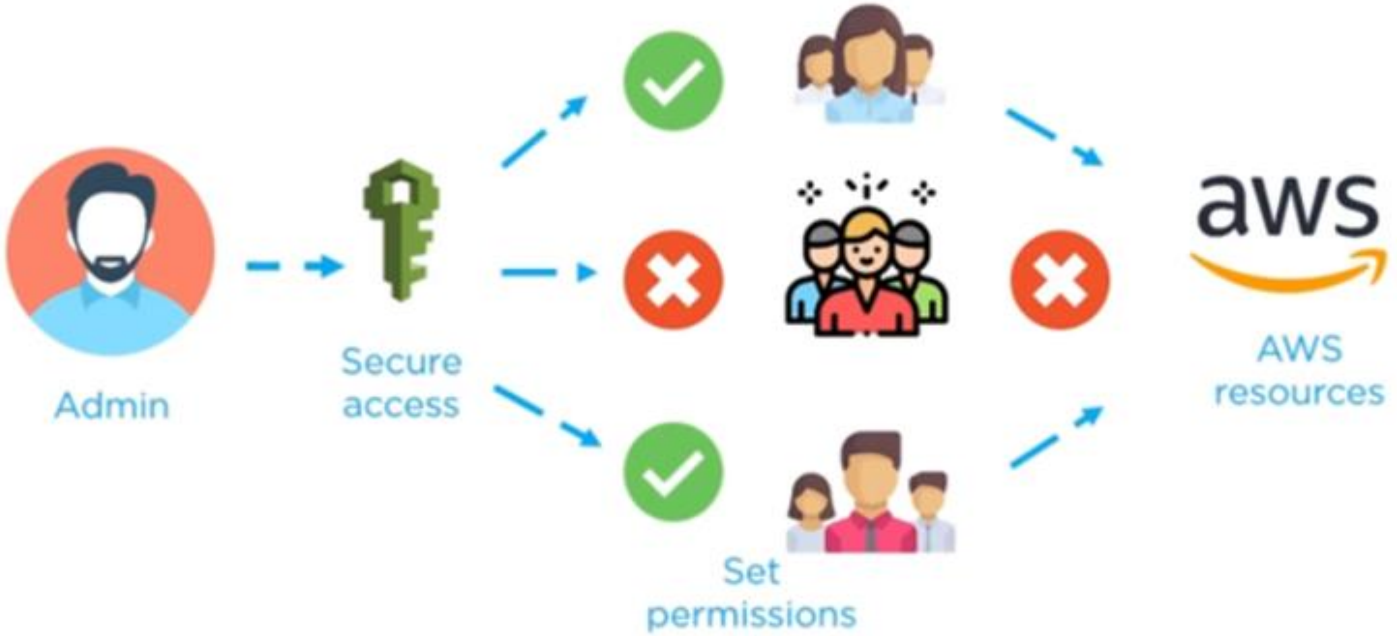
Identity & Access Management

AWS
IAM

- AWS Identity and Access Management (IAM) is a web service for securely controlling access to AWS resources
- It enables you to create and control services for user authentication or limiting access to a certain set of users on your AWS resources



IAM Components -

Identity and Access Management is an AWS service that enables you to provide fine grained access control to:

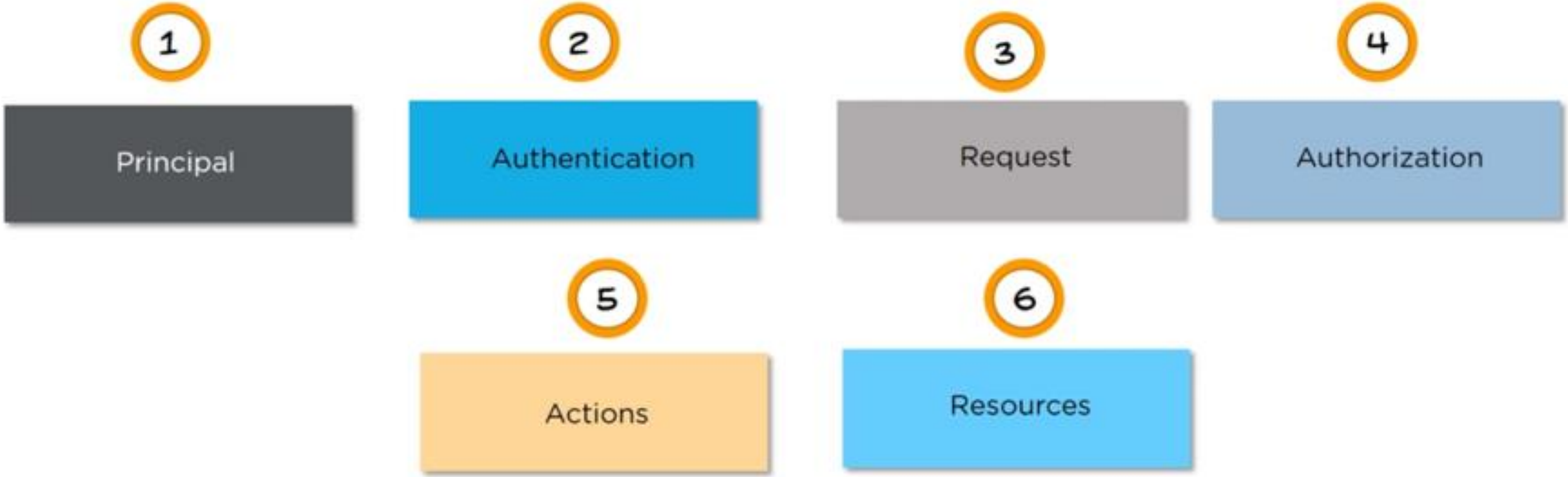
- Interact with AWS services on behalf of your AWS account
- Interact with AWS resources created in your AWS account

The main components are:

- IAM Users
- IAM Groups
- IAM Roles
- IAM Polices

How does it work?

IAM workflow includes below elements -



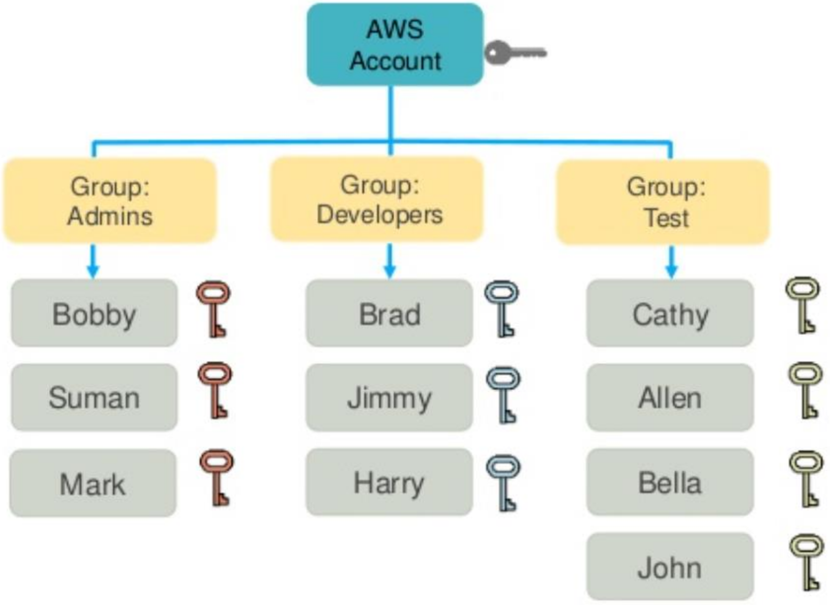
IAM Components

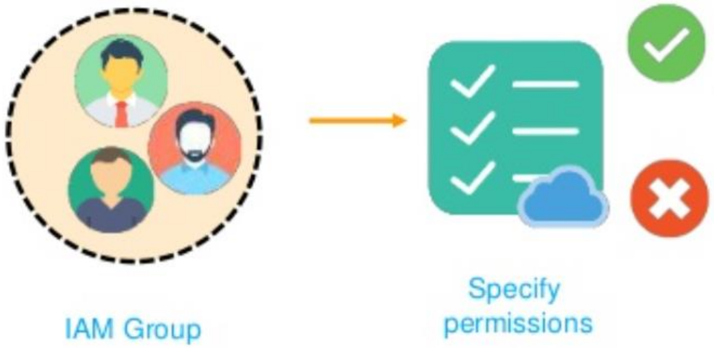
IAM User

- Can have username / password to login to the AWS Console
- Can have AWS credentials for making API calls to interact with AWS services
- An IAM user doesn't necessarily have to represent an actual person. An IAM user is really just an identity with associated permission.

IAM Group

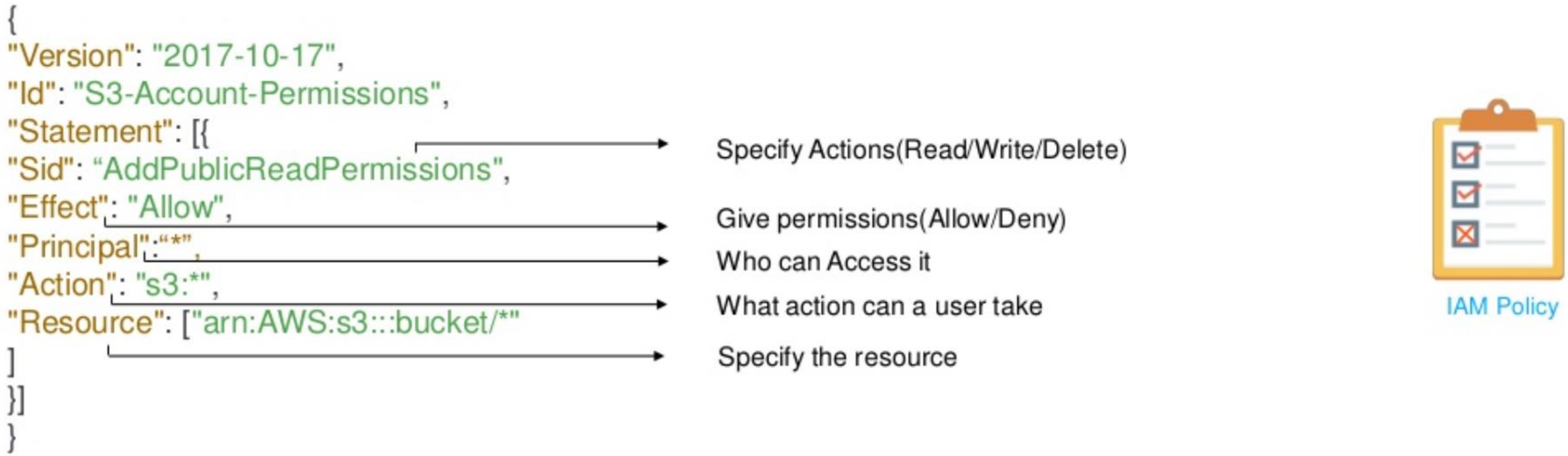
- A collection of IAM Users
- You assign permissions to the IAM Group, all IAM Users in the Group inherit those permissions.





IAM Policies

- Policy is set of permissions and controls to access AWS resources.
- Policies are stored as JSON docs.
- You attach policies to users and groups.

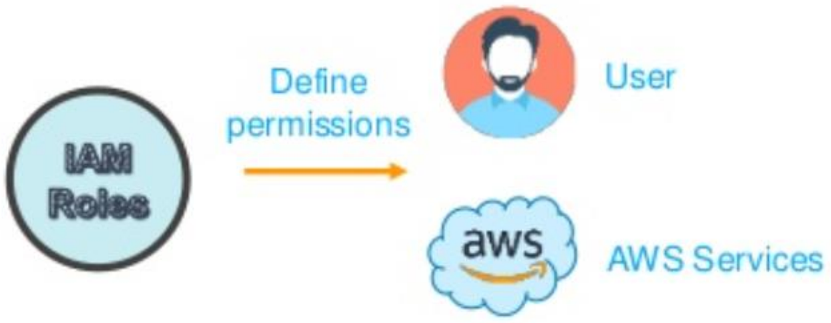


```
{
"Version": "2017-10-17",
"Id": "S3-Account-Permissions",
"Statement": [{
"Sid": “AddPublicReadPermissions",
"Effect": "Allow",
"Principal":“*”,
"Action": "s3:*",
"Resource": ["arn:AWS:s3:::bucket/*"
]
}]
}
```

Specify Actions(Read/Write/Delete)
Give permissions(Allow/Deny)
Who can Access it
What action can a user take
Specify the resource
IAM Policy

IAM Roles

- IAM role is set of permissions that defines the actions allowed/denied to certain entity in AWS console.
- It is similar to a user BUT they do not have -
  - Username/password like an IAM User can
  - AWS creds that can be retrieved like an IAM User creds



Next

Hands on!

Thank You!!