**AWS CSA-Pro Linux Academy Notes Networking in AWS (VPCs):**

**VPC Essentials: Part 1:**

**VPC Basics:**

* VPCs provide isolated network domains
* Private networking (VPCs) you need to configure communications
* AWS Public Zone is sandwiched in between the VPC and the public internet
* VPCs are regional services
* By default there are no communication between VPCs
* Certain AWS services depend on the default VPC and required it
* If deleted you can create a new default VPC by creating a new VPC and selecting the default VPC option
* VPC can be set to 2 tenancy modes. Default and Dedicated
  + Dedicated limits you
  + Default allows you to change tenancy at a resource level. Usually choose default
* DHCP options sets are created when you make a VPC. Cannot edit them directly so to change them you need to create a new set and associate it with the VPC
* Subnets architecture
  + VPC needs subnets and they occupy a single AZ (1 subnet per 1 AZ) Multiple subnets can share the same AZ
  + Times the number of AZ by the number of tiers you want to deploy

**Reserved IP Addresses:**

* Within every VPC subnet a number of IP addresses are reserved
* The first 4 (Assume 10.0.0.0/24 is subnet)
  + 10.0.0.0 Network Address
  + 10.0.0.1 VPC Router
  + 10.0.0.2 DNS
  + 10.0.0.3 Reserved for future use
  + 10.0.0.255 Broadcast not supported

**Connecting VPCs:**

* VPC Peers- Connect individual VPCs to other VPCs
  + Same account, Same region
  + Same Region, different account
  + Same account, different region
  + Both different
* Internet Gateways- Provide internet connectivity
* VPN Gateways- Provide access to on-prem networks
* Bastion Hosts- Used to access VPC resources from the internet
* VPC Endpoint- Use to access AWS Public Zone resources privately from your VPC
* Egress Only Gateway- Ipv6 gateway

**Tips:**

* Aim for no overlap between CIDR ranges in your VPCs. This will makes sure you can set up VPC peering connections
* Advance planning with tiers and adding buffer zone
* AZ planning and AZ buffering

**AWS Resource Access Manager (RAM):**

* Allows the sharing of VPC resource between accounts
* The ability to create a subnet in one AWS accounts and then share it into other AWS accounts within your organization
* By default you will need a handshaking architecture. You can check a box to not need to require this handshake
* Org needs all features enabled for this to take place. Ticking this box removes a lot of the admin overhead

**AZ ID-** the AZ ID is the actual geographical location your AZ is mapped at. Upon account creation AZs are randomly assigned an AZ Name for your account. AZ IDs are consistent between accounts

**Owner-** The owner of an AWS resource

**Participant-** If an owner shares a resource to you then you become a participant in Resource Access Manager. Do not have permissions on any of the resources created by the owner or any permissions on the resource created by other participants

**Create Resource Share-** This is a share that provides specific resources to specific AWS accounts, Organizations, or Organizational Units.

When sharing subnets you are limited to sharing only to other accounts within your org. Some services do not allow sharing right now like Network Load Balancer, EMR, and Glue

You can’t use Security groups directly that are owned by the owner of the resource or other participants, but you can reference them in your Security Groups. You cannot launch a resource with the default security group as you do not own that.

You can unshare a resource share even when participant resources are running in subnets. Participants will no longer be able to create new resources, but they can still modify and delete existing resources they already created. You cannot delete subnets with resources from these participants.

**VPC Routing:**

**VPC Router:**

* Every VPC comes with a VPC Router
* It is the CORE network entity responsible for touring traffic between a VPC and other networks
* The VPC router places an interface in the Network+1 address of every subnet
* Occupies the 10.0.0.1 ip address or the Network+1 address in every single subnet
* Configurable by route tables
  + Every VPC comes with a default Route Table
  + Contains subnets without a separate Route Table location
  + Every route table starts off with a single route (The local route)
  + You can add additional routes in your Route Tables
  + Priority of Routes are processed in the order of the CIDR range. The higher the CIDR number the higher chance it gets routed. Most specific route wins out
  + /32 which is a single IP 10.10.23.67/32 would be routed instead of 0.0.0.0/0
  + You can have static routes or Route Propagation
  + Route Propagation are routes that are learned via Virtual Private Gateways and auto added to Route Tables
* Route Tables are used for a lot of VPC Resources
  + IGW, Nat Gateways, Peering, Endpoints, so on (learning later)