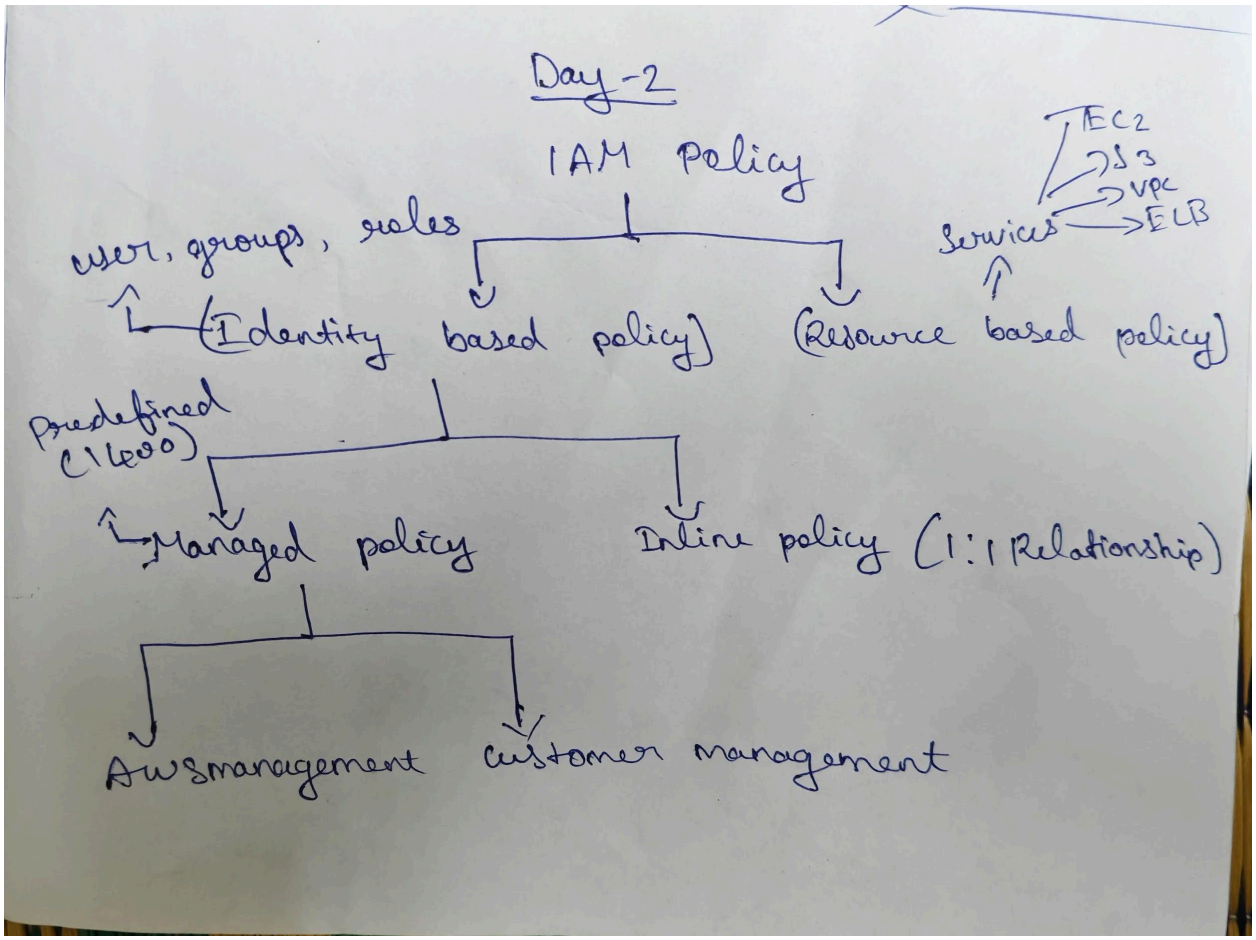
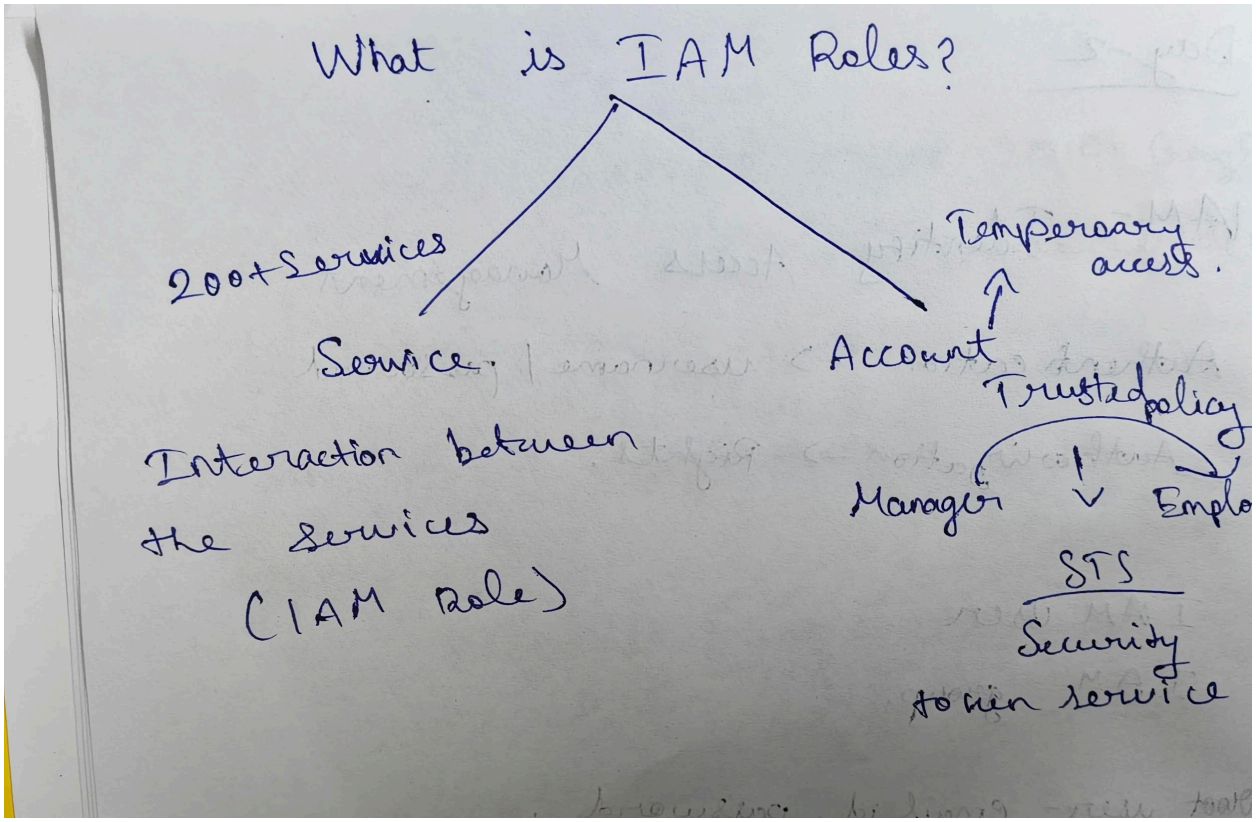
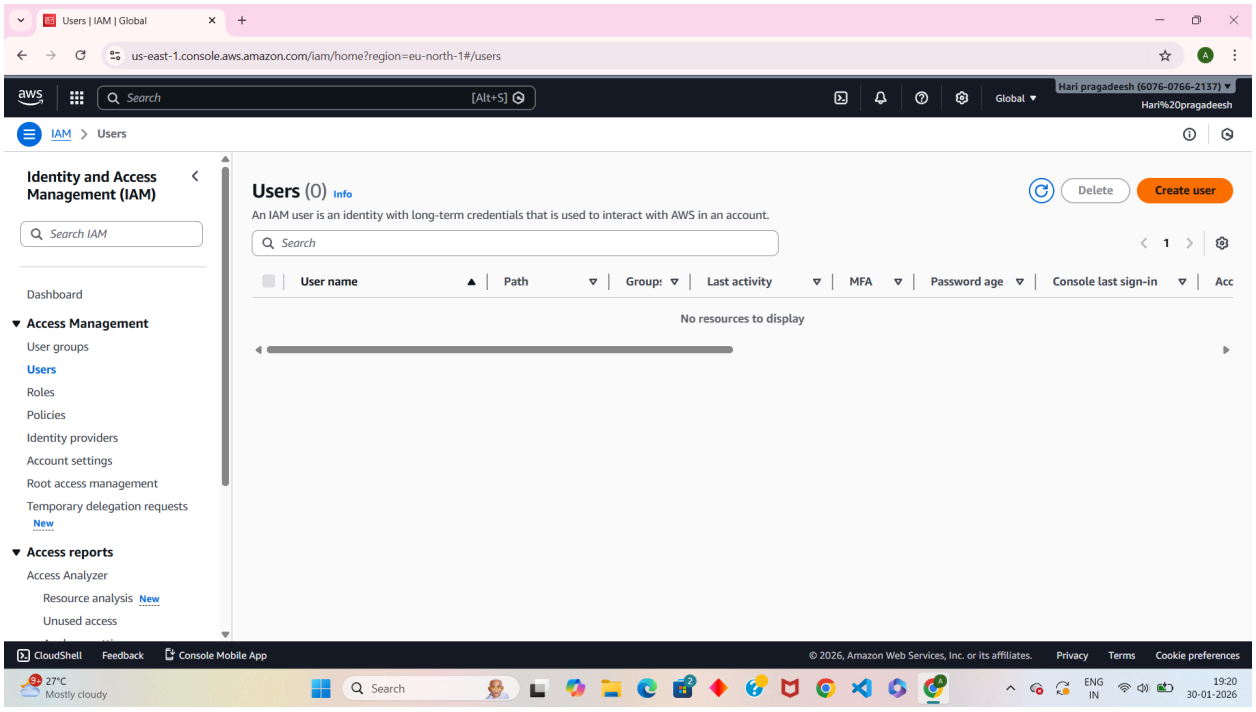
IAM ROLES AND POLICIES

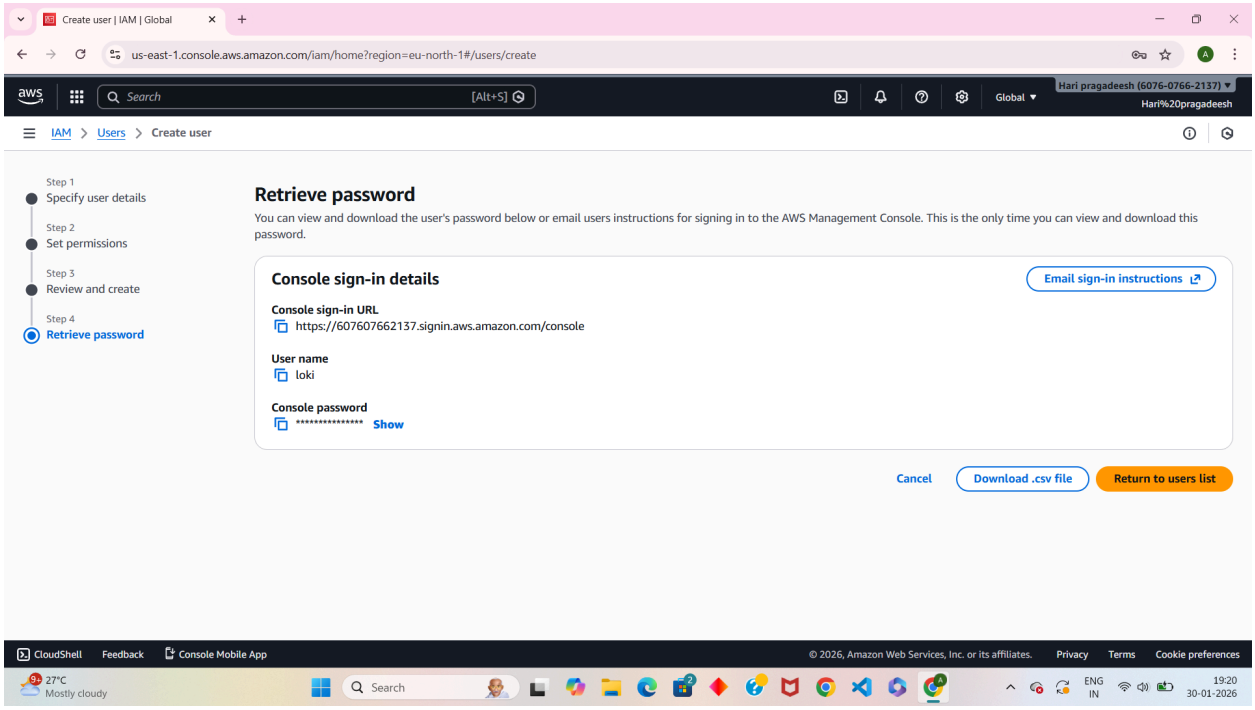




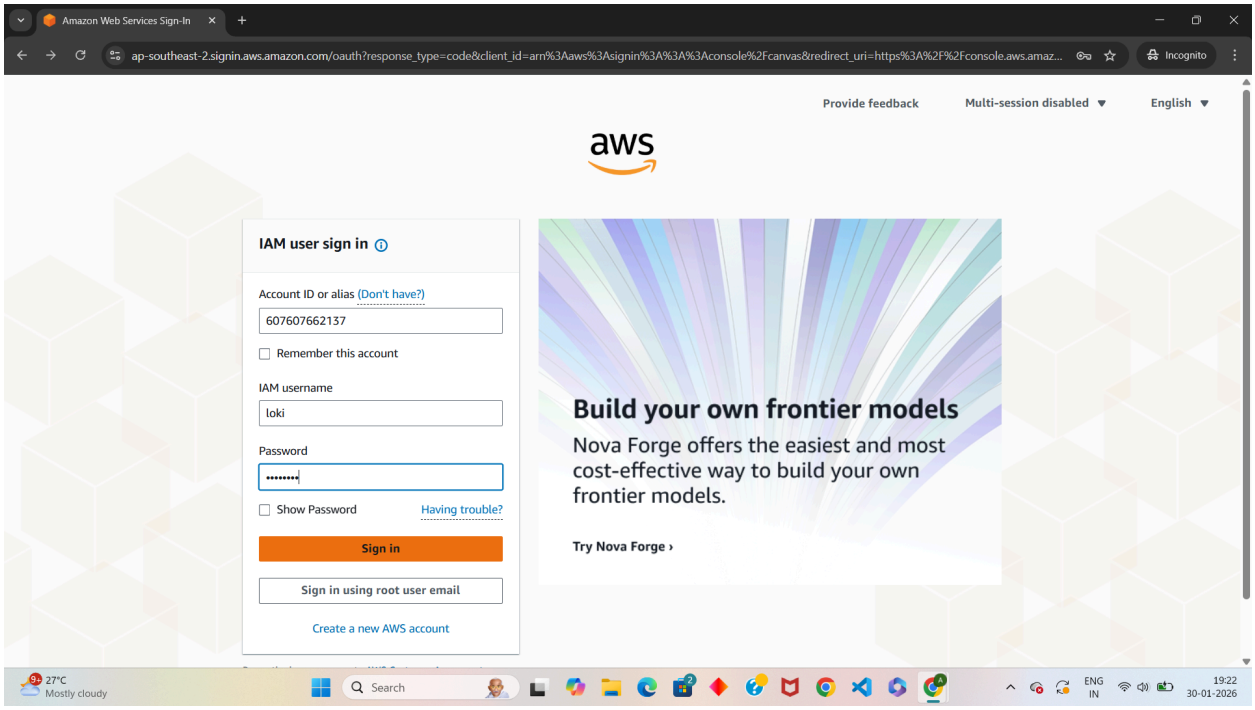


- IAM **Users section is opened**

- **No IAM users** are currently listed (Users = 0)
- Option available to **Create a new IAM user**
- This page is used to **manage users and their access**



- **A new IAM user “loki” has been created**
- **Console sign-in URL is generated**
- **Temporary password is shown (only visible once)**
- **Option to download credentials as CSV**
- **Used to share login details with the user**

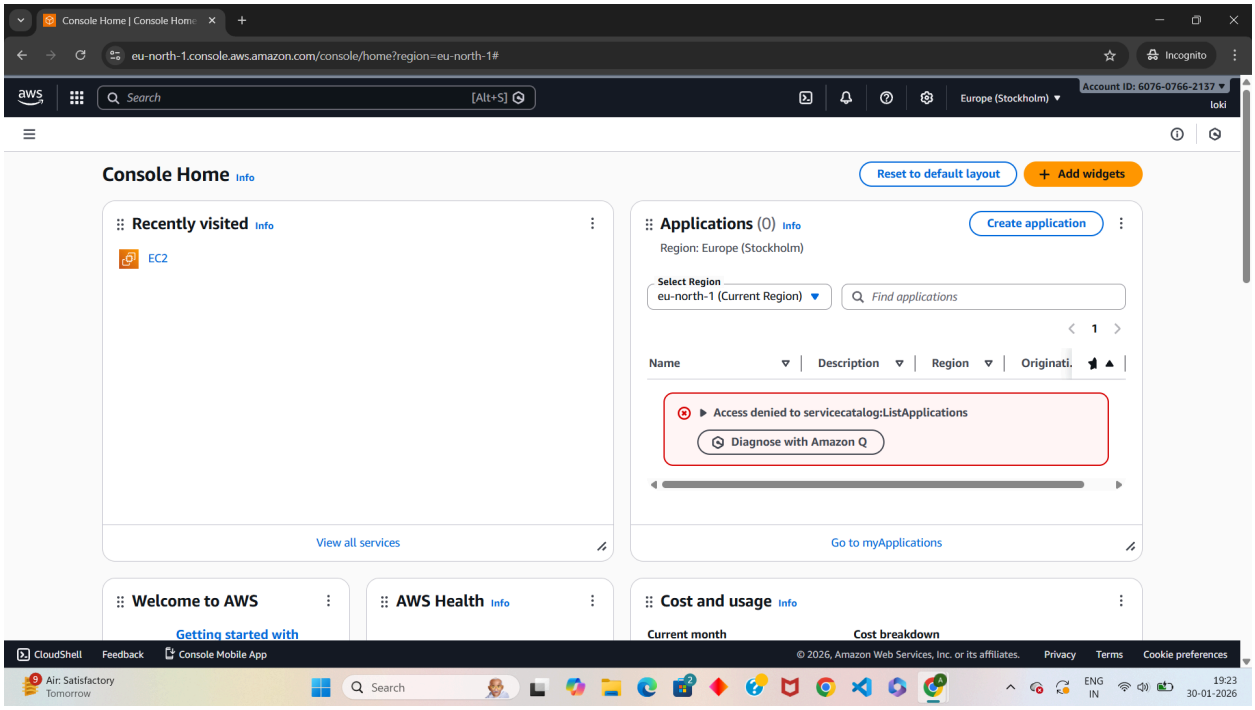


IAM user login screen

Account ID, username, and password are entered

User is signing in as an IAM user (not root)

Used to access AWS Console with limited permissions



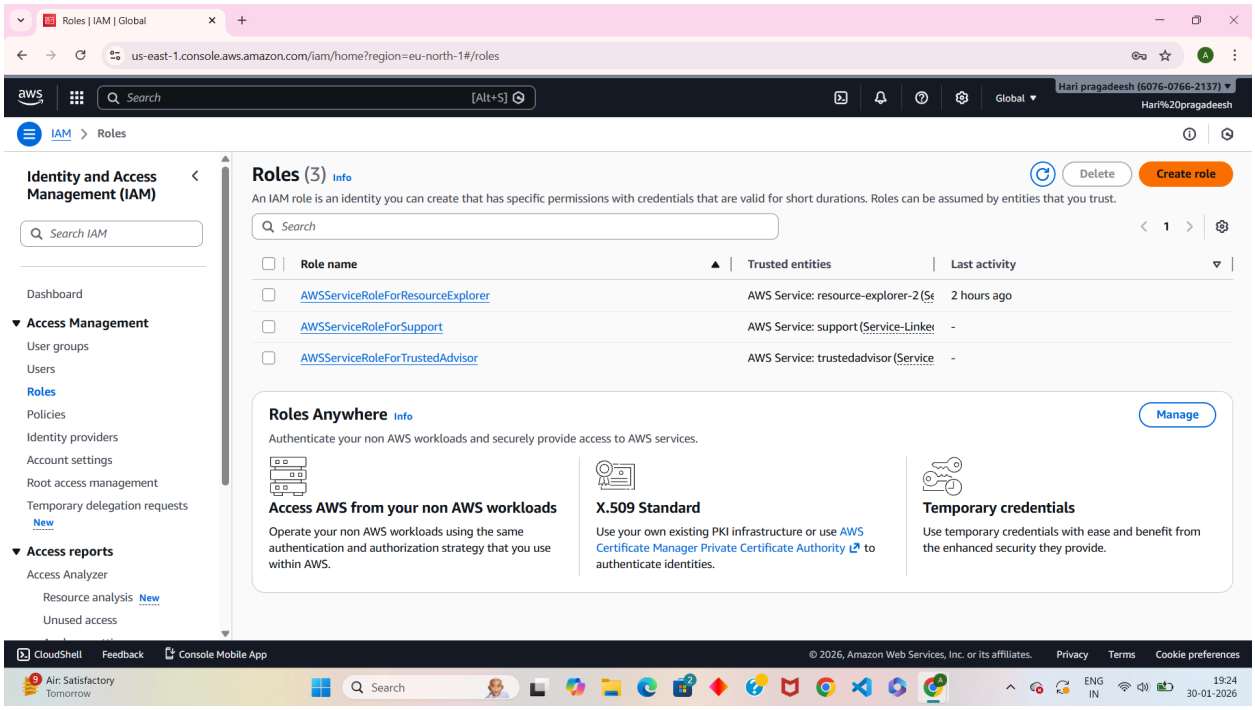
IAM user successfully logged in

Region selected: Europe (Stockholm)

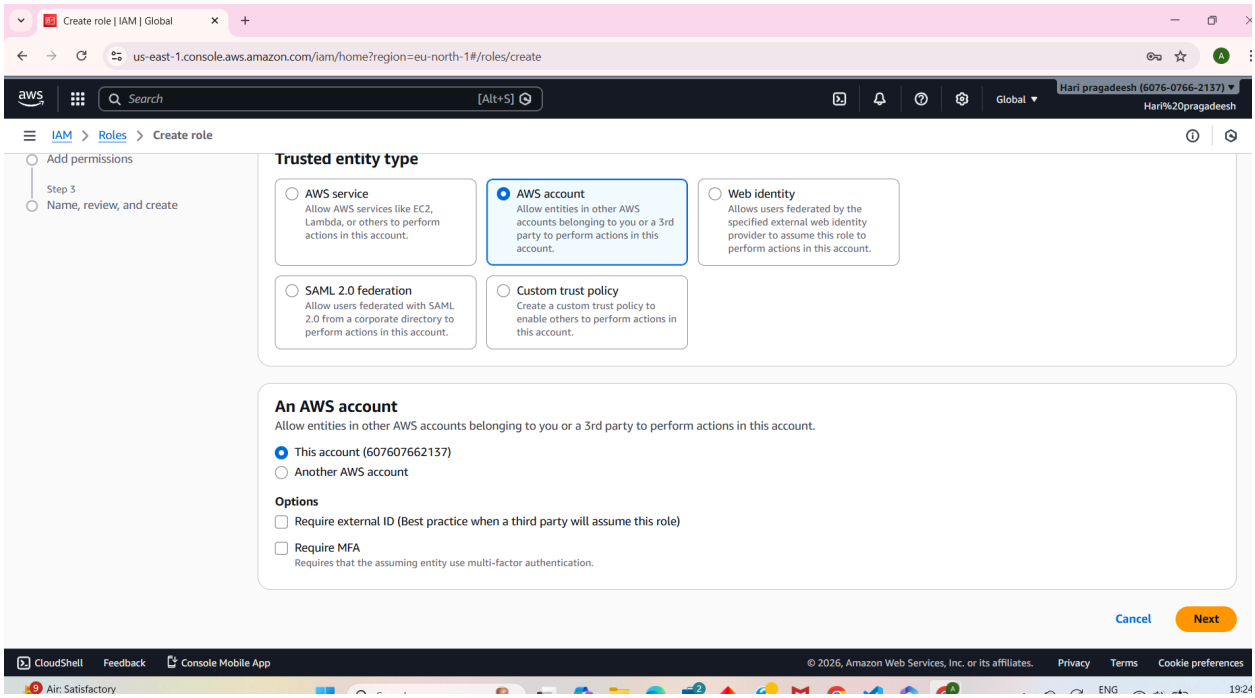
EC2 shown under recently visited services

Access denied error appears (insufficient permissions)

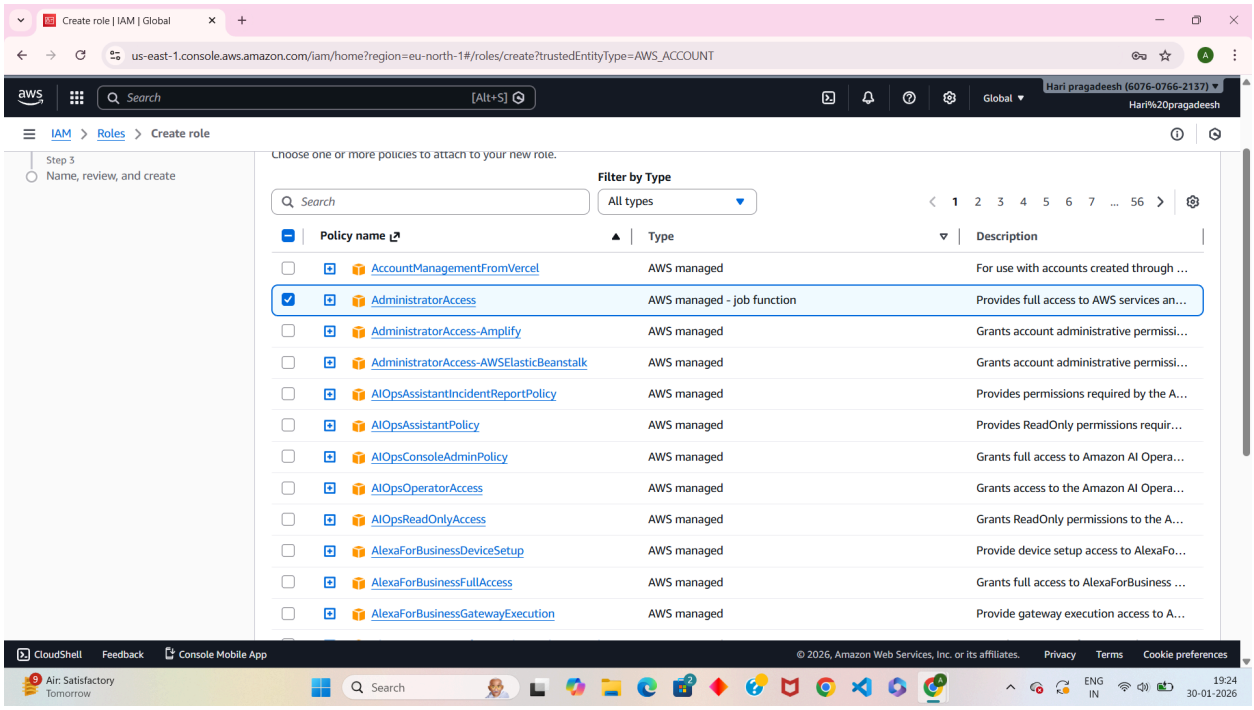
Indicates IAM user does not have required policies



- **IAM Roles section is opened**
- **3 existing roles are listed**
- **Roles are AWS service-linked roles**
- **Option available to Create a new role**



- **Creating a new IAM role**
- **AWS account selected as trusted entity**
- **This allows entities in the same account to assume the role**
- **Option to require MFA / External ID (not selected)**

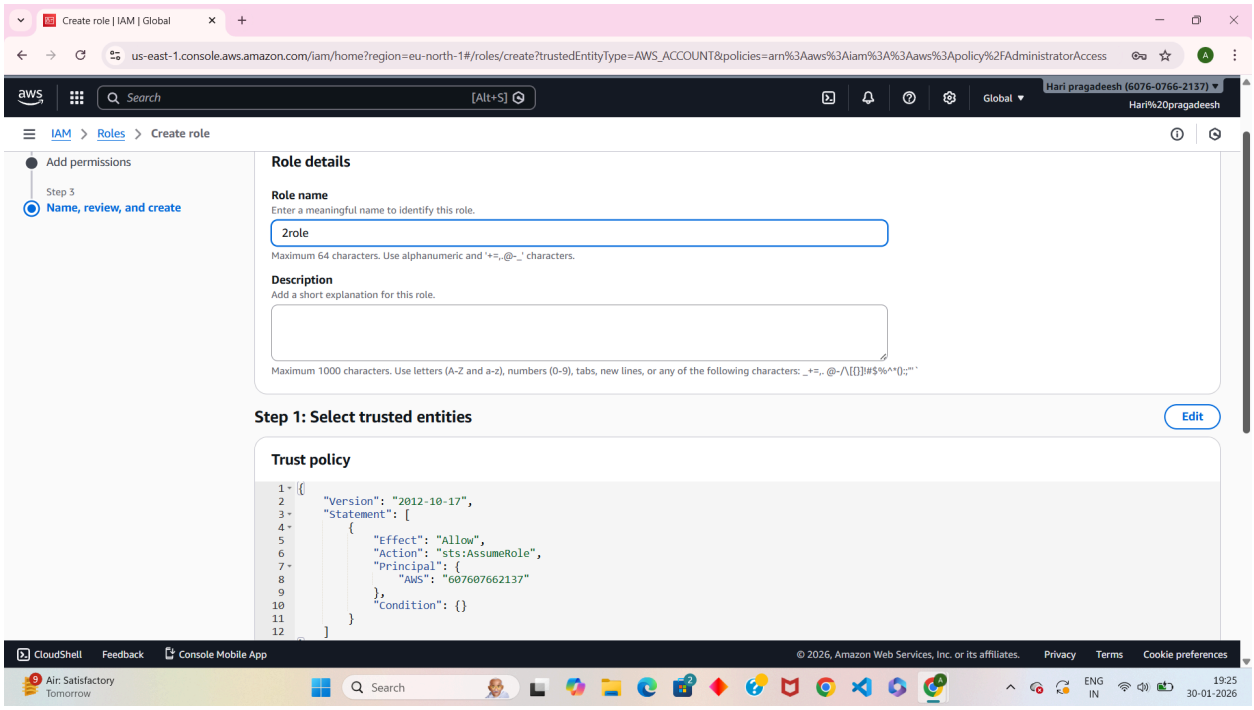


AdministratorAccess policy selected

This policy gives full access to AWS services

Policy type: AWS managed

Used to grant admin-level permissions to the role

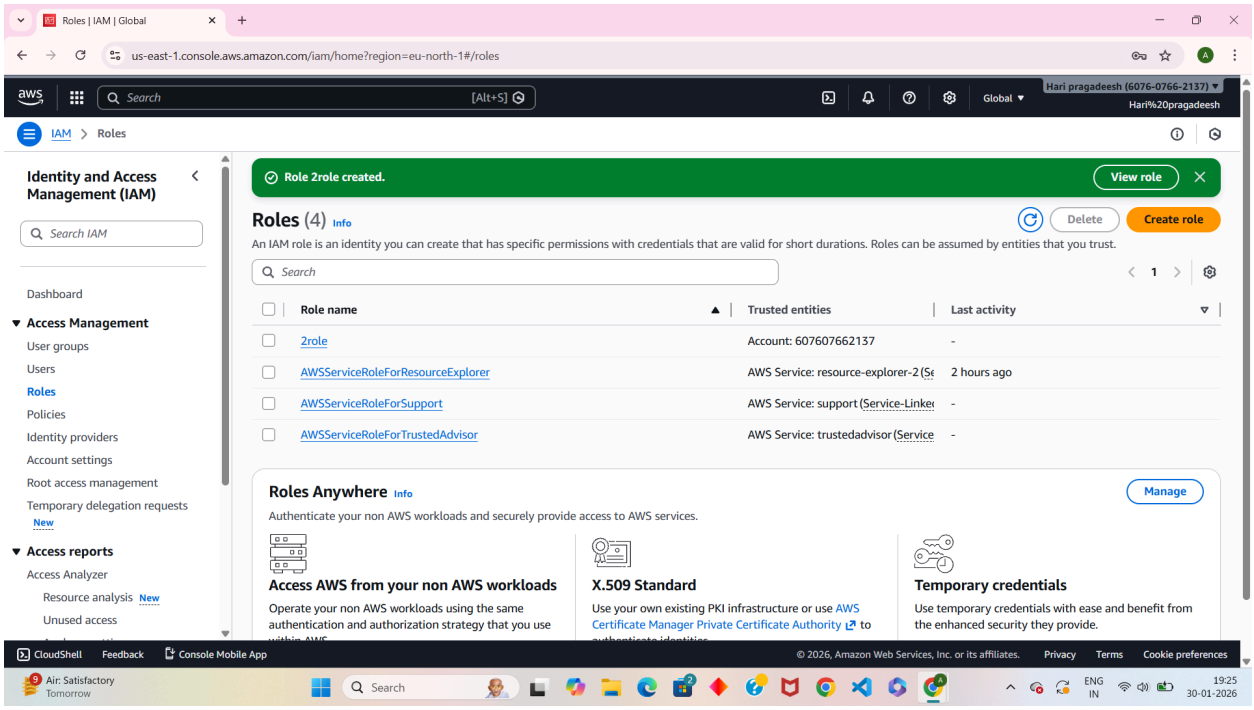


Role name entered: `2role`

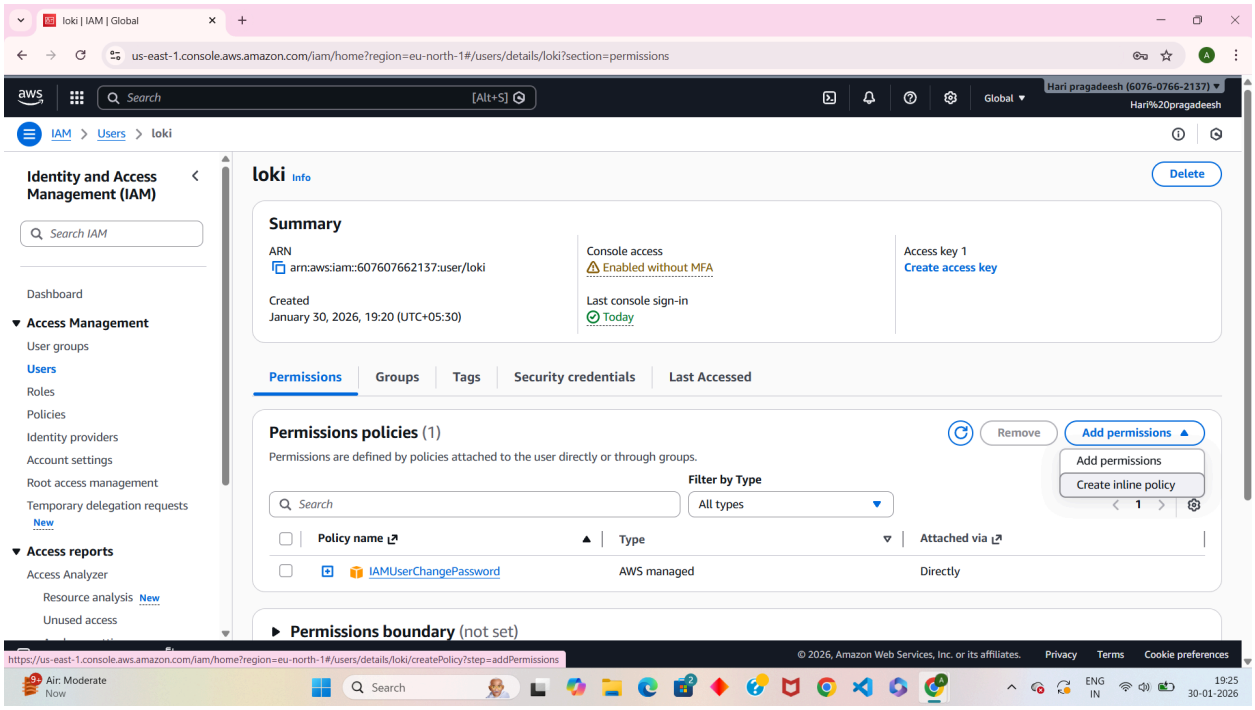
Trust policy shows this AWS account can assume the role

Role is being reviewed before creation

Shows STS AssumeRole permission in trust policy



- **Role “2role” created successfully**
- **Total roles increased from 3 to 4**
- **Trusted entity: AWS Account**
- **Role is now ready to be assumed**

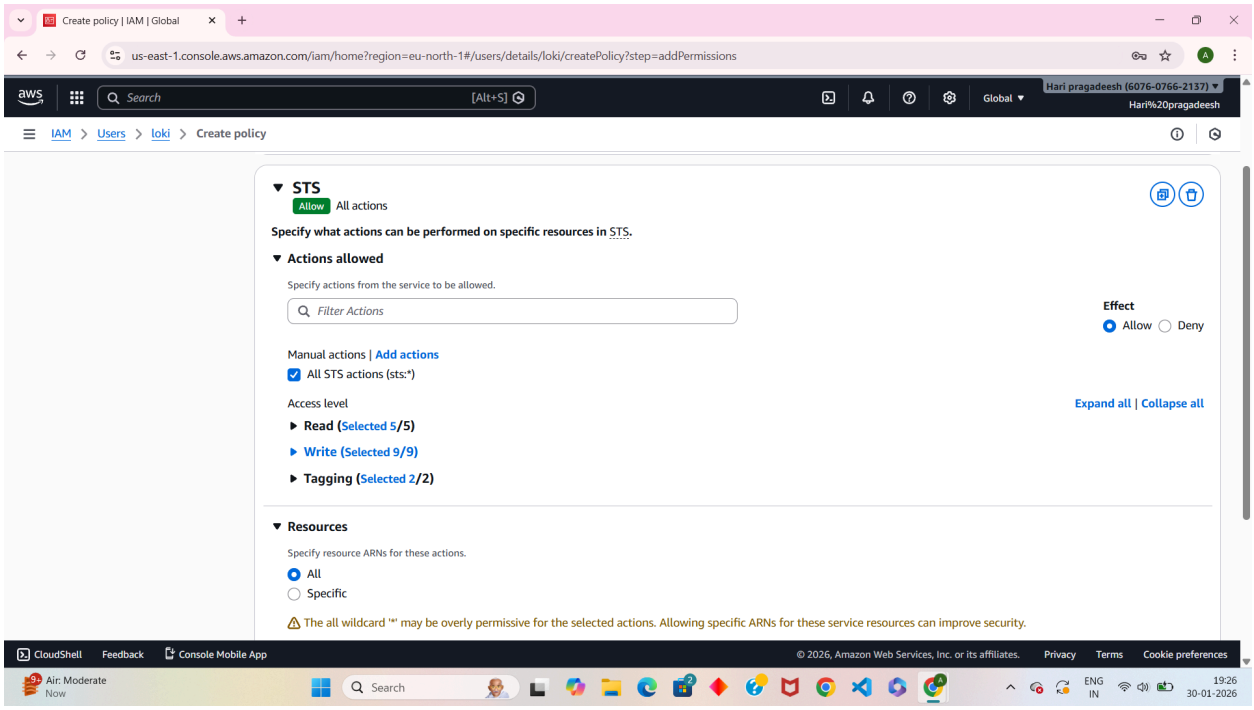


IAM user loki details displayed

Console access enabled without MFA

User currently has limited permissions

Only basic policy attached initially

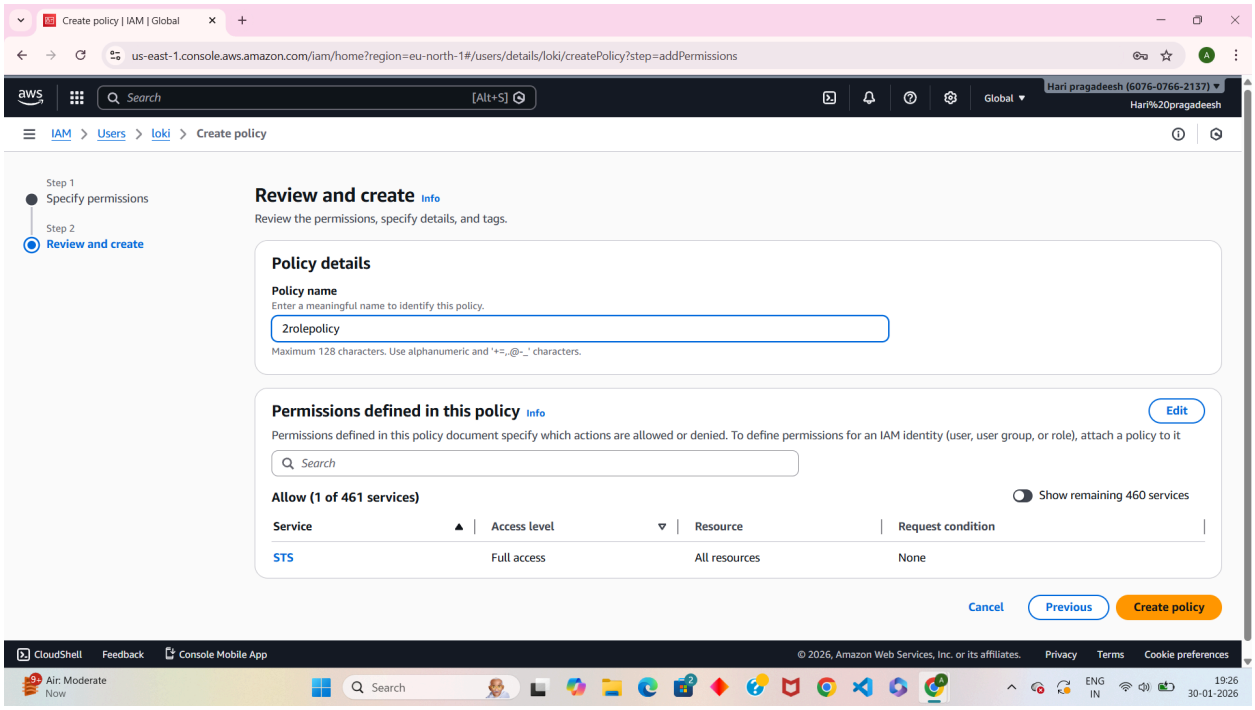


Creating a custom inline policy for user

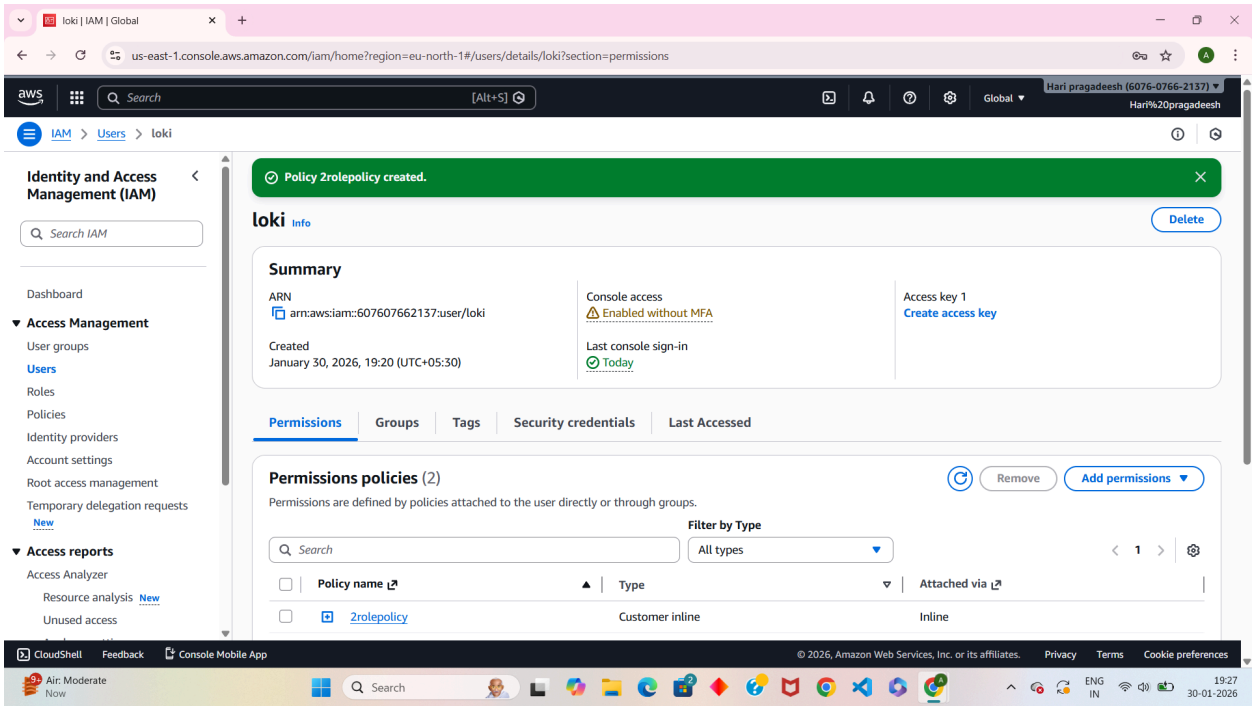
STS service selected

All STS actions (sts:*) allowed

Resources set to All



- **Policy name entered: `2rolepolicy`**
- **Policy allows full STS access**
- **This enables role assumption**
- **Ready to create the policy**

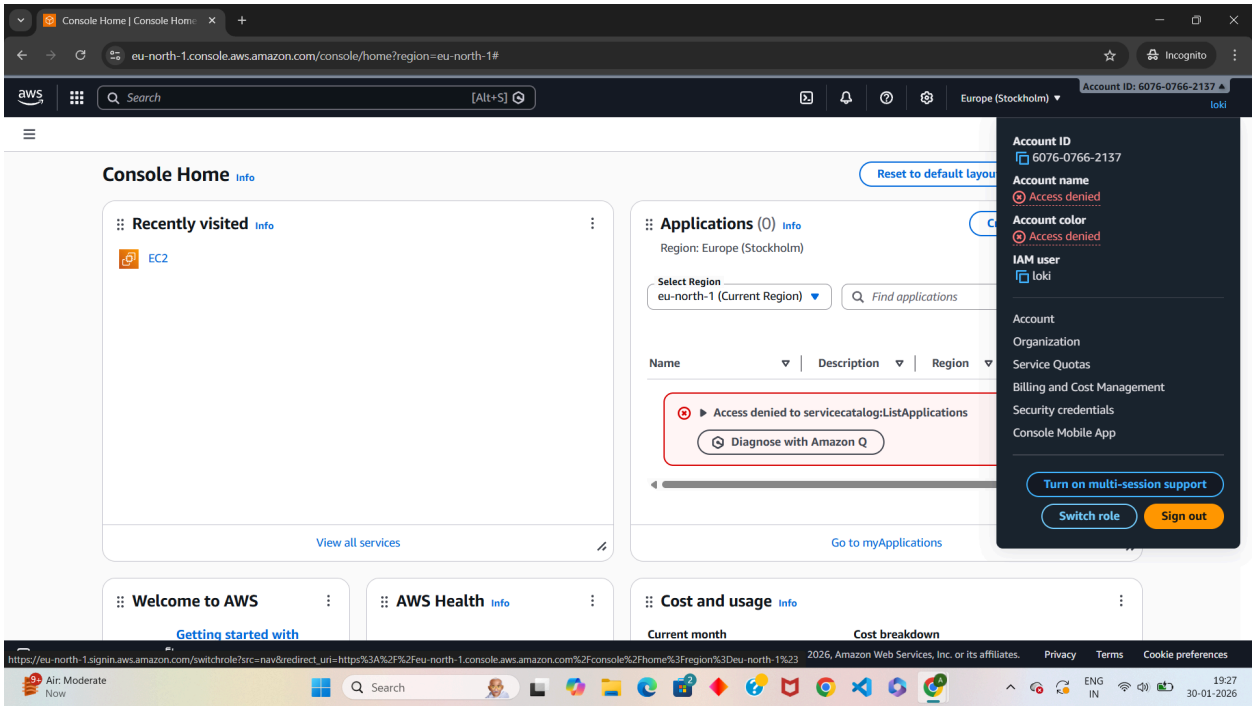


Policy 2rolepolicy created and attached

Policy type: Customer inline

User now has STS permissions

Used for Switch Role / Assume Role

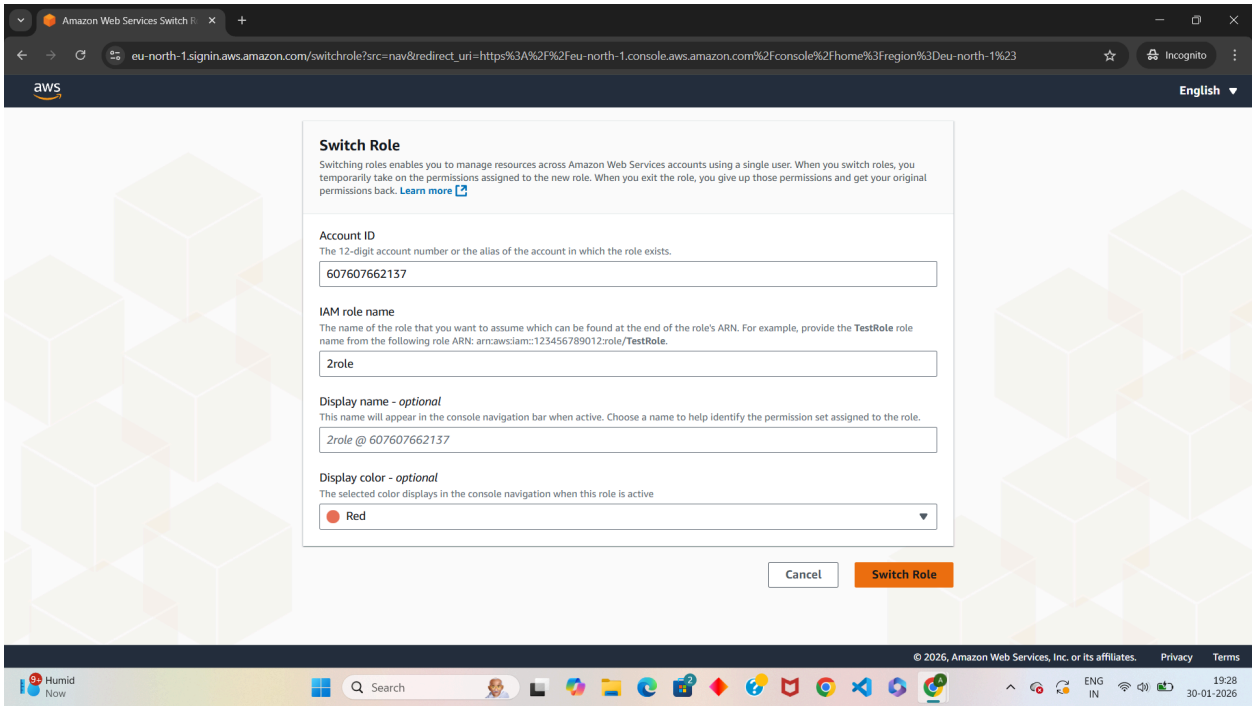


User loki logged in successfully

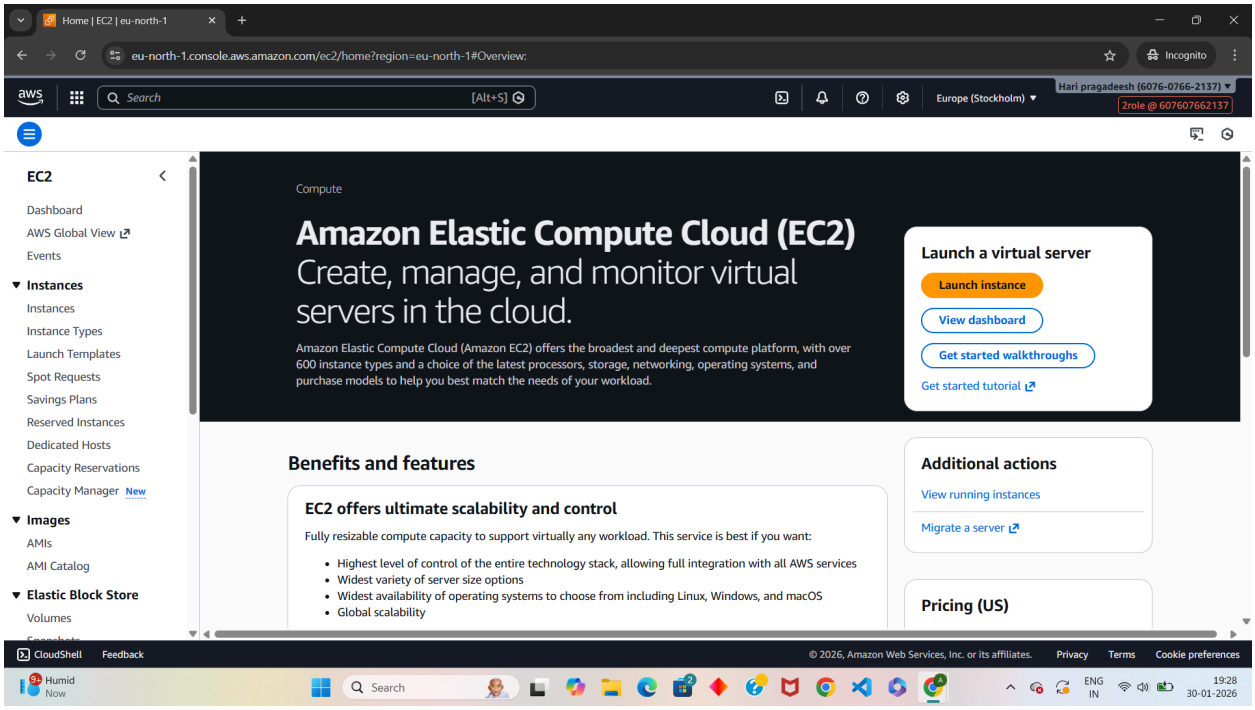
Region: Europe (Stockholm)

Still shows Access Denied for some services

Indicates user must switch to role to get admin access



- **Switch Role option is opened**
- **Account ID of the same AWS account is entered**
- **IAM role name `2role` is provided**
- **Display name and color selected for identification**
- **Used to assume the role temporarily**

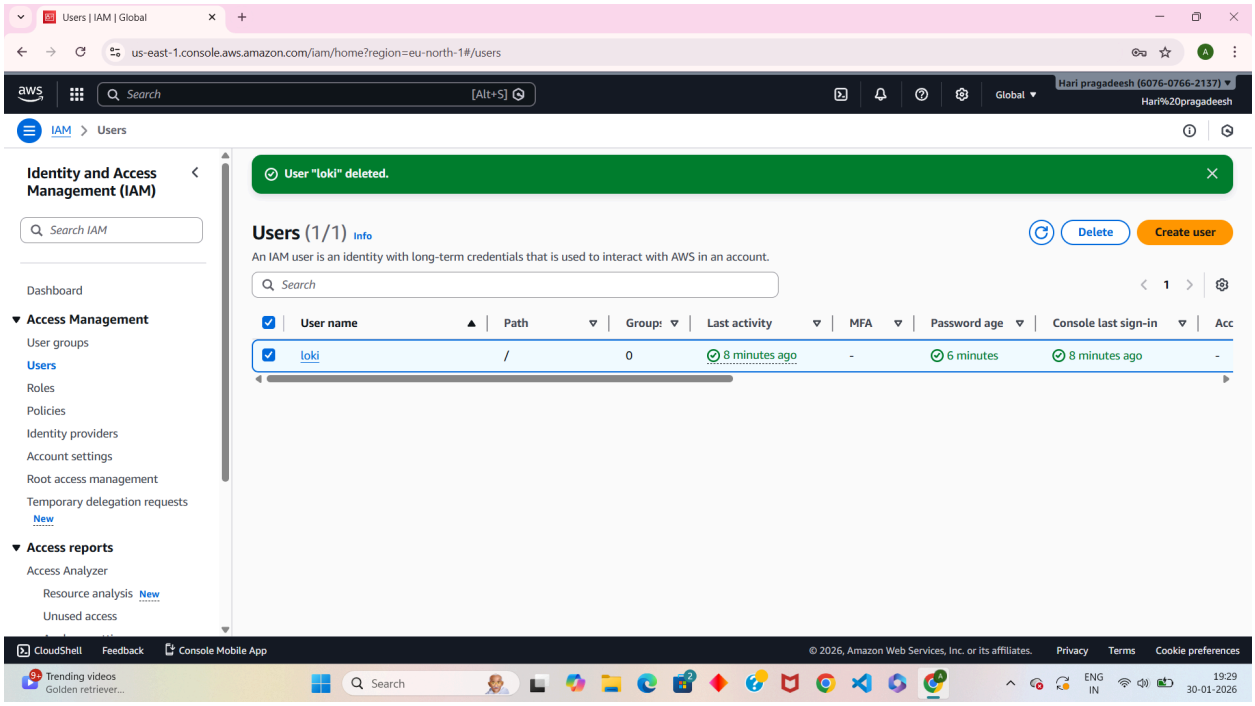


Role 2role is successfully assumed

EC2 service opens without access denied

AdministratorAccess permissions are active

User can now launch and manage EC2 instances

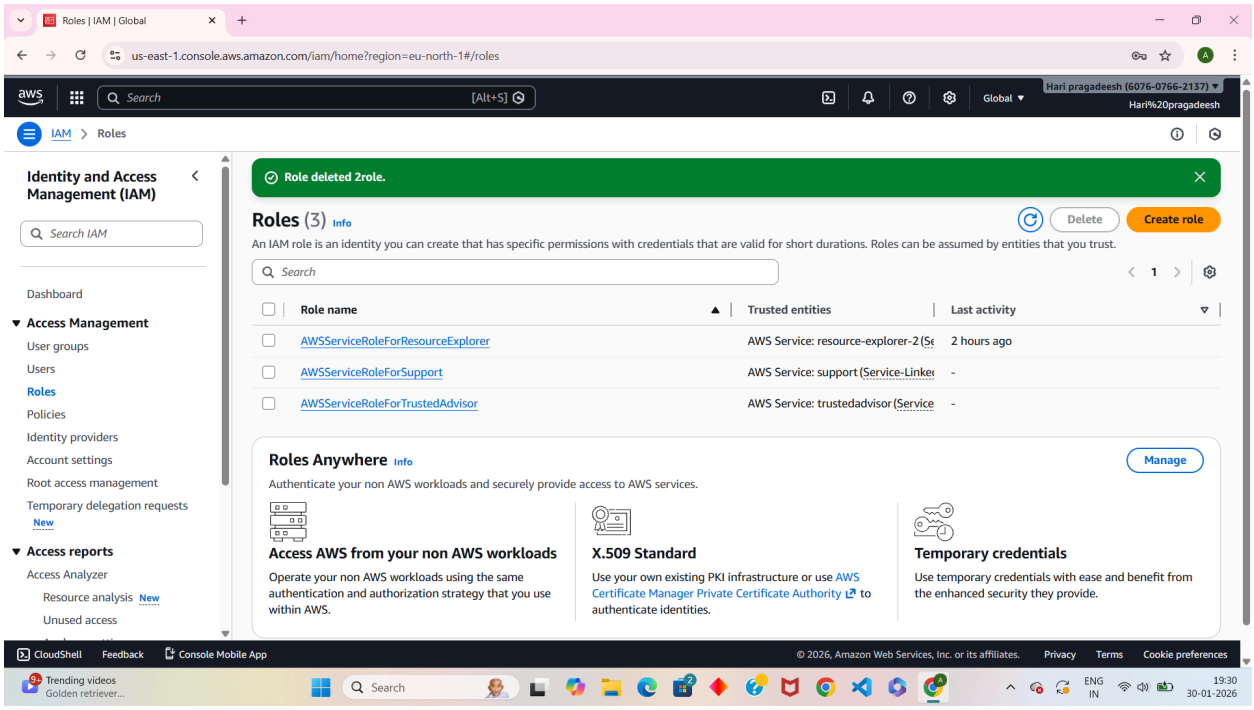


IAM user `loki` deleted successfully

Confirmation message displayed

Shows last activity and login time

User is no longer available for access



IAM role `2role` deleted

Roles count reduced back to 3

Only AWS service-linked roles remain

Cleanup of temporary role completed