**Методическое пособие к практическому занятию**

**Тема: Создание базы данных на Amazon RDS DB instance**

**Цель: Знакомоство с облачным ресурсом** the Amazon EC2

**Create a web server and an Amazon RDS DB instance**

This tutorial helps you install an Apache web server with PHP and create a MySQL database. The web server runs on an Amazon EC2 instance using Amazon Linux, and the MySQL database is an Amazon RDS MySQL DB instance. Both the Amazon EC2 instance and the DB instance run in a virtual private cloud (VPC) based on the Amazon VPC service.

n the tutorial that follows, you specify the VPC, subnets, and security groups when you create the DB instance. You also specify them when you create the EC2 instance to host your web server. The VPC, subnets, and security groups are required for the DB instance and the web server to communicate. After the VPC is set up, this tutorial shows you how to create the DB instance and install the web server. You connect your web server to your DB instance in the VPC using the DB instance endpoint endpoint.

1. Complete the tasks in [Tutorial: Create an Amazon VPC for use with a DB instance](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Tutorials.WebServerDB.CreateVPC.html).

Before you begin this tutorial, make sure that you have a VPC with both public and private subnets, and corresponding security groups. If you don't have these, complete the following tasks in the tutorial:

* 1. [Create a VPC with private and public subnets](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Tutorials.WebServerDB.CreateVPC.html#CHAP_Tutorials.WebServerDB.CreateVPC.VPCAndSubnets)
  2. [Create additional subnets](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Tutorials.WebServerDB.CreateVPC.html#CHAP_Tutorials.WebServerDB.CreateVPC.AdditionalSubnets)
  3. [Create a VPC security group for a public web server](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Tutorials.WebServerDB.CreateVPC.html#CHAP_Tutorials.WebServerDB.CreateVPC.SecurityGroupEC2)
  4. [Create a VPC security group for a private DB instance](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Tutorials.WebServerDB.CreateVPC.html#CHAP_Tutorials.WebServerDB.CreateVPC.SecurityGroupDB)
  5. [Create a DB subnet group](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Tutorials.WebServerDB.CreateVPC.html#CHAP_Tutorials.WebServerDB.CreateVPC.DBSubnetGroup)

1. [Create a DB instance](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Tutorials.WebServerDB.CreateDBInstance.html)
2. [Create an EC2 instance and install a web server](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Tutorials.WebServerDB.CreateWebServer.html)

The following diagram shows the configuration when the tutorial is complete.


            Single VPC Scenario
        

Рис 1.

# Create an Amazon VPC for use with a DB instance

A common scenario includes a DB instance in an Amazon VPC, that shares data with a web server that is running in the same VPC. In this tutorial you create the VPC for this scenario.

The following diagram shows this scenario. For information about other scenarios, see [Scenarios for accessing a DB instance in a VPC](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_VPC.Scenarios.html).

Because your DB instance only needs to be available to your web server, and not to the public Internet, you create a VPC with both public and private subnets. The web server is hosted in the public subnet, so that it can reach the public Internet. The DB instance is hosted in a private subnet. The web server is able to connect to the DB instance because it is hosted within the same VPC, but the DB instance is not available to the public Internet, providing greater security.

This tutorial describes configuring a VPC for Amazon RDS DB instances. For more information about Amazon VPC, see [Amazon VPC Getting Started Guide](https://docs.aws.amazon.com/AmazonVPC/latest/GettingStartedGuide/) and [Amazon VPC User Guide](https://docs.aws.amazon.com/vpc/latest/userguide/).

## 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/>

 .

 In the top-right corner of the AWS Management Console, choose the region to create your VPC in. This example uses the US West (Oregon) region.

 In the upper-left corner, choose **VPC Dashboard**. To begin creating a VPC, choose **Launch VPC Wizard**.

 On the **Step 1: Select a VPC Configuration** page, choose **VPC with Public and Private Subnets**, and then choose **Select**.

 On the **Step 2: VPC with Public and Private Subnets** page, set these values:

* **IPv4 CIDR block:** 10.0.0.0/16
* **IPv6 CIDR block:** No IPv6 CIDR Block
* **VPC name:** tutorial-vpc
* **Public subnet's IPv4 CIDR:** 10.0.0.0/24
* **Availability Zone:** us-west-2a
* **Public subnet name:** Tutorial public
* **Private subnet's IPv4 CIDR:** 10.0.1.0/24
* **Availability Zone:** us-west-2a
* **Private subnet name:** Tutorial Private 1
* **Instance type:** t2.small
* 

**Key pair name:** No key pair

* **Service endpoints:** Skip this field.
* **Enable DNS hostnames:** Yes
* **Hardware tenancy:** Default

 When you're finished, choose **Create VPC**.

## Create additional subnets

You must have either two private subnets or two public subnets available to create a DB subnet group for a DB instance to use in a VPC. Because the DB instance for this tutorial is private, add a second private subnet to the VPC.

**To create an additional subnet**

1. Open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>

 .

 To add the second private subnet to your VPC, choose **VPC Dashboard**, choose **Subnets**, and then choose **Create subnet**.

 On the **Create subnet** page, set these values:

* **Name tag:** Tutorial private 2
* **VPC:** Choose the VPC that you created in the previous step, for example: vpc-identifier tutorial-vpc
* **Availability Zone:** us-west-2b
* 

**IPv4 CIDR block:** 10.0.2.0/24

 When you're finished, choose **Create**. Next, choose **Close** on the confirmation page.

 To ensure that the second private subnet that you created uses the same route table as the first private subnet, complete the following steps:

1. Choose **VPC Dashboard**, choose **Subnets**, and then choose the first private subnet that you created for the VPC, Tutorial private 1.
2. Below the list of subnets, choose the **Route Table** tab, and note the value for **Route Table**—for example: rtb-98b613fd.
3. In the list of subnets, deselect the first private subnet.
4. In the list of subnets, choose the second private subnet Tutorial private 2, and choose the **Route Table** tab.
5. If the current route table is not the same as the route table for the first private subnet, choose **Edit route table association**. For **Route Table ID**, choose the route table that you noted earlier—for example: rtb-98b613fd. Next, to save your selection, choose **Save**.

## Create a VPC security group for a public web server

Next you create a security group for public access. To connect to public instances in your VPC, you add inbound rules to your VPC security group that allow traffic to connect from the internet.

**To create a VPC security group**

1. Open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>

 .

 Choose **VPC Dashboard**, choose **Security Groups**, and then choose **Create security group**.

 On the **Create security group** page, set these values:

* **Security group name:** tutorial-securitygroup
* **Description:** Tutorial Security Group
* **VPC:** Choose the VPC that you created earlier, for example: vpc-identifier (tutorial-vpc)

 Add inbound rules to the security group.

1. Determine the IP address to use to connect to instances in your VPC. To determine your public IP address, in a different browser window or tab, you can use the service at <https://checkip.amazonaws.com>

. An example of an IP address is 203.0.113.25/32.

If you are connecting through an Internet service provider (ISP) or from behind your firewall without a static IP address, you need to find out the range of IP addresses used by client computers.

1. 

In the **Inbound rules** section, choose **Add rule**.

1. Set the following values for your new inbound rule to allow Secure Shell (SSH) access to your EC2 instance. If you do this, you can connect to your EC2 instance to install the web server and other utilities, and to upload content for your web server.
   * **Type:** SSH
   * **Source:** The IP address or range from Step a, for example: 203.0.113.25/32.
2. Choose **Add rule**.
3. Set the following values for your new inbound rule to allow HTTP access to your web server.
   * **Type:** HTTP
   * **Source:** 0.0.0.0/0.

 To create the security group, choose **Create security group**.

Note the security group ID because you need it later in this tutorial.

Обычный сценарий включает в себя экземпляр БД в Amazon VPC, который совместно использует данные с веб-сервером, работающим в том же VPC. В этом руководстве вы создадите VPC для этого сценария.

На следующей диаграмме показан этот сценарий. Дополнительные сведения о других сценариях см. В разделе сценарии доступа к экземпляру БД в VPC.

Поскольку ваш экземпляр БД должен быть доступен только вашему веб-серверу, а не общедоступному Интернету, вы создаете VPC как с публичной, так и с частной подсетями. Веб-сервер размещается в общедоступной подсети, поэтому он может выходить в общедоступный Интернет. Экземпляр БД размещается в частной подсети. Веб-сервер может подключаться к экземпляру БД, поскольку он размещен в том же VPC, но экземпляр БД недоступен для общедоступного Интернета, что обеспечивает большую безопасность.

**Создать VPC с частными и публичной подсетью**

Используйте следующую процедуру для создания VPC с публичной и частной подсетями.

**Для создания VPC и подсетей**

Шаг 1. Откройте консоль Amazon VPC по адресу https://console.aws.amazon.com/vpc/

Шаг 2. В правом верхнем углу консоли управления AWS выберите регион для создания VPC. В этом примере используется регион запад США (штат Орегон).

Шаг 3. В левом верхнем углу выберите пункт панель мониторинга VPC. Чтобы начать создание VPC, выберите Запустить мастер VPC.

Шаг 4. На Шаге 1: Выберите страницу конфигурации VPC, выберите VPC с общедоступными и частными подсетями, а затем нажмите кнопку Выбрать.

Шаг 5. На странице Шаг 2: VPC с публичными и частными подсетями установите следующие значения:

* Блок IPv4 CIDR: 10.0.0.0/16
* Блок IPv6 CIDR: нет блока IPv6 CIDR
* Наименование СИЗ: учебник-ВКК
* IPv4 CIDR публичной подсети: 10.0.0.0/24
* Зона доступности: us-west-2a
* Имя подсети: учебник общественное
* IPv4 CIDR частной подсети: 10.0.1.0/24
* Зона доступности: us-west-2a
* Имя частной подсети: учебник Private 1
* Тип экземпляра: t2.small
* Имя пары ключей: нет пары ключей
* Конечные точки обслуживания: пропустите это поле.
* Включить DNS-имена хостов: да
* Аренда оборудования: по умолчанию
* Когда вы закончите, выберите **Создать VPC**.