account alias: pankaj-admin-v2

MFA: multi factor authentication => for additional security to your root account we can add device verification in authentication. We configure Virtual MFA application (mobile app) with our account by scanning code. And by doing so whenever we try to login to root account it will ask for MFA token code.

With IAM => Acc settings password change policies =>

* We can set password validations
* Password expiry etc.

Ways to access AWS account:

1. AWS management console: password and MFA
2. AWS CLI: protected by access key
3. AWS software development kit: protected by access key

Aws key is generated by AWS console

Access key id =~ userid

Secret access key =~ password

Commands to set up AWS CLI on windows:

1. Google: AWS cli install windows
2. Select AWS cli version 2
3. Download and run msi installer
4. Install the downloaded msi file
5. Check on cmd: AWS –version

Access key generation

IAM user login

* Search IAM and enter
* Click on user security credentials
* Click on create access key
* Then download csv file

To configure cmd with AWS

* Cmd : aws configure
* Cmd : enter access key id
* Cmd : enter access key
* Cmd : just enter

Aws cloud shell:

* Echo “test” > demo.txt => will create demo file
* To download we need to provide absolute path
* Pwd => to get absolutely path

IAM roles:

* AWS service will need to perform actions on our behalf
* So we create users for purpose of AWS services and provide permissions with IAM Roles
* Generally, we create roles for EC2 services or lambda functions

Create Role:

* IAM => roles =>create roles => select AWS service => select EC2 service => permission => tag =>name

IAM security tools:

1. IAM Credential reports => IAM =>credential report => download report

* It gives details of all the users
* password renewal status
* access key status (generated or not last use timestamp
* Audit permissions of any or all users
* MFA status etc.

1. IAM Access advisor=> IAM => user => Access advisor => we can see recent activities within last 4 hours

* To check whether user using permissions regularly

EC2 (Elastic Compute Cloud)

* It is infrastructure as service
* Renting virtual machines (EC2)
* Operating System:
* Windows, Linux, Mac OS

EC2 instance:

* T2.micro => It is free tear general purpose ec2 instance for free
* T is instance class
* 2 means 2nd generation
* Micro in size of an instance

EC2 types:

1. General purpose (for balance between compute, memory & networking) => T series
2. Compute Optimized => C series
3. Memory Optimized => R series
4. Storage Optimized => I or D or H1 series

Security Groups:

* SG rules allow how traffic in and out of instance is allowed
* They act like firewall on EC2 instance
* They regulate
* Access to ports
* Authorized IP range IPv4 & IPv6
* They control
* Control of inbound network (other to instance )
* Control of outbound network (instance to other)

Classic ports to know

* 22 => SSH (secure shell) = log into a linux instance
* 21 => FTP (file transfer protocol) = upload files into a file share
* 22 => SFTP (secure file transfer protocol) = upload files using ssh
* 80 => HTTP – access unsecured website
* 443 => HTTPS – access secured website
* 3389 => RDP (remote desktop protocol) – log into a windows instance

SSH trouble shooting material available on lecture no. 38

Use EC2 using SSH (purpose -> to allow to use remote machine on AWS using local machine cmd):

* First create folder aws-course(anything)
* Prepare key pair for the EC2 instance that is .pem file
* Aws-course: chmon 0400 xyz.pem
* Aws-course : ssh –i xyz.pem ec2-user@publicIPID
* Aws-course: logout

For windows 10 :

Set properties -> security

ssh -i C:\Users\pankajcha\Downloads\EC2instance.pem ec2-user@ 3.110.216.69