

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

Task 46:17

The Nautilus DevOps team is strategizing the migration of a portion of their infrastructure to the AWS cloud. Recognizing the scale of this undertaking, they have opted to approach the migration in incremental steps rather than as a single massive transition. To achieve this, they have segmented large tasks into smaller, more manageable units. This granular approach enables the team to execute the migration in gradual phases, ensuring smoother implementation and minimizing disruption to ongoing operations. By breaking down the migration into smaller tasks, the Nautilus DevOps team can systematically progress through each stage, allowing for better control, risk mitigation, and optimization of resources throughout the migration process.

For this task, create a key pair with the following requirements:

- Name of the `key pair` should be `datacenter-kp`.
- Key pair `type` must be `rsa`

Use below given AWS Credentials: (You can run the `showcreds` command on `aws-client` host to retrieve these credentials)

Concept Overview

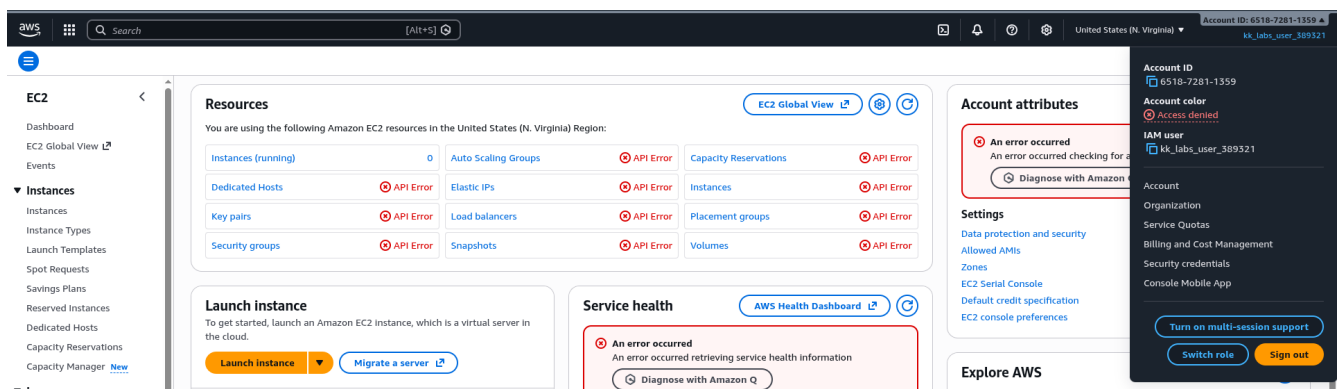
An **AWS Key Pair** is a set of cryptographic keys (public & private) used to securely authenticate to EC2 instances. AWS uses key pairs instead of passwords to improve security.

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

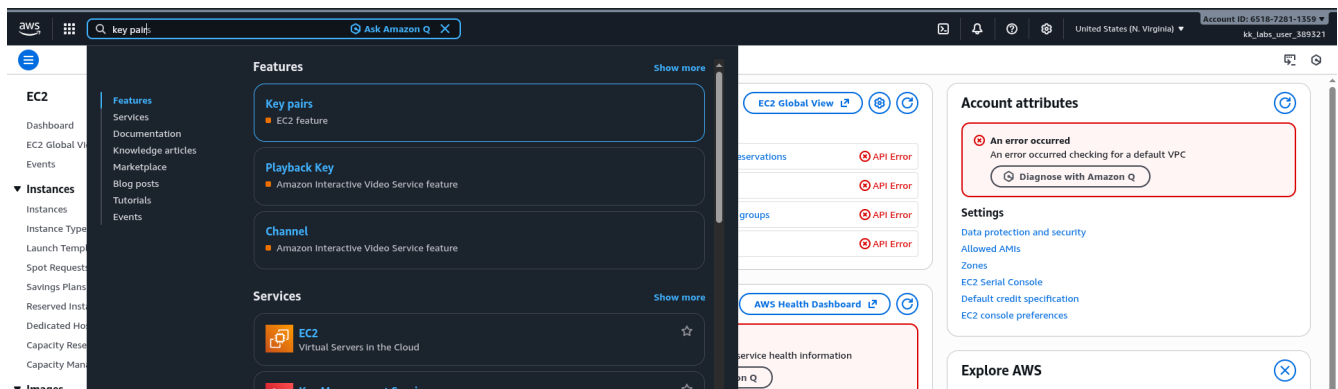


AWS Management Console (GUI)

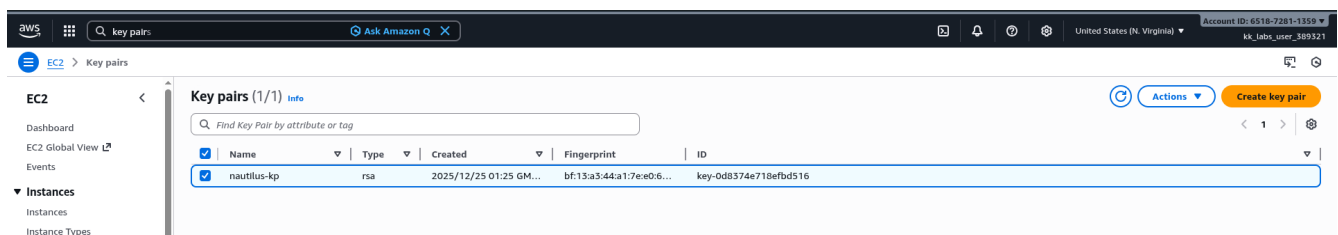
1. Logged into AWS Console using provided credentials



2. Navigated to EC2 → Key Pairs



3. Clicked Create Key Pair



4. Entered the following:

- o **Name:** datacenter-kp
- o **Type:** RSA
- o **Region:** us-east-1

The screenshot shows the AWS Management Console interface for creating a key pair. The breadcrumb navigation at the top indicates the path: EC2 > Key pairs > Create key pair. The main heading is 'Create key pair' with an 'Info' link. Below this, a description states: 'A key pair, consisting of a private key and a public key, is a set of security credentials that you use to prove your identity when connecting to an instance.' The form contains three main sections: 1. 'Name': A text input field containing 'datacenter-kp'. A note below the field states: 'The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.' 2. 'Key pair type': A section with an 'Info' link. It contains two radio buttons: 'RSA' (which is selected) and 'ED25519'. 3. 'Private key file format': A section with two radio buttons: '.pem' (selected) and '.ppk'. A note below states: 'For use with OpenSSH' for .pem and 'For use with PuTTY' for .ppk. Below these sections is a 'Tags - optional' section with the text 'No tags associated with the resource.' and an 'Add new tag' button. At the bottom right of the form are 'Cancel' and 'Create key pair' buttons.

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