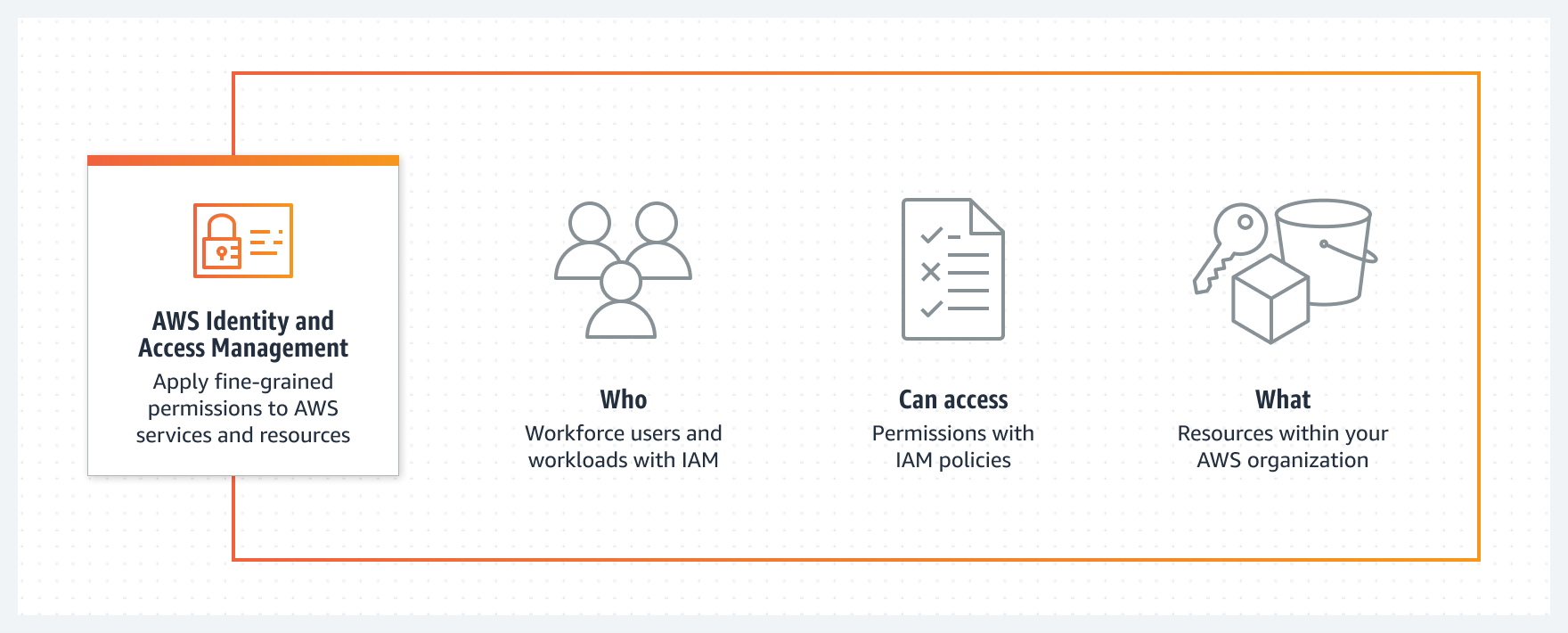
**What is IAM:**

 IAM:

Stands for Identity Access Management.

1. IAM allows you to manage users and their level of access to the aws console.
2. It is used to set users, permissions and roles. It allows you to grant access to the different parts of the aws platform.
3. AWS Identity and Access Management is a web service that enables Amazon Web Services (AWS) customers to manage users and user permissions in AWS.
4. With IAM, Organizations can centrally manage users, security credentials such as access keys, and permissions that control which AWS resources users can access.

****

**Features Of IAM**

* **Centralized control of your AWS account:**

You can control creation, rotation, and cancellation of each user's security credentials. You can also control what data in the aws system users can access and how they can access.

* **Shared Access to your AWS account:**

Users can share the resources for the collaborative projects.

* **Granular permissions:**

It is used to set a permission that user can use a particular service but not other services.

* **Multifactor Authentication:**

An AWS provides multifactor authentication as we need to enter the username, password, and security check code to log in to the AWS Management Console.

* **Networking controls:**

IAM also ensures that the users can access the AWS resources within the. Organization’s corporate network

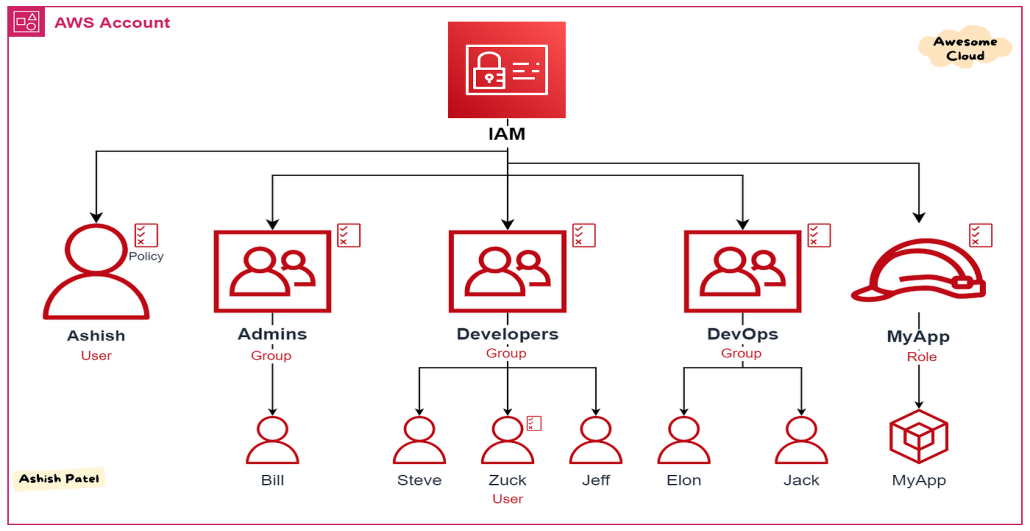
* **Free to use:**

AWS IAM is a feature of AWS account which is offered at no additional charge. You will be charged only when you access other AWS services by using IAM user.

**IAM Identities**

**USER:**

1. Using IAM you can create and manage aws user and use permissions to allow and deny their access to aws resources.
2. With the help of the user we can interact all the resources that are present in our aws account.
3. IAM user limit is 5000 per aws account.



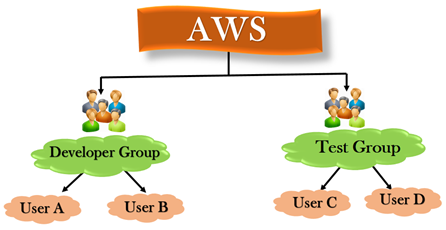
**ROLES:**

An IAM role is an IAM entity that defines a set of permission for making aws service requests. IAM roles are not a associated with a specific user or group instead trusted entities assume roles, such as IAM user application ,or AWS service such as EC2

****

**GROUPS:**

The user created, can also be divide among groups and then the rules and policies that apply on the group apply on the user level as well.



**POLICY:**

Policy is just a set of guidelines and rules. To assign permission to a user,group,role or resource. You create a policy which is a document explicitly list permission.

