Overview

AWS offers centralized policy-based management (Service Control Policy) as well as the features of consolidated billing for multiple AWS accounts via the feature of AWS Organization.

This is helpful for:

a. Centrally Manage Policies Across Multiple AWS Accounts
b. Control Access to AWS Services
c. Easily create a new AWS Account Creation and Management
d. Consolidate billing across all accounts
   Pricing benefits from aggregated usage

Allows you to manage multiple AWS accounts and it's a Global Service

The main account is a **master account** - You can't change it

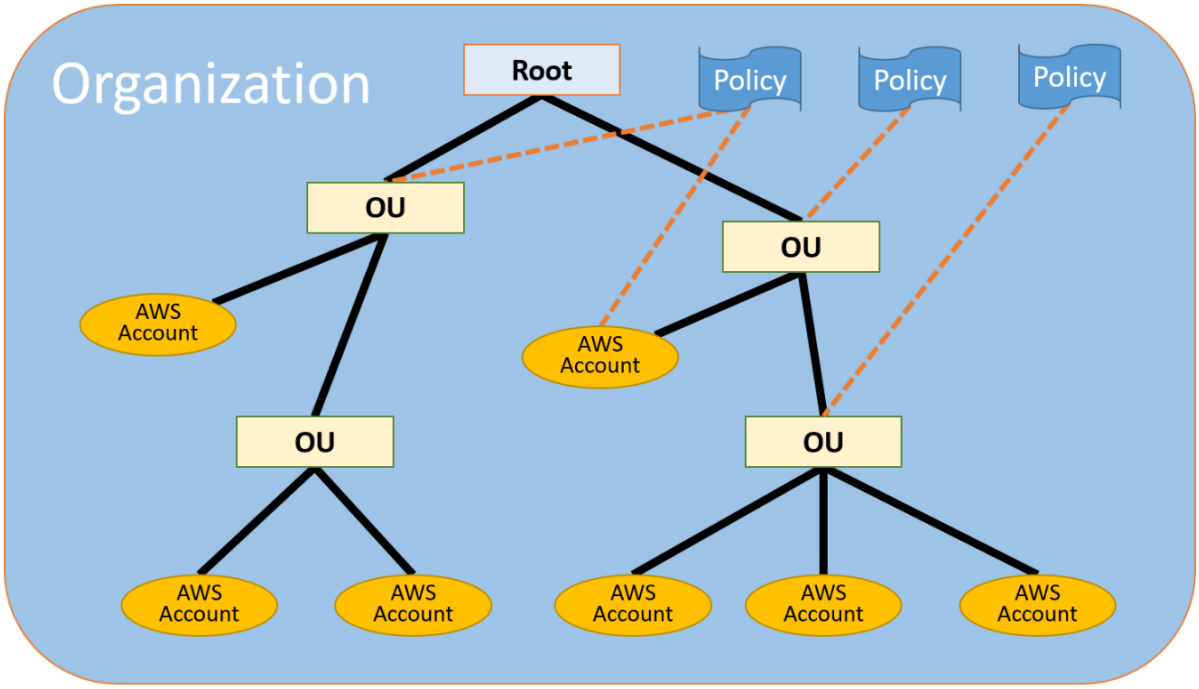
Mater account in AWS used in AWS Organization to:
Create an organization,
Invite new AWS Accounts

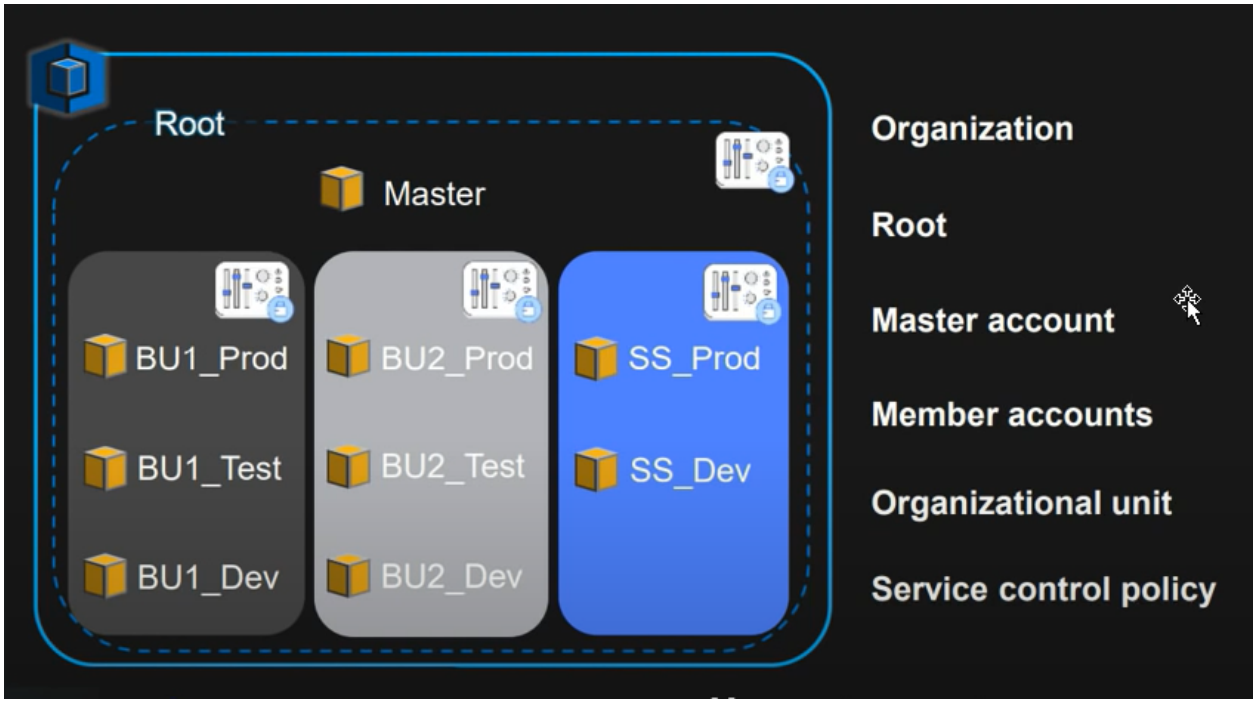
Other accounts are **member accounts**

Member accounts can only be part of **ONE ORGANIZATION**

Terminologies:

The following diagram shows a basic organization that consists of seven accounts that are organized into four organizational units (OUs) under the root.





Organization:

An entity that you create to consolidate your AWS accounts so that you can administer them as a single unit

An organization has **one master account along with zero or more member accounts**.

Root

The parent container for all the accounts for your organization. If you apply a policy to the root, it applies to all organizational units (OUs) and accounts in the organization.

Currently, you can have only one root. AWS Organizations automatically creates it for you when you create an organization.

Organizational Unit (OU)

A container for accounts within a root.

An OU also can contain other OUs, enabling you to create a hierarchy that resembles an upside-down tree, with a root at the top and branches of OUs that reach down, ending in accounts that are the leaves of the tree

When you attach a policy to one of the nodes in the hierarchy, it flows down and affects all the branches (OUs) and leaves (accounts) beneath it

An OU can have exactly one parent, and currently each account can be a member of exactly one OU.

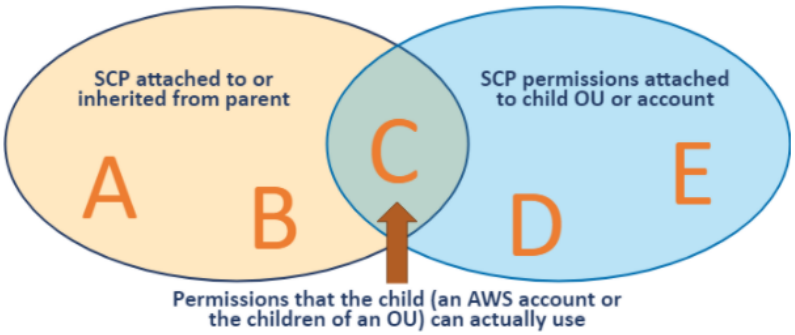
Service Control Policy (SCP)

A policy that specifies the services and actions that users and roles can use in the accounts that the SCP affects.

Instead, SCPs specify the maximum permissions for an organization, organizational unit (OU), or account.

When you attach an SCP to your organization root or an OU, the **SCP limits permissions for entities in member accounts.**

How does the SCP work?



Strategies for Using SCPs

You can configure the SCPs in your organization to work as either of the following:

- A blacklist – actions are allowed by default, and you specify what services and actions are prohibited
- A whitelist – actions are prohibited by default, and you specify what services and actions are allowed

Example:

Policy Based Restriction.