Day 2 – AWS Core Services

Introduction

On Day 2, we focus on understanding and working with three of the most essential AWS services — EC2, S3, and IAM. These services form the foundation for computing, storage, and access control within the AWS ecosystem. This day combines theoretical understanding with practical, hands-on activities to get familiar with the AWS Management Console.

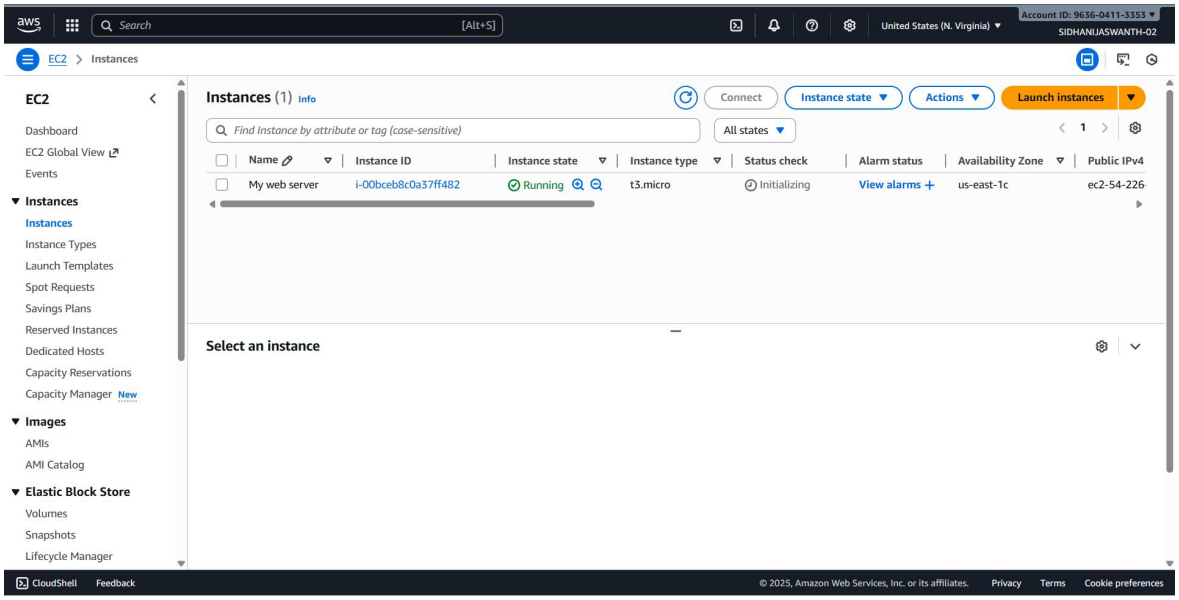
1. Amazon EC2 (Elastic Compute Cloud)

Amazon EC2 provides resizable virtual servers (instances) that allow users to run applications on-demand. It offers flexibility in selecting operating systems, storage, and networking configurations. You can start, stop, and terminate instances as needed, making it a scalable and cost-effective compute solution.

Hands-On Steps:

• 1. Log in to your AWS Management Console.
• 2. Navigate to EC2 under the Compute section.
• 3. Click on 'Launch Instance' and select an Amazon Machine Image (AMI).
• 4. Choose an instance type (e.g., t2.micro for the free tier).
• 5. Configure instance details and storage as per default settings.
• 6. Create or select a key pair for SSH access.
• 7. Launch the instance and verify it in your EC2 dashboard.

■ Screenshot



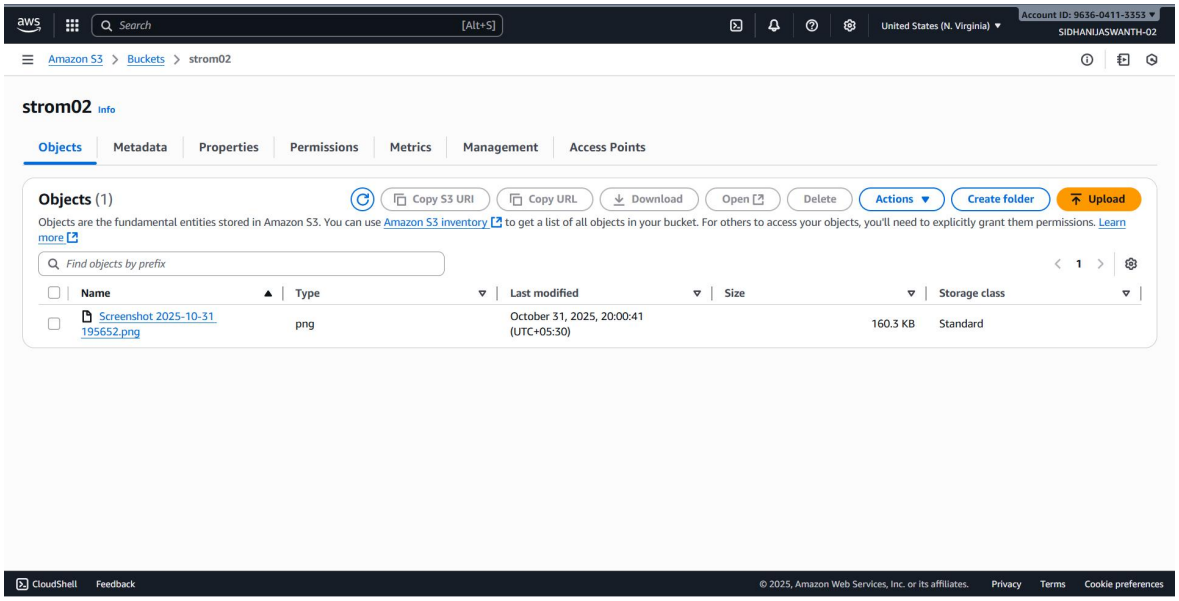
2. Amazon S3 (Simple Storage Service)

Amazon S3 is a scalable storage service designed to store and retrieve any amount of data from anywhere. It’s commonly used for backups, static website hosting, and data storage for applications. S3 buckets organize your files (objects) and manage access permissions.

Hands-On Steps:

• 1. Go to the AWS Management Console and open S3.
• 2. Click on 'Create Bucket' and give it a unique name.
• 3. Choose the AWS region closest to you.
• 4. Keep default settings for other options and create the bucket.
• 5. Open your bucket and upload a sample file (e.g., image or text file).
• 6. Verify that the file appears inside your S3 bucket

Screenshot



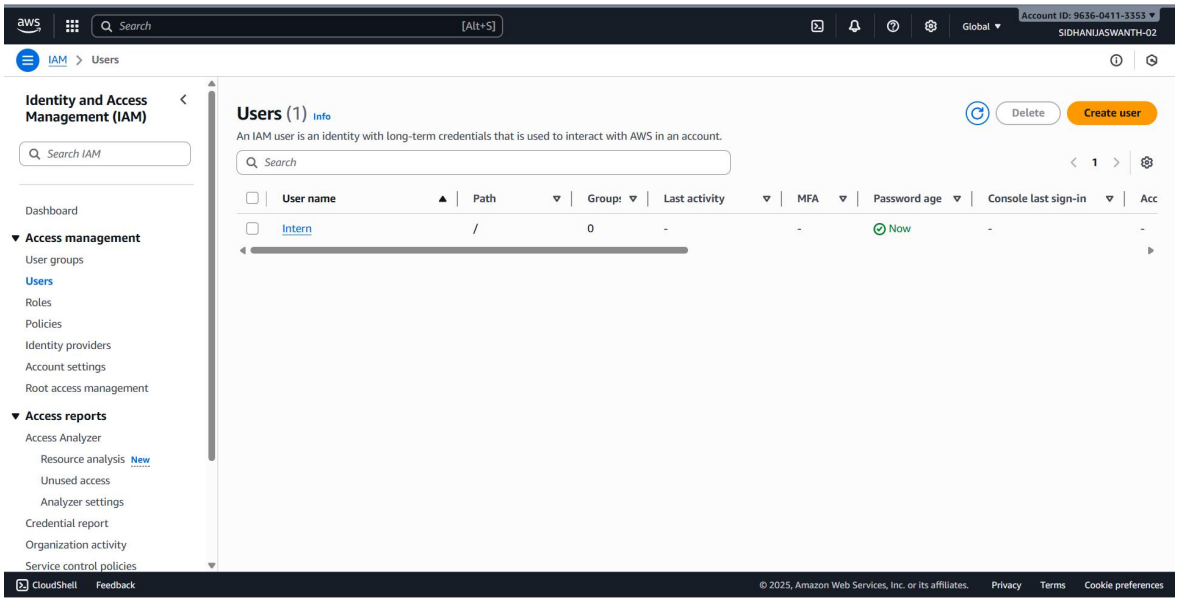
3. Identity and Access Management (IAM)

AWS IAM enables secure control of user access to AWS resources. It allows you to create and manage AWS users, groups, and permissions policies. IAM helps ensure that users have the right level of access based on the principle of least privilege.

Hands-On Steps:

• 1. Open the IAM service from your AWS Console.
• 2. Select 'Users' and click on 'Add User'.
• 3. Enter a username and choose 'Programmatic access' if required.
• 4. Assign user permissions by adding them to a group or attaching policies (e.g., S3FullAccess).
• 5. Review and create the user. Download the access key credentials if prompted.
• 6. Verify the new user in the IAM dashboard.

■ Screenshot



Reflection

Day 2 gave me hands-on experience with AWS's core services — EC2 for compute, S3 for storage, and IAM for security management. I found EC2 particularly interesting because it makes deploying virtual machines extremely simple. S3 impressed me with its simplicity and scalability for file storage. Setting up IAM helped me understand access management and permissions better. Initially, navigating between these services was a bit confusing, but I quickly realized how interconnected they are. This day helped me gain practical confidence in managing cloud resources effectively.