

## # Lab: Creating a Multi-Account AWS Environment

### ## Objective

Use both the AWS Console and Terraform to:

- Create an Organization
- Add accounts
- Attach SCPs
- Set up IAM roles for cross-account access

### ## Part A: AWS Console Steps

1. Navigate to AWS Organizations
2. Create a new Organization
3. Add a new Organizational Unit (OU)
4. Invite an existing AWS account
5. Create and attach an SCP that denies S3 access

### ## Part B: Terraform Steps

1. Use `aws_organizations_organization` and `aws_organizations_account`
2. Attach SCP using `aws_organizations_policy_attachment`
3. Create cross-account IAM roles and trust policy

### ## Validation

- Verify SCP effects using policy simulator
- Use `sts:AssumeRole` to test cross-account access