

Networking on AWS Notes

CIDR Notation

An important concept that's used in networking on AWS is CIDR, or *Classless Inter-Domain Routing*. CIDR network addresses are allocated in a virtual private cloud (VPC) and in a subnet by using CIDR notation. A /16 block provides 65,536 IPv4 addresses. A /24 block provides 256 addresses. [See this article](#) for more information about CIDR.

Amazon Virtual Private Cloud

Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including the selection of your own IP address range, the creation of subnets, and the configuration of route tables and network gateways. You can use both IPv4 and IPv6 in your VPC for secure and easy access to resources and applications. You could create up to five non-default VPCs per AWS account per Region. (See below for information about default VPCs.)

Details on Amazon VPC can be found here: <https://aws.amazon.com/vpc>

Subnets

A VPC spans all the Availability Zones in the Region. After creating a VPC, you can add one or more subnets in each Availability Zone. When you create a subnet, you specify the CIDR block for the subnet, which is a subset of the VPC CIDR block. Each subnet must reside entirely within one Availability Zone, and it can't span Availability Zones.

This is an important fundamental topic, and we strongly recommend that you review the information at: https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Subnets.html

Security in a VPC is provided by using Security Groups and Network Access Control Groups. We will talk about AWS Security in a later module.

Default VPC

In each Region, AWS will provision a default VPC. This VPC has a /16 IPv4 CIDR address block of 172.31.0.0/16. This provides 65,536 private IPv4 addresses. In addition, there will be a /20 subnet that is created for each Availability Zone in the Region, which provides 4,096 addresses per subnet, with a few addresses reserved for AWS usage. The route table that is associated with the default VPC will have a public route, which in turn is associated with a provisioned internet gateway.

You can modify or delete the default VPC if you want to do so.

The most current details on the default VPC can be found

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