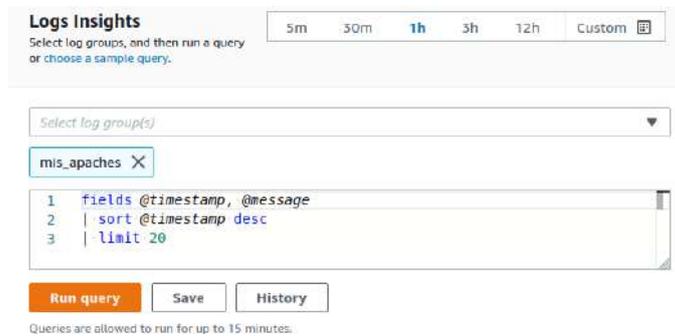
```

Se puede crear un log group. Nos pedirá el nombre, cuanto tiempo se retienen los logs y el KMS key ARN (Si estuviera encriptado). Además también se puede etiquetar. Dentro de log group se puede crear un log stream y dentro crear un log event.

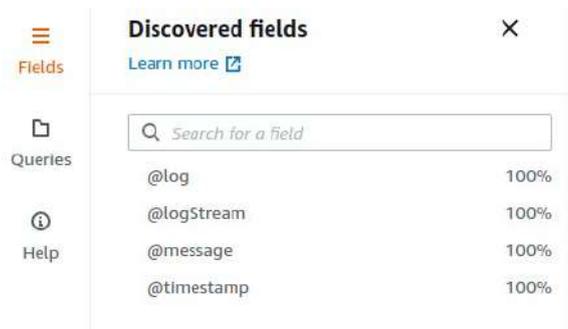


- Logs Insights – Para efectuar búsquedas dentro de los grupos de logs. Se pueden buscar patrones, filtrar filas, información concreta, etc

Tenemos que seleccionar la query en fielfs, decir el orden en sort y el limite.



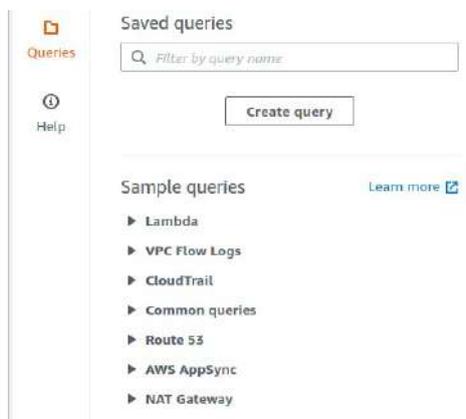
En el sidebar derecho hay facilidades para buscar. Por ejemplo, los fields (Campos de las columnas)



Cuando aplicamos con run query aparecen los datos de la búsqueda



En las queries del sidebar derecho tenemos ejemplos de búsqueda y las búsquedas que guardamos.



Ejemplo. **Generar Logs desde RDS.** Cuando creamos una BBDD, por una parte, desde monitoring podemos configurar eventos que se envían a CloudWatch

**Monitoring**

**Performance Insights** [Info](#)

Turn on Performance Insights [Info](#)

Retention period [Info](#)

7 days (free tier) ▼

AWS KMS key [Info](#)

(default) aws/rds ▼

Account  
992365247711

KMS key ID  
6dc023fb-4283-4775-a277-a92ece554f56

**⚠ You can't change the KMS key after enabling Performance Insights.**

▼ **Additional configuration**

Enhanced Monitoring

**Monitoring**

Enable Enhanced monitoring  
Enabling Enhanced monitoring metrics are useful when you want to see how different processes or threads use the CPU.

Granularity

60 seconds ▼

Monitoring Role

default ▼

Clicking "Create database" will authorize RDS to create the IAM role rds-monitoring-role

Además, en opciones avanzadas podemos indicar los logs concretos que queremos que se envíen.

**Log exports**

Select the log types to publish to Amazon CloudWatch Logs

- Audit log
- Error log
- General log
- Slow query log

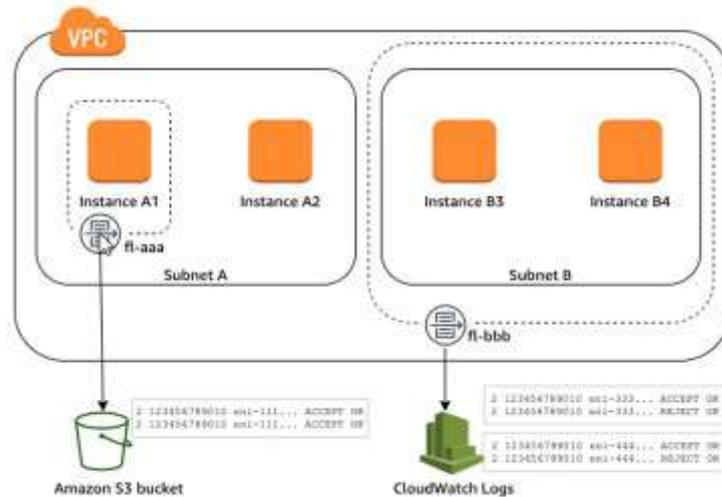
Los logs de error siempre se mandan, pero los otros tres (Audit, General y Slow Query) no se mandarían por si solos. Debemos configurar los parámetros con un parameter group que lo indique:

general\_log 1 ▼

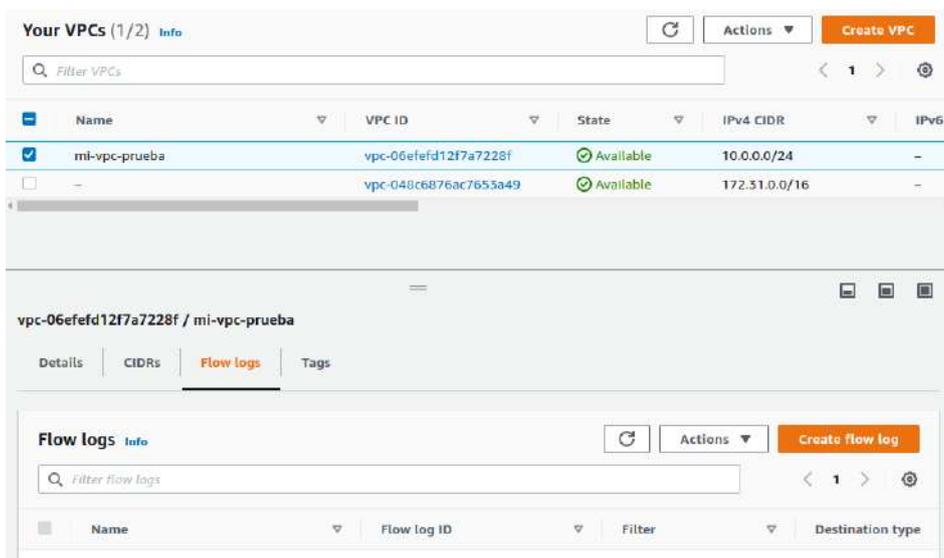
slow\_query\_log 1 ▼

Ahora, en la BBDD creada con el parameter group configurado y los logs activado, podemos ver los logs. Y en CloudWatch, en el grupo de logs “RDSOSMetrics” aparecerán los logs de SO de esta BBDD (CPU, RAM, etc) por tener activada la monitorización detallada.

Se puede capturar el tráfico de las VPC, de las subnet e incluso a nivel instancia con **VPC Flow Logs**.



Para crear un Flow log debemos estar en las VPCs y tiene una pestaña Flow Logs.

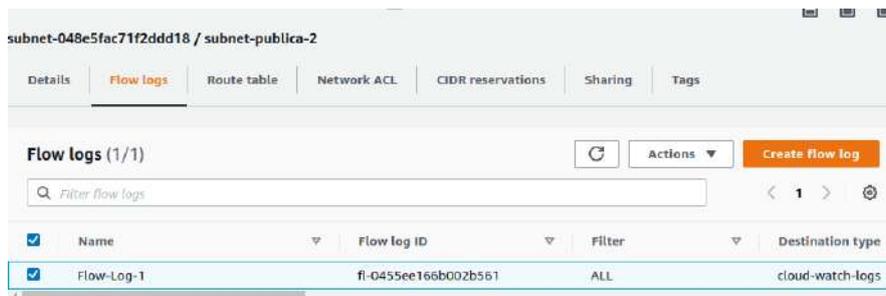


Podremos configurar algunos parámetros:

- Nombre
- Filtros. Accept, Reject o All
- Intervalo de las agregaciones
- Complimentando algunos datos lo podemos mandar a
  - CloudWatch Log – Tendremos que escoger un Log Group y un IAM role
  - Amazon S3 Bucket

- Kinesis Firehose con la misma cuenta o con otra cuenta. (Es un servicio de transmisiones generadas en tiempo real para el análisis de datos.)
- Podemos escoger el formato en el que queremos la grabación de logs. Puede ser por defecto o personalizada escogiendo los datos.

En una subnet también podemos crear un flowlog. Ahora que hemos creado un flow log a nivel de VPC las subnets han heredado este flowlog

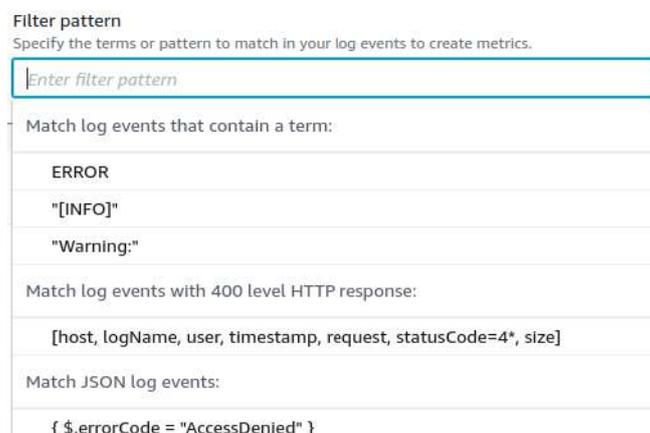


En las Network interfaces (Tarjetas de red) de EC2 también podemos crear un Flow Log. Como pasa con las subnets, al tener la VPC un flow log las tarjetas de red lo heredan.



Con lo cual, las instancias también lo heredan.

Las **metric Filters** son filtros para limitar el resultado que queremos extraer. Se hace a través de patrones de filtros.





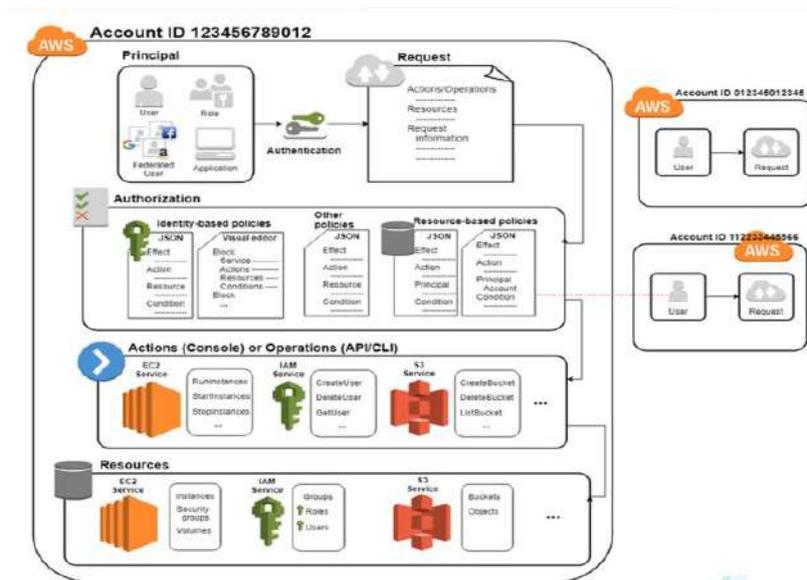
# TEMA 25 - IAM Identify Access Management. Gestión de identidades en AWS

Se debe dejar de trabajar con el usuario root inicial.



IAM permite definir el acceso a los recursos de AWS.

- **Recurso IAM:** Usuarios, grupos, roles, políticas, providers.
- **Identities:** Identifican accesos(Usuarios, grupos y roles)
- **Entities:** Objetos que usan para autenticarse (Usuarios y roles)
- **Principal:** Persona o aplicación que asume un usuario o rol. (User, role, Federated User, application)



Lo primero que tenemos que hacer es **autenticarnos** para tener la **autorización** (permisos). Podemos tener políticas (permisos) basadas en identidad (usuarios) o basadas en recursos o en tags u otras. Luego tenemos **acciones** que se pueden efectuar en los recurso que queremos acceder.

Principal - Podemos entrar de tres formas: Usuario ROOT, Usuario IAM y AWS ROLE.

## Usuario ROOT

- Usuario principal con el que se crea la cuenta al que se le denomina “root user”. Es similar al usuario root de Linux.
- Se puede usar para acceder por consola o a través de código.

- Puede hacer cualquier tipo de operación.
- No se debería usar para las tareas diarias

### Usuario IAM

- Es el usuario que se debe usar en el día a día.
- Representan usuario o aplicaciones que se conectarán y usarán los recursos de AWS
- Pueden acceder desde la consola o desde un entorno CLI o SDK
- Se les puede asignar distintos tipo de permisos para su trabajo diario.

### Grupos

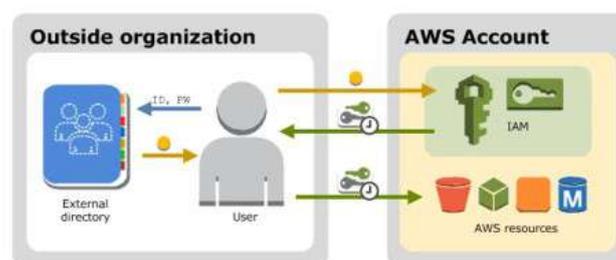
- Colección de usuario IAM que permite agrupar permisos para asignarlos a los usuarios.

### AWS ROLE

- Se usan para dar permisos y privilegios durante un momento determinado.
- Cuando un determinado actor asume un rol, se le asigna un token temporal que le permite acceder a un determinado recurso para poder utilizarlo.
- Es similar a un usuario IAM pero en vez de estar asociado a una persona, es asumido por quien lo necesite para unas gestiones concretas.
- No tiene credenciales ni claves u por tanto no tienen que ser enviadas o integradas dentro de una aplicación
- El servicio que asigna estos Tokens se denomina “AWS Security Token Service”

### Federación

- Se pueden “federar” usuarios ya creados dentro de nuestro propio entorno.
- De esta forma se puede asumir unas credenciales temporales para el acceso a AWS.



### Políticas y permisos

- Para gestionar el acceso a un usuario o rol a AWS se crean políticas para asignarles.
- Es un objeto AWS que al ser asignado a un usuario o recurso define sus permisos. Por lo tanto, identifican que se puede o no se puede hacer.
- Suelen estar hechas con un fichero JSON.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "dynamodb:*",
    "Resource": "arn:aws:dynamodb:us-east-2:123456789012:table/Books"
  }
}
```

## Tipos de políticas

- **identity policy** – Se asocian a una entidad IAM, como usuarios, grupos o roles. Permite controlar las acciones que se pueden realizar en un recurso y bajo que condiciones. Pueden ser:
  - **Manager** – Políticas independientes que pueden ser asignadas a multiples usuarios, grupos o roles. Pueden ser creadas por AWS o personalizadas por nosotros. Es lo habitual.
  - **Inline** – Se integran en un usuario, grupo o rol. Son las menos adecuadas.
- **Resource-Based Policies** – Se asocian a un determinado recurso AWS (por ejemplo S3) y determinan las acciones que se pueden hacer sobre ese recurso.
- Otras políticas: como las de tags.

## 25.1. - Consola IAM

The screenshot shows the AWS IAM console dashboard. On the left is a navigation menu with sections like 'Access management', 'Access reports', and 'IAM resources'. The main content area is titled 'IAM dashboard' and features a 'Security recommendations' section with two alerts: 'Add MFA for root user' and 'Deactivate or delete access keys for root user'. Below this is an 'IAM resources' summary table:

User groups	Users	Roles	Policies	Identity providers
0	0	18	1	0

At the bottom, there is a 'What's new' section with updates for IAM features. On the right side, there are sections for 'AWS Account' (showing Account ID and Alias) and 'Quick Links' (including 'My security credentials' and 'Tools').

Solo abrirla aparecen dos avisos:

- Añadir el MFA para el usuario root
- Desactivar o eliminar access keys para usuario root. Las hemos utilizado para CLI pero no se deberían usar.

Lo ideal es que root solo se pueda conectar por consola.

A la derecha tenemos:

- Account ID que es única, la comparten root y todos los usuarios que se creen.
- Account Alias. Es único para cada usuarios que se cree.
- URL de acceso para los usuarios IAM
- Más herramientas. Seguridad, simulador de políticas, federación de identidades...

En la izquierda tenemos a los grupos de usuarios, usuarios, roles, políticas, proveedores de identidad y opciones.

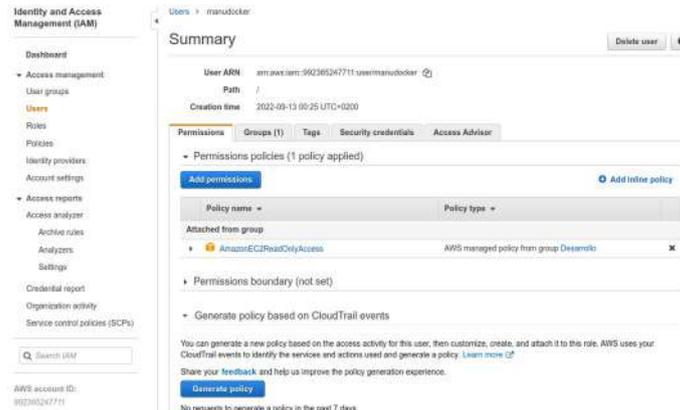
Para **crear un grupo de usuarios** podemos configurar los siguientes parámetros:

- Nombre
- Se pueden añadir usuarios y otros grupos.
- Indicar los permisos (Políticas) del grupo.

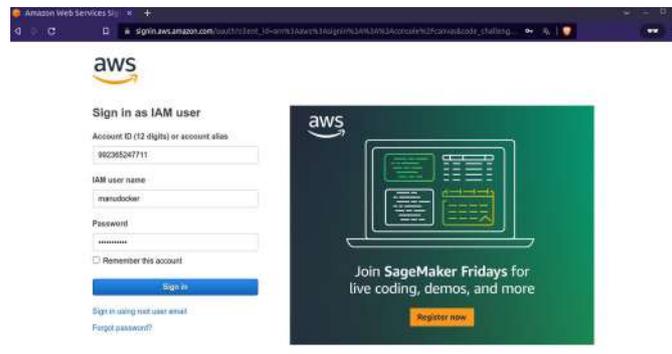
Para **crear un usuario** podemos configurar los siguientes parámetros:

- Nombre/s. Se puede añadir hasta 10 usuarios para crearlos de una vez.
- El tipo de acceso
  - A través de código AWS API, CLI, SDK... Herramientas de desarrollo
  - Con el management Console Access.
    - Pregunta contraseña y si la primera vez que se entra se debe cambiar.
- Políticas de permisos.
  - Añadir a un grupo
  - Copiar permisos de otro usuario
  - Asignar políticas
- Tags
- Muestra resumen y después la posible descarga de un CSV para enviar el usuario y contraseña.

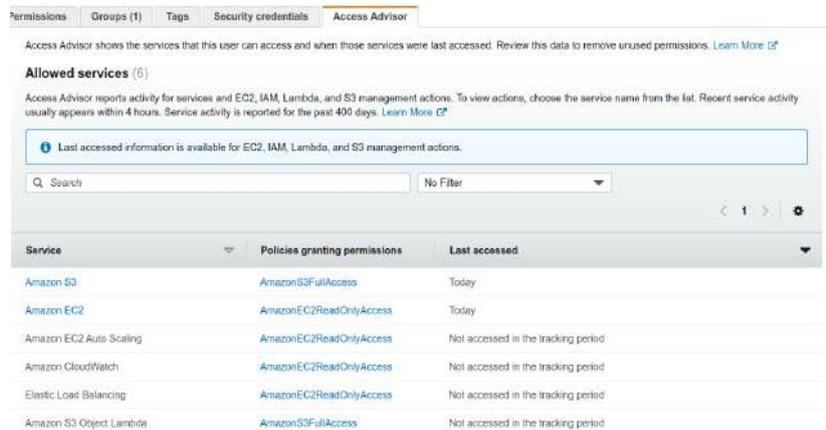
Se puede entrar en el usuario y en el grupo para poder visualizar las opciones, modificar y borrar.



Para acceder tendremos que entrar por la URL con la ID account



**Access Advisor** es una herramienta para poder comprobar que clases de políticas tiene un grupo o un usuario.



Para **crear un rol** (Un grupo de permisos) podemos configurar los siguientes parámetros:

- Tipo de entidad de confianza
  - Servicios AWS
    - Caso de uso
      - EC2

- Lambda
- Otro servicio
- Cuentas AWS
- Identidad web – AWS Cognito. Para crear usuarios para aplicaciones externas.
- federación SAML 2.0
- Políticas de confianza personalizadas.
- En los permisos podemos filtrar los que queremos. Clicando en el buscador tenemos más filtros.
- Nombre y descripción
- Aparece el json de las políticas seleccionadas y un resumen de las que son.
- Tags

### Políticas de seguridad –

- **Identity** – que se asocian a un usuario, un rol o un grupo.
  - **Manager** – Políticas independientes que pueden ser asignadas a multiples usuarios, grupos o roles. Pueden ser creadas por AWS o personalizadas por nosotros. Es lo habitual.
  - **Inline** – Se integran en un usuario, grupo o rol. Son las menos adecuadas.
- **Resource** – que se asocian a un recurso.

Todas comparten el mismo **fichero JSON**. Esqueleto, empezando por los parámetros Identity y Resource:

- **Versión** – En estos momentos es 2012-10-17
- **Statement** – Nombre del grupo completo de parámetros.
- **SID** – Código / id de la política
- **Effect** – Permitir o denegar acceso. Puede ser Allow o Deny
- **Action** – Acciones que se quieren denegar o permitir
- **Resource** – El recurso donde se aplica el permisos
- **Condition** – Condiciones para restringir o limitar el acceso.

Ahora, este parámetro tan solo se añade a políticas de recursos (Resources)

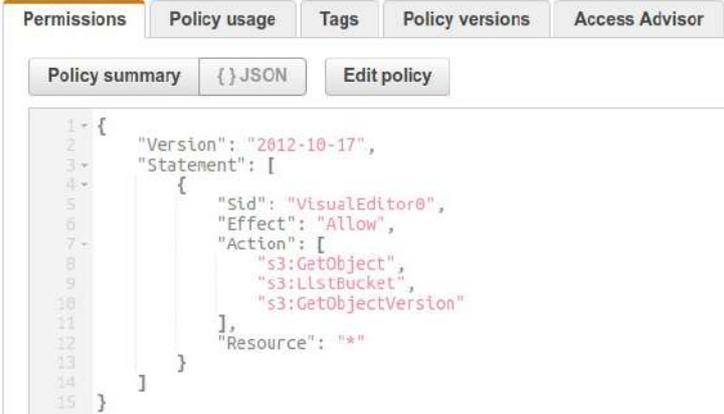
- **Principal** – Usuario, rol o cuenta para el que debería aplicarse la política.

Para **crear una Managed Policy** podemos hacerlo directamente en un JSON o seguir un asistente visual configurando los siguientes parámetros:

- Servicio - para el que será la política.
- Acciones - que se suelen dividirse en
  - List – Listar, describir
  - Read – Lectura
  - Tagging – Etiquetado
  - Write – Escritura
  - Permisos de gestión
- Recursos. Por ejemplo, si hemos escogido S3 podremos decir uno o n buckets, uno o n object, uno o n accesspoint
- Condiciones. Requerir MFA, Recurso IP u Otras
- Luego podemos poner Tags
- Nombre y descripción. Nos enseña un resumen.

Dentro de la política vemos

- Permisos
- Uso – Quien o qué la está usando
- Tags
- Versiones de política – pueden haber hasta 5 versiones guardadas.
- Access Advisor



The screenshot shows the AWS IAM console interface for a Managed Policy. At the top, there are tabs for 'Permissions', 'Policy usage', 'Tags', 'Policy versions', and 'Access Advisor'. Below these, there are buttons for 'Policy summary', '{ }JSON', and 'Edit policy'. The main area displays a JSON configuration for a policy with the following structure:

```
1- {
2-   "Version": "2012-10-17",
3-   "Statement": [
4-     {
5-       "Sid": "VisualEditor0",
6-       "Effect": "Allow",
7-       "Action": [
8-         "s3:GetObject",
9-         "s3:ListBucket",
10-        "s3:GetObjectVersion"
11-       ],
12-       "Resource": "*"
13-     }
14-   ]
15- }
```

Si queremos modificarla tan solo tenemos que abrirla y “Edit policy”. Tendremos las mismas opciones que creando: Fichero JSON o Editor visual. Cuando guardamos tendremos dos versiones.

Version	Creation time
▶ Version 2 (Default)	2022-09-13 10:19 UTC+0200
▶ Version 1	2022-09-13 10:03 UTC+0200

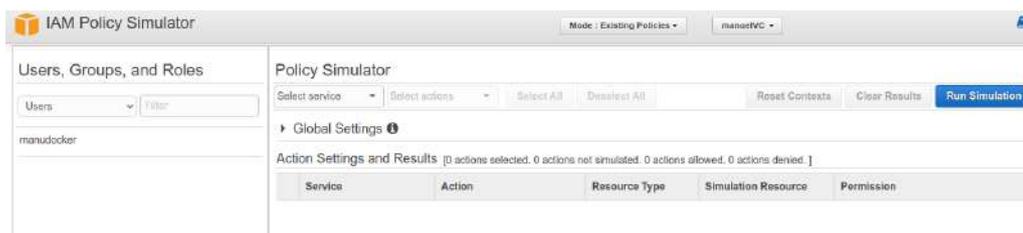
Para **asignar las políticas** a un grupo, a un usuario o a un rol tan solo tenemos que ir a la identidad concreta y, en permisos, añadirla con Attach policy.

Para **crear una política inline** (Es mejor no usarlas, se asocian directamente a la identidad) tan solo hay que ir al rol, usuario o grupo y a la hora de añadir se selección “Create inline policy”.

Para **crear una política de recurso** se hace en el mismo recurso dentro del servicio. Por ejemplo, dentro de un topic concreto de SNS.

Tenemos un **simulador de políticas** en el sidebar derecho, es un servicio a parte.

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



En la izquierda podemos escoger la identidad concreta para simular. A la derecha podemos comprobar las acciones que puede realizar la identidad seleccionada. En algunos casos, puede haber ACL o elementos que puedan dar resultados diferentes a los reales.

**Credential Report** – Se pueden descargar informes en CSV de IAM para poder tratar los datos de usuarios.

**Actividad de la organización** – Tenemos la estructura de la organización. Las organizaciones se utilizan para tener una división de los servicios y utilidades de AWS. Aquí podemos ver los últimos accesos. Se pueden gestionar las organizaciones en el servicio AWS organizations.

**Service control policies (SCPs)**– Son políticas a nivel de organización. Aquí se puede ver los usos de estas políticas. También se gestionan desde AWS organizations. Un ejemplo de SCPs es que no se puedan arrancar instancias caras para que nadie pueda dar estos usos con los costes que supone.

**Access analyzer** – Podemos crear análisis personalizados para comprobar por partes los componentes de AWS. Nos pedirá el nombre y podremos lanzarlo para toda la organización o solo en la cuenta actual. A través de las tags podemos filtrar los recursos que queremos analizar. Con el

resultado se podrá ver los activos, los archivados, los resueltos y todos. Se pueden mover entre estos resultado. Tenemos 3 espacio: Reglas archivadas, análisis y opciones.

**Storage Lens en S3** - Se puede crear un Dashboard personalizado con métricas y datos en relación a S3. Tendrá cuadros de mandos para una visualización rápida y poder gestionar los datos. No se puede acceder a un dashboard con usuario ROOT, tiene que ser un usuario IAM con los permisos:

- s3:ListStorageLensConfigurations
- s3:GetStorageLensConfiguration
- s3:GetStorageLensDashboard

En cambio, si que podemos crear un Dashboard con usuario ROOT. Podemos darle los siguientes parámetros:

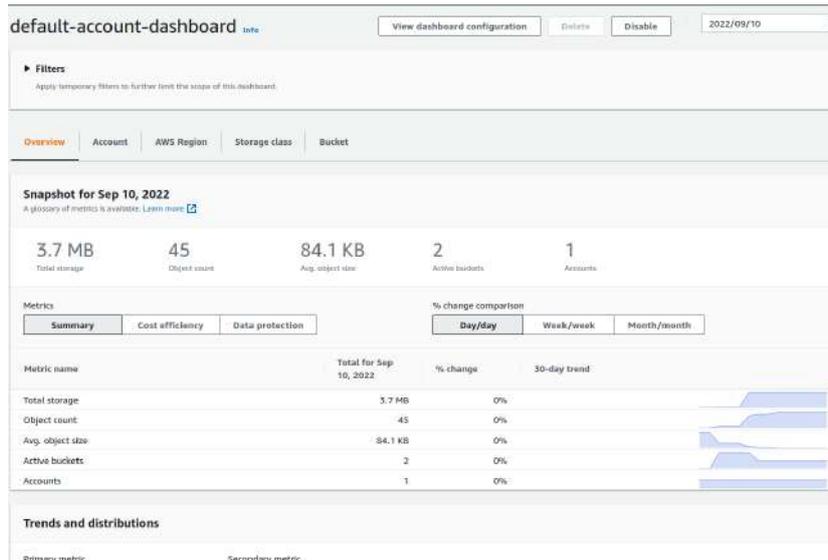
- Nombre
- Elegimos la region
- Si queremos actualizar las métricas diariamente.
- Tags
- Datos de la organización
- Que buckets queremos incluir
- Elegir entre métricas gratis o métricas avanzadas.
- Si queremos exportar las métricas cada 24 horas. Si habilitamos la exportación:
  - Podemos elegir el formato entre csv o Apache Parquet
  - Podemos elegir el bucket destino
  - Los permisos del bucket
  - Encriptación

Aun creando el Dashboard desde usuario ROOT no podremos entrar en él con esta cuenta, tendremos que entrar con un usuario IAM con los permisos adecuados.

Podemos crear una política de acceso a Dashboards de Storage Lens para un usuario que solo se encargue de esto.

Cuando entramos en el Dashboard recién creado no tiene datos.

En el default-account-dashboard aparece de todas las regiones y todos los buckets.



El panel aparece las métricas que ha ido recogiendo de los buckets.

Volviendo a las políticas de IAM, existe un **generador de políticas** en este enlace: <https://awspolicygen.s3.amazonaws.com/policygen.html>

**Step 1: Select Policy Type**

Select Type of Policy:

**Step 2: Add Statement(s)**

Effect:  Allow  Deny

Principal:

AWS Service:   All Services (\*)

Actions:   All Actions (\*)

Amazon Resource Name (ARN):

**Step 3: Generate Policy**

Es algo parecido al asistente que tenemos en la creación de las políticas. Antes de crearla nos da un resumen.

You added the following statements. Click the button below to Generate a policy.

Effect	Action	Resource	Conditions
Allow	<ul style="list-style-type: none"> <li>ec2:DescribeInstances</li> <li>ec2:StartInstances</li> <li>ec2:StopInstances</li> </ul>	*	None

### Step 3: Generate Policy

A *policy* is a document (written in the [Access Policy Language](#)) that acts as a container for one or more statements.

[Generate Policy](#)

[Start Over](#)

Nos dará un fichero JSON

#### Policy JSON Document

Click below to edit. To save the policy, copy the text below to a text editor. Changes made below will not be reflected in the policy generator tool.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmnt1663064560509",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Puede ser un mecanismo para descargar el archivo json. Hay que copiar y guardar en un documento plano con la extensión.

## 25.2. - CLI IAM

En **CloudShell** entramos en una shell virtual de la region. Aquí tenemos 1 GB gratuito por region. Tenemos preinstalado AWS CLI, Python, Node.js y otros.

El comando de IAM es

```
aws iam
```

Listar grupos

```
aws iam list-groups
```

Recordatorio de query y del formato de salida

```
aws iam list-groups --query "Groups[].GroupName" --output table
```

Listar las políticas (Saca todas las políticas, pueden ser muchas)

```
aws iam list-policies
```

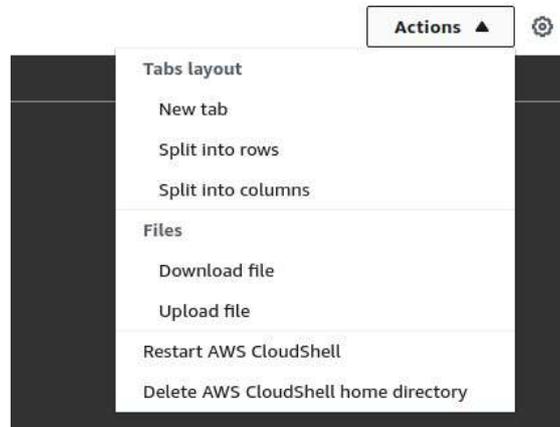
Nos ayuda a filtrar la opción scope con las posibilidades Local o AWS o All

```
aws iam list-policies --scope Local
```

Para listar los usuarios

aws iam list-users

Desde CloudShell podemos realizar algunas acciones en actions como “Nueva pestaña”, “Dividir filas”, “Dividir columnas”, “Descargar archivos” (Le daremos el path), “Subir archivos” (Lo dejará en la carpeta del usuario), “Reiniciar el servicio” o “Borrar el directorio home de AWS CloudShell”.



En la rueda dentada podemos cambiar algunas opciones del diseño.

Subimos el fichero de la política creada con el generador.

Para crear una políticas:

aws iam create-policy --policy-name politica-desde-cli--01 --policy-document [Podría subirlo desde un bucket con el arn y los permisos adecuado. O desde local con file://nombredocumento]

```
[cloudshell-user@ip-10-1-57-232 ~]$ aws iam create-policy --policy-name politica-desde-cli--01 --policy-document file://generador.json
{
  "Policy": {
    "PolicyName": "politica-desde-cli--01",
    "PolicyId": "ANPA60DMT7TPXQMR7IZU3",
    "Arn": "arn:aws:iam::992365247711:policy/politica-desde-cli--01",
    "Path": "/",
    "DefaultVersionId": "v1",
    "AttachmentCount": 0,
    "PermissionsBoundaryUsageCount": 0,
    "IsAttachable": true,
    "CreateDate": "2022-09-13T11:01:05+00:00",
    "UpdateDate": "2022-09-13T11:01:05+00:00"
  }
}
```

Ahora podemos darles estas políticas a una identidad o crear una identidad con él, etc

Añadir la política a un usuario y comprobar política del usuario en concreto:

aws iam attach-user-policy --user-name manudocker --policy-arn arn:aws:iam::992365247711:policy/politica-desde-cli--01

aws iam list-attached-user-policies --user-name manudocker

```
[cloudshell-user@ip-10-1-57-232 ~]$ aws iam attach-user-policy --user-name manudocker --policy-arn arn:aws:iam::992365247711:policy/politica-desde-cli--01
[cloudshell-user@ip-10-1-57-232 ~]$ aws iam list-attached-user-policies --user-name manudocker --query "AttachedPolicies[].PolicyName" --output table
ListAttachedUserPolicies
+-----+
| politica-desde-cli--01 |
+-----+
| AmazonS3FullAccess    |
+-----+
```

**Todos los subcomandos de aws iam:**

add-client-id-to-open-id-connect-provider  
add-role-to-instance-profile  
add-user-to-group  
attach-group-policy  
attach-role-policy  
attach-user-policy  
change-password  
create-access-key  
create-account-alias  
create-group  
create-instance-profile  
create-login-profile  
create-open-id-connect-provider  
create-policy  
create-policy-version  
create-role  
create-saml-provider  
create-service-linked-role  
create-service-specific-credential  
create-user  
create-virtual-mfa-device  
deactivate-mfa-device  
delete-access-key  
delete-account-alias  
delete-account-password-policy  
delete-group  
delete-group-policy  
delete-instance-profile  
delete-login-profile  
delete-open-id-connect-provider  
delete-policy  
delete-policy-version  
delete-role  
delete-role-permissions-boundary  
delete-role-policy  
delete-saml-provider

delete-server-certificate  
delete-service-linked-role  
delete-service-specific-credential  
delete-signing-certificate  
delete-ssh-public-key  
delete-user  
delete-user-permissions-boundary  
delete-user-policy  
delete-virtual-mfa-device  
detach-group-policy  
detach-role-policy  
detach-user-policy  
enable-mfa-device  
generate-credential-report  
generate-organizations-access-report  
generate-service-last-accessed-details  
get-access-key-last-used  
get-account-authorization-details  
get-account-password-policy  
get-account-summary  
get-context-keys-for-custom-policy  
get-context-keys-for-principal-policy  
get-credential-report  
get-group  
get-group-policy  
get-instance-profile  
get-login-profile  
get-open-id-connect-provider  
get-organizations-access-report  
get-policy  
get-policy-version  
get-role  
get-role-policy  
get-saml-provider  
get-server-certificate  
get-service-last-accessed-details  
get-service-last-accessed-details-with-entities  
get-service-linked-role-deletion-status  
get-ssh-public-key  
get-user  
get-user-policy  
list-access-keys

list-account-aliases  
list-attached-group-policies  
list-attached-role-policies  
list-attached-user-policies  
list-entities-for-policy  
list-group-policies  
list-groups  
list-groups-for-user  
list-instance-profile-tags  
list-instance-profiles  
list-instance-profiles-for-role  
list-mfa-device-tags  
list-mfa-devices  
list-open-id-connect-provider-tags  
list-open-id-connect-providers  
list-policies  
list-policies-granting-service-access  
list-policy-tags  
list-policy-versions  
list-role-policies  
list-role-tags  
list-roles  
list-saml-provider-tags  
list-saml-providers  
list-server-certificate-tags  
list-server-certificates  
list-service-specific-credentials  
list-signing-certificates  
list-ssh-public-keys  
list-user-policies  
list-user-tags  
list-users  
list-virtual-mfa-devices  
put-group-policy  
put-role-permissions-boundary  
put-role-policy  
put-user-permissions-boundary  
put-user-policy  
remove-client-id-from-open-id-connect-provider  
remove-role-from-instance-profile  
remove-user-from-group  
reset-service-specific-credential

resync-mfa-device  
set-default-policy-version  
set-security-token-service-preferences  
simulate-custom-policy  
simulate-principal-policy  
tag-instance-profile  
tag-mfa-device  
tag-open-id-connect-provider  
tag-policy  
tag-role  
tag-saml-provider  
tag-server-certificate  
tag-user  
untag-instance-profile  
untag-mfa-device  
untag-open-id-connect-provider  
untag-policy  
untag-role  
untag-saml-provider  
untag-server-certificate  
untag-user  
update-access-key  
update-account-password-policy  
update-assume-role-policy  
update-group  
update-login-profile  
update-open-id-connect-provider-thumbprint  
update-role  
update-role-description  
update-saml-provider  
update-server-certificate  
update-service-specific-credential  
update-signing-certific  
update-user  
upload-server-certificate  
upload-signing-certificate  
upload-ssh-public-key  
wait  
wizard



## TEMA 26 - CloudTrail: Monitorización accesos de usuarios

Es una herramienta de monitorización de la actividad de las cuentas de AWS. Se captura toda la actividad de AWS y se puede guardar en la consola de CloudTrail, a un bucket S3 o en CloudWatch Log.

Podemos activar alarmas en eventos.

Se puede encontrar información en la consola o en otros servicios como Amazon Athena (queries sobre ficheros de log con lenguaje light SQL).

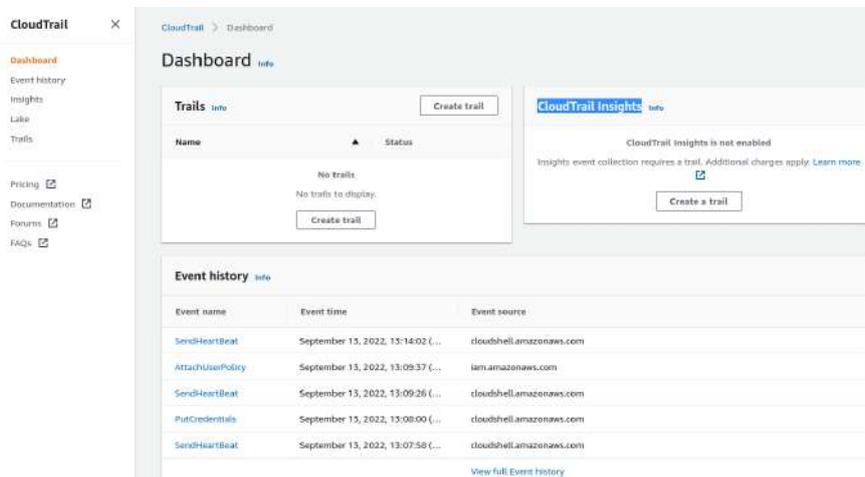
Otro servicio es CloudTrail lake donde almacenamos los datos como Data store y podemos hacer consultas SQL.

Por defecto, se capturan todos los datos de administración gratuitos, reteniendolos por 90 días.

Cloud Trail Lake nos permite guardar la información más tiempo, pero es caro.

En el dashboard vemos:

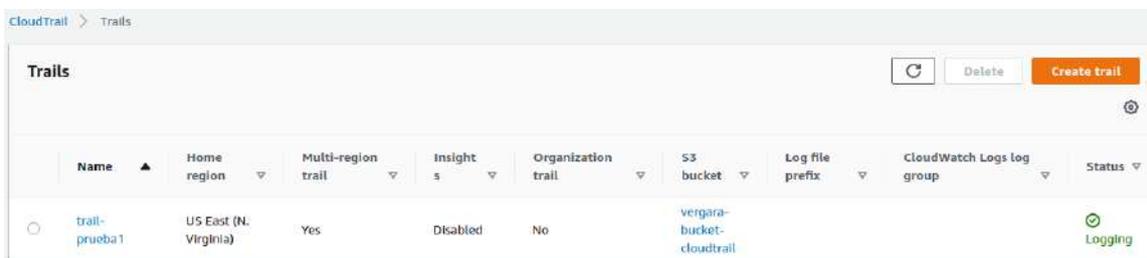
- Trails
- CloudTrails Insights
- Event history



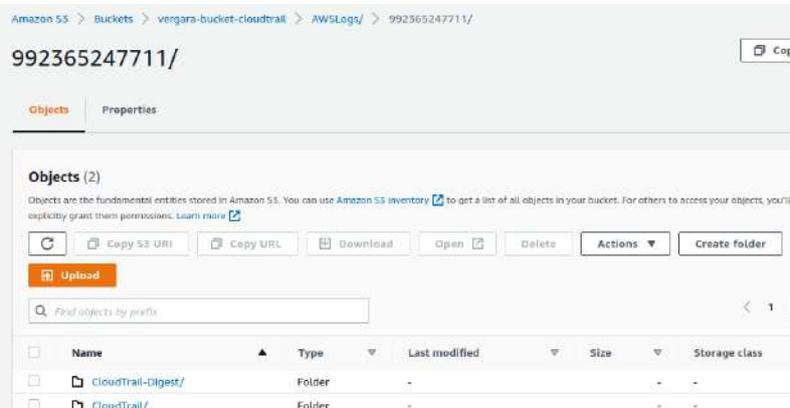
Un **trail** es un contenedor donde guardamos los eventos con los que trabajar. Cuando creamos uno podemos configurar:

- Nombre
- Almacenamiento. Podemos crear un bucket o usar uno existentes.
- Encriptación

- Clave KMS. Podemos crear una o usar una existente.
- Validación de logs – Para controlar que no haya manipulaciones.
- Crear notificación de entrega por SNS.
- Activar CloudWatch Logs
- Eventos a guardar
  - Administración
    - Read
    - Write
    - Excluir AWS KMS
    - Excluri RDS
  - Data (gestión de recursos)
    - Podemos escoger los recursos
  - Insights (actividades inusuales). - Cuando activamos esta opción suele tardar en activarse porque busca patrones. Además, tiene una pantalla de eventos con detalles.
    - API call rate
    - API error rate



En el bucket crea un esqueleto de carpetas para guardar eventos.

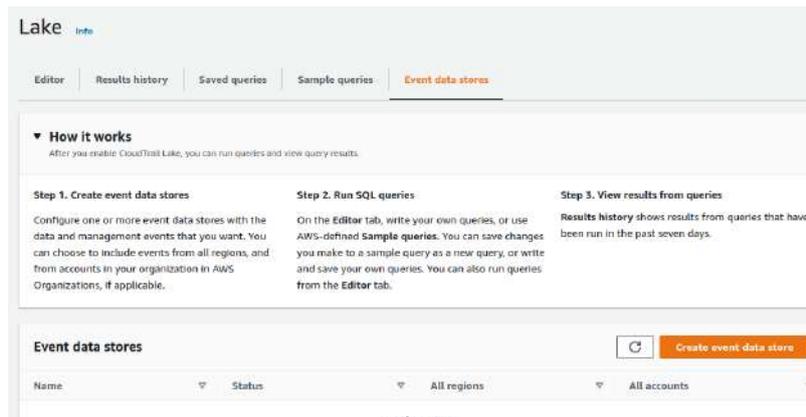


En CloudTrail-Digest se guardan ficheros de metadatos. En CloudTrail estarán lo eventos que se guardan con un esqueleto de region y fecha en json comprimidos

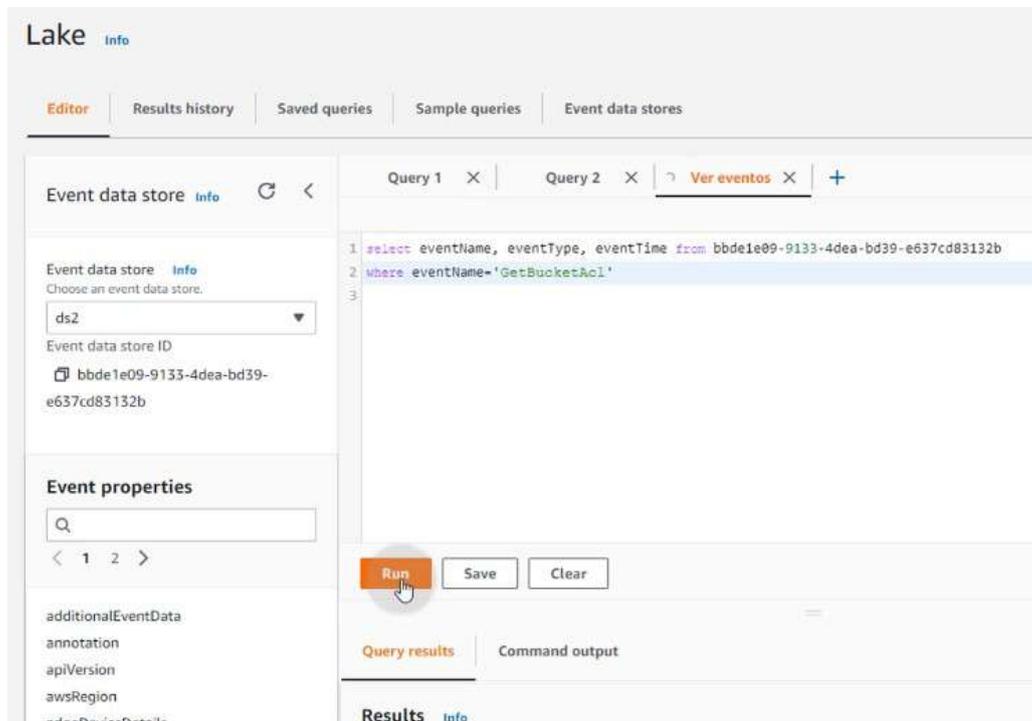


Lo más cómodo es enviar los logs a CloudWatch para poder visualizarlos.

Consola de **CloudTrail Lake** – Guarda los eventos en un formato que permite las SQL queries.



Consulta SQL:



Para eliminar un datastore tendremos que quitar la protección de borrado. Luego ya podremos borrar pero hasta que no pasen los días de retención que hayamos puesto no desaparecerá, eso sí, dejará de guardar datos.

## 26.1. - AWS CLI

El subcomando utilizado es

```
aws cloudtrail
```

Por ejemplo, listar la trails

```
aws cloudtrail list-trails
```

o para ver propiedades

```
aws cloudtrails describe-trails --trail-name-list nombre nombre-bucket
```

Crear un trail en un bucket existente. Necesitaremos una política y para conseguirla rápido, si ya tenemos el bucket asociado con CloudTrail podemos ir a sus permisos, copiar la política de resources y pegarla con una coma más abajo, indicando el nombre del trail nuevo. Entonces, ya podemos crearlo.

```
aws cloudtrail create-trail --name Nombre-Trail --s3-bucket-name nombre-bucket
```

Por defecto, guarda los datos de administración.

Para eliminar un trail

```
aws cloudtrail delete-trail --name nombre-del-trail
```

Las opciones del comando son:

```
add-tags  
cancel-query  
create-event-data-store  
create-trail  
delete-event-data-store  
delete-trail  
describe-query  
describe-trails  
get-channel  
get-event-data-store  
get-event-selectors  
get-insight-selectors  
get-query-results  
get-trail  
get-trail-status  
list-channels  
list-event-data-stores
```

list-public-keys  
list-queries  
list-tags  
list-trails  
lookup-events  
put-event-selectors  
put-insight-selectors  
remove-tags  
restore-event-data-store  
start-logging  
start-query  
stop-logging  
update-event-data-store  
update-trail  
validate-logs

## TEMA 27 - Cloud9 y las SDK – Entorno de desarrollo y pruebas

**Cloud9** es un entorno en cloud para desarrollar, testear y probar código. Tiene un IDE (Entorno de Desarrollo Integrado) incorporado con herramienta gráfica online que permite incorporar AWS CLI, Clientes SDK (Kit de desarrollo de software), entre otras herramientas. Además de almacenar el código en AWS y compartirlo entre otros usuarios. En definitiva, es una instancia con una plantilla instalada con todo el entorno necesario para trabajar, es muy pequeña y muy barato. Por ejemplo, una máquina para trabajar 40 horas semanales puede salir a 5 dólares al mes.

**Cloud Shell** es una línea de comandos que también nos permite trabajar online.

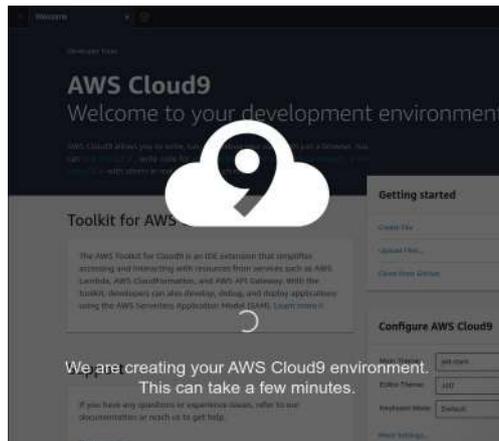
Se puede utilizar con DocumentDB (servicio de base de datos escalable, de larga duración y completamente administrado para operar cargas de trabajo de MongoDB esenciales) o con Red Shift (servicio de almacenamiento de datos en la nube).

No es recomendable utilizar usuario ROOT con cloud9

Para **crear un entorno**, entramos en el servicio y los parámetros configurables son:

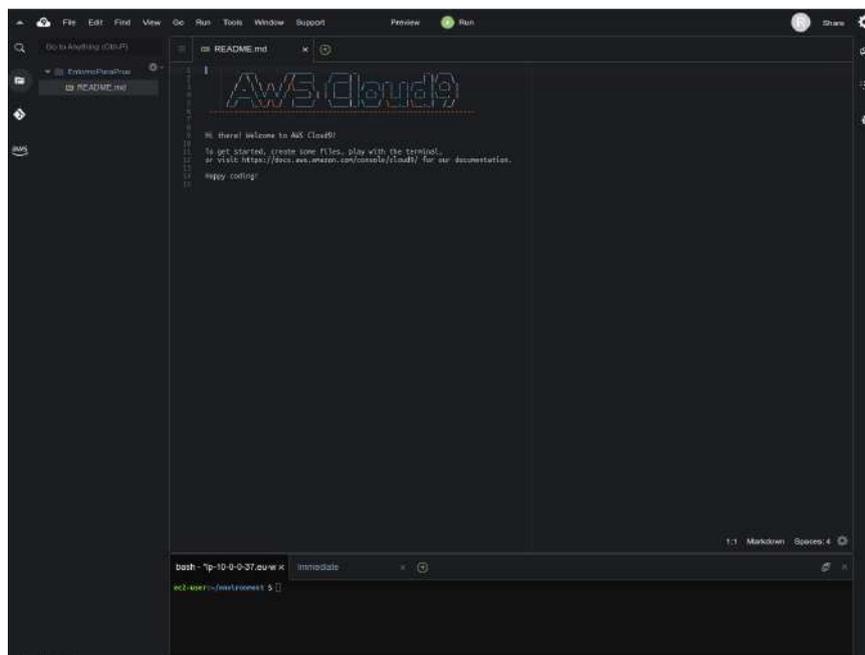
- Nombre y descripción
- Tipo de entorno
  - Instancia nueva
  - De acceso con System Manager
  - En una instancia existente
- Tipo de instancia – Son instancias pequeñas.

- SO – Da 3 opciones: Amazon Linux 2, Amazon Linux AMI o Ubuntu Server 18,04 LTS
- Opciones de hibernación
- IAM role
- Network (VPC, subnet)
- Tags



Cuando lo abres con ROOT te da un aviso.

Es un IDE normal como eclipse, NetBeans o demás, pero está dentro de un entorno de AWS y con acceso directo a los servicios AWS.



En la parte izquierda tenemos varias pestañas. De archivos, de git y de navegación por AWS.

Como otros IDEs podemos abrir varias pestañas de ficheros que se controlan arriba.

En la parte de abajo hay un terminal linux y immediate que nos permite trabajar con un entorno REPL de javascript.

En la parte de menu superior podemos acceder a todas las acciones posibles. Tenemos un preview y un run. Y más a la derecha esta nuestro usuario, el botón de compartir y una rueda dentada con las opciones del diseño de la interfaz.

En las pestañas se puede crear también terminales. El terminal está preparado como una máquina normal, pero además tiene instalado AWS CLI, Python, Java, Go, node, ruby, C, git, docker, perl, kotlin, .NET, Rust, Swift, php, sqlite, terraform, etc

SDK en AWS: <https://aws.amazon.com/es/developer/tools/> Aquí podremos encontrar los SDK necesarios para trabajar en los distintos lenguajes.

En concreto, en Java, podemos utilizar una version del OpenJDK, podemos descargar Amazon Corretto.

Adaptación de Visual Studio Code para AWS: <https://aws.amazon.com/es/visualstudiocode/>

## 27.1. - Ejemplo de código python

El SDK que necesitamos es Boto3, que es una librería que nos permite acceder a todos los recursos de AWS.

Necesitamos utilizar el gestor de paquetes pip.

```
pip install boto3
```

Se puede hacer las pruebas en el modo comando de python

```
python
```

Importamos la librería boto3, si no hay mensaje de error la hemos descargado correctamente.

```
>>> import boto3
```

Para acceder a un recurso nos ayudaremos de una variable. Si empezamos a escribir boto3 y le damos a tabulador nos saldrán las opciones que podemos utilizar.

```
>>> s3=boto3.
```

```
>>> s3=boto3.
boto3.DEFAULT_SESSION      boto3.client()             boto3.exceptions           boto3.resources            boto3.setup_default_session(
boto3.NullHandler()        boto3.compat               boto3.logging              boto3.session              boto3.utils
boto3.Session()            boto3.docs                 boto3.resource()           boto3.set_stream_logger(
```

Lo que queremos es preparar la conexión en la variable, así que elegimos el recurso

```
>>> s3=boto3.resource('s3')
```

Ahora la variable s3 es un recurso de tipo servicio y podremos lanzarle comandos.



```
bucket=s3.Bucket('vergara-bucket-03')
```

Y subimos un objeto al bucket.

```
bucket.put_object(Key='fichero',Body='/home/ec2-user/environment/README.md')
```

Y ahora podemos listar los objetos que hay en el bucket

```
for objeto in s3.Bucket('vergara-bucket-03').objects.all():  
...     print(objeto.key)  
...
```

Podemos añadir a una variable el puntero al objeto concreto

```
v1=s3.Object('vergara-bucket-03','fichero')
```

y preguntar por su tamaño y su tipo

```
print(v1.content_length)  
print(v1.content_type)
```

## TEMA 28 - Bases de Datos: DocumentDB

Una versión de MongoDB en AWS. Está orientada a Cloud. Cualquier dato en MongoDB es fácil reapuntarla a DocumentDB.

Conceptos básicos:

- NOSQL (NotOnlySQL) es una evolución del sistema clásico de BBDD relacionales cuya principal característica es que no se requiere una definición inicial de las estructuras sobre las que se almacenarán los datos.
- Evolución del modelo entidad-relación para el soporte de estructuras variables en el tiempo.
- MongoDB es una BBDD NOSQL orientada a documento.
- Desarrollada por 10gen (Ahora llamados MongoDB)

Características

- Flexibilidad de los Modelos
- Alto rendimiento, alta disponibilidad
- Escalabilidad
- etc

El modelo de documentos se basa en el estándar JSON/BSON (BSON es una serialización binaria de JSON). Características de BSON

- Permite tener documentos dentro de documentos
- Podemos definir arrays dentro de documentos.

Comparación SQL vs MongoDB

SQL	MongoDB
Tabla	Colección
Fila	Documento
Columna	campo
Clave primaria	Id de objeto
Índice	Índice
Vista	Vista
Tabla u objeto anidado	Documento incrustado
Array	Array

Ejemplo de un documento con vista JSON

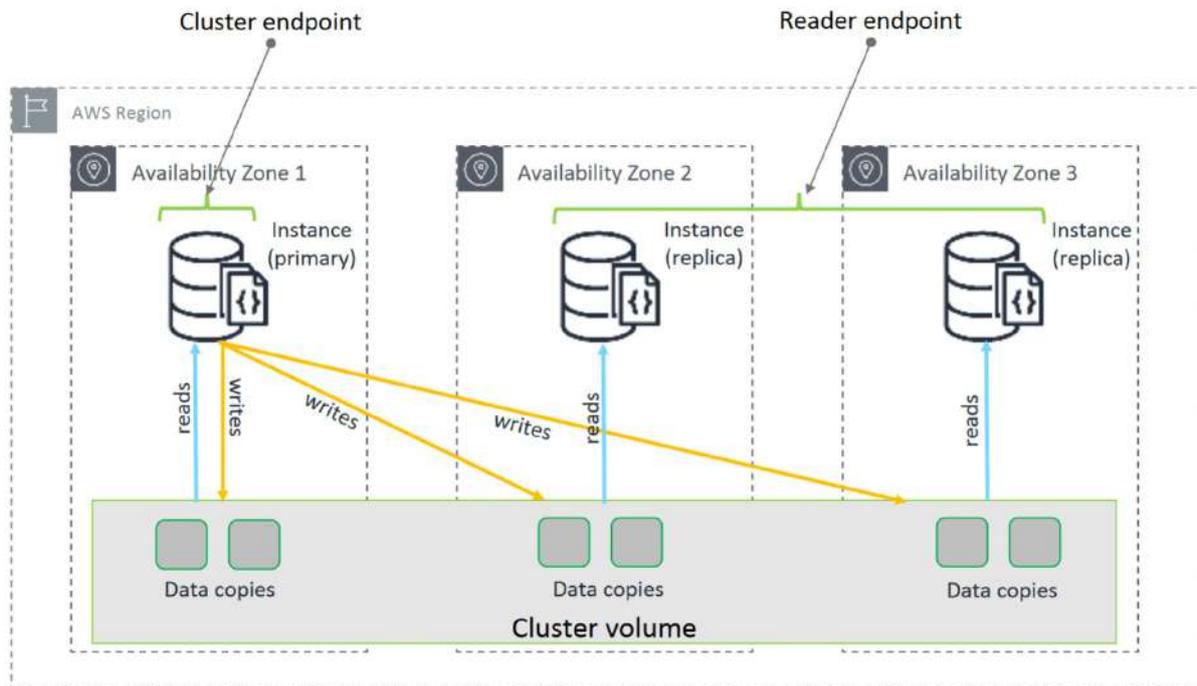
```
{
  "_id": 1,
  "name": { "first" : "John", "last" : "Backus" },
  "contribs": [ "Fortran", "ALGOL", "Backus-Naur Form", "FP" ],
  "awards": [
    {
      "award": "W.W. McDowell Award",
      "year": 1967,
      "by": "IEEE Computer Society"
    }, {
      "award": "Draper Prize",
      "year": 1993,
      "by": "National Academy of Engineering"
    }
  ]
}
```

Este documento sería una fila, se podría subir a una collection, que sería una tabla.

Cuando se crea una collection se respeta el tipo de documento que tienen dentro.

## 28.1. - Arquitectura

Un cluster consta de 0 a 16 instancias y un volumen de almacenamiento de cluster que gestiona los datos de esas instancias. Los datos del clúster se almacenan en el volumen del clúster con copias en tres zonas de disponibilidad diferentes.



El cluster volume es el almacenamiento global. Solo escriben datos la instancia primaria. Tanto la primaria como las réplicas leen datos.

## 28.2. - Consola DocumentDB

Opciones en la consola:

- Dashboard
- Clusters – Nos pedirá más o menos las mismas propiedades que en Aurora. Igual que pasa con las instancias de RDS, las instancias de DocumentDB son Platform as a Service, es decir no se pueden administrar. Siempre van a cobrar 10 minutos como mínimo y no existe opción gratuita. Para **crear un cluster** podremos:
  - Nombre
  - Versión – Permite 2 versiones. 3.6.0 y 4.0.0
  - Instancia
  - Número de instancias – Lo mínimo ideal son 3 para tener un cluster en alta disponibilidad.
  - Autenticación – Usuario master (No puede ser una palabra reservada: admin, master, etc) y contraseña.
  - Opciones avanzadas
    - Network – VPC, grupo de subnets y Security groups

- Opciones Cluster – Puerto (27017) y Grupo de parámetros
- Encriptación – La master key por defecto es la de AWS/RDS
- Además: Backup, Performance Insights, Exportar logs, Mantenimiento, Etiquetado y Protección de borrado

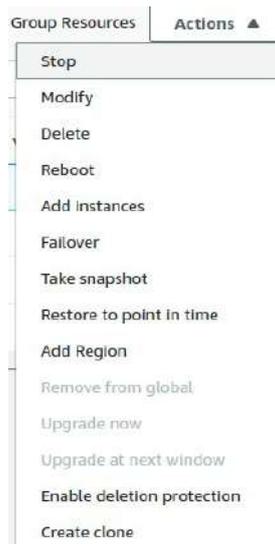
Cluster identifier	Role	Engine version	Region & AZ	Status	CPU	Current
documentdb-cluster-01	Regional c...	4.0.0	eu-west-3	creating	-	-
documentdb-cluster-01	Replica in...	4.0.0	-	creating	-	-
documentdb-cluster-012	Replica in...	4.0.0	-	creating	-	-
documentdb-cluster-013	Replica in...	4.0.0	-	creating	-	-

- Performance insights
- Snapshots
- Subnets groups - Comparte con RDS los grupos de subnets, pero siempre es mejor personalizar el grupo para cada cluster. Para **crear un grupo de subnets** podemos configurar:
  - Nombre, descripción y en añadir subnet se debe indicar la VPC, la AZ y la subnet concreta. Se debe añadir al listado cada subnet que se necesite.
- Parameter groups – Son los parámetros configurables de la BBDD. Son pocos los parámetros si lo comparamos a otros tipos de BBDD.

Cluster parameter name	Values	Allowed...	Modifica...	Apply t...	Data type	Description
audit_logs	disabled	enabled,di...	true	dynamic	list	Enables auditing o...
change_stream_log_retention_duration	10800	3600-604...	true	dynamic	integer	Duration of time in...
profiler	disabled	enabled,di...	true	dynamic	string	Enables profiling f...
profiler_sampling_rate	1.0	0.0-1.0	true	dynamic	float	Sampling rate for l...
profiler_threshold_ms	100	50-21474...	true	dynamic	integer	Operations longer ...
tls	enabled	disabled,e...	true	static	string	Config to enable/d...
ttl_monitor	enabled	disabled,e...	true	dynamic	string	Enables TTL Monit...

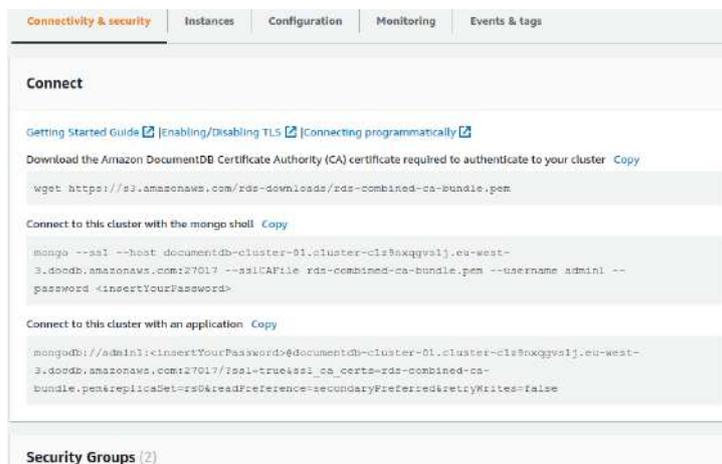
- Event Subscriptions – Nos sirve para conectar con SNS. También los comparte con RDS.
- Events – Nos dará información de arranque, parada y otros generales.

Las acciones en los cluster son muy parecidas a las de RDS



### Componentes de un cluster

- Connectivity & security – Nos indica como podemos conectarnos a un cluster de este tipo
  - Mongo shell – Es una herramienta en modo comando de MongoDB. Documentación oficial: <https://www.mongodb.com/docs/v4.4/mongo/>
  - Aplicación -



- Existen muchas otras herramientas para conectarse a un MongoDB: Robo 3T, Nosqlclient, Umongo, Mongotro
- Instances – Con la primaria y las réplicas que tengamos.
- Configuration – Acepta modificaciones. Indica todas las conexiones
- Monitoring
- Events & tags

En las **propiedades de las instancias** (primarias y réplicas) aparece los datos de la instancia en concreto.

## 28.3. - Conectar con la BBDD Mondo

Para conectarnos fácilmente podemos utilizar Cloud9 y seguir los siguientes pasos:

Crear el repositorio

```
echo -e "[mongodb-org-4.0] \nname=MongoDB
Repository\nbaseurl=https://repo.mongodb.org/yum/amazon/2013.03/mongodb-org/4.0/x86_64/
ngpgcheck=1 \nenabled=1 \ngpgkey=https://www.mongodb.org/static/pgp/server-4.0.asc" | sudo tee
/etc/yum.repos.d/mongodb-org-4.0.repo
```

Instalar mongo shell. Primero siempre es mejor una actualización (sudo yum update). Si pusieramos mongodb lo instalaría todo, pero podemos trabajar con solo la shell.

```
sudo yum install -y mongodb-org-shell
```

Ahora ya está descargado, pero no podemos conectarnos. Lo siguientes pasos ya están en la pestaña de connectivity del cluster.

Descargar el certificado

```
wget https://s3.amazonaws.com/rds-downloads/rds-combined-ca-bundle.pem
```

Conectar el cluster con mongo shell

```
mongo --ssl --host documentdb-cluster-01.cluster-c1z9nxqgvs1j.eu-west-
3.docdb.amazonaws.com:27017 --sslCAFile rds-combined-ca-bundle.pem --username admin1 --
password <insertYourPassword>
```

Podemos probar **algunos comandos de MongoDB**

Comprobar las bases de datos existentes

```
show dbs
```

Creamos una nueva Base de datos denominada datos

```
use datos
```

Creamos un documento para comprobar que funciona. Hasta que no creamos un documento dentro de una base de datos, esta no se inicializa

```
db.movie.insert({"name":"Ejemplo de documento"})
```

Comprobamos que está

```
show dbs
```

Comprobamos la colección que acabamos de crear

```
show collections
```

```
rs0:PRIMARY> use datos
switched to db datos
rs0:PRIMARY> show dbs
rs0:PRIMARY> db.pelicula.insert({"nombre":"Lo que el viento se llevo"})
WriteResult({ "nInserted" : 1 })
rs0:PRIMARY> show dbs
datos 0.000GB
rs0:PRIMARY> show collections
pelicula
rs0:PRIMARY>
```

Podemos comprobar que tiene la BBDD concentrador

```
db.pelicula.find()
```

```
pelicula
rs0:PRIMARY> db.pelicula.find()
{ "_id" : ObjectId("6322fe05985b2824b53508a4"), "nombre" : "Lo que el viento se llevo" }
rs0:PRIMARY>
```

Podemos insertar más campos (columnas) en el documento (fila) en la misma colección (tabla)

```
rs0:PRIMARY> db.pelicula.insert({"nombre":"Terminator","Actor":"Arnold"})
WriteResult({ "nInserted" : 1 })
rs0:PRIMARY> db.pelicula.find()
{ "_id" : ObjectId("6322fe05985b2824b53508a4"), "nombre" : "Lo que el viento se llevo" }
{ "_id" : ObjectId("6322ff62985b2824b53508a5"), "nombre" : "Terminator", "Actor" : "Arnold" }
rs0:PRIMARY>
```

CUIDADO. Se pueden poner datos que no correspondan

```
rs0:PRIMARY> db.pelicula.insert({"codigo_factura":100,"Descripcion":"Ejemplo de descripcion"})
WriteResult({ "nInserted" : 1 })
rs0:PRIMARY> db.pelicula.find()
{ "_id" : ObjectId("6322fe05985b2824b53508a4"), "nombre" : "Lo que el viento se llevo" }
{ "_id" : ObjectId("6322ff62985b2824b53508a5"), "nombre" : "Terminator", "Actor" : "Arnold" }
{ "_id" : ObjectId("6322ffb0985b2824b53508a6"), "codigo_factura" : 100, "Descripcion" : "Ejemplo de descripcion" }
rs0:PRIMARY>
```

Creamos una colección manualmente, denominadas facturas

```
db.createCollection("facturas")
```

```
show collections
```

```
rs0:PRIMARY> db.createCollection('facturas')
{ "ok" : 1, "operationTime" : Timestamp(1663238143, 1) }
rs0:PRIMARY> show collections
facturas
pelicula
rs0:PRIMARY>
```

Podemos crear colecciones con límites

```
db.createCollection("foros", { capped : true, vsize : 6142800, max : 10000 } )
```

Borramos la colección

```
db.facturas.drop()
```

```
show collections
```

```
rs0:PRIMARY> db.facturas.drop()
true
rs0:PRIMARY> show collections
pelicula
rs0:PRIMARY> □
```

Podemos hacer un find con un formato JSON

```
db.pelicula.find().pretty()
```

```
rs0:PRIMARY> db.pelicula.find().pretty()
{
  "_id" : ObjectId("6322fe05985b2824b53508a4"),
  "nombre" : "Lo que el viento se llevo"
}
{
  "_id" : ObjectId("6322ff62985b2824b53508a5"),
  "nombre" : "Terminator",
  "Actor" : "Arnold"
}
{
  "_id" : ObjectId("6322ffb0985b2824b53508a6"),
  "codigo_factura" : 100,
  "Descripcion" : "Ejemplo de descripcion"
}
```

Podemos insertar varios documentos

```
db.facturas.insert([
{
  title: 'Servidores',
  description: 'Servidores para el CPD',
  by: 'Departamento de informatica',
  url: 'https://www.ibm.com',
  tags: ['servidores', 'informatica', 'ibm'],
  likes:100
},
{
  title: 'Boligrafos',
  description: 'Compra de bolis',
  by: 'Pepe',
  tags: ['servidores', 'informatica', 'ibm'],
  comments:[
  {
    precio: 5,
    descuento: 0,
    pagado: 'con visas'
  }
]
}
])
```

Insertar mediante script cargar.js

```
db.articulos.drop()
for(i = 1; i <= 10; i++) {
db.articulos.insertOne(
{
_id: i,
nombre: 'nombre'+i
}
)
}
```

Y lo insertamos mediante el comando load

```
load('cargar.js')
```

Comprobar que se ha cargado

```
db.articulos.find()
```

Actualizar la fila numero 1

```
db.articulos.update({"_id":1},{ $set: {"nombre": "PEPITO"} })
```

Borrar fila con nombre3

```
db.articulos.remove({"nombre": "nombre3"})
```

Contar documentos de una colección

```
b.articulos.count()
```

Buscar documentos

```
db.articulos.find()
```

Sin formato json

```
db.articulos.find().pretty()
```

Buscar documentos con query clave/valor

```
db.facturas.find({"by":"Pepe"}).pretty()
```

o

```
b.facturas.find({"tags":"informatica"}).pretty()
```

Buscar documentos con precio menor de 6

```
db.facturas.find({"comments.precio":{$lt:6}}).pretty()
```

Añadir campo

```
db.facturas.update({"title":"Servidores"},{$set:{"precio":10}})
```

Borramos documento

```
db.facturas.remove({"title":"cables"})
```

Visualizar solo un campo de cada documento

```
db.facturas.find({}, {"title":1})
```

Visualizar solo un campo de cada documento sin el id

```
db.facturas.find({}, {"title":1,_id:0})
```

Visualizar solo un campo de cada documento sin el id y solo los primeros dos documentos

```
db.facturas.find({}, {"title":1,_id:0}).limit(2)
```

Visualizar ordenados por nombre

```
db.facturas.find({"title":{$ne:""}}, {"title":1,_id:0}).sort({"name":1})
```

Crear un indice sobre title

```
db.ejemplo.find({"title":{$ne:""}}, {"title":1,_id:0}).sort({"title":1})
```

## 28.4. - Gestión de instancias y cluster

La gestión es idéntica a la de Aurora en RDS.

## TEMA 29 - CloudFormation. Plantillas para nuestra infraestructura

No tiene nada que ver con la formación. Es una herramienta que nos permite modalizar y provisional las estructuras en AWS.

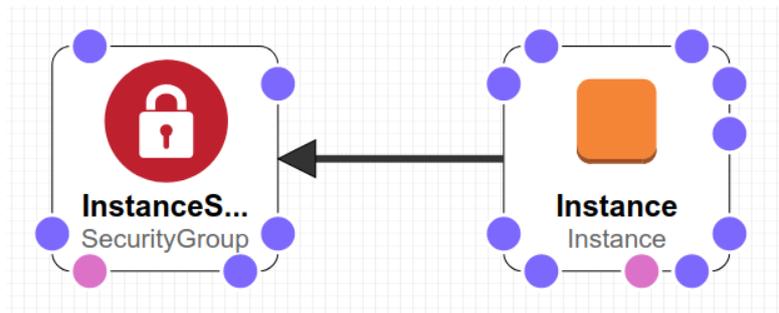
Se utiliza para repetir la misma estructura con una plantilla de la misma, que se llaman stack. Mientras se lanza un stack se puede modificar (nombre, componentes, etc)

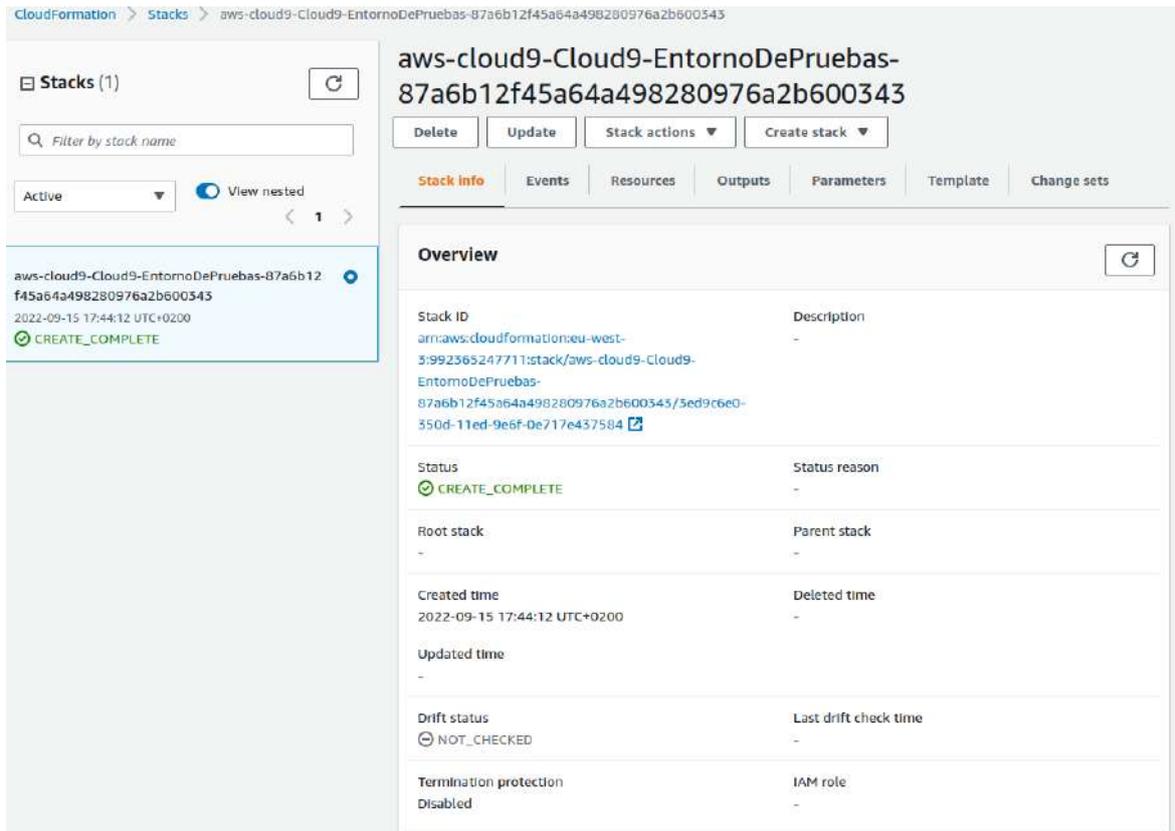
Posibilita crear infraestructuras complejas de manera muy fácil.

Hay un diseñador donde se puede dibujar la infraestructura para ahorrar ciertas conexiones.

Cuando se borra un stack se borran todos los componentes que se incluyen dentro.

Cuando se crea un entorno cloud9 automáticamente se crea el stack en CloudFormation. Lo único que hace es crear un grupo de seguridad y una instancia. Diseño del stack de cloud9:





Los elementos que tiene son:

- Stack info
- Events – Los eventos por los que ha pasado el stack
- Resource – Lista de los recursos que tiene el stack
- Outputs – Las salidas
- Parameters – Los parámetros que se piden al crear el stack
- Template – La plantilla que se ha utilizado. Es el core del stack. En un archivo JSON o YAML que indica las características del stack.
- Change sets – Son los cambios que se hacen del stack.

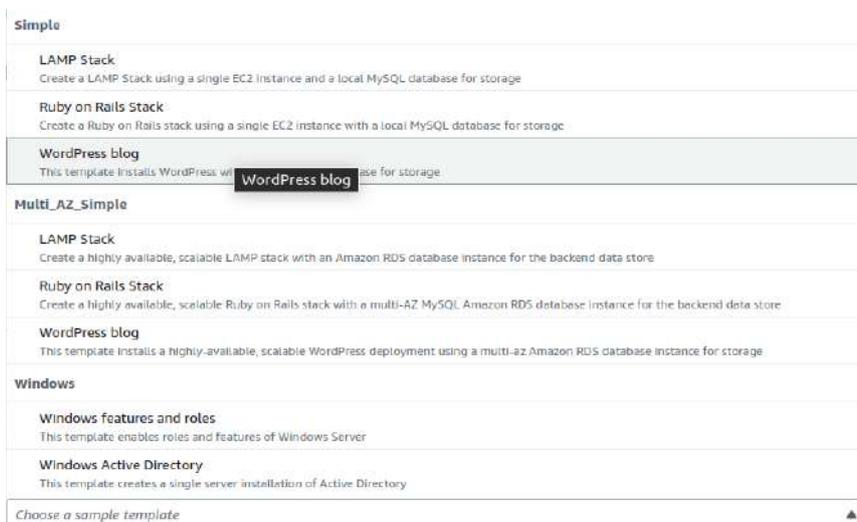
## 29.1. - Crear un stack

Para crear un stack se puede elegir con nuevos recursos o con recursos existentes



Para crear un stack indicamos:

- Una plantilla
  - Que hemos creado
    - Indicar Amazon S3 URL
    - Subir el archivo de plantilla
  - Las de ejemplo
    - Escoger tipo de plantilla



Cuando seleccionas puedes ver el diseño

- Utilizando en la herramienta Designer.

Una vez seleccionada la plantilla tendremos que dar algunos parámetros más. Por ejemplo, en el LAMP Stack simple:

- Nombre stack
- Parámetros (Depende de la plantilla pedirá unos parámetros u otros)

**Parameters**  
Parameters are defined in your template and allow you to input custom values when you create or update a stack.

**DBName**  
MySQL database name

**DBPassword**  
Password for MySQL database access

**DBRootPassword**  
Root password for MySQL

**DBUser**  
Username for MySQL database access

**InstanceType**  
WebServer EC2 instance type:

**KeyName**  
Name of an existing EC2 KeyPair to enable SSH access to the Instance:

**SSHLocation**  
The IP address range that can be used to SSH to the EC2 instances.

- Tags y Permisos
- Stack failure options – Comportamiento cuando falla. Puedes escoger entre rollback de todos los recursos o guarda los que se ha conseguido crear.
- Stack policy – Política de seguridad para configurar permisos.
- Rollback – A través de una alarma se efectua un rollback
- Opciones de notificación
- Opciones de creación del stack – Controlar el tiempo de creación. Protección de eliminación.

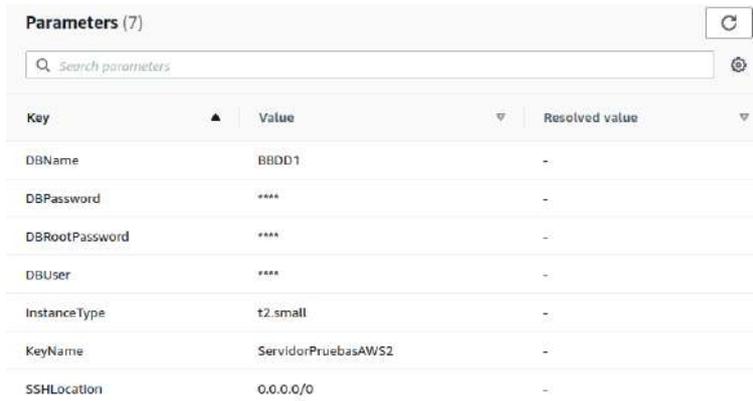
Después de crear, en los eventos se puede ver justo lo que está haciendo si vamos actualizando la lista. En este caso también ha creado un ouput, una URL.

**Outputs (1)** 🔄

⚙️

Key	Value	Description	Export name
WebsiteURL	<a href="http://ec2-35-180-139-201.eu-west-3.compute.amazonaws.com">http://ec2-35-180-139-201.eu-west-3.compute.amazonaws.com</a>	URL for newly created LAMP stack	-

Los parámetros que ha solicitado al crear los refleja en la pestaña de parámetros.



Key	Value	Resolved value
DBName	BBDD1	-
DBPassword	****	-
DBRootPassword	****	-
DBUser	****	-
InstanceType	t2.small	-
KeyName	ServidorPruebasAWS2	-
SSHLocation	0.0.0.0/0	-

## 29.2. - Designer para crear una plantilla

Documentación tipo de propiedades y recursos:

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-template-resource-type-ref.html>

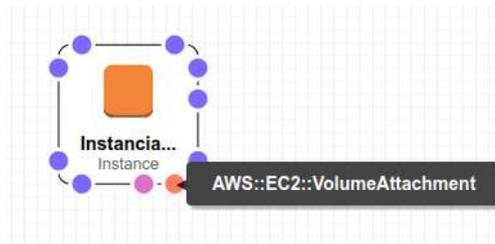
Cuando creamos un stack, sea plantilla ya creada, ejemplo de plantilla o designer. Siempre podemos ir al designer.

Componentes de designer:

- A la izquierda una lista de todos los recursos.
- En el panel central aparecen los recursos seleccionados. Si clicamos con el botón derecho salen opciones: Editar propiedades (Irá al documento inferior, al asiento del elemento), duplicar, borrar o documentación (A la ayuda de AWS).
- En la parte inferior está la plantilla que se puede ver en JSON o YAML. Además hay pestañas:
  - Plantilla completa
  - Componentes – Dentro de los componentes sale el que este seleccionado en el panel central. Según el que sea tendrá distintas pestañas superiores, por ejemplo:
    - Propiedades, Metadata, Política de borrado, Dependiente de ..., Condiciones
- En la pestaña superior se puede:
  - Guardar en local o en Amazon S3.
  - Deshacer algún paso.
  - Crear el stack
  - Validar el stack – Que puede validarlo pero que tenga errores.
  - Cerrar

Ejemplo de creación:

Dentro de EC2 puedo arrastrar las instancias. En el diseño tiene una serie de bolas para añadir algunos recursos como:



- VolumeAttachment
- Grupo de seguridad
- Subnet
- Volumen
- Zona de disponibilidad
- Placement Group
- Host
- Network interface

Lo primero que hacer es configurar las propiedades de la instancia. Para ello tendremos que ir a la documentación para ver cuales son las obligatorias. En el caso de la instancia es SecurityGroupIds e ImageId

```

Instancia01
1 {
2   "Resources": {
3     "Instancia01": {
4       "Type": "AWS::EC2::Instance",
5       "Properties": {
6         "InstanceType": "t2.nano",
7         "SecurityGroupIds": "sg-0527f1d8d88d4ff0e",
8         "ImageId": "ami-001e91733d45a953a"
9       }
10    }
11  }
12 }

```

Para crear los parametros, se clicla en un espacio vacío del centro y en componentes nos sale la lista.

Existen parámetros dinámicos para pedir valores del sistema. Se definen en la plantilla. Por ejemplo, podemos añadir en el json que pida tipos de capacidad de volumen y tipos de instancias así:

```
{
  "Parameters": {
    "DiskSize": {
      "Type": "Number",
      "Default" : 5,
      "AllowedValues":[
        5,
        10,
        15
      ],
      "Description" : "Introduce la capacidad del disco."
    },
    "maquina" : {
      "Type": "String",
      "Default" : "t2.micro",
      "Description" : "Introduce el tipo de maquina"
    }
  }
}
```

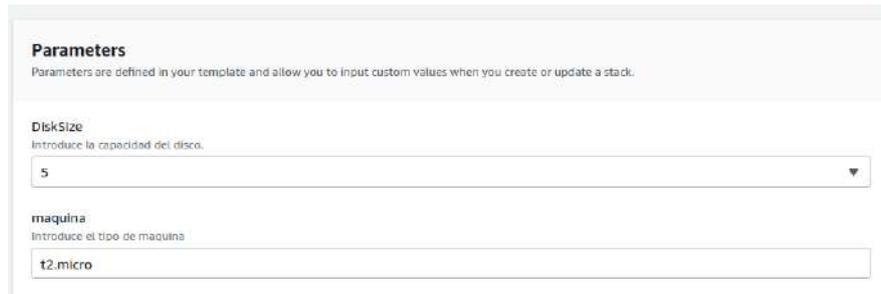
Para ponerlo en los objetos, en el lugar donde va el parámetro va "Ref" : "NombreParametro". Por ejemplo:

```
"Size": {
  "Ref" : "DiskSize"
},
```

y

```
"InstanceType": {
  "Ref": "maquina"
},
```

Cuando creamos el stack lo vemos así:



The image shows a screenshot of the 'Parameters' section in the AWS CloudFormation console. The title is 'Parameters' and the subtitle is 'Parameters are defined in your template and allow you to input custom values when you create or update a stack.' There are two parameters listed: 'DiskSize' with a description 'Introduce la capacidad del disco.' and a value of '5'; and 'maquina' with a description 'Introduce el tipo de maquina' and a value of 't2.micro'.

CloudFormation guarda las plantillas en buckets S3

Un Drifts pertenece a cada uno de los posibles stacks que tengamos. Cuando ejecutas un drift puede tardar un poco. Intenta detectar si se ha producido un cambio después de lanzar un stack.

## TEMA 30 - Compute – Lightsail

Dentro de Compute AWS ofrece distintos servicios:

- **AWS app Runner** – Permite desplegar desde código fuente o desde un contenedor en un entorno escalable, orientado a contenedores.
- **Batch** – Procesa cargas de trabajo en modo batch dentro la nube
- **EC2** – Elastic Compute. Máquinas virtuales
- **EC2 Image Builder** – Constructor de AMIs
- **Elastic Beanstalk** – Implementar y administrar aplicaciones dentro de la nube de AWS sin tener que preocuparse por la infraestructura que las ejecuta.
- **Lambda** – Permite ejecutar código en un entorno serverless.
- **Lightsail** – Entorno destinado a usuarios con menos nivel técnico donde pueden crear instancias, contenedores, BBDD, redes, etc
- **Outpost** – Permite ejecutar servicios de AWS en entornos on-premise.

**Lightsail** tiene 6 tipos de creaciones de componentes de manera rápida:

- **Instances**
  - Podemos seleccionar la zona.
  - Blueprint son entornos preparados con aplicaciones para poderlos crear una instancia rápida con ellos. (Wordpress, LAMP, node.js, Joomla, etc). El principal preparador de estas instancias es Bitnami, una empresa que se dedica a las librerías de instaladores o paquetes de software para aplicaciones web y stacks de software.
  - Se puede añadir un script de lanzamiento.
  - Se puede añadir un SSH key pair. Se puede usar por defecto o subir una clave.
  - Se pueden automatizar snapshots (Backups)
  - Se escoge el plan económico.
  - Se pueden añadir tags sin valor o con valor.
- **Containers** – Podemos crear nuestros contenedores Docker, como si fuese ECS (Elastic Containers Services) o EKS (Elastic Kubernetes Services) pero con una gestión simple.
  - Escogemos la region para trabajar.
  - Escogemos las características
  - Cuantos nodos queremos

- Podemos escoger la aplicación a desplegar en los contenedores. Ofrece Hello World, Nginx y Redis, pero también podemos especificarla de docker hub. Aquí también se especifican variables, puertos, etc
- **Databases** – La creación es bastante parecida a la opción “easy” de RDS.
  - Podemos escoger entre MySQL y PostgreSQL
  - Definimos las credenciales de acceso y el nombre de la BBDD maestra.
  - Nos preguntan si queremos standard o alta disponibilidad.
  - Los distintos planes de precios.
  - Podemos identificar la BBDD y crear tags.
- **Networking** – Se puede crear
  - **IP estática.** Es una elastic IP.
  - **Balanced de carga** de HTTP y HTTPS
  - **CDN** (Content Delivery Netowrk), que se puede crear con cloudFront. Lo que hace básicamente es acercar los datos y los componentes a local (Pequeños CPD que tiene amazon cerca de ciudades). Con esto se mejora la latencia. Se escoge el origen, la cache, la distribución y la identificación de la distribución.
  - **Zona DNS** – Con un dominio propio registrado se puede crear nuestra zona. En Amazon es Route 53.
- **Storage** – Podemos crear
  - Buckets
  - Discos
- **Snapshots**

Cuando creamos estos componentes tendremos unos paneles simples para poder gestionarlos, ver métricas, conectarnos a ellos, etc

En los contenedores se pueden subir imagenes personalizadas de docker desde local usando AWS CLI. Hay que tener en cuenta que debemos tener un contenedor creado en Lightsail, debemos tener la imagen construida en docker local (A través de Dockerfile o como se quiera) y necesitamos el plugin “Lightsail control”. El comando para subir la imagen:

```
aws lightsail push-container-image --region <nombre-region> --service-name <nombre-contenedor-en-lightsail> --label <nombre-nuevo-contenedor> --image <nombre-imagen-docker>
```

Esto hace un push en el entorno de contenedores de LightSail para tener la imagen en LighSail.



## TEMA 31 - Compute – Elastic Beanstalk

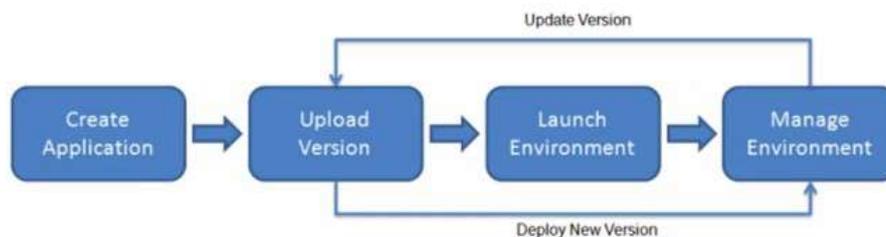
Permite implementar y administrar aplicaciones dentro de la nube de AWS sin tener que preocuparse por la infraestructura que las ejecuta. Se pueden desplegar en python, en node, en java, en go, en .NET, en php y ruby... sin indicarle si necesita un balanceador de carga, un grupo de seguridad... A través de un asistente creará un entorno apropiado a la aplicación.

Reduce la complejidad de la administración sin restringir la libertad de elección ni el control.

Solo tiene que cargar la aplicación y Beanstalk gestionará de manera automática los detalles de aprovisionamiento de capacidad, balanceo de carga, escalado y monitorización de estado de la aplicación.

Los componentes son accesibles para poder modificarlos.

Cuando se implementa la aplicación se crea la versión de la plataforma compatible seleccionada y aprovisiona uno o varios recursos de AWS, como instancias EC2.



Amazon tiene una serie de demos para probar este servicio. Para crearlo podemos detallar las siguientes configuración:

- Nombre y tags
- Plataforma, rama y versión. (.NET, Docker, Go, Java, Node, PHP, Python, Ruby o Tomcat)
- El código de la aplicación. Se puede elegir una aplicación de ejemplo.

Crea un environments para la aplicación. Por ejemplo, en Tomcat crea un bucket, un grupo de seguridad, un target group, crea una instancia en EC2, un grupo de autoescalado, alarmas CloudWatch y un balanceador de carga.

**Demo1-env**  
 Demo1-env.cba-7jymc7lp.eu-west-3.elasticbeanstalk.com [c-ymb4hp2w7k]  
 Application name: demo1

**Health**  
  
 Ok  
 Causes

**Running version**  
 Sample Application  
 Upload and deploy

**Platform**  
  
 Tomcat 8.5 with Corretto 11  
 running on 64bit Amazon Linux  
 2/4.2.18  
 Change

En el sidebar izquierdo podemos ver:

- Ir al environment
- Configuración – Se pueden ver los componentes y editarlos.
- Logs
- Health
- Monitorización
- Alarmas
- Gestionar actualizaciones
- Eventos
- Tags

En la creación, si escogemos subir nuestro propio código, podremos subirla desde local o desde un enlace publico S3. Además podemos taggear la aplicación.

Las configuraciones avanzadas son para el entorno, donde podemos parametrar los siguientes componentes:

- Preajustes (Instancia simple, spot, alta disponibilidad, personalizada...)
- Plataforma Tomcat
- Software
- Instancias – Podemos activar/desactivar el IMDS, que permite acceder a los metadatos de la instancia.
- Capacidad
- Balanceador de carga
- Actualizaciones y despliegues continuos

- Política de despliegue
  - All at once – Es el despliegue más rápido porque actualiza en todas las instancias al mismo tiempo, pero durante ese tiempo la aplicación estará parada.
  - Rolling – No habrá indisponibilidad. Irá actualizando una instancia tras otra. Se puede indicar porcentaje de máquinas en cada actualización o el número de máquinas que actualiza a la vez
  - Rolling with additional batch - Tarda un poco más en acabar la actualización que el anterior, porque creará nuevas instancias para poder atender las peticiones de los usuarios. Se podrá mantener el ancho de banda.
  - Immutable – No actualiza instancias, crea nuevas y vuelve a desplegar la aplicación. Es el que más tarda.

Políticas de implementación admitidas		
Política de implementación	Entornos con balanceo de carga	Entornos de una sola instancia
Todo a la vez	✔ Sí	✔ Sí
Continua	✔ Sí	✘ No
Continua con un lote adicional	✔ Sí	✘ No
Inmutable	✔ Sí	✔ Sí
División de tráfico	✔ Sí (Balanceador de carga de aplicaciones).	✘ No

- Seguridad
- Monitorización
- Gestión de actualizaciones
- Notificaciones
- Red
- BBDD
- Etiquetas

Una vez creado un entorno, podemos pasarlo de single-instance a multi-instance para tener alta disponibilidad. Se haría en capacidad, donde indicamos que queremos balanceo de carga.

Para actualización la aplicación a una nueva versión, entramos dentro de las versiones de la aplicación y clicamos en upload. Una vez lo tenemos subido lo seleccionamos y en “Actions” desplegamos clicando en “Deploy”. Nos dará a elegir el entorno.

El botón de Actions, nos permite en aplicaciones:

- Crear entorno
- Borrar aplicación.

- Ver las versiones
- Salvar la configuración

En los entornos nos permite:

- Salvar la configuración
- Cargar configuraciones guardadas
- Swap environment URLs
- Clonar el entorno
- Reconstruir el entorno
- Reiniciar el servidor de la aplicación.
- Terminar con el entorno

Cabe recordar que se puede entrar en la instancia EC2 de manera normal.

## TEMA 32 - Compute AWS Lambda

Nos permite a trabajar en entorno Serverless.

Ejecuta el código en una infraestructura informática de alta disponibilidad y realiza todas las tareas de administración de los recursos informáticos, incluido el mantenimiento del servidor y del sistema operativo, el aprovisionamiento de capacidad y el escalado automático, así como la monitorización del código y las funciones de registro.

Se puede ejecutar código para prácticamente cualquier tipo de aplicación o servicio de backend.

Está basado en eventos.

El código se ejecuta basado en respuesta a eventos de otros servicios de Amazon como por ejemplo S3, DynamoDB, peticiones HTTP, etc

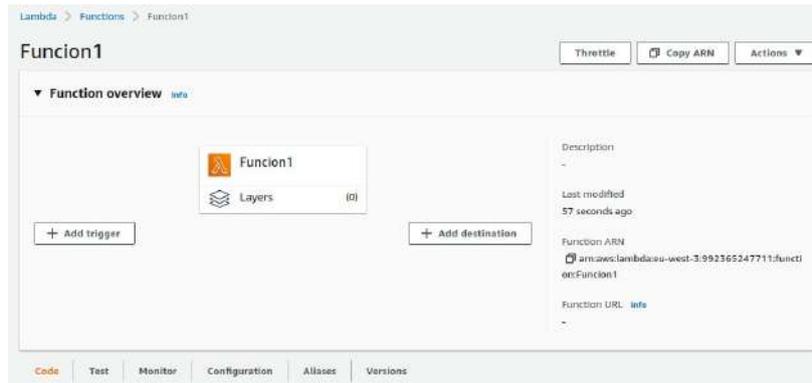
Solo tenemos que poner nuestro código dentro del servicio Lambda, configurar el trigger y esperar a que se reciban los eventos que disparan el trigger.

Los lenguajes que admite Lambda son: NodeJS, t Java, Python, C#, go , etc...

Documentación: [https://docs.aws.amazon.com/es\\_es/lambda/latest/dg/welcome.html?icmpid=docs\\_lambda\\_help](https://docs.aws.amazon.com/es_es/lambda/latest/dg/welcome.html?icmpid=docs_lambda_help)

Si creamos una función Lambda podemos parametrizar:

- 4 opciones
  - Desde scratch. Una prueba con un hola mundo
    - Nombre
    - Se selecciona el lenguaje
    - Roles de ejecución
    - Opciones avanzadas: Firma del código, URL, etiquetas y VPC
  - Con blueprint, que es una plantilla
  - Desde una imagen de contenedor
  - Desde un repositorio de app serverless



Una vez creada, tendremos un panel de control con el trigger, la función y el destino.

Con la función tenemos Layers que nos permite implementar librerías, dependencia, etc..

En la parte de abajo veremos las pestañas:

- Code – El código fuente. Aparece en un editor parecido a Cloud9.
- Test – Podemos enviar un evento para probar si funciona correctamente. Crear uno o utilizar alguno guardado.
- Monitor – Podemos ver Métricas, logs y trazas.
- Configuration – Aquí tenemos toda la configuración.
  - Configuración general
  - Triggers
  - Permisos
  - Destinos
  - URL
  - Variable de entorno
  - Etiquetas
  - VPC
  - Monitorización y herramientas de operaciones
  - Concurrencia
  - Invocación asíncrona
  - Firma de código
  - Proxy BBDD
  - Sistema de ficheros
  - Estado de las máquinas

- Aliases – Nombre alternativos que podemos darle a la Lambda y que pueden apuntar a determinadas versiones.
- Versiones

El código de prueba en node de hola mundo desde scratch:

```
exports.handler = async (event) => {
  // TODO implement
  const response = {
    statusCode: 200,
    body: JSON.stringify('Hello from Lambda!'),
  };
  return response;
};
```

Export.handler es la función que inicia todo el proceso del Lambda cuando recibe el evento.

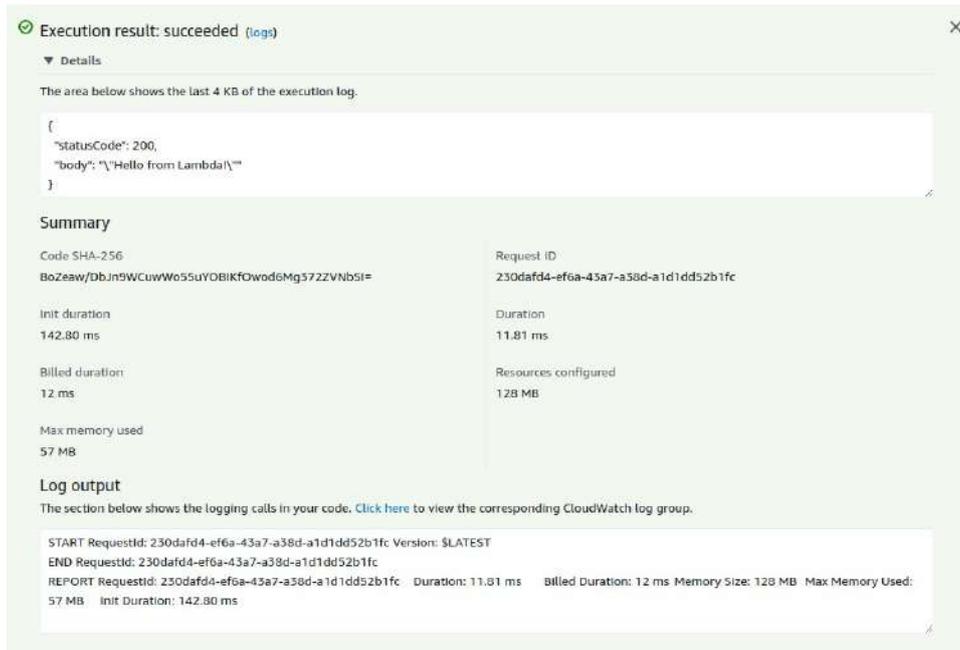
Se crea una constante llamada response con dos campos: StatusCode entero y body con un print de Hola mundo.

Por último devuelve el componente

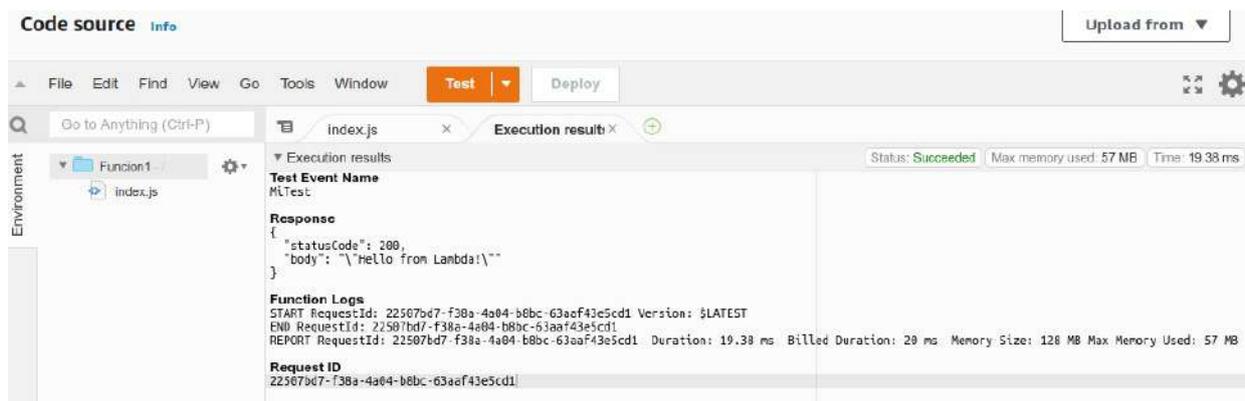
El código de test por defecto:

```
{
  "key1": "value1",
  "key2": "value2",
  "key3": "value3"
}
```

En este caso no prueba nada de la aplicación porque no da ningún valor que interprete. En todo caso si aplicamos el test la aplicación retorna su constante. Pantalla del testeo desde pestaña “Test”



Resultado del testeo desde pestaña “Code”:



El código de prueba en python de hola mundo desde scratch:

```
import json
def lambda_handler(event, context):
    # TODO implement
    return {
        'statusCode': 200,
        'body': json.dumps('Hello from Lambda!')
    }
```

### 32.1. - Conceptos

- **Handler** – Es el fichero main, el que se ejecutará el primero cuando se reciba el evento. Desde este fichero se iniciarán el resto.

- **Evento** – Son los parámetros de la función, los que se tratarán.
- Las funciones Lambda pueden ser invocadas por eventos externos o por internos como SNS, S3, CloudFormation, etc. En el segundo caso los eventos son específicos, los parámetros que lanzan según el servicio se tendrán que consultar en la documentación:  
<https://docs.aws.amazon.com/lambda/latest/dg/lambda-services.html>
- **Contexto** – Es el entorno donde se lanza la versión Lambda. Por ejemplo, tenemos en la documentación el contexto de cuando se trabaja con Python:  
<https://docs.aws.amazon.com/lambda/latest/dg/python-context.html>

Tanto el evento como el contexto se pueden utilizar para realizar procesos en la función.

## 32.2. - Probando blueprint

Como ejemplo usaremos la función “Get S3 object”..:

- Le ponemos nombre, creamos rol y plantilla de políticas.
- Seleccionamos bucket (Tiene que estar en la misma region que la función), tipo de evento, prefijo, sufijo...

El código es el siguiente:

```
import json
import urllib.parse
import boto3

print('Loading function')

s3 = boto3.client('s3')

def lambda_handler(event, context):
    #print("Received event: " + json.dumps(event, indent=2))

    # Get the object from the event and show its content type
    bucket = event['Records'][0]['s3']['bucket']['name']
    key = urllib.parse.unquote_plus(event['Records'][0]['s3']['object']['key'], encoding='utf-8')
    try:
        response = s3.get_object(Bucket=bucket, Key=key)
        print("CONTENT TYPE: " + response['ContentType'])
        return response['ContentType']
    except Exception as e:
        print(e)
        print('Error getting object { } from bucket { }. Make sure they exist and your bucket is in the
same region as this function.'.format(key, bucket))
        raise e
```

Los import son los módulos que necesita para poder trabajar: Con json, con url y con amazon.

Prepara la conexión s3 en una variable.

Dentro de la función lambda prepara en la variable bucket los datos que quiere recolectar del event: Records, la posición 0, dentro de s3, dentro de bucket, dentro del nombre. Recorre el documento json hasta el dato que le interesa.

Prepara la variable key con la url, la librería parse y dentro el evento

Una vez se tiene preparadas las anteriores variables, prepara la variables response con el getObject, que será lo que retornará con el print enviado al return.

Por último hay un except por si falla lo anterior imprime un mensaje de error.

### 32.3. - Ejemplo de trigger

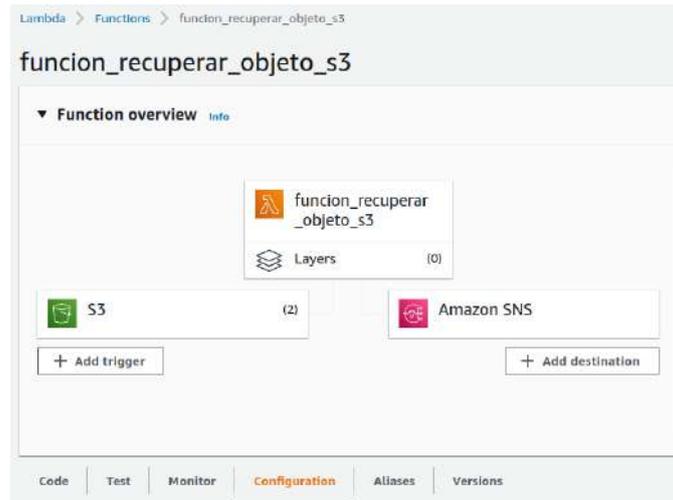
Podemos seleccionar un trigger ya preconfigurado. Si escogemos un bucket de S3 podremos ver la configuración en el bucket concreto, en el apartado de properties en la sección de “Event notifications”. Aquí también podemos crear el evento para lanzarlo contra Lambda, SNS o SQS. Los eventos contra Lambda aparecerán también en el panel de functions de Lambda.

### 32.4. - Ejemplo de destino

Nos permite mandar a otro recurso cierta información. Cuando creamos un destino podemos escoger entre:

- Asincrono (On failure(En caso de fallo) o On succes (Encaso de éxito)) o stream (DynamoDB stream)
- Tipo de destino entre SNS, SQS Lambda o EventBridge event bus (Gestor de eventos de AWS).
- El destino

Ahora, el panel de funciones queda así:



Tiene 2 triggers que recoge la creación y eliminación de objetos en un bucket S3. La función recupera información de los triggers para mostrarla y el destino es un SNS con un correo electrónico.

### 32.5. - Ejemplo con todos los pasos para crear una función, trigger y destino

- Creamos la función con “Author from scratch”, ponemos nombre, escogemos python y decidimos los permisos (Creamos un rol con permisos de lectura en S3).
- Vamos a la parte del código para sustituirlo con lo que queramos que haga la función y le damos a deploy. El código que utilizo es el siguiente:

```
import json
import urllib.parse
import boto3

print('Loading function')

s3 = boto3.client('s3')

def lambda_handler(event, context):
    #print("Received event: " + json.dumps(event, indent=2))

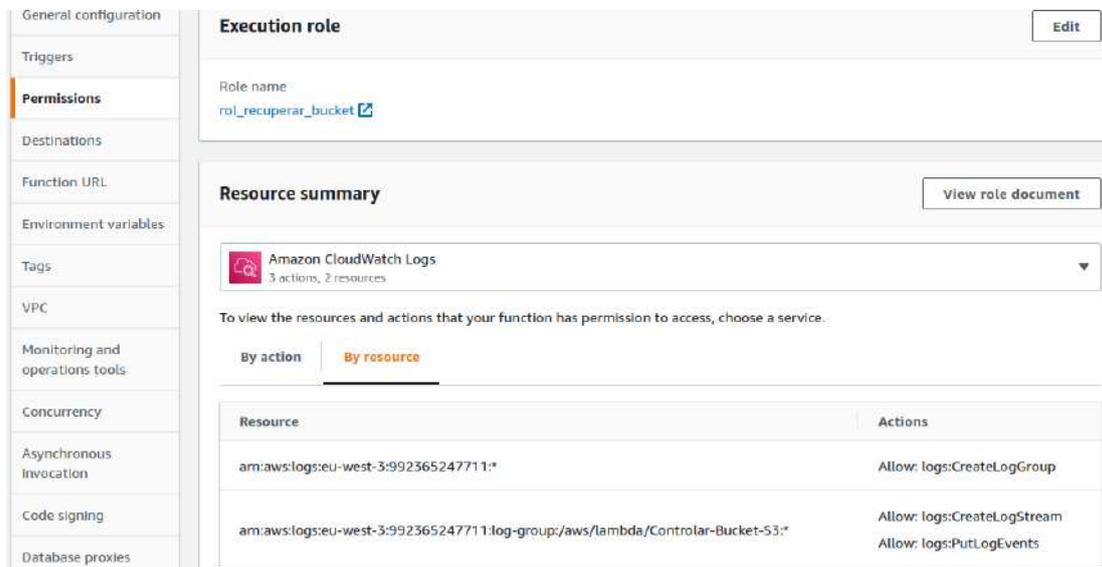
    # Recuperar el objeto y ver su content type
    bucket = event['Records'][0]['s3']['bucket']['name']
    key = urllib.parse.unquote_plus(event['Records'][0]['s3']['object']['key'], encoding='utf-8')
    try:
        respuesta = s3.get_object(Bucket=bucket, Key=key)
        print("Nombre del objeto:"+key)
        print("Tamaño: " + str(respuesta['ContentLength']))
        return "El objeto "+key+ "tiene un tamaño de -->"+str(respuesta['ContentLength'])+" Bytes"
    except Exception as e:
        print(e)
```

```
print('Error al recuperar el objeto {} del bucket {}'.format(key, bucket)). Comproba que existe y que se encuentra en la misma region.'.format(key, bucket))
raise e
```

- Añadimos un trigger, que se disparará cuando se cree un objeto en s3.
- Creamos el topic de las Lambda. Añadimos dos destinos para que mande la información en caso de fallo y otra en caso de éxito, en este caso al mismo SNS.

Si añadimos objetos a nuestro bucket enviará un SNS al correo configurado con el mensaje de la función.

Podemos revisar en “Monitor” las métricas, los logs y las trazas. En el caso de los logs, también podemos verlas en CloudWatch. Si nos vamos a Configuración y entramos en permisos podremos ver que CloudWatch tiene permisos para coger logs (Stream y events) para ponerlos en grupos de logs que va creando.



Podemos ver el role de permisos, que estará el que configuramos expresamente y los que va añadiendo Lambda por ser necesarios.

Si vamos a CloudWatch veremos en el grupo de logs los streams que se han generado por cada evento.

### 32.6. - AWS Step Functions

Es un servicio de orquestación que le permite conectar sus funciones de Lambda en flujos de trabajo sin servidor, denominados máquinas de estado. Cree flujos de trabajo de larga duración para la automatización de TI y los casos de uso de aprobación humana, o cree flujos de trabajo de gran volumen y corta duración para el procesamiento e ingestión de datos en streaming.



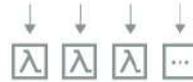
**Chaining**

Connect functions into a series of steps, with the output of one step providing the input to the next step.



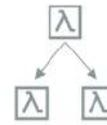
**Catch and retry**

Handle errors using sophisticated catch-and-retry functionality.



**Parallelism**

Run functions in parallel, or use dynamic parallelism to invoke a function for every member of any array.



**Branching**

Design your workflow to choose different branches based on Lambda function output.

## TEMA 33 - SQS – Servicio de mensajes de Amazon

**Amazon SQS** proporciona colas para la mensajería de alto rendimiento entre sistemas. Puede utilizar las colas para desacoplar procesos pesados y para almacenar en búferes y por lotes el trabajo. Amazon SQS almacena los mensajes hasta que los microservicios y las aplicaciones sin servidor los procesan.

### 33.1. - Diferencia SNS vs SQS

Servicio de mensajería como SNS pero más orientado a aplicaciones. La diferencia es que **SNS** es un sistema distribuido publicar-suscribirse. Los mensajes son empujado a los suscriptores cuando los editores los envían a SNS. En cambio, **SQS** esta distribuido hacer cola sistema. Los mensajes son no empujado a los receptores. Los receptores tienen que sondear o tirar mensajes a SQS (pull). Varios receptores no pueden recibir mensajes al mismo tiempo. Cualquier receptor puede recibir un mensaje, procesarlo y eliminarlo. Otros receptores no reciben el mismo mensaje más tarde. El sondeo introduce inherentemente cierta latencia en la entrega de mensajes en SQS, a diferencia de SNS, donde los mensajes se envían inmediatamente a los suscriptores. SNS admite varios puntos finales como correo electrónico, SMS, punto final HTTP y SQS. Si desea que un número y tipo de suscriptores desconocidos reciban mensajes, necesita SNS.

SQS es un sistema distribuido, un receptor recibe el mensaje, lo procesa y lo elimina. No puede haber más receptores.

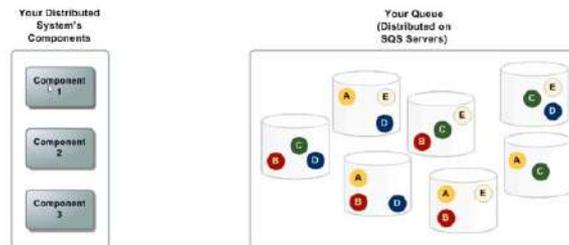


Es un concepto muy utilizado, los primeros sistemas de mensajes eran mainframe de IBM con IBMMQ. En el mundo Java se llaman JMS. Permiten que dos aplicaciones que estén desacopladas puedan compartir información mediante la cola de mensajes del servidor.

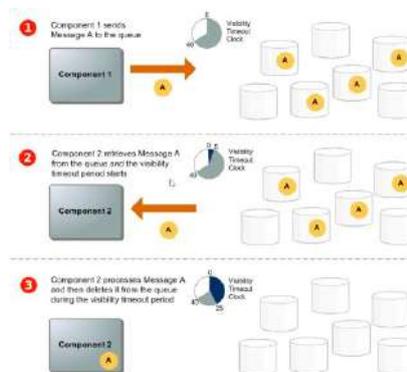
### 33.2. - Tipos de colas de mensajes

- Estandar
  - Tienen un nivel de procesamiento ilimitada.
  - Los mensajes se entregan al menos una vez.
  - El orden de entrega puede ser distinto al del envío. La aplicación tiene que ser consciente de este hecho y tratar el mensaje de forma coherente.
- FIFO – First In First Out
  - Se admiten hasta 300 mensajes por segundo y agrupando se pueden conseguir hasta 3000 mensajes por segundo

- Los mensajes solo se mandan una vez hasta que se procesan y eliminan. No se introducen duplicados
- El orden de entrega es igual al del envío.



El modo de tratar los mensajes SQS es de alta disponibilidad en las colas estándar. Hace duplicados en distintos servidores para asegurar su entrega.



El ciclo de vida de las colas estándar es:

1. Un componente envía un mensaje a la cola de SQS, se reparte entre servidores.
2. Otro componente pide el mensaje con un pull y empieza lo que se llama el VTC (Visibility Timeout Clock). Durante cierto tiempo el mensaje estará oculto mientras que el componente 2 no lo procesa.
3. Cuando el componente 2 procesa el mensaje se elimina de los servidores.

Esta es la manera de trabajar para que el mensaje se envíe solo una vez.

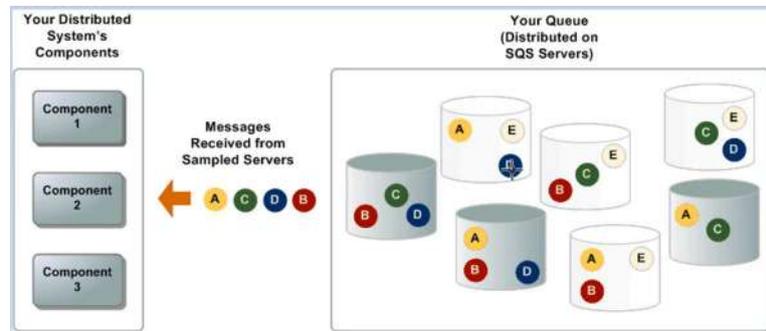
En las colas FIFO solo se envía un mensaje.

### 33.3. - Crear cola standard

Cuando creamos una cola standard podemos configurar:

- Visibility Timeout – El tiempo que está invisible mientras se procesa el mensaje.
- Periodo de retención del mensaje – Los mensajes que no se reclaman se eliminan después de este tiempo.
- Delivery delay – Cuanto espera un mensaje que llega a la cola en estar disponible.
- Capacidad máxima del mensaje.

- Receive message wait time – Determina si hacemos short o long polling (Sondeo corto o largo). Con Short polling se recoge un conjunto de servidores y se devuelve, no mira todos los servidores. Utiliza un proceso aleatorio, con lo que puede quedarse alguno fuera. Si ponemos más de 0 segundos será Long Polling se preguntará a todos los servidores de manera que se devolverán todos los mensajes.



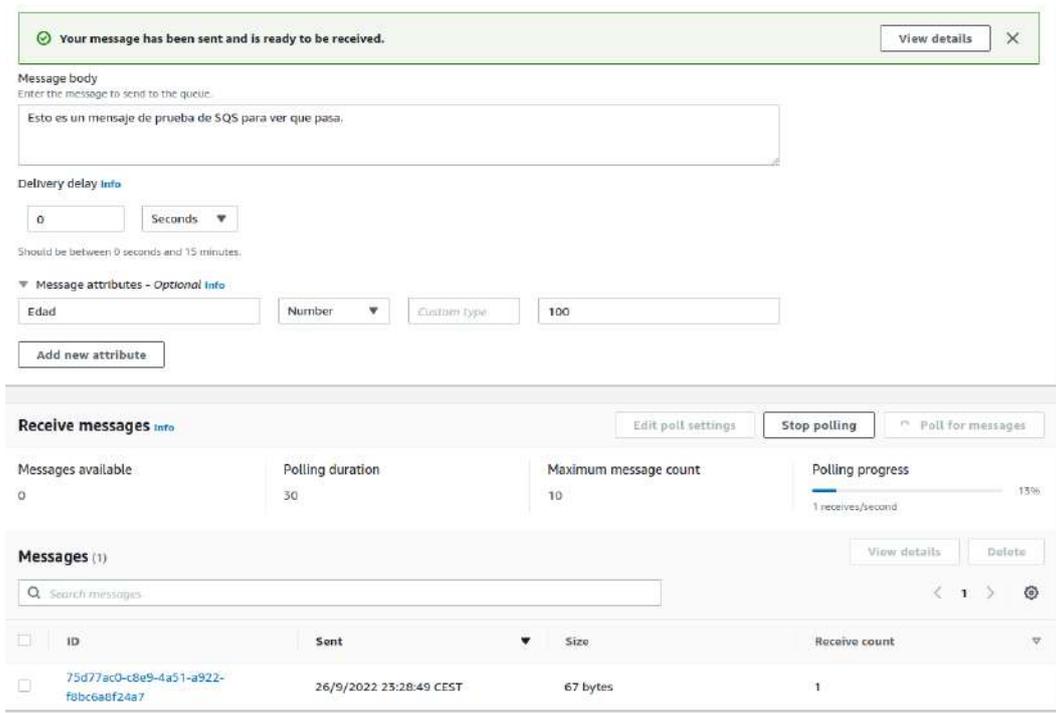
En este ejemplo de short polling vemos que no recoge todos los mensajes, le falta E que lo recogerá en un segundo polling. Short polling es razonable con menos de 1000 mensajes.

- La política de acceso – En basico nos da las opciones de quien puede enviar mensajes y quien puede enviarlos.

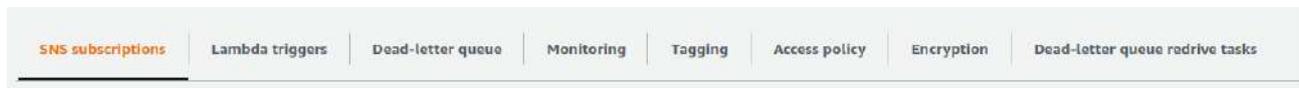
Una vez creada la cola podemos probarla en el botón “Send and receive messages”, indicando:

- Cuerpo del mensaje
- Delivery delay
- Atributos – Podrían ser utilizados para encontrar más información o para dar un valor que se necesite.

Se podrá testear si se envía y también si se puede recoger el mensaje. Una vez recibido el mensaje veremos el que se ha enviado exitosamente.



En las colas tendremos distintas pestañas con componentes



- Suscripciones SNS – Se puede seleccionar un topic para recibir los mensajes.
- Triggers Lambda – Tan solo funcionan con colas standard
- Cola de mensajes muertos – Es una cola donde se pueden enviar los mensajes que no se han procesado correctamente o se hayan rechazado.
- Monitorización
- Etiquetas
- Política de acceso
- Encriptación
- Tareas de colas de mensajes muertos

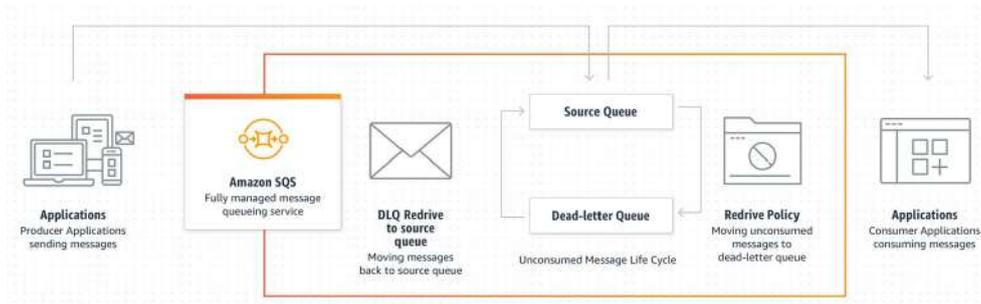
### 33.4. - Crear cola FIFO

Cuando creamos una cola FIFO además de las propiedades standard podemos configurar:

- Content-based deduplication – En cada mensaje le dará un hash para controlar que no hayan repetidos. Si no utilizamos esta opción, el productor del mensaje tendrá que dar a cada mensaje un `messageDeduplicationId` para poder identificar inequívocamente cada mensaje.
- Enable high throughput FIFO – Si lo habilitamos el scope y el límite será por grupo de mensajes.
  - Deduplication scope
    - Por cola
    - por Grupo de mensajes
  - FIFO throughput limit
    - Por cola
    - Por ID de grupo de mensajes.

La deduplicación tiene un tiempo de 5 minutos de control. Pasado ese tiempo deja de controlar si el mensaje ha llegado. A día de hoy este rango no se puede cambiar.

### 33.5. - Cola de mensajes muertos



Las DLQ nos permiten reconducir los mensajes a la cola fuente para volver a procesar.

Para esto necesitamos una cola del mismo tipo que la cola a la que queremos ponerle DLQ (Standard con standard y FIFO con FIFO). Una vez creada, nos vamos a Dead-letter queue de la cola origen y editamos para activar el Dead-letter queue. Indicamos la cola de mensajes incorrecto (La cola creada) y el número de mensajes que queremos que provoque que vaya a la cola de incorrectos.

Ahora, en la cola de mensajes incorrectos, marcamos DLQ redrive indicando que los mande a la cola original. Podríamos indicar otra cola de mensajes.

### 33.6. - Enviar y recibir desde python

**Para enviar** usamos el siguiente programa:

```
import boto3
```

```

# Crear un cliente SQS
sqs = boto3.client('sqs')

# Enviar una mensaje a una cola SQS
def mandar_mensaje(cola,cuerpo,nombre,apellidos):
    response = sqs.send_message(
        QueueUrl=cola,
        DelaySeconds=10,
        MessageAttributes={
            'nombre': {
                'DataType': 'String',
                'StringValue': nombre
            },
            'apellidos': {
                'DataType': 'String',
                'StringValue': apellidos
            }
        },
        MessageBody=cuerpo
    )
    print(response['MessageId'])

```

Entramos en python y importamos el programadores

```
import enviar
```

Luego utilizamos el método de dentro del programa añadiendo los argumentos que se deseen. El primero debe ser el enlace de la cola.

```
enviar.mandar_mensaje("https://sqs.eu-west-3.amazonaws.com/992365247711/Cola-standard","Esto es un mensaje de prueba desde python","Rosa","Rodriguez");
```

Y ya podremos comprobar que se ha enviado.

**Para recibir** usamos el siguiente programa:

```

import boto3

# Create SQS client
sqs = boto3.client('sqs')

def recibir_mensaje(cola):
# Recibir un mensaje de la cola

```

```

response = sqs.receive_message(
    QueueUrl=cola,
    AttributeNames=[
        'SentTimestamp'
    ],
    MaxNumberOfMessages=1,
    MessageAttributeNames=[
        'All'
    ],
    VisibilityTimeout=0,
    WaitTimeSeconds=0
)

message = response['Messages'][0]
receipt_handle = message['ReceiptHandle']

# Borrar el mensaje que hemos recibido
sqs.delete_message(
    QueueUrl=cola,
    ReceiptHandle=receipt_handle
)

print('El mensaje ha sido recibido y borrado: %s' % message)

```

Este programa va a devolver tan solo un mensaje, en plano de pruebas nos sirve, pero en un entorno real no es adecuado.

Entonces, importamos en python el programa

```
import recibir
```

Utilizamos el método del programa

```
recibir.recibir_mensaje("https://sqs.eu-west-3.amazonaws.com/992365247711/Cola-standard");
```

## TEMA 34 - EKS Elastic Kubernetes Service

Puede ser montado con instancias normales o con fairgate (Entorno sin servidor).

Como todo clúster de Kubernetes se creará un servidor maestro y el resto serán servidores workers.

Antes de crear un clúster tendremos que tener:

- Creada la red
- Roles IAM para el clúster:
  - Uno para el servidor maestro
  - Uno para los servidores workers

Necesitaremos una VPC para EKS con algunas peculiaridades deseables. Algunas opciones:

- Redes públicas y redes privadas. Normalmente 2 de cada. Deben estar en distintas AZ para mantener el alta disponibilidad.
- 3 redes públicas distribuidas en distintas AZ. Entornos de desarrollo y no críticas
- 3 redes privas distribuidas en distintas AZ. Entornos de desarrollo y no críticas

Lo interesante es desplegar plantillas de CloudFormation para estas opciones:

<https://docs.aws.amazon.com/eks/latest/userguide/creating-a-vpc.html>

Con estas plantilla podemos crear la red fácilmente con CloudFormation. Por ejemplo, la plantilla de 3 redes públicas creará:

- La VPC
- Las subredes
- Tablas de rutas
- Internet Gateway
- Un grupo de seguridad

Para crear el **rol de IAM del maestro** iremos a roles (dentro de IAM). Seleccionamos en “AWS service”, entre los casos de uso “EKS” y EKS cluster. Por defecto, en los permisos pone “AmazonEKSClusterPolicy de tipo de gestión. Le ponemos un nombre que le identifique: rol-eks-master.

Para crear el **rol de IAM de los workers** le daremos permisos con EC2 y buscaremos las siguientes políticas:

- AmazonEC2ContainerRegistryReadOnly
- AmazonEKS\_CNI\_Policy
- AmazonEKSEWorkerNodePolicy

Le ponemos un nombre que le identifique: rol-eks-nodos

Siempre conviene mirar la documentación porque puede cambiar las políticas:

<https://docs.aws.amazon.com/eks/latest/userguide/add-user-role.html>

### 34.1. - Crear un cluster

Ahora que ya tenemos la red y el IAM podemos crear el clúster. En el primer paso crearemos el controlplane, el maestro. Para crear sin gestionar muchos parámetros podemos configurar:

- Nombre y versión de kubernetes
- Ahora nos pide el rol para el servicio, que debe ser el preparado para el master. Si lo tenemos preparado ya aparecerá.
- Luego podemos encriptar los secrets
- Ahora indicamos la red, que debe ser apropiada, como las plantillas que ofrece AWS. Podemos crear un grupo de seguridad o el que creo la plantilla.
- Indicamos si queremos un endpoint público o no
- Nos pregunta sobre la configuración de logs

Una vez creado podemos entrar para ver sus propiedades:

- **Overview** – Detalles del cluster
  - API server endpoint – Será la entrada por donde ejecutaremos las ordenes.
  - Certificate authority – Es el que tendremos que usar para conectarnos
  - OpenID Connect provider URL
  - Cluster IAM role ARN
  - Cluster ARN
- **Resources** -
  - Workloads
  - Cluster
  - Service and networking
  - Config and secrets
  - Storage
  - Authentication
  - Authorization
  - Policy

- Extensions
- **Compute** – Gestionaremos y veremos los workers
- **Networking** – Veremos la VPC con las subnets, el grupo de seguridad y otros detalles de red.
- **Add-ons** – Por defecto, en un cluster vienen coredns, kube-proxy y vpc-cni.
- **Authentication** -
- **Logging** -
- **Update history** -
- **Tags** -

## 34.2. - Crear workers

En la pestaña “Compute” podremos lanzar grupos de nodos. Podremos especificar:

- Nombre
- Node IAM role. Debe ser el preparado para los workers
- Launch template – Es una plantilla de tipos de EC2.
- Kubernetes labels
- Kubernetes taints - Es una propiedad, una clave, para que el pod sea lanzado o no.
- Tags

Después podemos configurar compute y la autoescalada.

- Tipo de AMI
- Tipo de capacidad – On-Demand o spot (Para pruebas lo más económico son las spot)
- Tipo de instancia
- Capacidad del disco
- Número de nodos deseados
- Número de nodos mínimos
- Número de nodos máximos
- Número de nodos indisponibles (Puedo indicar el número o el porcentaje)

En el siguiente paso indicamos las propiedades de red.

- Subnets
- Configuración del acceso por SSH

- Indicamos la Key pair
- Habilitar accesos para...
  - Grupos de seguridad
  - Todo

Al final podemos hacer una revisión de toda la configuración que hemos hecho en el asistente.

Ahora, dentro del clúster, en la pestaña de “Compute”, podremos ver el grupo de nodos creado. Si entramos veremos las siguientes pestañas:

- Detalles
- Nodes
- Health issues
- Kubernetes labels
- Update configuraKubernetes taints –
- Update history
- Tags

En EC2 se podrán ver las instancias desplegadas. Al final, es un grupo de autoescalada dentro del EKS.

### 34.3. - AWS CLI con EKS

Deberíamos comprobar si tenemos las claves correcta y si estamos en la region.

aws configure

```
administrador@ubuntudocker:~$ aws configure
AWS Access Key ID [*****MNYK]:
AWS Secret Access Key [*****jvm/]:
Default region name [eu-west-3]:
Default output format [None]:
administrador@ubuntudocker:~$
```

Para trabajar con eks es con el comando

aws eks

Documentación: <https://awscli.amazonaws.com/v2/documentation/api/latest/reference/eks/index.html>

Subcomandos:

associate-encryption-config

associate-identity-provider-config

create-addon  
create-cluster  
create-fargate-profile  
create-nodegroup  
delete-addon  
delete-cluster  
delete-fargate-profile  
delete-nodegroup  
deregister-cluster  
describe-addon  
describe-addon-versions  
describe-cluster  
describe-fargate-profile  
describe-identity-provider-config  
describe-nodegroup  
describe-update  
disassociate-identity-provider-config  
get-token  
list-addons  
list-clusters  
list-fargate-profiles  
list-identity-provider-configs  
list-nodegroups  
list-tags-for-resource  
list-updates  
register-cluster  
tag-resource  
untag-resource  
update-addon  
update-cluster-config  
update-cluster-version  
update-kubeconfig  
update-nodegroup-config  
update-nodegroup-version  
wait

Comandos destacados:

Listar los clústers activos:

```
aws eks list-clusters
```

Listar los grupos de nodos de un clúster

```
aws eks list-nodegroups --cluster-name <nombre-cluster>
```

Información de un cluster

```
aws eks describe-cluster --name <nombre-cluster>
```

Información sobre un grupo de nodos

```
aws eks describe-nodegroup --cluster-name <nombre-cluster> --nodegroup <nombre-nodegroup>
```

## 34.4. - kubectl

Para configurar la conexión desde kubectl al cluster deberemos utilizar:

- API server endpoint
- Certificate authority

Se puede configurar mediante el fichero config de .kubectl. Pero para hacerlo más fácil, también se puede hacer desde AWS CLI generando la configuración con el comando:

```
aws eks update-kubeconfig --name <nombre-cluster>
```

Si tenemos una configuración creada tendremos que borrar el fichero .kube/config para que se pueda añadir el nuevo.

En el archivo de configuración podemos ver los siguientes datos:

apiVersion: v1

clusters:

- cluster:

```
certificate-authority-data: LS0tLS1CRUdJ*****
```

```
server: https://6C*****.sk1.eu-west-3.eks.amazonaws.com
```

```
name: arn:aws:eks:eu-west-3:99*****:cluster/EKS1-redes-publicas
```

contexts:

- context:

```
cluster: arn:aws:eks:eu-west-3:99*****:cluster/EKS1-redes-publicas
```

```
user: arn:aws:eks:eu-west-3:99*****:cluster/EKS1-redes-publicas
```

```
name: arn:aws:eks:eu-west-3:99*****:cluster/EKS1-redes-publicas
```

```

current-context: arn:aws:eks:eu-west-3:99*****:cluster/EKS1-redes-publicas
kind: Config
preferences: {}
users:
- name: arn:aws:eks:eu-west-3:99*****:cluster/EKS1-redes-publicas
  user:
    exec:
      apiVersion: client.authentication.k8s.io/v1beta1
      args:
        - --region
        - eu-west-3
        - eks
        - get-token
        - --cluster-name
        - EKS1-redes-publicas
      command: aws

```

El current-context es importante porque indica cual es el cluster por defecto, en casa de tener más de uno. En principio se quedará siempre el último cluster creado.

Ahora, si pedimos la versión a kubectl nos dirá también si estamos conectados al cluster

```
kubectl version
```

Si le pedimos los nodos veremos los de AWS

```
kubectl get nodes
```

### 34.4.1. - Crear un despliegue con kubectl

Primero creamos un namespace

```
kubectl create namespace <nombre-namespace>
```

Ver los namespace

```
kubectl get ns
```

Vamos a poner el namespace creado por defecto

```
kubectl config set-context --current --namespace=<nombre-namespace>
```

Vamos a efectuar un despliegue

```
kubectl create deployment apache1 --image=httpd
```

Vamos a ver los despliegues

```
kubectl get deploy
```

Vemos los replicaset

```
kubectl get rs
```

Vemos los pods

```
kubectl get pods
```

Podemos ver logs del pod

```
kubectl logs <nombre-pod>
```

Ahora, si vamos al dashboard de AWS y entramos en el cluster, en la pestaña Resources, en el apartado Workloads/pods, veremos el pod creado. Podemos entrar dentro y ver detalles.

Para probar el apache tendremos que crear un servicio de kubernetes. Primero exponemos el despliegue

```
kubectl expose deploy apache1 --port=80 --name=apache1-svc --type=LoadBalancer
```

Podemos comprobarlo en

```
kubectl get svc
```

Aquí nos dará la dirección para poder entrar en apache. Puede tardar unos minutos.



**It works!**

Vamos a cambiar la página index de apache.

```
Kubectl exec -it <nombre-pod> -- bash
```

Entonces entramos dentro del contenedor. Aquí vamos a cambiar el texto del index con

```
echo "Esto es una prueba" > htdocs/index.html
```



## 34.5. - Borrar cluster

Tenemos que seguir el sentido contrario de la creación. A veces nos genera algún error por los grupos de seguridad o por otros componentes. Es importante que esperemos el borrado de cada servicio/componente para seguir borrando el siguiente.

1. Borramos el nodegroup – Dentro del clúster, en la pestaña Compute
2. Borramos el cluster – (Dentro del cluster)
3. Borramos la red – Igual que lo creamos, desde CloudFormation borramos el stack

## TEMA 35 - ECS Elastic Container Service

Comentario inicial: En el servicio ECS, a fecha de septiembre de 2022, su interfaz se encontraba en transición de diseño, con lo cuál tiene muchas posibilidades que en un periodo breve de tiempo no corresponda con las descripciones aquí mencionadas.

Un entorno para trabajar con contenedores de manera sencilla. Se pueden lanzar contenedores docker dentro de un entorno controlado, y da algunas funcionalidades más que Docker puro.

Se pueden crear:

- Clusters. Pero no son como Kubernetes. Ahora es un poco distinto el asistente, antes AWS daba 3 opciones: Solo con red, EC2 Linux + Red y EC2 Windows + Red
- Tareas – Son fichero json para ejecutar contenedores.

### 35.1. - Crear un cluster

Podemos configurar:

- Nombre y la red (VPC + subnet)
- Infraestructura
  - AWS Fargate (Serverless)
  - Amazon EC2
  - Instancias externas
- Monitorización y Tags

Una vez creado podemos entrar y movernos entre las pestañas:

- Services
- Tasks
- Infraestructure – Aparecen las instancias desplegadas.
- Metrics
- Tags

### 35.2. - Crear una tarea

Una tarea es una plantilla en donde definimos como será el despliegue de los contenedores.

En Task definition escribiremos los detalles de la tarea. Tenemos que crear una nueva con las siguiente opciones:

- Nombre

- Datos del contenedor. Nombre, URI de la imagen, puertos, variables de entorno y fichero de entorno. Se puede añadir más contenedores
- Entorno
  - Entorno de la app – Podemos escoger Fargate (serverless) o Instancia EC2
  - Sistema operativo – Linux lo mejor.
  - Capacidad de la tarea (CPU y memoria). Se puede añadir otro contenedor
  - Rol de la tarea. Puede que los contenedores utilicen servicios de Amazon, se debería añadir un rol IAM que pueda hacer llamadas a AWS
  - Rol de ejecución de la tarea
  - Network mode – Bridge, Host, awsvpc, none. Por defecto viene awsvpc
- Almacenamiento – Se puede especificar un almacenamiento efímero de entre 21 GiB y 200 GiB. Además, se pueden asociar volúmenes
- Monitorización y logueo
- Etiquetas

Para lanzar la tarea vamos dentro del clúster, en la pestaña task, clicamos en “Run new task”. También podemos lanzarla en Task definition. Podemos indicar:

- El entorno -
  - Estrategia del proveedor de capacidad – Se le puede dar más detalles
  - Tipo de lanzamiento (Fargate, EC2 o External)
- Configuración del despliegue
  - Definimos el tipo de aplicación – Servicio o tarea.
  - Podemos decir las tareas deseadas.
- Red – Concretamos la VPC, subredes, grupo de seguridad y si queremos IP pública.
- Anulación de tareas -
  - Un rol que permite a los contenedores de la tarea realizar solicitudes a los servicios AWS.
  - Un rol de ejecución de la tarea
- Etiquetas

Una vez lanzada podemos ver la ip pública y si entramos veremos el servicio apache

Para borrar la tarea primero tendremos que pararla. Hay que diferenciar entre la «Definición de tarea» y la «Tarea».

### 35.3. - Crear un servicio

Tenemos que ubicarnos en el clúster, en la pestaña de servicios, y clicamos en “Deploy”. El asistente es el mismo que las tareas. Podremos configurar:

- El entorno -
  - Estrategia del proveedor de capacidad – Se le puede dar más detalles
  - Tipo de lanzamiento (Fargate, EC2 o External)
- Configuración del despliegue
  - Definimos el tipo de aplicación – Servicio o tarea.
  - Especificar la revisión manualmente.
  - Nombre del servicio
  - Tareas deseadas
  - Tareas mínimas en ejecución
  - Tareas máximas en ejecución
  - Utilice el interruptor de despliegue de Amazon ECS
    - Retirada en caso de fallo
- Red – Concretamos la VPC, subredes, grupo de seguridad y si queremos IP pública.
- Balanceador de carga
- Emplazamiento de tareas - personalizar cómo se colocan las tareas en las instancias de su clúster. [https://docs.aws.amazon.com/es\\_es/AmazonECS/latest/developerguide/task-placement-strategies.html](https://docs.aws.amazon.com/es_es/AmazonECS/latest/developerguide/task-placement-strategies.html) Podemos elegir: AZ balanced spread, AZ balanced binpack, Binpack, Una tarea por host, Al azar o Personalizado
- Etiquetas

Si entramos en el servicio podremos ver:

- Health & metrics
- Logs
- Configuration and tasks
- Deployments and events
- Networking
- Tags

## TEMA 36 - ECR Elastic Container Registry

AWS cobra por el espacio de almacenamiento y por la entrada y salida. Tiene dos tipos de registros: Público y privado.

Dentro de los registros tendremos repositorios. Y dentro de cada repositorio tendremos distintas versiones de la misma imagen.

Un registro público tendrá un alias para facilitar el acceso desde internet. Hasta que no creamos el primer repositorio no tendremos el alias, que lo da AWS. Podemos tener uno personalizado si lo solicitamos a soporte. Lo primero es configurar un repositorio.

### 36.1. - Crear repositorio público

Podremos parametrizar los siguientes componentes:

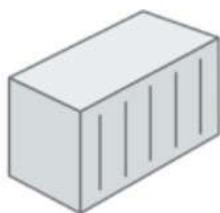
- Privado o público – Una vez creado no se podrá cambiar.
- Nombre repositorio
- Subir logo
- Descripción
- Asociar a un sistema operativo y a una arquitectura
- Descripción más detallada
- Descripción del uso

La creación es inmediata. Una vez entramos podemos subir las imágenes. Podremos ver:

- Comandos push – Resumen de los comandos necesarios para subir imágenes
- Eliminar repositorio
- Acciones (Ver imagen, permisos, detalles o etiquetas. Editar).

Dentro del repositorio podremos ir a la lista pública que recuerda a docker hub. Es la ECR Public Gallery.

Amazon ECR Public Gallery > x5z2u4c6 > x5z2u4c6/mi-apache



x5z2u4c6/mi-apache (0 downloads)

Choose an Image ▼ Copy

Prueba de repositorio de Imagen Apache

OS/Arch: Linux, x86-64

About Usage Image tags

About the repository

## 36.2. - Crear una imagen de Docker

Utilizaremos la imagen para probar push, siguiendo los comandos:

1. Recuperar token de autenticación y autenticar cliente Docker en su registro:

```
aws ecr-public get-login-password --region us-east-1 | docker login --username AWS --password-stdin public.ecr.aws/x5z2u4c6
```

Nota: Ante un error asegurar de que la versión de AWS CLI y de Docker son recientes.

2. Construir imagen Docker utilizando el siguiente comando (Tendremos que tener el Dockerfile preparado en la ubicación del prompt):

```
docker build -t mi-apache .
```

Comprobar que se ha creado:

```
docker images
```

3. Después de que la construcción se complete, etiquetar imagen para push al repositorio:

```
docker tag mi-apache:latest public.ecr.aws/x5z2u4c6/mi-apache:latest
```

4. Ejecutar push de la imagen:

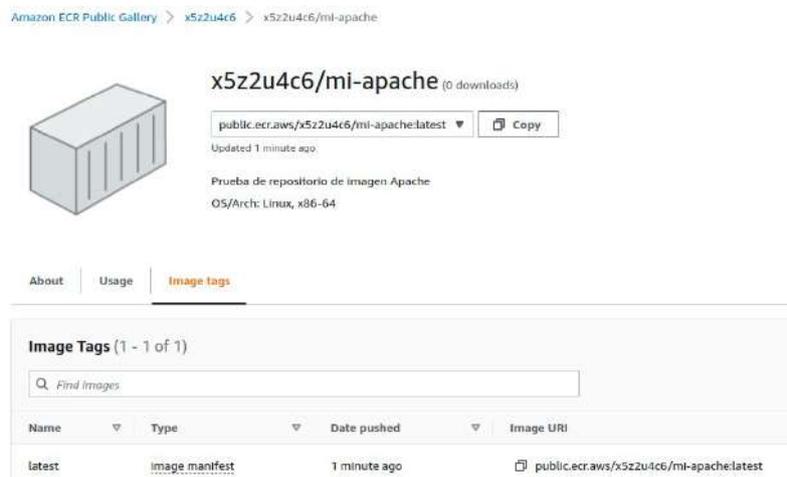
```
docker push public.ecr.aws/x5z2u4c6/mi-apache:latest
```

```

administrador@ubuntuodocker:~/pruebas_aws/docker$ docker build -t mi-apache .
[+] Building 13.6s (8/8) FINISHED
=> [internal] load build definition from Dockerfile
=> [internal] load dockerfile Dockerfile
=> [internal] load .dockerignore
=> [internal] transfer context: 2B
=> [internal] load metadata for docker.io/library/ubuntu:latest
=> [internal] load metadata for registry-1.docker.io
=> [internal] load metadata for registry-1.docker.io
=> [internal] resolve docker.io/library/ubuntu:sha256-2f1ca271b01de722f2c42be5922600c4d794270f639e4a6e91c
=> [internal] fetch sha256-2f1ca271b01de722f2c42be5922600c4d794270f639e4a6e91c: 39.43MB / 39.43MB
=> [internal] sha256-2f1ca271b01de722f2c42be5922600c4d794270f639e4a6e91c: 1.42kB / 1.42kB
=> [internal] sha256-2f1ca271b01de722f2c42be5922600c4d794270f639e4a6e91c: 529B / 529B
=> [internal] sha256-2f1ca271b01de722f2c42be5922600c4d794270f639e4a6e91c: 1.46kB / 1.46kB
=> [internal] extracting sha256-2f1ca271b01de722f2c42be5922600c4d794270f639e4a6e91c: 0/77
=> [2/3] RUN apt-get update && apt-get install -y nginx
=> [3/3] RUN echo "hi" >> /var/www/html/index.html
=> exporting image
=> writing image manifest to docker.io/library/mi-apache
administrador@ubuntuodocker:~/pruebas_aws/docker$ docker images
REPOSITORY          TAG             IMAGE ID        CREATED         SIZE
mi-apache           latest         8485dfc8a091   31 seconds ago 171MB
n8nio/n8n           latest         57b3eda52658   13 days ago    496MB
jenkins/jenkins    lts            cb535f2a7054   4 months ago   464MB
administrador@ubuntuodocker:~/pruebas_aws/docker$ docker tag mi-apache:latest public.ecr.aws/x5z2u4c6/mi-apache:latest
administrador@ubuntuodocker:~/pruebas_aws/docker$ docker push public.ecr.aws/x5z2u4c6/mi-apache:latest
The push refers to repository [public.ecr.aws/x5z2u4c6/mi-apache]
38d5f4b77215: Pushed
ac3be9c52a79: Pushed
7f5cb89cc787: Pushed
latest: digest: sha256:98c2bcab155670fb8d0a9862410ee73bd05757bbee1caca85da418797247d55 size: 948
administrador@ubuntuodocker:~/pruebas_aws/docker$

```

Ahora ya lo tenemos en ECR Public Gallery



Amazon ECR Public Gallery > x5z2u4c6 > x5z2u4c6/mi-apache

x5z2u4c6/mi-apache (0 downloads)

public.ecr.aws/x5z2u4c6/mi-apache:latest

Updated 1 minute ago

Prueba de repositorio de imagen Apache  
OS/Arch: Linux, x86-64

About Usage **Image tags**

Image Tags (1 - 1 of 1)

Find images

Name	Type	Date pushed	Image URI
latest	image manifest	1 minute ago	<input type="button" value="Copy"/> public.ecr.aws/x5z2u4c6/mi-apache:latest

Desde la terminal podemos probar que se lanza la imagen con el comando:

```
docker run --name apache-1 -d -p 80:80 public.ecr.aws/x5z2u4c6/mi-apache
```

Podemos comprobar si está lanzada con

```
docker ps
```

En caso de que queramos descargar la imagen del registro público sería con

```
docker pull public.ecr.aws/x5z2u4c6/mi-apache:latest
```

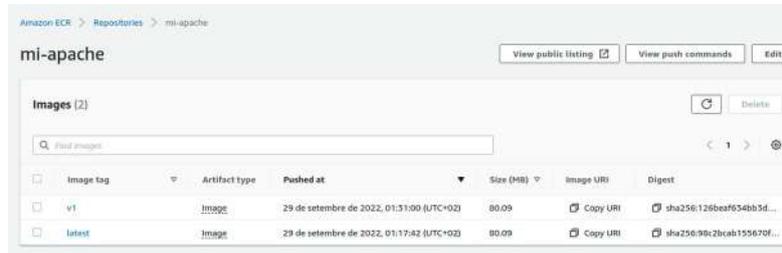
Se puede hacer una segunda versión modificando el Dockerfile y con el siguiente comando que ya indicamos directamente la etiqueta con el nombre completo del registro:

```
docker build -t public.ecr.aws/x5z2u4c6/mi-apache:v1 .
```

Y la volvemos a subir

```
docker push public.ecr.aws/x5z2u4c6/mi-apache:v1
```

Pero en esta ocasión solo subirá la última capa de cambios.



### 36.3. - Probar un despliegue con Lightsail

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

Nos vamos a los contenedores, creamos uno. Tendremos que configurarlo al gusto y en el espacio de deployment tendremos que especificar la imagen indicando:

- Nombre del contenedor que se creará
- Dirección de la imagen pública. La copiaremos de la imagen en el repositorio ECR o de ECR Public Gallery.
- Indicar más comandos si lo necesitamos
- Variables de entorno
- Puerto por donde escuchará el contenedor a la aplicación.

Después es importante indicar cuál es el contenedor que debe escuchar.

### 36.4. - Crear repositorio privado

Para poder utilizar las imágenes en un repositorio privado se requerirá permisos adecuados. Es muy parecida a la creación del repositorio público, las diferencias son:

- En el nombre aparecerá el id de la cuenta.
- Se puede activar la inmutabilidad de los tags.
- Se puede hacer un escaneo a la imagen en el momento de subirla. Se puede escanear a nivel repositorio (Deprecated) y a nivel de registro.
- Además, se puede utilizar la encriptación con su KMS.

Las instrucciones para el push son parecidas pero cambia el nombre de la autenticación.

Para descargar la imagen privada primero nos logueamos y después ya podremos efectuar el pull:

```
aws ecr get-login-password --region eu-west-3 | docker login --username AWS --password-stdin 992365247711.dkr.ecr.eu-west-3.amazonaws.com
```

```
docker pull 992365247711.dkr.ecr.eu-west-3.amazonaws.com/mi-apache:latest
```

## 36.5. - Asignar permisos de acceso

Se pueden dar permisos a nivel de registro o de repositorio para usuarios/grupos/roles concretos.

Dentro del repositorio privado, veremos los permisos en donde podemos subir un json con las políticas. Podemos seguir un asistente que dará al usuario que escojamos los permisos que configuramos de manera fácil.

No solo se pueden dar permisos de nuestra cuenta, también a usuario externos de AWS.

Clicamos en “Add Statement” y configuramos:

- Nombre statement
- Efecto – habilitado o denegado
- Avanzado – Podemos dar permisos a todo el mundo pero no es lo apropiado
- Principal del servicio – Podemos darle permisos a una entidad principal.
- AWS account Ids – Podemos darle permisos a una cuenta principal y se aplicarán a todos los usuarios.
- Entidad IAM – Podemos darselo a un usuario, grupo o rol.
- Actions – Decidimos las tareas concretas que le queremos dar. Por ejemplo, para dar permisos de solo lectura:
  - ecr:DescribeImages
  - ecr:DescribeRepositories
  - ecr:GetDownloadUrlForLayer
  - ecr:ListImages:
- También le podemos dar condiciones

Desde la consola de comandos podemos ver el usuario conectado con

```
aws sts get-caller-identity
```

Si nos conectamos con el usuario con el que tenemos los permisos anteriores, podríamos hacer un pull de la imagen a través de la url.

## 36.6. - AWS CLI

Los comandos principales para ECR son para trabajos con repositorios privados y públicos.

### Repositorios privados:

```
aws ecr
```

Documentación: <https://docs.aws.amazon.com/cli/latest/reference/ecr/index.html>

Los subcomandos son:

```
batch-check-layer-availability
batch-delete-image
batch-get-image
batch-get-repository-scanning-configuration
complete-layer-upload
create-pull-through-cache-rule
create-repository
delete-lifecycle-policy
delete-pull-through-cache-rule
delete-registry-policy
delete-repository
delete-repository-policy
describe-image-replication-status
describe-image-scan-findings
describe-images
describe-pull-through-cache-rules
describe-registry
describe-repositories
get-authorization-token
get-download-url-for-layer
get-lifecycle-policy
get-lifecycle-policy-preview
get-login
get-login-password
get-registry-policy
get-registry-scanning-configuration
get-repository-policy
initiate-layer-upload
list-images
list-tags-for-resource
put-image
put-image-scanning-configuration
put-image-tag-mutability
```

put-lifecycle-policy  
put-registry-policy  
put-registry-scanning-configuration  
put-replication-configuration  
set-repository-policy  
start-image-scan  
start-lifecycle-policy-preview  
tag-resource  
untag-resource  
upload-layer-part  
wait

**Repositorios públicos:**

aws ecr-public

Documentación: <https://docs.aws.amazon.com/cli/latest/reference/ecr-public/index.html>

Los subcomandos son:

batch-check-layer-availability  
batch-delete-image  
complete-layer-upload  
create-repository  
delete-repository  
delete-repository-policy  
describe-image-tags  
describe-images  
describe-registries  
describe-repositories  
get-authorization-token  
get-login-password  
get-registry-catalog-data  
get-repository-catalog-data  
get-repository-policy  
initiate-layer-upload  
list-tags-for-resource  
put-image  
put-registry-catalog-data  
put-repository-catalog-data  
set-repository-policy  
tag-resource  
untag-resource  
upload-layer-part

**Ejemplos:**

Para describir el registro privado:

```
aws ecr describe-registries
```

Para describir repositorios

```
aws ecr describe-repositories
```

Para listar las imágenes de un repositorio

```
aws ecr list-images --repository-name <nombre-repositorio>
```

Para crear un repositorio

```
aws ecr create-repository --repository-name <nombre-repositorio>
```

Se pueden subir imágenes con AWS CLI pero el mismo AWS recomienda que se use el comando DOCKER.

Los comandos que tienen que ver con el subcomando *ecr-public* solo funcionan en la region us-east-1, con lo que hay que especificarla para poder utilizarlos.

Por ejemplo, para describir el registro público:

```
aws ecr-public describe-registries --region us-east-1
```

Podemos pedir los repositorios con:

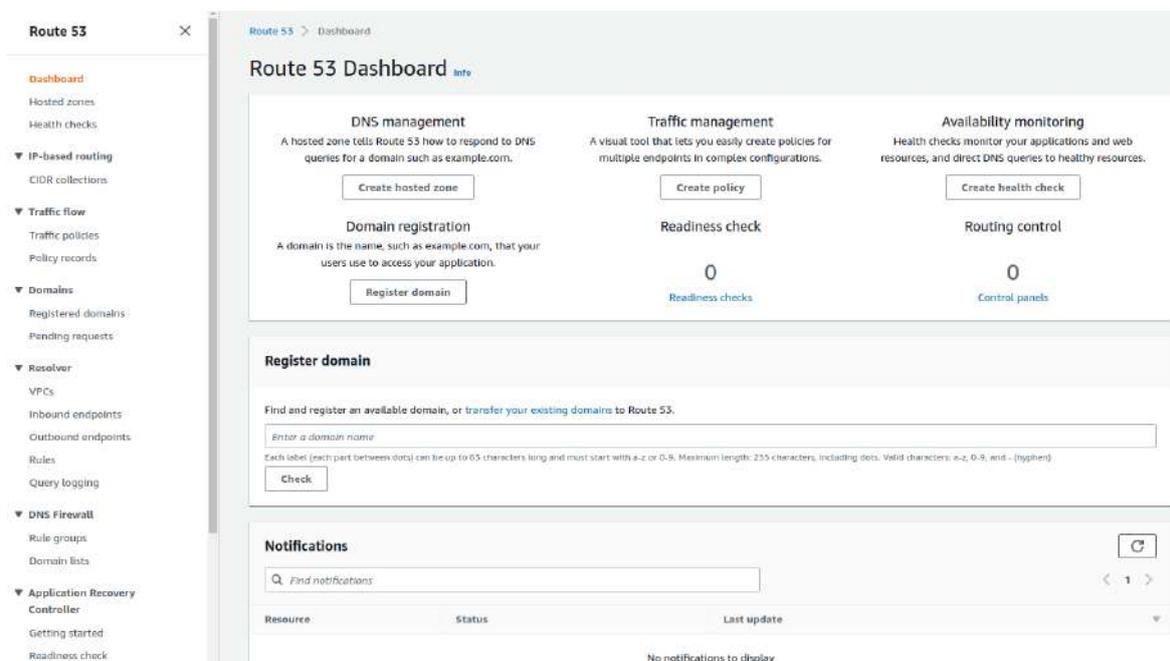
```
aws ecr-public describe-repositories --region us-east-1
```

## TEMA 37 - Route 53

Es un DNS que se integra perfectamente con los productos de AWS. Características:

- Permite toda la **gestión de dominios**. Crear dominios y subdominios, etc
- Configuración de **zonas de host** para responder a peticiones concretas de los dominios.
- Controles de **seguridad** – Monitorización, etc
- **Traffic flow** – es una herramienta que mediante gráficos nos permite crear políticas de acceso de manera que podemos crear configuraciones muy complejas de manera fácil.
- **Resolver** – Va a permitir identificar hacia donde deben ir ciertas peticiones que lleguen a nuestra red.

El Dashboard es muy completo:



En el panel central tenemos las opciones más importantes:

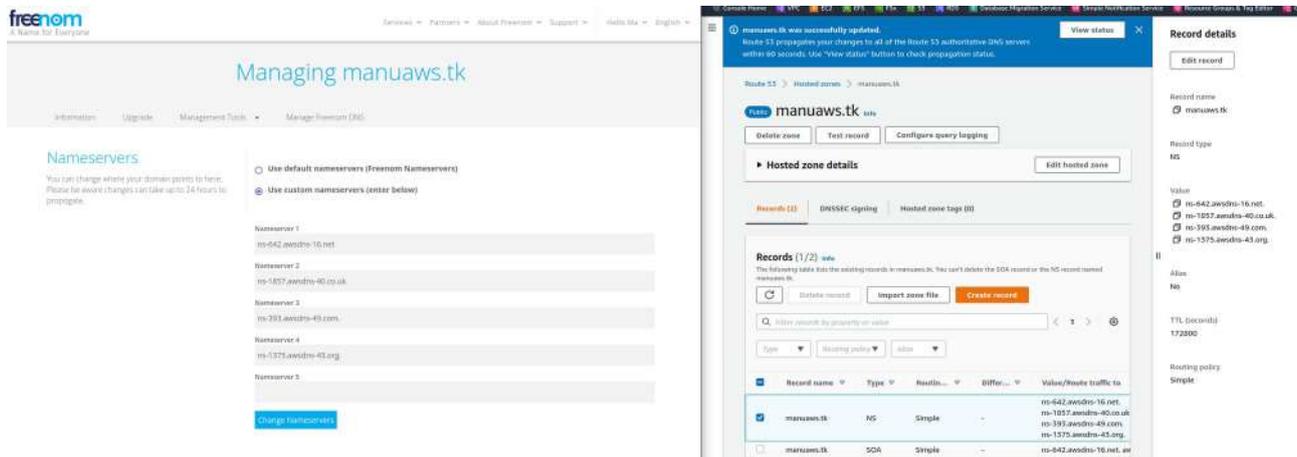
- Crear una zona de host
- Crear políticas de seguridad
- Crear tests
- Registrar dominios

En el sidebar izquierdo tenemos más detalles.

Lo primero que debemos hacer es crear, añadir o registrar un nuevo dominio.

## 37.1. - Dominio

El registro de dominio sigue con el formato antiguo. AWS es caro para el registro del dominio. Personalmente he creado un dominio gratuito en [freenom](https://freenom.com) y apunto sus DNS a una zona de host creada en AWS. (También cobran por la zona de host, normalmente es un servicio gratuito cuando tienes un dominio o un hosting).



Este mecanismo tendrá que propagar las DNS y puede tardar hasta 48 horas. Normalmente se efectúa en menos de 24 horas.

En el caso de registrar o transferir un dominio, aparecerán las propiedades en el dashboard "Registered domains". Tiene las mismas propiedades que cualquier otro registrador de dominios.

## 37.2. - Hosted zone

En una zona de host indicaremos la configuración de DNS para darle la ubicación a cada uno de los dominios y subdominios.

Las zonas pueden ser públicas (Para acceder desde Internet) o privadas (Para redirigir el tráfico interno de las VPC). Si creamos una zona nos pedirá nombre, descripción tipo (público o privado) y etiquetas.

Cuando se crea una zona, por defecto, nos crea 2 registros:

- Un NS simple con 4 servidores de nombres que son los autorizados para su zona alojada.
- Un SOA de autoridad con un servidor de nombres, la dirección del mail administrador, número de serie, el tiempo de actualización, el intervalo de reintento, el tiempo de intentos de un servidor secundario en completar una zona y el TTL.

CUIDADO, no se pueden borrar.

Documentación de los tipos de registros que soporta Route 53 (son los comunes):

[https://docs.aws.amazon.com/es\\_es/Route53/latest/DeveloperGuide/ResourceRecordTypes.html?icmpid=docs\\_console\\_unmapped](https://docs.aws.amazon.com/es_es/Route53/latest/DeveloperGuide/ResourceRecordTypes.html?icmpid=docs_console_unmapped)

### 37.3. - Probar zona host con una instancia

Para probar la zona de host podemos abrirnos una instancia con un apache instalado, crear una pequeña web en /var/www/html

Luego hacemos un nuevo registro con la IP del servidor. Vamos a la zona de host y “Create record”.

Ahora vamos a darle el subdominio www y de tipo A.

Indicamos la dirección IP de la instancia y mantenemos por defecto el TTL y la política de seguridad (Simple routing). Y ya lo tenemos



### 37.4. - Probar zona host con un bucket S3

Necesitaremos un bucket preparado para web. Le llamaremos igual que el dominio. Ponemos al region que queramos, le podemos dejar las ACLs deshabilitada y lo importante es desbloquear el acceso público

#### Block Public Access settings for this bucket

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

- Block all public access**  
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.
- Block public access to buckets and objects granted through new access control lists (ACLs)**  
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- Block public access to buckets and objects granted through any access control lists (ACLs)**  
S3 will ignore all ACLs that grant public access to buckets and objects.
- Block public access to buckets and objects granted through new public bucket or access point policies**  
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- Block public and cross-account access to buckets and objects through any public bucket or access point policies**  
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

Confirmamos que somos conscientes que no es seguro el bucket. El resto lo dejo todo deshabilitado.

Vamos al final de las propiedades del bucket y habilitamos “Static Website Hosting”. También indicamos el fichero index y si queremos el error.

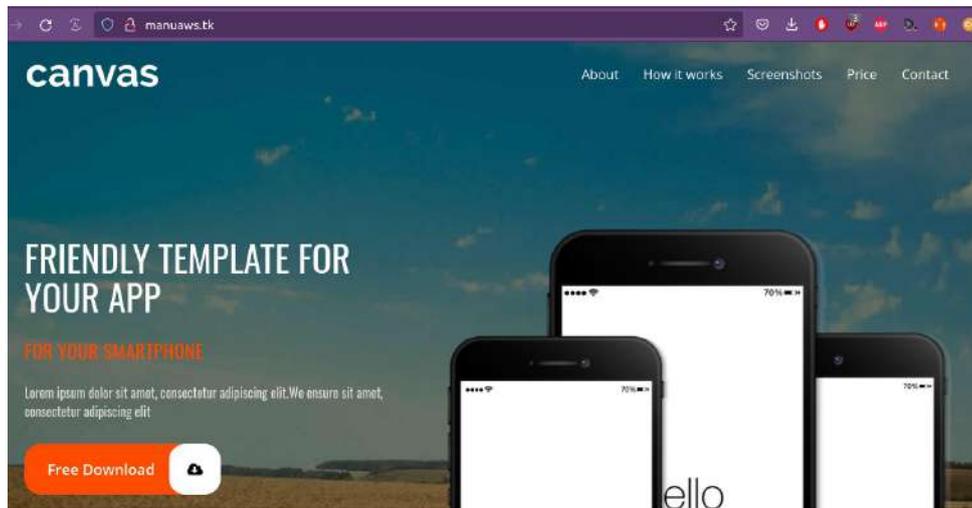
Subimos los ficheros de una web estática y vamos a darle los permisos necesarios. Para hacerlo rápido, le damos un statement genérico:

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

Ahora ya tenemos listo el bucket y le podemos dar la ubicación en la zona de host a las DNS. “Create record”

Esta vez no tenemos IP, vamos a apuntar a un recurso con alias, podremos escoger “S3 website endpoint”. Podremos ver que podemos escoger entre API Gateway, AppRunner, AppSync, CloudFont, etc

Creamos registro



### 37.5. - Probando subdominio

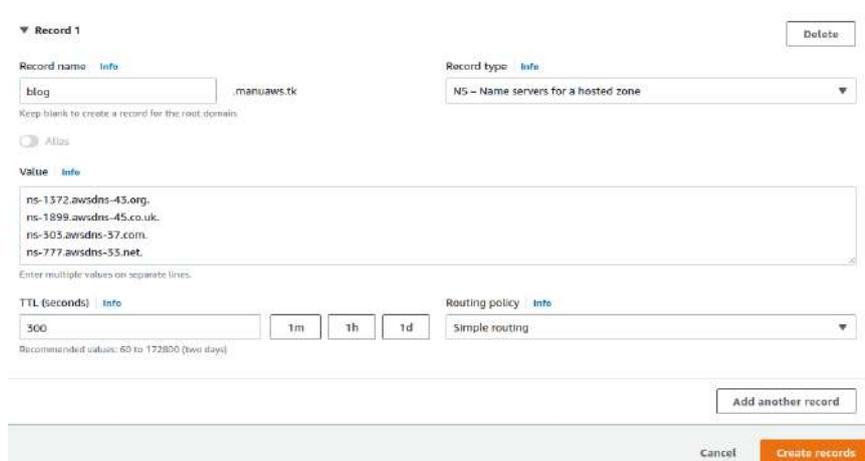
Utilizaremos una instancia con otra web, igual que antes la pondremos en el apache.

Dentro de las zonas alojadas crearemos otros record, le pondremos un nombre de subdominio. Le ponemos la IP de la instancia y listo.

Visto esto, vamos a **crear una zona de host para un subdominio**, lo que se denomina la delegación de responsabilidades a nivel de subdominio.

Vamos a crear una zona. Le ponemos el nombre del subdominio y la descripción que queramos. Luego dejamos la zona como pública y creamos. Tendremos los cuatro NS y el SOA.

Ahora tendremos que mapearla dentro de la zona principal, así que vamos a copiar los NS. Vamos al dominio principal, creamos registro con el nombre del subdominio, de tipo NS y con los valores de las NS de la zona del subdominio.



Para probarlo podemos crear un registro en la zona del subdominio apuntando a una de las instancias o buckets que ya tenemos.

## 37.6. - Apuntando a un load balancer

Tan solo se tiene que mapear a través del alias pero esto nos sirve para ver el failover. Debemos tener el balanceador de carga creado apuntando a un grupo de autoescalado. Para probar algo nuevo podemos probar el switch to wizard donde crearemos el registro con un asistente:

- Escogemos la política de enrutamiento. Simple routing
- Ahora definimos el registro
  - Podemos el subdominio que queramos.
  - Tipo de registro A
  - Enrutamos a un recurso de AWS, la región y la ALB que hemos creado.

## 37.7. - Health Check

Tendremos que tener creada una DNS apuntando a un host con una web. Seleccionamos health Check en el sidebar izquierdo y creamos el Health Check. Configuramos:

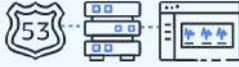
- El nombre
- Podemos monitorizar
  - Endpoint – un host concreto
  - Otros health check– Podemos agrupar otros chequeos
  - CloudWatch alarm
- Podemos ponerle una IP o un nombre de dominio. Podemos chequear cualquier dominio de Route53 o los dns públicos que asocia AWS a las instancias y otros servicios.
- Configuración avanzada
  - Cada cuanto tiempo hacemos el chequeo
  - Umbral para considerar que es un error.
  - String matching – podemos añadir el texto que devuelve el error.
  - Gráfico de latencia
  - Si queremos invertir el chequeo.
  - Desactivar el chequeo
  - Indicar las regiones desde donde se hace el chequeo.
- Además de las acciones anteriores podemos activar una alarma SNS. Si decimos que sí tendríamos que seleccionar el topic o crearlo.

## 37.8. - Políticas de enrutamiento

Cuando se crea un registro en modo wizard se pueden ver bastante claras

**Routing policy**
Switch to quick create

**Simple routing**  
Use if you want all of your clients to receive the same response(s).



**Weighted**  
Use when you have multiple resources that do the same job, and you want to specify the proportion of traffic that goes to each resource. For example: two or more EC2 instances.



**Geolocation**  
Use when you want to route traffic based on the location of your users.



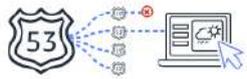
**Latency**  
Use when you have resources in multiple AWS Regions and you want to route traffic to the Region that provides the best latency.



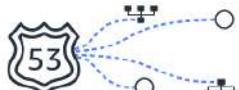
**Failover**  
Use to route traffic to a resource when the resource is healthy, or to a different resource when the first resource is unhealthy.



**Multivalue answer**  
Use when you want Route 53 to respond to DNS queries with up to eight healthy records selected at random.

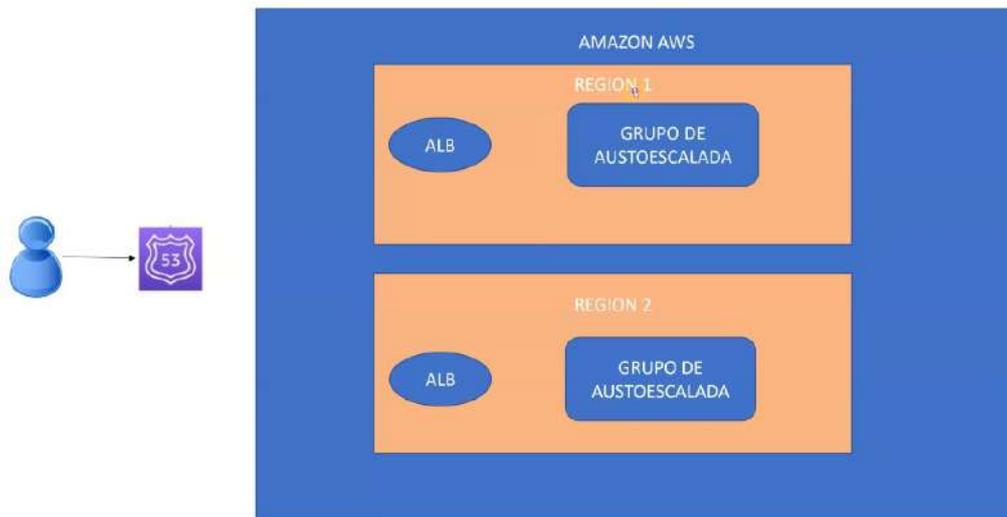


**IP-based**  
Use to route traffic to locations of IP address ranges in CIDR notation.



- Simple routing
- Weighted – De tipo peso, que sirve para cuando tenemos distintos recursos haciendo el mismo trabajo, podremos enrutar según las necesidades que se tengan a través del peso.
- Geolocation – Hace que se enrute en la localización que este más cerca de los usuarios.
- Latency – Con recursos en distintas regiones el tráfico se enruta en la que menos latencia exista.
- Failover – Permite un entorno activo pasivo. Si cae el principal se enrutará el pasivo.
- Multivalue answer – Se va a responder con hasta 8 registros correctos que se escogen de manera aleatoria para que el cliente pueda escoger como acceder.
- IP-based - Se utiliza para enrutar el tráfico a ubicaciones de rangos de direcciones IP en notación CIDR.

### 37.8.1. - Failover



Vamos a tener un cliente conectado a través de route 53 que irá a dos regiones de tipo activo-pasivo. Con un balanceador de carga (ALB) en cada región apuntando a un grupo de autoescalada.

De tal manera que si falla una continuará la otra dando el servicio.

Entonces, tendremos que crear un Health Check apuntando a un balanceador de carga. ALB-A.

Crearemos otro Health Check apuntando al segundo balanceador de carga. ALB-B

Ahora vamos a la zona de host, creamos un registro con failover. Le damos un subdominio, enrutamos a un recurso de AWS. Escogemos "Alias to Application and Classic Load Balancer"/region y balanceador de carga.

El tipo de failover tendremos que indicar que Primary, que será el que responderá a las peticiones.

Tendremos que indicar un ID.

Ahora definimos el segundo, con la segunda region y le indicamos Secondary. Creamos.

Entonces, si entramos en el subdominio creado entraremos en ALB-A. Si eliminamos el grupo de autoescalada de ALB-A y volvemos a entrar, nos llevará a ALB-B.

### 37.8.2. - Enrutamiento por peso

Probamos un entorno activo-activo. Necesitaremos 3 instancias con webs identificables.

Volvemos a Route 53, a nuestra zona de host y creamos un registro con Weighted con un subdominio. Tendremos que definir el Weighted record de cada servidor, pondremos el peso entre 0 y 200. Si ponemos 0 no participará en este enrutamiento. También tendremos que indicar la ID.

Esto lo tendremos que hacer con las tres instancias. Creamos el registro. Ahora entramos en el subdominio para ver los resultados.

### 37.9. - Traffic Flow

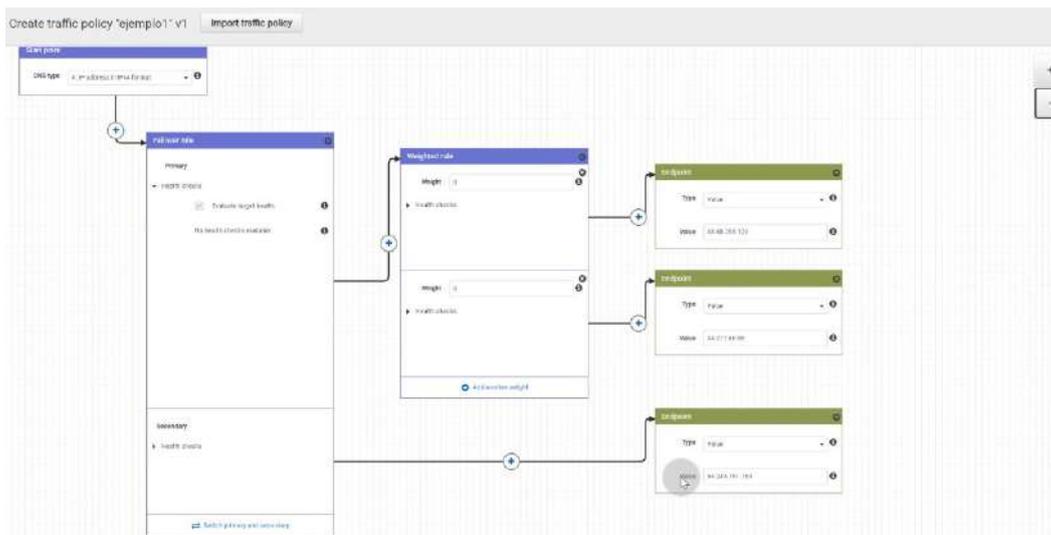
Si entramos en Traffic Flow veremos que es un editor visual para crear políticas de enrutamiento complejas.



Concepts

- Visual editor**  
Use an intuitive visual editor to create complex configurations and save them as traffic policies.  
[View documentation](#)
- Traffic policy versions**  
Create multiple versions of a traffic policy, and use versioning to roll out or roll back updates.  
[View documentation](#)
- Policy records**  
Create policy records to associate traffic policies with domain or subdomain names.  
[View documentation](#)

Necesitaremos 3 instancias. Creamos una política de tráfico. Nos pedirá nombre y descripción, después ya podremos dibujar la política de tráfico. Podemos importar y exportar un json con todos los datos.



Una vez dibujado lo creamos y tendremos que crear otro registro que tenga esta política. CUIDADO Tendríamos que ver el coste porque suelen ser caro.

✔ Successfully created traffic policy ejemplo1 v1  
Optional next step Create policy records using the traffic policy that you just created. You can also create policy records later.

### Create policy records with traffic policy

You can create policy records that use the configuration in your new traffic policy.

Traffic policy: ejemplo1

Version: 1

Hosted zone: cursos-epasoft.es (Z00597911JY712Z17V121)

Policy records: Type the DNS name and TTL for each policy record that you want to create in the specified hosted zone.

Policy record DNS name	TTL (in seconds)	DNS type	Pricing per month
www.trafico.cursos-epasoft.es	60	A	\$50.00

[Add another policy record](#)

[Skip this step](#) [Create policy records](#)

## TEMA 38 - Resumen de todos los servicios

### 38.1. - Administración de costes

- [Cost Explorer](#): Una buena vista de todos los costes de AWS. Importante revisarlo periódicamente y **crear alguna alarma**, para controlar los costes mensuales
- [Budgets](#): Añade o crea **presupuestos y alarmas** para avisarte cuando tus costes pasan de un umbral.
- [Marketplace Subscriptions](#): Aquí dispones de todo un catálogo de soluciones de terceros, listos para usar con la tecnología AWS, por ejemplo suscripciones de PFsense, Citrix, Microsoft o distribuciones específicas de linux.
- [ABC](#): AWS Billing Conductor es más fácil que nunca para los equipos de FinOps configurar, generar y compartir las tarifas correctas con los usuarios finales, independientemente de las tarifas que el cliente haya negociado con AWS.

### 38.2. - Computación (máquina)

- [EC2](#): Genera **máquinas virtuales** elásticas y escalables (Linux/Windows/Mac). De computo general, hasta 448 Vcpu y 12 TBytes RAM, o complejas con GPUs, alto rendimiento, P4d (para machine learning)...
- [Lightsail](#): Las instancias y contenedores **virtuales básicos** (Linux y Windows), para competir en precio, más básicas, convertibles en EC2. Pago mensual al estilo tradicional, con Balanceador de Carga, Bases de datos Postgresql y Mysql, .
- [Lambda](#): Las funciones en **serverless** (sin servidor), pago por uso en llamadas a las funciones ([Node.js](#), [Python](#), [Java](#), [C#](#), [Go](#), Ruby).
- [Batch](#): **Procesamiento** por lotes totalmente administrado para cualquier escala. Por ejemplo lanzar jobs de ejecución de un script o ejecutable linux en cientos de miles de máquinas.
- [Elastic Beanstalk](#): Rápida forma de **implementar y escalar** servicios y aplicaciones web desarrollados con Java, NET, PHP, Node.js, Python, Ruby, Go y Docker en servidores familiares con Apache, Nginx, Passenger e IIS. (genera máquinas virtuales EC2).
- [Amazon EKS](#): Amazon Elastic Container Service for Kubernetes es un servicio administrado que le permite ejecutar fácilmente **Kubernetes** en AWS sin necesidad de instalar ni usar sus propios clústeres de Kubernetes.
- [Fargate](#): Te permite ejecutar **contenedores** sin tener que administrar servidores ni clústeres. Ya no tendrá que aprovisionar, configurar ni escalar clústeres de máquinas virtuales para ejecutar los contenedores
- [Elastic Container Service](#): Servicio de administrador de contenedores compatible con **Dockers**. (puede ser alternativa a k8s)
- [Outpost](#) : Ejecuta infraestructura de **AWS en tu CPD**, es decir on-premise. Utilizas la misma API tanto para tus servidores como para la infraestructura AWS.
- [Parallel Cluster](#): Herramienta de **administración de clústeres** de código abierto, mantenida y totalmente compatible que facilita a científicos, investigadores y administradores de TI la

implementación y administración de clústeres de informática de alto rendimiento (HPC) en la nube.

- [Bracket](#): Si quieres probar proyectos en máquinas cuánticas este servicio te permite explorar algoritmos para la informática cuántica.

### 38.3. - Almacenamiento

- [S3](#): **Almacenamiento de objetos** con 99.999999999% durability (para guardar ficheros, backups, imágenes, código, etc) (no confundir con un dropbox/onedrive, aunque tiene similitudes). Primer servicio creado por AWS
- [SFTP](#): Un servicio para S3 que permite acceder por el protocolo **seguro FTP** a los objetos S3.
- [EBS](#): **Almacenamiento a nivel de bloque** de Sistemas Operativos, para las EC2.
- [EFS](#): **Almacenamiento en red** para instancias EC2, como un NAS-iscsi.
- [Glacier](#): Para **backups a largo plazo**, duradero y a super bajo coste (0,007\$/mes/gbyte ).
- [Storage Gateway](#): Varios tipos de **conectores al S3**, (Hardware Appliance, con tu NAS on-premise), Tape Gateway y FileGateway para montar (on premise) desde Linux, Windows o Mac una unidad a un bucket S3.
- [Snowball](#): Solución de **transporte de datos (Hardware) a escala** de petabytes que utiliza dispositivos diseñados para ser seguros y para transferir grandes volúmenes de datos hacia y desde la nube de AWS
- [Snowmobile](#): **Snowball pero a lo bestia** (a escala de exabytes), hasta 100 PB en un contenedor para transportarlo en un camión.
- [Snowcone](#): Curioso dispositivo versátil, que permite guardar datos y/o calcular y/o transmitir a s3, de apenas 2.1 Kg.
- [FSx for lustre](#): Sistema de ficheros pensado para trabajar con **cientos de Gigas por segundo**, millones de IOPs y latencias de milisegundos.
- [AWS Backup](#): (Servicio de backup, **copia de seguridad**, centralizado y gestionado para automatizar copias de EFS, EBS, etc...
- [Fsx for Windows File Server](#): Ofrece un sistema de **archivos de Microsoft Windows nativo** completamente administrado para que pueda migrar con facilidad sus aplicaciones basadas en Windows que requieren almacenamiento de archivos en AWS. Amazon FSx, basado en Windows Server

### 38.4. - Bases de datos

- [RDS](#): Las **Bases de datos relacionales** administradas, MsSQL, MySQL, MariaDB, PostgreSQL, Oracle, todas escalables y con alta disponibilidad, ahora con **Storage Auto Scaling** etc...
- [RDS Proxy](#): proxy de base de datos de alta disponibilidad y completamente administrado que hace que las aplicaciones sean más escalables, más resistentes a fallos de bases de datos y más seguras.

- [Aurora](#): Base de datos Relacional, compatible MySQL, PostgreSQL. Aurora es hasta **cinco veces más rápida que las bases de datos** de [MySQL](#) estándar y tres veces más rápida que las bases de datos de PostgreSQL estándar.
- [DynamoDB](#): **Base de datos no relacional** (no-sql), super-rápida y auto-escalable, con un 99.999 % SLA
- [ElastiCache](#): Caches o **datastores en memoria**. Compatible con Redis y Memcached.
- [Amazon Redshift](#): Para **almacenamiento de datos para BI** (permite ejecutar consultas complejas en petabytes).
- [Neptune](#): Servicio de **base de datos de gráficos rápido**, de confianza y totalmente administrado que le permite crear y ejecutar fácilmente aplicaciones que funcionen con conjuntos de datos muy conectados
- [DocumentDB](#): Base de datos no relacional, compatible con **mongoDB**, rápida, escalable y alta disponibilidad totalmente gestionada por Amazon.
- [Timestream](#): Es un servicio de **base de datos de serie temporal rápida**, escalable y completamente administrado para IoT, etc, que facilita el almacenamiento y análisis de billones de eventos diarios
- [SimpleDB](#): Pues estaba un poco escondido, pero es un servicio de AWS desde el 2007 que se parece mucho a **DynamoDB pero más básico y sencillo**.

## 38.5. - Red y contenido

- [VPC](#): **Red Aislada Virtual**, dentro de tu entorno en la nube. similar a una vlan dentro de tu red de AWS
- [CloudFront](#): El **CDN** de amazon con más de 300 ubicaciones de borde y 13 cachés de nivel medio regionales, distribuidos en más de 90 ciudades de 47 países, para acelerar tu contenido estático y mejorar las latencias y seguridad.
- [Direct Connect](#): **Conexión de red dedicada** con amazon a su red/ubicación on-premise, sin pasar por Internet.
- [Route 53](#): Un potente **gestor DNS**, incluso reparte la carga por ejemplo en función de geolocalización o latencia, balanceo.
- [API Gateway](#): Facilita a los desarrolladores la creación, la publicación, el mantenimiento, la monitorización y la protección de **API** a cualquier escala
- [AWS PrivateLink](#): Permite **conectar VPC** directamente sin pasar por Internet y válido para que on-premise use servicios de AWS de forma privada
- [AWS GroundStation](#): Servicio gestionado con **conexión** con la mayoría de los actuales **satélites**, puedes conectar tu VPC a un satélite y procesar información, pagas por minutos.
- [DATAsync](#): Servicio de **transferencia de datos**, para conectar EFS a tu on-premise
- [Global Accelerator](#): Servicio de red que usa las propias redes de AWS para que tenga menos congestión y mayor disponibilidad, **un enrutamiento inteligente** en sus redes.
- [Private 5G](#): Crear redes móviles privadas 5G nunca ha sido tan facil

## 38.6. - Migración

- [AWS Migration Hub](#): Ofrece una ubicación única para realizar el seguimiento de los avances de las **migraciones de aplicaciones** en varias soluciones de AWS y otras empresas del sector.
- [Application Discovery Service](#): Ayuda a los clientes empresariales a planificar proyectos de migración al **recopilar información sobre sus centros de datos** on-premise.
- [Database Migration Service](#): Ayuda a **migrar las bases de datos a AWS** de manera rápida, sencilla y segura.
- [Server Migration Service](#): Servicio sin agente que le permite **migrar de forma más rápida** y sencilla miles de cargas de trabajo on-premise a AWS. Con AWS SMS, puede automatizar, programar y monitorizar replicaciones incrementales de volúmenes de servidores en vivo, lo que facilita la coordinación de migraciones de servidores a gran escala.
- [Transit Gateway](#): Permite conectar sus Amazon Virtual Private Clouds (VPC) y sus **redes locales a una única gateway**. Funciona como un concentrador que controla la manera en la que el tráfico se direcciona a todas las redes conectadas que funcionan como radios.

## 38.7. - Herramientas de desarrollo

- [SDK](#): Completo set de librerías para desarrolladores que permite que su aplicación obtenga acceso directo a los servicios de AWS. Hay librerías para node.js, Ruby, PHP, Go, C++, Python, JavaScript, .NET, y Java
- [Cloud9](#): Un IDE en la nube, permite escribir código, ejecutar y depurar solamente con un navegador, incluye un terminal con las CLI todo pre-configurado.
- [CodeStar](#): Facilita la **configuración de toda la cadena de herramientas** de desarrollo y entrega continua para codificar, compilar, probar e implementar el código de la aplicación. Para comenzar un proyecto, puede elegir entre varias plantillas de Amazon EC2, AWS Lambda y AWS Elastic Beanstalk.
- [CodeCommit](#): Servicio de **control de código fuente** totalmente administrado que facilita a las empresas el hospedaje de repositorios Git privados, seguros y altamente escalables.
- [CodeBuild](#): Es un servicio de creación totalmente administrado que crea **código fuente, ejecuta pruebas y produce paquetes** de software listos para su implementación. No es necesario aprovisionar, administrar y escalar sus propios servidores de creación.
- [CodeDeploy](#): Servicio que **automatiza las implementaciones de código** en cualquier instancia, incluidas las instancias de Amazon EC2 y aquellas ejecutadas on-premise.
- [CodePipeline](#): Es un servicio de **integración continua y entrega continua** para realizar actualizaciones de aplicaciones e infraestructura rápidas y de confianza. CodePipeline compila, prueba e implementa el código cada vez que se produce un cambio en este, de acuerdo con los modelos de procesamiento de la publicación que defina.
- [X-Ray](#): Ayuda a **desarrolladores a analizar y depurar aplicaciones** distribuidas de producción, como las creadas con una arquitectura de micro-servicios

- [Amplify](#): Conjunto de herramientas y características especialmente diseñadas que permite a los desarrolladores frontend web y móviles crear rápida y fácilmente aplicaciones integrándose en AWS.
- [App Mash](#): Facilita la ejecución de **microservicios** al proporcionar una visibilidad constante y controles de tráfico de red para cada microservicio en una aplicación
- [Corretto](#): Es una distribución sin costo, multiplataforma y lista para producción de Open Java Development Kit (**OpenJDK**)

## 38.8. - Herramientas de Administración

- [CloudWatch](#): **Monitoriza todos** los servicios de AWS con métricas, disparadores, detección de anomalías (usa ML en tu infraestructura), etc...
- [CLI](#): Interface de **línea de comandos** para Mac, linux, Windows, para poder controlar varios servicios de AWS desde la línea de comando y automatizarlos mediante secuencias de comandos.
- [CloudFormation](#): **Infraestructura como código**, creador de mundos de AWS todo con scripts (yaml y json).
- [CloudTrail](#): Permite realizar regulaciones y **auditorías operativas**, de riesgo/seguridad y conformidad en su cuenta de AWS.
- [Config](#): Permite examinar, auditar y **evaluar las configuraciones** de tus recursos en AWS.
- [OpsWorks](#): Administración de configuraciones que utiliza **Chef**, una plataforma de automatización que trata las configuraciones de servidor como código.
- [Service Catalog](#): Permite a las organizaciones crear y administrar **catálogos de servicios** de TI aprobados para su uso en AWS. Incluye todo lo relacionado con imágenes, servidores, software y bases de datos de máquinas virtuales para completar las arquitecturas de aplicaciones multi-nivel.
- [Trusted Advisor](#): Ayuda a **reducir los costos**, incrementar el desempeño y mejorar la seguridad al optimizar el entorno de AWS, proporciona asesoramiento a tiempo real para ayudarle a aprovisionar los recursos de acuerdo con las prácticas recomendadas de AWS.
- [Systems Manager](#): **Recabe información** operativa e implemente acciones en recursos: Unifica, agrupa y automatiza tareas operativas de los recursos. Permite conectarse a las instancias (Windows/Linux) sin abrir puertos ni claves .PEM (Session Manager)
- [Personal Health Dashboard](#) proporciona **alertas y orientación** para solucionar problemas en caso de que AWS esté experimentando eventos que puedan afectarle
- [Security HUB](#) : Ver y administrar de **forma centralizada, las alertas de seguridad** y automatizar las verificaciones de cumplimiento.
- [Cloud Map](#) : Te permite **registrar cualquier recurso de la aplicación**, como bases de datos, colas, microservicios y otros recursos en la nube con nombres personalizados.
- [Instance Scheduler 2.0](#) : Configuración de inicios y detección de las instancias EC2 y RDS para un ahorro de costes.

## 38.9. - Servicios Multimedia

- [Elastic Transcoder](#): Realiza tareas de **trans-codificación** de contenido.
- [Kinesis Video Streams](#): Aprendizaje automático y tareas analíticas
- [Elemental MediaConvert](#): **Trans-codificador de vídeos basado en archivos** con características de emisión.
- [Elemental MediaLive](#): **Procesamiento de vídeo** en directo para emisión
- [Elemental MediaPackage](#): **Prepare y proteja fácilmente vídeos** para entrega bajo demanda y en directo.
- [Elemental MediaStore](#): Ofrece nivel de desempeño, consistencia y **baja latencia para entrega de vídeo**.
- [Elemental MediaTailor](#): **Inserta anuncios** dirigidos individualmente en sus transmisiones de vídeo.
- [Elemental MediaConnect](#): Transferencia de **vídeos en directo** segura y fiable
- [Interactive Video](#): Cree experiencias de transmisión en directo atractivas

## 38.10. - Identidad, Seguridad y Conformidad.

- [IAM](#): Controle el acceso de forma segura a los servicios y recursos de AWS de sus **usuarios, grupos, roles, políticas..**
- [Inspector](#): Servicio de **evaluación de seguridad** con y sin agente para máquinas EC2, evalúa si se puede comprometer. A diferencia de Guard Duty que vigila si hay malware en ejecución
- [GuardDuty](#): Es un servicio de detección de amenazas administradas que monitoriza continuamente el comportamiento malicioso o no autorizado para proteger sus cuentas y cargas de trabajo de AWS. Supervisa la actividad, como llamadas API inusuales o implementaciones potencialmente no autorizadas que indican un posible compromiso de la cuenta. También detecta instancias potencialmente comprometidas.
- [Certificate Manager](#): Permite aprovisionar, administrar e implementar con facilidad certificados de capa de conexión segura/seguridad de la capa de transporte (**SSL/TLS**) para su uso con servicios de AWS.
- [Directory Service](#): **Microsoft AD** - Active Directory administrado en la nube de AWS. Migre con facilidad aplicaciones y cargas de trabajo compatibles con el directorio, disponible también como (Standard Edition)
- [WAF & Shield](#): Un **cortafuegos de aplicación** web que permite monitorizar accesos a tu CloudFront o evitar DDoS.
- [Artifact](#): Portal de **auditoria y conformidad** para el acceso bajo demanda, permite descargar los informes de conformidad (pdf) de AWS y administrar acuerdos seleccionados.
- [Amazon Macie](#): Es un **servicio de seguridad que utiliza el aprendizaje automático** para descubrir, clasificar y proteger datos confidenciales automáticamente en AWS. Reconoce los datos confidenciales, como la información personalmente identificable (PII) o la propiedad intelectual y le proporciona paneles de control y alertas que aportan visibilidad acerca de cómo se están trasladando estos datos o se está accediendo a ellos.

- [CloudHSM](#): Es un módulo de **seguridad de hardware (HSM)** basado en la nube que le permite generar con facilidad y usar sus propias claves de cifrado en la nube de AWS.
- [Cognito](#): Permite agregar **el registro y el inicio de sesión** de forma sencilla a sus aplicaciones web y móviles. También tiene las opciones de autenticar a los usuarios a través de proveedores de identidad social, como Facebook, Twitter o Amazon, con soluciones de identidad SAML.
- [Single Sign-on](#): Administre de manera centralizada el acceso con **inicio de sesión único** a varias aplicaciones empresariales de AWS, o conectable con Active Directory.
- [AWS Control Tower](#): Automatiza la configuración de un entorno de referencia, o zona de almacenamiento, que es un **entorno con varias cuentas**, seguro y bien diseñado de AWS. La configuración de la zona de almacenamiento está basada en las prácticas recomendadas que han sido establecidas al trabajar con miles de clientes empresariales para crear un entorno seguro que facilite controlar las cargas de trabajo de **AWS con reglas de seguridad, operaciones y cumplimiento**.

### 38.11. - Analítica

- [Athena](#): fácil generador de consultas que facilita el **análisis de datos en Amazon S3 con SQL estándar para crear data Lakes**. Athena es serverless, de manera que no es necesario administrar infraestructura y solo paga por las consultas que ejecuta.
- [EMR](#): Proporciona un marco **Hadoop** hospedado que facilita, acelera y rentabiliza procesar enormes cantidades de datos en instancias Amazon EC2 dinámicamente escalables.
- [CloudSearch](#): servicio administrado en la nube de AWS que **facilita la configuración**, la administración y el escalado rentables de una solución de búsqueda para su sitio web o aplicación.
- [OpenSearch](#) (Elasticsearch Service): Petabytes de texto y datos y facilita el uso y el escalado de **Elasticsearch** para el análisis de logs, la búsqueda de texto completo, la monitorización de aplicaciones y mucho más.
- [Kinesis](#): Facilita la **recopilación, el procesamiento y el análisis de datos de streaming** en tiempo real para obtener conocimiento de manera oportuna y reaccionar rápidamente ante información nueva.
- [Data Pipeline](#): Servicio web pensado para ayudarle a procesar datos y a transferirlos, de manera fiable y a intervalos definidos, entre diferentes servicios de almacenamiento e informática de AWS, así como entre orígenes de datos on-premise.
- [QuickSight](#): El rápido y fácil BI (**Business Intelligence**) de amazon, a una décima parte del precio.
- [AWS Glue](#): Servicio de extracción, transformación y carga (**ETL**) totalmente administrado que facilita a los clientes la preparación y carga de sus datos para su análisis, puede trabajar con Athena.

## 38.12. - Inteligencia Artificial - Machine Learning

- [DeepRacer](#): Ofrece una **forma divertida** de comenzar a utilizar el aprendizaje por refuerzo (RL). El RL es una técnica avanzada de aprendizaje automático (ML) que adopta un enfoque muy diferente respecto de otros modelos de ML
- [Lookout for Vision/Metrics/Equipment](#): Detecte defectos de productos utilizando visión artificial para automatizar la inspección de calidad.
- [Textract](#): Servicio que **extrae automáticamente texto y datos de documentos** escaneados. Amazon Textract no se limita al simple reconocimiento óptico de caracteres (OCR), sino que también identifica el contenido de campos en formularios e información almacenada en tablas.
- [Personalize](#): Personalización y **recomendaciones en tiempo real** basadas en la misma tecnología que se utiliza en Amazon.com
- [Fraud Detector](#): Servicio completamente administrado que simplifica la tarea de **identificación de actividades en línea potencialmente fraudulentas**, como los fraudes de pagos en línea y la creación de cuentas falsas.
- [CodeGuru](#): Servicio de aprendizaje automático para revisiones de código automatizadas y recomendaciones de rendimiento de aplicaciones. **Le ayuda a encontrar las líneas de código más "pesadas"** que perjudican el rendimiento de la aplicación.
- [Kendra](#): Servicio de búsqueda empresarial altamente preciso y fácil de usar que funciona con **ML con capacidades de búsqueda en lenguaje natural** para sus sitios web y aplicaciones.
- [Forecast](#): servicio administrado que utiliza ML para ofrecer pronósticos altamente precisos. Basado en la misma tecnología de **pronóstico de aprendizaje automático utilizada por Amazon.com**
- [Lex](#): Servicio para crear interfaces de conversación en cualquier **aplicación con voz y texto**.
- [Amazon Polly](#): Convierte **texto en habla realista**, lo que permite crear aplicaciones y categorías totalmente nuevas de productos con esta capacidad.
- [Rekognition](#): Facilita la agregación de **análisis de imágenes** a sus aplicaciones. Puede detectar objetos, escenas, rostros; reconocer a famosos; e identificar contenido inapropiado en las imágenes.
- [Tensorflow](#): Se ha convertido en una opción popular para la investigación de **aprendizaje profundo y desarrollo de aplicaciones**, en particular en áreas como la visión por computadora, la comprensión del lenguaje natural y la traducción del habla.
- [Machine Learning](#): Sustituido o dentro del "mundo" de [SageMaker](#)
- [Amazon Translate](#): Permite **traducir grandes volúmenes** de texto de manera sencilla y eficiente. Actualmente están disponibles 137 pares de idiomas.
- [Amazon Transcribe](#): **Reconocimiento de voz automático** (ASR) y por supuesto con API .
- [SageMaker](#) : Cree, entrene e implemente modelos de **aprendizaje automático** a escala también dispone de [SageMaker Autopilot](#)
- [DeepLens](#): La primera **cámara de vídeo** (Hardware) con aprendizaje profundo para programadores. Si quieres verla funcionando en Bilbao, llámame.

- [Amazon Comprehend](#): Servicio de **procesamiento de lenguaje natural** (NLP) que usa el aprendizaje automático para encontrar información y relaciones en el texto
- [Apache MXNet](#) es un marco rápido de inferencia y entrenamiento de escala ajustable con un **API concisa y fácil de usar para aprendizaje automático**.
- [Monitron](#): Es un servicio con sensórica, que usa ML para detectar anomalías en motores, ventiladores, Bombas, Compresores, etc
- [Panorama](#): es un dispositivo de ML y un SDK (kit de desarrollo de software) que le permite agregar CV (video captura)

### 38.13. - Internet de las cosas (IoT)

- [IoT Core](#): **Gestión principal** de Internet de las Cosas y conexión con el ecosistema de AWS.
- [IoT 1 click](#): Permite a dispositivos sencillos activar funciones de **AWS Lambda** que pueden ejecutar una acción
- [IoT Device Management](#): Incorpore, organice, monitoree y administre de manera remota dispositivos conectados a escala
- [IoT Device Defender](#): Servicio completamente administrado que lo ayuda a **asegurar su flota de dispositivos de IoT**.
- [FreeRTOS](#): Sistema Operativo con funciones **IoT para micro-controladores**
- [AWS Greengrass](#): Es software que le permite ejecutar capacidades de **informática local**, mensajería, almacenamiento de datos en caché y sincronización para dispositivos conectados de manera segura para IoT.
- [IoT Analytics](#): **Análisis** para dispositivos compatibles IoT

### 38.14. - Centro de contacto / Atención al cliente

- [Amazon Connect](#): Servicio de centro de contacto o centralita telefónica (**chat/voz**) basado en la nube con modalidad autoservicio que le permite a cualquier empresa ofrecer un mejor servicio al cliente con facilidad y a un costo menor.
- [Simple Email Service](#): Plataforma de **envío y recepción de emails**, super-escalable.
- [Pinpoint](#) Facilita el **envío de mensajes** a usuarios directamente desde su aplicación o servicio de backend, así como ejecutar campañas focalizadas para mejorar la interacción de los usuarios.

### 38.15. - Desarrollo de juegos

- [Amazon GameLift](#): Servicio administrado para implementar, utilizar y escalar **servidores de videojuegos** dedicados para videojuegos multi-jugador basados en sesiones.
- [Amazon Lumberyard](#): Es un **motor de videojuegos AAA** gratuito con un profundo nivel de integración con AWS y Twitch. Puedes descargar gratis la aplicación para Windows
- [Amazon GameOn](#): Es un set de **API para desarrolladores de juegos** que permite tener a tus jugadores más entretenidos o conectado con el comercio electrónico de amazon para que los jugadores ganen premios.

- [GameSparks](#): La forma sencilla de construir, desplegar y escalar el backends de los juegos.

### 38.16. - Servicios móviles

- [Mobile Hub](#): Simplifica el proceso de construir, probar y **monitorizar aplicaciones móviles** que usan servicios de AWS.
- [Device Farm](#): Mejore la calidad de las aplicaciones **iOS, Android y web probándolas** en dispositivos móviles reales en la nube de AWS.
- [Mobile Analytics](#): Recopile, visualice y exporte **análisis de la aplicación**.
- [AppSync](#): **Crea aplicaciones guiadas** por datos con capacidades en tiempo real y sin conexión.
- [AWS Wavelength](#): Entregue aplicaciones con una latencia extremadamente baja para los dispositivos 5G

### 38.17. - AR / VR Realidad Aumentada / Realidad Virtual

- [Sumerian](#): Crear **experiencias tridimensionales**, de VR y AR.

### 38.18. - Integración de aplicaciones

- [Step Functions](#): Cree aplicaciones distribuidas con **flujos de trabajo visuales**.
- [MQ](#): Servicio de **agente de mensajes** administrado para Apache ActiveMQ
- [Simple Queue Service](#): **Colas de mensajes** completamente administradas para micro-servicios, sistemas distribuidos y aplicaciones sin servidor.
- [Simple Notification Service](#): **Notificaciones móviles** y mensajes de publicación/suscripción para micro-servicios, sistemas distribuidos y aplicaciones sin servidor.
- [SWE](#): Ayuda a los desarrolladores a diseñar, ejecutar y escalar trabajos de fondo que siguen **pasos paralelos o secuenciales**.

### 38.19. - Productividad Empresarial

- [HoneyCode](#): Haz aplicaciones rápidas 100% administradas como un gestor de tareas, proyectos, TO-DOs, sin programar.
- [Alexa para negocios](#): El "SIRI" de Amazon se llama **Alexa** y ahora está especializado para ayuda en el trabajo, reservas en el calendario, etc...:
- [WorkDocs](#): Servicio empresarial seguro de **almacenamiento y uso compartido totalmente** administrado con controles administrativos estrictos y funciones de comentarios que mejoran la productividad de los usuarios, tipo dropbox.
- [WorkMail](#): **Servicio de email y calendario empresarial** tipo webmail, seguro y administrado que soporta las aplicaciones clientes de email para dispositivos móviles y de escritorio existentes. pop3 y smtp.
- [Amazon Chime](#): **Vídeo Conferencia** de amazon, alternativa a Skype.

- [Amazon WorkLink](#): los empleados pueden obtener **acceso al contenido de un sitio web interno** con la misma facilidad que a cualquier sitio público, sin las molestias de conectarse a una red corporativa vpn.
- [Nimble Studio](#): Permite a los estudios creativos producir efectos visuales, animación y contenido interactivo completamente en la nube.
- [QnABot](#). Crea un chatBot multicanal, voz, SMS, chat para mejorar la experiencia del cliente.

### 38.20. - Escritorio y transmisión de aplicaciones

- [WorkSpaces](#): Solución de **escritorio virtual** (Windows 7, Windows 10 o Amazon Linux 2) como servicio (DaaS) segura y completamente administrada que se ejecuta en AWS.
- [AppStream 2.0](#): Permite enviar las **aplicaciones de Windows a cualquier dispositivo** por web, de forma desatendida.

### 38.21. - Blockchain

- [Amazon Blockchain](#): Servicio totalmente gestionado que facilita la creación y gestión de redes de **blockchain** escalables utilizando los populares frameworks de código abierto Hyperledger Fabric and Ethereum.

### 38.22. - Robótica

- [RoboMaker](#): Facilitan el desarrollo, las pruebas y la implementación de **aplicaciones de robótica inteligentes** a gran escala. Con RoboMaker se extiende el marco de software robótico de código abierto más utilizado, Robot Operating System (ROS, Sistema operativo de robots), con conectividad a servicios en la nube

### 38.23. - Licenciamiento

- [License Manager](#): **Gestiona, Descubre y reporta las licencias** de Microsoft, SAP, etc. en AWS y on-premise

### 38.24. - Enlaces de interés:

- **Comparador** de los servicios Cloud en <http://comparecloud.in/> (AWS / Azure / Google / IBM Cloud / Oracle / AlibaCloud / Huawei Cloud) de nuestro amigo [Ilyas F](#)
- Vídeo [TOP 50 Servicios AWS en 10 minutos](#)
- [Infraestructura AWS](#) de forma muy gráfica.
- [pingaws.cdm.guru](http://pingaws.cdm.guru) mide la **latencia de todas las regiones** de AWS desde tu ubicación, con un ping.
- Grupo de usuarios Meetup de AWS en **Bilbao (Spain)** [bilbaws.com](http://bilbaws.com) y otros grupos [por el mundo](#):
- RSS de AWS: <https://aws.amazon.com/es/about-aws/whats-new/recent/feed/>