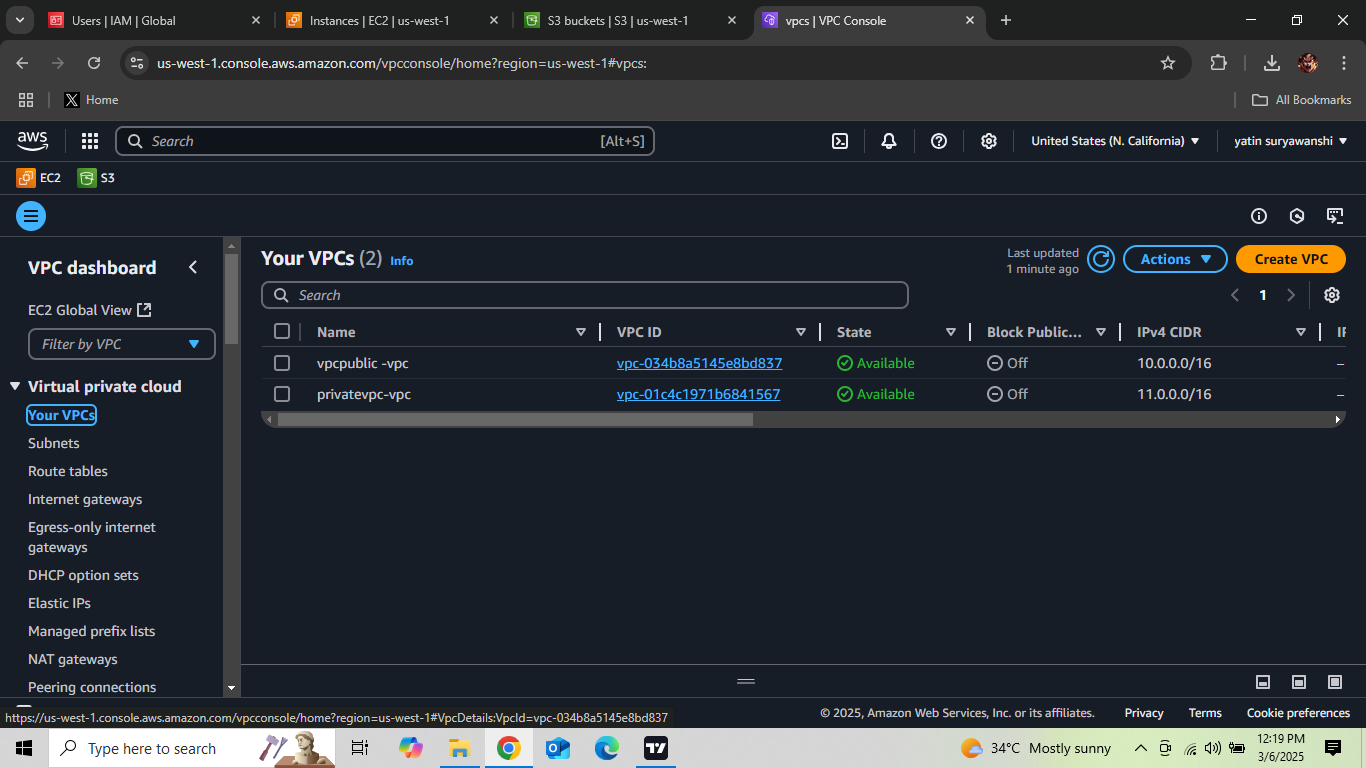
**Project Documentation: Accessing S3 from a Private VPC via Public VPC**

**Project Overview**

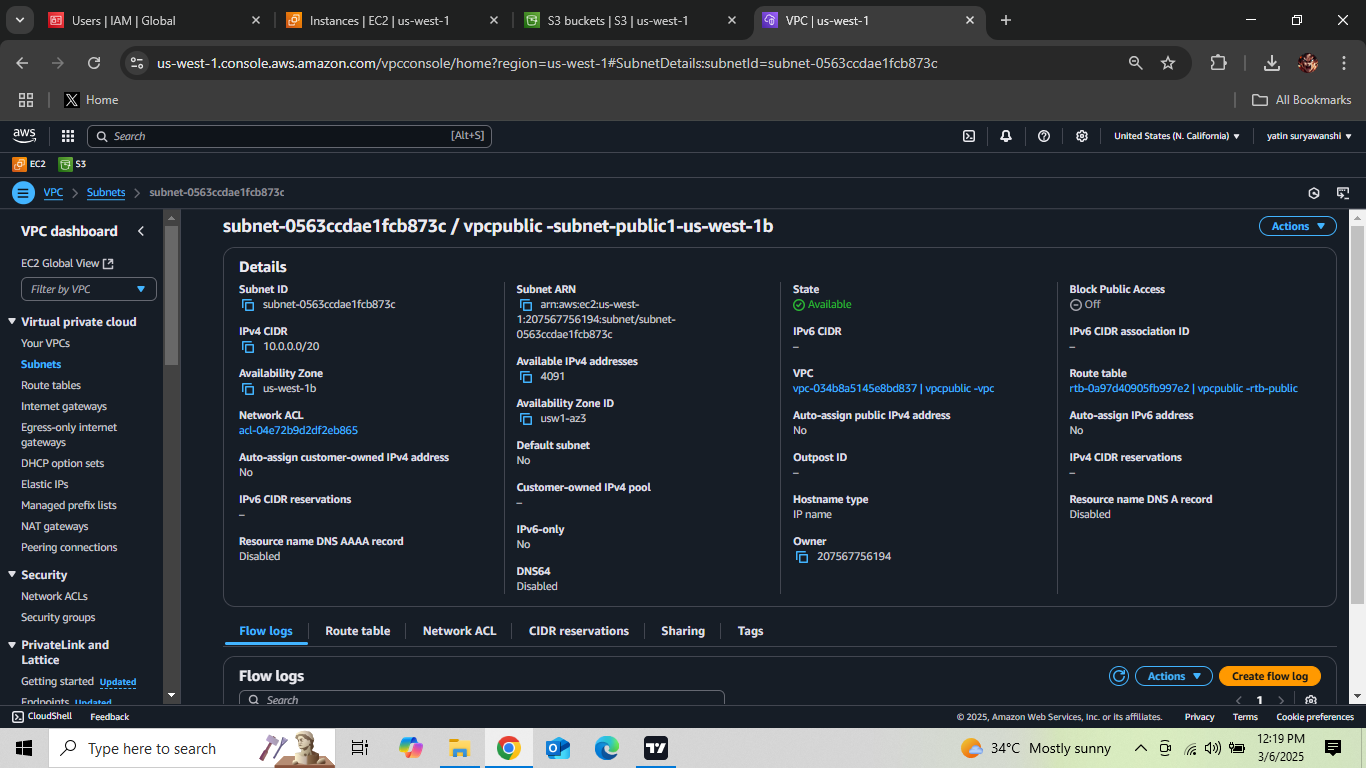
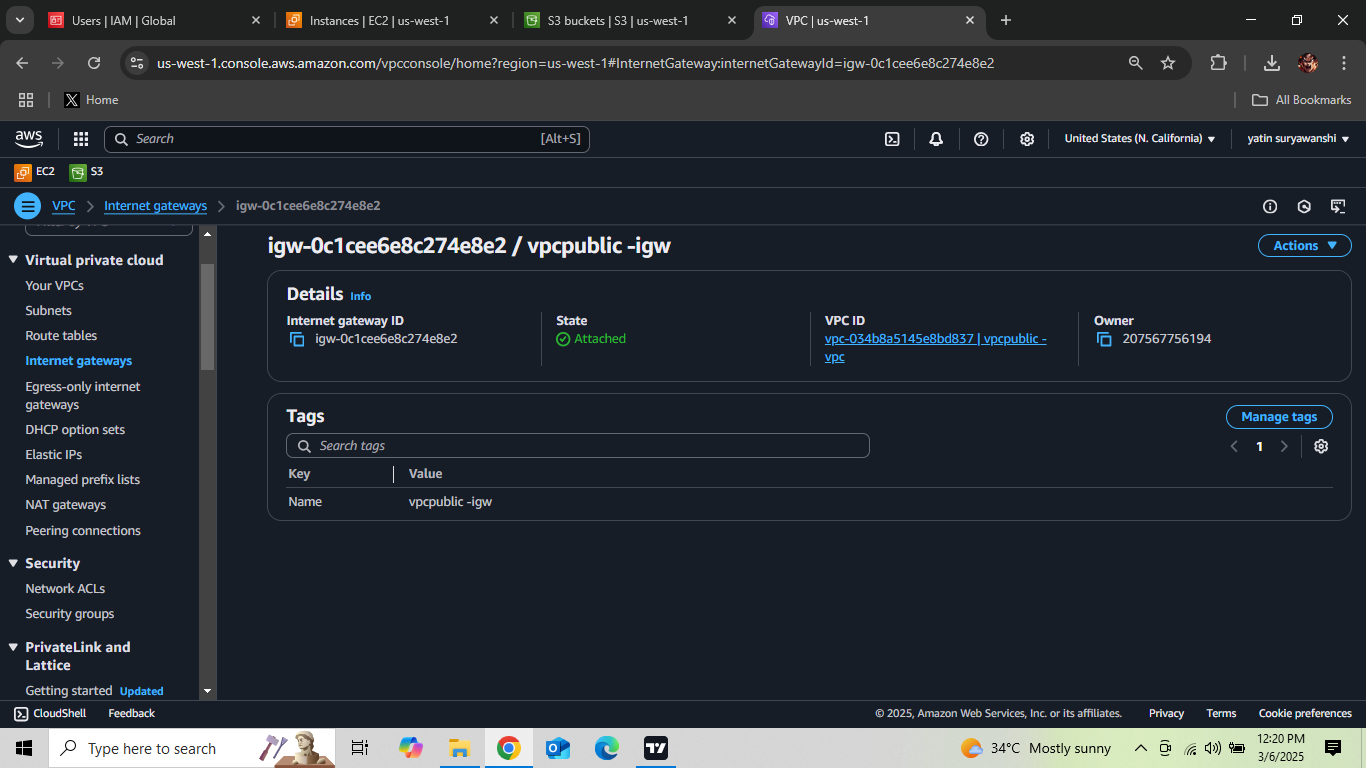
This project involves setting up two VPCs in AWS: one public and one private. The private VPC has an S3 bucket attached, and access to this bucket is provided through the public VPC. The goal is to securely access resources in the private VPC while maintaining isolation.

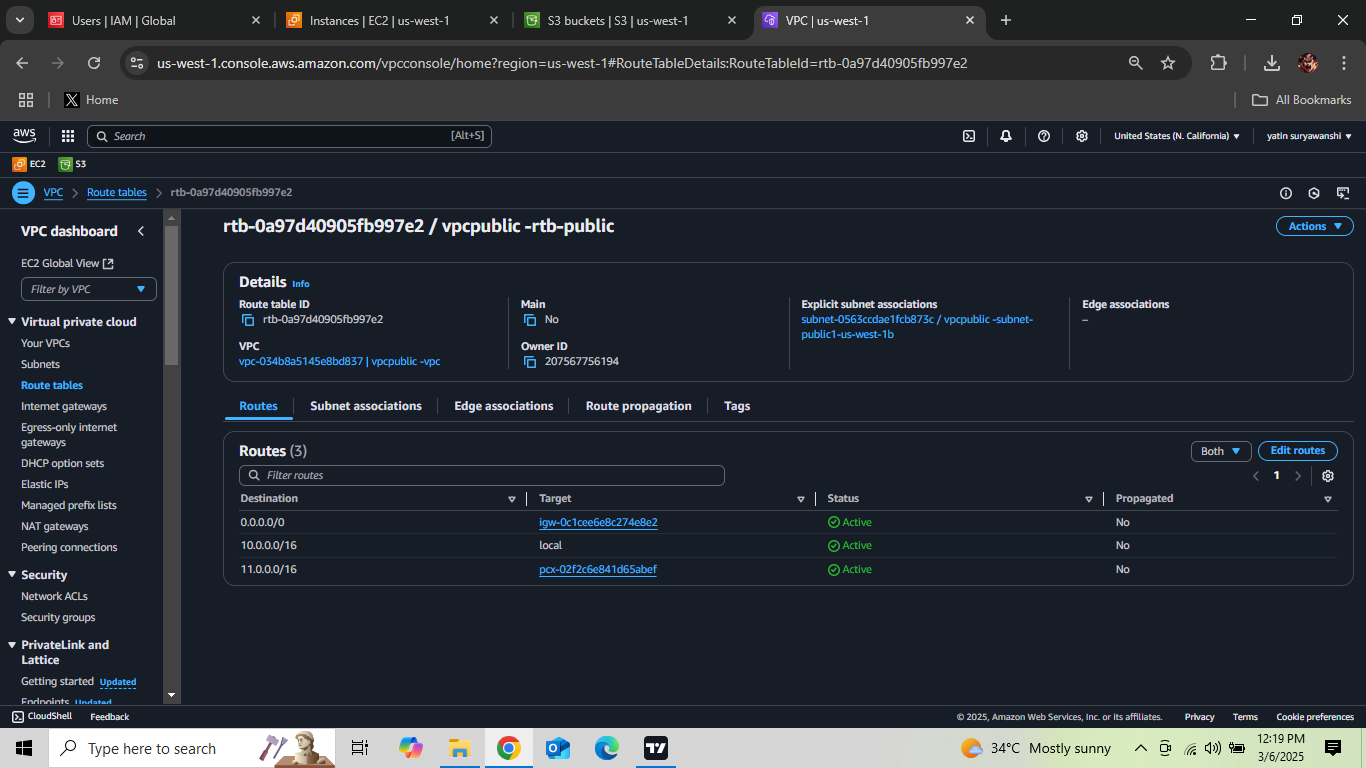
**Architecture Design**

* **VPC 1 (Public VPC)**
  + Contains a bastion/jump host to allow SSH access.
  + Connected to the private VPC via VPC peering.
  + Has an internet gateway for outbound access.
* **VPC 2 (Private VPC)**
  + Contains EC2 instances that require access to S3.
  + Has an S3 bucket for storage.
  + Uses a VPC endpoint to access S3 securely.
  + 

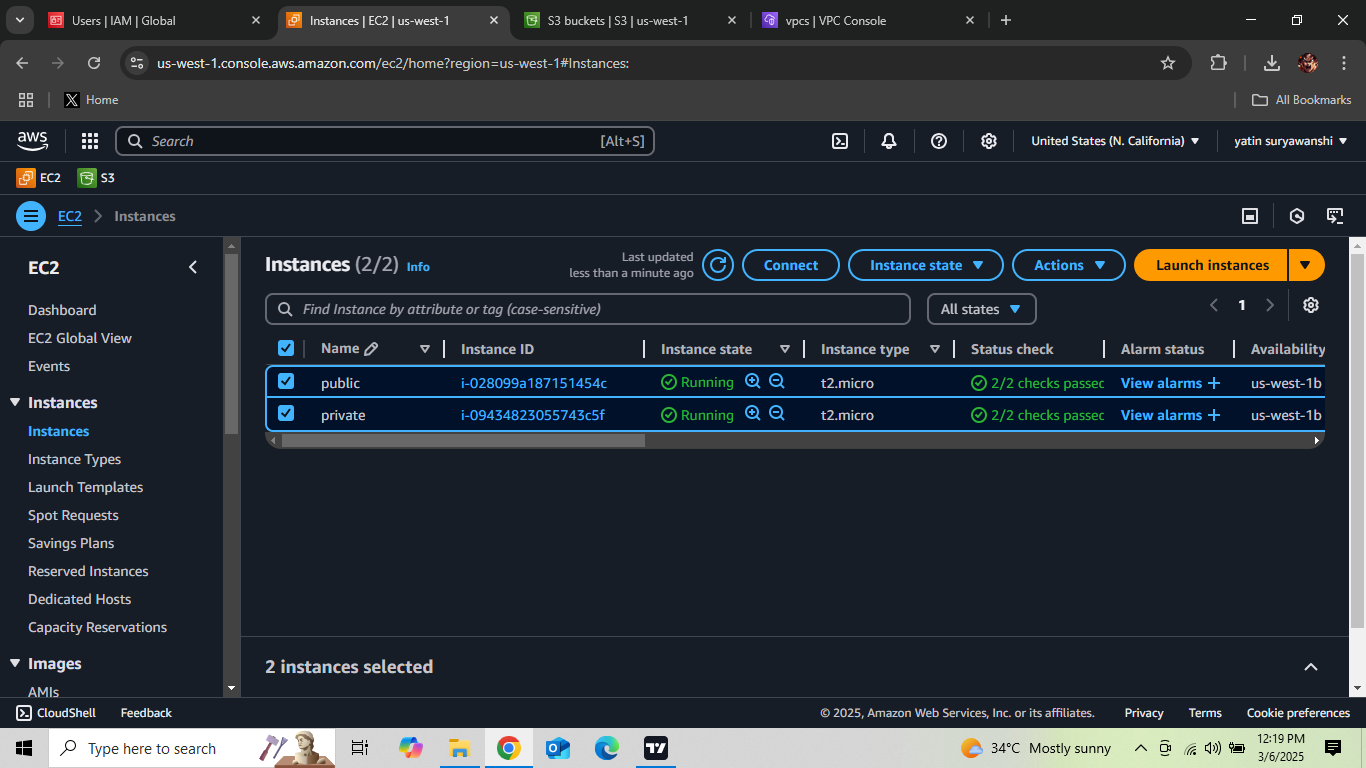
**Implementation Steps**

**1. Create the Public VPC**

* Create a VPC with CIDR block 10.0.0.0/16.
* Add a public subnet 10.0.1.0/24.
* 
* Attach an Internet Gateway.
* 
* Create a route table allowing internet access and associate it with the public subnet.



**2. Create the Private VPC**

* Create a VPC with CIDR block 11.0.0.0/16.
* Add a private subnet 11.0.1.0/24.
* Do not attach an Internet Gateway (ensuring it remains private).
* 

**3. Set Up VPC Peering**

* Create a VPC peering connection between the public and private VPCs.
* Update the route tables to allow traffic between them.

**4. Configure an S3 VPC Endpoint in the Private VPC**

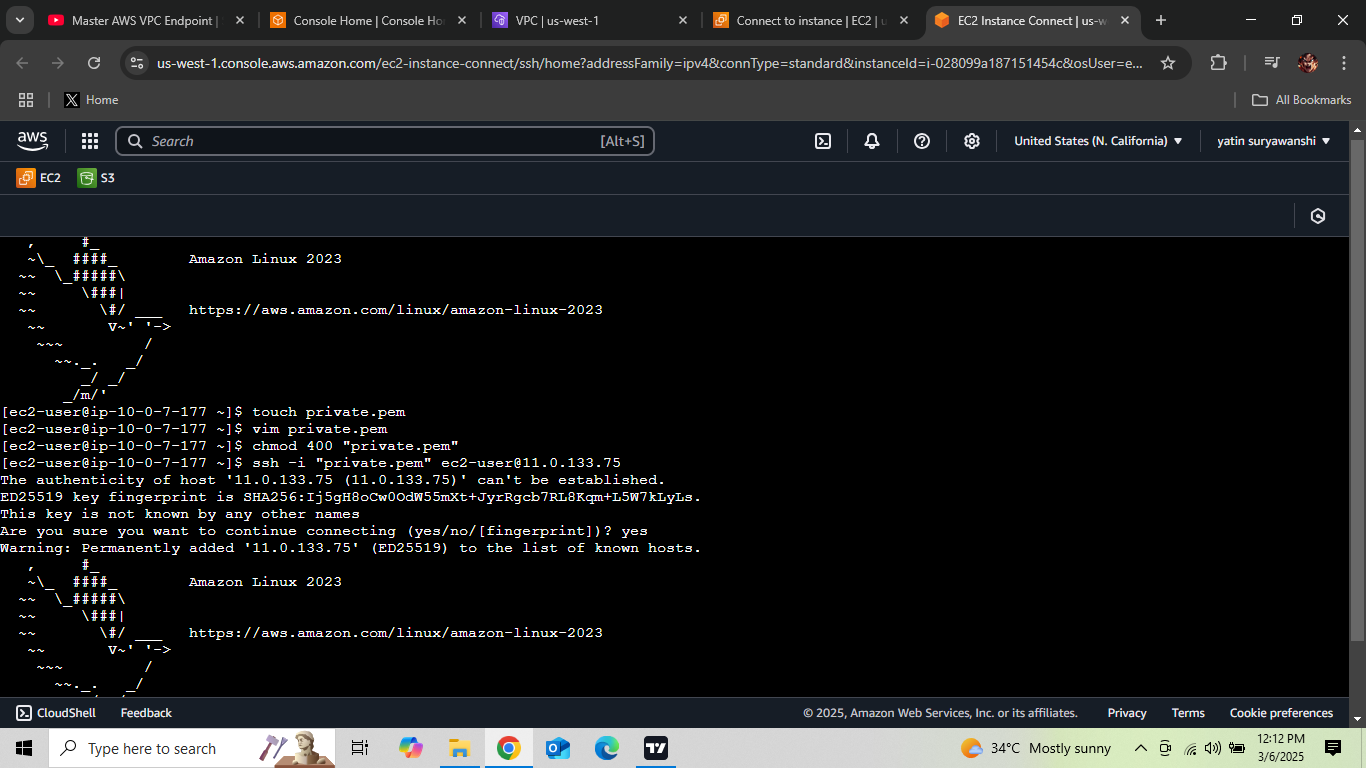
* Navigate to the **AWS VPC Console**.
* Select **Endpoints** from the left panel.
* Click **Create Endpoint**.
* Choose the **AWS Services** category and select **S3** as the service.
* Select the **Private VPC (11.0.0.0/16)**.
* Choose the **Private Subnet (11.0.1.0/24)** for the endpoint.
* Attach the endpoint to the private route table to allow S3 traffic.
* Modify the security group rules to allow S3 access only from the private subnet.
* Save and create the endpoint.

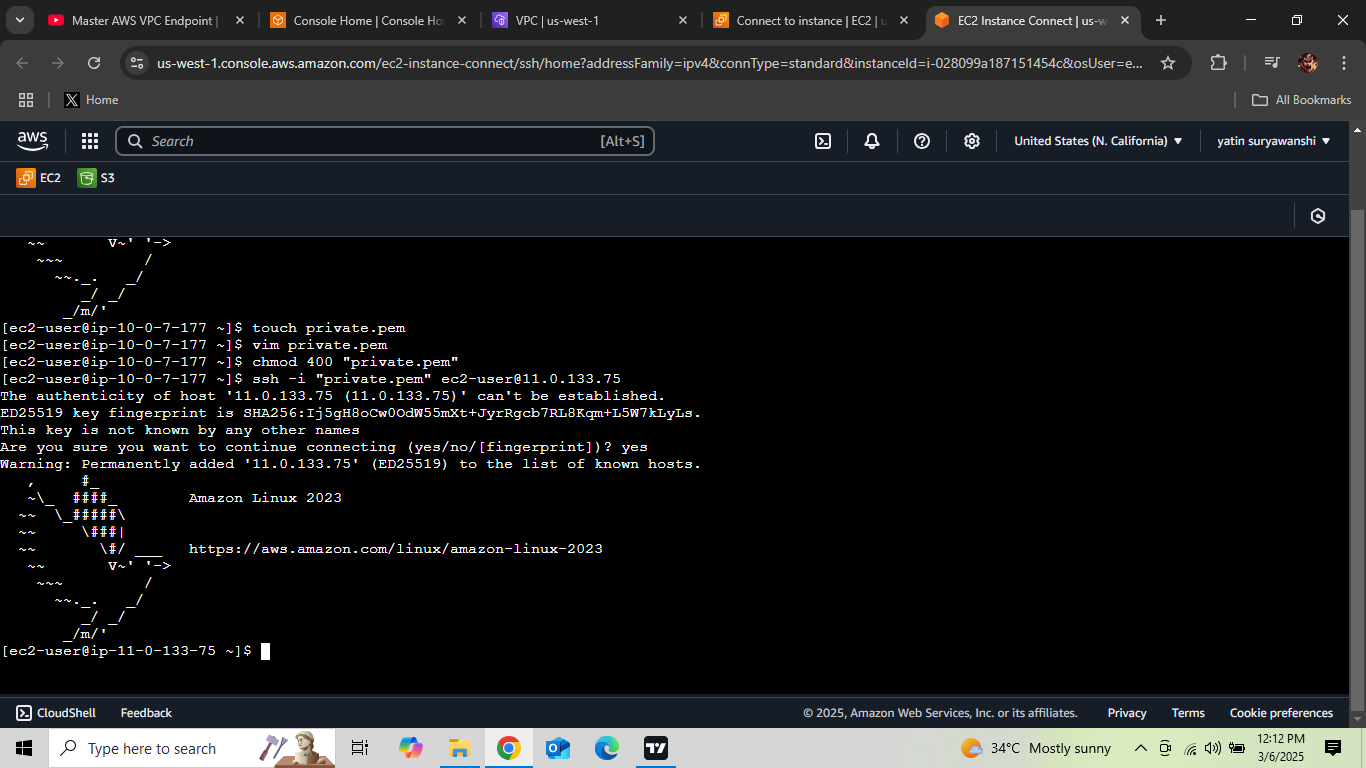
**5. Configure S3 Bucket in the Private VPC**

* Create an S3 bucket and restrict access using an IAM policy.
* Ensure the bucket policy allows access only from the configured VPC endpoint.

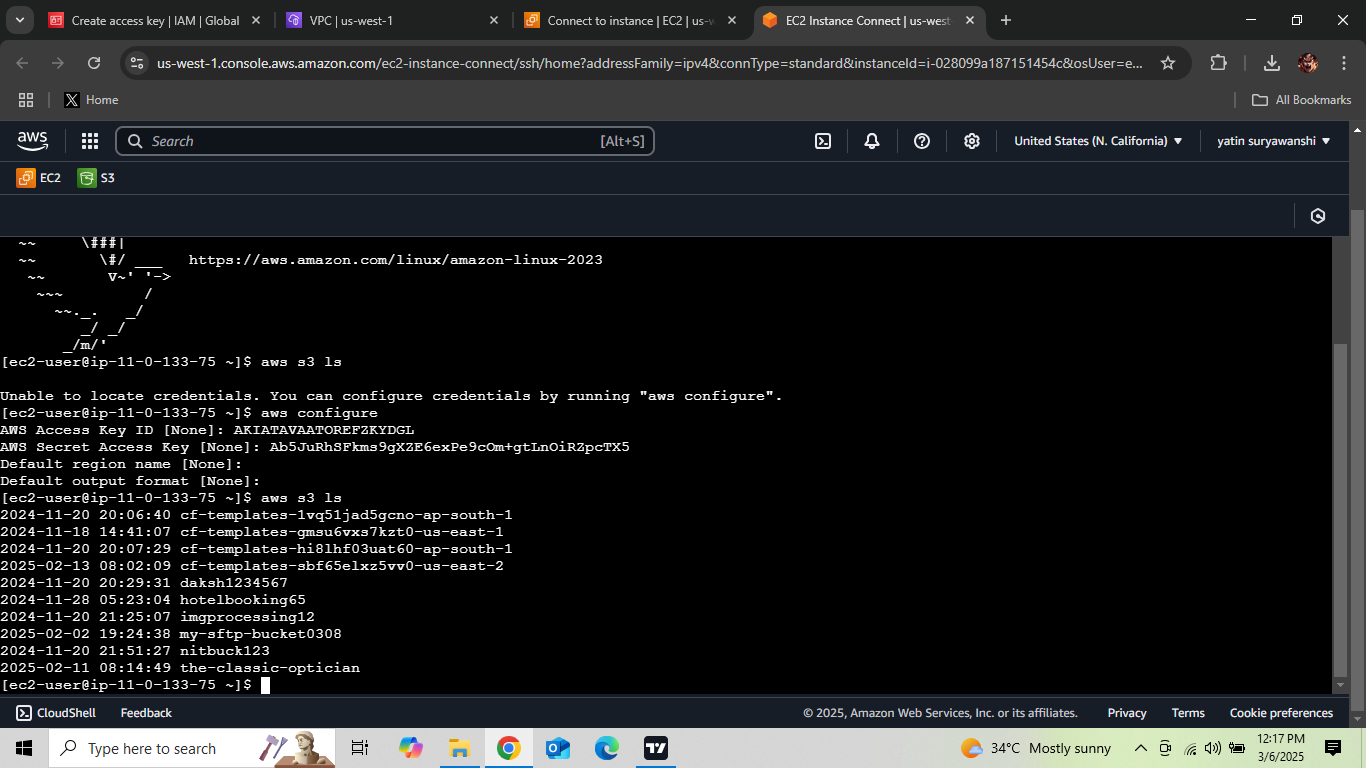
**6. Enable Access Through the Public VPC**

* Deploy an EC2 instance in the public VPC as a bastion host.
* Deploy an EC2 instance in the private VPC.
* SSH into the bastion host, then use it to connect to the private instance.

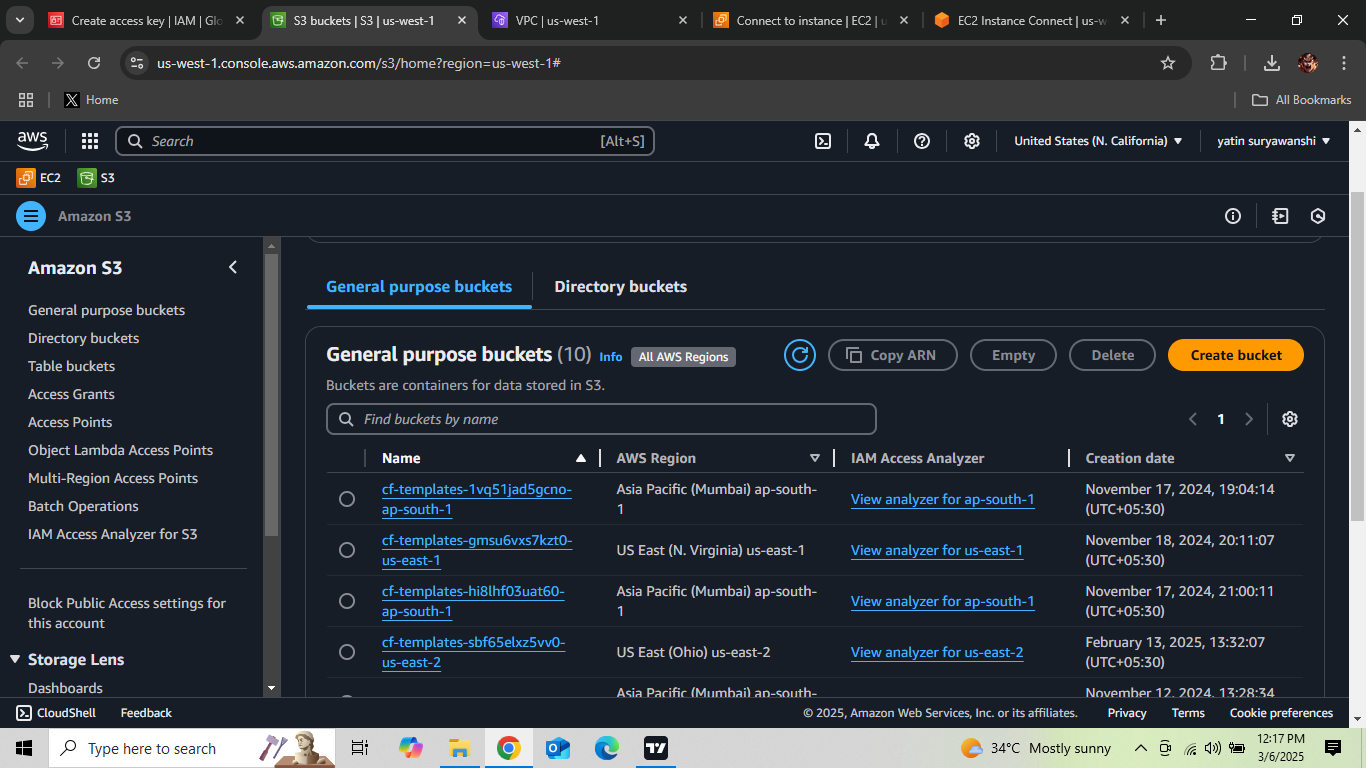




* Verify access to the S3 bucket from the private instance using the AWS CLI.



* aws s3 ls s3://your-private-bucket-name --region your-region



**Security Considerations**

* **IAM Policies**: Restrict S3 access to only necessary resources.
* **Security Groups**: Limit inbound and outbound traffic.
* **VPC Endpoint**: Ensures secure access to S3 without an internet gateway.
* **Bastion Host**: Used as an intermediate access point to keep the private network secure.

**Conclusion**

This setup enables secure access to an S3 bucket in a private VPC using a public VPC. By implementing VPC peering and an S3 VPC endpoint, the private VPC remains isolated while still allowing necessary access.

**Future Enhancements**

* Implement AWS Transit Gateway for better scalability.
* Use AWS Systems Manager Session Manager to eliminate the need for a bastion host.
* Apply strict network ACLs and monitoring using AWS CloudTrail and AWS Config.