AWS Organizations

AWS Organizations

- AWS Organizations helps you centrally govern your environment as you grow and scale your workloads on AWS. Whether you are a growing startup or a large enterprise, Organizations helps you to centrally manage billing; control access, compliance, and security; and share resources across your AWS accounts.

- Using AWS Organizations, you can automate account creation, create groups of accounts to reflect your business needs, and apply policies for these groups for governance. You can also simplify billing by setting up a single payment method for all of your AWS accounts.

Benefits of AWS Organizations

- Centrally manage policies across multiple aws accounts

- Govern access to aws services, resources, and regions

- Automate aws account creation and management

- Configure aws services across multiple accounts

- Consolidate billing across multiple aws accounts

Organizational Units (OU)

- You can use organizational units (OUs) to group accounts together to administer as a single unit. This greatly simplifies the management of your accounts.

- For example, you can attach a policy-based control to an OU, and all accounts within the OU automatically inherit the policy.

- You can create multiple OUs within a single organization, and you can create OUs within other OUs.

- Each OU can contain multiple accounts, and you can move accounts from one OU to another. However, OU names must be unique within a parent OU or root.

Consolidated Billing

- You can use the consolidated billing feature in AWS Organizations to consolidate billing and payment for multiple AWS accounts. Every organization in AWS Organizations has a *master (payer) account* that pays the charges of all the *member (linked) accounts*

- **One bill** – You get one bill for multiple accounts.

- **Easy tracking** – You can track the charges across multiple accounts and download the combined cost and usage data.

- **Combined usage** – You can combine the usage across all accounts in the organization to share the volume pricing discounts, Reserved Instance discounts, and Savings Plans. This can result in a lower charge for your project, department, or company than with individual standalone accounts.

- **No extra fee** – Consolidated billing is offered at no additional cost.

Consolidated Billing

- Reserved Instances : For billing purposes, the consolidated billing feature of AWS Organizations treats all the accounts in the organization as one account. This means that all accounts in the organization can receive the hourly cost benefit of Reserved Instances that are purchased by any other account.

- Eg : For an Amazon EC2 Reserved Instances example, suppose that Bob and Susan each have an account in an organization. Susan has five Reserved Instances of the same type, and Bob has none. During one particular hour, Susan uses three instances and Bob uses six, for a total of nine instances on the organization's consolidated bill. AWS bills five instances as Reserved Instances, and the remaining four instances as regular instances.

- Bob receives the cost benefit from Susan's Reserved Instances only if he launches his instances in the same Availability Zone where Susan purchased her Reserved Instances.

Service Control Policies

- Service control policies (SCPs) are one type of policy that you can use to manage your organization. SCPs offer central control over the maximum available permissions for all accounts in your organization, allowing you to ensure your accounts stay within your organization's access control guidelines. SCPs are available only in an organization that has all features enabled.

- Attaching an SCP to an AWS Organizations entity (root, OU, or account) defines a guardrail for what actions the principals can perform. You still need to attach identity-based or resource-based policies to principals or resources in your organization's accounts to actually grant permissions to them.

Service Control Policies Example

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ec2:DeleteFlowLogs",
        "logs:DeleteLogGroup",
        "logs:DeleteLogStream"
      ],
      "Resource": "*"
    }
  ]
}
```

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_example-scps.html