

mpid=docs_headercta_contactus)

RDS&topic_url=https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Tutorials.WebServerDB.CreateVPC.html



▶ Documentation
(<https://docs.aws.amazon.com/index.html>) > [Amazon RDS](#)
(https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Tutorials.WebServerDB.CreateVPC.html)

Tutorial: Create a VPC for use with a DB instance (IPv4 only)

▶ [↓ PDF \(/pdfs/AmazonRDS/latest/UserGuide/rds-ug.pdf#CHAP_Tutorials.WebServerDB.CreateVPC\)](#)

▶ [↓ RSS \(rdsupdates.rss\)](#) Focus mode

On this page

- [Create a VPC with private and public subnets\(#CHAP_Tuto](#)
- [Create a VPC security group for a public web server\(#CHA](#)
- [Create a VPC security group for a private DB instance\(#CH](#)
- [Create a DB subnet group\(#CHAP_Tutorials.WebServerDB.Cr](#)
- [Deleting the VPC\(#CHAP_Tutorials.WebServerDB.CreateVP](#)

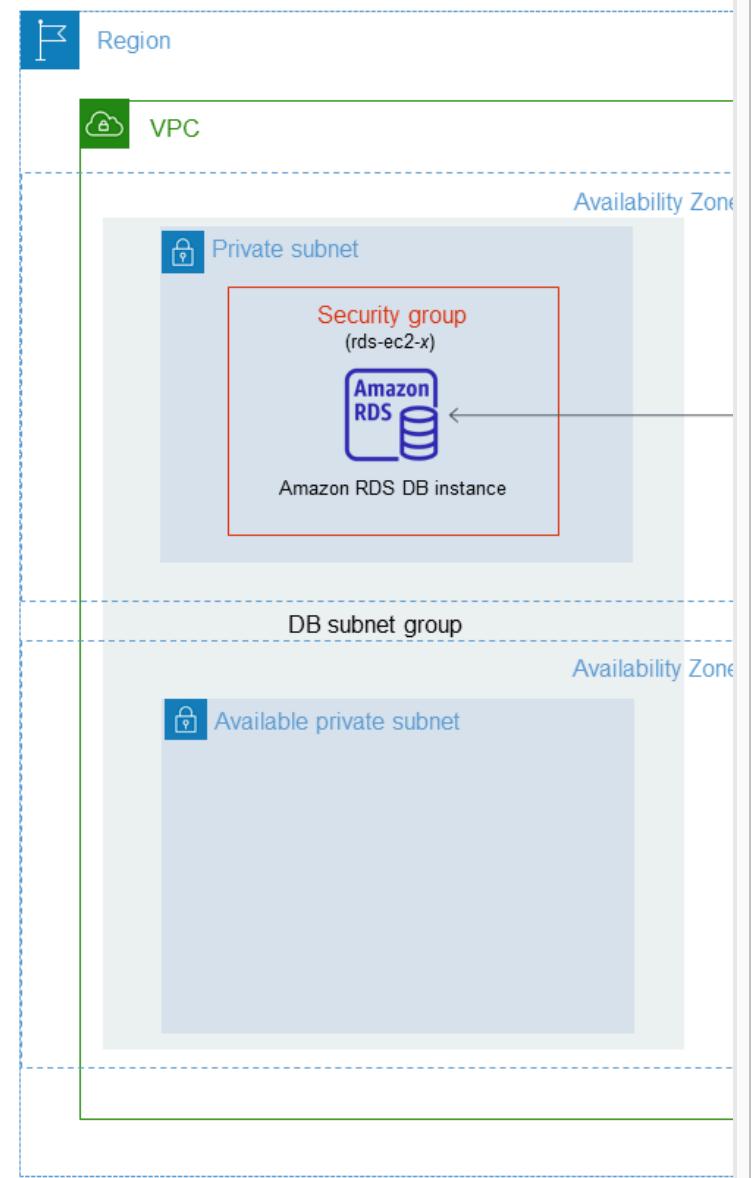
Related resources

- [Amazon RDS API Reference \(<https://docs.aws.amazon.com/AmazonRDS/latest/APIReference/>\)](#)
- [AWS CLI commands for Amazon RDS \(<https://docs.aws.amazon.com/cli/latest/reference/rds/>\)](#)

[groups](#)[\(Overview.RDSSecurityGroups.html\)](#)[Master user account privileges](#)[\(UsingWithRDS.MasterAccounts.htm\)](#)[SDKs & Tools ↗ \(<https://aws.amazon.com/tools/>\)](#)

A common scenario includes a DB instance in a virtual private cloud (VPC). This VPC shares data with a web server that is running in another VPC. This diagram shows this scenario.

The following diagram shows this scenario. For information about how to set up this scenario, see [Accessing a DB instance in a VPC \(./USER_VPC.Scenario\)](#).



Your DB instance needs to be available only to your VPC. To do this, you must create a VPC with both public and private subnets. This way, the DB instance can reach the public internet. The DB instance is hosted within the same VPC as the web server, so it cannot access the public internet, providing greater security.

This tutorial configures an additional public and private subnet for the DB instance. These subnets aren't used by the tutorial. An RDS DB subnet group contains three subnets: one public and two private. This additional subnet makes it easier to switch to a Multi-AZ deployment later.

This tutorial describes configuring a VPC for Amazon RDS. If you want to create a web server for this VPC scenario, see [Tutorial: Create a VPC for use with a web server \(IPv4 only\) \(./TUT_WebAppWithRDS.html\)](#). For more information about VPCs, see the [Amazon VPC User Guide \(https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/index.html\)](#) or the [Amazon VPC User Guide \(https://docs.aws.amazon.com/vpc/latest/userguide/index.html\)](#).

ⓘ Tip

You can set up network connectivity between the DB instance and the web server automatically when you create the DB instance. For more information, see [How to Set Up Network Connectivity Between an RDS DB Instance and an EC2 Instance \(./USER_CreateDBInstance.html#SetUpNetworkConnectivity\)](#).

Create a VPC with private and public subnets

Use the following procedure to create a VPC with both public and private subnets.

To create a VPC and subnets

1. Open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>.
2. In the top-right corner of the AWS Management Console, choose the Region. This example uses the US West (Oregon) Region.
3. In the upper-left corner, choose **VPC dashboard**.
4. For **Resources to create** under **VPC settings**, choose **Create VPC**.
5. For the **VPC settings**, set these values:
 - **Name tag auto-generation** – **tutorial**
 - **IPv4 CIDR block** – **10.0.0.0/16**

- **IPv6 CIDR block – No IPv6 CIDR block**
- **Tenancy – Default**
- **Number of Availability Zones (AZs) – 2**
- **Customize AZs** – Keep the default values.
- **Number of public subnet – 2**
- **Number of private subnets – 2**
- **Customize subnets CIDR blocks** – Keep the default values.
- **NAT gateways (\$)** – **None**
- **VPC endpoints** – **None**
- **DNS options** – Keep the default values.

i Note

Amazon RDS requires at least two subnet AZ DB instance deployments. This tutorial requirement makes it easier to convert to

6. Choose **Create VPC**.

Create a VPC security group for your DB instance

Next, you create a security group for public access. This security group will contain inbound rules to your VPC security group. These allow traffic from the Internet to your DB instance.

To create a VPC security group

1. Open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>.
2. Choose **VPC Dashboard**, choose **Security Group**.
3. On the **Create security group** page, set these values:
 - **Security group name:** **tutorial-security-group**
 - **Description:** **Tutorial Security Group**
 - **VPC:** Choose the VPC that you created earlier.
4. Add inbound rules to the security group.
 - a. Determine the IP address to use to connect to your DB instance. You can determine your public IP address, in a different section of this tutorial.

<https://checkip.amazonaws.com> (https://c

203.0.113.25/32.

In many cases, you might connect through a firewall without a static IP address. If so, fin

⚠ Warning

If you use **0.0.0.0/0** for SSH access to your public instances using SSH. This is safe in a development environment, but it's unsafe for production environments. Instead, use a specific IP address or range of addresses.

- b. In the **Inbound rules** section, choose **Add rule**.
 - c. Set the following values for your new inbound rule:
Instance type: Amazon Linux 2
Instance ID: The ID of your EC2 instance.
Port: 22
Protocol: TCP
Type: SSH
Source: The IP address or range from Step 1.
 - d. Choose **Add rule**.
 - e. Set the following values for your new inbound rule:
Port: 80
Protocol: TCP
Type: HTTP
Source: **0.0.0.0/0**
5. Choose **Create security group** to create the security group. Note the security group ID because you need it later.

Create a VPC security group for your DB instance

To keep your DB instance private, create a second security group. When you add inbound rules to your security group, you add inbound rules to your DB instance. You can't connect to your DB instance unless it has a security group with inbound rules that allow connections from your server only.

To create a VPC security group

1. Open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>.
2. Choose **VPC Dashboard**, choose **Security Groups** in the left navigation bar.
3. On the **Create security group** page, set these values:

- **Security group name:** tutorial-db-security-group
 - **Description:** Tutorial DB Instance Security Group
 - **VPC:** Choose the VPC that you created earlier.
4. Add inbound rules to the security group.
 - a. In the **Inbound rules** section, choose **Add rule**.
 - b. Set the following values for your new inbound rule:
 - Amazon EC2 instance. If you do this, you can connect to your database instance from other Amazon EC2 instances. Doing so, you can store and retrieve data from your database instance.
 - Type: MySQL/Aurora
 - Source: The identifier of the **tutorial-security-group** that you created in this tutorial, for example: sg-9edd5c1
 5. Choose **Create security group** to create the security group.

Create a DB subnet group

A *DB subnet group* is a collection of subnets that you can associate with your database instances. A DB subnet group makes it possible for your database instances to communicate with each other.

To create a DB subnet group

1. Identify the private subnets for your database instances.
 - a. Open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>.
 - b. Choose **VPC Dashboard**, and then choose **Subnets**.
 - c. Note the subnet IDs of the subnets named **subnet-private1-us-west-2a** and **subnet-private2-us-west-2b**.You need the subnet IDs when you create your DB subnet group.
2. Open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
Make sure that you connect to the Amazon RDS service.
3. In the navigation pane, choose **Subnet groups**.
4. Choose **Create DB subnet group**.
5. On the **Create DB subnet group** page, set these values:
 - **Name:** tutorial-db-subnet-group

- **Description: Tutorial DB Subnet Group**
 - **VPC: tutorial-vpc (vpc- identifier)**
6. In the **Add subnets** section, choose the **Available subnets** dropdown and select **us-west-2a**. Then choose **Add**.
- For this tutorial, choose **us-west-2a** and **us-west-2b** as the private subnets you identified in the previous step.
7. Choose **Create**.
- Your new DB subnet group appears in the DB subnet groups list. Click the name of the DB subnet group to see details in the details pane, including a list of the subnets associated with the group.

Note

If you created this VPC to complete [Tutorial: Create a VPC for use with a DB instance \(IPv4 only\) \(./TUT_WebAppWithRDS.html\)](#), create the DB instance and the [Amazon RDS DB instance \(./CHAP_Tutorials.WebServerDB.CreateVPC.html\)](#).

Deleting the VPC

After you create the VPC and other resources for this tutorial, you can delete the VPC and other resources as needed.

Note

If you added resources in the VPC that you created before you can delete the VPC. For example, the VPC contains an Amazon S3 bucket or Amazon RDS DB instances. For more information, see https://docs.aws.amazon.com/vpc/latest/userguide/VPC_User_Guide.html.

To delete a VPC and related resources

1. Delete the DB subnet group.
 - a. Open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
 - b. In the navigation pane, choose **Subnet groups**.
 - c. Select the DB subnet group you want to delete.
 - d. Choose **Delete**, and then choose **Delete** in the confirmation dialog.

2. Note the VPC ID.

- a. Open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>.
- b. Choose **VPC Dashboard**, and then choose **VPCs**.
- c. In the list, identify the VPC that you created.
- d. Note the **VPC ID** of the VPC that you created.

3. Delete the security groups.

- a. Open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>.
- b. Choose **VPC Dashboard**, and then choose **Security Groups**.
- c. Select the security group for the Amazon RDS instance that you created in Step 1.
- d. For **Actions**, choose **Delete security groups**.
- e. On the **Security Groups** page, select the security group that you identified in Step 1, and then choose **Delete**. The security group name is **tutorial-securitygroup**.
- f. For **Actions**, choose **Delete security groups**.

4. Delete the VPC.

- a. Open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>.
- b. Choose **VPC Dashboard**, and then choose **VPCs**.
- c. Select the VPC you want to delete, such as **tutorial-vpc**.
- d. For **Actions**, choose **Delete VPC**.

The confirmation page shows other resources that will be deleted, including the subnets associated with the VPC.

- e. On the confirmation page, enter **delete**, and then choose **Delete**.

Related resources

[Amazon RDS API Reference](https://docs.aws.amazon.com/AmazonRDS/latest/APIReference/) (<https://docs.aws.amazon.com/AmazonRDS/latest/APIReference/>)

[AWS CLI commands for Amazon RDS](https://docs.aws.amazon.com/cli/latest/reference/rds/index.html) (<https://docs.aws.amazon.com/cli/latest/reference/rds/index.html>)

[SDKs & Tools](https://aws.amazon.com/tools/)  (<https://aws.amazon.com/tools/>)

View related pages Abstracts generated by AI

AmazonRDS › AuroraUserGuide

[Tutorial: Create a VPC for use with a DB cluster \(IPv4 only\)...](#)

Create VPC private public subnets, security groups for public web server, private DB cluster; create DB subnet group.

January 25, 2024

Discover highly rated pages Abstracts generated by AI

AmazonRDS › UserGuide

[Regions, Availability Zones, and Local Zones](#)

(<https://docs.aws.amazon.com/AmazonRDS/latest...>)

Amazon RDS enables placing resources like DB instances in multiple locations including Regions, Availability Zones, and Local Zones for low-latency access.

September 29, 2024