 AWS IAM Lab

## What:

Identity and Access Management service to securely control access to AWS resources.

## How:

Create users, groups, roles, and policies to grant permissions based on the principle of least privilege.

## How Much:

Free to use; no additional costs for IAM.

# 🎯 Objective

- Create IAM users (instead of using the root account).  
- Apply least privilege policies.  
- Enable Multi-Factor Authentication (MFA).  
- Test access to verify permissions.

# 🖥 Step 1 — Log in as Root User (One Time)

1. Go to AWS Console (https://console.aws.amazon.com/).  
2. Log in using your root account credentials (email & password).  
⚠️ Important: Do not use the root user for daily tasks. This step is only to create your first admin.

# 👤 Step 2 — Create an IAM Admin User

1. In the AWS Console, search for IAM → Open it.  
2. Click Users → Add users.  
3. Enter a username: admin-user.  
4. Select AWS Management Console access.   
5. Create Password and Check 'Require password reset' for first login.  
6. Permissions → Attach existing policies directly → Select: AdministratorAccess (only for this admin user).  
7. Finish and download .csv file with login details.  
💡 This ensures you use the admin IAM user going forward, not the root account.

# 🧑‍💻 Step 3 — Create a New IAM User (Limited Access)

1. IAM → Users → Add users.  
2. Username: dev-user.  
3. Console access: (Optional, CLI only users don’t need this).  
4. Permissions → Create a new group called Developers.  
5. Attach policy: AmazonS3ReadOnlyAccess (example of least privilege).  
6. Complete user creation.  
  
💡 The dev-user now has read-only access to S3 buckets and cannot perform other actions.

# 🔒 Step 4 — Apply the Principle of Least Privilege

1. Go to Policies in IAM.  
2. Click Create policy → Choose JSON editor.  
3. Example custom policy (allows only listing S3 buckets):

**{  
 "Version": "2012-10-17",  
 "Statement": [  
 {  
 "Effect": "Allow",  
 "Action": [  
 "s3:ListAllMyBuckets",  
 "s3:GetBucketLocation"  
 ],  
 "Resource": "\*"  
 }  
 ]  
}**

4. Save policy as S3ListOnlyPolicy.  
5. Attach it to dev-user.  
  
💡 Always start with minimal permissions → add more if required.

# 🔑 Step 5 — Enable Multi-Factor Authentication (MFA)

1. IAM → Users → Select admin-user.  
2. Go to Security credentials → Assign MFA device.  
3. Choose Authenticator App (Google Authenticator or Authy).  
4. Scan QR code → Enter 2 codes from the app → Finish.  
5. MFA now protects your admin login.  
  
💡 Best practice: Always enable MFA for root user and admin accounts.

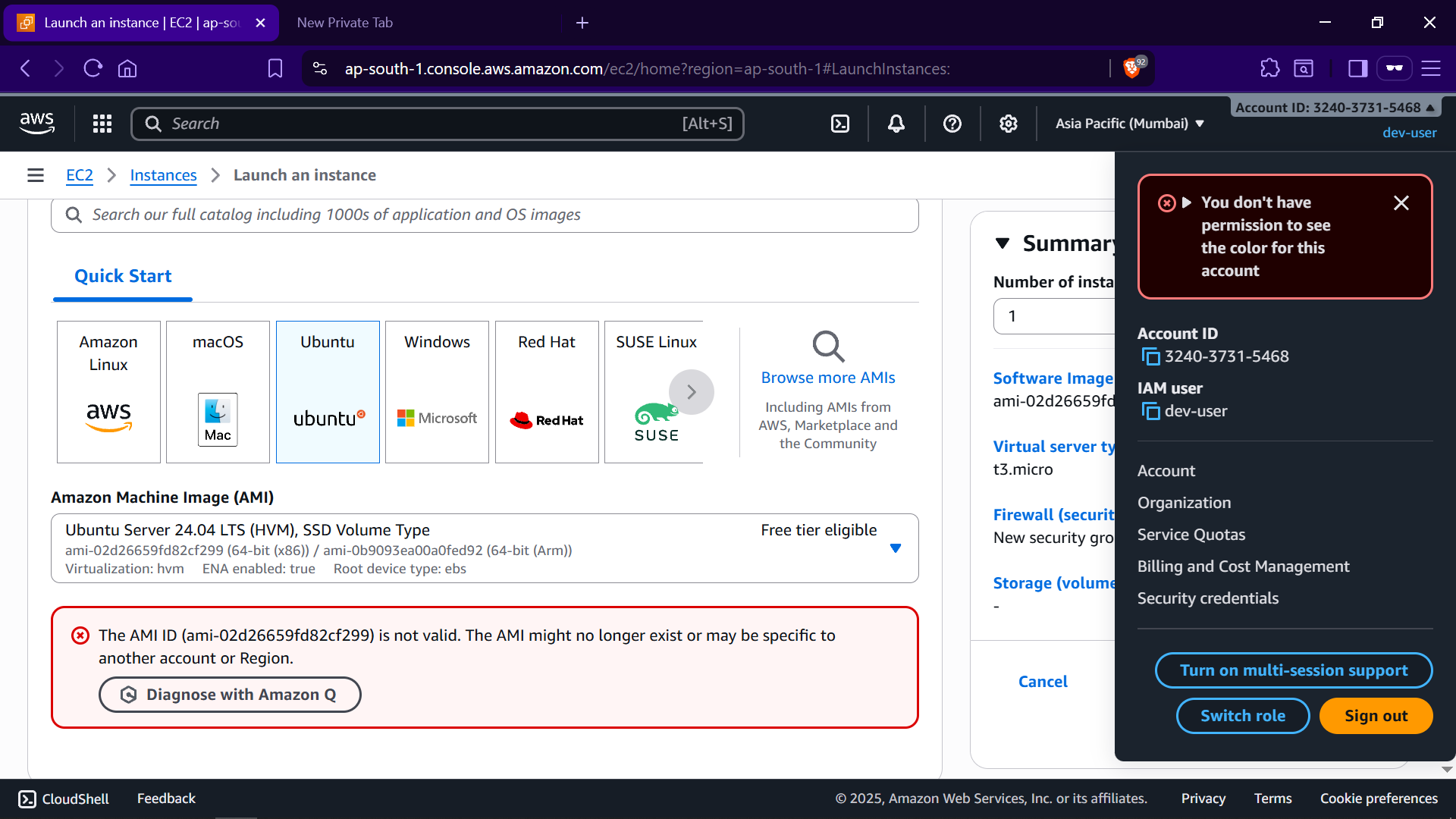
# 🧪 Step 6 — Test the Setup

- Log in as dev-user → Try accessing EC2 → Access Denied (expected).  
- Try listing S3 buckets → Works ✅.  
- Log in as admin-user → Full access with MFA prompt ✅.

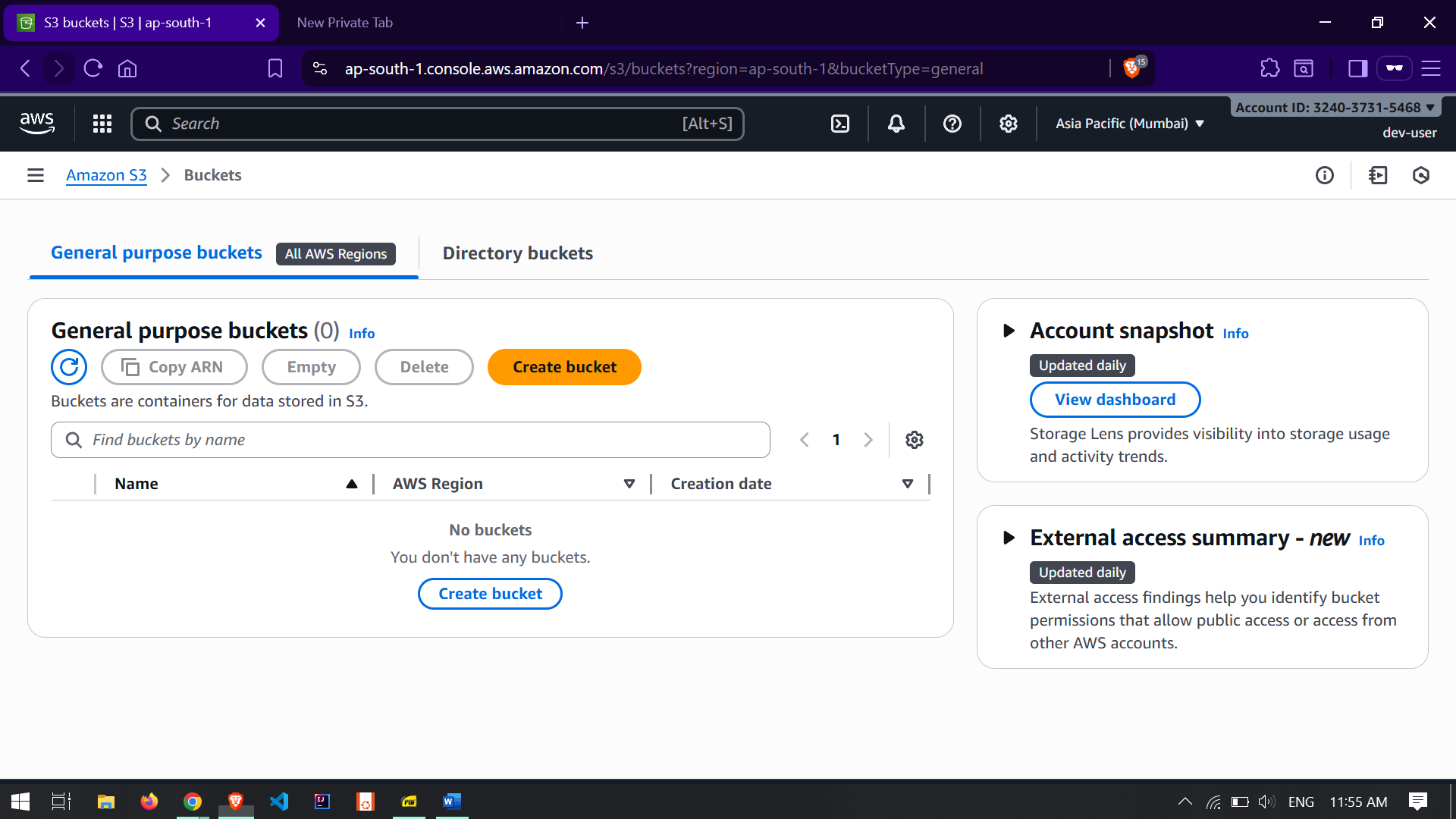
# 🧹 Step 7 — Cleanup (Optional)

If this was just practice:  
1. Delete test users/groups/policies.  
2. Keep only admin-user + MFA.

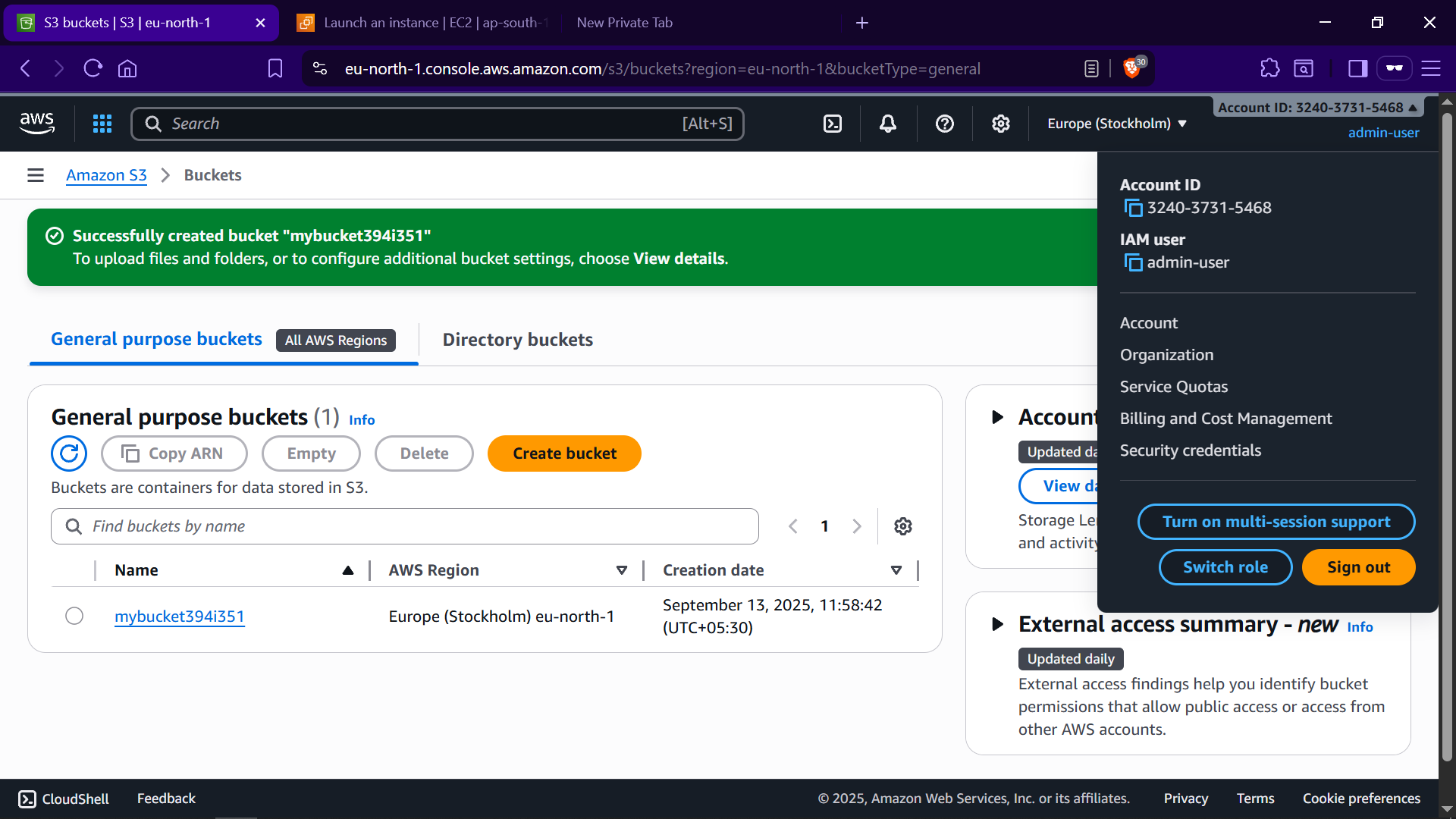
✅ Congratulations! You’ve completed your first AWS IAM Lab and secured your AWS environment using best practices.



**dev-user cannot create ec2 instance**



**dev-user can list S3 Buckets**



**admin-user has all permissions**

