**Global service and Regional service**

**IAM Lab**

- Least privilege

- Add an user.

- Programmatic access and console access

- Access keys and secret keys - Not the same as password, you cannot login into Console with access keys.

- Best practices - Rotate access keys.

- Password policies

- New users have no permissions.

- MFA

End users accessing AWS resources.

**S3 Lab**

1. Versioning lab

2. Lifecycle Management with S3

- Under Management tab

- Filters - Image prefix

- Transition to more than one storage classes

QwikLabs: https://run.qwiklabs.com/focuses/15683?catalog\_rank=%7B%22rank%22%3A5%2C%22num\_filters%22%3A0%2C%22has\_search%22%3Atrue%7D&parent=catalog&search\_id=8643764

3. Security

- Upload an object to S3.

- Manage Bucket level permissions

- Manage object level permissions

4. Encryption

- Encrypt an object

- Select the object and scroll down

- Encrypt the bucker

- Properties > Default Encryption

5. Cross Region Replication

- Management tab

6. CloudFront

- Serve the images from S3 bucket using CloudFront

**EC2 Lab**

1. Launch an EC2 instance - Create a web server.

Terms:

- AMI

- Bootstrap scripts

- EBS volumes

- Security Groups

- Allow port 22 and port 80

- Key pair

- Enable public IP

- Turn on Termination protection.

apt update -y

apt install apache2 -y

cd /var/www/apache2/sites-enabled/

create a index.html

<html><h1> My First Web server </h1></html>

sudo service apache2 start

sudo service apache2 enable

- Overview, Status, Monitoring and Tags tabs. - Detailed Monitoring

- Terminate the instance

- Instance settings > Change Termination protection

- Purchase Reserved Instances

2. Security Groups Demo -

- Change HTTP port for web server - Reflects change immediately.

- Delete Outbound rules - Stateful

- Cannot Block Ports/ Blacklist IP

3. EBS Volumes

- While launching an instance.

- Root volume can only be gp2.

- Additional volumes can be added and encrypted.

- Turn Default off Delete on Termination.

- Root volume is removed automatically.

- Modify root volume (increase only) or add an additional volume.

- Modify root volume type.

- Copy AMI to different regions.

- Create a snapshot of the volume. Create an AMI (Image)

- Create a Image of the snapshot.

- Copy AMI to a different region.

- Create a new instance from copied AMI.

4. Encrypted Volumes and snapshots.

- Additional volumes

- Create an instance without encryption enabled.

- Actions > Create Snapshots.

- Snapshot > Copy > Encrypt this snapshot.

- Create an image from the snapshot

- Launch an instance from the AMI.

- Enable encryption while launching an instance.

5. AMI types Demo

- Launch an instance with EBS volumes.

- Launch an instance from Community AMI > Instance store

- Instance volume is not seen on Console.

6. AWS CLI

- Create a new user and assign programmatic access.

- Login into an instance.

- aws s3 ls and aws configure

- cd .aws, cat config and credentials --> Not safe

7. IAM Roles

8. Using Bootstrap scripts

9. Instance Metadata

10. EFS Lab

- Create an EFS filesystem.

- Launch 2 EC2 instances.

- Open NFS port on EC2 instance security group.

- SSH into both instances

- EFS console > Mount instructions from Local VPC

- Create a file on one server and the change should be reflected on the other.

11. CloudWatch

- Enable cloudwatch detailed monitoring while launching the instance.

- Create an Alarm

- while true; do echo; done

- Events

12. EC2 overall

- Create an IAM role with S3 full access.

- Create a Security group with tags and related rules.

- Create an EC2 instance and attach the role to EC2.

- Enable encryption and termination protection.

- Attach the security group to the instance.

- Configure aws cli in the EC2 and test S3 permissions.

Use this script.

apt update -y

apt install apache2 -y

cd /var/www/apache2/sites-enabled/

create a index.html

<html><h1> My First Web server </h1></html>

sudo service apache2 start

sudo service apache2 enable

- Create a directory and a file name.

- Cloudwatch metric status.

- Create an AMI, move to another region and launch an EC2 instance there.

**Database Lab**

1. Creating the first DB instance.

- Create a free tier RDS instance.

- Login into Database instance

- **psql -U cubedstepsadmin -h "cubedsteps-training.cz3o048gih14.us-east-1.rds.amazonaws.com" -d cubedsteps**

- Modify the database

- Turn on Multi-AZ

- Configuration - Multi AZ

- Can force reboot to failover to another AZ.

- Create read replica, cannot.

- Modify the database

- Turn on automatic backups, retention period to 35 days.

- Actions > Create a read replica.

- Promote to a stand alone database.

- Delete the read replica.

- Notes:

- RDS is not serverless. RDS runs on virtual machines.

- Aurora Serverless is serverless.

- You cannot log in to the operating system.

- Patching and maintenance of Operating system and Database is AWS's responsibility.

**Advanced IAM**

- Share Aurora DB clusters

**VPC Lab**

- Default VPC

- Default VPC

- Default Subnets

- Default Route Table

- IGW

- NACL

- Security Groups

- Create a Custom VPC

- 172.16.0.0/16

- 172.17.0.0/16

- 172.18.0.0/16

- 172.19.0.0/16

- 172.20.0.0/16

- Tenancy - Default/Dedicated

- Route Table, NACL and Security groups are created by default

- Create a Subnet

- Choose AZ.

- 172.16.10.0/24

- Create another Subnet

- Choose AZ.

- 172.16.20.0/24

- cidr.xyz

- 172.16.0.0: Network Address

- 172.16.0.1: Reserved by the VPC Router

- 172.16.0.2: Reserved for DNS Server

- 172.16.0.3: Reserved for future purposes

- 172.16.0.255: Gateway Address

- Make a subnet public.

- Create an EC2 instance in the subnet.

- Internet access to the subnet

- Create an internet Gateway

- Attach an internet gateway to VPC.

- Create a route table

- Add an entry on the route table.

- Associate a subnet to the route table.

- Launch an instance in a private subnet

- Create necessary security groups.

- SSH from Public.

- Introduce NAT gateway.

- Create a route to NAT GW

- NACL Lab

- Create a NACL.

- All Inbound/Outbound rules are Denied by default.

- Rule #1 to #65536

- Associate Subnet to NACL.

- A subnet can be associated with only one NACL.

- A NACL can have multiple subnets associated with it.

- Ephemeral ports - 1024 - 65535

- A NAT Gateway used uses ports 1024 - 65535

- Deny port 22 from my-ip. Rules are evaluated on priority.

- NACL changes are immediate.

- NACL is evaluated before security groups.

- VPC Flow Logs

- VPC > Select VPC > Actions > Enable FLow Logs

- VPC Peering

- Send Peering Request from Source VPC

- Accept Peering request from Destination VPC

- Add entries in the route table for both VPCs.

- VPC Endpoints

- Create a VPC endpoint for S3.

- Use endpoints from EC2 instances.

**Route53**

--> Simple Routing Policy

- Create 3 EC2 instances.

- Bootstrap script:

apt update -y

apt install apache2 -y

cd /var/www/apache2/sites-enabled/

create a index.html

<html><h1> Hello World ! This is <region> server </h1></html>

sudo service apache2 start

sudo service apache2 enable

- Create a hosted zone as training.jyatha.com and enter three IPs. Reduce the TTL to 1 min.

--> Weighted Routing Policy

- Create three different record sets.

- Create 3 Health checks for all record sets

--> Latency based routing

--> Failover routing policy

- Create failover record sets.

- Fail primary site on purpose.

--> Multivalue Answer

- Stop the instance and that will be removed from the list.

**Parameter Store**

- Create three different keys

- /prod/db/

- List of string - Servers Name, Cube1, Cube2, Cube3

- DB Password