VPC

1. VPC – Virtual Private Cloud (Your Private Cloud)
2. We have Regions, Availability Zones,
   1. We can think of AZ as data centers.
   2. Region can have multiple data centers.
   3. We can launch EC2 instances, RDS instances in these availability zones.
   4. To protect against failures, fault tolerances, we can create multiple instances in different availability zones, so if 1 AZ goes does we can provide services from other AZ.
   5. Different AZ
3. Each AWS account you create, comes with default VPC.
4. VPC is ur data center in the cloud.
5. Ip subset range can be divide among multiple AZ using subnet.

Subnet

1. Internal IP Range inside VPC
2. Public IP can help us to communicate to internal ip range.

Public vs Private Subnet

1. Public subnet can host webservers that can be accessible by outside network
2. Database and internal apps can be available in private subnet.

Internet Gateway

1. To communicate with outside world from inside VPC we can use Internet Gateway

Security Group

1. You can assign instances in VPC with security groups.
2. Security Groups can be shared across AZ.
3. Security Groups allows to control
   1. Which access is allowed to instances
   2. Which traffic can leave instances
   3. Acts as Firewall
   4. More granular as applied to instances

Network Access Control List (NACL)

1. Applies at subnet level
2. Which traffic can access subnet

NAT Gateway

1. Ability to route private subnet traffic to access outside world (for updates etc)
2. Nat Gateway has public ip
3. Instances in private subnet don’t have public ip but they can access outside world using NAT gateway
4. NAT is private to public routing.

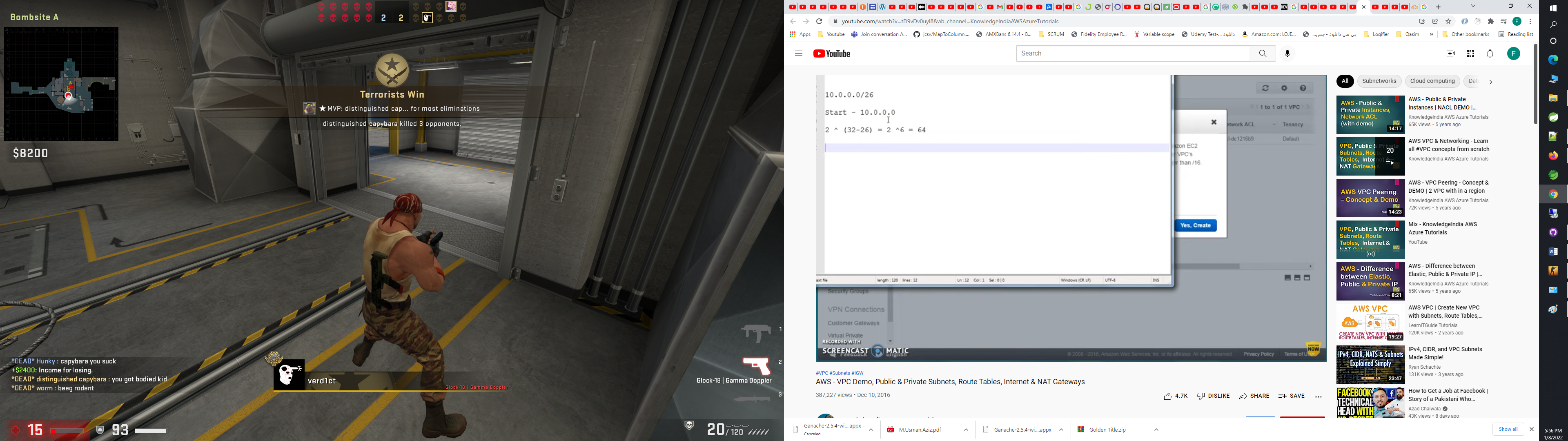
How many valid Ips

1. Subnet mask = 26
2. 2 ^ (32-26) = 2 ^ 8 => 64 Valid ips in CIDR
3. We will divide in 4 subnets of 16
4. Deploy VPC
5. Create subnets

Luanch VPC and aws work

<https://www.youtube.com/watch?v=tD9vDv0uyI8&ab_channel=KnowledgeIndiaAWSAzureTutorials>

Range



Route Table

1. How network is routed when it leaves VPC
2. Is traffic allowed to leave/enter VPC
3. Controls routing of out-going network requests

Public IP

1. If the instance launch in the subnet will receive Public IP
2. So we can create two subnets, one can be accessible by public ip and other for internal use only.

VPC span multiple AZ

Subnet is tied to a specific AZ.

CIDR Block

1. Ip Ranges

Why do we want to isolate our network under a region?

For

1. Compliance Perspective
2. PROD/UAT/QA/DEV
3. Maybe to connect cloud network with on premise data center.

Resources

<https://www.youtube.com/watch?v=bGDMeD6kOz0&ab_channel=Academind>

Create VPC with subnets

<https://www.youtube.com/watch?v=tD9vDv0uyI8&ab_channel=KnowledgeIndiaAWSAzureTutorials>

FAQ:

1. **What is VPC**

Amazon VPC provision a logically isolated section of the Amazon Web Services (AWS) cloud where you can launch AWS resources in a virtual network that you define

1. IP Address range
2. Creation of subnets
3. Route Table configuration
4. Network Gateway
5. Enable us to VPN , on-premise data center with AWS VPC.
6. Layers of security
   1. Security Groups
   2. Network Access control lists.
   3. etc
7. **Components of VPC**
8. Virtual Private Cloud
9. Subnet
10. Internet Gateway: Amazon VPC side of connect to public internet
11. NAT Gateway: A highly available, managed Network Address Translation (NAT) service for your resources in private subnet to access the internet.
12. Virtual Private Gateway: The Amazon VPC side of a VPN connection
13. Peering connection: A peering connection enables you to route traffic via private IP addresses between two peered VPCs.
14. VPC Endpoints: Enables private connectivity to services hosted in AWS, from within your VPC without using an Internet Gateway, VPN, Network Address Translation (NAT) devices, or firewall proxies.
15. Egress-only Internet Gateway: A stateful gateway to provide egress only access for IPv6 traffic from the VPC to the Internet.
16. **VPC network architecture**

VPC comes with four basic options for network architectures.

* 1. Amazon VPC with a single public subnet only
  2. Amazon VPC with public and private subnets
  3. Amazon VPC with public and private subnets and AWS Site-to-Site VPN access
  4. Amazon VPC with a private subnet only and AWS Site-to-Site VPN access

1. **What are the different types of VPC endpoints available on Amazon VPC?**
2. Gateway type endpoints
3. Interface type endpoints
4. **VPC endpoints**
   1. enable you to privately connect your VPC to services hosted on AWS without requiring an Internet gateway, a NAT device, VPN, or firewall proxies.
   2. Endpoints are horizontally scalable
   3. highly available virtual devices that allow communication between instances in your VPC and AWS services.
5. **Gateway type endpoints** are available only for AWS services including S3 and DynamoDB. These endpoints will add an entry to your route table you selected and route the traffic to the supported services through Amazon’s private network.
6. **Interface type endpoints** provide private connectivity to services powered by PrivateLink, being AWS services, your own services or SaaS solutions, and supports connectivity over Direct Connect.

Billing

1. There are no additional charges for creating and using the VPC itself.
2. Data transfer charges are not incurred when accessing Amazon Web Services, such as Amazon S3, via your VPC’s Internet gateway.
3. If you access AWS resources via your VPN connection, you will incur Internet data transfer charges.
4. If you connect your VPC to your corporate datacenter using the optional hardware VPN connection, pricing is per VPN connection-hour (the amount of time you have a VPN connection in the "available" state.)
5. Partial hours are billed as full hours.
6. Data transferred over VPN connections will be charged at standard AWS Data Transfer rates.

Connectivity

1. What are the connectivity options for my Amazon VPC?

You may connect your Amazon VPC to:

* The internet (via an internet gateway)
* Your corporate data center using an AWS Site-to-Site VPN connection (via the virtual private gateway)
* Both the internet and your corporate data center (utilizing both an internet gateway and a virtual private gateway)
* Other AWS services (via internet gateway, NAT, virtual private gateway, or VPC endpoints)
* Other Amazon VPCs (via VPC peering connections)

**How do I connect my VPC to the Internet?**

Amazon VPC supports the creation of an Internet gateway. This gateway enables Amazon EC2 instances in the VPC to directly access the Internet. You can also use an Egress-only internet gateway which is a stateful gateway to provide egress only access for IPv6 traffic from the VPC to the Internet.

**How do instances in a VPC access the Internet?**

You can use public IP addresses, including Elastic IP addresses (EIPs) and IPv6 Global Unique addresses (GUA)

**Are there any bandwidth limitations for Internet gateways? Do I need to be concerned about its availability? Can it be a single point of failure?**

No. An Internet gateway is horizontally-scaled, redundant, and highly available. It imposes no bandwidth constraints.

**When is an IP address considered a Public IP address?**

Any IP address that is assigned to an instance or a service hosted in a VPC that can be accessed over the internet is considered a public IP address. Only public IPv4 addresses, including Elastic IP addresses (EIPs) and IPv6 GUA can be routable on the internet. To do so, you would need to first connect the VPC to the internet and then update the route table to make them reachable to/from the internet.

1. VPC Notes:
2. AWS resources are automatically provisioned in a ready-to-use default VPC.

Notes;

1. Whenever we create subnet in AWS, 5 are reserved.
2. For each VPC, one route table is created by default. That route table is marked as Main and will be used as default route table for all subnets. Unless changed
3. 1-1 relationship b/w subnet and route table.
4. 1 route table can be associated with multiple subnets.
5. 1 -1 relationship b/w Internet Gateway and VPC.
6. Custom route tables are not set with any subnet, unless u assigned them.
7. NAT Gateway allows internal traffics to get response from outside (Public) networks.
   1. Those instances who don’t have Public IP , can use NAT gateway to communicate with external world.
   2. Act as forward proxy
   3. NAT Gateway use 1 IP from Available public ip range