**Placement Empowerment Program**

***Cloud Computing and DevOps Centre***

Set Up IAM Roles and PermissionsCreate an IAM role on your cloud platform. Assign the role to your VM to restrict/allow specific actions.

Name: Mahalakshmi N Department: IT



**Introduction and Overview**

IAM (Identity and Access Management) roles and permissions are a critical part of cloud security. They define **who can access what resources and perform what actions** within your cloud infrastructure. By creating IAM roles, you can assign specific privileges to users, applications, or services, ensuring fine-grained control over resources. For example, when working with a virtual machine (VM), attaching an IAM role enables the VM to securely access other cloud resources without exposing sensitive credentials. This enhances security and simplifies permissions management.

**Objective**

The main objectives of setting up IAM roles and permissions include:

1. **Enhancing Security**: Restrict access to sensitive resources and actions, reducing the risk of unauthorized activity.
2. **Simplifying Access Management**: Assign roles to users or services instead of managing individual permissions.
3. **Enabling Least Privilege**: Grant only the minimum required permissions for tasks, ensuring better security.
4. **Facilitating Automation**: Allow virtual machines and applications to perform actions securely without hardcoding credentials.
5. **Ensuring Compliance**: Maintain a clear audit trail for access and usage of cloud resources.

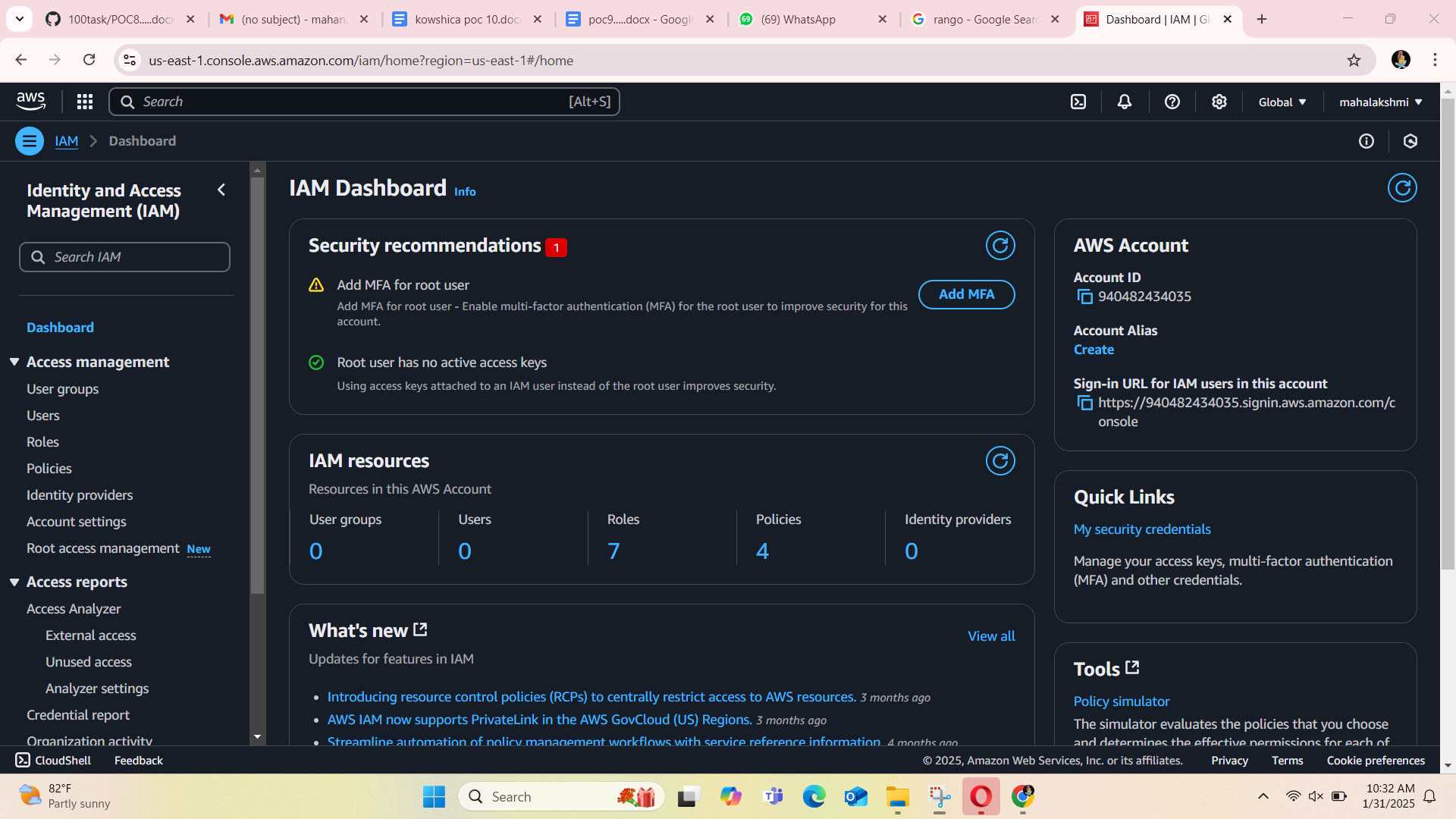
**Importance of Cloud CLI**

1. **Strengthened Security**: IAM roles enforce strict control over who can perform what actions, reducing vulnerabilities.
2. **Scalability**: As your infrastructure grows, IAM roles simplify permissions management across multiple resources.
3. **Compliance Assurance**: Helps meet regulatory requirements by maintaining clear access controls and logs.
4. **Seamless Integration**: Enables secure communication between cloud services and applications.
5. **Cost Efficiency**: Prevents unintended actions like unauthorized access or resource deletions that could lead to financial losses.

**Step-by-Step Overview**

#### Step 1 **Log In to Your Cloud Platform**

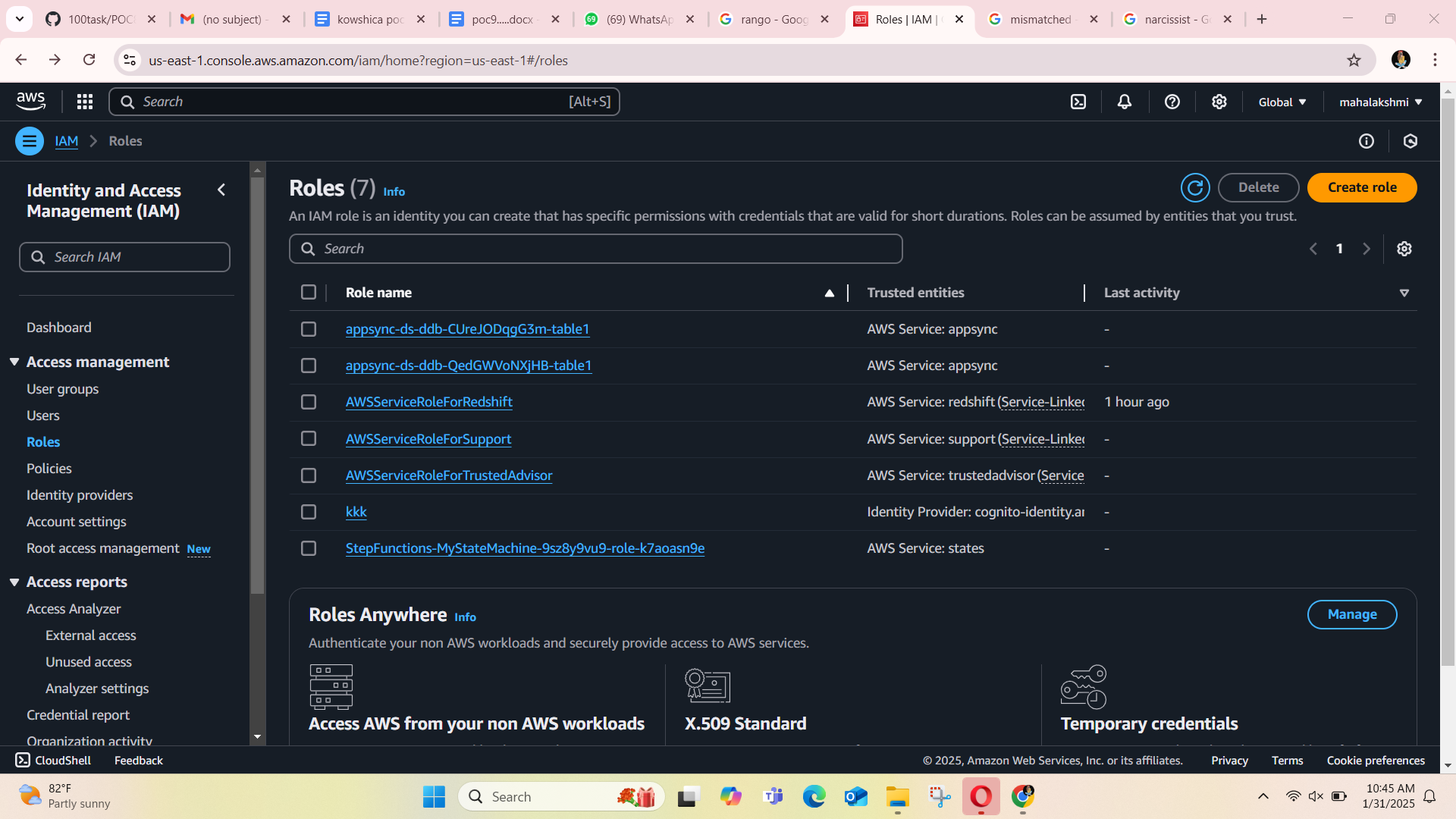
1. Sign in to your cloud platform's console (e.g., AWS, Azure, or GCP).
2. Navigate to the **IAM (Identity and Access Management)** section



Step 2:

**Create a New IAM Role**

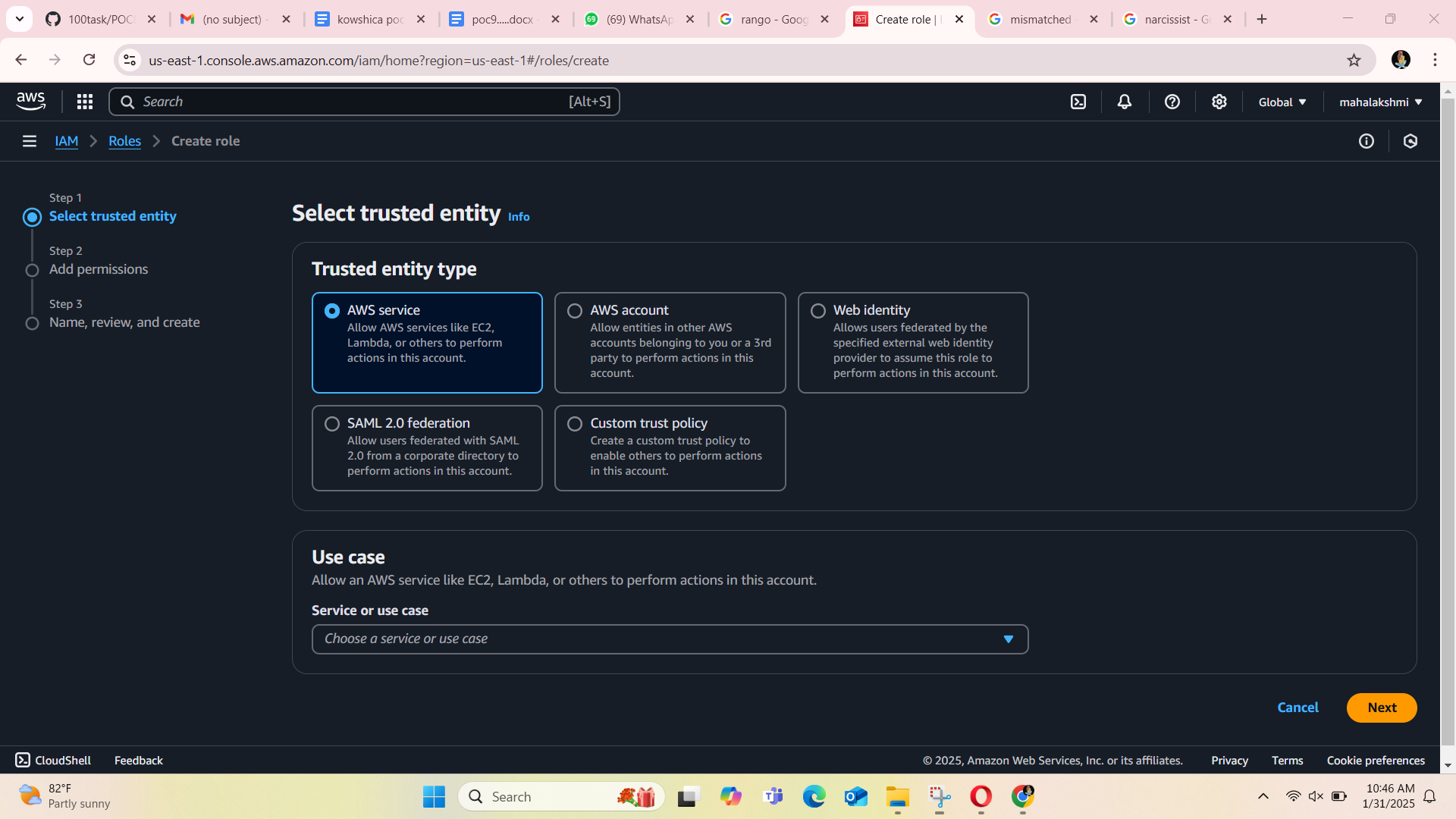
1. **AWS:**
   * Go to the **Roles** section in IAM.
   * Click **Create Role**.
   * Choose a **trusted entity type** (e.g., AWS service for EC2).
   * Select the service (e.g., EC2) and click **Next**.



Step 3:

**Attach Permissions to the Role**

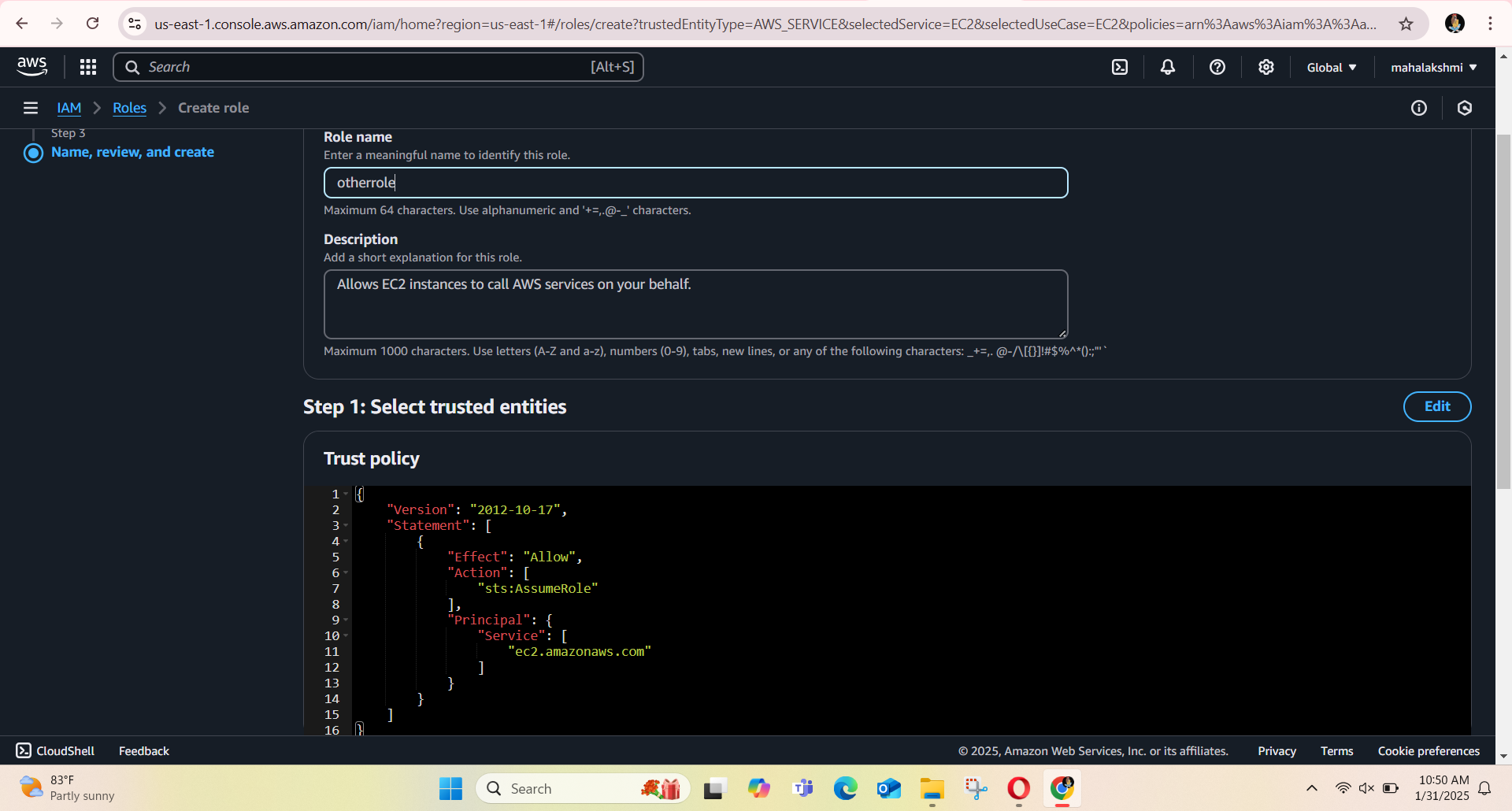
1. Choose the permissions needed for the role:
   * Examples: ReadOnlyAccess, S3FullAccess, ComputeAdmin, etc.
   * Use the **policy editor** or predefined policies to assign permissions.
2. Review the permissions to ensure they match the actions you want to allow or restrict.
3. For custom policies, define them using JSON in AWS/GCP or with the built-in Azure UI.



Step 4:

**Save and Create the Role**

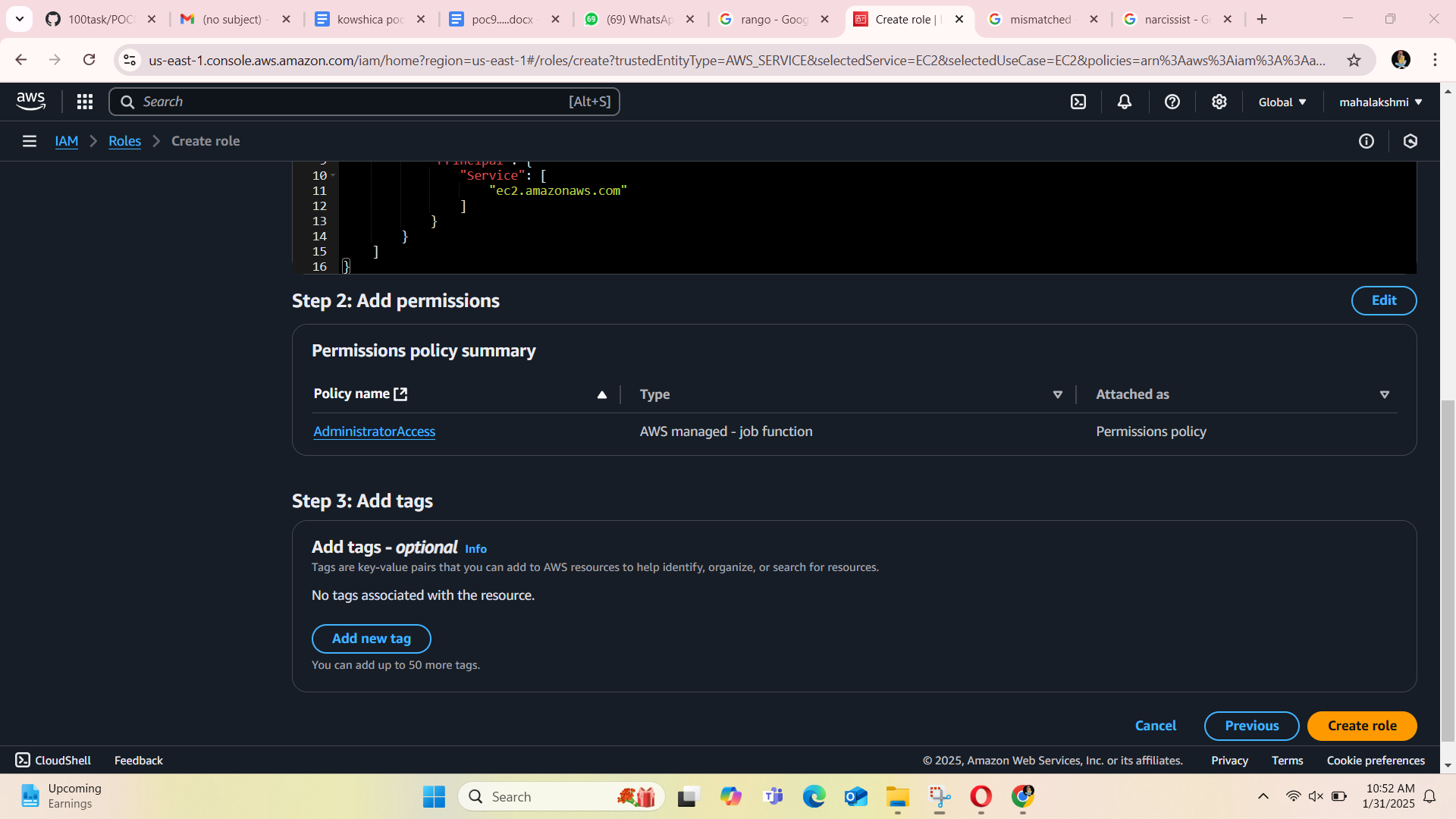
1. Review the role details and click **Create**.
2. Note the role name and any associated policy details for later use



Step 5:

**Assign the IAM Role to Your Virtual Machine (VM)**

1. **AWS:**
   * Go to the **EC2 Dashboard**.
   * Select the instance you want to assign the role to.
   * Click **Actions** > **Security** > **Modify IAM Role**.
   * Choose the IAM role you created and click **Update IAM Role**

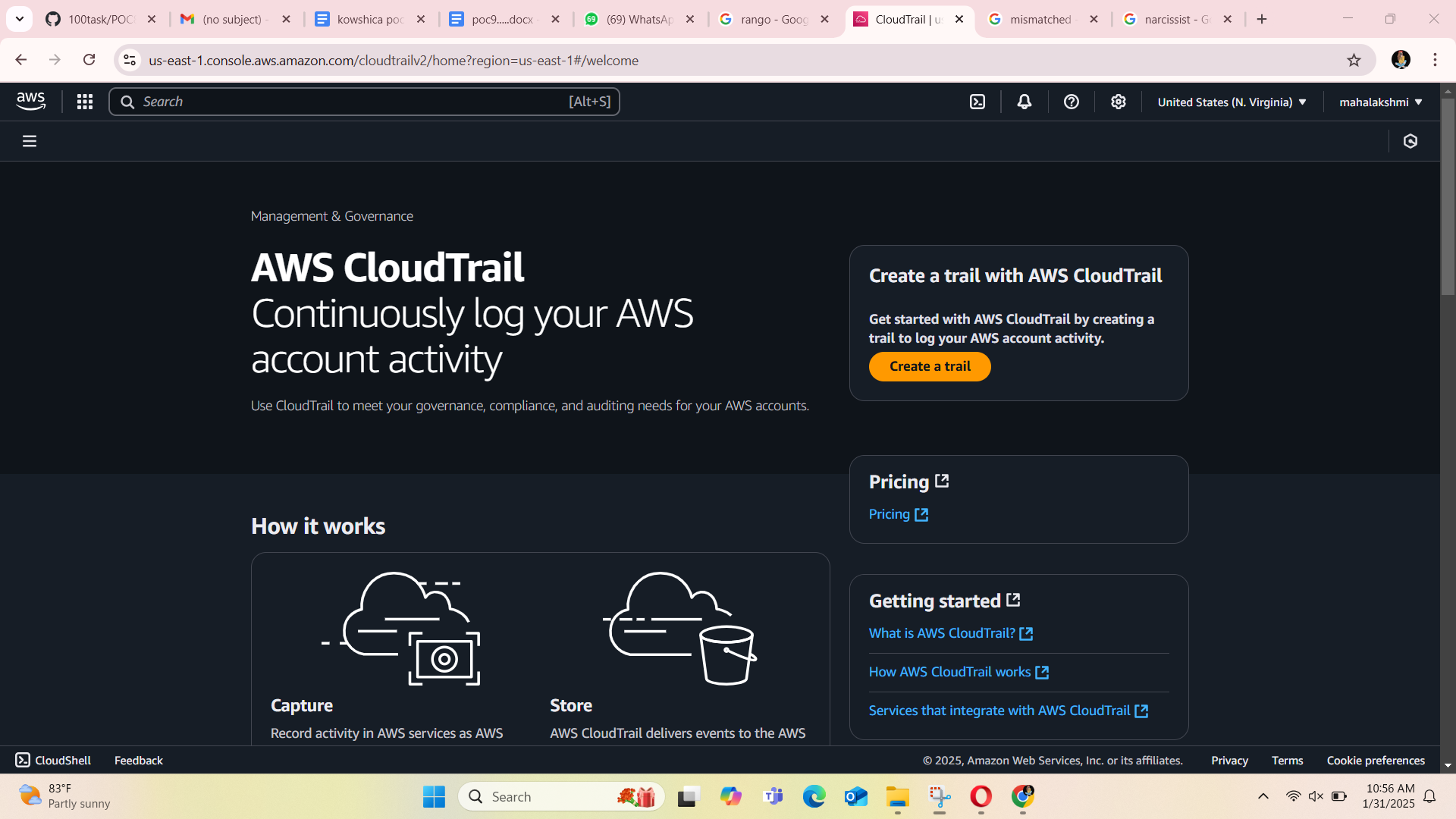


#### Step 6: **Test the Role’s Functionality**

1. SSH into your VM and attempt actions based on the assigned role.
   * Example: Accessing S3, making API calls, etc.

Verify that restricted actions are blocked and allowed actions work correctly.  Go back to the **IAM section** and check for any anomalies in the role’s usage.

1.  Use **CloudTrail (AWS)**, **Activity Logs (Azure)**, or **Cloud Audit Logs (GCP)** to monitor access and activity related to the role.



**Expected Outcome**

By completing this POC, you will:

By setting up IAM roles and permissions, you can achieve the following:

1. **Secure Access Control**:
   * Virtual machines can interact with cloud resources like storage buckets, databases, or APIs securely.
   * Users and services have limited access to sensitive resources.
2. **Improved Resource Management**:
   * Easily update and manage permissions through role assignments instead of modifying individual users or policies.
3. **Minimized Risk of Credential Leakage**:
   * Since IAM roles eliminate the need to store credentials directly on VMs, the risk of credentials being exposed is reduced.
4. **Audit and Monitoring Capabilities**:
   * Detailed logging of resource access helps identify unauthorized attempts and ensures compliance with security standards.
5. **Increased Efficiency**:
   * Roles and policies streamline permissions management, especially in complex cloud environments.