WHAT IS AWS ORGANIZATIONS? HOW IT WORKS & BEST PRACTICES

AWS Organizations is an AWS account management service that lets users centrally manage and control groups of AWS accounts, and the workflows and policies that apply to them.

The management process can be done manually or programmatically at the API level. Users can:

- Integrate multiple AWS services with multiple unique AWS accounts.
- Manage the user environments based on organizational, legal, or project-based policies.

The accounts can also share resources, security mechanisms, audit requirements, configurations, and policies between multiple AWS organizations.

In this article, we will give an overview of the AWS Organization service and how you can use it as a best practice for your AWS user environments.

(This article is part of our [AWS Guide](#). Use the right-hand menu to navigate.)

User accounts in AWS Organizations

Originally, Amazon Web Services began with a single user account that enrolled [multiple AWS services](#). Each person used a single AWS account and subscribed to multiple AWS services as necessary.

However, using a single account per user limits how organizations can manage the services, security permissions, audits, policies, and billings across multiple business divisions and projects assigned to the same user account.

The concept of AWS account has evolved significantly since the inception of the AWS cloud service, which continues to grow, particularly in the areas of:

- Solutions
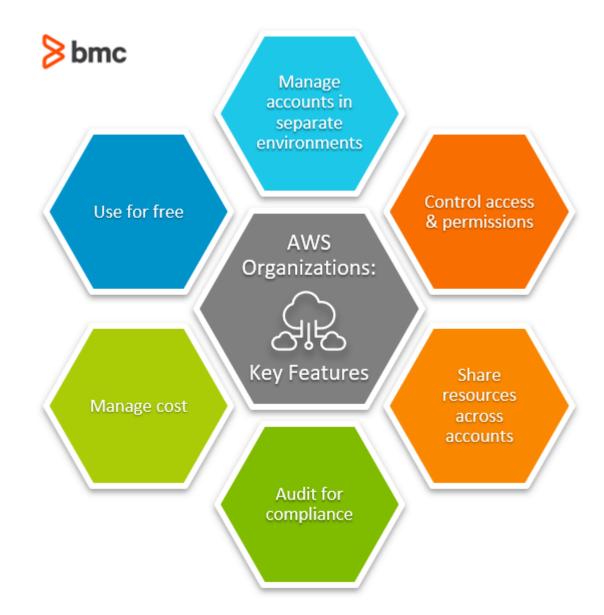- Resource options
- Billing
- Configuration features

Now, we can consider AWS accounts as [containers](#) that consist of such capabilities, all governed and managed across multiple AWS accounts but within the same centralized environment.

(Explore [other AWS management tools](#).)

Benefits of AWS Organizations

Here's why it makes sense to use multiple AWS accounts for the same categories of AWS resources contained in multiple unique and manageable account environments:

- **Easily categorize and discover services.** Find and assign AWS applications programmatically using APIs, command line interface (CLI), and GUIs.
- **Apply logical boundaries to all aspects of policies.** Different projects within the organization may be exposed to different security and compliance requirements. For example, by segregating AWS resources within multiple AWS accounts across all of those different projects, you can easily enforce unique identity policies in compliance to the applicable regulatory frameworks.
- **Contain damage within logically isolated user accounts.** If a specific user account is compromised, only the resources assigned to that AWS Organizations user account will be exposed to the higher risk.
- **Easily manage billing and resources on a project or task basis.** Employees can switch between their AWS Organizations accounts assigned to them and utilize resources optimally as required.

Key features of AWS Organizations

The AWS Organizations is a service that enables organizations to define, manage, and govern groups of AWS user accounts and centrally provision services and policies—and maintain a single bill for the AWS Organization and the set of underlying user accounts.

To realize these capabilities, AWS Organizations lets you:

- **Manage multiple AWS Accounts in separate environments.** Establish boundaries that define the policies, services, and resources used across grouped organizational units (OUs).
- **Control access & permissions.** Enforce policies for identity and access management across users based on teams, business divisions, and projects.
- **Share resources across accounts.** Once an AWS service is created and configured, you can share that service across multiple users, both within and beyond the same AWS organization.
- **Audit for compliance.** Maintain an extensive audit trail of all accounts for auditing purposes.
- **Manage cost.** Single consolidated billing process allows users to track, manage and optimize usage across all accounts and user environments.
- **Use for free.** Activating this feature is free. The accounts are only charged for the AWS services and resources they consume, as usual.

Drawbacks of AWS Organizations

While AWS Organizations makes it easy to manage multiple user accounts, it can also make the entire system more complicated and possibly introduce security lapses.

Here are a few security best practices, suggested by AWS, to make sure AWS Organizations works best for managing multiple user account environments:

- **Security.** Use an email address managed by your organization for the AWS Organizations root user. Use complex passwords, multi-factor authentication, and a phone number for account recovery.
- **Monitoring.** Apply the necessary controls to monitor the usage of root user accounts. The root user access should be rare and trigger flags immediately in event of unauthorized access.
- **Restrict privileges.** Attach Service Control Policy (SCP) to the root user account. As a result, the security policy will extend to all AWS Organization users.

By understanding how AWS Organizations works, you can limit any concerns and maximize its advantages for your AWS usage.

Related reading

- BMC Multi-Cloud Blog
- Amazon's Elastic File System (EFS) Explained
- The AWS Well-Architected Framework: 5 Pillars & Best Practices
- Enterprise Password Management Best Practices
- SaaS in 2021: Growth Trends & Statistics
- State of the Cloud Today