



Amazon - VPC

What is VPC?

“Amazon Virtual Private Cloud (VPC) allows the users to use AWS resources in a virtual network. The users can customize their virtual networking environment as they like, such as selecting own IP address range, creating subnets, and configuring route tables and network gateways.”





Amazon - VPC

≡ Benefits:

EASY TO USE

Ease of creating a VPC in very simple steps by selecting network setups as per requirement. define Subnets, IP ranges, route tables, and security groups will be automatically created.

PRICING FOR AMAZON VPC

There's no additional charge for using Amazon VPC. Pay the standard rates for the instances and other Amazon EC2 features that you use.





Amazon - VPC

≡ Features:

- Create an Amazon VPC on AWS scalable infrastructure and specify its private IP address range from any range you choose.
- Expand VPC by adding secondary IP ranges.
- Divide VPC private IP address range into one or more public or private subnets to facilitate running applications and services in VPC.
- Control inbound and outbound access to and from individual subnets using network access control lists.





Amazon - VPC

☰ Features:

- Store data in Amazon S3 and set permissions such that the data can only be accessed from within Amazon VPC.
- Attach one or more Amazon Elastic IP addresses to any instance in VPC so it can be reached directly from the Internet.
- Connect VPC with other VPCs and access resources in the other VPCs via private IP addresses using VPC Peering.





Amazon - VPC

☰ Features:

- Privately connect to other AWS services without using an internet gateway, NAT or firewall proxy through a VPC Endpoint.
- Bridge VPC and onsite IT infrastructure with an encrypted VPN connection.
- VPC Flow Logs to log information about network traffic going in and out of network interfaces in VPC.





Amazon - VPC

≡ Key Concepts VPCs and Subnets:

- A subnet is a range of IP addresses in VPC.
- Use a public subnet for resources that must be connected to the internet, and a private subnet for resources that won't be connected to the internet.
- While creating a VPC, must specify a range of IPv4 addresses for the VPC in the form of a Classless Inter-Domain Routing (CIDR) block.





Amazon - VPC

Destination

10.0.0.0/16

Target

Local

The following diagram shows a new VPC with an IPv4 CIDR block, and the main route table.



Web Services





Amazon - VPC

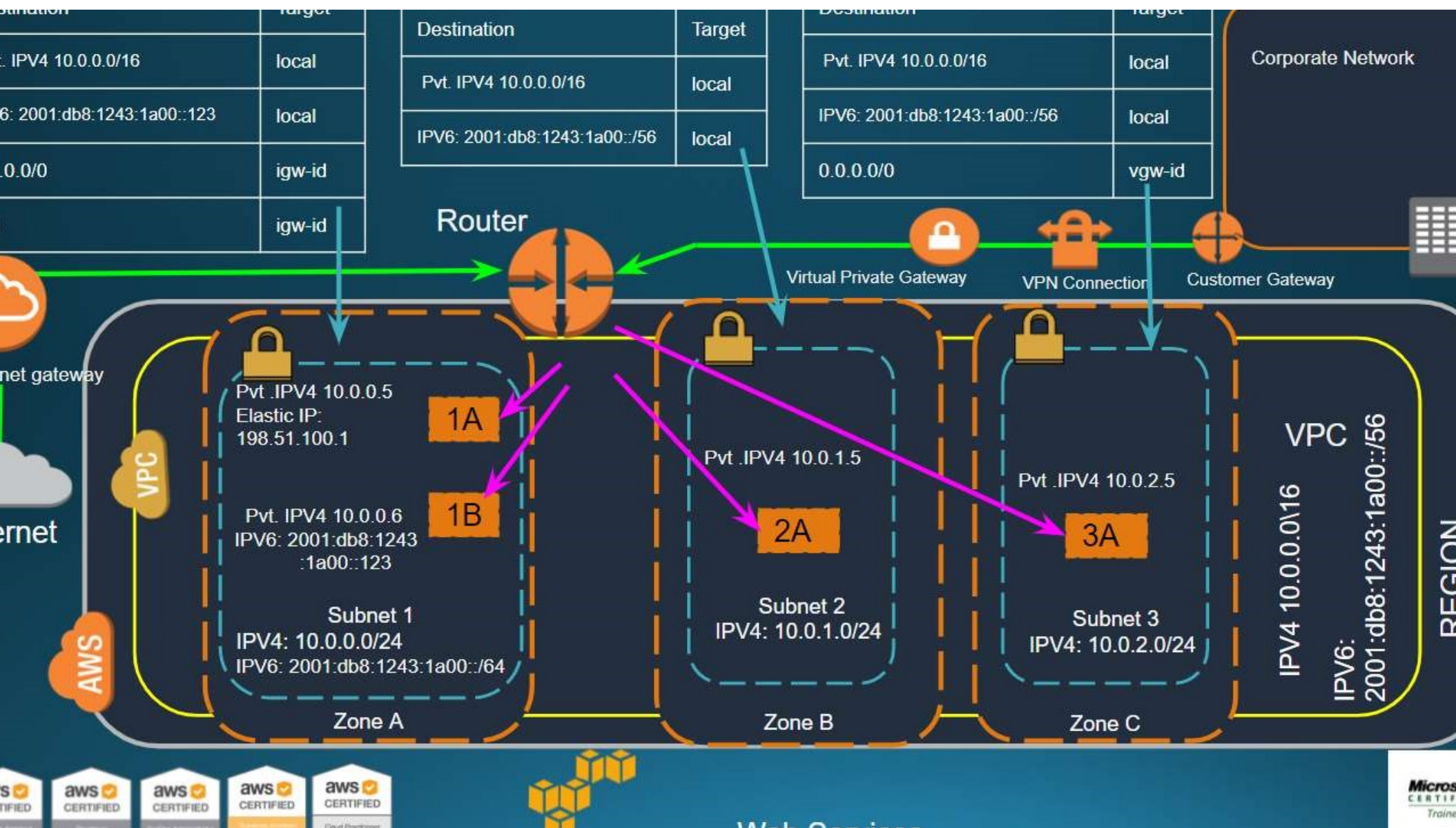


Key Concepts | VPCs and Subnets:

- After creating a VPC, user can add one or more subnets in each Availability Zone.
- Create a subnet, 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 cannot span zones.
- Availability Zones are distinct locations that are engineered to be isolated from failures in other Availability Zones.



W16-01





Amazon - VPC

≡ Key Concepts | VPCs and Subnets:

The above mentioned diagram shows a VPC that has been configured with subnets in multiple Availability Zones. 1A, 1B, 2A, and 3A are instances in the VPC.

- An IPv6 CIDR block is associated with the VPC, and an IPv6 CIDR block is associated with subnet 1.
- An internet gateway enables communication over the internet, and a virtual private network (VPN) connection enables communication with your corporate network.
- If, a subnet's traffic is routed to an internet gateway, the subnet is known as a public subnet. In this diagram, subnet 1 is a public subnet.



W16-01



Amazon - VPC

≡ Key Concepts | VPCs and Subnets:

- If 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).
- If instance in the public subnet to communicate with the internet over IPv6, it must have an IPv6 address.
- If a subnet doesn't have a route to the internet gateway, the subnet is known as a private subnet. In this diagram, subnet 2 is a private subnet.





Amazon - VPC

VPC Endpoints

- A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by AWS Private Link without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection.
- Instances in your VPC do not require public IP addresses to communicate with resources in the service.
- Traffic between your VPC and the other service does not leave the Amazon network.





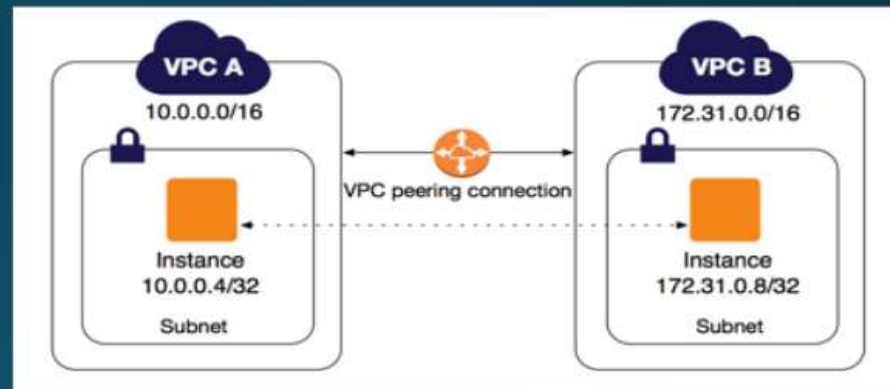
Amazon - VPC

Press **Esc** to exit full screen

VPC Peering

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account. The VPCs can be in different regions (also known as an inter-region VPC peering connection).

<https://docs.aws.amazon.com/vpc/latest/peering/invalid-peering-configurations.html#edge-to-edge-vgw>



Invalid Configurations

- Overlapping CIDR blocks
- Transitive peering
- Edge to edge routing through a gateway or private connection





Amazon - VPC



Amazon VPC | Integrated with Other AWS Services:

- AWS Data Pipeline
- Amazon EC2
- Auto Scaling
- Elastic Beanstalk
- Elastic Load Balancing
- Amazon WorkSpaces
- Amazon ElastiCache
- Amazon EMR
- AWS OpsWorks
- Amazon RDS
- Amazon Redshift
- Route 53





Amazon - VPC

Hands-On Lab

- Create a VPC with Public & Private Subnet using VPC Wizard
- Create a VPC by using individual VPC components & Verify
- Create a VPC Peering and Endpoint



Web Services