# AWS Certified

# Cloud Practitioner Exam

# Success Guide 2

Prepare for CLF-C01 Exam with quizzes, assessment tests, cheat sheets, hands-on lessons, and practice exams to build real-life experiences

By

*Ojula Technology Innovations*

**AWS Certified**

**Cloud Practitioner Exam**

**Success Guide**

*Volume 2*

Prepare for CLF-C01Exam with quizzes, assessment tests, cheat sheets, hands-on lessons and practice exams to build real-life experiences

ISBN: 9791220878692



**Published in the United States**

# Table of Contents

## About the Author

My name is Ojula Bright. I’m the CEO of Ojula Technology Innovations. My educational background is in software development, and I work with a few software developers and system engineers. I spent over 17 years as a software developer, and I’ve done a bunch of other things too. I've been involved in SDLC/process, data science, operating system security and architecture, and many more.

My most recent project is serverless computing where I simplify the building and running of distributed systems. I always use a practical approach in my projects and courses.

I hold a bunch of AWS certifications. As far as GCP goes, I've been certified by Google as both Associate Cloud Engineer and Professional Cloud Architect. Now I specialize in cloud computing and machine learning. I have created courses on cloud computing, operating systems, machine learning, data science and databases.

# 1. Getting Started

## 1.0. Introduction to Volume 2: How to Complete Your Preparation of the CLF-C01 Exam

This book is volume 2 of *AWS Certified Cloud Practitioner Exam Success Guide*. In this volume, you'll continue your lessons on Amazon Web Services. I'll help you complete your preparation and fast-track your AWS Certified Cloud Practitioner exam success. The great thing about the cloud practitioner exam is it's very suitable for people coming from many different backgrounds. So, it doesn't matter if you have little or no technical experience, or if you do have a technical background and you're looking to transition your skill sets into the cloud.

Whatever background you're coming from, the two volumes of my guide are all you need. If you've not read the first volume, please order it now and read it first. Everything you need is both volumes. They will help you pass your exam. You're not in this alone because I'm going to help you through it. My support link is at the end of this book for you to contact me any time if you need further help.

Whatever your preferred learning style, I've also got you covered. If you're a visual learner, you'll love my clear diagrams and illustrations throughout this book. You'll enjoy the facts I present to you and the cheat sheets I created because they have exam specific information in them. If you're a practical learner, you'll love my hands-on lessons so that you can get practical with AWS and learn in a hands-on way.

About the hands-on lessons, there're two different types of practical lesson in this volume. The first one is a **demo**. A demo is a pure demonstration in which I show you something, but you don't need to follow along. The reason I do that is that there are a few examples of where I want to show you something visually so that I can demonstrate to you some feature of AWS. But the set up might be a bit more complex than the cloud practitioner exam requires. Although there're just a few of those, they're a useful way to show you some things.

Now, the other one is a **hands-on lesson**. A hands-on lesson is a follow-along, so you can go through AWS in your own free tier account and build on AWS. It will give you practical experience, which is really the best way to learn and become competent.

At the end of many chapters of this volume, you'll find a lesson with links to cheat sheets and quizzes that you can use to test yourself as you go through the lessons. There's often an **exam cram** lesson as well at the end of each chapter. This is a fast-paced run through of the cool facts ideal for quick revision before you sit your exam.

At the end of this volume, I also provide **a link to download training resources, graphics and screenshots used in this book, cheat sheets, assessment tests, practice exams, and other helpful documents**. You can use them for quick references and revision as well. In this volume, I also provide a link to **full-length practice exams** so you can test yourself and see if you're

ready to sit the real thing. So, if you've read volume one, get started with volume 2 right now. I really hope you'll enjoy it.

# 2. Amazon VPC, Networking, and Hybrid

## 2.0. Introduction

Networking is a topic that can be quite complex. I've left it until this second volume of the guide to cover Amazon VPC because I wanted to expose you to it first. In the first volume, you've already deployed instances into VPCs, containers and so on. So, you've seen what it is and what it's about, but now I'll go into a lot more detail.

I'll also cover many of the other services for connecting into our VPC, such as Direct Connect and VPN technologies. I've done my best to make these complex subjects easy to digest, so I hope you enjoy this chapter.

## 2.1. Amazon Virtual Private Cloud (VPC)

You've already had some exposure to the Amazon Virtual Private Cloud, VPC. But what I've done is I've given you that exposure before we actually cover the topic in depth because it helps you understand what it is. You've kind of used it and also used something called a default VPC, which already exists in each region in your account by default.

So, the VPC is a virtual private cloud, and you can think of it as a virtual data center. So, it has a perimeter around it. Within that, you can create and launch your own AWS resources which you can keep private if you want to, or publish them to the outside world. Now, have a look at this diagram to help you understand what a VPC is.

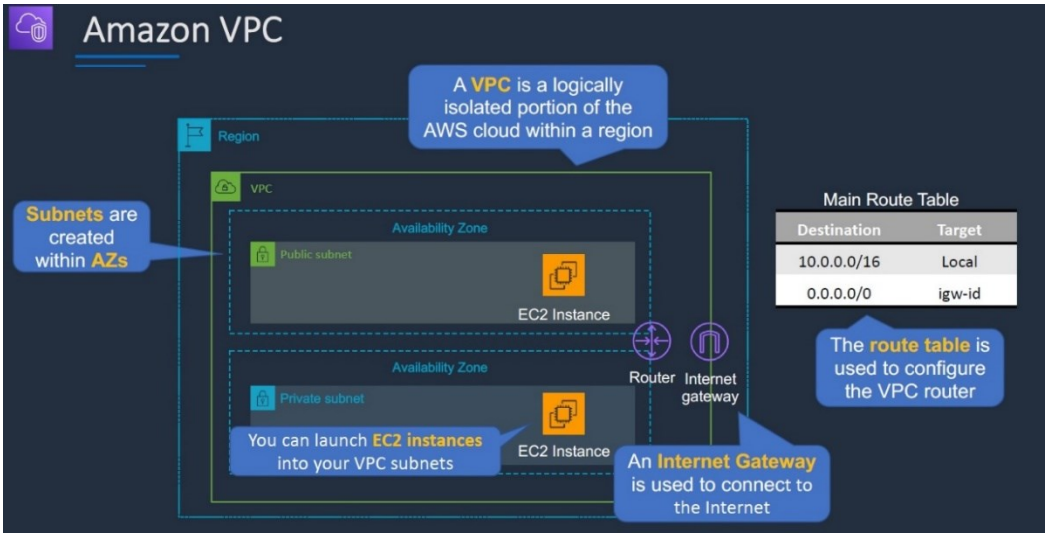


*Figure 2.1.1: An illustration of Amazon VPC*

A VPC is a logically isolated portion of the cloud within a region. So, it's always within a region. It cannot span across regions. Within a region, we have a VPC. We can have more than one but within the region shown in Figure 2.1.1, we have one VPC. We then create our subnets within

availability zones. In the diagram, we have two subnets, and each one is in a separate availability zone. A subnet cannot go across availability zones, but you can have multiple subnets within an availability zone.

Now, we have something called a **router**. You don't need to understand too much about routing and IP addressing for the Cloud Practitioner Exam. But you *do* need to understand at a basic level what's happening in Figure 2.1.1. Within a VPC, we have a block of addresses. In this case, our block of addresses is 10.0.0.0/16. That's an address space. Within that space, all of our resources will have their own specific IP address, which is a unique IP address that's within that range.

Now, you don't see a router in AWS but you control it through the route table (shown on the far right of Figure 2.1.1). The router essentially knows how to forward traffic. For example, if you send data from an instance in one subnet to an instance in another subnet, when the router receives that data, it looks at the IP address information and knows where to send it. It also knows whether it's within the VPC. If it is, then here it's going to route it locally, that is, it knows not to send it outside. If it's an internet address we have the entry 0.0.0.0/0 in the route table that says for every other address (that is, anything that's not in this range), send it to the internet Gateway ID (**igw-id**).

The Internet Gateway attached to your VPC helps to send traffic to the outside world. So, if you're sending traffic to an internet address, the router says, well, that's not within my internal space. So, let's send it to the internet gateway. So, the internet gateway will forward it to the internet. We can then launch our EC2 instances and other resources into our subnets. Then they will be able to communicate with each other, either host to host, or via the router if it's in another subnet. If they want to connect to the outside world, they can use an Internet Gateway. But there's a little nuance to that with private subnets, which we'll cover later on in the chapter.

Within the region, we can create multiple VPCs. See Figure 2.1.2.

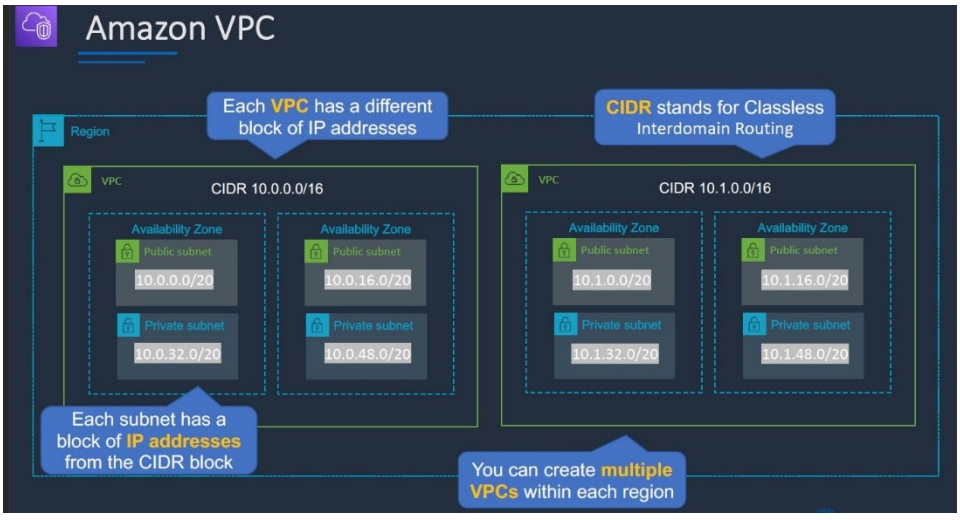


*Figure 2.1.2: An illustration of multiple VPCs*

Each VPC has a different block of IP addresses called CIDR. In the VPC block on the left, for example, we have a **CIDR**, which stands for **C**lassless **I**nter **D**omain **R**outing. It's a bit of a complex subject that's beyond the scope of this course. But just understand that within each VPC you have a block of addresses.

The subnets within the VPC have an address range, such as 10.**0**.0.0/20, that's from the overall block 10.**0**.0.0/16. So, 10.**0**.0.0/16 is a big block of addresses, and each subnet has a smaller block of addresses. Those addresses can then be assigned to EC2 instances. So, each subnet has the block of addresses that come from the overall CIDR block. Also, as you can see in Figure 2.1.2, each VPC has a slightly different block of addresses (10.**0**.0.0/16 is different from 10.**1**.0.0/16).

### 2.1.1. Components of a VPC

Now, there's quite a few components to a VPC and we're going to cover some of these in more detail. But you don't need to know too many of them in too much detail for this exam.

| VPC Component | What it is |
|---|---|
| Virtual Private Cloud (VPC) | A logically isolated virtual network in the AWS cloud |
| Subnet | A segment of a VPC's IP address range where you can place groups of isolated resources |
| Internet Gateway/Egress-only Internet Gateway | The Amazon VPC side of a connection to the public Internet for IPv4/IPv6 |
| Router | Routers interconnect subnets and direct traffic between Internet gateways, virtual private gateways, NAT gateways, and subnets |
| Peering Connection | Direct connection between two VPCs |
| VPC Endpoints | Private connection to public AWS services |
| NAT Instance | Enables Internet access for EC2 instances in private subnets managed by you) |
| NAT Gateway | Enables Internet access for EC2 instances in private subnets (managed by AWS) |
| Virtual Private Gateway | The Amazon VPC side of a Virtual Private Network (VPN) connection |
| Customer Gateway | Customer side of a VPN connection |
| AWS Direct Connect | High speed, high bandwidth, private network connection from customer to aws |
| Security Group | Instance-level firewall |
| Network ACL | Subnet-level firewall |

*Figure 2.1.3: Components of a VPC*

Firstly, we just discovered what a VPC is and what a subnet is. In Figure 2.1.3, we then have the Internet gateway, which is the Amazon VPC side of a connection to the public Internet. Now, an **Egress-only Internet gateway** is very similar to an Internet gateway, except it's used for the **IPv6** protocol, which is the newer protocol that replaces the IPv4 protocol. As I mentioned earlier, the router interconnects your subnets, and it routes traffic within your VPC and it's able to send traffic outside your VPC via other devices like Internet gateways.

A **peering connection** is a way that you can connect VPCs to each other so that they can send traffic internally between each other using their VPC routers. A **VPC endpoint** is something we will cover in a bit more detail. This is a way that you can connect to those public AWS services but using private IP addresses.

**NAT instances** and **NAT Gateways** will be covered in a bit more detail soon. These are a way that you can connect from a private subnet to the internet when your instances don't have a public IP address.

Next, we have two components in the diagram which are related to Amazon VPNs. With a virtual private network (VPN), we have something called a **Virtual Private Gateway**, which is an item on the AWS side, and then a **Customer Gateway**, which is the customer side of the connection. With these two together, we've then got the AWS side of the connection and the customer side of the connection, and you can create a virtual private network to your on-premises data center.

**AWS Direct Connect** is another way to connect from your data center. It offers much better performance and lower latency. It's another one that we'll talk about in a bit more detail soon. Next, we have **Security Groups** and **Network ACLs**. We're going to cover these in more detail. The security group is instance-level firewall and the Network ACL is subnet-level firewall.

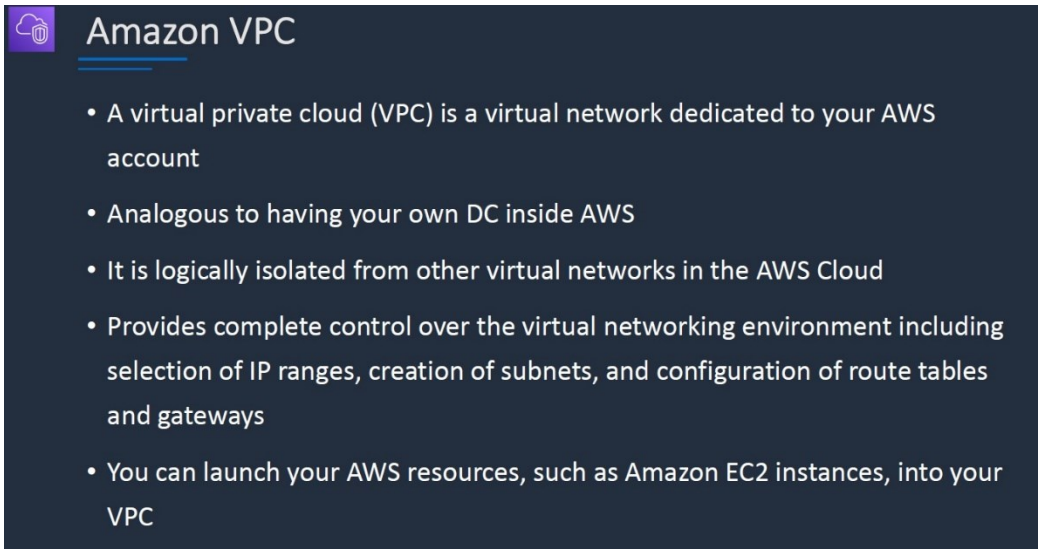


*Figure 2.1.4: Overview of Amazon VPC, part 1*

A virtual private cloud (VPC) is a virtual network dedicated to your account. It's similar to having your own data center in AWS and it's logically isolated from other virtual networks. You have complete control over the virtual networking environment. That means you can configure the IP ranges that you want to use, create your own subnets and configure your route tables the way you need to configure them for your own purposes. You can launch resources like EC2 instances into your VPC.

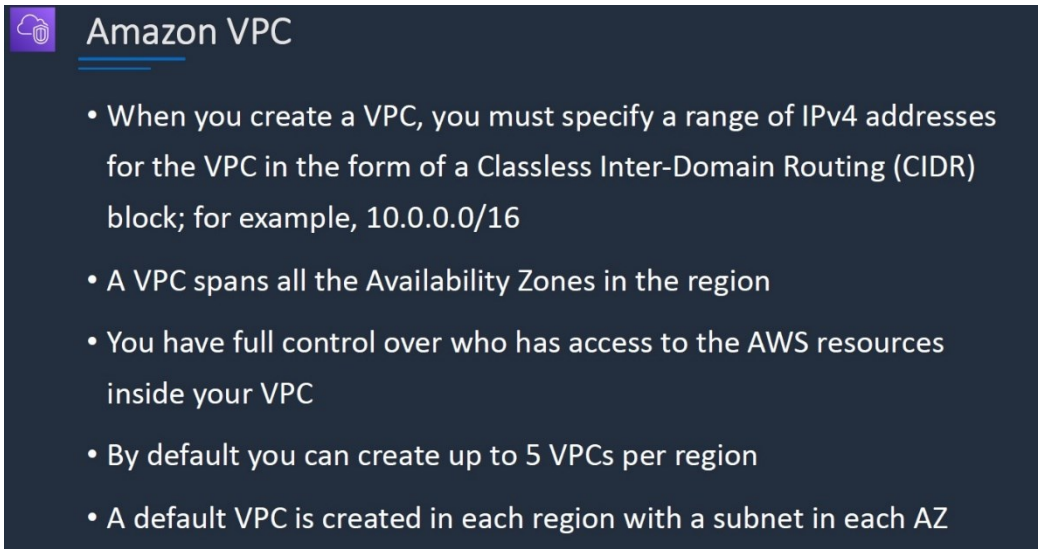


*Figure 2.1.5: Overview of Amazon VPC, part 2*

When you create a VPC (you're going to see this in the hands-on lesson), you're going to create your own custom VPC. You need to specify the IPv4 addresses, and you will use the classless inter-domain routing notation, for example, the address block 10.0.0.0/16.

A VPC spans all of the availability zones in the region. That means that you can create a subnet in each availability zone or multiple subnets in each availability zone. That gives you the ability to spread your resources across different availability zones, and that means different data centers. So, you get better redundancy.

You get full control over the access to resources inside your VPC as well. By default, you can create up to five VPCs per region and you can increase that limit if you need to. There's a default VPC that's created in each region and it always has one subnet in each availability zone.

That's it for the theory around VPC. In the next lesson, you're going to do some hands-on and create a custom VPC.