TRAINING CONTENT

Cloud Computing

YOUR NEXT DESTINATION

OF SOFTWARE OUTSOURCING

Lecture Outline

- Introduction to AWS Cloud
- Creating AWS account
- Free tier Eligible services
- Understanding AWS Regions and availability zones
- Elastic Compute Cloud (EC2)
- Simple Storage Service (S3)
- Elastic Block Storage (EBS)
- Relational Database System (RDS)
- Identity and Access Management (IAM)
- Scaling Types
- AWS Services Pricing

Lecture Outline

- DynamoDB
- SQS
- AWS Elasticcache (Redis)
- AWS Elasticsearch
- Route 53
- CloudFront
- AWS Serverless (Lambda and API Gateway)
- SNS
- CloudWatch
- WAF
- AWS Code pipeline – Code build, code deploy

What is Cloud Computing

Cloud computing

Most important use case :

- On Demand
- Scalability and flexibility
- Advanced security
- Data loss prevention
- Cost savings

Creating AWS Account

- Open the https://aws.amazon.com/
- Choose **Create an AWS Account**.
- Enter your account information, and then choose **Continue**.
- Choose **Personal** or **Professional**.
- Enter your company or personal information.
- Read and accept the AWS Customer Agreement.
  Note: Be sure that you read and understand the terms of the AWS Customer Agreement.
- Choose **Create Account and Continue**.
- On the **Payment Information** page, enter the information about your payment method and then choose **Verify and Add**.

AWS Cloud

- Why AWS
- History
- IaaS- EC2
- PaaS- AWS Lambda, S3
- SaaS- Amazon WorkDocs, Amazon Chime

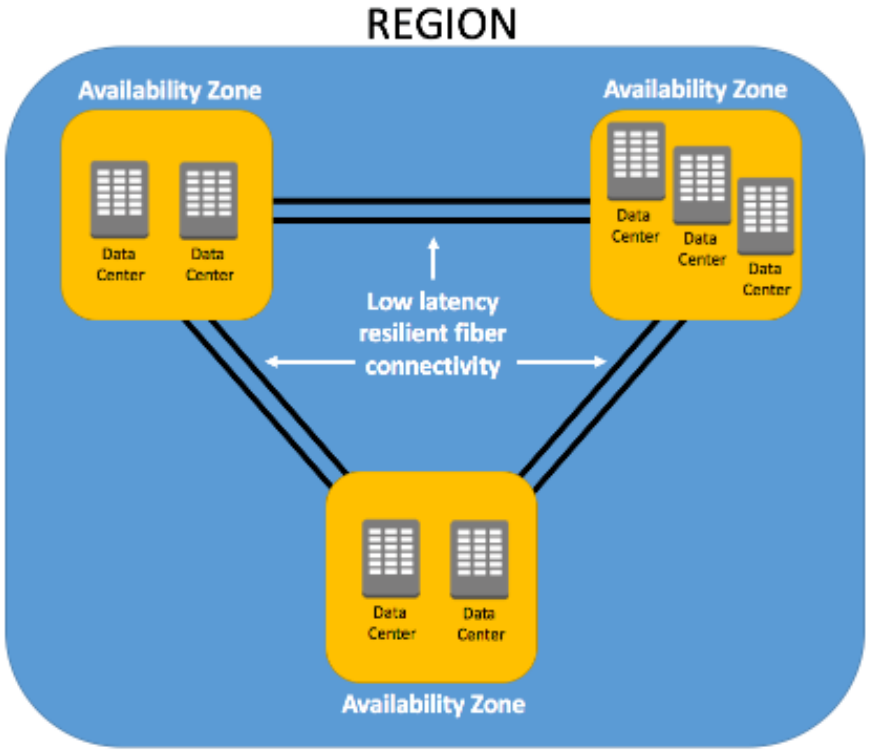
Free Tier Eligible Services

AWS offer more than 100 products and start building on AWS using the Free Tier. The AWS Free Tier includes services that are always free, free for one year, and shorter-term free trials.

Visit below sites to check free tier
https://aws.amazon.com/free/?enkwrd=Samsung

AWS regions and availability zones

AWS Regions are large and widely dispersed into separate geographic locations. Availability Zones are distinct locations within an AWS Region that are engineered to be isolated from **failures in other Availability Zones**.



IAM

- AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources. You use IAM to control who is authenticated (signed in) and authorized (has permissions) to use resources.
- Features:
  - Shared access to your AWS account
  - Granular permissions
  - Secure access to AWS resources for applications that run on Amazon EC2
  - Multi-factor authentication (MFA)
  - Free to use
  - Identity information for assurance
  - Password policy.
  - Integrated with many AWS services

Identity and Access Management (IAM)

- ***Users***: An AWS Identity and Access Management (IAM) user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS. A user in AWS consists of a name and credentials.
- ***Groups***: An IAM group is a collection of IAM users.
- ***Policy***: A policy is an object in AWS that, when associated with an identity or resource, defines their permissions.
- ***Role***: An IAM role is an IAM identity that you can create in your account that has specific permissions. An IAM role is similar to an IAM user, in that it is an AWS identity with permission policies that determine what the identity can and cannot do in AWS.
- ***Access Key***: Access keys are long-term credentials for an IAM user or the AWS account root user. You can use access keys to sign programmatic requests to the AWS CLI or AWS API (directly or using the AWS SDK).

IAM – Hands-on

- Create User
- Create Group
- Assign Policy