AWS VPC (Virtual Private cloud)

VPC intro

- VPC is network layer
- Create own network, assign ip address range, set route tables, nw gateways etc.
- To create VPC
  - specify address range
  - CIDR max /16 to min /28
  - no overlap if you are connecting another VPC
- Contains
  1. Subnet
  2. Route tables
  3. Security group
  4. ACLs
  5. DHCP option set
  6. IGW
  7. Elastic ip
  8. ENIs
  9. Nat gateway/ instance
  10. Endpoints
  11. Peering
  12. VGW

Subnet

- Segment/Subset of VPC's IP address range
- CIDR block is used to select particular Subset
- Minimum /28
- Five IP are reserved within subnet
  - First - network , Second - Router , Third - DNS server , Fourth -Reserved , Last- Broadcast

Types

- Public - route table have default route to IGW
- Private - route table don't have route to IGW
- VPN only - route table have default route to VGW

Route tables

- Determines Where network traffic of a subnet is directed
- Tool to create public , private or VPN only subnet
- Default root
  - direct traffic within VPC
  - cant delete or remove

Important points to remember for exam

- Every VPC has implicit (default) Router
- Every VPC has default route tavpble (main table)
- YOu can create custom route table
- You can associate custom route table to subnet. When you dont do it , it refers to main
- route table has CIDR block and target. AWS uses most specific route.
  - 10.2.1.122 --> VGW
  - 0.0.0.0 --> IGW
  - When traffic is sent to 10.2.1.122 ; specific rule is used (VGW) and not 0.0.0.0

Internet gateways

- AWS managed (redundant , highly available, scalable)
- Enables traffic between instance & Internet
- performs network address translation for EC2 which has public ip
  - ec2 intance is only aware about private ip
  - IGW translates private ip to its public ip.
  - Keeps mapping between private <--> pulic ip
- EC2 Incoming traffic Enable
  - attach IGW to VPC
  - update subnet route table (0.0.0.0/0 to IGW)
  - set network ACL and securiy group to allow certain traffic
- EC2 Outgoing traffic enable
  - assign public or elastic ip to your instance

DHCP option set (pending)

Elastic IP addresses

- AWS has pool of IP address (in a region)
- Elastic IP is static public IP address that can be assigend to EC2/ gateway etc
- Elastic - IP remains same while you can change underlying infrastructure
- Maximum 5 IP. Better have it assigned to NAT gateway.

Important points to remember for exam

- Allocate EIP before assign
- Cant assign to different region
- One-to-one relationship between EIP <--> Network interface
  - So EC2 can have multiple interfaces, so it can multiple EIP's ??
  - No - because ENIs can have only one public IP address
- can assign within VPC or different VPC of same region
- keeps tagged to your account even if instance stopped/ terminated
- gets chanrged unless explicitly released

Elastic network interface

- Attach or detach ENI to instance
- At create, must associate with subnet (and hence security group is associated with ENIs)
- One ENI --> 1 public IP, multiple private IP
- ENI persists even after instance is stopped or terminated

uses

- Dual home instace (web server , db traffic)
- Management network (web server, ssh access)
- Network and security appliance (web server, firewall or load balencer)
- Low budget high availability (hot attach to ENI other instance)

Endpoints

- Create connection between AWS VPC and AWS services which are on internet (S3, DynamoDB)
    - No need to configure IGW, Direct connect etc.
- Multiple endpoints to same service
    - configure different route in this way to have different access policies

VPC Peering

- Allow instances in two different VPCs to communicate
- It does not introduce any single point of failure (like NAT instance)

Important points to remember

- 2 VPCs must be in same region
- Cant have overlapping CIDRs
- Cant allow trasitive Peering
- Only One peering connection allowed between two VPCs

Security group

- Virtual firewall. Assciated with ENI's.

Points to remember

- 500 security groups in VPCs
- 50 inbound and 50 outbound rules in one security group. Attach multiple SGs if 101 rules are required.
- You can only add allow rules. No deny rules. Use ACLs for deny.
- By default allow all outbound traffic. YOu can restrict it
- By default disallow all inbound traffic. You have to use accept rules.
- Stateful - responses of outbound traffic are allowed if inbound rule is allowed.
- Can change security group on the fly. Changes are effective immediately.

ACL

- Additional level of defense at subnet level

- Numbered rules , processed from low to high by AWS
- Default ACL - allow all traffic , Custom ACL - initially denies all traffic

Difference

	SG	**ACL**
1	ENI level	Subnet level
2	Allow only	Allow + deny
3	All rules evaluted for specific rule	Evalution is numbered
4	Stateful	Stateless

NAT instance

VPN gateway