# AWS hierarchy structure

AWS contains thousands of services, which all seem like separate units. As you dive deeper into the structure of AWS resources, you'll find that there's a hierarchy to manage how all the services operate, how you interact with them and how users and service accounts manage them.

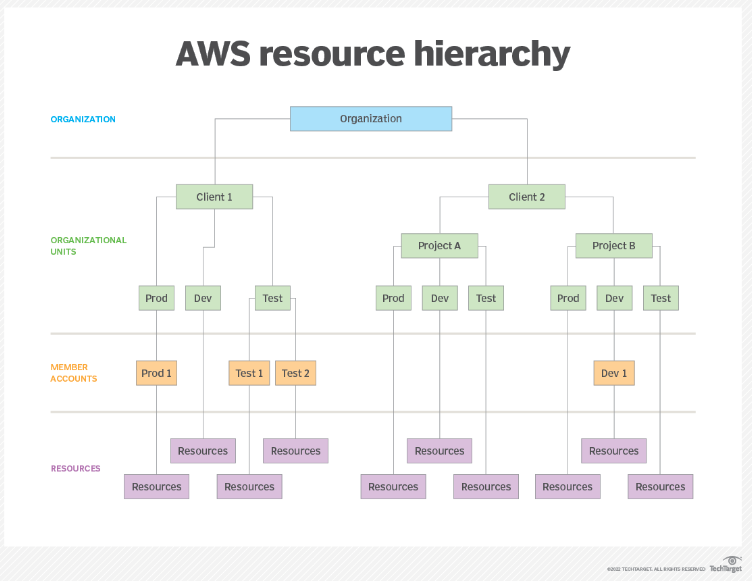
**Hierarchy structure explained**

Within AWS, there are four measurements of the hierarchy structure, which are the following:

* AWS Organization----12 digit ac
* Organizational unit (OU)-----invites root
* Account
* Resource

**Example:-**

Say you have two AWS accounts, one for development and one for production, and they communicate with each other. While this scenario is great for deployment and testing, it can open several security holes if there is no access control. For example, you could accidentally deploy test code to production when you intended for it to go to the development environment.



### Organization

Think of an organization like a house frame. It's well built, allows you to protect resources inside it and ensures everything is safe. An organization in AWS is the way that you centrally govern your AWS environment. It allows you to do the following:

* focus on security for your accounts as your environment grows;
* centrally provision accounts;
* audit environments for compliance purposes;
* share resources; and
* [optimize billing](https://www.techtarget.com/searchcloudcomputing/feature/Lower-your-cloud-bill-with-these-AWS-cost-control-tips).

It's the primary access point to all tasks that you perform inside of AWS. Without an organization, there is no structure. It acts as the parent for every member account that your organization manages. It holds all the resources, accounts, security control policies (SCPs), billing and auditing policies available inside of AWS.

### Organizational unit

An OU is a way to almost replicate an organization's SCPs throughout other member accounts. It allows admins to manage and group member accounts inside of one root. An OU can also hold other OUs and send out SCPs to them. An organizational unit is meant to group member accounts that have the same type of SCPs or operational needs. For example, if you have a development account and a production account that share the same type of [compliance needs](https://www.techtarget.com/searchcio/tip/Top-cloud-compliance-standards-and-how-to-use-them) for audits, admins will group them in the same OU.

Organizational units can have exactly one parent and each member account belongs to only one organizational unit.

There are a few recommended OUs, which are the following:

* security OU
* infrastructure OU
* sandbox OU
* workload OU

#### Service control policies

SCPs for a production-level environment enable you to centrally manage control over all accounts inside your environment. Although SCPs are great from a security perspective, they should not be your only security measure. They only set limits. Users still need to use Identity Access Management (IAM) to allow access to resources via roles and users inside your production AWS accounts.

The organization holds all SCPs that manage permissions -- they do not grant them. They ensure that member accounts operate within an organization's access control guidelines.

Following are a few key takeaways about SCPs:

* SCPs only affect IAM users and roles managed by accounts inside the organization.
* SCPs only affect member accounts in the organization.
* SCPs affect all users and roles.
* Even if an SCP is active, you still need to give permissions to IAM users and roles.

### Member account

Inside an organization, admins can create multiple resources and services. Those services are inside a container-like structure called [member accounts](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_accounts_access.html). Some of those include the following:

* EC2 instances
* S3 buckets
* VPCs

Do not confuse a member account with a management account. The management account is what creates the organization. It's the first account that has access to the organization's resources, OUs and SCPs. You'll typically see this referred to as the root account.

### Resource

Resources encompass AWS resources and services. These are the components that we work with every day, including EC2 instances, Lambda functions and S3 buckets. However, these resources don't manage themselves. Organizations, OUs and member accounts manage them. When you interact with resources, you interact with the rest of the AWS hierarchy structure.

* Users
* Groups
* Policy etc..

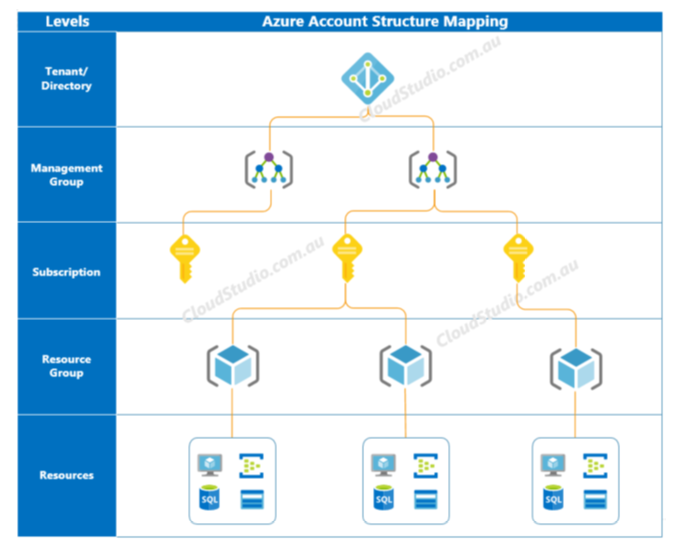
------------------------------------------------End-------------------------------------------

# Azure hierarchy structure

**Hierarchy structure explained**

Within Azure, there are five measurements of the hierarchy structure, which are the following:

* Tenant Directory – Root Management Group
* Management Group - organizational unit (OU)
* Subscription ---billing
* Resources group
* Resource



# GCP hierarchy structure

**Hierarchy structure explained**

Within GCP, there are four Pillars of Google Cloud Resources

* Organization
* Folders
* Projects
* Resources

