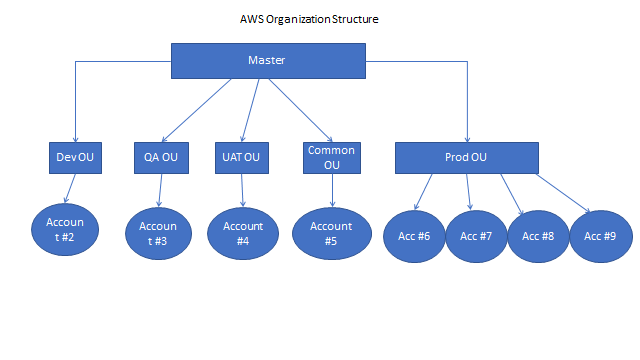
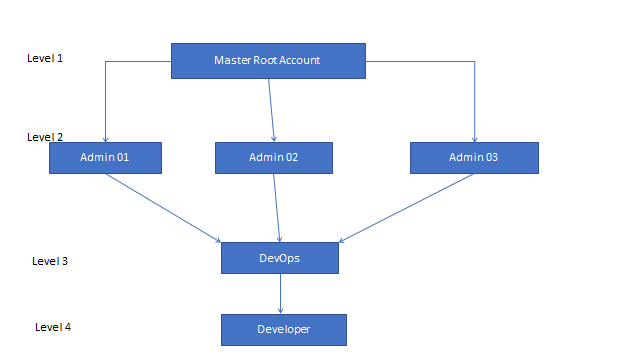
**AWS User Access Security Best Practices**

* Only with Fixed set of IPs will be allowed to access the Cloud infrastructure from Bastion server
* All the allowed IAM users who can access AWS Cloud infrastructure must have access through 2-factor authentication.
* AWS organizations can be distributed into various domains like developers( with limited access) , DevOps ( with Read / Write access across all accounts and Organizational Units) , No access is required to QA
* Developers will have limited access with only execution privileges in their developer account itself
* DevOps will have creation, configure & execution privileges in all accounts like Dev , QA, UAT, Production etc.
* Single user policy is attached to one individual Organization Unit
* **Organizational Units** (OU) will make it easier to apply management access controls as applying user access policies at OU level will be better practice.
* Single DevOps access related policy will be applied for all DevOps resources & same way Single Developer access related policy will be applied for all developer resources. So that access rights will remain same across domains.
* Developers will not have access of other setups in AWS Infrastructure e.g. QA, UAT & Production
* There will be no resources in the master account.





Master Root Access

|-> Admin access01

|-> Admin access02

|-> Admin access03

|-> DevOps

|-> Developer