AWS Organizations

AWS Organizations enable you to centrally manage and administer your environment as you develop and manage your AWS resources. You may use AWS Organizations to create new AWS accounts and assign resources programmatically, group accounts to organize your operations, apply policies to accounts or groups for administration, and simplify billing by utilizing a single payment option for all of your accounts.

Besides that, AWS Organizations is connected with other AWS services, allowing you to create central configurations, security methods, audit requirements, and sharing resources across your organization's accounts. AWS Organizations is offered at no additional cost to all AWS users.

AWS Organizations Features:

AWS Organizations provides the following functionalities:

1. All your AWS accounts are manageable from a single location.

You may group your existing accounts into an organization, allowing you to manage them all from one location. You may establish accounts automatically added to your organization and invite other users to join your group.

You may also add policies that apply to any or all of your accounts.

2. Billing for all member accounts is centralized.

AWS Organizations support consolidated billing. You may use your organization's administration account to combine and pay for all member accounts. Management accounts in consolidated billing have access to the billing and account activity information of member accounts in their company.

Services like Cost Explorer might utilize this data to assist management accounts in improving their organization's cost performance.

3. Accounts are grouped hierarchically to fulfill financial, security or compliance requirements.

You may organize your accounts into organizational units (OUs) and assign various access controls. For instance, if you have accounts that must only access AWS services that fulfill particular regulatory standards, you may group them into a single OU.

You may then apply a policy to that OU that prevents access to services that do not fulfill regulatory criteria. You may nest OUs within the other OUs up to five layers deep, giving you more freedom to build your account groups.

4. Policies to centralize control over the AWS services and API operations available to each account

You may use service control policies (SCPs) as an organization's management account administrator to establish the maximum permissions for member accounts. SCPs let you limit which AWS services, resources, and particular API activities each member account's users and roles may access.

You may also specify when access to AWS services, resources, and API operations should be restricted.

5. Integration and support for AWS Identity and Access Management

IAM provides precise control over users and responsibilities in accounts. AWS Organizations extends that control to the account level, allowing you to specify what users and roles in an account or set of accounts may do.

The resultant permissions are the natural intersection of what AWS Organizations allow at the account level and what IAM expressly grants at the user or role level inside that account.

6. Integration with other AWS services

To conduct tasks on every account that is a member of an organization, you may combine the multi-account management services provided in AWS Organizations with chosen AWS services. When you allow an AWS service in your organization's member accounts to conduct actions on your behalf, AWS Organizations establishes an IAM service-linked role for that service in every member account.

The service-linked part comes with specified IAM permissions that enable the other AWS service to conduct particular actions in your organization and its accounts.

7. Global Access

AWS Organizations is a global service with a single endpoint that works from all AWS Regions. You don't need to select a region to operate in explicitly.

8. Free to Use

Security in AWS Organizations

AWS and you share responsibility for security. The shared responsibility model defines this as security of the cloud and security in the cloud:

Security of the Cloud - AWS is in charge of securing the infrastructure that powers AWS services in the AWS Cloud. AWS also offers services that may be used securely. As part of the AWS compliance processes, third-party auditors regularly examine and verify our security's efficacy.

Security in the Cloud - The AWS service you use determines your responsibility. Other things to include are the sensitivity of your data, your company's requirements, and applicable laws and regulations.

Accessing AWS Organizations

You can gain access to AWS Organizations in the following ways:

1. AWS Management Console
2. AWS command line tools
3. AWS SDK
4. AWS Http Query API