Day 1 – AWS Key Pair Creation (AWS)

📅 Challenge

100 Days of Cloud (AWS & Azure)
Day 1 – AWS Fundamentals

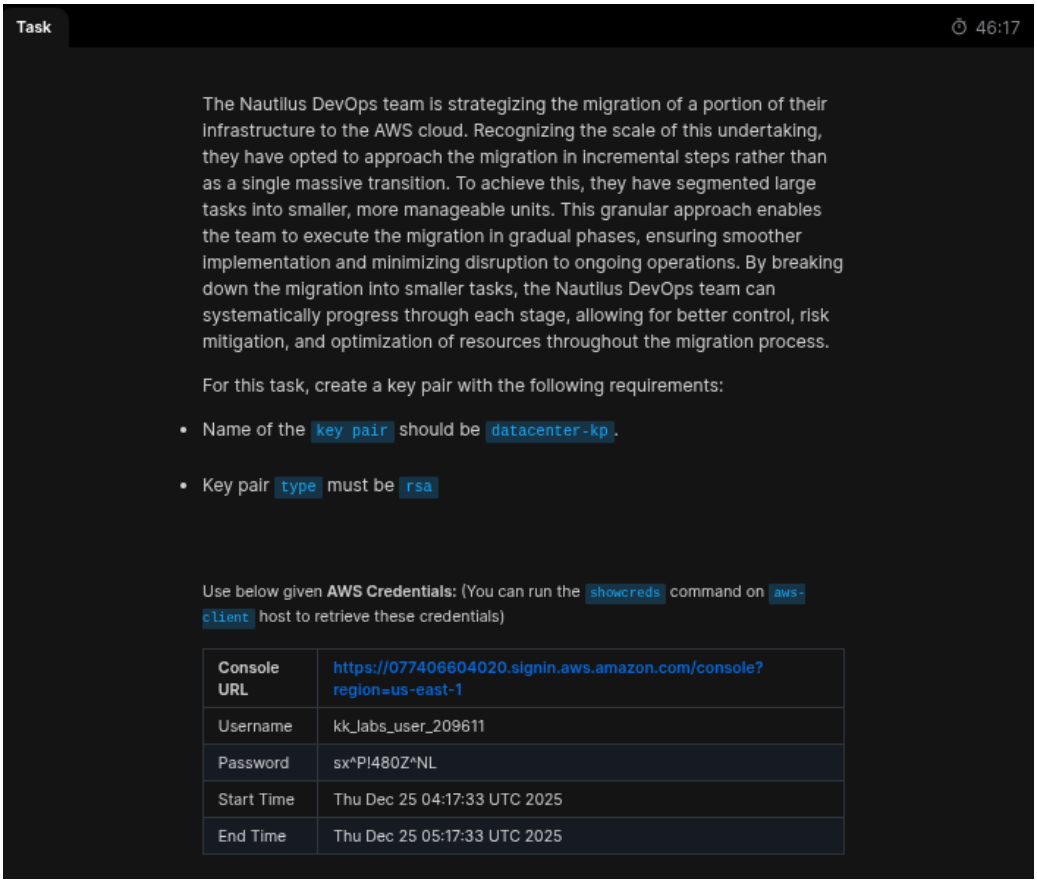
🎯 Objective

Create an AWS EC2 key pair that will later be used for secure access to cloud servers.

This task validates understanding of basic AWS security concepts and correct regional configuration.

📌 Task Requirements

Requirement	Value
Key Name	datacenter-kp
Key Type	RSA
AWS Region	us-east-1



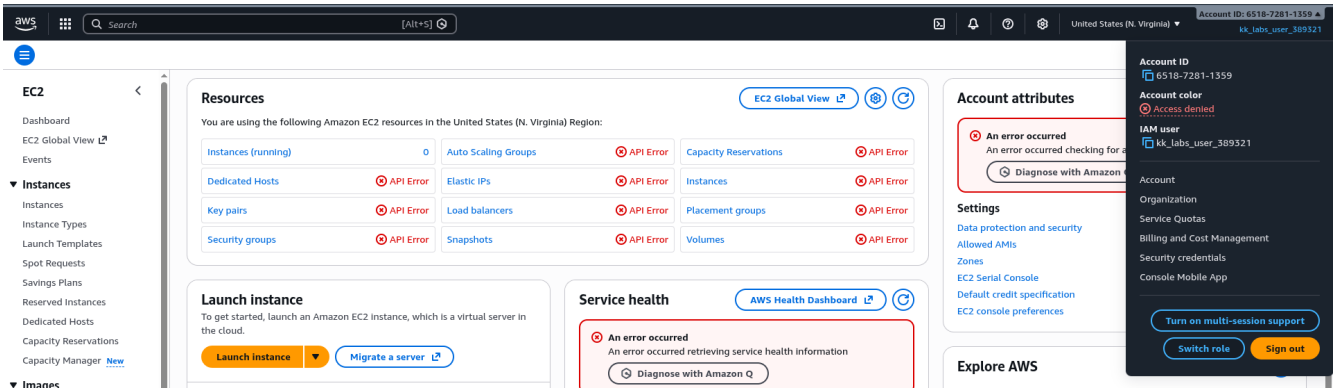
Concept Overview

An **AWS Key Pair** is a set of cryptographic keys (public & private) used to securely authenticate to EC2 instances. AWS uses key pairs instead of passwords to improve security.

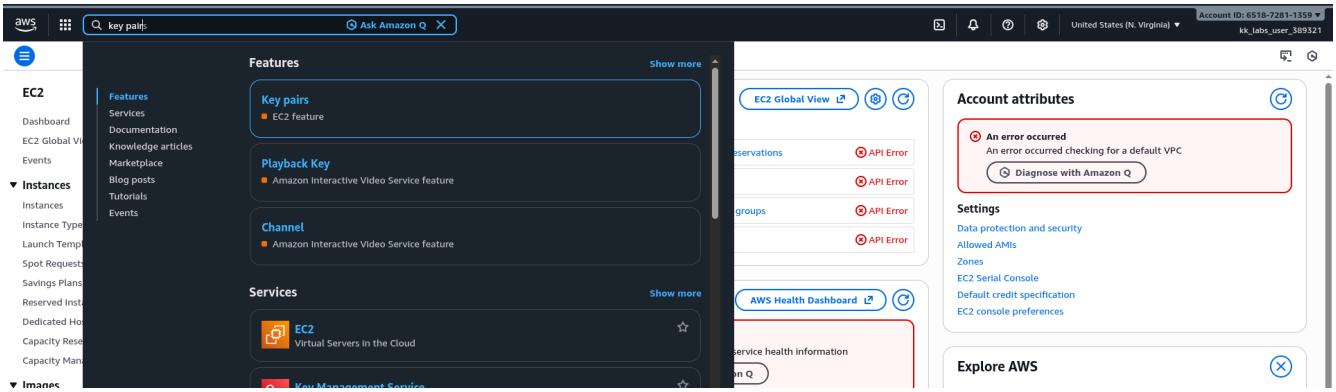
- Public key → stored in AWS
- Private key → downloaded and kept securely by the user

AWS Management Console (GUI)

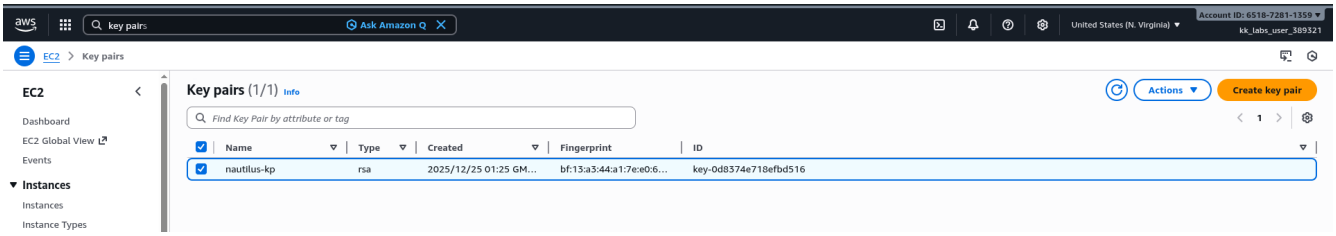
1. Logged into AWS Console using provided credentials



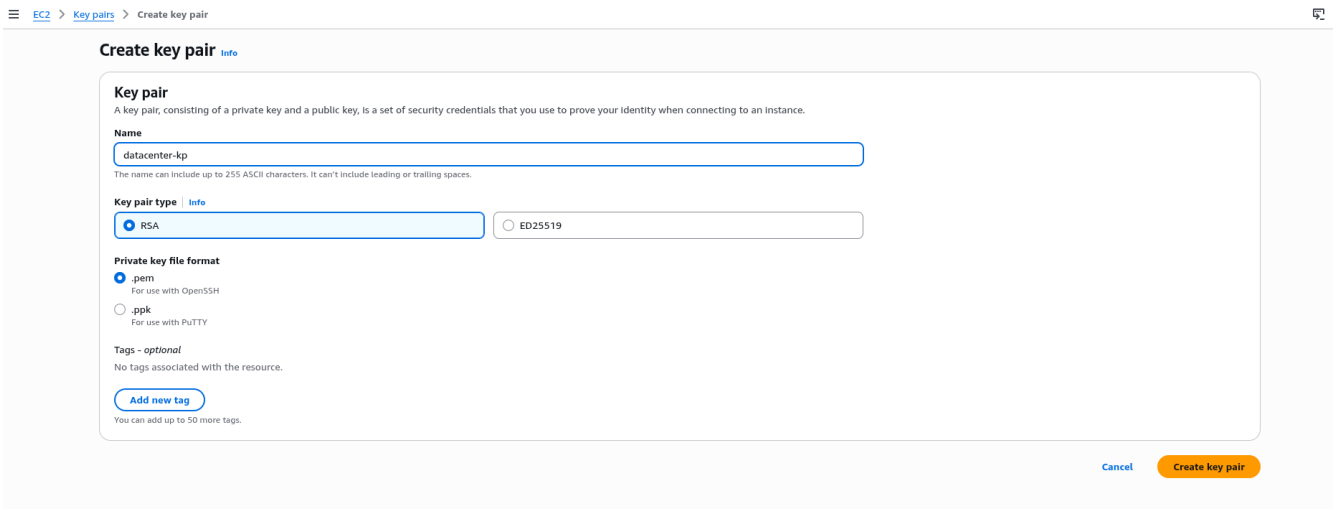
2. Navigated to **EC2 → Key Pairs**



3. Clicked **Create Key Pair**



4. Entered the following:
    - **Name:** datacenter-kp
    - **Type:** RSA
    - **Region:** us-east-1



5. Created and downloaded the key

✅ Outcome

- Successfully created an RSA key pair named datacenter-kp
- Verified creation via CLI and AWS Console
- Private key secured with correct file permissions

📚 Key Takeaways

- AWS uses key pairs instead of passwords for EC2 access
- Correct region selection is critical in AWS

🔖 Proof of Work

This task demonstrates hands-on experience with: - AWS IAM authentication - EC2 key pair management - Secure handling of private keys

📁 Screenshots included as evidence of real cloud work

Next: Day 2 – EC2 Instance Launch & SSH Access