Identity and Access Management on AWS: Designing and Implementing an AWS Organization

CREATING AND MANAGING AN AWS ORGANIZATION

Brian Eiler
CLOUD ARCHITECT

www.thecoursewaregroup.com

Overview

Introduction to Globomantics

Quick Overview: IAM

Need for Multiple Accounts

Introduction to AWS Organizations

- Creating an Organization

Accounts

- Creating, Accessing, and Removing Accounts

Organization Units

Introduction to Globomantics

GLOBOMANTICS : Current

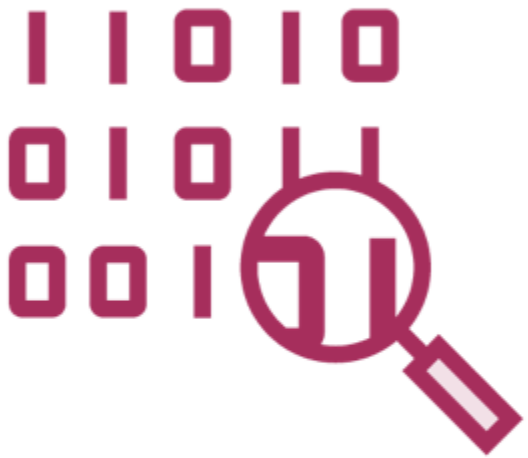
Global presence with locations in North America, Europe, and Asia

One AWS account for each location

Frequent audits

GLOBOMANTICS : Needs

Apply corporate and compliance policies across all AWS accounts



Fine-tune access control

Maintain compliance

Quick Overview: IAM

AWS Identity & Access Management

Secure access

Granular control

Temporary access

Federate identity

Integrate with other AWS services

AWS Identities

IAM User

IAM Group

IAM Role

IAM Users

User
or
Application

Joe

Unique Name
and
Unique Identifier

Kathy

Unique Credentials
for
AWS Console or
Programmatic Access

IAM Groups

- A collection of IAM Users
- One or more IAM policies can be attached to a group
- IAM users within a group inherit permissions from one or more policies
- IAM user can belong to multiple groups

IAM Roles

- An IAM identity used to assign temporary credentials
- One or more IAM policies can be attached to an IAM role
- IAM users, applications, or external users can assume this role
- External users can access an AWS account using federated identities from corporate directories (such as Active Directory) or websites (such as Facebook)

IAM Policies

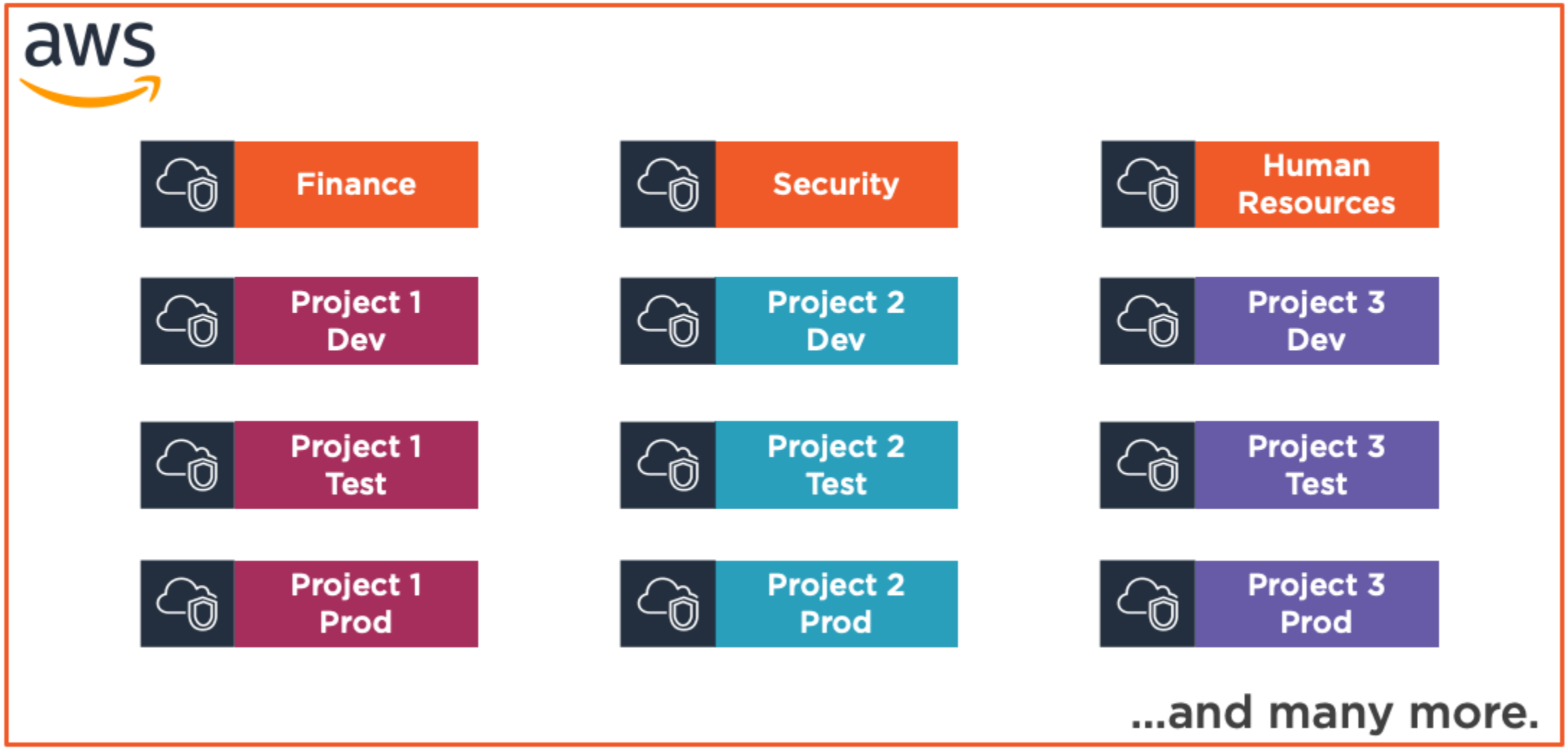
- IAM Identities (user, group, or role) have no permissions or policies attached by default
- Identity-based policies (IAM policies) are attached to these IAM identities
- IAM identities are authorized to perform or not perform certain actions based on these policies.

Need for Account Management

GLOBOMANTICS

"At Globomantics, we have multiple projects at a single location. How can we ideally manage all these projects in AWS?"

One Account for All



Challenges with One AWS Account

No Environment Isolation	Complex IAM for Whole Enterprise	Huge Blast Radius
Difficulty Applying Different Policies & Standards	Unrealistic Billing Separation	AWS Service Limitations per Account

Solution: Multiple Accounts

Standalone Multiple Accounts

Standalone Multiple Accounts: Why or Why Not

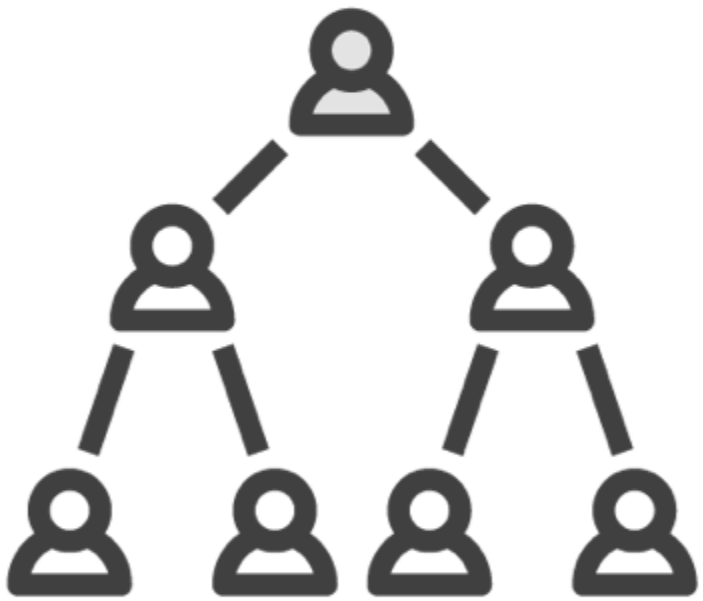
Pros	Cons
Well-controlled access	No centralized governance
Autonomous operations	No volume discounts
Reduced blast radius	No credit sharing
Work around service limits per account	Requires separate Reserved Instances (RI) in each account
Simplified billing	Requires contract agreements and billing setup for each account creation
	Separate billing

GLOBOMANTICS

"Having standalone accounts certainly helps with multiple projects. However, without centralized governance, we cannot use this setup to maintain our enterprise security policies and compliance requirements such as GDPR, HIPAA, and PCI."

Introduction to AWS Organizations

Description



An account management service that enables centralized management of multiple AWS accounts

Purpose and Structure

Centralized Management	Hierarchical Groups
Combine all existing AWS accounts and/or easily create new accounts into a single organization for centralized management	AWS Accounts can be grouped into Organizational Units (OUs) for flexible management

Capabilities

Policy Framework	Consolidated Billing
Accounts within an organization can be controlled by directly or indirectly applying policies to them	Accounts are consolidated under a single master account that is responsible for all accounts' charges

Scalability and Interoperability

Automate Account Creation and Management	IAM Integration
Using AWS Organizations APIs, account creation and management can be automated Policies can be automatically applied	In addition to IAM's granular control over IAM identities, policies applied at the account level add more control

Use Cases

Apply policies to comply with corporate security and compliance policies

Create different groups of accounts for different teams and projects

Provide isolation and better resource management across multiple accounts

Benefits

Work around any hard or soft limits on an account

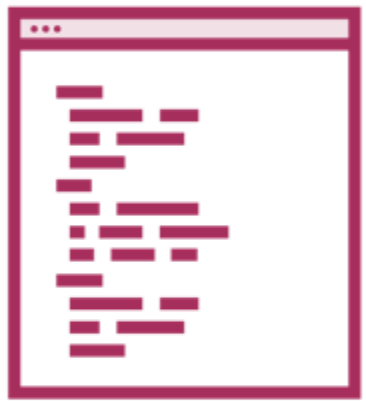
Credit sharing supported

Reserved instances can be utilized across all accounts

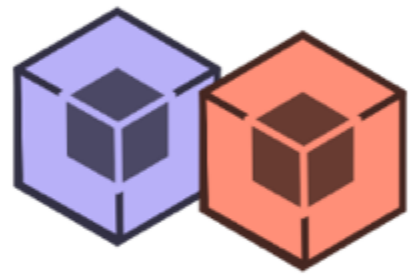
Free of Charge

Access

Management Console



AWS Command Line Tools



AWS SDKs

AWS Organizations HTTPS Query API

Creating an Organization

Master Account

Master account is a standard AWS account used to create an organization

- Creates accounts in an organization
- Invites other existing accounts to the organization
- Removes accounts from the organization
- Manages policies within the organization
- Ultimately, pays for all charges accrued by the member accounts

Creating an Organization

- Create an organization from a master account
- Can be created using a root user (not recommended) or using an IAM user with a minimum permission of organizations:CreateOrganization
- Two options: “all features” (recommended) and “only consolidated billing features”

Organization Types

Only Consolidated Billing Features	All Features
Consolidated billing	Consolidated billing
Create and invite accounts	Create and invite accounts
	Policy-based controls
	Hierarchical group management

Rules for Enabling All Features

- An organization can switch from “only consolidated billing” to “all features”, but not vice versa
- To enable “all features”, all invited accounts must approve the enabling process within 90 days
- During this process, accounts can be created within an organization, but existing accounts cannot be invited

Enabling All Features: Permissions Required

- To start the process, master account administrators require organizations:EnableAllFeatures permission
- To approve the request, member account administrators require organizations:AcceptHandshake permission
- To finalize the process, master account administrators require organizations: AcceptHandshake permission.

Root Container

The parent container for all the accounts in an organization

There can only be one root in an organization

AWS automatically creates this root

Accounts

Accounts

Accounts can be created within an organization

Accounts can be invited to an organization

Terminology Usage

Member Account

Created Account	Invited/Joined Account
An AWS account created within an organization	An existing AWS account that is invited or has joined an organization

Creating an Account in an Organization

- Master account administrators require organizations:CreateAccount and organizations:DescribeOrganization (console only) permissions to create an account
- Member accounts created within an organization automatically become a part of the organization
- Created accounts do not require separate setup for payment

Creating an Account: Security

- AWS Organizations automatically creates an IAM role in the member account
- This IAM role's default name is OrganizationAccountAccessRole
- This IAM role provides full administrative control over the member account

Inviting an Existing Account to an Organization

- Master account must verify its email address before it can start inviting other existing AWS accounts
- Invitation requires either email address or account ID of the other account
- 20 invitations are allowed per day in an organization
- Other account owner must accept or reject the invitation within 15 days or invitation expires

Inviting an Existing Account: Permissions

To send an invitation, master account administrators require

organizations:DescribeOrganization (console only)
organizations:InviteAccountToOrganization

To cancel an invitation, master account administrators require

organizations:DescribeOrganization (console only)
organizations:ListHandshakesForOrganization
organizations:CancelHandshake

Inviting an Existing Account: Permissions

To accept or decline an invitation, administrators from other accounts require

organizations:ListHandshakesForAccount
organizations:AcceptHandshake
organizations: DeclineHandshake

Administrators yield enough power to create, add, or remove accounts; therefore, all these permissions must be properly assigned.

Inviting an Existing Account: Security

- IAM role is not automatically created in an invited account, unlike created accounts
- Member account should create an OrganizationAccountAccessRole IAM role in the member account and provide access to the master account to assume the role
- This role can grant full or limited administrative control over an invited member account

GLOBOMANTICS

"Globomantics recently acquired two companies that are already running on AWS cloud. We can easily add those accounts into our existing AWS account and manage them all using AWS Organizations."

Demo

Starting with AWS Organizations

- Create an AWS Organization
- Create an account within the organization
- Invite an existing account to the organization
- Accept invitation from the existing account

IAM for Created Member Accounts

- AWS Organizations automatically creates a root user for a created account
- It also creates an IAM role (OrganizationAccountAccessRole) within a created account
- It does not create any IAM users, groups or other roles

Accessing Member Accounts: Options

Newly created account can be accessed using:

Root User

Pre-configured IAM Role

Accessing Member Accounts via Root User

- AWS Organizations auto-assigns root user password that is minimum 64 characters long
- You cannot retrieve this password
- To access as the root user of newly created, password recovery process must be used

IAM in Member Accounts: Best Practices

- As best practice, do not use root user on regular basis
- Instead, create IAM users and roles with appropriate permissions
- Enable multi-factor authentication (MFA) for the root user

Joined Accounts and Their Visibility

Standalone Account's cost and usage	Joined Account's cost and usage	Standalone Account's cost and usage	Joined Account's cost and usage
Standalone Account	Joined Account	Standalone Account (Left an organization)	Joined Account (Rejoined)

Demo

Accessing the Created Member Account

- Use Password Recovery
- Log into the Created Account as a Root User
- Create an IAM User with Admin Access
- Access the Created Account from the Master Account using an IAM Role

Demo

Accessing the Joined Member Account

- Create an IAM Role in the account
- Access the Joined Account from the Master Account using an IAM Role

Removing a Member Account: Requirements

- An account can only be removed from an organization if the account has all account sign-up information entered
- This information includes AWS Customer Agreement, support plan, contact information and payment method
- Invited accounts have this information
- Created accounts do not have this information; therefore, it must be entered before their removal from an organization

Removing a Member Account: Implications

- **Master account can remove a member account, or member account can remove itself**
- **Removed member accounts become standalone accounts and are responsible for their own charges**
- **Organization policies no longer apply to these removed accounts**
- **Master account remains jointly and severally liable for created account's actions *even after removal* unless prior authorization has been obtained from AWS**

Closing a Member Account

- Back up any applications and data first
- To close a member account, sign in as root user and close the account from Billing and Cost Management console
- It is recommended to remove the account from the organization first and then close the account

Organizational Units (OUs): Purpose

A container for grouping accounts within the root container or another OU

Simplifies management of multiple accounts

OU Hierarchy

Create a hierarchy starting with root at the top and ending with an account at the bottom

OUs are used for branching this hierarchy

OU Limitations

OUs can be nested up to five levels deep

You can have 1000 OUs within an organization

All OUs must have a unique name within a parent container

OU Policies

Policies can be attached to an OU

An OU nested within another OU will inherit the policies from all parent OU(s)

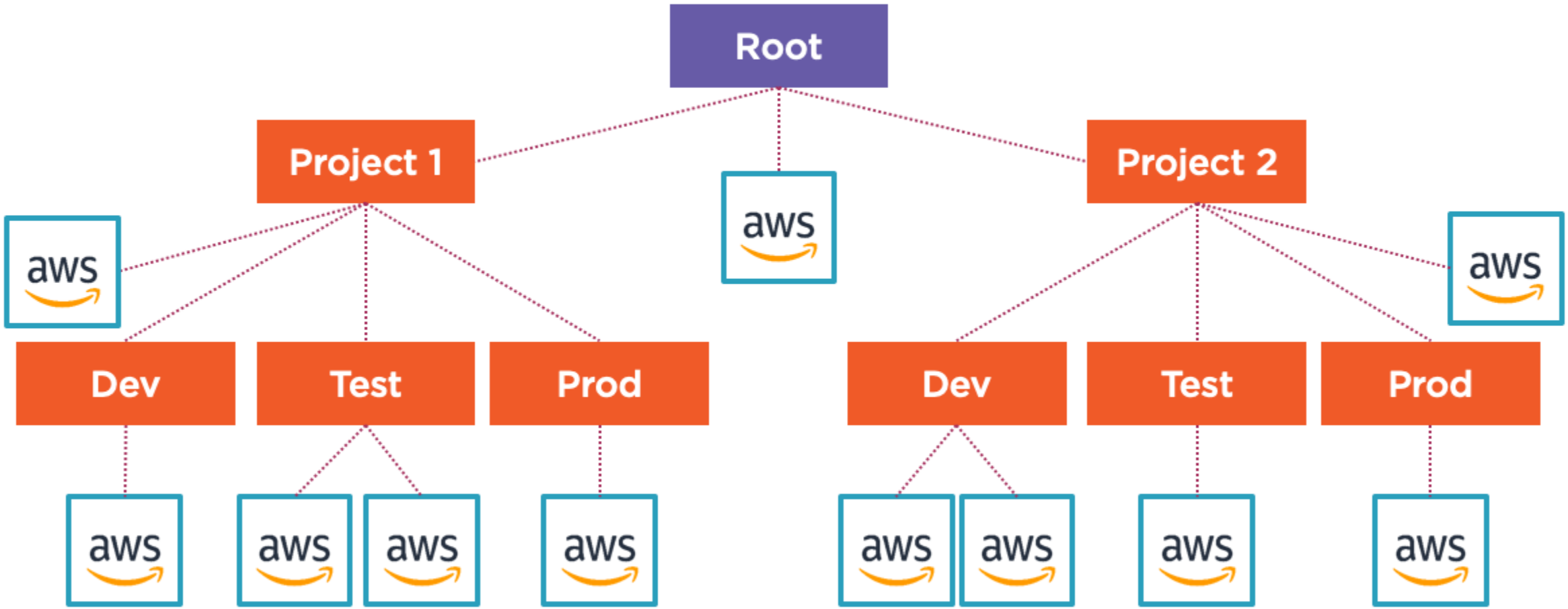
Accounts and Organizational Units

An account can belong to a single OU, not multiple

An account can be moved to another OU or to the root level

To delete an OU, all accounts must be first removed from the OU

Organizational Units Sample Diagram



Demo

Working with Organizational Units (OUs)

- Creating an OU
- Moving Accounts to OUs
- Renaming and Removing OUs

Summary

Introduction to Globomantics

Quick Overview: IAM

Need for Multiple Accounts

Introduction to AWS Organizations

- Creating an Organization

Accounts

- Creating, Accessing, and Removing Accounts

Organization Units