AWS Multi Account Architecture & Deployment

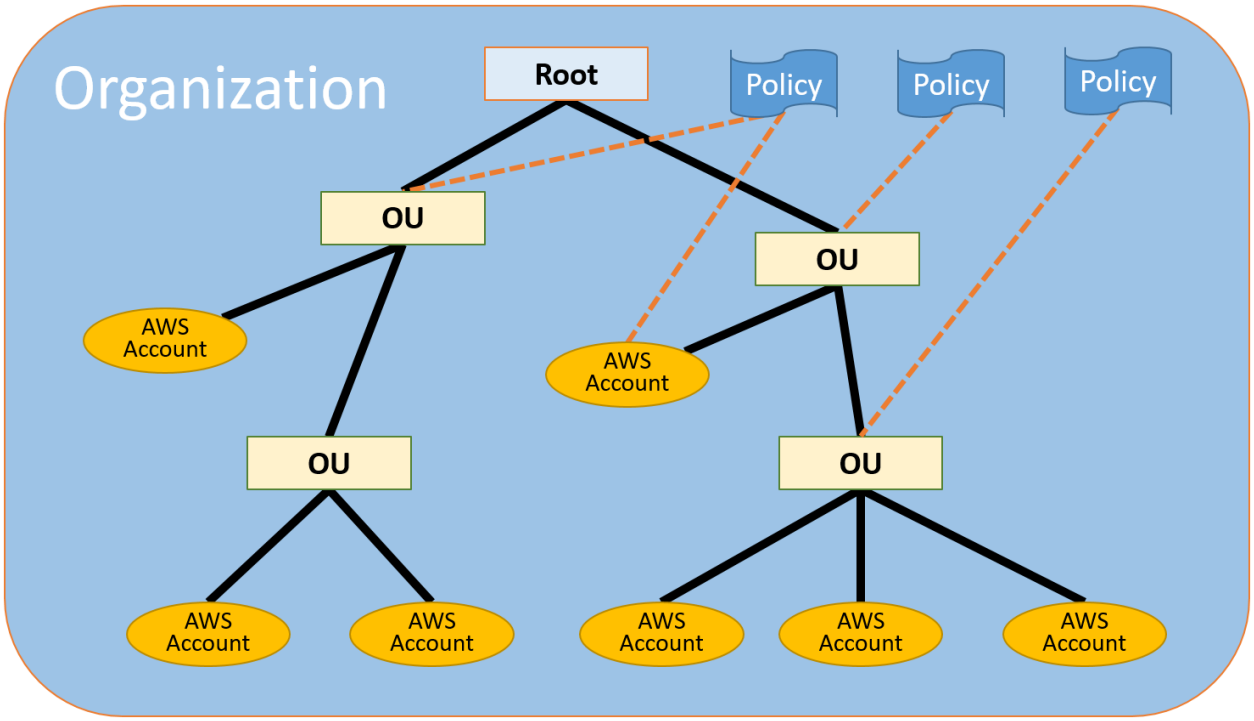
What is AWS Organization ?

AWS Organizations is an account management service that enables you to consolidate multiple AWS accounts into an *organization* that you create and centrally manage. AWS Organizations includes account management and consolidated billing capabilities that enable you to better meet the budgetary, security, and compliance needs of your business.

AWS Organization Pricing :

AWS Organizations is offered at no additional charge. You are charged only for AWS resources that users and roles in your member accounts use

AWS Organization Architecture :



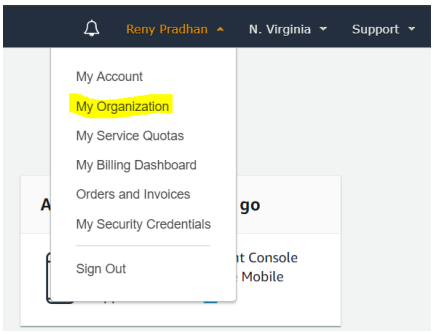
AWS Organization Limits :

1. 4 is the default maximum number of accounts allowed in an organization. *If you need to increase your limit, contact AWS Support.*
2. Five levels of OUs deep under a root in Nested way.

Ref Link : https://docs.aws.amazon.com/organizations/latest/userguide/orgs_reference_limits.html

How to Create an Organization ?

1. Login to AWS Master Account -> Click on Account Name beside Bell Icon -> Click on My Organization



2. On the introduction page, choose **Create organization** -> In the **Create organization** confirmation dialog box, choose **Create organization**
3. The organization is created. You're now on the **Accounts** tab. The star next to the account email indicates that it's the master account.
4. A verification email is automatically sent to the address that is associated with your master account, open the email and click on the link to confirm.

Invite an Existing Account to Join the Organization :

1. Login to the master account and on the **Accounts** tab, choose **Add account** and then choose **Invite account.**
2. In the **Account ID or email** box, enter the email address of the owner of the account that you want to invite.
3. Choose **Invite**. AWS Organizations sends the invitation to the account owner.
4. Open the email that AWS sent from the master account and choose the link to accept the invitation. When prompted to sign in, do so as an administrator in the invited member account.

Create a New Child Account Under Organization :

1. Login to the master account and on the **Accounts** tab, choose **Add account** and then choose **Add account**.
2. For **Full name**, enter a name for the account, such as **Production Account.**
3. For **Email**, enter the email address of the individual who is to receive communications on behalf of the account. This value must be globally unique, multiple accounts can not be created using a single Email ID.
4. For **IAM role name**, you can leave this blank to automatically use the default role name of **OrganizationAccountAccessRole**. This role enables you to access the new member account when signed in as an IAM user in the master account.
5. Choose **Create.** Now you will have a child/member account under your master account.

How to Create an Organizational Unit (OU) :

1. On the AWS Organizations console, choose the **Organize Accounts** tab and then choose **+ New organizational unit.**
2. For the name of the OU, enter **Production** and then choose **Create organizational unit**.
3. Choose your new **Production** OU to navigate into it and then choose **+ New organizational unit**.
4. For the name of the second OU, enter **RnD-OU** and then choose **Create organizational unit**. Now you can move your member accounts into these OUs.
5. In the tree view on the left, choose the **Root**.
6. Select the first member account, 222222222222, and then choose **Move**.
7. In the **Move accounts** dialog box, choose **Production** and then choose **Move**.
8. Select the second member account, 333333333333, and then choose **Move**.
9. In the **Move accounts** dialog box, choose **Production** to expose **RnD-OU**. Choose **RnD-OU** and then choose **Move**.

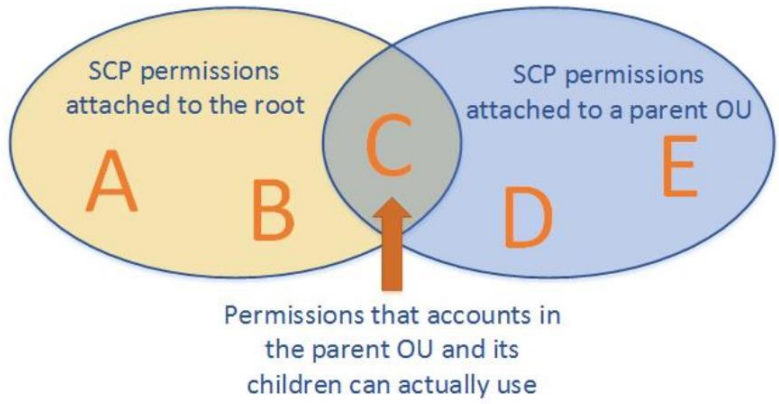
What is Service Control Policies (SCP) :

Service control policies (SCPs) are similar to IAM permission policies and use almost the same syntax. However, an SCP never grants permissions. Instead, SCPs are JSON policies that specify the maximum permissions for an organization or organizational unit (OU).

1. Every user including Root user in the account can perform only the allowed activities by SCPs.
2. SCPs ***do not*** affect any service-linked role. Service-linked roles enable other AWS services to integrate with AWS Organizations and can't be restricted by SCPs.
3. Users and roles must still be granted permissions with appropriate IAM permission policies. A user without any IAM permission policies has no access at all, even if the applicable SCPs allow all services and all actions.
4. Any account has only those permissions permitted by ***every*** parent above it.

How SCPs Work ?

The following illustration shows how SCPs work.



In this illustration, the root has an SCP attached that allows permissions A, B, and C. An OU in that root has an SCP that allows C, D, and E. Because the root's OU doesn't allow D or E, nothing in the root or any of its children can use them, including the parent OU. Even though the parent OU explicitly allows them, they end up blocked because they're blocked by the root. Also, because the OU's SCP doesn't allow A or B, those permissions are blocked for the parent OU and any of its children. However, other OUs under the root that are peers to the parent OU could allow A and B.

Creating Service Control Policies (SCPs) :

create three service control policies (SCPs) and attach them to the root and to the OUs to restrict what users in the organization's accounts can do. The first SCP prevents anyone in any of the member accounts from creating or modifying any AWS CloudTrail logs that you configure.

1. **Create the First SCP That Blocks CloudTrail Configuration Actions :**
   I. Choose the **Policies** tab and then choose **Create policy** from the Organization Console.
   II. For **Policy name**, enter **Block CloudTrail Configuration Actions**.
   III. In the **Policy** section on the left, select CloudTrail for the service. Then choose the following
   actions: **AddTags**, **CreateTrail**, **DeleteTrail**, **RemoveTags**, **StartLogging**, **StopLogging**, and **UpdateTrail**.
   IV. Still in the left pane, choose **Add resource** and specify **CloudTrail** and **All Resources**. Then choose**Add resource**.
   V. Choose **Create policy**
   VI. The policy statement on the right updates to look similar to the following.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1234567890123",
      "Effect": "Deny",
```

```
      "Action": [
        "cloudtrail:AddTags",
        "cloudtrail:CreateTrail",
        "cloudtrail:DeleteTrail",
        "cloudtrail:RemoveTags",
        "cloudtrail:StartLogging",
        "cloudtrail:StopLogging",
        "cloudtrail:UpdateTrail"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

2. Create the Second Policy that Allows Approved Services for the Production OU :

I. From the list of policies, choose **Create policy**.

II. For **Policy name**, enter **Allow List for All Approved Services**.

III. Position your cursor in the right pane of the **Policy** section and paste in a policy like the following.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1111111111111",
      "Effect": "Allow",
      "Action": [
        "ec2:*",
        "elasticloadbalancing:*",
        "codecommit:*",
        "cloudtrail:*",
        "codedeploy:*"
       ],
      "Resource": [ "*" ]
    }
  ]
}
```

IV. Choose **Create policy**.

3. **Create the Third Policy that Denies Access to Services that Can't be Used in The RnD-OU :**
    I. From the **Policies** tab, choose **Create policy**.
    II. For **Policy name**, enter **Deny List for MainApp Prohibited Services**.
    III. In the **Policy** section on the left, select **Amazon DynamoDB** for the service. For the action, choose **All actions**.
    IV. Still in the left pane, choose **Add resource** and specify **DynamoDB** and **All Resources**. Then choose **Add resource**.
    V. The policy statement on the right updates to look similar to the following

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Deny",
   "Action": [ "dynamodb:*" ],
   "Resource": [ "*" ]
  }
 ]
}
```

    VI. Choose **Create policy** to save the SCP.

Enable SCPs for your Root :

Before you can attach a policy of any type to a root or to any OU within a root, you must enable the policy type for that root.

1. On the **Organize accounts** tab, choose your root.
2. In the **Details** pane on the right, under **ENABLE/DISABLE POLICY TYPES** and next to **Service control policies**, choose **Enable**.

Attach SCPs to the OUs :

1. On the **Organize accounts** tab, in the **Details** pane on the right, under **POLICIES**, choose **SERVICE CONTROL POLICIES**.
2. Choose **Attach** next to the SCP named Block CloudTrail Configuration Actions to prevent anyone from altering the way that you configured CloudTrail. In this tutorial, you attach it to the root so that it affects all member accounts.
3. Choose the **Production** OU (not the check box) to navigate to its contents.

4. Under **POLICIES**, choose **SERVICE CONTROL POLICIES** and then choose **Attach** next to Allow List for All Approved Services to enable users or roles in member accounts in the Production OU to access the approved services.
5. To remove the default policy from the Production OU, next to **FullAWSAccess**, choose **Detach**. After you remove this default policy, all member accounts under the root immediately lose access to all actions and services that are not on the allow list SCP that you attached in the preceding step.
6. Now you can attach the SCP named Deny List for **RnD-OU** Prohibited services to prevent anyone in the accounts in the **RnD-OU** from using any of the restricted services. choose the **RnD-OU** (not the check box) to navigate to its contents.
7. In the **Details** pane, under **POLICIES**, expand the **Service control policies** section. In the list of available policies, next to **Deny List for RnD-OU Prohibited Services**, choose **Attach**.

Test Cases :

1. If you sign in as a user in the master account, you can perform any operation that is allowed by your IAM permissions policies.
2. If you sign in as the root user or an IAM user in account 222222222222, you can perform any actions that are allowed by the allow list. Denies any attempt to perform one of the CloudTrail configuration actions.
3. If you sign in as a user in account 333333333333, you can perform any actions that are allowed by the allow list and not blocked by the deny list. Denies any attempt to perform one of the CloudTrail configuration actions.

SCP :

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_inheritance_auth.html

boomterbm@gmail.com

OrganizationAccountAccessRole