Module 10: Organizations Assignment

Tasks To Be Performed:

1. Create an AWS Organization.
2. Create 3 organization units – OU1, OU2 and OU3.
3. Attach a service control policy that only allows access to EC2.

Solution

AWS Organization is a tool that lets us centrally manage multiple AWS accounts added to our 'Organization'. If we are the Administrators of the organization, then we can invite the existing AWS accounts to join organizations or we can create accounts in the organization directly.

Suppose you have a company operating in multiple fields, but now you created AWS accounts for each of them like you have a company in the IT fields at different locations or in the Instruments fields at different locations, and you have different AWS accounts for them in order to manage their product that is producing, but if you thought that manage these things centrally, then AWS Organization is very helpful.

As an administrator, you can add multiple accounts to your AWS account and those will be your child accounts and you can manage them. AWS Organization is used to manage multiple AWS accounts from one administrator account.

Features of AWS Organization

- Centralized management.
- Consolidated billing for all member accounts, means there will be only one bill generated for all the accounts.
- Control over the account's usage of services or APIs, we can manage the control of what APIs or services they are going to use.
- Integration with AWS IAM.
- Consistent data replication, eventually means whatever data is given to the administrator you can share it with all the children at a single go.
- Standardized tags across accounts, you can manage the accounts by giving tags so that you can be recognized which tag is available for which accounts which will make it easier to perform functions with them.

Pricing of AWS Organization- There are no additional charges for AWS Organization. The charges apply to only the usage of other AWS resources by all member accounts.

AWS Organization Quotas

Maximum and Minimum Values

- Number of roots in an organization= 1
- Number of Organizational Units (OUs) in an organization- 1000(child accounts).
- Number of policies in an organization= 1000
- OUs maximum nesting in a root= 5 (Nesting means I have created one and that child again created one like that)
- Number of member accounts that can be created concurrently= 5, so if I have to create members account concurrently which means side by side, at the same time in that case we can add 5 accounts at the same time but the maximum limit is 1000.

Expiration time for handshakes

- Invitation to join an organization= 15 days.
- Request to enable all features in an organization= 90 days.
- Handshake is deleted and no longer appears in lists= 30 days.

How does AWS IAM work with Organizations?

Suppose, I have to create a group of AWS accounts and attach services to them like Service control policies to them, so that's where our IAM comes into place. We can write the policies with the help of AWS IAM for our Organizations and entities which are available to our AWS account, they can use only the IAM role/policy that we have written for them.

AWS Organization concepts

Organization- Organizations can be used to consolidate multiple AWS accounts so that we can administer them all as a single unit. An organization will have one master account and zero or more member accounts. We can organize our organization in hierarchical order with a root on the top.

Root- This is the master account for all subaccounts. If we apply a policy to the root, it will be applied to all the member accounts and organization units. We can have only one root and that will be automatically created when we create an organization.

Organization Unit(OU)- A container for accounts within a root. An OU can contain other Ous and this is what enables the tree-like hierarchy that ends in accounts. If we attach a policy to an OU, this affects all the other Ous under it, as well as the member account.

Account- An account is basically an AWS account that contains AWS resources. We can apply policies to the account only to control that account's resources. A master account creates the organization and we can administer using it. All other accounts are member accounts, they can be part of only one organization.

Invitation- This is the process of asking another AWS account to join our organization, only a master account can send out an invite. If they accept, they become members.

Handshake- Handshake is a multi-step process of sharing information between two accounts/ parties. Handshakes are used to send out invitations and get back acknowledgment. We can work with handshakes directly if we are working with the organization’s API or AWS CLI tools.

Steps for the creation of organization

- Open the AWS Management console, and then choose your account name from the navigation bar.
- Choose my organization.
- Choose Create organization.
- Choose to enable all features or enable only consolidated billing.
- Choose Create.

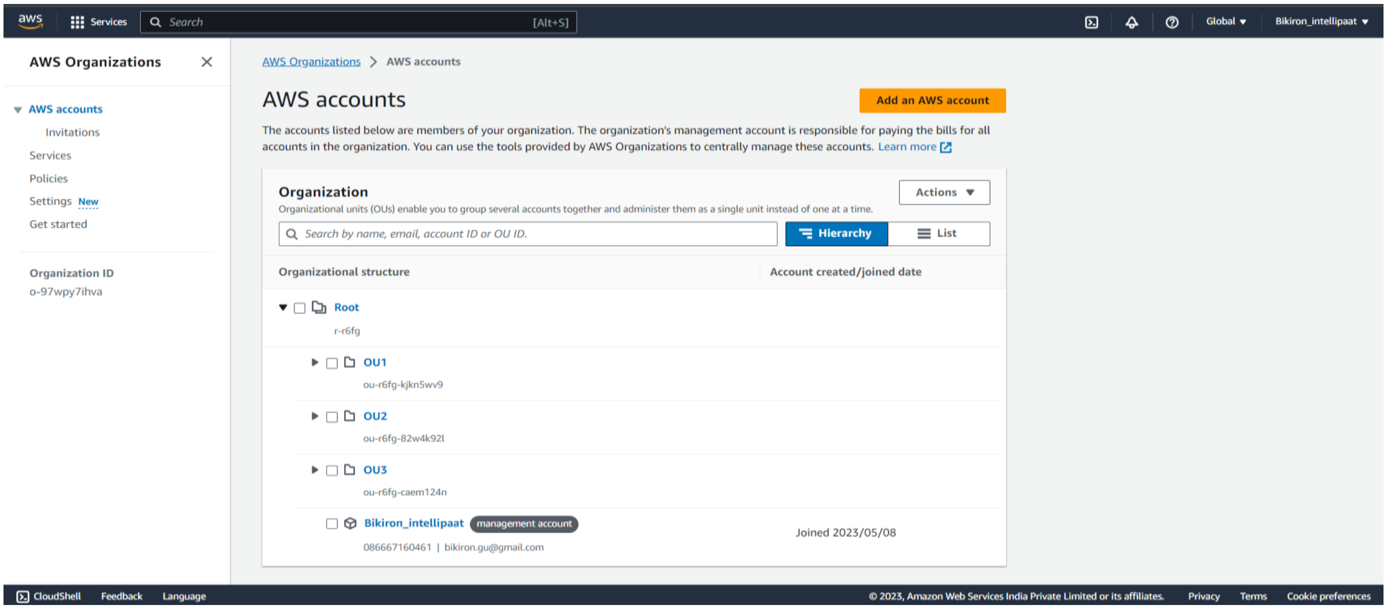
Steps for the Creation of Organizational Unit(OU)

- Open the AWS Management Console, click on the account name select organization.
- Choose the Root, go to action→ Click on create new→Put the Name→ Create OU

Steps for the creation of a Service control policy(SCP)

- Before going to create SCP, we have to first ‘enable’ the SCP, for that click on Organization→Policies→Choose SCP→ Enabling SCP.
- After enabling SCP, click on create policy→ give the policy name →Add action→ Add resource→ Create policy

RESULTS



Organization ID
o-97wpy7ihva

AWS accounts

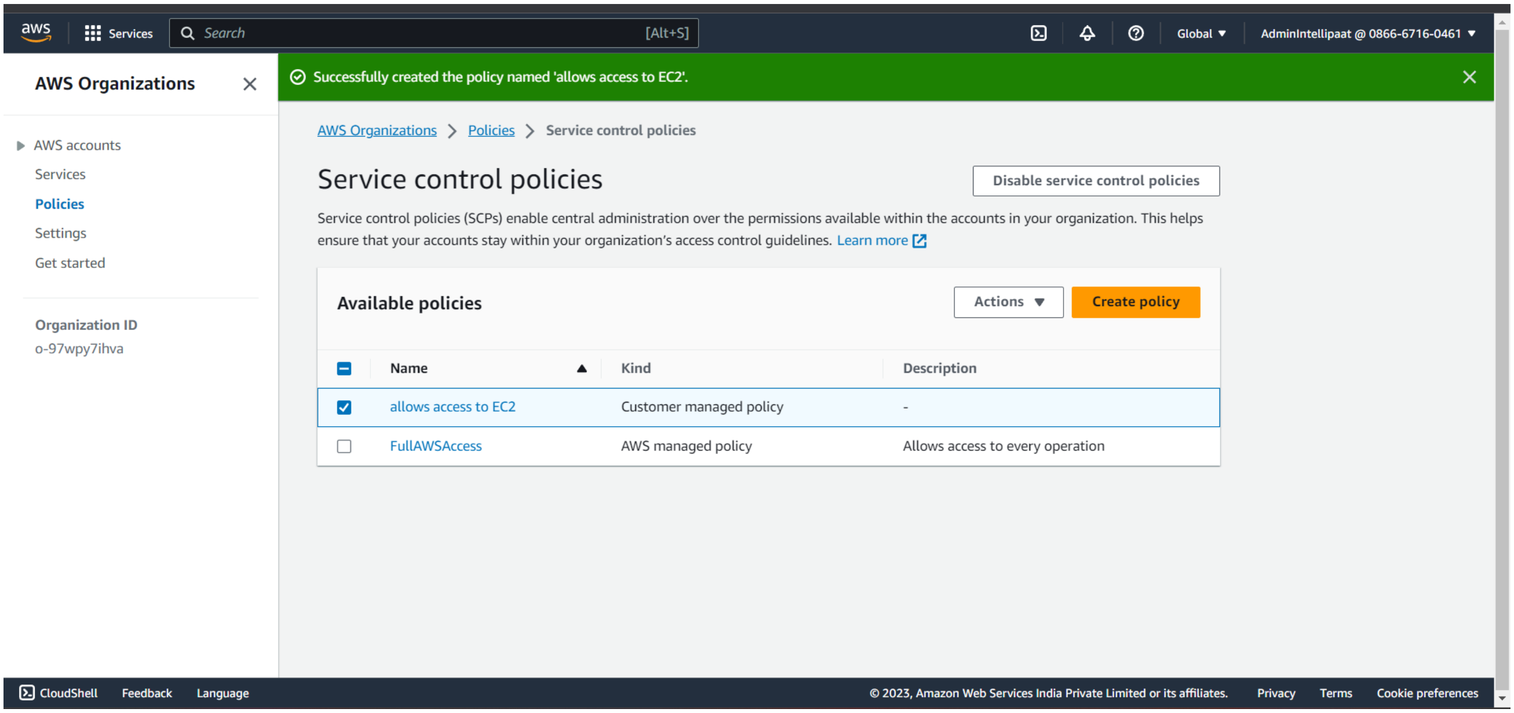
The accounts listed below are members of your organization. The organization's management account is responsible for paying the bills for all accounts in the organization. You can use the tools provided by AWS Organizations to centrally manage these accounts. Learn more

Organization

Organizational units (OUs) enable you to group several accounts together and administer them as a single unit instead of one at a time.

Search by name, email, account ID or OU ID.

Organizational structure	Account created/joined date
Root r-r6fg	
OU1 ou-r6fg-kjkn5wv9	
OU2 ou-r6fg-82w4k92l	
OU3 ou-r6fg-caem124n	
Bikiron_intellipaat management account 086667160461 | bikiron.gu@gmail.com	Joined 2023/05/08



Organization ID
o-97wpy7ihva

Successfully created the policy named 'allows access to EC2'.

AWS Organizations > Policies > Service control policies

Service control policies

Service control policies (SCPs) enable central administration over the permissions available within the accounts in your organization. This helps ensure that your accounts stay within your organization's access control guidelines. Learn more

Available policies

☐	Name	Kind	Description
☑	allows access to EC2	Customer managed policy	-
☐	FullAWSAccess	AWS managed policy	Allows access to every operation

© 2023, Amazon Web Services India Private Limited or its affiliates.