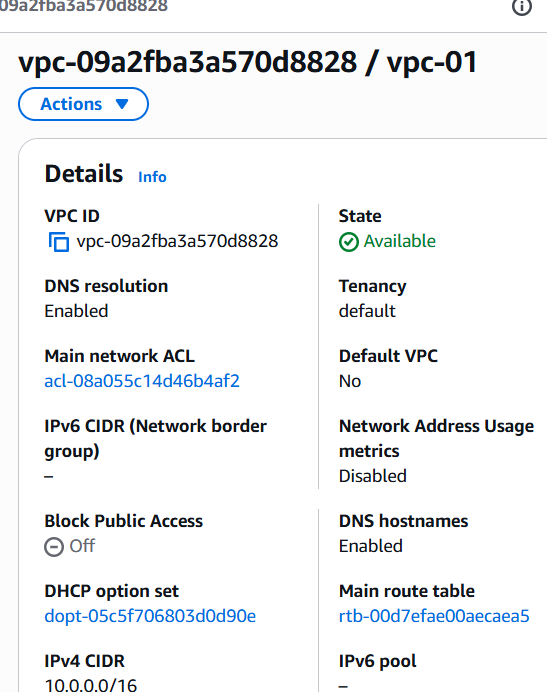
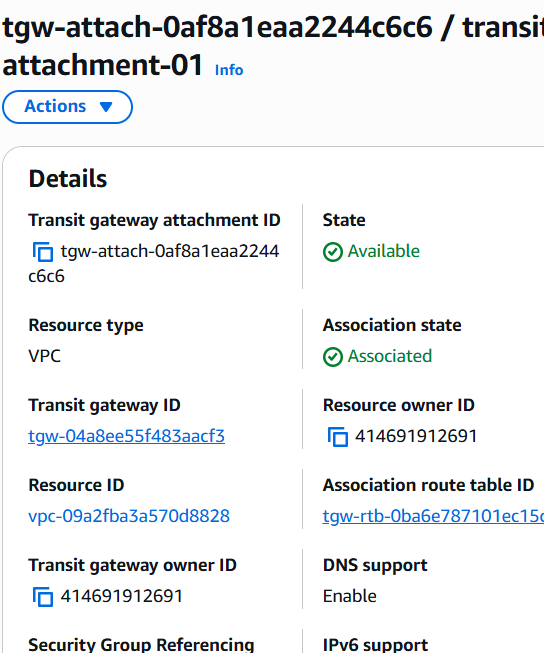
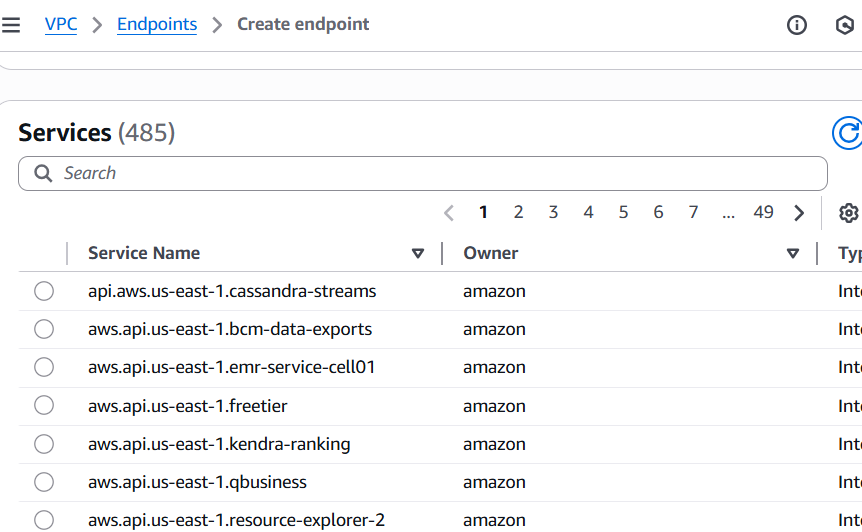
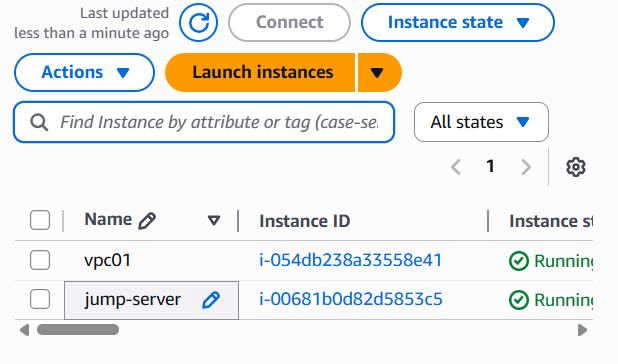
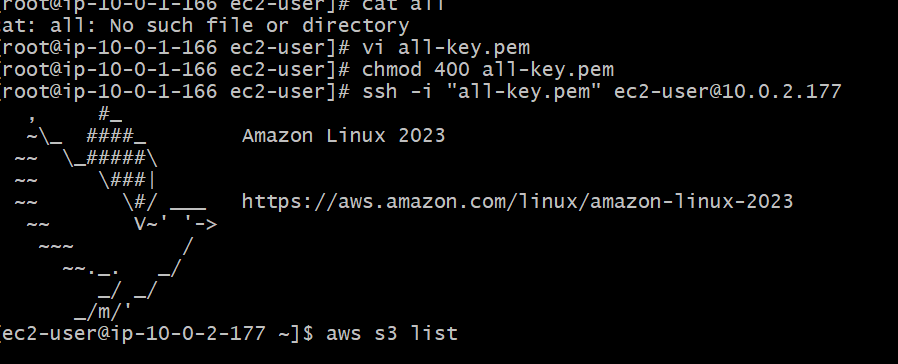
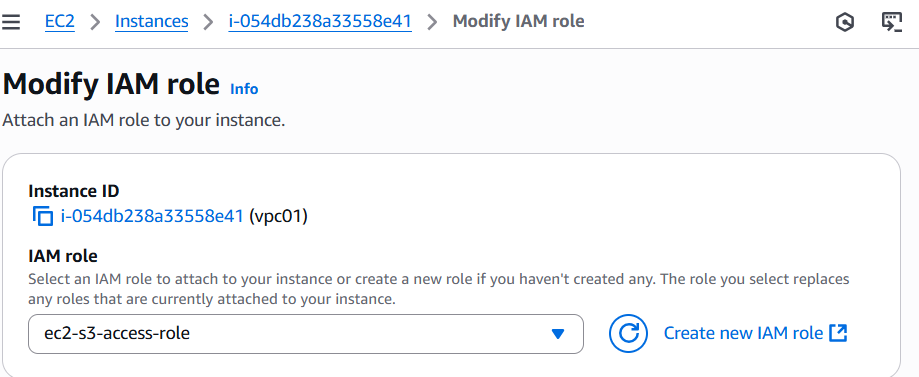
**VPC CHALLENGE**

Use Case: Setting up Transit Gateway and VPC Endpoints for a Multi-VPC Architecture  
**Scenario:**  
A large organization is migrating its on-premises infrastructure to the AWS cloud.  
The organization's architecture involves multiple VPCs for different departments and applications, each requiring secure communication with centralized services and external resources.  
The IT team needs to design and implement a scalable and efficient network architecture to accommodate the organization's growth and ensure robust connectivity between VPCs and external services.  
**Objectives:**

* Design and deploy a scalable network architecture using AWS Transit Gateway to simplify network connectivity between multiple VPCs.
* Configure VPC endpoints to securely access AWS services without internet gateways or NAT gateways, ensuring data privacy and minimizing exposure to external threats
* Create a vpc ,
* Create 2 subnets 1 one for public and 1 for private
* 
* Create transit gateway
* Create trasit gateway attachment and attach it to created vpc
* 
* Update the route tables and associations
* Created internet gateway for public instance and give route
* Transit gateway for private subnet
* Launch an ec2 instance with public subnet
* And one more ec2 instace for private subnet
* Create endpoints and add required services
* 
* 
* Login into public instance with pem key and try to loginto private instance give inbound rules and 22 in security groups
* Now , change to root user in terminal and create a same pem key file and give permissions for chmod 400
* Add pem.key to private instance pem key
* 
* And start using
* Aws configure give iam user -acces key and secret key
* Or create iam role , by selecting instance and click actions and go to setting and create role give permission and attach this permission to iam role
* 
* To verify enter command aws s3 ls
* 