Nociones sobre la infraestructura global de la nube y Seguridad

Para entender la red y los servicios de cómputo hay que acercarse a su forma de despliegue

La infraestructura global de AWS se diseñó y se creó para ofrecer un entorno de cómputo en la nube fiable, confiable, escalable y seguro con un rendimiento de red global de alta calidad.

Por ello se ha desplegado en Regiones

Regiones de AWS

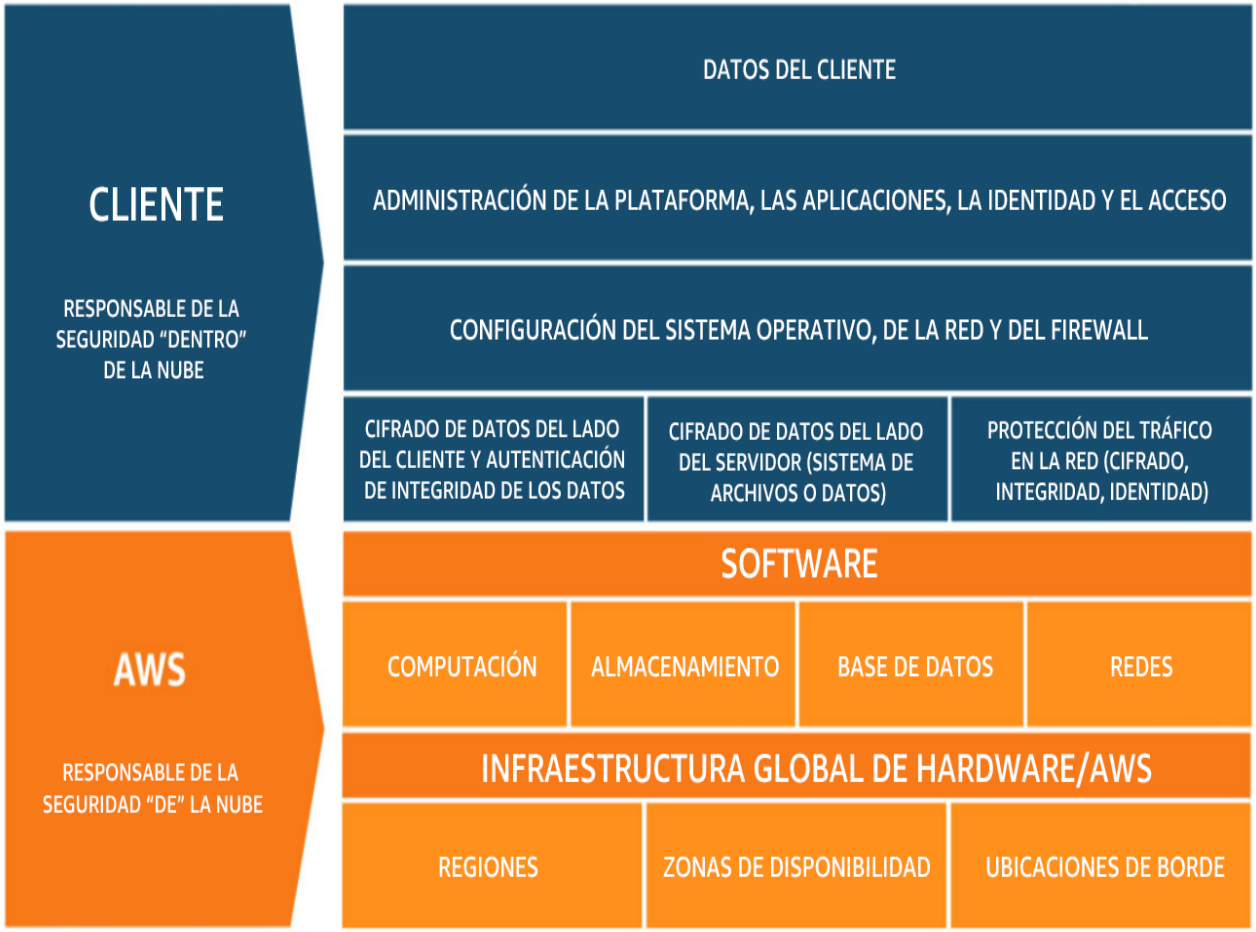
- Una región de AWS es una zona geográfica.
  - Usted controla la replicación de datos entre regiones.
  - La comunicación entre regiones utiliza la infraestructura de red troncal de AWS.
- Cada región proporciona a la red niveles plenos de redundancia y conectividad.
- Una región normalmente consta de dos o más zonas de disponibilidad.

Selección de una región

- Gobernanza de datos, requisitos legales
- Proximidad con los clientes (latencia)
- Servicios disponibles dentro de la región
- Costos (varían según la región)

El modelo de Seguridad en la nube de AWS se basa en un

→ Modelo de responsabilidad compartida de AWS



Responsabilidad de AWS: seguridad de la nube

- Seguridad física de los centros de datos
  - Acceso controlado basado en las necesidades

- Infraestructura de hardware y software
  - Baja de recursos de almacenamiento, registro de acceso del sistema operativo (SO) del host y auditoría

- Infraestructura de red
  - Detección de intrusiones

- Infraestructura de virtualización
  - Aislamiento de instancias

Responsabilidad del cliente: seguridad en la nube

- Sistema operativo de la instancia de Amazon Elastic Compute Cloud (Amazon EC2)
  - Incluidos los parches y el mantenimiento
- Aplicaciones
  - Contraseñas, acceso basado en roles, etc.
- Configuración del grupo de seguridad
- SO o firewalls basados en host
  - Incluidos los sistemas de detección o prevención de intrusiones
- Configuraciones de red
- Administración de cuentas
- Configuración de inicio de sesión y permisos para cada usuario

Con más detalle …

Características del servicio y responsabilidad en materia de seguridad

Infraestructura como servicio (IaaS)
El cliente tiene más flexibilidad en lo que respecta a la configuración de redes y almacenamiento.
El cliente es responsable de administrar más aspectos de la seguridad.
El cliente configura los controles de acceso.

Plataforma como servicio (PaaS)
El cliente no necesita administrar la infraestructura subyacente.
AWS gestiona el sistema operativo, la implementación de parches a la base de datos, la configuración del firewall y la recuperación de desastres.
El cliente puede centrarse en la administración de código o datos.

Software como servicio (SaaS)
El software está alojado de forma centralizada.
Cuenta con licencia según un modelo de suscripción o de pago por uso.
Normalmente, el acceso a los servicios se realiza a través de un navegador web, una aplicación móvil o una interfaz de programación de aplicaciones (API).
Los clientes no necesitan administrar la infraestructura que respalda el servicio.

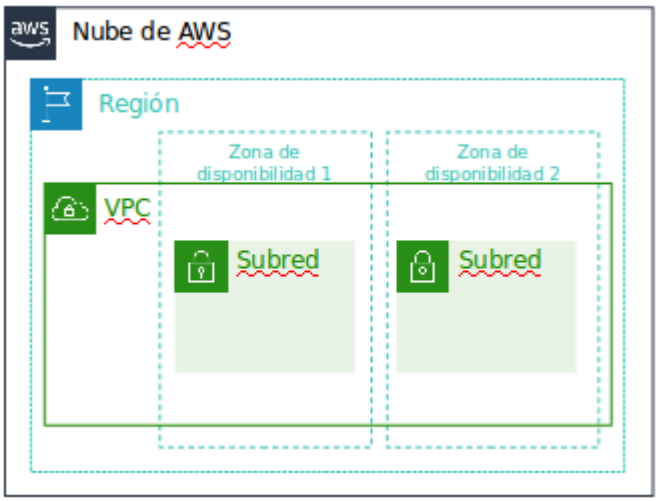
Amazon VPC. Redes

Amazon VPC

- Le permite aprovisionar una sección aislada de forma lógica de la nube de AWS, donde puede iniciar recursos de AWS en una red virtual que usted defina
- Le permite controlar sus recursos de redes virtuales, entre ellos:
  - Selección de un rango de direcciones IP
  - Creación de subredes
  - Configuración de tablas de enrutamiento y puertas de enlace de red
- Le permite personalizar la configuración de red de su VPC
- Permite utilizar varios niveles de seguridad

VPC y subredes

- **VPC:**
  - Se encuentra aislada de forma lógica de otras VPC
  - Dedicada a su cuenta de AWS
  - Pertenece a una única región de AWS y puede abarcar varias zonas de disponibilidad
- **Subredes:**
  - Intervalo de direcciones IP que divide una VPC
  - Pertenece a una única zona de disponibilidad
  - Se clasifica como pública o privada



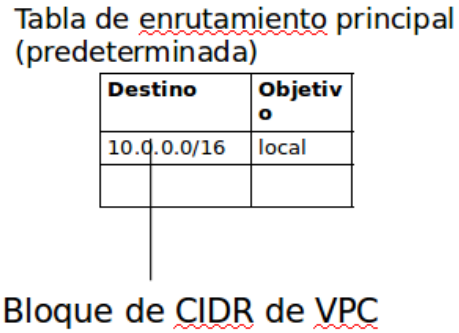
Direccionamiento IP

- Al crear una VPC, se le asigna un bloque IPv4 de CIDR (un rango de direcciones IPv4 privadas).
- No puede cambiar el rango de dirección después de crear la VPC.
- El tamaño de bloque de CIDR IPv4más grande es /16.
- El tamaño de bloque de CIDR IPv4más pequeño es /28.
- También se admite IPv6 (con un límite de tamaño de bloque diferente).
- Los bloques de CIDR de las subredes no pueden superponerse.

VPC	Direcciones x.x.x.x/16 o 65.536 (máx) a Direcciones x.x.x.x/28 o 16 (mín)

Direcciones IP.

Ejemplo:
Una VPC con un bloque de CIDR IPv4 de 10.0.0.0/16 tiene 65.536 direcciones IP en total.
Cada VPC tiene una serie de subredes donde se organiza las direcciones disponibles.



Una VPC es una sección aislada de forma lógica de la nube de AWS.
Una VPC pertenece a una región y requiere un bloque de CIDR.
Una VPC se subdivide en subredes.

Una subred pertenece a una zona de disponibilidad y requiere un bloque de CIDR.
Tablas de enrutamiento para controlar el flujo de tráfico para una subred.
Las tablas de enrutamiento tienen una ruta local integrada.
Tiene rutas adicionales para la tabla.

Tablas de enrutamiento y rutas

- Una tabla de enrutamiento contiene un conjunto de reglas (o rutas) que puede configurarpara dirigir el tráfico de red de su subred.
- Cada ruta especifica un destino y un objetivo.
- De forma predeterminada, cada tabla de enrutamiento contiene una ruta local para la comunicación dentro de la VPC.
- Cada subred de su VPC debe estar asociada a una tabla de enrutamiento(cómo máximo una).

Puerta de enlace de internet

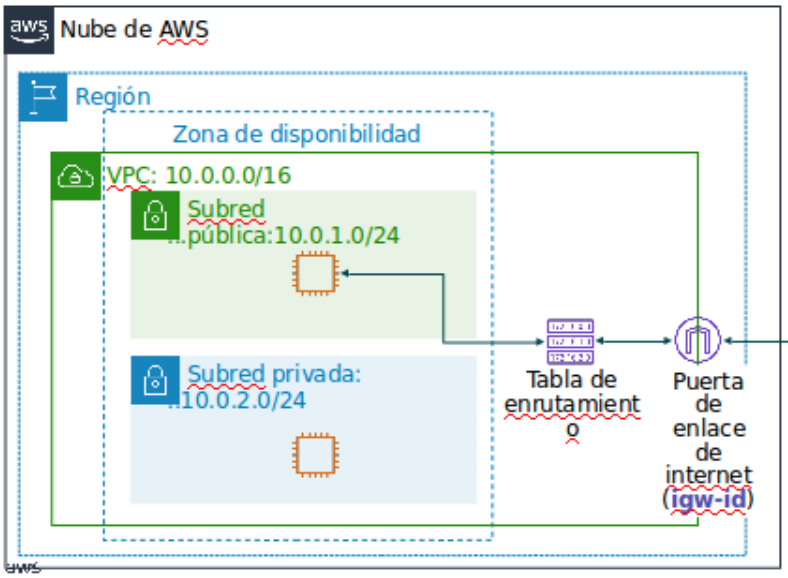
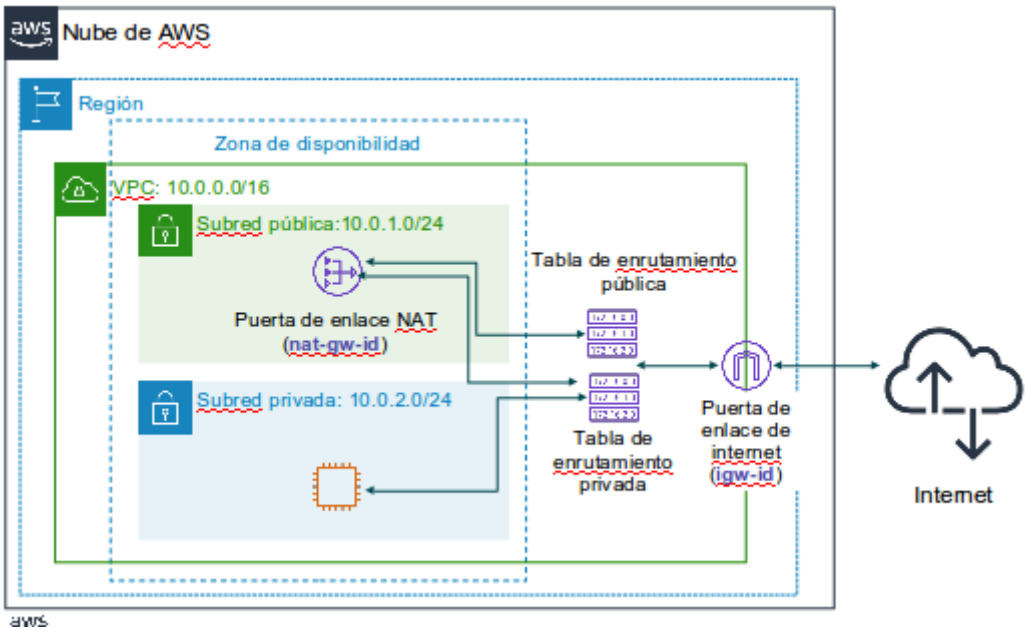


Tabla de enrutamiento de subred pública

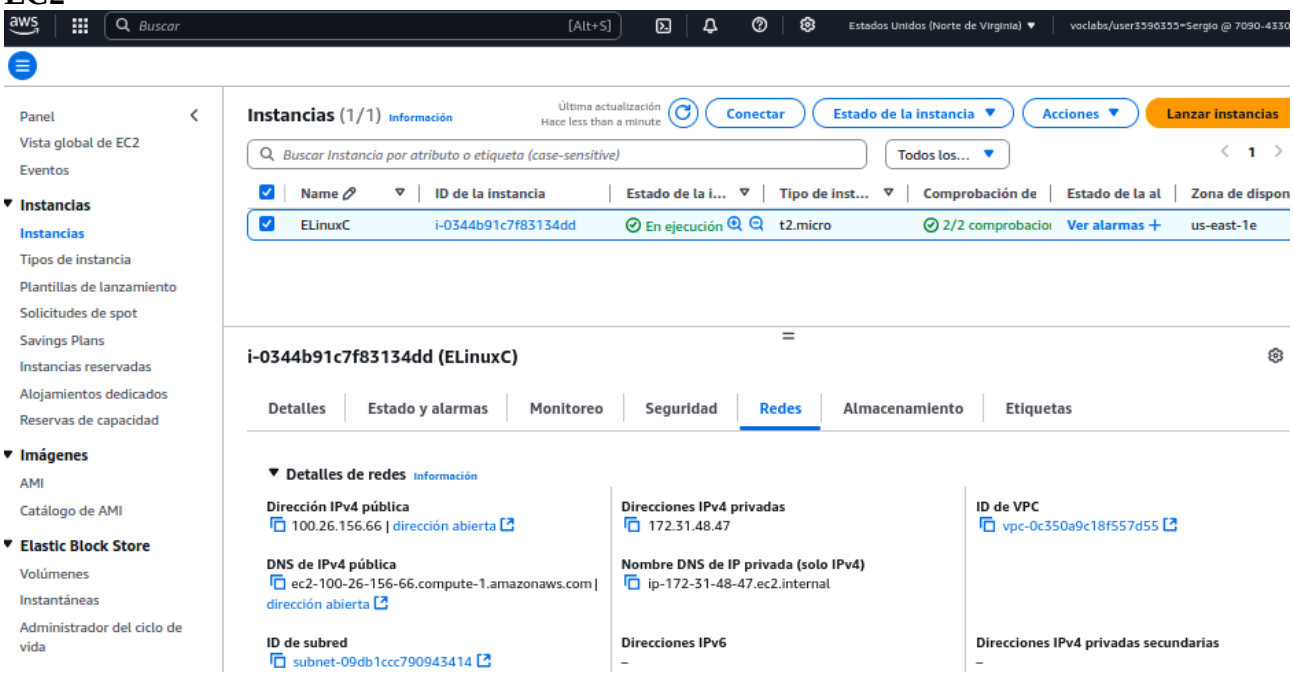
Destino	Objetivo
10.0.0.0/16	local
0.0.0.0/0	igw-id

Puerta de enlace de traducción de direcciones de red (NAT)

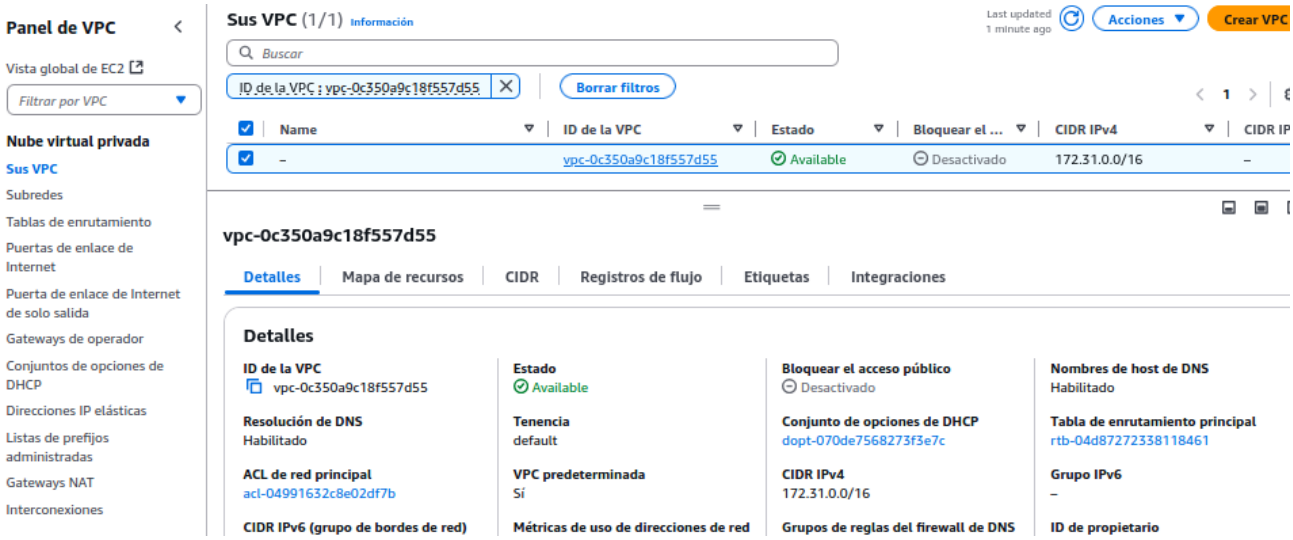
Tabla de enrutamiento de **subred pública**	
Destino	**Objetivo**
10.0.0.0/16	local
0.0.0.0/0	igw-id
Tabla de enrutamiento de **subred privada**	
Destino	**Objetivo**
10.0.0.0/16	local
0.0.0.0/0	nat-gw-id



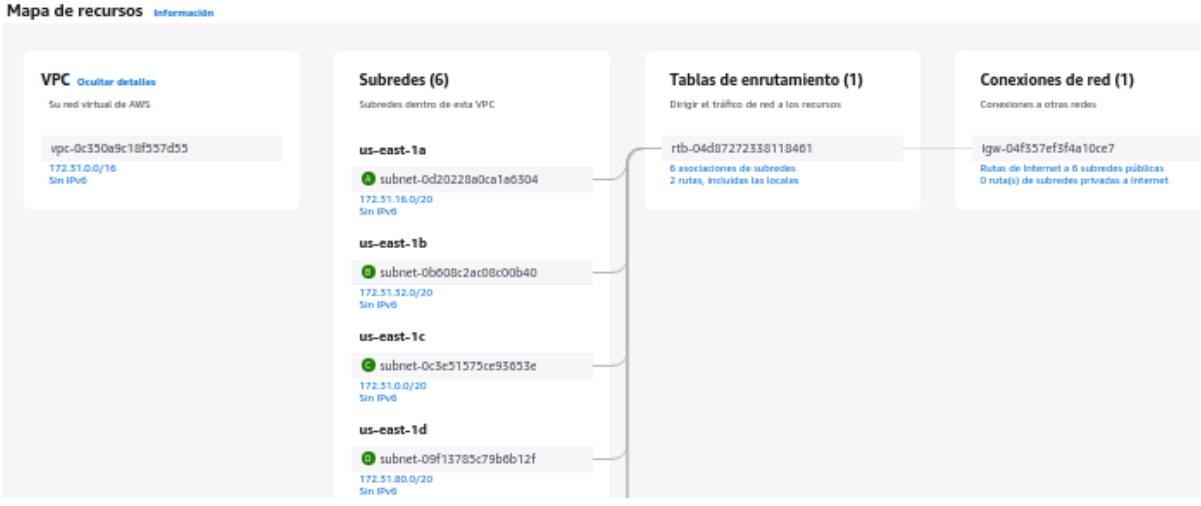
EC2



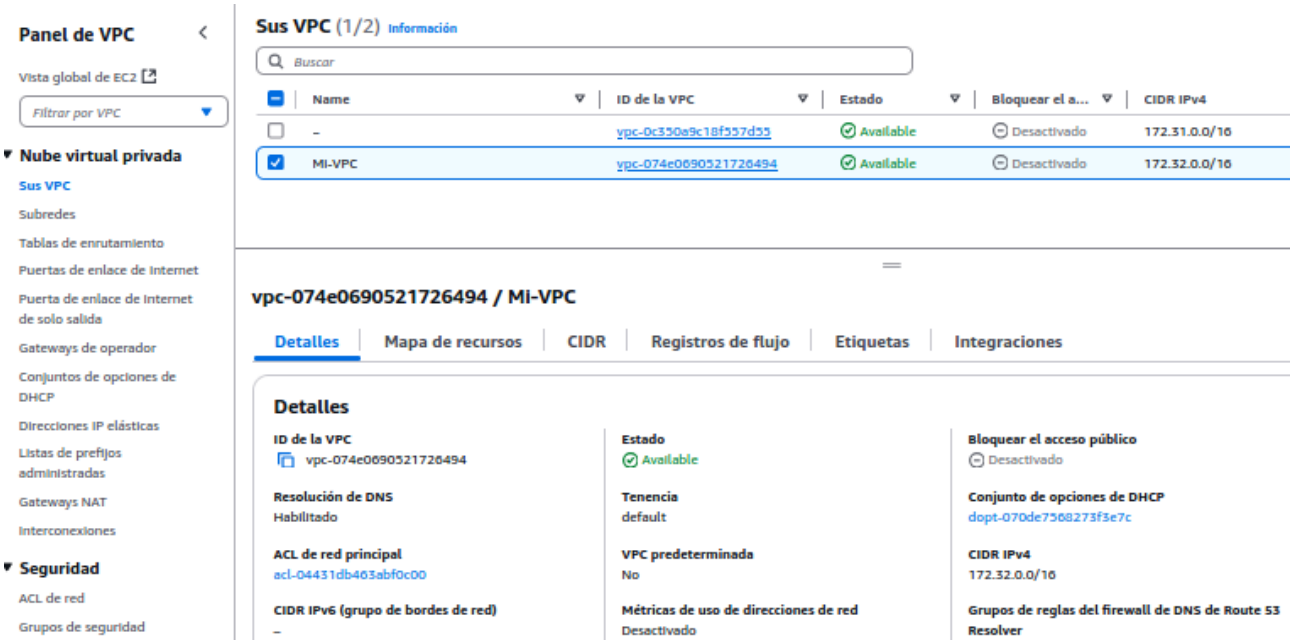
VPC



Mapa de recursos



Panel de VPC



Mapa de recursos