

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

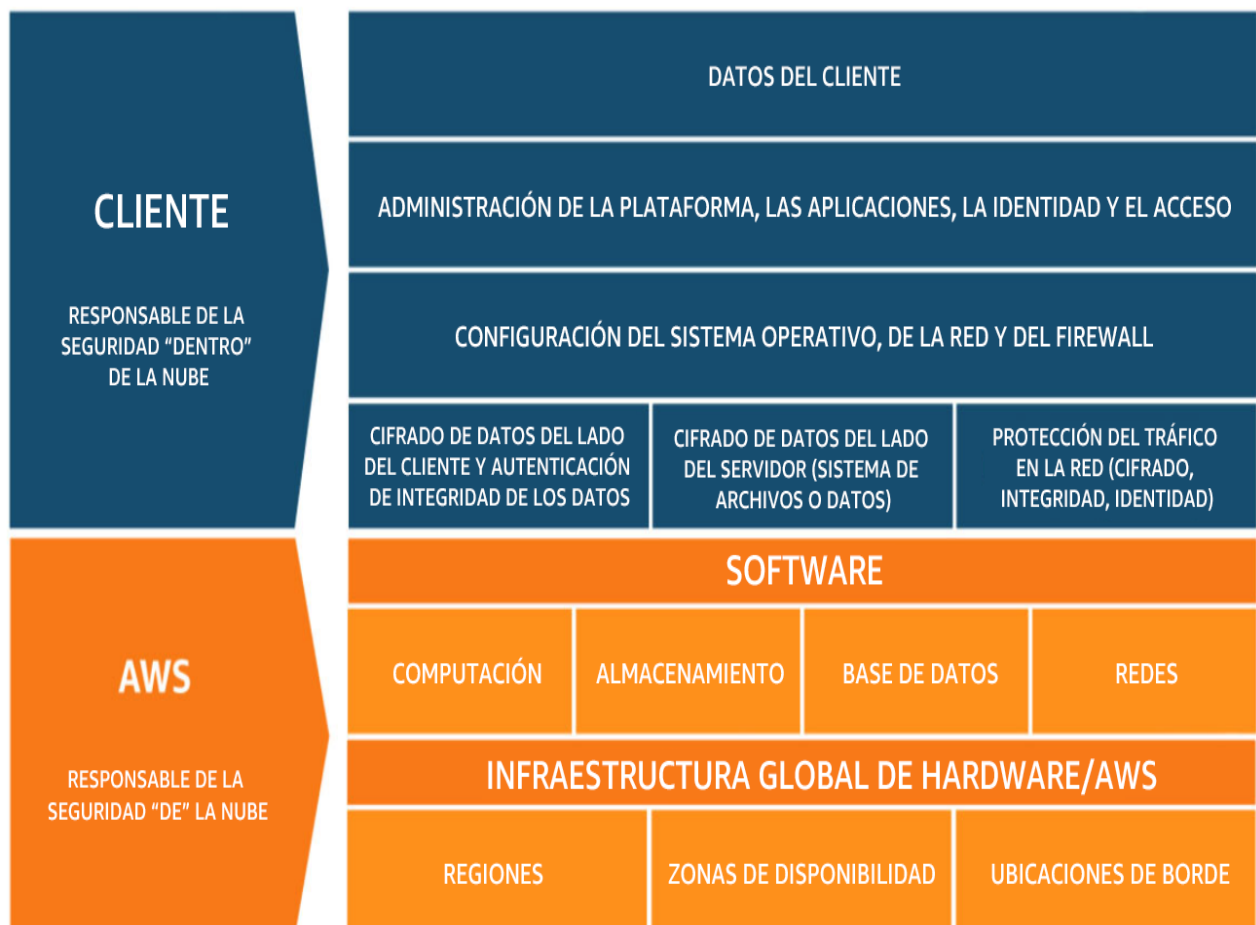
- Una región de AWS es una zona geográfica.
 - Usted controla la replicación de datos entre regiones.
 - La comunicación entre regiones utiliza la infraestructura de red troncal de AWS.
- Cada región proporciona a la red niveles plenos de redundancia y conectividad.
- Una región normalmente consta de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

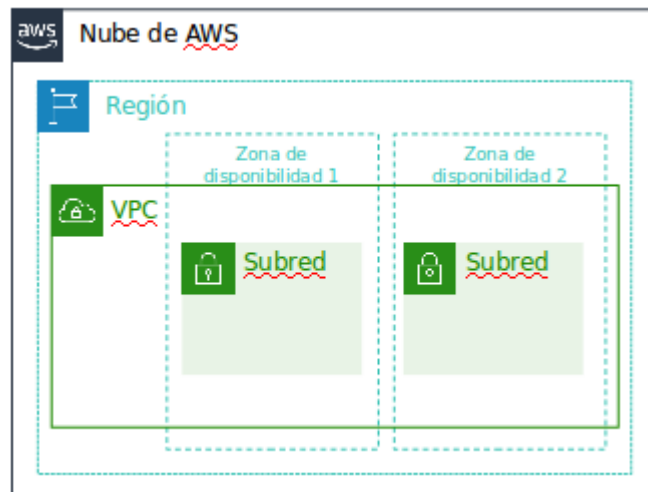
Amazon VPC. Redes

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 IPv4 más grande es /16.
- El tamaño de bloque de CIDR IPv4 más 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.

Tabla de enrutamiento principal (predeterminada)

Destino	Objetivo
10.0.0.0/16	local

Bloque de CIDR de VPC

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.

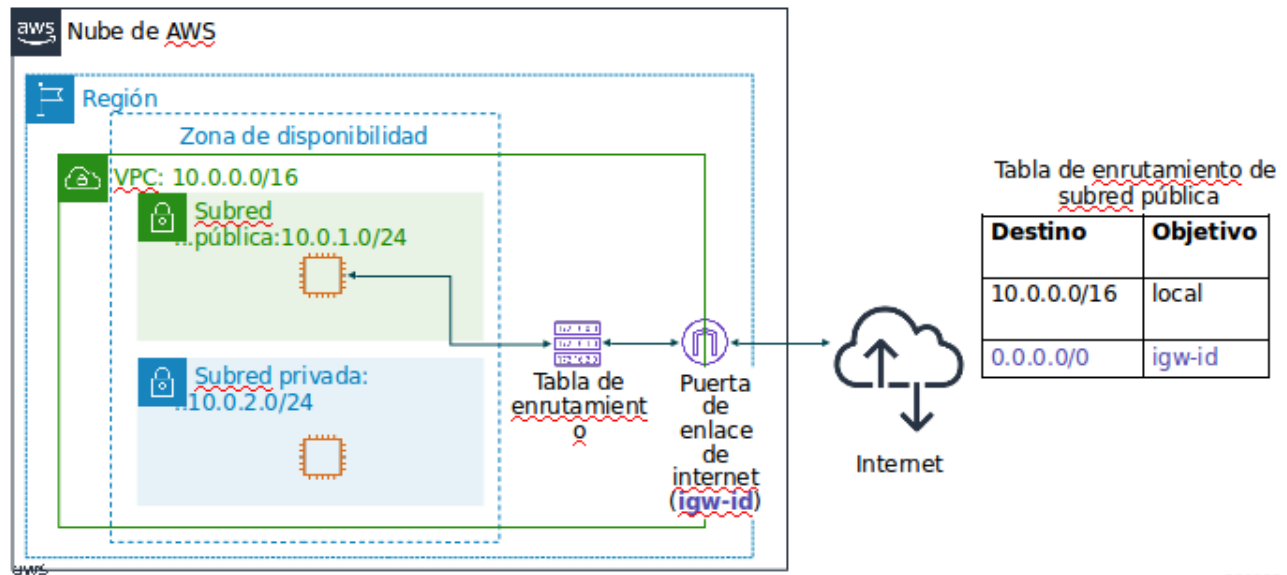
Las tablas de enrutamiento tienen una ruta local integrada.

Tiene rutas adicionales para la tabla.

Tablas de enrutamiento y rutas

- Una tabla de enrutamiento contiene un conjunto de reglas (o rutas) que puede configurarse para 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 (como máximo una).

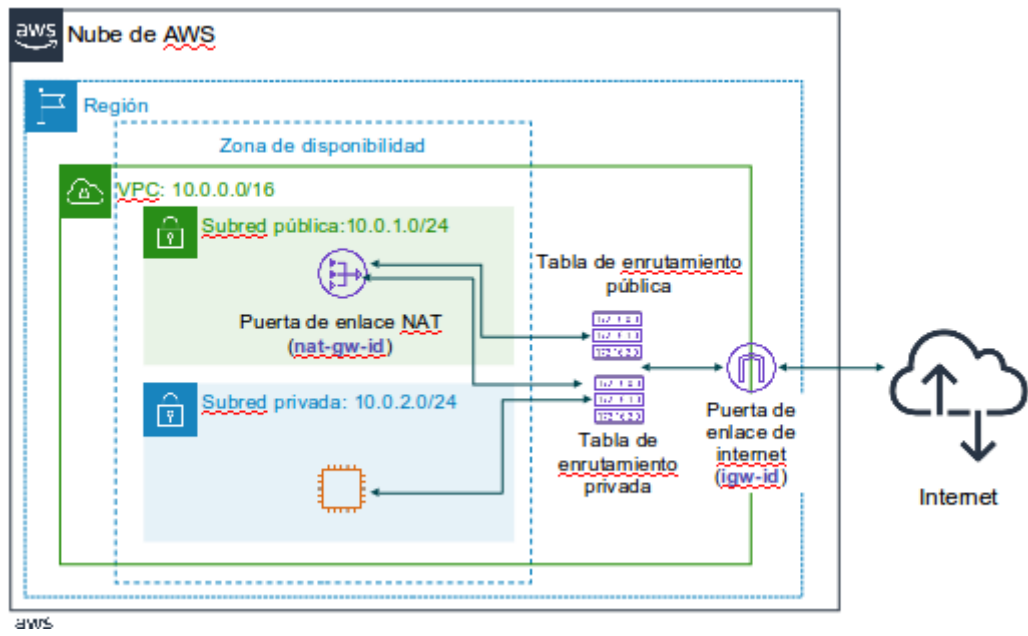
Puerta de enlace de internet



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

Panel

Vista global de EC2

Eventos

▼ Instancias

Instancias

Tipos de instancia

Plantillas de lanzamiento

Solicitudes de spot

Savings Plans

Instancias reservadas

Alojamientos dedicados

Reservas de capacidad

▼ Imágenes

AMI

Catálogo de AMI

▼ Elastic Block Store

Volúmenes

Instantáneas

Administrador del ciclo de vida

Instancias (1/1) Información

Última actualización: Hace less than a minute

Conectar

Estado de la instancia

Acciones

Lanzar instancias

Buscar instancia por atributo o etiqueta (case-sensitive)

Todos los...

1

<input checked="" type="checkbox"/>	Name	ID de la instancia	Estado de la i...	Tipo de inst...	Comprobación de	Estado de la al	Zona de dispon
<input checked="" type="checkbox"/>	ELinuxC	i-0344b91c7f83134dd	En ejecución	t2.micro	2/2 comprobaci	Ver alarmas +	us-east-1e

i-0344b91c7f83134dd (ELinuxC)

DetallesEstado y alarmasMonitoreoSeguridadRedesAlmacenamientoEtiquetas

▼ Detalles de redes Información

Dirección IPv4 pública

100.26.156.66 | dirección abierta

DNS de IPv4 pública

ec2-100-26-156-66.compute-1.amazonaws.com | dirección abierta

ID de subred

subnet-09db1ccc790943414

Direcciones IPv4 privadas

172.31.48.47

Nombre DNS de IP privada (solo IPv4)

ip-172-31-48-47.ec2.internal

Direcciones IPv6

-

ID de VPC

vpc-0c350a9c18f557d55

Direcciones IPv4 privadas secundarias

-

VPC

Panel de VPC

Vista global de EC2

Filtrar por VPC

Nube virtual privada

Sus VPC

Subredes

Tablas de enrutamiento

Puertas de enlace de Internet

Puerta de enlace de Internet de solo salida

Gateways de operador

Conjuntos de opciones de DHCP

Direcciones IP elásticas

Listas de prefijos administradas

Gateways NAT

Interconexiones

Sus VPC (1/1) Información

Last updated 1 minute ago

Acciones

Crear VPC

Buscar

ID de la VPC: vpc-0c350a9c18f557d55

Borrar filtros

1

<input checked="" type="checkbox"/>	Name	ID de la VPC	Estado	Bloquear el ...	CIDR IPv4	CIDR IP
<input checked="" type="checkbox"/>	-	vpc-0c350a9c18f557d55	Available	Desactivado	172.31.0.0/16	-

vpc-0c350a9c18f557d55

DetallesMapa de recursosCIDRRegistros de flujoEtiquetasIntegraciones

Detalles

ID de la VPC

vpc-0c350a9c18f557d55

Resolución de DNS

Habilitado

ACL de red principal

acl-04991632c8e02df7b

CIDR IPv6 (grupo de bordes de red)

Métricas de uso de direcciones de red

Estado

Available

Tenencia

default

VPC predeterminada

Sí

Bloquear el acceso público

Desactivado

Conjunto de opciones de DHCP

dopt-070de7568273f3e7c

CIDR IPv4

172.31.0.0/16

Grupos de reglas del firewall de DNS

Nombres de host de DNS

Habilitado

Tabla de enrutamiento principal

rtb-04d87272338118461

Grupo IPv6

-

ID de propietario

-

Mapa de recursos

Mapa de recursos Información

VPC Ocultar detalles

Su red virtual de AWS

vpc-0c350a9c18f557d55

172.31.0.0/16

Sin IPv6

Subredes (6)

Subredes dentro de esta VPC

us-east-1a

subnet-0d20228a0ca1a6304

172.31.16.0/20

Sin IPv6

us-east-1b

subnet-0b008c2a08c00b40

172.31.32.0/20

Sin IPv6

us-east-1c

subnet-0c3e51575ce93033e

172.31.0.0/20

Sin IPv6

us-east-1d

subnet-09f13785c79b6b12f

172.31.0.0/20

Sin IPv6

Tablas de enrutamiento (1)

Dirige el tráfico de red a los recursos

rtb-04d87272338118461

6 asociaciones de subredes

2 rutas, incluidas las locales

Conexiones de red (1)

Conexiones a otras redes

igw-04f557ef3f4a10ce7

Rutas de Internet a 6 subredes públicas

0 ruta(s) de subredes privadas a Internet

Panel de VPC

Panel de VPC

Vista global de EC2

Filtrar por VPC

Nube virtual privada

Sus VPC

Subredes

Tablas de enrutamiento

Puertas de enlace de Internet

Puerta de enlace de Internet de solo salida

Gateways de operador

Conjuntos de opciones de DHCP

Direcciones IP elásticas

Listas de prefijos administradas

Gateways NAT

Interconexiones

Seguridad

ACL de red

Grupos de seguridad

Sus VPC (1/2) Información

Buscar

	Name	ID de la VPC	Estado	Bloquear el a...	CIDR IPv4
<input type="checkbox"/>	-	vpc-0c350a9c18f557d55	Available	Desactivado	172.31.0.0/16
<input checked="" type="checkbox"/>	MI-VPC	vpc-074e0690521726494	Available	Desactivado	172.32.0.0/16

vpc-074e0690521726494 / MI-VPC

Detalles

Mapa de recursos

CIDR

Registros de flujo

Etiquetas

Integraciones

Detalles

ID de la VPC

vpc-074e0690521726494

Resolución de DNS

Habilitado

ACL de red principal

acl-04431db403abf0c00

CIDR IPv6 (grupo de bordes de red)

-

Estado

Available

Tenencia

default

VPC predeterminada

No

Métricas de uso de direcciones de red

Desactivado

Bloquear el acceso público

Desactivado

Conjunto de opciones de DHCP

dopt-070de7568273f3e7c

CIDR IPv4

172.32.0.0/16

Grupos de reglas del firewall de DNS de Route 53 Resolver

Mapa de recursos

Mapa de recursos Información

VPC Ocultar detalles

Su red virtual de AWS

MI-VPC

172.32.0.0/16

Sin IPv6

Subredes (2)

Subredes dentro de esta VPC

us-east-1f

Red-publica-bls

172.32.100.0/24

Sin IPv6

Red-publica

172.32.40.0/24

Sin IPv6

Tablas de enrutamiento (1)

Dirigir el tráfico de red a los recursos

rtb-0e16a1c9c74e29d3c

2 asociaciones de subredes

2 rutas, incluidas las locales

Conexiones de red (1)

Conexiones a otras redes

MI-puerta

Rutas de Internet a 2 subredes públicas

0 ruta(s) de subredes privadas a Internet