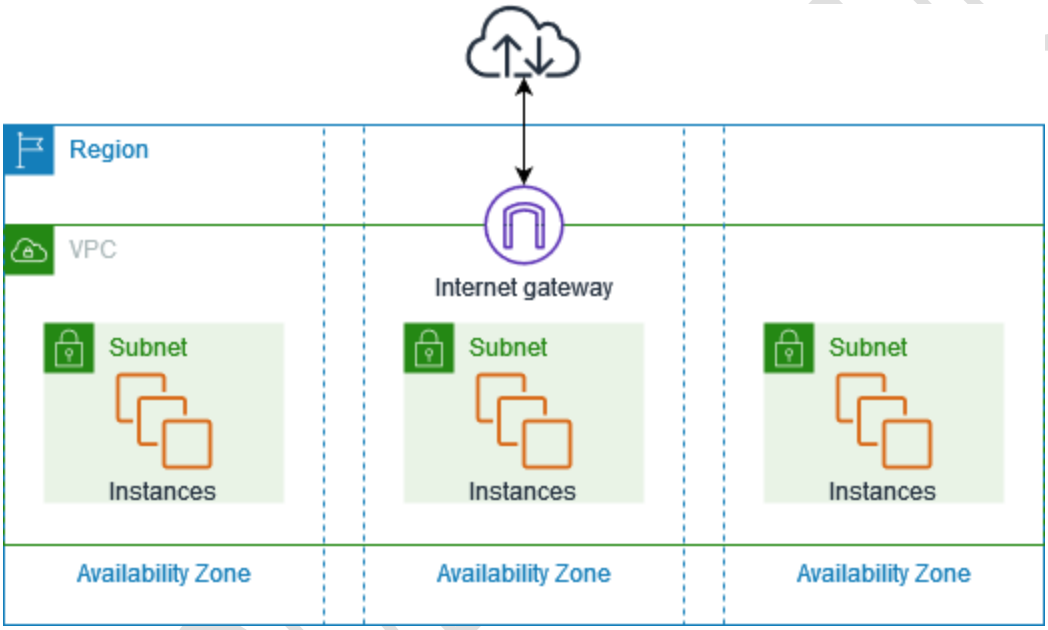
Amazon Virtual Private Cloud (VPC)

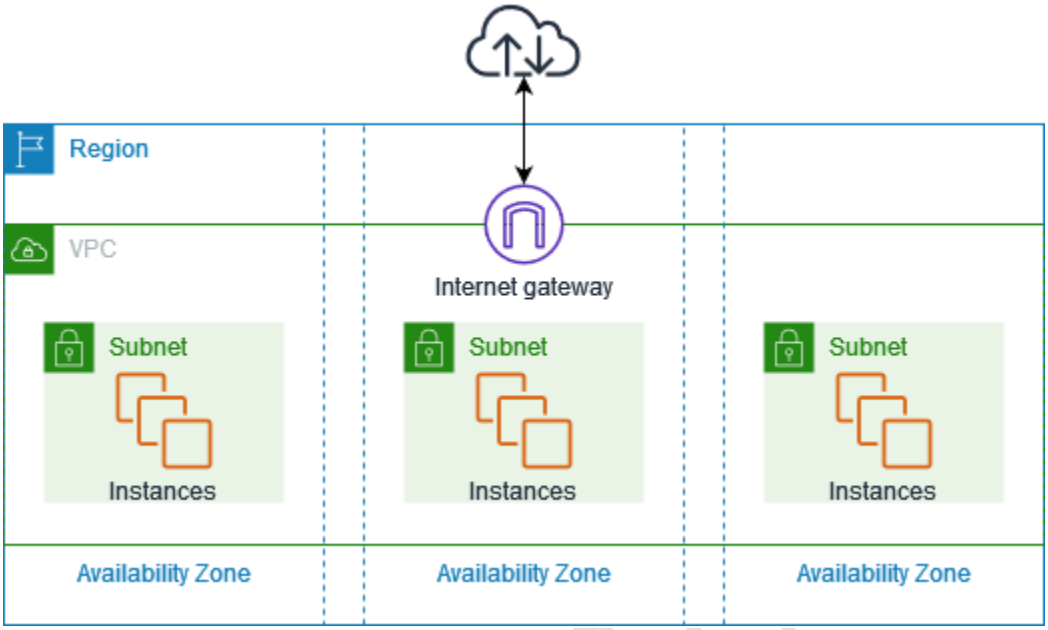
With Amazon Virtual Private Cloud (Amazon VPC), you can launch AWS resources in a logically isolated virtual network that you've defined. This virtual network closely resembles a traditional network that you'd operate in your own data center, with the benefits of using the scalable infrastructure of AWS.

The following diagram shows an example VPC. The VPC has one subnet in each of the Availability Zones in the Region, EC2 instances in each subnet, and an internet gateway to allow communication between the resources in your VPC and the internet.

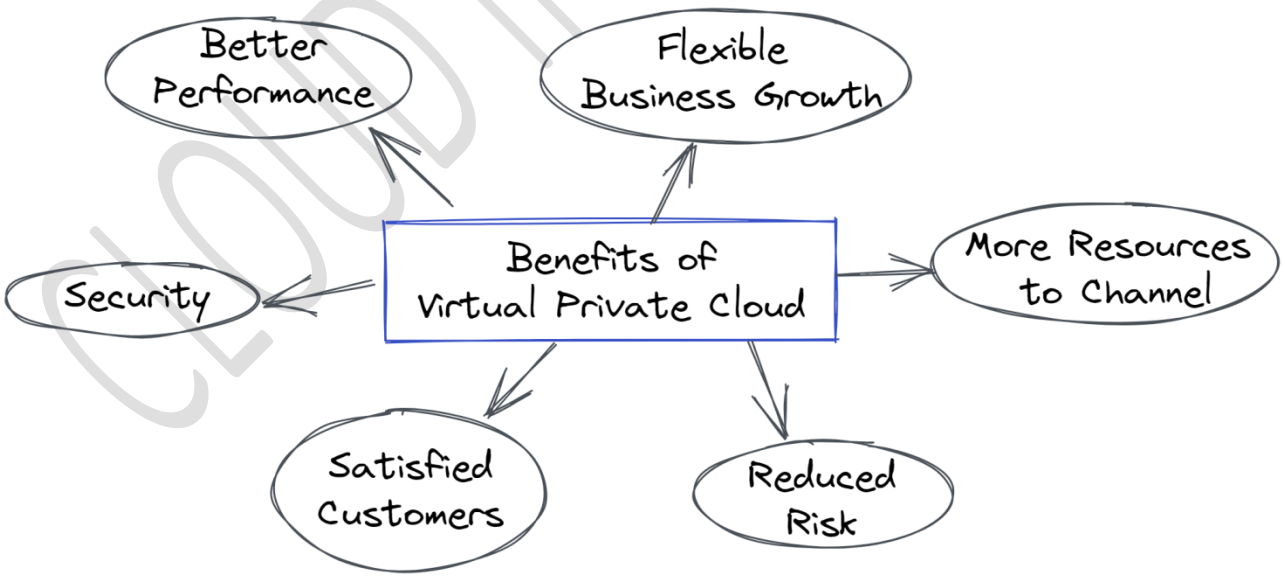


Introduction to Amazon Virtual Private Cloud (VPC)

- With Amazon Virtual Private Cloud (Amazon VPC), you can launch AWS resources in a logically isolated virtual network that you've defined. This virtual network closely resembles a traditional network that you'd operate in your own data center, with the benefits of using the scalable infrastructure of AWS.
- The following diagram shows an example VPC. The VPC has one subnet in each of the Availability Zones in the Region, EC2 instances in each subnet, and an internet gateway to allow communication between the resources in your VPC and the internet.



VPC Advantages



Default and Non-default VPC

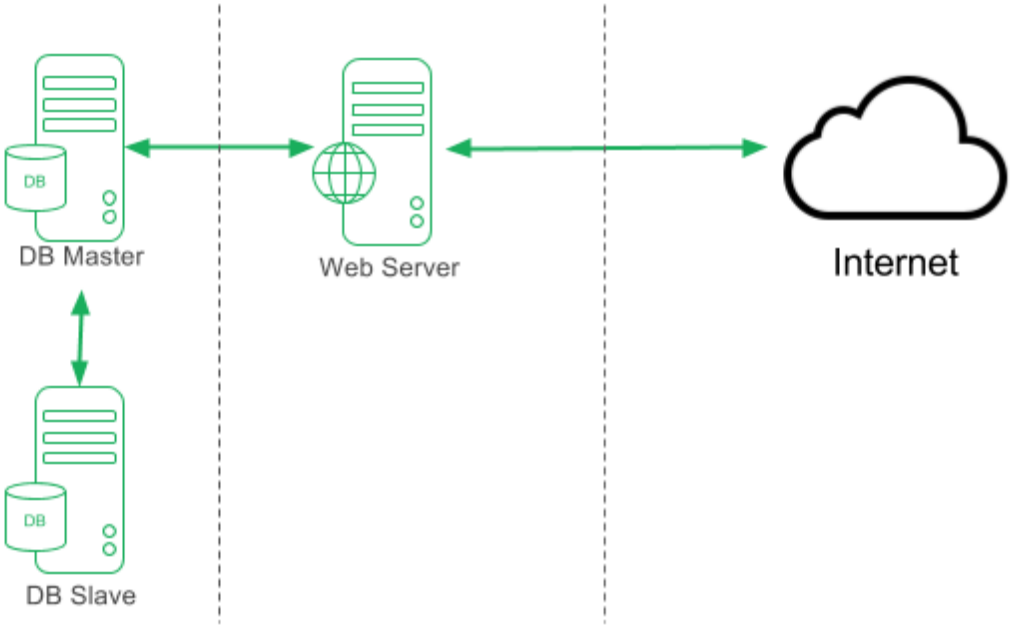
Defalut

When you start using Amazon VPC, you have a default VPC in each AWS Region. A default VPC comes with a public subnet in each Availability Zone, an internet gateway, and settings to enable DNS resolution. Therefore, you can immediately start launching Amazon EC2 instances into a default VPC. You can also use services such as Elastic Load Balancing, Amazon RDS, and Amazon EMR in your default VPC.

Default VPC components

When we create a default VPC, we do the following to set it up for you:

- Create a VPC with a size /16 IPv4 CIDR block (172.31.0.0/16). This provides up to 65,536 private IPv4 addresses.
- Create a size /20 default subnet in each Availability Zone. This provides up to 4,096 addresses per subnet, a few of which are reserved for our use.
- Create an internet gateway and connect it to your default VPC.
- Add a route to the main route table that points all traffic (0.0.0.0/0) to the internet gateway.
- Create a default security group and associate it with your default VPC.
- Create a default network access control list (ACL) and associate it with your default VPC.
- Associate the default DHCP options set for your AWS account with your default VPC.



Before we start..

It is a good idea to familiarize yourself with AWS VPC (Virtual Private Cloud) if you are not familiar with it already, please spend sometime to understand its concepts. This will help you greatly to go through this guide of how we create our stack template for our AWS non-default VPC.
We will create a VPC (Virtual Private Cloud) with subnets created in different availability zones *(different physical locations)* to ensure higher availability. *Learn more about AWS availability zones*
In this guide we will learn how to create:

1. AWS VPC (Virtual Private Cloud)
2. Subnets
3. Internet Gateway
4. Routing Tables
5. Security Groups
6. Attach Elastic IPs to our VMs
7. Create a VM within a subnet

Components of VPC

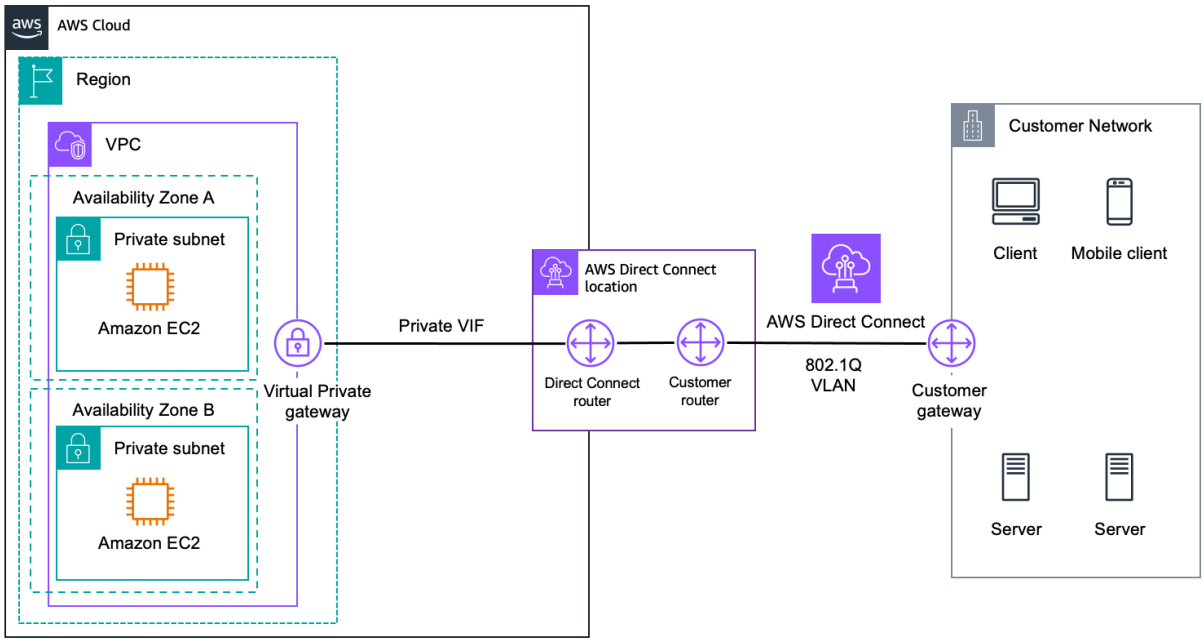
AWS VPC is a logically separated network isolated from other networks. It lets you set your own IP address range and configure security settings and routing for all your traffic. AWS VPC is made up of several networking components, as shown in the following figure; some of them are as follows:

- Subnets
- Elastic network interfaces
- Route tables
- Internet gateways
- Elastic IP addresses
- VPC endpoints
- NAT
- VPC peering

Direct Connect

AWS Direct Connect makes it easy to establish a dedicated connection from an on-premises network to one or more VPCs. AWS Direct Connect can reduce network costs, increase bandwidth throughput, and provide a more consistent network experience than internet-based connections. It uses industry-standard 802.1Q VLANs to connect to Amazon VPC using private IP addresses. The VLANs are configured using virtual interfaces (VIFs), and you can configure three different types of VIFs:

- **Public virtual interface** - Establish connectivity between AWS public endpoints and your data center, office, or colocation environment.
- **Transit virtual interface** - Establish private connectivity between AWS Transit Gateway and your data center, office, or colocation environment. This connectivity option is covered in the section AWS Direct Connect + AWS Transit Gateway.
- **Private virtual interface** - Establish private connectivity between Amazon VPC resources and your data center, office, or colocation environment.



Describe, create, and manage Amazon Virtual Private Cloud

Amazon Virtual Private Cloud (Amazon VPC), you can launch AWS resources in a logically isolated virtual network that you've defined. This virtual network closely resembles a traditional network that you'd operate in your own data center, with the benefits of using the scalable infrastructure of AWS.

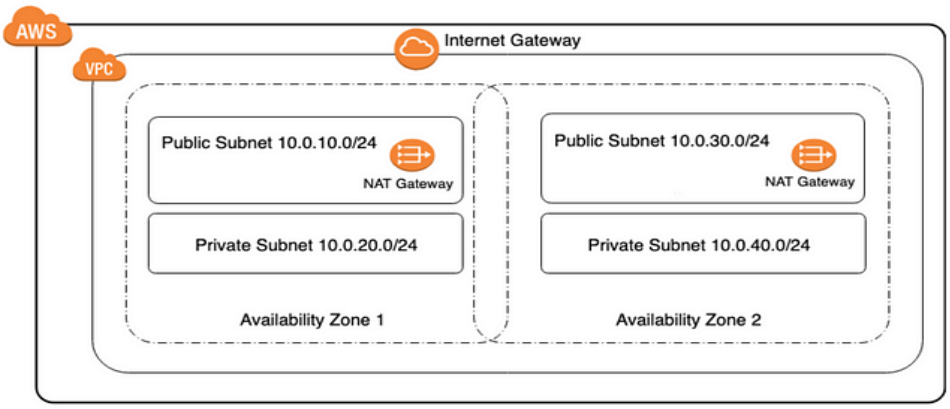
Get started with Amazon VPC

1. Sign up for an AWS account.
2. Verify permissions.
3. Determine your IP address ranges.
4. Select your Availability Zones.
5. Plan your internet connectivity.
6. Create your VPC.
7. Deploy your application

Amazon Virtual Private Cloud (Amazon VPC) enables you to launch Amazon Web Services resources into a virtual network you've defined. This virtual network resembles a traditional network that you'd operate in your own data center, with the benefits of using the scalable infrastructure of AWS.

Amazon VPC, Private Subnet, and Public Subnet

The purpose of this lab is to demonstrate how create a custom VPC with public subnet and an Internet gateway that will access our web server.



AWS Networking, Security Groups, and Network ACLs

Security groups and network ACLs are similar in that they allow you to control access to AWS resources within your VPC. But security groups allow you to control inbound and outbound traffic at the instance level, while network ACLs offer similar capabilities at the VPC subnet level. There is no additional charge for using security groups or network ACLs.

You can choose whether to specify security groups when you launch an instance or associate the instance with a security group at a later time. All internet traffic to a security group is implicitly denied unless you create an *allow* rule to permit the traffic.

For example, when you have Amazon EC2 instances behind an Elastic Load Balancer, the instances themselves should not need to be publicly accessible and should have private IPs only. Instead, you could provide the Elastic Load Balancer access to the required target listener ports using a Security Group rule that allows access to 0.0.0.0/0 (to avoid connection tracking issues – see note below) in conjunction with a Network Access Control List (NACL) on the target group subnet to allow only the Elastic Load Balancing IP ranges to communicate with the instances. This ensures that internet traffic can't directly communicate with your Amazon EC2 instances, which makes it more difficult for an attacker to learn about and impact your application.

When you create network ACLs, you can specify both allow and deny rules. This is useful if you want to explicitly deny certain types of traffic to your application. For example, you can define

IP addresses (as CIDR ranges), protocols, and destination ports that are denied access to the entire subnet. If your application is used only for TCP traffic, you can create a rule to deny all UDP traffic, or vice versa. This option is useful when responding to DDoS attacks because it lets you create your own rules to mitigate the attack when you know the source IPs or other signature.

Configuration and management of VPN connectivity

VPN configuration is the process of setting up a new VPN connection on a device or router. It involves choosing performance and security-related parameters to achieve an optimized private browsing experience with your current internet service provider

When it comes to the VPN support lifecycle, IT teams must understand VPNs, make technology decisions and know how to integrate a VPN platform into an enterprise network. But that's only the beginning.

Many technology managers are under extreme pressure to get VPNs up and running as quickly and cost-effectively as possible. Once the VPN is installed and running, however, it is generally too late to understand what VPN maintenance and management require on an ongoing basis. This overview examines key areas organizations must address for ongoing VPN maintenance and management, which is true for both remote access and site-to-site VPN connectivity.

IT teams must continuously maintain four critical aspects of VPNs in order for the service to scale and adapt to ever-increasing security requirements of enterprise network traffic.

Subnet and Subnet Mask

Subnet Mask is used in networking to create multiple sub networks in a network. It divides the IP address into multiple parts which can be assigned to every computer. Subnet Mask is made by setting the network bits to all "1"s and setting host bits to all "0"s. Within a given network, two host addresses are reserved for a special purpose, and cannot be assigned to hosts.

The binary "0" in the subnet mask tell us about the host address. It tells us about the IP of the host which has done subnetting.

Example

Suppose we have a subnet address as 192.168.1.0. In this, all host addresses are zero. It will be represented in binary as

11000000 10101000 00000001 00000000

Subnet (sub network)

Every website needs a unique IP address, in order to uniquely identify the website, we are dividing the IP network into two or more networks called subnet, which is preferred to control network traffic.

It is a smaller network inside a large network. This technique makes the network routing an efficient one.