AWS Services?

1.AWS Identity and Access Management (IAM)- System used to manage user and group access for different AWS resources and services

* User is a specific person
* Multifactor authentication can be assigned to a user to permission so when they try to login into resource they will need to login using a mobile device. You can mobile app such as Authy
* Secret Keys and Secrete access keys
* Group is a collection of users. Policies are assigned to groups so any user assigned to that group with have those permissions specified in the policy
* Roles is assigned certain permissions to an entity (user, aws service, aws accounts etc). Users can assume that role and use those permissions define in that role. For example third party user can be granted access to aws resource through a define role instead of creating new user and adding the user to group with assigned policy
* Policies defines certain permission for AWS resources. You can assign default policy to group/user that is already integrated into AWS or create a custom policy using JSON
* Create custom polices using JSON policy generator
  + - <https://awspolicygen.s3.amazonaws.com/policygen.html>
* **VPC (Virtual Private cloud)** is network layer were aws service instances can be ran within the VPC. VPC can manage be managed within AWS portal. IP address can be specified for the VPC and you can add subnets and gateways and security groups within the VPC.
* **Subnet** is range of Ips in VPC. AWS services run in subnet. A private subnet doesn’t accept traffic from the internet and can’t connect to internet. Private subnets don’t have a public IP. Public subnets connect to the internet
* **Security Group** controls the traffic that in enters and leave the instances running in subnet(operates at instance level). There is a default security group available when creating a VPC. Custom security groups can be created in VPC dashboard
* **Internet gateway** is used to allow resource instances to connect and receive internet traffic. To get traffic from internet you need to add route to subnet route table to route internet traffic to instance
* **NAT Gateway(Network Address Translation)-** used so instance in private subnet can access external services or internet but the external services cannot connect to internal services. NAT gateways are managed by aws.
* **NAT instance** can also be created to managed connects from internal private subnet instances to internet. This is an alternative to from NAT gateway and is managed by the user
* **Route tables** are set of rules used for routing the traffic within subnet. By default there is a main route table in AWS when creating VPC. You can also create your own custom route table in VPC dashboard
* **Softlimit** is limit number of vpc, subnets, security groups, etc. that can be created within a datacenter. But a hard limit cannot be changed
* **VPC peering** is a connection between 2 VPCs to each other. VPCs are connect through a private IP. Can connect to other VPCs in different AWS account and different region
* **Network ACLs**- Additional layer of security to control subnet traffic. Acts as firewall