Scenarios for accessing a DB instance in a VPC

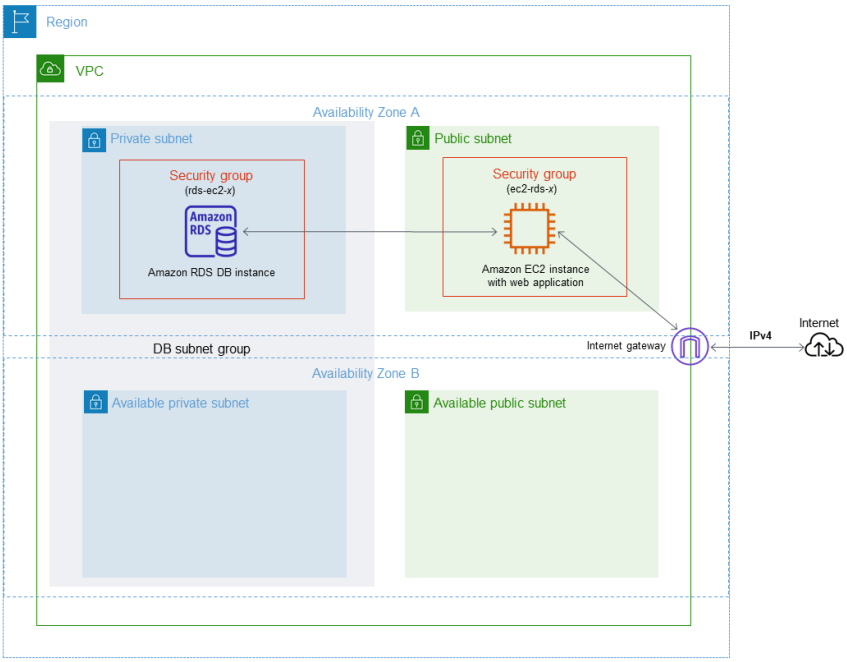
PDF (/pdfs/AmazonRDS/latest/UserGuide/rds-ug.pdf#USER_VPC.Scenarios) | RSS (rdsupdates.rss)

Amazon RDS supports the following scenarios for accessing a DB instance in a VPC:

A DB instance in a VPC accessed by an EC2 instance in the same VPC

A common use of a DB instance in a VPC is to share data with an application server that is running in an EC2 instance in the same VPC.

The following diagram shows this scenario.



The simplest way to manage access between EC2 instances and DB instances in the same VPC is to do the following:

- Create a VPC security group for your DB instances to be in. This security group can be used to restrict access to the DB instances. For example, you can create a custom rule for this security group. This might allow TCP access using the port that you assigned to the DB instance when you created it and an IP address you use to access the DB instance for development or other purposes.
- Create a VPC security group for your EC2 instances (web servers and clients) to be in. This security group can, if needed, allow access to the EC2 instance from the internet by using the VPC's routing table. For example, you can set rules on this security group to allow TCP access to the EC2 instance over port 22.
- Create custom rules in the security group for your DB instances that allow connections from the security group you created for your EC2 instances. These rules might allow any member of the security group to access the DB instances.

There is an additional public and private subnet in a separate Availability Zone. An RDS DB subnet group requires a subnet in at least two Availability Zones. The additional subnet makes it easy to switch to a Multi-AZ DB instance deployment in the future.

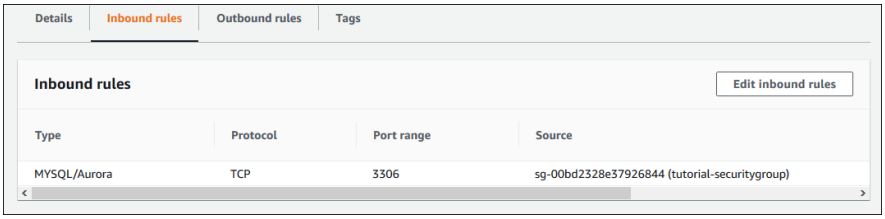
For a tutorial that shows you how to create a VPC with both public and private subnets for this scenario, see Tutorial: Create a VPC for use with a DB instance (IPv4 only) (./CHAP_Tutorials.WebServerDB.CreateVPC.html) .

> **Tip**
>
> You can set up network connectivity between an Amazon EC2 instance and a DB instance automatically when you create the DB instance. For more information, see .

To create a rule in a VPC security group that allows connections from another security group, do the following:

1. Sign in to the AWS Management Console and open the Amazon VPC console at https://console.aws.amazon.com/vpc (https://console.aws.amazon.com/vpc) .
2. In the navigation pane, choose **Security groups**.
3. Choose or create a security group for which you want to allow access to members of another security group. In the preceding scenario, this is the security group that you use for your DB instances. Choose the **Inbound rules** tab, and then choose **Edit inbound rules**.
4. On the **Edit inbound rules** page, choose **Add rule**.
5. For **Type**, choose the entry that corresponds to the port you used when you created your DB instance, such as **MYSQL/Aurora**.
6. In the **Source** box, start typing the ID of the security group, which lists the matching security groups. Choose the security group with members that you want to have access to the resources protected by this security group. In the scenario preceding, this is the security group that you use for your EC2 instance.
7. If required, repeat the steps for the TCP protocol by creating a rule with **All TCP** as the **Type** and your security group in the **Source** box. If you intend to use the UDP protocol, create a rule with **All UDP** as the **Type** and your security group in **Source**.
8. Choose **Save rules**.

The following screen shows an inbound rule with a security group for its source.

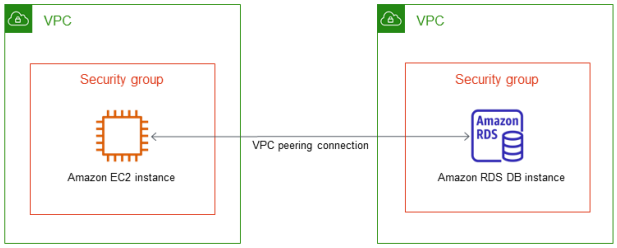


For more information about connecting to the DB instance from your EC2 instance, see Connecting to an Amazon RDS DB instance (./CHAP_CommonTasks.Connect.html) .

A DB instance in a VPC accessed by an EC2 instance in a different VPC

When your DB instances is in a different VPC from the EC2 instance you are using to access it, you can use VPC peering to access the DB instance.

The following diagram shows this scenario.

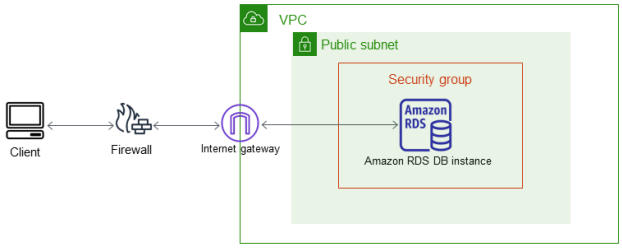


A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IP addresses. Resources in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, with a VPC in another AWS account, or with a VPC in a different AWS Region. To learn more about VPC peering, see VPC peering (https://docs.aws.amazon.com/vpc/latest/userguide/vpc-peering.html) in the *Amazon Virtual Private Cloud User Guide*.

A DB instance in a VPC accessed by a client application through the internet

To access a DB instances in a VPC from a client application through the internet, you configure a VPC with a single public subnet, and an internet gateway to enable communication over the internet.

The following diagram shows this scenario.



We recommend the following configuration:

- A VPC of size /16 (for example CIDR: 10.0.0.0/16). This size provides 65,536 private IP addresses.
- A subnet of size /24 (for example CIDR: 10.0.0.0/24). This size provides 256 private IP addresses.
- An Amazon RDS DB instance that is associated with the VPC and the subnet. Amazon RDS assigns an IP address within the subnet to your DB instance.
- An internet gateway which connects the VPC to the internet and to other AWS products.
- A security group associated with the DB instance. The security group's inbound rules allow your client application to access to your DB instance.

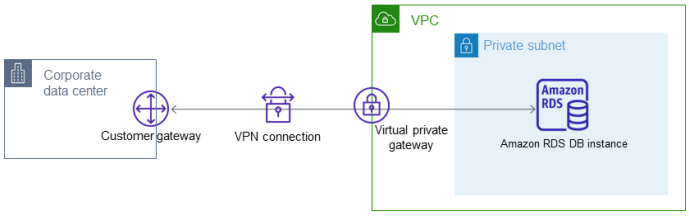
For information about creating a DB instances in a VPC, see Creating a DB instance in a VPC (./USER_VPC.WorkingWithRDSInstanceinaVPC.html#USER_VPC.InstanceInVPC) .

A DB instance in a VPC accessed by a private network

If your DB instance isn't publicly accessible, you have the following options for accessing it from a private network:

- An AWS Site-to-Site VPN connection. For more information, see What is AWS Site-to-Site VPN? (https://docs.aws.amazon.com/vpn/latest/s2svpn/VPC_VPN.html)
- An AWS Direct Connect connection. For more information, see What is AWS Direct Connect? (https://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html)
- An AWS Client VPN connection. For more information, see What is AWS Client VPN? (https://docs.aws.amazon.com//vpn/latest/clientvpn-admin/what-is.html)

The following diagram shows a scenario with an AWS Site-to-Site VPN connection.



For more information, see Internetwork traffic privacy (./inter-network-traffic-privacy.html) .