

# VPC

## Virtual Private Cloud

- red aislada
- puedes tener más de una por región (o en varias regiones)
- defines rangos, subredes, tablas de ruta y gateways
- ...
- seguridad:
  - NACL :
    - a nivel de subred
    - permite allow y deny
  - Security Groups:
    - solo allow
- subnet : recursos aislados
- internet gateway : acceso a internet (por defecto no hay definido)
- nat gateway : acceso a internet de salida
- hardware VPN connection
  - virtual private gateway : lado amazon
  - customer gateway : lado cliente
  - Direct Connect para conexiones más potentes (por ver)
- Peering Connection: interconexión entre diferentes VPC
- VPC endpoints : tráfico interno
- GRAFICO AWS VPC COMPONENTS
- al crearlo, el wizard nos permite:
  - VPC con 1 subnet
  - VPC con 2 subnets (público y privada)
  - ...
  - ...
- tamaño mínimo subnet: /28
- tamaño máximo: /16
- se puede añadir otro rango de IPs (nuevo, no examen)
- instancias sin IP pública se pueden conectar de 2 maneras:
  - NAT
  - hardware VPN connection o Direct connect : la salida a internet es a través del cliente (con sus recursos: conexión, firewall, etc)
- que puedo hacer:
  - lanzar instancias en una subnet
  - asignar rangos de IPs en las subnets
  - enrutado entre las subnets
  - crear internet gateway
  - más seguridad
  - Instance Security Groups - Stateful
  - NACL - Statefulless
- Default VPC VS Custom VPC
  - permite lanzar instancias inmediatamente
  - todas las subredes tiene acceso a internet
- VPC Peering
  - conexión de 2 VPC
  - permite entre-regiones
  - permite diferentes cuentas
  - han de tener rangos de IPs que no se solapen
  - no transitivas

## Laboratorio

- crear VPC propia (rango 10.0.0.0)
- crear 2 subnets
  - solo disponible en una AZ
  - nombre: rango IP = 10.0.1.0-private
  - aunque tenga una IP pública, será innacesible hasta que no haya un internet gateway
- crear internet gateway
  - solo 1 por VPC
- atacharlo a la VPC
  - siguen sin tener acceso a internet
  - hay que modificar la Main Route Table
- crear una Route Table en la VPC
  - añadir una ruta de salida 0.0.0.0 al gateway que hemos creado anteriormente
- al crear un nuevo SG, el inbound está deshabilitado (o no tiene ninguna regla)

From:  
<https://miguelangel.torresegea.es/wiki/> - **miguel angel torres egea**

Permanent link:  
<https://miguelangel.torresegea.es/wiki/info:cursos:itformacion:awsassociate:vpc?rev=1539624830>

Last update: **15/10/2018 10:33**

