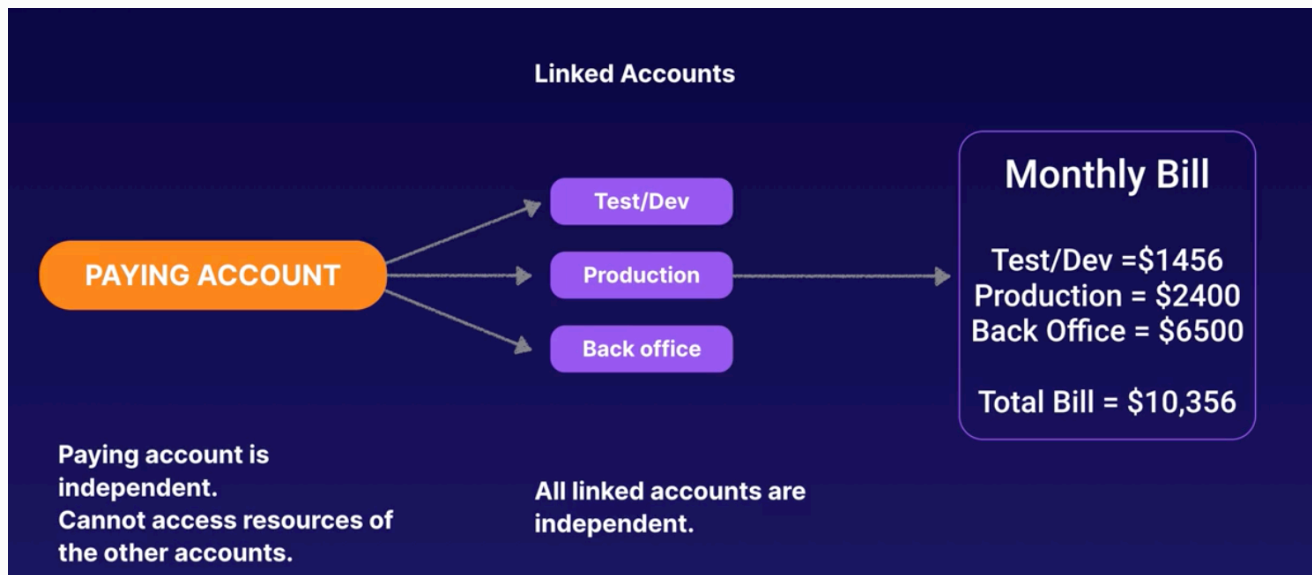


## AWS Organizations

an account management service that enables you to consolidate multiple AWS accounts into an organization that you create and centrally manage.



AWS Organizations helps you centrally manage and govern your environment as you grow and scale your AWS resources. Using AWS Organizations, you can create accounts and allocate resources, group accounts to organize your workflows, apply policies for governance, and simplify billing by using a single payment method for all of your accounts. AWS Organizations is integrated with other AWS services so you can define central configurations, security mechanisms, audit requirements, and resource sharing across accounts in your organization. AWS Organizations is available to all AWS customers at no additional charge.

## How it works



### Manage your AWS accounts

AWS accounts are natural boundaries for security, costs, and workloads. We recommend using a multi-account approach to scale your cloud environment. Simplify account creation by using the AWS Command Line Interface (CLI), SDKs, or APIs. You can centrally provision recommended resources and permissions to those accounts with AWS CloudFormation.



### Define and manage your organization

Group your accounts into organizational units (OUs) and manage them as a unit. Apply tag policies to classify or track resources. Provide attribute-based access control for users or applications. You can delegate administration of supported AWS services to accounts so users can manage them on behalf of your organization.



### **Secure and monitor your accounts**

Provide tools and access for your security team to manage security for the organization. Provide read-only security access across accounts, detect and mitigate threats using Amazon GuardDuty, review access to resources using AWS IAM Access Analyzer, and secure data using Amazon Macie.



### **Control access and permissions**

Set up AWS Single Sign-On (SSO) to provide access to AWS accounts and resources using your Active Directory, and customize permissions to match job roles. Apply service control policies (SCPs) to users, accounts, or OUs to control access to AWS resources, services, and Regions within your organization.



### **Share resources across accounts**

Share AWS resources across your organization using AWS Resource Access Manager (RAM). Create your AWS Virtual Private Cloud subnets once and share them across your organization. Centrally agree to software licenses using AWS License Manager. Share a catalog of IT services and custom products across accounts using AWS Service Catalog.



### **Audit your environment for compliance**

Use AWS CloudTrail across your accounts to create a secure log of all activity in your cloud environment. Set policies to enforce backups on your schedule using AWS Backup. Define configuration settings for resources across accounts and AWS Regions using AWS Config.

## **Some Best Practices With AWS Organizations**

- Always enable multi-factor authentication on root account.
- Always use a strong and complex password on root account.
- Paying account should be used for billing purposes only. Do not deploy resources into the paying account.
- Enable/Disable AWS services using Service Control Policies (SCP) either on OU or on individual accounts.

### **Sharing S3 Buckets Across Account Access**

- Using Bucket Policies & IAM (applies across the entire bucket). Programmatic Access Only.

- Using Bucket ACLs & IAM (individual objects). Programmatic Access Only.
- Using Cross-account IAM Roles. Programmatic And Console access.

## Create role





1

2

3

4

### Select type of trusted entity


 <b>AWS service</b> EC2, Lambda and others	 <b>Another AWS account</b> Belonging to you or 3rd party	 <b>Web identity</b> Cognito or any OpenID provider	 <b>SAML 2.0 federation</b> Your corporate directory
--	---	---	--

Allows entities in other accounts to perform actions in this account. [Learn more](#)

### Specify accounts that can use this role

Account ID\*

This field is required.

- Options**
- ☐ Require external ID (Best practice when a third party will assume this role)
  - ☐ Require MFA 

## 3 Different ways to share S3 buckets across accounts

- Using Bucket Policies & IAM (applies across the entire bucket). Programmatic Access Only
- Using Bucket ACLs & IAM (individual objects). Programmatic Access Only.
- Cross-account IAM Roles. Programmatic AND Console access.