**AWS Class Notes**

**EC2 Dashboard**

**Features associated with EC2 Instances**

1. **Security Groups –** Required to create an EC2 instance
   1. What is the role of a security group?
      1. By Default, Security Groups will block all access into EC2 instance unless allowed
   2. How do you create a security?
   3. How to you associate a SG to an existing Server
2. **Instance Types**
   1. What is an instance type and how is it related to an EC2 instance?
   2. How do you change the instance type for an existing EC2 instance?
3. **EIP (Elastic Internet Protocol)**
   1. What is an EIP?
   2. How do you create an EIP?
   3. How do you associate it to an EC2 instance?
4. Snapshots
5. **AMI** (Amazon Machine Image)
   1. What is an AMI
   2. How to create a custom AMI from an existing EC2 instance
   3. How to Copy an AMI from one region to another
6. EBS (Elastic Block Storage)
   1. This is a storage volume
   2. The main storage within our EC2 instance
      1. Required for storing data
      2. Required for installing software
7. Snapshots
   1. How do we backup our EC2 instances
      1. The way to take backup of our EC2 instance/EBS Volumes
      2. A Snapshots is a recovery plan for an EC2 instance to restore in the event of a disaster.
   2. How do you create a snapshot?
      1. EBS volume
      2. EC2 instance
   3. How do we copy a snapshot from one region to another?
   4. How do you create an EBS volume from a snapshot?
   5. How do we create an AMI from a snapshot?
8. Backup in AWS
   1. RTO – Recovery Time Objective
      1. How much time can a server be offline/down?
      2. What is the downtime for a particular server/server?
   2. RPO – Recovery Point Object
      1. How much data can be lost for an EC2 instance in the even of a disaster?
      2. The specified time indicated by app team or respective development team will match the criterial for the backup plan. E.g Daily backup or Monthly backup
9. AMI – Amazon Machine Image
   1. How do you create an AMI from an EC2 instance?
   2. How do we launch/create an EC2 instance from a custom AMI?
      1. By launching from AMI
      2. By selecting “My AMI”
10. Lifecycle Manager
    1. Automate the backup of EC2 instances or EBS volumes
       1. Assigning custom tags to these resources and using the tags are backup source.

**Homework:**

How can you copy a snapshot from one AWS account to another?

1. Share with my account number 1727-7514-0033

IAM – Identity and Access Management Server

1. Authentication
   1. Ability to login into aws account
      1. Username/Password
   2. You say you are who you are.
2. Authorization
   1. What resources you are authorized to **view** or make changes (create/update/delete)
3. Users
   1. Authentication
      1. Programmatic
         1. No MFA
         2. Service accounts
         3. Comes with Access Key ID
         4. Comes with Secret Key
         5. SDK – software development kits
         6. APIs – Application programing interface
         7. CLI – Command Line Interface
         8. Third party tools or applications or some other programing languages. E.g java python, .net
      2. AWS Management Console
         1. Ability to login though the web browser (AWS console)
         2. Enable MFA (Multi-factor Authentication)
4. Roles
   1. Trust policy (Relationship)
5. Policies
   1. Authorization
      1. Written in JSON
         1. Set of rules(permission) granting or denying access into aws resources
6. Groups
   1. Set of users performing the same tasks
      1. Example – Administrators, Developers, Designers, Solutions Architect
   2. Assign the sample policy to every user in a group
7. ARN – Amazon Resource Name

VPC – Virtual Private Cloud

1. Networking in the cloud
   1. Two types of IP Address
      1. IPv4 (Internet Protocol Version 4)
         1. 5 Classes of IPv4
            1. A,B,C,D,E

Class A

First Octave ranges between 1-127

Class B

First Octave ranges between 128-191

Class C

First Octave ranges between 192-223

* + 1. IPv6 (Internet Protocol Version 6)

1. Security feature in AWS
2. Provides a network skeleton for some AWS resources
   1. Example – We need a VPC to create/provision for an EC2 instance
3. To understand Virtual Private Cloud, we need to know the basics of IP addressing
4. VPC CIDR (Network Range) = 10.0.0.0/8 (Thousands of IP addresses range/network) e.g Data center address
   1. Multiple Subnets
      1. 10.0.1.0/16
      2. 10.0.2.0/16
      3. 10.0.3.0/16

IP Addressing

1. 4 Octaves
2. 32bits
   * 1 octave = 8
   * 8.8.8.8=32
   * 3.86.84.185 (1 IP address)

**Requirement**

They want to build a 3-tier application in AWS

1st Tier

1. Elastic Compute Cloud Dashboard
   * Web Server Layer (Website)
     + Domain Name (FQDN – Fully Qualifies Domain Name) 🡪 [www.tngs.com](http://www.tngs.com)
   * EC2 Instance 🡪 WebServer
2. Publicly accessible
   * Public Subnet

2nd Tier

1. Elastic Compute Cloud Dashboard
   * Application Layer (Caching Server)
   * EC2 Instance 🡪 ApplicationServer
2. Privately accessible
   * Private Subnet

3rd Tier

1. RDS – Relational Database Service
   * Database Layer
2. Privately accessible
   * Private Subnet

**Solutions**

1. Build a network
   1. VPC
      1. Have a network for communication
   2. Subnets
      1. Separated chunks of VPC
      2. Multiple parts of a larger Network
         1. Public Subnet
         2. Private Subnet
   3. IGW
      1. Supplies internet to resources inside the VPC
   4. NAT – Network Address Translator/Translation
      1. Translate Communication between public and private resources
   5. Security Group
      1. Firewall behind ECS and Database
      2. By Default, will restrict/Deny all access unless allowed
      3. Allows users to connect to AWS resources
      4. Allows resources to communicate with each other
   6. Network ACL – Access Control List
      1. Firewall behind Subnets
      2. By Default, NACL will allow all access
   7. Route Tables
      1. Configuring traffic movement
2. We need at least 2 running EC2 instances

**Advantages of AWS**

Fault Tolerance

High Availability

* + Able to withstand/tolerate failure

1. **Load Balancer**
   1. Application Load balancer
      1. Prevent downtime in the event of a failure
      2. Serves as an extra layer on top of our applications/web servers for security reasons
      3. Distributing traffic to 2 or more servers – Balances traffic coming into the environment.
   2. Network Load balancer
      1. Does same thing as Application Load balancer but instead of balancer application traffic, NLB balancer Network traffic
      2. In times of high traffic NLB will help to distribute traffic to multiple targets equally to avoid any failure in the event of bandwidth overload.
         1. IOPS (input and output per second)
   3. Classic Load balancer
      1. Round robin Load Balancer
         1. Even distribution of service/request into the environment.

Question:

What features in AWS provides a highly scalable, fault tolerance and a highly available environment?

**Scalability**

* Multi Availability zone
  + Spread resources so if one AZ becomes unavailable, then we have other AZs as backup
* **Auto Scaling** 
  + Vertical Scaling
    - Scaling up (Increasing/adding) – t2.micro to t3.xlarge
    - Scaling down (Decreasing/subtracting) - t3.xlarge – t2.micro
    - Increasing or reducing size of a single EC2 instance (instance type – t2.micro)
    - Requires Downtime
  + Horizontal Scaling
    - Scaling out (Increasing/adding)
    - Scaling in (Decreasing/subtracting)
    - Adding or reducing the number of EC2 instance
      * E.g from 1 to 2 EC2 instance
    - Doesn’t require download

RDS – Relational Database Service

* Offers database service
  + Storing data
    - Structured/Organized
    - Unstructured/Not organized
  + Processing data
  + Stores data in the for of tables and columns
  + Used a language called sql to query, update, delete data
  + RDBMS (Relational Database Management system) – is a type of database that uses SQL to process data.
  + Example are mysql database, oracle database, Microsoft SQL Database
  + Multi-AZ should be applied to our production database servers
    - In case of a disaster, we will have a secondary backup server to retrieve data
    - Having 2 redundant db servers for same purpose, in case of an emergency
    - Disaster recovery
    - High Availability
      * Avoid downtime
        + Disaster recovery
        + Database patching
    - Scalability
    - Exact replica of each other
      * Realtime replication from primary database to secondary database

LAB - RDS (Relational Database management Service)

Requirements for Creating Database in the RDS

1. Network and Security

a. VPC

b. 2 public subnets

c. IGW

d. Security Group

2. Create a Subnet Group (Associate 2 public subnets)

3. Create a public database (MySQL Database) - **make it public**

5. Connect to public database using our local computer

Download and Install:

https://www.jetbrains.com/datagrip/download/#section=windows

Task: Create a MySQL DB and connect using datagrid

1. Navigate to Amazon RDS web service

2. Create database, and chose mysql (select free tier)

3. Give database name as mysqldb, user as admin, password as Admin123

4. Create db

5. Download and install Datagrid

6. Open datagrid

71. Connect using database parameters

Cloudwatch Service

* Monitoring service in AWS
* Use to measure performance feature in AWS

2 types of cloudwatch monitoring

1. **Basic Monitoring** 
   1. Its free
   2. Pulls updates every 5 minutes
   3. 10 metrics available for monitoring
   4. 5GB of data ingestion
   5. 5GB of data storage
2. **Detail Monitoring** 
   1. Chargeable
   2. Charger per aws service monthly
   3. Pulls data every 1 minute

Simple Notification Service (SNS)

What is the difference between cloudwatch and cloudtrail.

Answer:

Cloudwatch is a monitoring service while cloudtrail is a auditing service

In cloudwatch we use custom metrics to capture the activities of our EC2 instances, like CPU, Networkin/out and set notification or event rules base on these activities

Cloudtrail is capturing all AWS API calls…..capturing all activities that occurs in our AWS account

With Cloutrail we can also store all logs for the activities in s3 storage.

**Storage In AWS**

There are 3 main types of storage in AWS.

1. **S3 – Simple Storage service**
   1. Cheapest in cost
   2. By default, data stored in S3 is replicated across 3 Availability zones
      1. High Availability meaning if one AZ goes offline then we have 2 more redundant copies of our data.
   3. Includes multiple tiers of storage classes base of cost frequent access
   4. File and data storage type
   5. Host a static website
   6. S3 Glacier to store long term data that does not require short term retrieval
   7. We cannot mount on EC2 Instance, but we can move data to and from S3 to EC2 instance
   8. We great parent folder called Bucket
   9. Every bucket in created in a specific region
      1. S3 Buckets are region specific
2. **EFS – Elastic File System**
   1. It is the middle class storage between S3 and EBS
   2. It is cheaper than EBS but more expensive than S3
   3. EFS can be mounted on multiple Linux EC2 instance
   4. Cannot be mounted on Windows
3. **FSx file system**
   1. **–** Can only mount on Windows servers.
4. **EBS – Elastic Block Storage**
   1. Block Storage
      1. Type of storage required for Operating system or software installation
      2. Store data and metadata (information about data like size, date created type of file etc)
   2. Block storage is required to spin a new EC2 instance/server
   3. Fast in processing data
   4. Costly more than EFS and S3
   5. EBS volume is prized based on allocated storage while EFS and S3 are prized based on usage (Pay as you go)
   6. We can attach and mount on a single EC2 instance at a time.