
AWS Lab 38

AWS Organization

Overview of the lab

In this lab you will learn how aws organization works with organizational unit and service control policy

AWS Organization

It is an account management service through which you can consolidate multiple aws accounts into an organization for billing, logging and management

Account Types with Organization

- Management account (responsible for management and bills)

- Member account

OU (Organizational Unit)

- It is to group multiple account

- By default root ou will be there just after enabling organization

Service Control Policy

- It is used to manage manage OU or accounts with policy

Architecture



Step by Step Lab


(to practice aws organization, you need multiple aws accounts - minimum two)

Enable Organization (config in account1)

1. In account1 and in AWS Organizations click on [create an organization](#) (single-click setup) -
(account1 becomes the management account)

Invite Member accounts

2. Click on [Add an AWS account](#)
 - a. Select [invite an existing AWS account](#)

- 
- b. Email or account ID - **11122223333**
 3. Click on [Send invitation](#)
 4. Click on [Invitations](#) to view the status of Invitations

Accept the Invitation (account2)

5. In account2 in AWS Organizations click on [view 1 invitation](#)
 6. Click on [Accept invitation](#)
- (now account2 is member of account1)

Verify the accounts (account1) & Enable Service Control Policies

7. In account1 click on [AWS accounts](#)
8. Click on [Invitations](#) to view the status of Invitations
9. Click on [Policies](#) and Click on [Service control policies](#)
10. Click on [Enable service control policies](#)

(By default there will be a Full access policy - member account can do all activities)

11. Click on [Create policy](#)
 - a. [Policy name](#) - **deny-to-allow-only-t2**
 - b. Remove the sample policy / copy and paste the below policy

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "RequireMicroInstanceType",  
      "Effect": "Deny",
```

```

    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
      "StringNotEquals": {
        "ec2:InstanceType": "t2.micro"
      }
    }
  }
]
}

```

12. Click on [Create policy](#)

13. Select the **deny-to-allow-only-t2** policy and in Actions
Click on Attach policy and Select Root OU

14. Click on [Attach policy](#)

(applying to an OU will inherit the policy to nested OU and accounts within it)

Launch an EC2 m5.xlarge instance in account2 (will be denied because of SCP)

Clean Up Step

(account1)

1. Click on **AWS accounts** , Select the **account2** and in **Actions**
click on **Remove from organization** and **Remove**
2. Click on **Settings** and Click **Delete Organization** and **Delete**