VPC- Virtual Private Cloud

* Amazon Virtual Private Cloud (Amazon VPC) - A *virtual private cloud* (VPC) is a virtual network dedicated to your AWS account. It is logically isolated from other virtual networks in the AWS Cloud. It lets you launch AWS resources such as EC2 in your virtual network. 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.AWS VPC is the networking layer of EC2.
* Amazon VPC supports the processing, storage, and transmission of credit card data by a merchant or service provider, and has been validated as being compliant with Payment Card Industry (PCI) Data Security Standard (DSS). For more information about PCI DSS, including how to request a copy of the AWS PCI Compliance Package, see [PCI DSS Level 1](https://aws.amazon.com/compliance/pci-dss-level-1-faqs/).
* Amazon VPC integrates with many other AWS services; furthermore, some services require a VPC in your account to carry out certain functions. Below are examples of services that use Amazon VPC.

|  |  |
| --- | --- |
| **Service** | **Relevant Topic** |
| Amazon EC2 | [Amazon EC2 and Amazon VPC](http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-vpc.html) |
| Auto Scaling | [Auto Scaling and Amazon VPC](http://docs.aws.amazon.com/autoscaling/latest/userguide/autoscalingsubnets.html) |
| Elastic Load Balancing | [Setting Up Elastic Load Balancing](http://docs.aws.amazon.com/elasticloadbalancing/latest/userguide/setting-up-elb.html) |
| Amazon RDS | [Amazon RDS and Amazon VPC](http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.RDSVPC.html) |
| Route 53 | [Working with Private Hosted Zones](http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/hosted-zones-private.html) |

* Concepts of VPC:
* Subnets
* IP addressing
* Security Groups and NACLs
* VPC Flow Logs
* Route Tables
* Internet Gateways & Egress Only Gateways
* NAT- gateways and instances
* DHCP options
* DNS
* VPC peering
* VPC endpoints (AWS PrivateLink)
* VPN connections

**Subnets**

* VPC and Subnets – Subnet is a range of IP addresses in your VPC. You can launch AWS resources into a specified subnet and a subnet must completely reside in one AZ. Each subnet must be associated with one and only one (at a time) route table. Multiple subnets can be associated with a route table. If you do not associate your subnet with any route table, the subnet is implicitly associated with the main route table (which cannot be deleted but can be modified).
* Public Subnet - If a subnet's traffic is routed to an internet gateway, the subnet is known as a public subnetIf you want your instance in a public subnet to communicate with the internet over IPv4, it must have a public IPv4 address or an Elastic IP address (IPv4)
* Private Subnet - If a subnet doesn't have a route to the internet gateway, but has its traffic routed to a virtual private gateway for a VPN connection, the subnet is known as a VPN-only subnet.
* Note: Regardless of the type of subnet, the internal IPv4 address range of the subnet is always private—we do not announce the address block to the internet.
* Understanding the Subnet Creation –
* To create only a single subnet in the VPC we can specify the CIDR block of VPC exactly same as CIDR block of the VPC
* Other wise to create multiple subnets specify non overlapping subnet CIDR blocks. The allowed block size is between /28 netmask and /16 netmask.
* First four and last IP is a subnet is reserved. For eg: in a subnet of CIDR block 10.0.0.0/24

1. 10.0.0.0 : Network address
2. 10.0.0.1 : Reserved by AWS for the VPC router
3. 10.0.0.2: The second address of the VPC (primary CIDR block’s 2nd IP) is reserved for Amazon DNS server. In each subnet the 2nd Ip is reserved for local DNS
4. 10.0.0.3 – reserved by AWS for future use
5. 10.0.0.255 – Network broadcast address. Broadcast in a VPC is not supported so this address is reserved.

* Secondary CIDR blocks can also be associated to a VPC. **See : IPv4 CIDR Block Association Restrictions**
* While creating a VPC you can also specify a CIDR block (allowed size - a/16 or smaller like a/12 or a/8) **for PRIVATE IPS.** This private IP block may be inside or outside the public IP block.
* When you add or remove a CIDR block, it can go through various states: associating | associated |disassociating | disassociated | failing | failed. The CIDR block is ready for you to use when it's in the associated stat
* Subnet Routing –
* Each Subnet must be associated with a route table, which specifies the allowed routes for outbound.
* Every subnet on creation is associated with the main route table for the VPC. If the primary CIDR block chosen for the VPC was 10.0.0.0/16 , the main table by default has one entry and looks like this:

|  |  |
| --- | --- |
| Destination | Target |
| 10.0.0.0/16 | local |

* You can allow an instance in your VPC to initiate outbound connections to the internet over IPv4 but prevent unsolicited inbound connections from the internet using a network address translation (NAT) gateway or instance.
* To make a number of instances available to the internet at static IP ,it is recommended not to use individual Elastic IPs for each (since no of Elastic IPs you can use are limited). Instead use a NAT and attach elastic IP to it, keep the instances at private IPs.
* Elastic IPs and public IPs are accessed through IGs. In a VPN connection a virtual private gateway is used which uses private IPs
* Subnet Security is provided by two features: Security Groups and Access Control Lists-Security groups control inbound and outbound traffic for your instances, and network ACLs control inbound and outbound traffic for your subnets.
* Connections with other LANs and VPCs – you can connect with hosts in other VPCs or LANs using an IPsec AWS managed VPN connection, making the AWS Cloud an extension of your data center, as long as their IP is outside the CIDR block(s) of your VPC(not just outside your subnet).
* However to connect to other VPCs we can also set up a VPC peering connection provided that the CIDR blocks of the networks should be different. For now VPC peering connection enables you to route traffic using private IPs.
* What can you do in a VPC (related to subnets): GUIDE - <https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/working-with-vpcs.html>
* Create a VPC
* Creating a subnet in your VPC
* Associating a secondary CIDR block with your VPC
* Launching instances in your subnet
* Disassociating CIDR block from VPC
* Deleting your subnet
* Deleting your VPC
* NAT - NAT device enables instances in a private subnet to connect to the Internet (for example, for software updates) or other AWS services, but prevent the Internet from initiating connections with the instances

IP Addressing

* Private IP
* Public IP
* Elastic IP
* Elastic Network Interface – a logical NIC

An ENI can have following components:

* Primary private IP
* One or more secondary IP
* Elastic IP/Public IP
* Security Groups
* MAC address
* Source/Destination Check Flag
* Description

<https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-ip-addressing.html>

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