EC2

- Amazon Elastic Compute Cloud
- proporciona computación escalable (hacía arriba y abajo)

opciones de compra

- bajo demanda
  - …
- instancias reservadas : 1 - 3 años
  - standard : no se puede modificar y la has de aguantar el tiempo contratado
  - convertible : permite alguna modificación
- instancias programadas : por franjas
  - …
- instancias spot : necesito mucha capacidad de computación en un momento dado. Sobre el precio de «computación» (depende de la demanda) adquiero máquinas para realizar mi trabajo (batch)
  - …
- hosts dedicados : máquina física solo para mi, accediendo incluso a ver el hardware asignado
- instancias dedicadas : máquina física solo para mi, pero no ves el hardware

tipos de instancias

- proposito general
- optimizada computacional
- optimiazada memoria
- optimizada acceso disco
- aceleración computacional

EBS

- Block Level Storage:
  - permite instalar OS
  - solo se puede atachar un EBS a una instancia EC2 de la misma AZ
- persistencia más allá de la máquina
- tipos:
  - General Purpose SSD (GP2) : 3 IOPS/GiB, siporta hasta 10000 IOPS y 160MG
  - Provisioned IOPS (IO1)
  - …
- se pueden cambiar los volúmenes y el tipo on the fly
- para mover un volumen entre AZ o regiones, se hace un snapshot y se copia a la nueva zona

EBS Snapshots

- backups incrementales de S3
- no apto para aplicaciones que escriban a disco a menudo (BDD, por ejemplo)
- es una copia de un volumen en un momento dado
- AMI = imágenes de OS
- snapshots de volúmenes encriptados, lo están por defecto
- se pueden compartir snapshots con otras cuentas, pero han de estar desencriptados

Security Groups

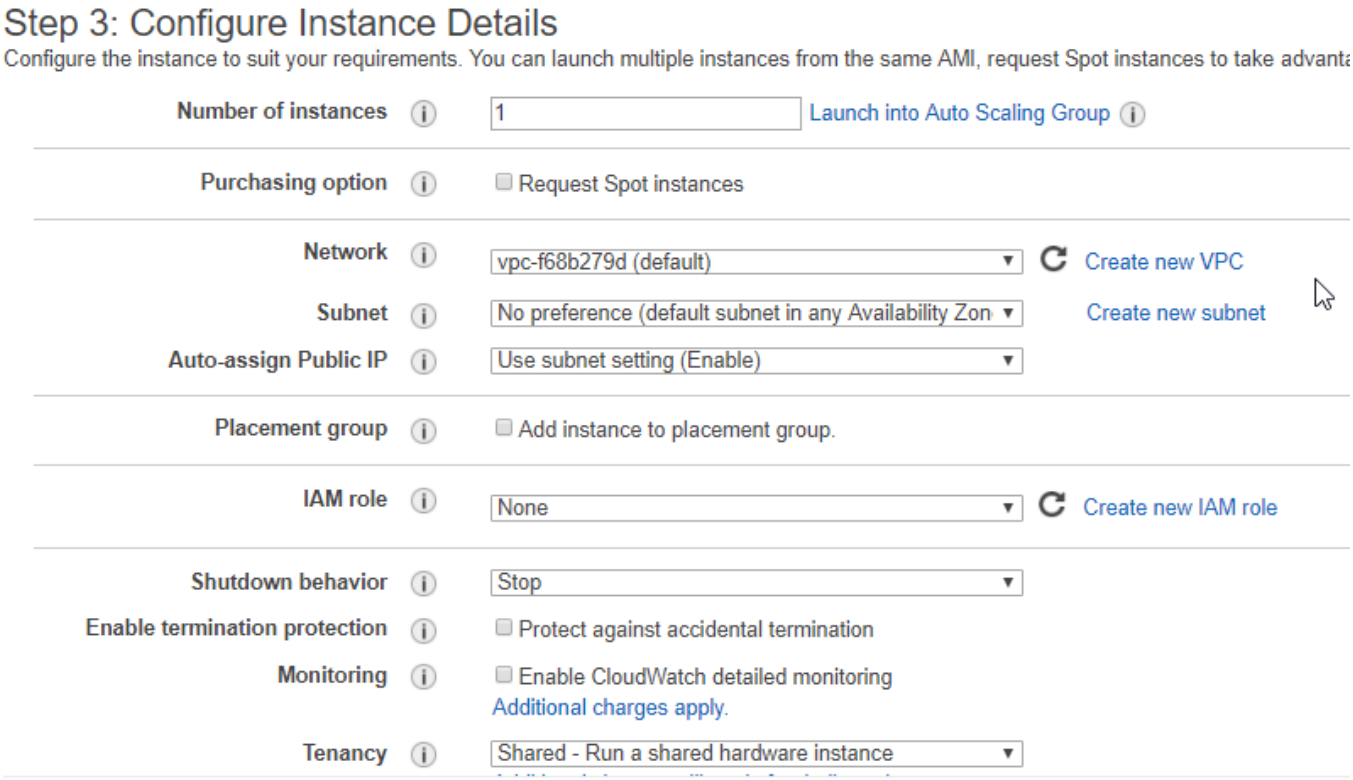
- es la primera barrera que separa la máquina del exterior
- existe por defecto en el VPC (no se puede borrar)
- STATEFUL : todo el tráfico establecido será permitido
    - por contra, en las ACL se ha de permitir la «ida» y la «vuelta»
- reglas de firewall inbound / outbound de ALLOW (todo denegado por defecto)
- inbound : ip, puerto, protocolo
- reglas por defecto del SG de por defecto:
    - permite todo el tráfico de entrada de otras instancias del mismo SG
    - permite todo el tráfico de salida
- reglas por defeceto del SG creado por mi
    - no permite tráfico (ni entre las máquinas del mismo SG creado por mi)
        - hay que crear un regla específica para que se hablen entre ellas (a nivel global o específico)
        - puedes especificar IPs u otros SG
    - permite todo el tráfico de salida

EC2 Examen

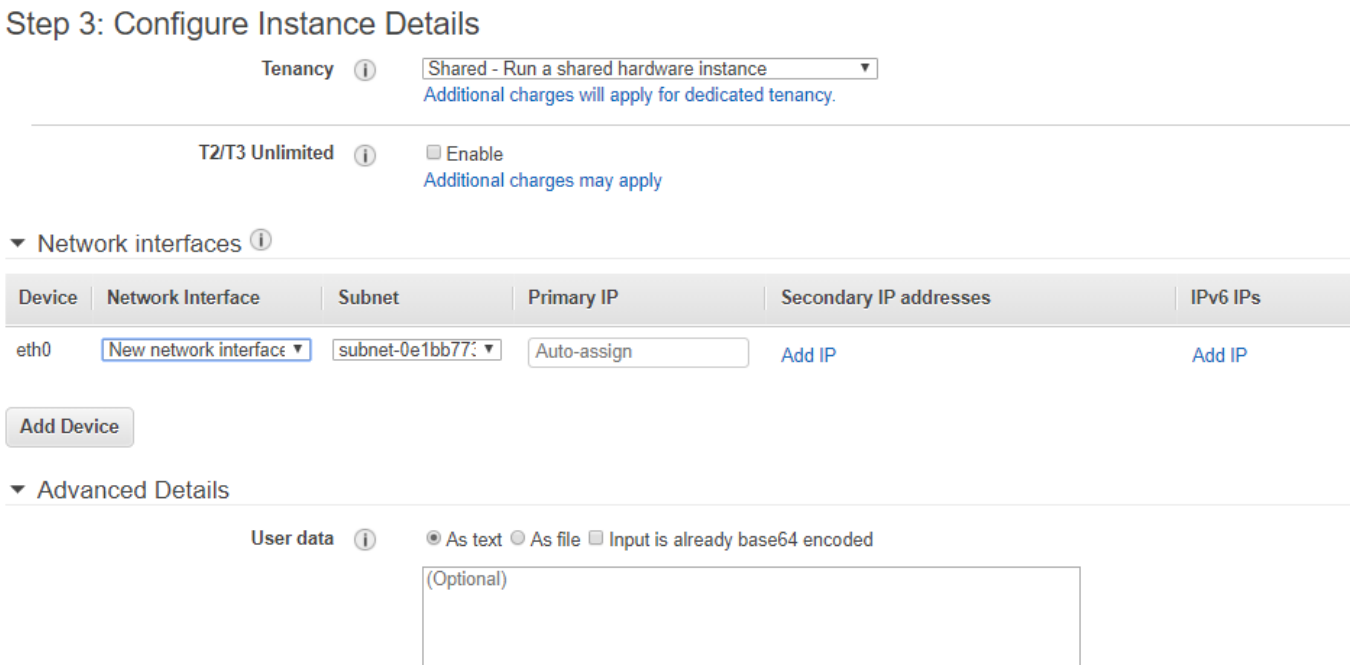
- termination protection está deshabilitado por defecto
- EBS-backed instances : puede parar y volver a arrancar
    - por defecto estos volúmenes son elimimandos al eliminar la máquina
- instance store-backed instance: ephemeral
    - Ephemeral : disco «local», al parar la máquina (como cada vez arranca en un hardware diferente) desaparece, al contra que los volúmenes EBS
- EBS root volumes son eliminados cuando se termina una máquina
- EBS root volumes por defecto de la AMI no puede ser encriptado
- EC2 User Data : running scripts

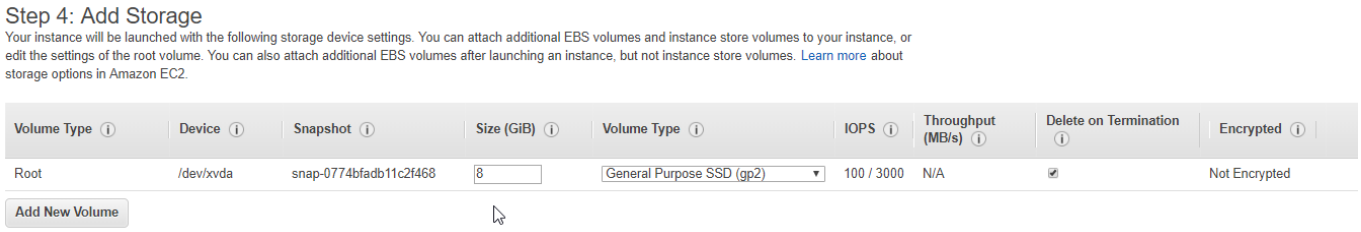
Laboratorio

- https://ec2instances.info



- IAM role : acceso a otros devices al asignarle un rol sin contraseñas ni keys
- Protected against accidental termination
- Enable CloudWatch detailed monitoring : métricas cada minuto, si no está activo, cada 5 (en este caso sin coste)
- Tenacy : compartido, dedicado o host dedicado





- Encrypted: KMS (gestión y auditado)
- los volúmenes añadidos no tienen activado el Delete on Termination por defecto
- los volúmenes root si
- el usuario por defecto en las Amazon Linux AMI es **ec2-user**
- al crear la máquina podemos crear un par de keys nuevos (o usar existentes)
    - si usamos putty, hay que pasar el fichero **.pem** por el Putty Key Gen para generar el tipo de llave que Putty necesita para realizar la conexión
- `ls /dev/disk/by*`

Snapshots

- volumen ligado a la AZ
- las llaves están ligadas a las regiones
- volumen → snapshot → copiar:
    - permite cambio de region
    - permite encriptar
- snapshot:
    - crear volumen (en misma región)
    - crear imagen (para nuevas instancias EC2)

roles y keys

acceso a los diferentes recursos de Amazon

- rol = conjunto de policys, atachándolo al servicio, dándole los permisos que necesite
- keys = se generan unas credenciales para actuar de manera programmatica con la API de AWS

Laboratorio

- creamos un snapshot del volumen de nuestra instancia EC2 del día anterior
- copiamos el snapshot encriptandolo
    - usará las llaves KMS de nuestra cuenta
- creamos una imagen del snapshot copiado
- creamos una instancia EC2 desde la imagen encriptada de nuestro volumen copiado
    - le añadimos las llaves SSH que generamos el otro día (vinculadas a nuestro usuario)
- podemos acceder con cliente SSH
- en nuestro IAM → Security Credencials → Access keys ← OJO! solo permite descargar una vez
- en nuestra EC2, `aws configure`, añadimos las Access Keys
- comprobamos que tenemos acceso a otros recursos: `aws s3 ls` o `aws s3 ls s3:`*`altran2018 * borramos la configuración en ~/.aws/credentials'' * AWS → AIM → Roles * creamos un nuevo Rol ( y le añadimos la policy `**`S3ReadOnly`**`, por ejemplo) * AWS → EC2 → instances → Actions → Instance Settings → Attach Role * volvemos a tener acceso a los recursos AWS de nuestra cuenta`*