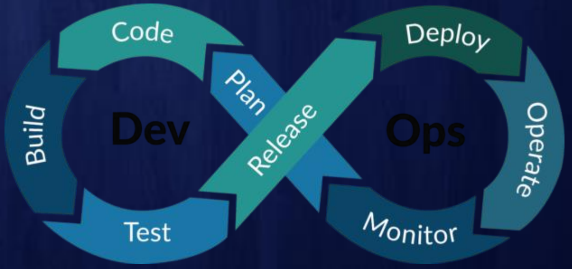
# AWS SAA + SysOps + Developer + DevOps Course #Day-5

We will start at 8 AM,
Stay tuned



RAKESH TANINKI
LEARN TO UNLEARN

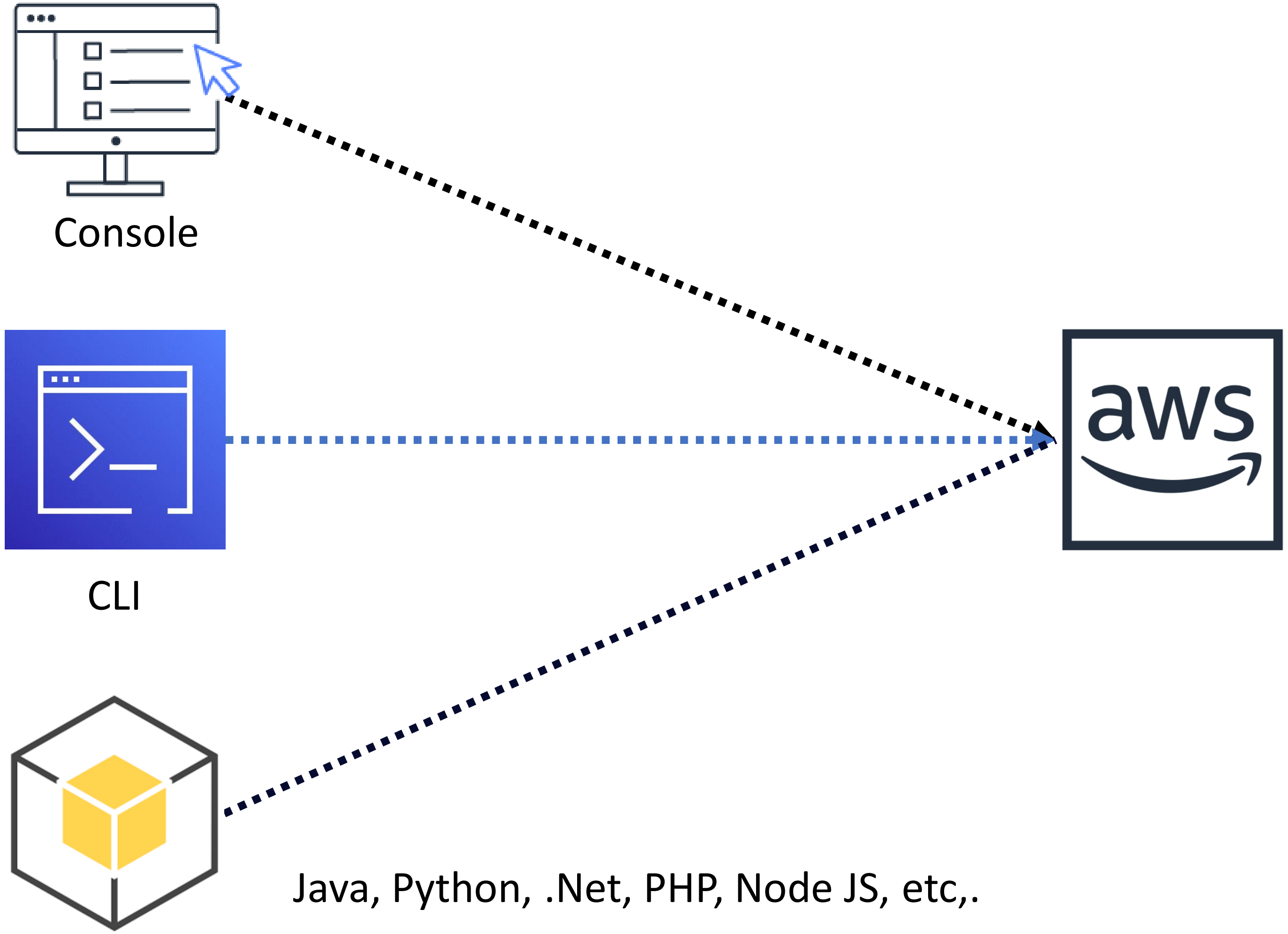
# Recap:

- Hands on - AWS Account Best Practices
- Hands on - AWS Budgets setup
- AWS Global Infrastructure
  - Regions
  - Availability Zones

# Today's topics:

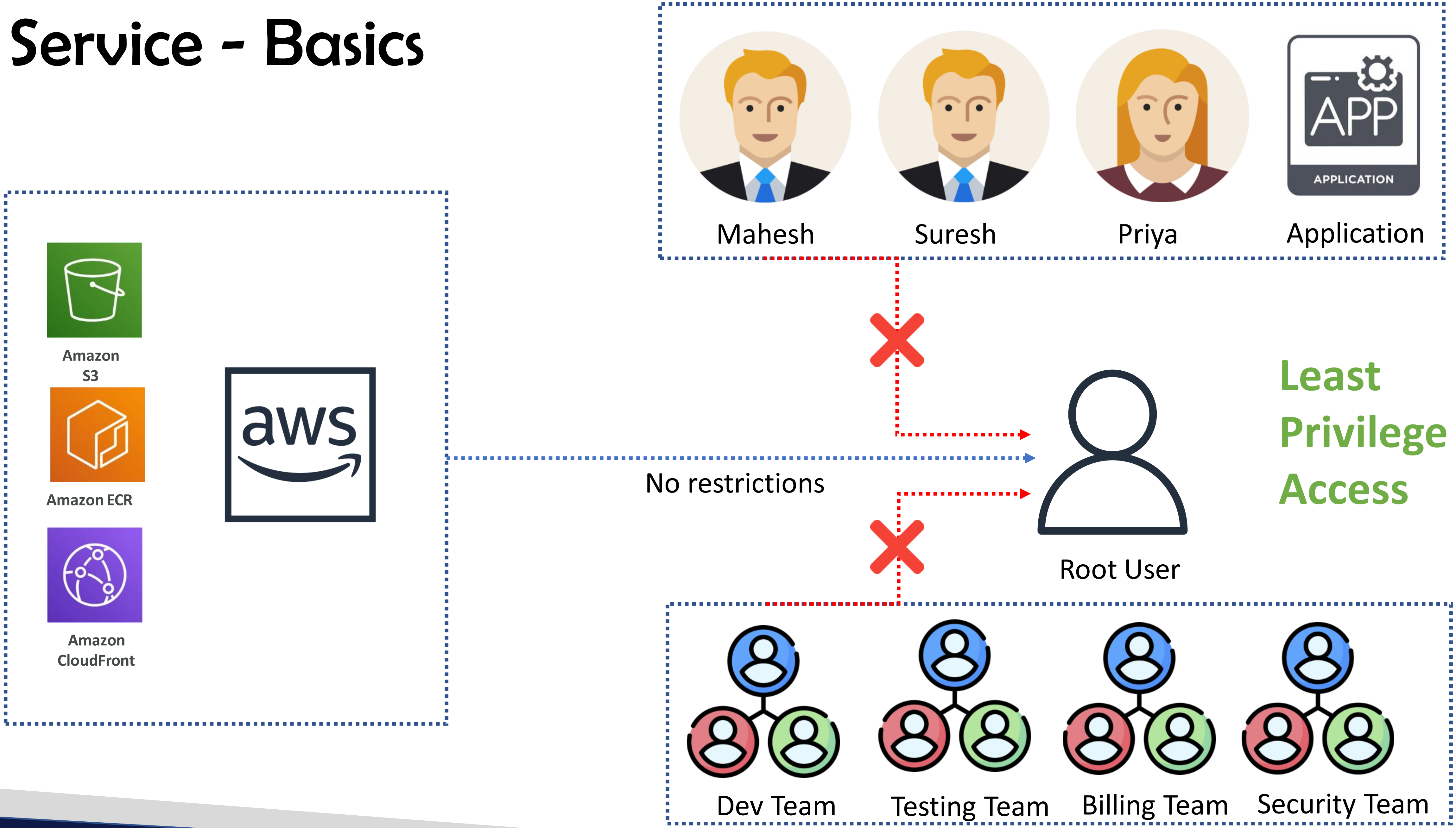
- Different ways to connect to AWS
- IAM – Basics
- IAM Users
- IAM Roles
- IAM Groups
- IAM Policies
- Hands on – IAM
- Access keys
- Hands on – AWS CLI

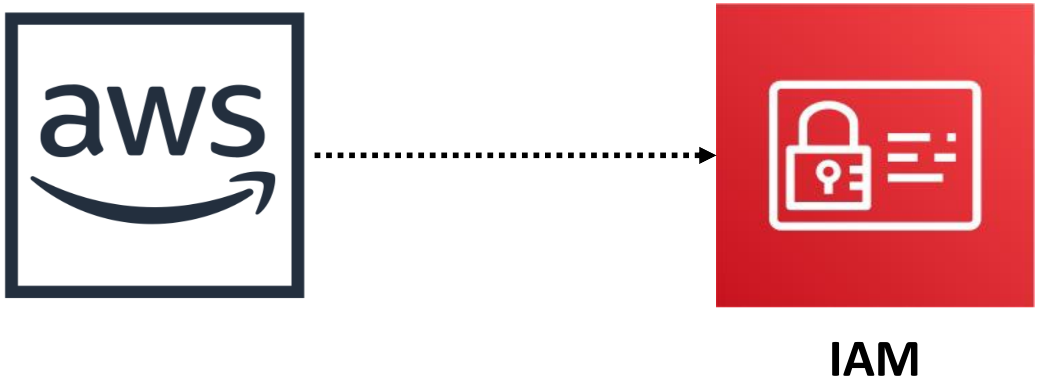
# Different ways to connect to AWS



Java, Python, .Net, PHP, Node JS, etc,.

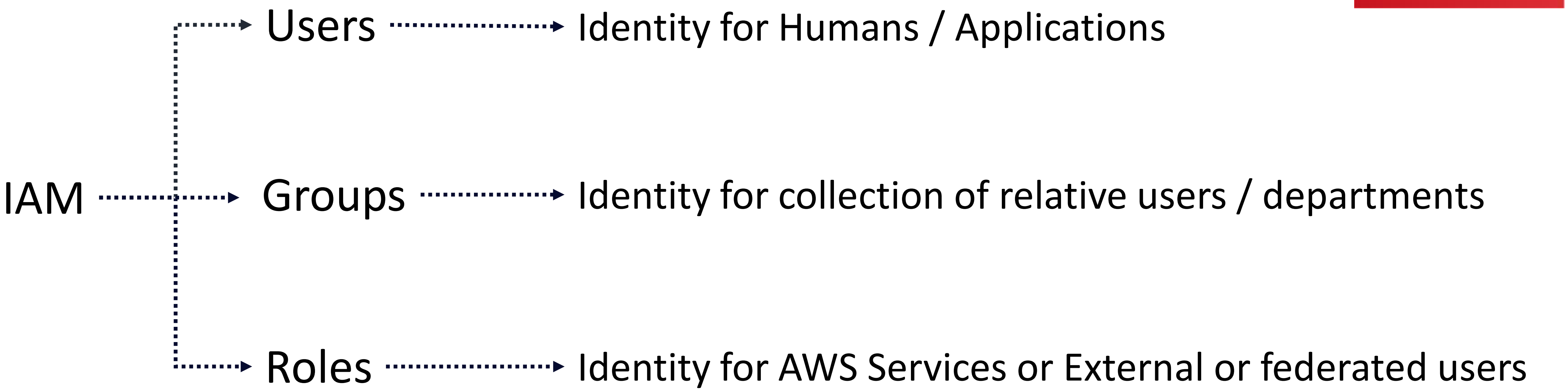
# IAM Service - Basics





- I – Identity
  - Manages the **Authentication**
  - User name and password (MFA)
  - Ex: Gmail, Facebook
- A – Access
  - Manages the **Authorization**
  - Provides the permissions to use services
- M – Management

# IAM Identities



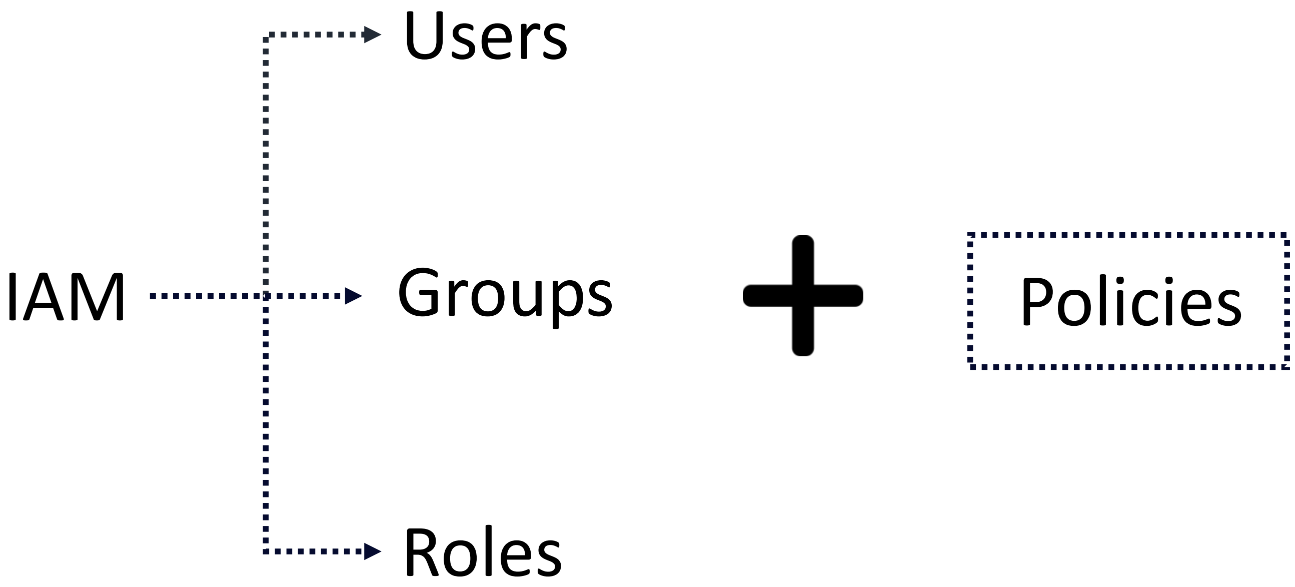
IAM

- Users → Identity for Humans / Applications
- Groups → Identity for collection of relative users / departments
- Roles → Identity for AWS Services or External or federated users

**Prabhas (normal)** →

**Prabhas (on Bahubali Role)**

# IAM Access



IAM

Users

Groups

Roles

+

Policies

- Provides permissions to identities
- Allow / Deny access to AWS services
- Deny has more priority than Allow

# IAM Key Points

- IAM is a global service
  - It is hosted in N. Virginia region
  - All endpoints reaches to N. Virginia region
- IAM is an AWS managed service
- IAM is a highly available service
- IAM is free of cost – no charges
- IAM has direct / indirect integration with all other AWS services

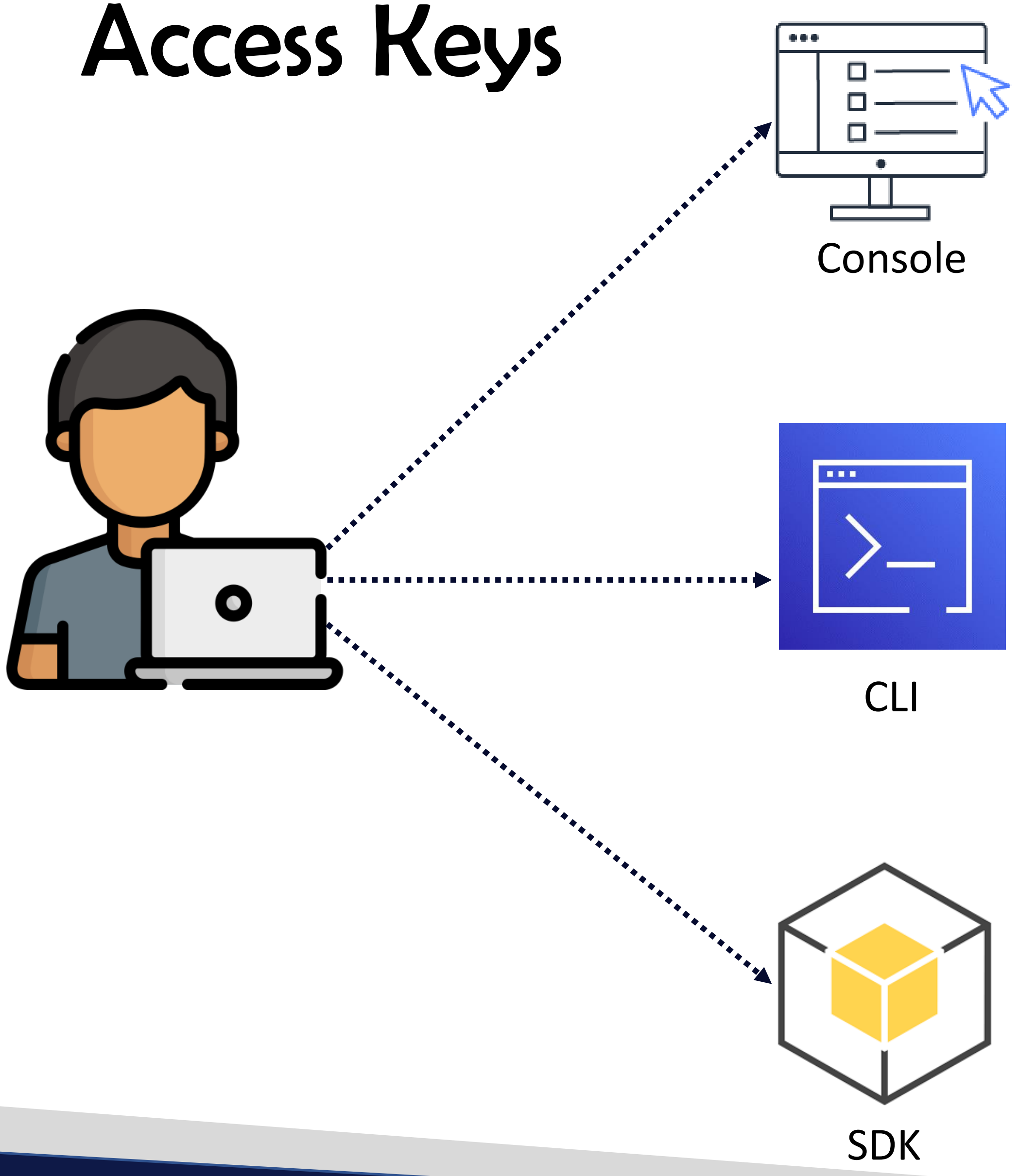
# IAM Key Points (contd)

- Allow / Deny with in your account
- Identity federation – Microsoft AD integration / Facebook / Google / Amazon

# IAM Demo cases

- Create **admin user** + **attach policy**
- Remove the attached policy and see the errors
- MFA setup on user
- Create admin group
- Add policy to the group
- Create 2nd user and add the group
- Check the permissions for the 2nd user

# Access Keys



Username: Suresh
Password: @ade!2345

1 ➔ Credential

AccessKeyId: AKIAIOSFODNN7EXAMPLE
SecretAccessKey: wJalrXUtnFEMI/K7MDENG/bEXAMPLEKEY

2 ➔ access keys

# Access Keys – Best Practices

- If you lost your secret key, **you cannot reset it**. You can only recreate it.
- Never share your keys
- Access keys rotation: **Must be rotated**
  - When rotating make the key inactive before the deletion

# Access Keys Demo cases

- Downloading CLI – click here
- Create Access Keys for user1 and user2
- Configure on local machine for both users
- Use below command s –
  - *aws configure (for user 1)*
  - *aws configure --profile user2 (for user 2)*
  - *aws sts get-caller-identity*
  - *aws sts get-caller-identity --profile user2*
  - *aws s3 ls*

ANY
QUESTIONS?
dreamstime

Thank you, will meet in tomorrow’s session