AWS SAA Stephen Mark

2024-09-23 21:27

Teacher :

Course Material : https://j2team.dev/go/018022db

Tags: AWS Architect Learning

AWS SAA Stephen Mark

1. Introduction

1.5

- `Upper Speed or Lower Speed depend on you`

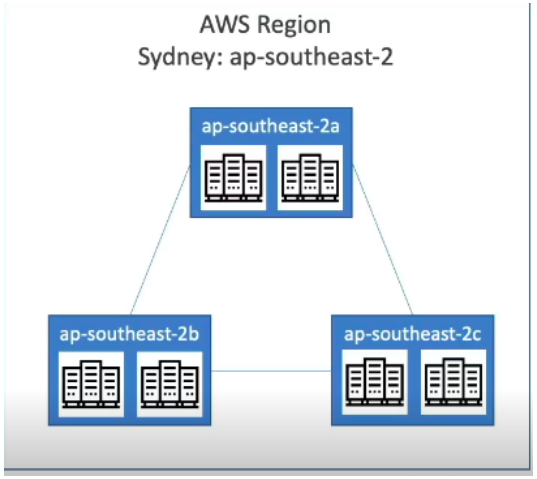
1.6 . About your instructor

- Data analyst, teacher , Big data , Solution Achitect.

3. Getting with AWS

3.1. AWS Cloud Overview - Regions & AZ

- 2006 : S3, EC2
- 2007 : Lauched in Europe
- Use Case : - Build Sophisticated, scable
  - Applicable to diverse set of industries
  - Use cases include : Enterprise IT, Backup & Storage , Big Data .
  - Hosting website
  - Gaming Service
- Global Infrastructure
  - AWS Region :
    - AWS has regions all around the world : us-east-l , eu-west-3 ,...
    - A region is a cluster of data centers
  - AWS Availability Zones (AZ)



- Each Region has many AZs (min 3, max 6)
- Each AZs is one or more datacenter
- They're connected with high bandwidth . They are separated , so that they're careful on disater.

- AWS Edge Locations

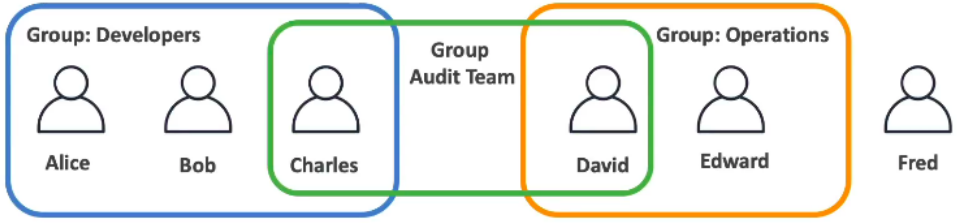
3.2. Tour of the AWS Console & Services in AWS

- Some service depend on region like EC2 ,.. . But some service is global usage like Route53 . You can see it when you click on service, it will show Global or region name

3.3. About the UI changes in the course

4. IAM & AWS CLI

4.1 IAM Introduction Users,Groups
- IAM is global Service
- Users are people within your organization, and can be grouped

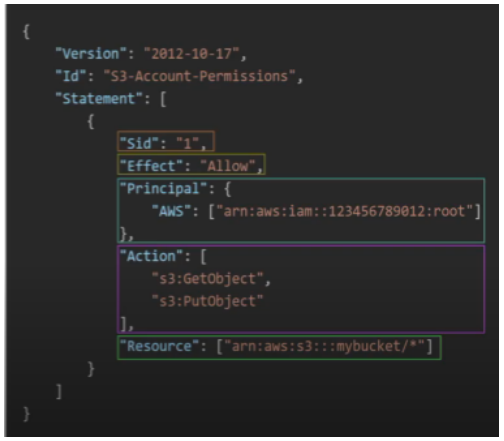


-
- User don't have to belong to a group, and user can belong to mutiple groups.
- Why do you create users and create group?
- Allowing user to account and we can them Permissions
- IAM : Permissions:

- Users and Groups can be assigned JSON documents called Policies.
- In AWS you apply "least privilege principle" : don't give more permissions than a user needs.

4.2 IAM Users & Groups Hands On
-

4.3 IAM Policies



- inheritance
- IAM Policies Structure
- Version : consist of day
- Id : Identifier for policy(optional)
- Statement (require)
- Sid : an identifier for statements
- Effect : Allow or Deny
- Principal : account/user/role who this policy applied to
- Action : list of action policy allows or denies
- Resource : list of resources to which the action applied to

4.4 IAM Policies Hands On
- "*" on AWS is meaning everything
-

4.5 IAM MFA Overview
- IAM - Password Policy
- Strong password
- In AWS, you can setup a password policy : lower, upper case, number or non-alphanumberic character
- Allow all IAM users to change their own passwords
- Require user to change their password after time (password expiration)
- Prevent password re-user
- MFA - Multi Factor Auth
- very recommend
- Can protect your RootAccounts and IAM usser

- MFA = password you know + security device you own
- MFA devices options in AWS : google auth, Authy

4.6 IAM MFA Hands On
-

4.7 AWS Access Keys, CLI and SDK
- How can users access AWS?
- Console (password + MFA
- CLI : access key
- SDK - for code : protected by access keys
- Access key ID : username
- Secret Access Key : password
- What's the AWS CLI?
- Enable to interact
- What's the AWS SDK?
- Language-specific APIs
- Embedded within your application

4.10 AWS CLI Setup on Linux

4.11 AWS CLI Hands On

4.13 AWS CloudShell
- CloudShell happend on console

4.14 IAM Roles for AWS Services
- The last component in IAM
- Có nghĩa là bạn cung cấp quyền cho dịch vụ (chứ không phải người dùng) quyền để thực hiện các hành động trên tài nguyên của bạn
- Ví dụ : Khi dùng EC2 instance , cần tải file lên S3, bạn sẽ tạo 1 IAM Role cho EC2 với quyền "putObject" lên S3.
- Comoon Roles :
- EC2 Instance roles
- Lambda Function Roles
- Roles for CloudFormation

4.15 IAM Roles Hands On

4.16 IAM Security Tools
- IAM Credentials Report (account -level) : lists all your account's users and status of their credentials
- IAM Access Advisor (user-level) : show service permissions grants to a user and when were last accessed
- You can use it to revise(edit) your policies .
- User root thường dùng nó để cho các previlige tới IAM user

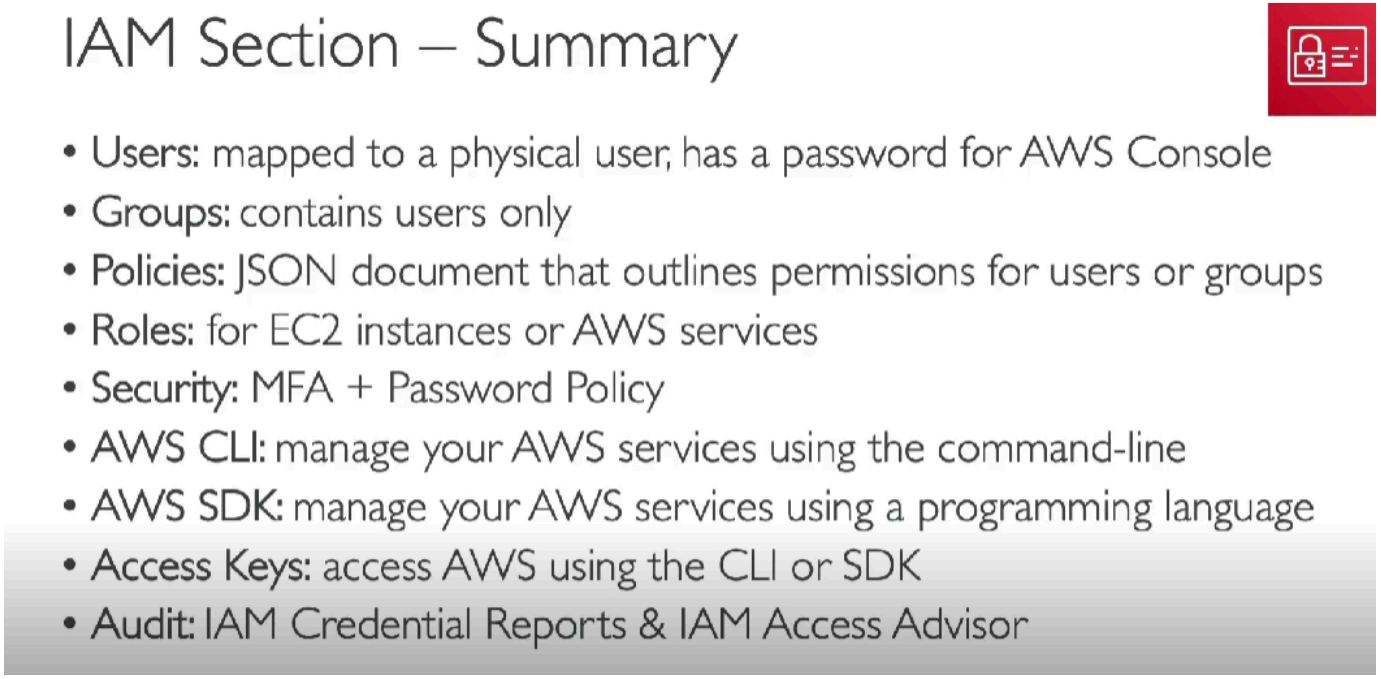
4.17 IAM Security Tools Hands On

4.18 IAM Best Practices

- Don't use the root except account setup
- One physical user = One AWS user

- Create a strong password policy
- Use and enforce
- create and use Role for service
- never share IAM users and Access Keys

4.19 IAM Summary



References