

Grado en Ingeniería de Software



Laboratorio de Bases de Datos y Sistemas Distribuidos

Curso 2023-2024



Tema 9

9

Servicio VPC y Security Groups

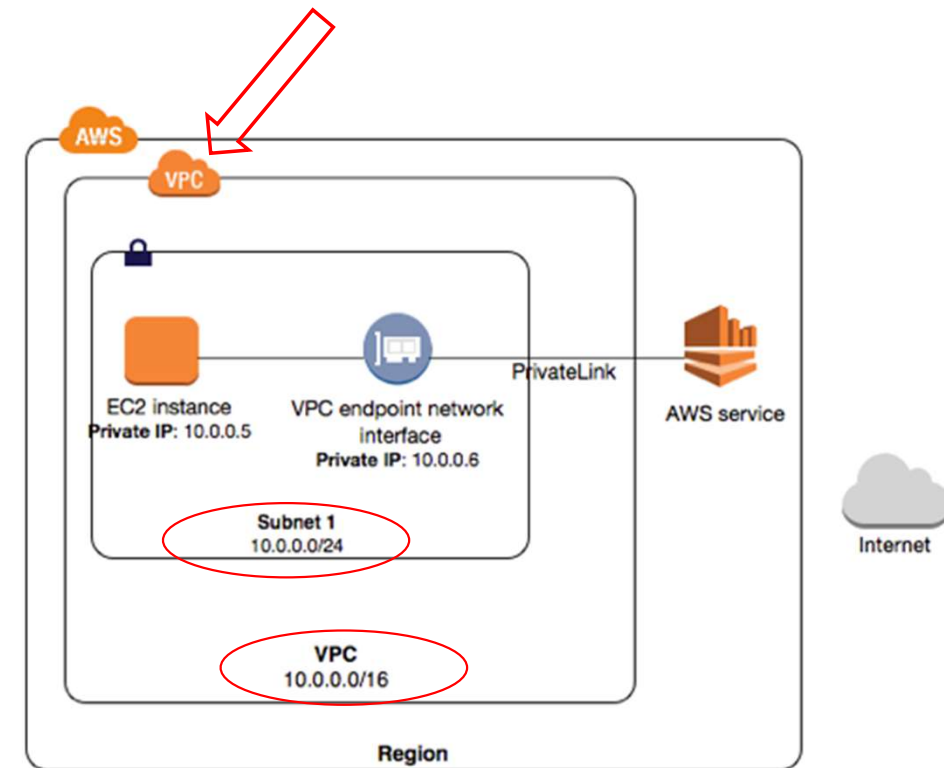
Ahora que ya sabemos crear una instancia de una máquina virtual (EC2) y una instancia de BD (RDS) vamos a profundizar en el servicio VPC y sus Security Groups.....

VPC – Virtual Private Cloud

Amazon **VPC** permite crear un entorno de red virtual en una sección **privada y aislada de la nube de AWS**, donde tener el control total sobre diversos elementos **como rangos de direcciones IP privadas, subredes, tablas de direccionamiento y gateways de red**. Digamos que una VPC nos permite definir una topología de red virtual y personalizar su configuración para simular una red IP tradicional que podemos utilizar en nuestro propio centro de datos.

Una instancia de EC2 y una instancia de BD se pueden ejecutar en una red virtual privada (VPC) de forma que se puede configurar el control de acceso a dichas instancias. Todas las instancias nuevas se crean en la VPC predeterminada, a menos que se especifique lo contrario.

La VPC predeterminada tiene asignado Grupos de Seguridad por defecto para definir las reglas del control de acceso a las instancias pertenecientes a esa red virtual.



Security Groups

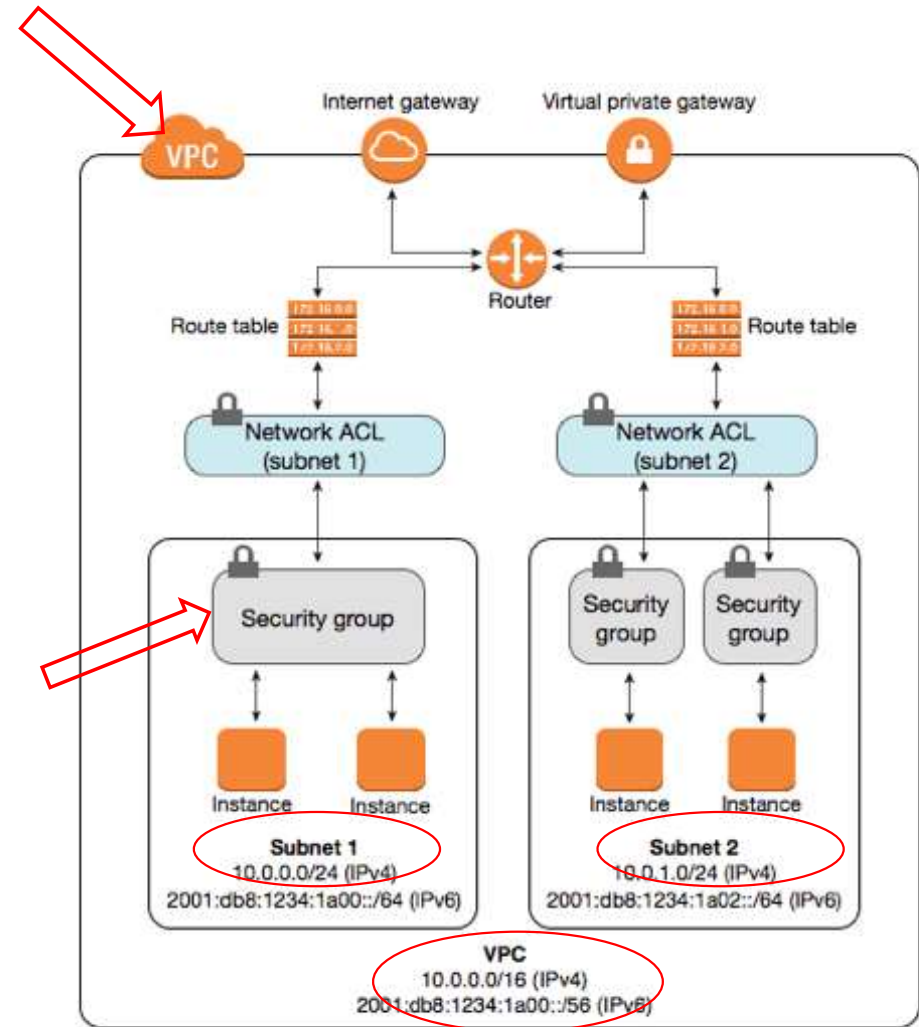
Un grupo de seguridad funciona como un firewall virtual que controla el acceso a una instancia.

Los grupos de seguridad controlan el acceso a las instancias de base de datos y a las instancias EC2 dentro de una VPC.

AWS tiene automáticamente un grupo de seguridad predeterminado para la VPC predeterminada en cada región. Si no especifica ningún grupo de seguridad al lanzar una instancia, esta se asocia automáticamente al grupo de seguridad predeterminado de la VPC. Si no desea que las instancias usen el grupo de seguridad predeterminado, puede crear sus propios grupos de seguridad personalizados y especificarlos al lanzar las instancias.

En cualquier momento podemos añadir reglas a cada grupo de seguridad que permitan el tráfico “a” o “desde” sus instancias asociadas. Las nuevas reglas se aplican automáticamente a todas las instancias que están asociadas al grupo de seguridad.

El servicio RDS utiliza diferentes tipos de grupos de seguridad, pero nosotros usaremos solo los Grupos de seguridad de VPC.

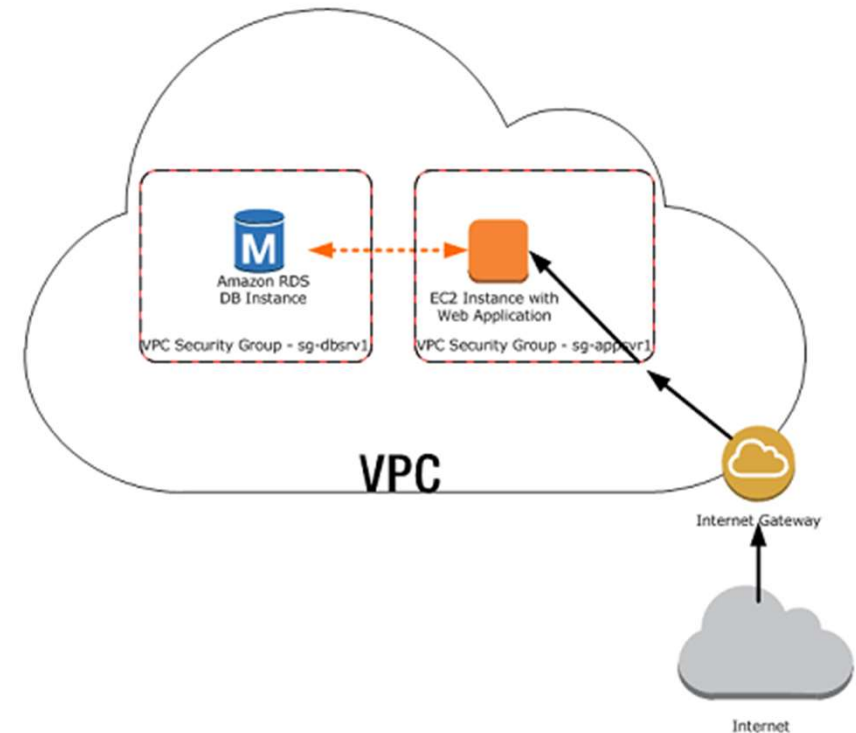


Escenario 1: acceso a una instancia de una BD desde una instancia EC2 situada en la misma VPC

Un uso común de una instancia de base de datos en una VPC es compartir datos con un servidor de aplicaciones que se ejecuta en una instancia EC2 de la misma VPC.

Este es el escenario de usuario que se crea cuando se utiliza AWS para crear una instancia EC2 y una instancia de base de datos en la misma VPC, utilizando dos grupos de seguridad diferentes, que debemos configurar adecuadamente, podemos permitir conexiones a la instancia de BD sólo desde las instancias EC2.

Se podría haber utilizado el mismo grupo de seguridad para ambos tipos de instancias.

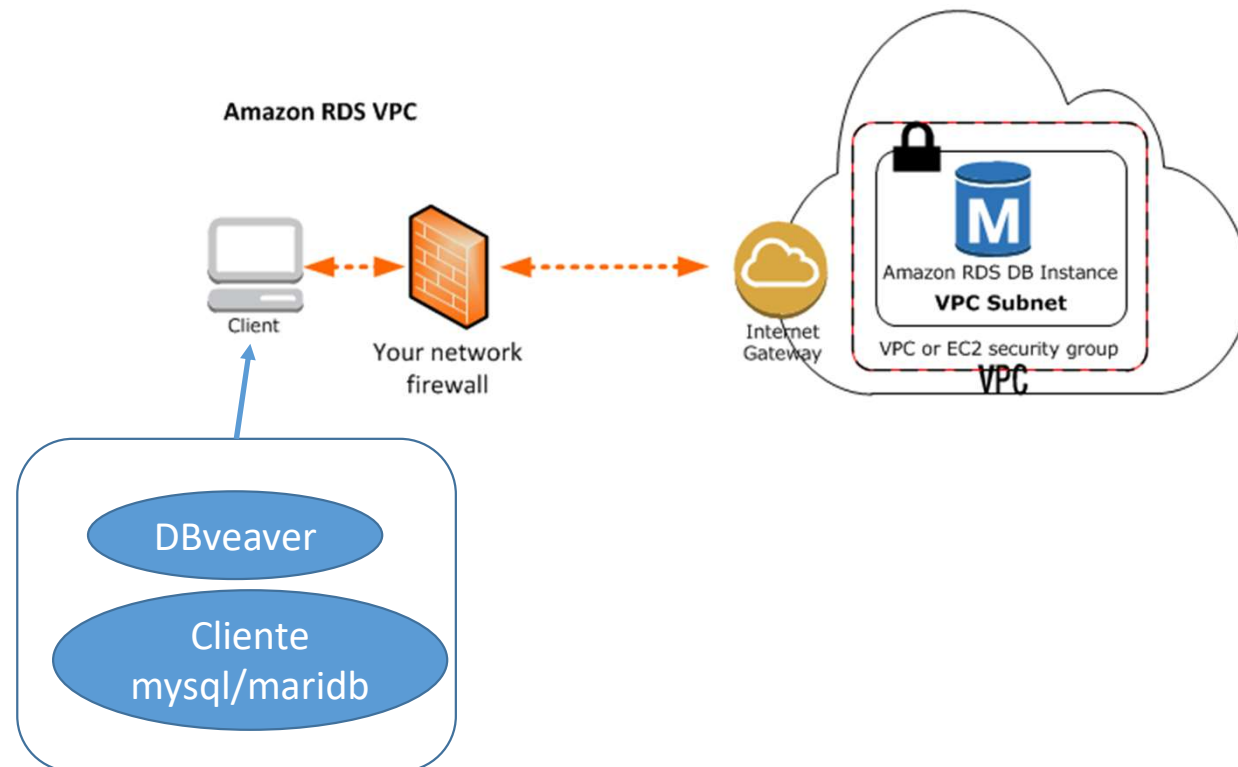


Escenario 2: Acceso a una instancia de base de datos situada en una VPC desde una aplicación cliente a través de Internet

Para acceder a una instancia de base de datos situada en una VPC desde una aplicación cliente a través de Internet, debemos configurar una VPC con una única subred pública y un gateway de Internet para permitir la comunicación a través de Internet.

En el siguiente diagrama se muestra este escenario.

Será necesario un grupo de seguridad (security group) asociado a la instancia de base de datos. Las reglas de entrada del grupo de seguridad permitirán a la aplicación cliente obtener acceso a la instancia de base de datos.





 Calle Playa de Liencres, 2 bis
(entrada por calle Rozabella)
Parque Europa Empresarial
Edificio Madrid
28290 Las Rozas, Madrid

 900 373 379  info@u-tad.com

 [SOLICITA MÁS INFORMACIÓN](#)



CENTRO ADSCRITO A:

 **Universidad
Camilo José Cela**

PROYECTO COFINANCIADO POR:

