

README

BitBeat is a new startup that is planning to take the record industry and world by storm with its new product **BitBanger**, a web-based music mixer app.

As the newest member of the **BitBeat** cloud team, you're in charge of launching infrastructure for software testing purposes within the organization's default **Amazon Virtual Private Cloud (Amazon VPC)**. Using the **default Amazon VPC** allows for sporadic testing. The Amazon Elastic Compute Cloud (Amazon EC2) instances that make up the infrastructure are spun up quickly, used for testing, and then terminated. *(You don't need to create an Amazon VPC for intermittent testing since there is no long-term business requirement.)*

Since you started working on your task, the testing requirements have changed because the new **BitBeat** voice recognition project is quickly making progress. You are asked to create a new VPC in which you can deploy an Amazon EC2 instance that can be used for long-term testing. The testing infrastructure requires only one Amazon EC2 instance.

Since deploying an Amazon EC2 instance in a non-default VPC is different than using the *default VPC* provided with the account, this is your chance to put your skills to the test and show what you can do.



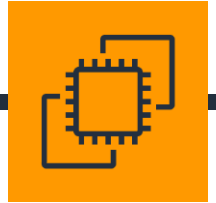
BEFORE GETTING STARTED

Here's some important information to know before starting this hands-on activity.

Activity time: 60 min

Requirements: You must have an AWS Educate account.

Getting help: If you experience any issues as you complete this activity, please ask your instructor for assistance.



Task overview

In this activity, you're going to create a new virtual private cloud (VPC) and deploy an Amazon EC2 instance in the network you create. Due to your **BitBeat** use case requirements, you will not use the *default* VPC in this activity. You will manually create your Amazon VPC, create and launch a webserver using a t-2 micro Amazon EC2 instance, and deploy your instance in the Amazon VPC you create.

You will create the new Amazon VPC without using the Wizard tool or default VPC and availability zones Amazon Web Services (AWS) provides.

Task objectives:

- Create an Amazon VPC
- Create route tables
- Configure and associate the route tables
- Create and attach an internet gateway (IGW)
- Create and launch an Amazon EC2
- Create a security group
- Test your webpage

Pro tip

AWS creates a *default* VPC that is ready for you to use so that you don't have to create and configure your own VPC.

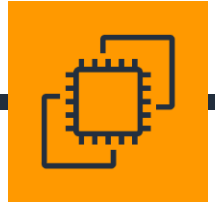
Learning outcomes

You will learn how to:

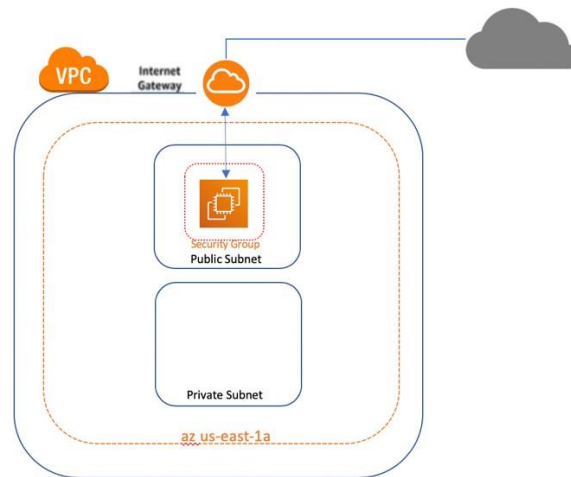
- Create a complete new Amazon VPC
- Provision and launch an Amazon EC2 instance within the Amazon VPC



Let's get started!



The diagram below shows the infrastructure you will build in this activity:



Create a virtual private cloud

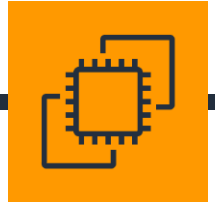
An Amazon VPC is a virtual network logically isolated from other networks in the AWS Cloud. Follow these steps to get started:

1. In the **AWS Management Console**, find and select VPC within the Network and Content Delivery category.
2. On the **VPC Dashboard** page, find and select *Your VPC*.
3. Click **Create VPC** and create a VPC with the following attributes:
 - a. **Name tag:** **VRTest VPC**
 - b. **IPv4CIDR block:** **10.0.0.0/16**
 - c. **Tenancy:** Default
4. Click **Create**.

Now that you have created your VRTest VPC, let's create subnets, route tables, an internet gateway (IGW), and configure the subnets and routing tables accordingly.

Subtask: Subnets

Subnets contain logical groupings of resources and are often how you segment a network for security. A public subnet is a subnet that's associated with a route table that has a route to the internet via an internet gateway. The public subnet is where you will be launching **BitBeat's** Amazon EC2 instance. Follow these steps to get started:



1. In the Virtual Private Cloud category of the VPC Dashboard, find and click on **Subnets**.
2. Click **Create subnet** and create a public subnet with the following attributes:
 - Name tag:** Public Subnet
 - VPC:** VRTest VPC
 - Availability Zone:** us-east-1a
 - IPv4 CIDR block*:** 10.0.1.0/24
3. Click **Create**, then **Close**.

Create a private subnet by repeating Steps 1 through 3:

- Name tag:** Private Subnet
- VPC:** VRTest VPC
- Availability Zone:** us-east-1a
- IPv4 CIDR block*:** 10.0.2.0/24

A private subnet is a subnet that's associated with a route table that allows communication of resources within your virtual private cloud and does not connect to the internet via an internet gateway. Resources in a private subnet are typically resources you want to keep secure from exposure to the internet. You will not be provisioning resources into the public subnet in this activity, but you need to know how to create one.

Create an internet gateway

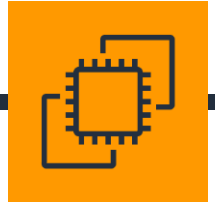
An internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between your VPC and the internet. An internet gateway serves two purposes: to provide a target in your VPC route tables for internet-routable traffic and to perform network address translation (NAT) for instances that have been assigned public IPv4 addresses. An internet gateway supports IPv4 and IPv6 traffic. It does not cause availability risks or bandwidth constraints on your network traffic. Essentially, the internet gateway connects your virtual private cloud to the internet. Follow these steps to get started:


1. In the Virtual Private Cloud category, click **Internet gateways** in the left sidebar.
2. Click **Create internet gateway**.
3. Enter a Name tag: VRTest IGW
4. Click **Create internet gateway**.

Subtask: Attach your internet gateway to your VPC

The internet gateway has been created and now needs to be attached to your VPC.

1. In the Virtual Private Cloud category, click **Internet gateways** in the left sidebar.



2. Find your Internet Gateway **VRTest IGW** and notice the state:  **Detached**
3. Select and highlight your internet gateway and go to **Actions** → **Attach to VPC**.
4. In the available VPCs box, click and select the **VRTest VPC** option from the list and click **attach internet gateway**.
5. Your IGW is now attached to your VRTest VPC.



DID YOU KNOW

Amazon reserves the first four (4) IP addresses and the last (1) IP address of every subnet for IP networking purposes. By default, you can create 200 subnets per VPC. If you would like to create more subnets, you need to contact AWS support.

Create route tables

A *route table* contains a set of rules, called *routes*, that are used to determine where network traffic from your subnet or gateway is directed. Your VPC has an implicit router, and you use route tables to control where network traffic is directed. Each subnet in your VPC must be associated with a route table, which controls the routing for the subnet (subnet route table). You can explicitly associate a subnet with a particular route table. Otherwise, the subnet is implicitly associated with the main route table. A subnet can only be associated with one route table at a time, but you can associate multiple subnets with the same subnet route table. Follow these steps to get started:

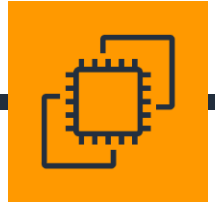
1. In the virtual private cloud category, find and click on **Route tables**.
2. Click the blue button **Create route table** and Create route table with **Name tag** *Public Route Table* and **VPC** *VRTest VPC*.
3. Click **Create**, then **Close**.

Repeat the above three steps—this time to create your private route table. Use the following:

Name tag *Private Route Table*
VPC *VRTest VPC*

Create route

1. In the virtual private cloud category, page find and click on **Route tables**.
2. Locate and select the box next to your public route table.



3. Click on the **Routes** tab and notice the route is 10.0.0.0/16 and local. You need to add a route to the internet using the IGW.
4. Click on the **Edit routes** button then click on the **Add route** button.

Important info

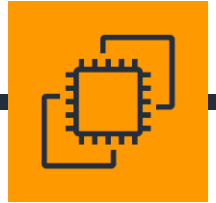
- Note the public route table isn't associated with any subnet. You need to attach this route table to the appropriate subnet.

5. Enter 0.0.0.0/0 in the **Destination** field and in the **Target** field, use the dropdown window and click on internet gateway. Locate your **VRTest VPC** IGW, select the VRTest VPC IGW, and click **Save routes**. Now, click **Close**.
6. With your public route table still selected, find and click the **Subnet associations** tab near the bottom of the page.
7. Click on the **Edit subnet associations** button. *You might have to resize your column headers to read correctly.* Then, click and highlight your **Public subnet**, and click **Save**.

The route table with the route you created to the IGW is now associated with your public subnet. Your public subnet now has access to the internet.

Important info

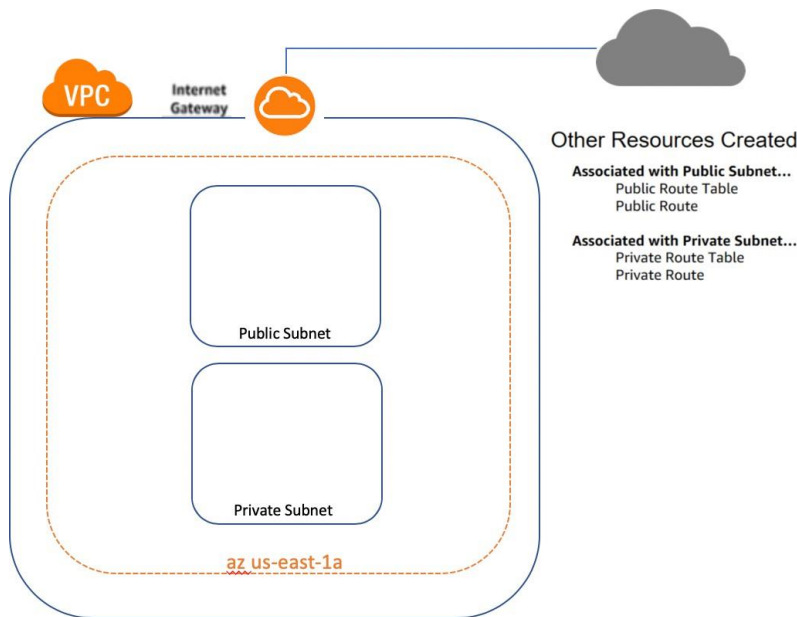
- You will not need to create a new route for your private route table, but you will need to associate the private route table with your private subnet. Note the public route table isn't associated with any subnet.



Create a private route table

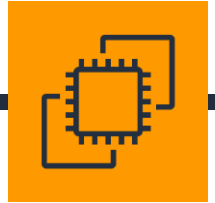
1. Repeat the above seven steps; this time editing your **private route table**.
2. Pay close attention and ensure you select **us-east-1a** for the AZ and the **Private subnet** options.

The diagram below shows the infrastructure you've created so far in this activity:



DID YOU KNOW

When you launch an Amazon EC2 instance, you must specify the subnet in which to launch the instance. The instance will be launched in the Availability Zone associated with the specified subnet. If you don't specify an Availability Zone, the default "no preference" option will be selected and the subnet will be created in an available Availability Zone in the region.



Create an Amazon EC2

1. In the **AWS Management Console**, find and select the Amazon EC2 dashboard.
2. From the **Amazon EC2 dashboard**, click **Launch instances**.
3. Notice the variety of AMIs located on the AMI page. These are different templates for different types of machines. Select the **Amazon Linux 2 AMI (HVM)**.
4. Notice the variety of instance types available. Select the **t2.micro instance**.
5. Select **Next: Configure instance details**.
6. In the **Step 3: Configure instance details** page, you need to configure the following settings:

Network: VRTest VPC

Subnet: Public subnet | us-east 1a

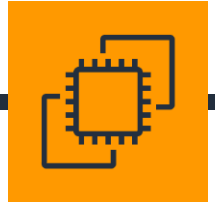
Auto-Assign Public IP: Enable



Scroll to the bottom of the page and locate the **Advanced details** section and expand if necessary. With the advanced details section expanded, insert the following bash script within the **User data** section:

```
#!/bin/bash
yum-y install httpd
systemctl enable httpd
systemctl start httpd
echo '<html><h1>Hello Earthling, Take me to your
leader! </h1></html>' >/var/www/html/index.html
```

7. Click **Next: Add storage**. You will not need another Amazon Elastic Block Store (Amazon EBS) volume.
8. Click **Next: Add tags**.
9. Click **Add tag**. Then, configure:
 - a. **Key:** Name **Value:** VR Testing Server
 - b. **Key:** Department **Value:** Development
10. Click **Next: Configure security group**.
11. Configure a new security group as follows:



1. **Security Group Name:** SSH and HTTP SG.
2. **Description:** This security group allows for SSH and HTTP.
3. By default, the Type SSH with Port 22 has been added.
4. Click the **Add rule** button and locate HTTP under the **Type** header. Then, change Custom to *Anywhere* under the **Source** heading.
5. Click **Review and launch**.

Important info

- You will not be using SSH in this activity so make sure you **proceed with a key pair** and **acknowledge**. Then, click **Launch instances**.

12. Review the details, scroll down, and click **Launch**.

This is an example snapshot from the AWS Management Console:

Select an existing key pair or create a new key pair ×

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

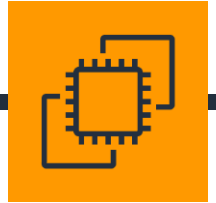
Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Proceed without a key pair ▼

☒ I acknowledge that I will not be able to connect to this instance unless I already know the password built into this AMI.

Cancel Launch Instances

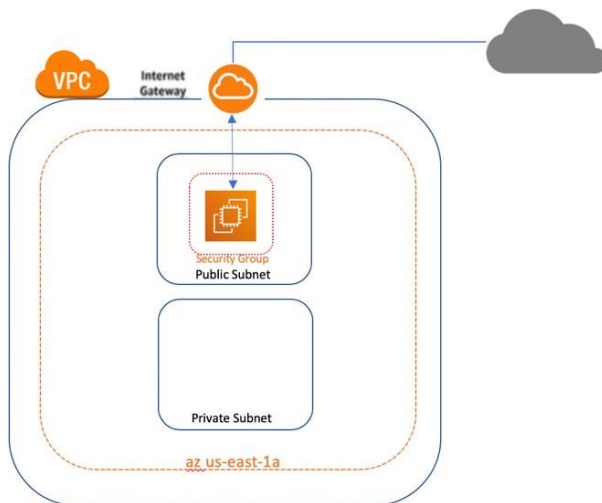
13. Click on **View instances** or navigate to the **Instances** category within the Amazon EC2 dashboard page.



Test your webpage

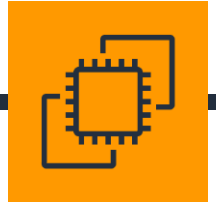
1. Select your **VR Amazon EC2 server** Instance and copy the **IPv4 public IP** address to your clipboard.
2. Open a new browser tab, paste the **public IP** address into a new browser window, and observe the results.
3. You should see **Hello Private Network. You did it! SUCCESS!** in your browser.

This is a diagram of the infrastructure you've just built in this activity:



DID YOU KNOW

You can run any number of Amazon EC2 instances within a VPC, so long as your VPC is appropriately sized to have an IP address assigned to each instance. You are initially limited to launching 20 Amazon EC2 instances at any one time and a maximum VPC size of /16 (65,536 IPs). If you would like to increase these limits, you need to contact AWS support.



Great job!

Let's review

You successfully launched an Amazon EC2 into an Amazon VPC that you created. You learned how to correctly configure a VPC and launch resources into it, instead of just relying on the default VPC AWS provides. You manually created the VPC from scratch and created and launched a webserver using a t-2 micro Amazon EC2 instance. You deployed your instance in the VPC you created and **did not** use any AWS provided defaults or wizard tools in this activity.

Take a few minutes to go back over this activity step by step and make sure you clearly understand each of the steps you completed and why you completed those steps for your task assignment. You will need to master these processes for success in your cloud computing career.

In this activity, you:

- Created an Amazon VPC
- Created route tables
- Configured and associated the route tables
- Created and attached an internet gateway
- Created and launched an Amazon EC2 instance
- Created a security group
- Tested your webpage

Test your knowledge

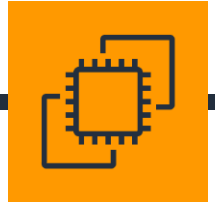
- ☐ What is a default VPC and why would you use it?

- ☐ When creating your public subnet, what must you do to make the subnet public?

- ☐ What role does the route table play in a VPC? _____

- ☐ If you do not specify the subnet and availability zone when creating an Amazon EC2 instance, what happens? _____

- ☐ What is the **auto-assign public IP** default setting? _____



- ☐ What will happen if you do not adjust the auto-assign public IP setting to “enable”? _____

- ☐ Describe what a security group is and why it’s important.

- ☐ Why did you create a private subnet? When would you use this?

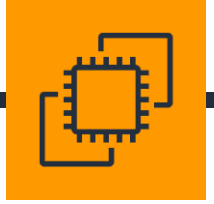
- ☐ What is the purpose of the internet gateway? What’s the result if you don’t create and attach an internet gateway to your VPC?

Bonus activity #1 – Create a stand-alone key pair

You launched an Amazon EC2 without a keypair in this activity because you didn’t need to SSH into the instance. In future activities, you may need to create a stand-alone keypair, or you may need to create a keypair in the process of launching an Amazon EC2 instance. In this bonus activity, let’s navigate the AWS Management Console and learn how to create a stand-alone keypair. The intended purpose of this bonus activity is to familiarize you with the location within the AWS Management Console where you would create a keypair if needed. Follow these steps to get started:

1. In the **AWS Management Console**, find and select the Amazon EC2 dashboard.
2. In the left-hand navigation, scroll down to the **Network and security** section and locate the *Key pairs* option.
3. After clicking on the **Key pairs** option, locate the **Create key pair** button and select.
4. On the Create key pair page, notice you will need to provide a name for the key pair you will create. Choose a name that will be easily recognized and will have meaning to you. The name can include up to 255 ASCII characters but cannot include leading or trailing spaces.
5. Notice there are two file formats in which you can save your key pair. The pem extension option is for use with OpenSSH, while the ppk extension option is used for PuTTY.

It is not necessary to create a key pair at this time. You can click **Cancel** and exit out of this bonus activity. In future activities, you may need to create a stand-alone key pair or create a key pair as part of the set-up process in creating an Amazon EC2 instance. You have achieved the objective of the bonus activity by navigating to and learning where key pair generation can be done.

**Bonus activity #2 – Cloud hygiene**

Make sure you practice good cloud hygiene. Terminate your Amazon EC2 instance and delete your VPC when it's no longer needed.

Resources

<https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html>

<https://docs.aws.amazon.com/vpc/latest/userguide/default-vpc.html>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-instance-addressing.html>

<https://aws.amazon.com/vpc/faqs/#:~:text=Currently%2C%20Amazon%20VPC%20supports%20five,ranges%20of%20your%20existing%20network.>