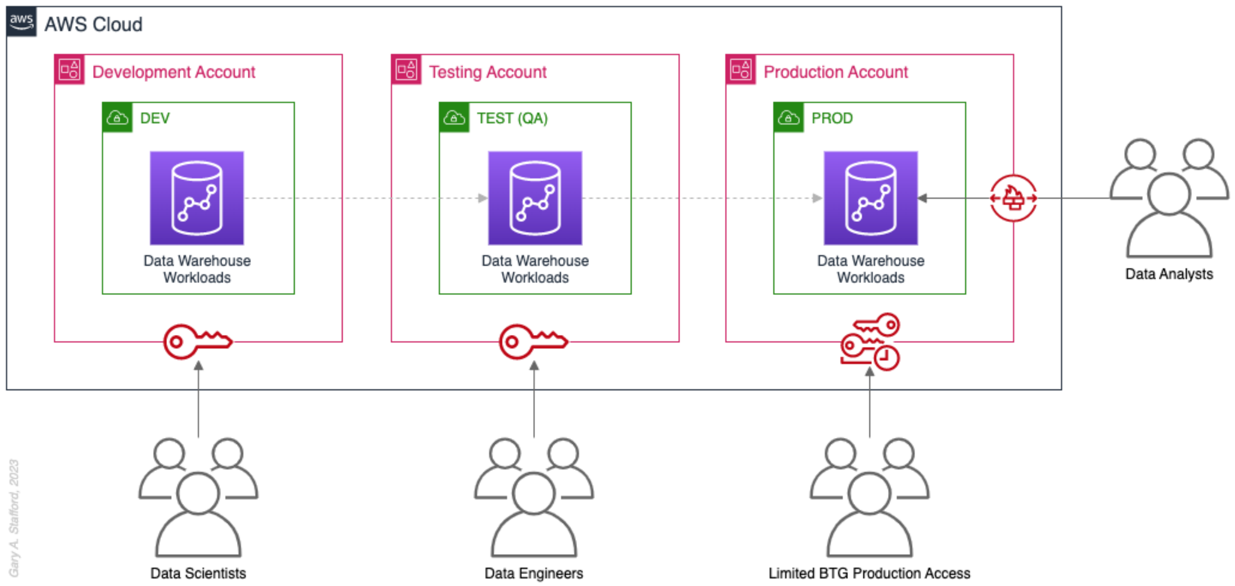
AWS Organizations and PrincipalOrg Id

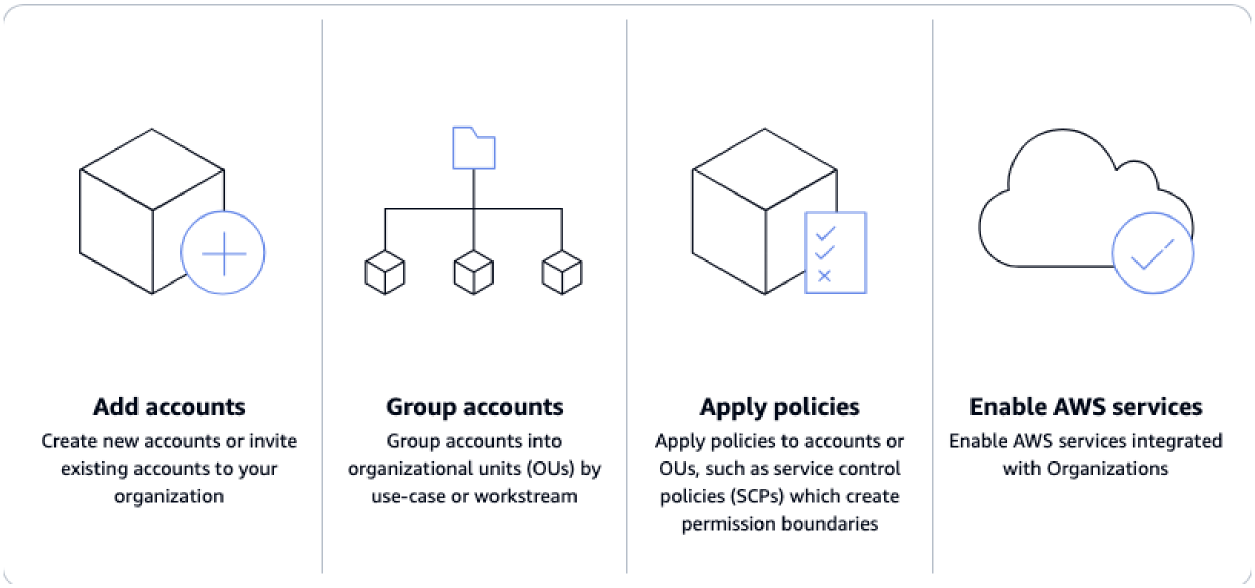
Now, multi-account AWS environments were mentioned previously once before but an explanation as to what they were and how they work was never explained. Multi-account AWS environments are, simply put, architectures that utilize multiple accounts to manage resources, users and workloads within an organization. This is often done for security and categorization reasons, allowing us to insulate workloads from one another and prevent unwanted users poking around in places where they do not belong, causing undesirable consequences.

An example of an environment which utilizes three different accounts for three different workloads, using separate accounts for development, testing and production, is given below:



Source: AWS

In order to more easily create and manage accounts that utilize a shared set of resources, AWS created a service called **AWS Organizations**. It works by grouping accounts into something called Organizational Units (or OUs), to which policies can be assigned/added to. These policies define the OUs permission boundary, i.e. which services, instances and other general AWS resources that they have access to, dictating what the accounts can and cannot do. An infographic presenting the mentioned capabilities of AWS Organizations is given below:



Add accounts
Create new accounts or invite existing accounts to your organization

Group accounts
Group accounts into organizational units (OUs) by use-case or workstream

Apply policies
Apply policies to accounts or OUs, such as service control policies (SCPs) which create permission boundaries

Enable AWS services
Enable AWS services integrated with Organizations

Source: AWS

Finally, OUs can help give some much needed structure to complex architectures and help conveniently locate, isolate and differentiate similar sets of resources from one another. This is because resources being governed by an OU can be quite easily identified by the presence of the Principal Org ID, whose value is used to uniquely identify and distinguish OUs from one another. In contrast, resources that do not belong to any OU have no such tag, making them easy to identify as well.