AWS :

2006 START

2013 Certification

NO Long term contract

U can stop anytime

Pay as much use

Region: Geographic area consist of 2 or more availability zone i.e. US east 1 , Us west 1, Australia ,….

Availability Zone: A data center.

Edge Location: CDN (Content distribution network) end point for cloud front

Cloud Front: Amazon CDN service.

50 Edge Location

North America: 3 different region :

1. Us east (North Virginia)
2. US west (California)
3. US West (Argon)

Networking :

1. VPC (Virtual private cloud)u can have multiple VPC
2. Direct Connect (Direct connection Without using internet connection)
3. Route 53(DNS service , 53 is a number where DNS seat )

Compute :

1. EC2 (Virtual server )
2. EC2 Container service( called as Amazon ECS )
3. Elastic Beanstalk( easy to use, deploying, elastic design to upload the code)
4. Lambda (Most powerful)

Storage:

1. S3(store a file , object based storage , place to stoare a flat based file , secure durable , scable , only pay for storage which is used)
2. Cloud Front( Amazon sub content delivery web service or CDN service , has different edge location , edge location is a place a cache a file )
3. Glacier (secure , durable , extreme low cost solution for data archiving and long term backup , offline storage its take 4 hours to access , Archiving service )
4. EFS (Elastic file system , file storage for EC2 instances , it is block label)
5. Snowball( amazon import and export service , send your hard drive data to aws platform )
6. Storage gateway (service connecting on premises software plans on virtual machine with cloud based storage).

Database:

1. RDS
2. Dynamo DB (no sql database)
3. ElastiCache(caching a most popular query in sql chache )
4. Redshift( BI service , )
5. DMS (Database migration service )

Analytics:

1. EMR( elastic map reduce , way of processing big data )
2. Data pipeline( moving data from one service to another )
3. Elastic search( Managed service , analytic engine )
4. Kinesis( streaming )
5. Machine learning( )
6. Quick Sight(BI service , visualization )

Security and Identity:

1. IAM
2. Directory service
3. Inspector
4. WAF(Web application file )
5. Cloud HSM (Hardware security module )
6. KMS(Key management servcie)

Management Tool:

1. Cloud Watch( monitoring tool , )
2. Cloud formation (script creation for creating cloud)
3. Cloud trail(use for auditing , change can be recorded in aws environment , )
4. OpsWorks ( configuration management service )
5. Config( configuration history )
6. Service catalog()
7. Trusted advisor(where can save money or can increase the sequrity )

Application service

1. API Gateway ( fully managed service to create publis managed api )
2. AppStream (application stream )
3. Cloud search( )
4. Elastic Transcoder( media transcoder to src format into the version in which it going to play in laptop , mobile …)
5. SES( Simple Email service , allow to send email and recive the mail )
6. SQS()
7. SWF(Simple work flow service , back groud job , )

Developer tool :

1. Code commit(like git)
2. Code deploy(like )
3. Code pipeline(continues delivery service )

Mobile service:

1. Mobile Hub
2. Cognito
3. Device farm
4. SNS ( Send Notification servce)

Enterprise Application:

1. Work space
2. Work Doc (drop box to store a file )
3. Work mail ()

Internet of thing(IOT)

1. Internet of thing

Arn(Amazon resource name )

**IAM**

Active Directory Authentication : Yes by using SAML

SSO (Single sign on)

SAML (secure assistive markup language)

Active directory authentication first then u assign the tempory credential

Web Identity Federation with mobile application:  
we can authenticate by using any social site

Fb verified authority then acces token given then temporary security credential

IAM consist of user Group and roles

IAm is effectively the management console for managing acces to aws resources for oragnisation

A user is an individual, group are a collection of user with one set of permission, rol;e can be applied to both user and AWS services(such as Lambda, EC2 )

How to create user group and role

How to enable multifactor authentication

How to create a single sign on link for user within organization

**Authentication :**

1. SAML 🡺 Secure Assertive Markup Language
2. Authenticate against identity provider (Facebook etc)
3. Obtain temporary security credential
4. Asume role with web identity
5. Able to access AWS resources.

EC2 instance user cant switch/ change the role of IAM but can change the permission .

**IAM 101 :**

* Manages User and there level of access to the AWS console
* Centralized control to your AWS account
* Shared access to your AWS Account
* Granular permission
* Identity Federation ( including active directive and Facebook )
* Multifactor authentication ( 2 level )
* Temporary access for user and service wherever needed)
* Integrates with many different AWS service.
* Supports PCI DSS compliance

Critical Term:

User: End user (think people)

Groups: A collection of user under one set of permission like hR , Account etc .

Roles:

Policies: (A document that define permission)

**How to setup :**

1. **Custamize the link**

* Login to AWS
* Change the region according to performance
* IAM is not a region specific
* Click on IAM
* IAM user sign in link by using this one can login for giving its alias name click on customize
* This alias name should be unique
* After this u can login by changed link

1. Activate MFA (motive factor authonticate) on root account

* Root account : is the email account when u setup a AWS account
* It has all the permission
* Click
* Manage MFA
* Hardware (RFA token )
* Select Virtual ()
* next
* next
* scan QR to mobile u will get 6 digit number
* put that and wait for other
* finish

1. Create Individual IAM user

* Click on IAM
* Create new user
* Enter name
* Create
* It will give different acess key and id
* Id : username e
* Key password
* Download it because we cant check it again
* Next
* Select user and click user action manage password
* Assign auto generated password working
* Download password
* close
* By default there is no permission to the new user we have to grant the permission
* Click on police for give permission
* There are lot of predefine police
* Click on particular police
* Select a police and then click on attach and then chechk the particular user

1. Create a group

* Provide name
* Attach the police to a group
* Create group
* Select user in group

1. Apply IAM password policey

* Click on IAM police
* Check according to your wish

Roles:

* Allows resource access
* Create
* Name
* Select role type
* Attach police to the role as required
* Next

**Putty and PuttyKeyGen**

Putty in order to access EC2 insentiences

PuttyKeyGEn : is used to convert to PAM (key pair file )file to putty doesnot support PAM file

* Go To AWS and launch Instance
* Select amazon linux ami
* Default
* Tag instances put value as putty
* Defulat
* Launch
* Crerate a new key
* And download (this is .pea file for acess we need to create )
* Got to putty gen
* Select download file
* Save private key
* Save it as .ppk file
* Open putty
* Go to Ec2 instence
* At down there’re is Ip address
* Login by using this ip
* And in ssh provide the PPK file