

# Máquinas virtuales en GCP

jueves, 23 de noviembre de 2023 10:30

Regiones: Espacio donde Google tiene 2 o más centros de cómputo.

- VPC debe de estar asociada a un proyecto
- VPC formadas por subredes, donde, al menos una de estas (subred) debe de existir dentro de la VPC.
- Las subredes tienen alcance regional.
- Subredes tienen asociados rangos de IP's, con esto se le puede dar un IP del rango a los recursos as: ociados a la misma.

Tres (3) tipos de VPC's en GCP:

1. Default:  
Se crea automáticamente una subred en cada una de las regiones de GCP.  
No se tiene control sobre los rangos de IP's que se le asigna a las subredes.
2. Auto Mode:  
Se crea automáticamente una subred en cada una de las regiones de GCP.
3. Custome Mode:  
Control total para definir las características de la VPC, crear solo las subredes necesarias, asignar rangos de IP definidos.

(!) El problema con auto mode, es que si quiero unir 2 recursos y tienen el mismo direccionamiento, estaría tratando de unir 2 universos con los mismos rangos de direcciones IP.

- Una subred está asociada a todos los datacenters de una región.

Una máquina virtual de GCP con solo direcciones IP privadas no se puede conectar a internet

Servicios de red o conectividad:

- Ruteo: Establecer para distintas VPC's la manera en la que se van a routear los paquetes de comunicación.
- VPN: Conectar un servicio que no sea parte de GCP.
- DNS: Nombre de dominio a una máquina, se usa el DNS para localizar a las máquinas de GCP por medio del nombre de dominio.
- NAT: Servicio para acceder a internet desde una máquina virtual con dirección IP privada.
- Firewall: Reglas de firewall para la comunicación entre servicios que pueden y rechazar los que no.
- Balanceo de cargas

**VPC peering:** Recurso para conectar 2 VPC's distintas entre sí.

Una VPC está asociada a un proyecto.

**Shared VPC:** Se define una red (proyecto HOST) que tiene definidos todos los recursos, reglas de firewall, subredes, rangos de IP, etc; este proyecto HOST le dará el servicio de conectividad a otros proyectos que lo soliciten. Proyecto central de comunicaciones.

- Trafico entrante (Ingress)
- Trafico de salida (Egress)

Reglas implícitas:

1. Todo el tráfico saliente a internet está permitido
2. Todo el tráfico de entrada esta rechazado.

IaaS:

Se gestiona: Apps, Data, Runtime, Middleware.

**Maquinas preemptibles:** Maquinas cuya vida va a ser de máximo 24 horas, Google puede quitarlas cuando quiera, lo bueno es que el precio es mucho más barato.

Familias de máquinas virtuales:

- E2:
  - Máquinas virtuales baratas usadas en ambientes de desarrollo y pruebas.
- Balanceados N2, N2D:
  - Excelente desempeño, aplicaciones para muchos usuarios.
- TAU T2D:
  - Escalamiento de forma rapida
- Optimización de cómputo (C2)
  - Mayor desempeño en procesamiento que en memoria
- Optimización de memoria (M1, M2)
  - Mayor memoria que capacidad de cómputo (Bases de datos en memoria SAP HANA, Redis)
- Optimización del proceso de gráficos (A2)
  - GPU de alto desempeño.
- Maquinas personalizables: Se puede tener personalizables de cualquier familia y modificar la memoria o procesador.

#comando para conectarse con una máquina virtual privada sin necesidad de VPN  
gcloud compute ssh <nombre-vm> --zone <zona> --tunnel-through-iaa (Tunnel Identity Aware Proxy).

Network services – cloud NAT – crear nuevo router; para crear una conexión a internet de una maquina virtual privada.