Lab 1 - AWS,EC2,EBS and S3

Week 1 Tasks:

a) AWS Management Console

b) Understanding and creating AWS EC2(Elastic Compute) virtual machines

Deliverables:

i. 1b1.png showing the summary of instance before launching (*Step 7: Review Instance Launch*)
ii. 1b2.png showing the EC2 instance in running state
iii. 1b3.png should be a screenshot of the SSH terminal, showing compiling and running a sample C program

c) Understanding and using AWS EBS(Elastic Block Store)

Deliverables:

i. 1c1.png showing the newly created EBS in an *available* state.
ii. 1c2.png showing the created EBS attached to an EC2 instance. The screenshot should be showing all the volumes of the EC2 instance on the EC2 management console.
iii. 1c3.png should show an output of the terminal, by running a linux command showing all the volumes, file systems and size attached to the EC2 instance.
iv. 1c4.png should the newly created *snapshot* on the management console
v. 1c5.png showing the newly created *volume* from the created snapshot

d) Object Storage using S3 Buckets

Deliverables:

i. 1d1.png showing the uploaded image using the public URL(URL must be clearly shown)

ii. 1d2.png showing different versions of the text file in the bucket overview

iii. 1d3.png showing the modified text file using the public URL of the file(URL must be clearly shown)

Task a : AWS Management Console

Before getting into the details of this lab (and further labs) it is important to be familiar with the central hub/point of AWS , the AWS Management Console. Take a read in the link to understand what you can do with the console.

What is AWS ?

Working with the AWS Management Console

All AWS services can be accessed using the AWS management console, take a look around the console and the services and familiarise yourself with the environment!

Questions:

1. The AWS management console is a web app to interact with AWS services. What other ways are there to interact with AWS services?

Task b : Understanding and creating AWS EC2(Elastic Compute) virtual machines

One of the most important is the AWS EC2 (Elastic Compute) service. This provides the actual ***compute*** for your cloud applications and as any cloud service should be, scalable(hence the name elastic!). EC2 is a service that provides resizable compute capacity in the cloud. It is designed to make web-scale cloud computing easier for developers.In simpler words EC2 is none other than a virtual machine.

Understanding AWS EC2 - 4 minute video explaining AWS EC2

Every EC2 instance has the following properties/options/attributes that need to compulsorily be configured:

- Amazon Machine Image(AMI)
- Instance Type (The Instance Type usually depends on the use of the VM)
- Specific Instance Details such as network,subnets,start up scripts etc.
- Security Groups - These are essentially the firewalls to your instance, they control the access to your instance.

The following steps will help you in setting up a EC2 instance. Make sure you really understand how to create an EC2 instance as EC2 will be used throughout this course

1. Make sure you have your AWS Educate credentials ready, you would have received a mail from AWS Educate to register and sign up and then change your password.
2. Once mail is received, login to AWS Educate. Go to AWS Management Console page. Under ‘Services’ tab, click on EC2.
3. You’ll reach the EC2 console page. Click Launch Instance.

4. Here you'll be presented with a list of Amazon Machine Images (AMI). They're essentially the virtual OSes that will run your server. We recommend you pick Ubuntu as you're likely to be familiar with its command line tools and package manager.
5. Now you'll be presented with a list of Instance Types. Each one has different machine specs like number of vCPUs, size of memory, storage volume type, etc. Pick one that is appropriate to your needs. For this a t2.micro(free tier eligible) is good enough.You can leave the default settings in the Configure Instance, Add Storage, and Add Tags pages, or configure it according to your needs.
6. On the Configure Security Group page, make sure you allow traffic on SSH and HTTP. Make sure to also install an SSH client on your local machine. This is a critical step whenever setting up an EC2 instance as this defines the access to your instance from the internet!
7. Create a cryptographic key pair and download the private key to your system. Then launch the instance. You may need to change the permissions of the PEM key.
    a. PEM Key Permissions
8. Change the instance name to your SRN
9. Learn about how to remotely login to another machine using SSH.
    a. SSH Basics
10. Find the public DNS for your instance. Use that and the private key to SSH into your instance. You'll need to figure out what the default username of your VM is, and how to point your SSH client to the private key.
    a. SSH into AWS instances
    b. General prerequisites for connecting to your instance
11. To delete an instance select the instance, choose *Instance State* and in the dropdown select *Terminate Instance*.

Note: AWS Educate probably does not allow you to create all kinds of instances. Make sure it's EC2. And ensure your Region is "US-East"(Northern Virginia). AWS Educate does not work for any other region.

Your task is to create an EC2 instance with the following configurations/settings:

AMI	Ubuntu Server 20.04 LTS (HVM), SSD Volume Type
Instance Type	t2.micro
Instance Details	Default values (But try to understand what the different options are)
Storage	Default values

You may get a warning saying “Improve your instances' security. Your security group, launch-wizard-1, is open to the world”, you can ignore this for now.

1. After creating and getting into your EC2 instance, update the “apt” package, and install GCC compiler.
2. Write a simple C program and compile it.

Questions to think about:

1. What happens when you *stop* an instance? How is it different from *terminating* an instance?
2. How are EC2 instances charged? How does it come under the pay-per-use model of cloud computing?

Task c : Understanding and using AWS EBS(Elastic Block Store)

Before getting into AWS EBS, it is important to understand what a block store is and how they are different from other types of cloud storage: What is Block Storage?

Think of EBS as the hard drive (SSD or HDD) that you have in your laptop.Amazon EBS offers persistent storage for Amazon Elastic Compute Cloud (Amazon EC2) instances. Amazon EBS volumes are network-attached and persist independently from the life of an instance. Amazon EBS volumes are highly available, highly reliable volumes that can be leveraged as an Amazon EC2 instance boot partition or attached to a running Amazon EC2 instance as a standard block device. Think of EBS as the hard drive (SSD or HDD) that you have in your laptop.

The following links will help you understand EBS in a good amount of detail:

Amazon Elastic Block Store (EBS) Overview

Amazon Elastic Block Store

- EBS Volume console can be accessed through the EC2 console. Go to the EC2 console , on the right hand side *Elastic Block Store -> Volumes.*
- To check the volumes attached to your instance, select the instance on the EC2 console, on the button you will see

Another important feature/concept of EBS is to create snapshots.You can back up the data on your Amazon EBS volumes to Amazon S3 by taking point-in-time snapshots. Snapshots are incremental backups, which means that only the blocks on the device that have changed after your most recent snapshot are saved.But note that although the EBS snapshots are stored in S3 buckets, you don't have access to this bucket as AWS abstracts those details from you as all you need are the snapshots.

Amazon EBS snapshots - Amazon Elastic Compute Cloud

Your sub tasks are to:

1. Create an EC2 instance with the below mentioned specs.The instance name should again be your SRN.
2. Create an EBS volume with the below mentioned specs. Check in the EBS console, the volume you have just created should have an “available” status, indicating it is ready to be attached to an EC2 instance. Name the EBS volume as SRN_ebs
3. Now, *attach* the created EBS volume to the created EC2 instance. Remember every EC2 instance already has a *boot volume EBS* , what you are *attaching* is an additional volume.

   Attaching a volume to an EC2 instance is analogous to just connecting a bare hard drive to a system without any file system,information etc. It is only physically connected but the OS needs more than just a physical attachment , i.e it needs a (1) Mount Point and (2) File system information of the volume.

4. SSH into the EC2 instance
5. Check to see the currently attached volume, can you see it?
6. Find the name of the block device from the shell. lsblk-command-in-linux.
7. Create a file system on the created EBS volume as per specifications. You need to create a file system on the new volume, don't modify any other file systems on any other volumes.
8. Create a directory on the host system(as per specs) and mount the file system-formatted volume to that directory.
9. List the current disks attached to the EC2 instance using the `df -h` command.
10. Snapshot the previously created volume:
    a. Give the description as: “Snapshot of my volume”
    b. Key: “Name”
    c. Value: “YOUR SRN_ebs”
11. Using the snapshot you just created, create another volume of 10 GiB. Name the newly created volume as “SNAPSHOT”

The specifications for the EBS volume are:

Volume Type	General Purpose SSD (gp2)
Size (GiB)	10
Availability Zone	Same availability zone as the EC2 instance
Encryption	Default(No Encryption)
File System	ext3
Mount Directory on host	/mnt/data-store

EC2 instance specs:

AMI	Ubuntu Server 18.04 LTS (HVM), SSD Volume Type
Instance Type	t2.micro
Instance Details	Default values
Storage	Default values

Note: Ensure the created EBS and EC2 volume belong to the same availability zone otherwise you will not be able to attach the volume

Creating an Amazon EBS volume - Amazon Elastic Compute Cloud

Creating & Attaching additional EBS

Viewing volumes and filesystems in Linux

Mounting volumes to directories in Linux

Questions:

1. Is there any relationship between an Amazon AMI and the EBS ?

   Hint: Think about the default EBS attached to the volume, what all should it have configured?

2. What are the different types of EBS volumes available? What kind of volume is used as the *boot volume* ? What should the different types be used for?
3. How many volumes can you attach to a single EC2 instance? What factors does this depend on?
4. What is the lifetime of an EBS volume? Is/Can an EBS volumes lifetime be bound to the lifetime the EC2 instance it is attached to?
5. Can a single volume be bound to different EC2 instances?

Task d : Object Storage using S3 Buckets

Before getting into AWS S3, it is important to understand what an object store is and how they are different from other types of cloud storage: What is object storage?

Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. This means customers of all sizes and industries can use it to store and protect any amount of data for a

range of use cases, such as websites, mobile applications, backup and restore, archive, enterprise applications, Internet of Things (IoT) devices, and big data analytics. Amazon S3 provides easy-to-use management features so you can organize your data and configure finely-tuned access controls to meet your specific business, organizational, and compliance requirements. Amazon S3 is designed for 99.999999999% (11 9's) of durability and stores data for millions of applications for companies all around the world.

Introduction to Amazon S3

AWS Cloud Object Storage

This lab on AWS S3 will focus on two parts:

1. Creating an S3 bucket,adding a file,modifying access
2. Enable and use versioning for objects in S3.

Your sub-tasks for 1 are to:

1. Create an S3 bucket with a unique name as per specs.
    a. How do I create an S3 Bucket? - Amazon Simple Storage Service
2. Upload an image file(mentioned in specs) to the S3 bucket.
    a. Uploading an object to a bucket - Amazon Simple Storage Service
3. Get the public URL for the uploaded image and check access by pasting the URL into a browser.
    a. How do I see an overview of an object? - Amazon Simple Storage Service
4. Change access of the bucket to allow objects to have public access.
    a. Change bucket public access
5. Make the object *public* so as to allow public access. Check access again in a similar manner as sub-task 3.
    a. Grant public read access to some objects in my Amazon S3 bucket

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures.

Object Versioning - Amazon Simple Storage Service

Using versioning - Amazon Simple Storage Service

Your sub-tasks for 2 are to:

1. Use the same S3 bucket in the previous step.
2. Enable bucket versioning for the previously created bucket.
    a. How do I enable or suspend versioning for an S3 bucket? - Amazon Simple Storage Service
3. Download the sample text file(mentioned in specs)

4. Upload the sample text file to the bucket, enable public access for the object and check public access.
5. Now modify the sample text file as follows:
    a. Add a new line to the file mentioning “This is version 2 of the file”
    b. Add a new line saying “My SRN is “ <Your SRN here>.
    c. Do not change the file name, if you change the file name the bucket will treat it as a different file
6. Upload the modified text file to the S3 bucket.
7. Enter the same URL of the text file as you did before uploading the modified text file - you should see the updated text.
8. Go back to the bucket overview page and ensure that the *List Versions* toggle is on.
9. Under the sample text file uploaded, a new line appears showing the older version of the text file.
10. Try to access the older version of the text file.

S3 bucket specs:

Bucket Name	Your SRN, letters of your SRN must be in small case
Image file	new-report.png
Text file	sample-file.txt

Few points to note:

1. Download the image and text file to your system before uploading to S3, don't change the file names while downloading.
2. Ensure the screenshots you upload clearly show the S3 object URL.

Questions:

1. This lab dealt with image and text files. What kind of objects can be uploaded to S3? Are there any types of objects you can’t upload to S3?
2. Is there any size limit for the S3 bucket? What is the largest size a single object can have in a S3 object?
3. Think of an application that uses S3 buckets to store user images. This application is used across continents(Americas,Europe,Asia). Should you use the same bucket across regions or multiple buckets across regions ? How would you do the latter?

Lab 2 - Web Server, Firewall Access, Monitor Cloud Usage, Beanstalk, RDS

Introduction:

Welcome to Lab 2! In this lab you'll learn how to set up a web server and host a web page. You'll learn how to Setup firewall rules. You'll also learn to monitor cloud usage.

General Instructions:

1. Ensure your AWS Educate account is set up, in case of any issues contact your lab in-charge.
2. Evaluation for the labs will be mixed, few labs will involve uploading screenshots and few might be auto-evaluated.
3. All the screenshots (for each task as mentioned in this document) and any other deliverable (as applicable to the experiment and mentioned in the instructions) must be uploaded to Edmodo before the stipulated deadline.
4. Every task has a number of questions, these will **not** be evaluated unless you are explicitly asked to submit the answers but are extremely important in understanding the concepts.
5. Try to solve the tasks by yourselves, all relevant information to complete the tasks have been provided. Watch demo video pertaining to this experiment. In case you are stuck and not able to solve the issue, feel free to ask your doubts on Edmodo or send email to your lab incharge or pesu_cc_lab_support@googlegroups.com

Task A:

Objective:

The Objective of this task is to setup up a web server on the AWS EC2 Instance and host a sample web page on the instance. You are also required to load test the web page by using ApacheBench and monitor the EC2 instance using AWS CloudWatch service

1. Create a EC2 Instance

Deliverables:

i. 1a.png Showing that Instance is Running

2. Install Apache web Server on AWS EC2 Instance

Deliverables:

i. 2a.png Showing that apache server status is active

3. Setup Firewall Rules

Deliverables:

i. 3a.png showing the list of rules updated

ii. 3b.png SS of the local browser showing EC2 Instance's Apache2 Ubuntu Default page (Use EC2's public DNS)

4. Host a Sample web page

i. 4a.png SS of the hosted webpage(Should be accessed from your local computer)

5. Apachebench and Cloudwatch

i. 5a.png SS of the Apachebench output report After complete Execution

ii. 5b.png SS of the All set of graphs.

iii. 5c.png SS of cpu utilization

- **Reading –** 20 mins
  - What is a Web Server? : Understand what a web server is.

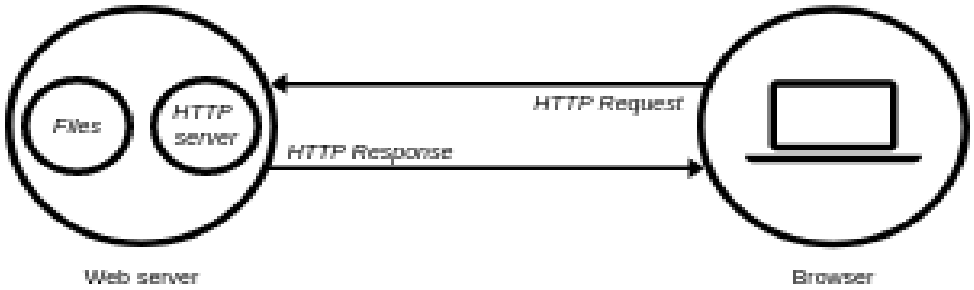
Sub Task 1: Launch a AWS EC2 Instance

- Launch a EC2 instance with the below Mentioned Configuration
- Follow **lab 1** steps to launch the instance.

EC2 instance specs:

AMI	Ubuntu Server 18.04 LTS (HVM), SSD Volume Type
Instance Type	t2.medium
Instance Details	Default values
Storage	Default values

Sub Task 2: install apache web server on the instance



It is important to understand the concept of web server before we jump into installing one.

The term web server can refer to hardware or software, or both of them working together.

- **On the hardware side**, a web server is a computer that stores web server software and a website's component files. (for example, HTML documents, images, CSS stylesheets, and JavaScript files) A web server connects to the Internet and supports physical data interchange with other devices connected to the web.
- **On the software side**, a web server includes several parts that control how web users access hosted files. At a minimum, this is an HTTP server. An HTTP server is software that understands URLs (web addresses) and HTTP (the protocol your browser uses to view webpages). An HTTP server can be accessed through the domain names of the websites it stores, and it delivers the content of these hosted websites to the end user's device.

Why Apache Web Servers?

Apache is considered open source software, which means the original source code is freely available for viewing and collaboration. One of the pros of Apache is its ability to handle large amounts of traffic with minimal configuration. It scales with ease and with its modular functionality at its core, you can configure Apache to do what you want, how you want it. You can also remove unwanted modules to make Apache more lightweight and efficient.

steps:

- SSH to the instance
- install Apache2
- check the apache2 status

Sub Task3: Setup Http and Firewall access

Normally, Amazon computers only allow shell logins via ssh (port 22 access). If we want to run a Web service or something else, we need to give the outside world access to other network locations on the computer.

Steps:

- Find “Security Groups” in the lower pane of your instance’s information page, and click on “launch-wizard-N” hyperlink
- Edit the Inbound Rules
- Add a new rule: HTTP, 80, Source Anywhere and save them.
- Wait for few seconds and copy paste the Public DNS of your instance in your local browser. You should be able to see apache2 home page.

Refer this link for detailed explanation.

Sub Task4: Host a Sample Web page

- You need to host a simple html Web Page in your instance using Apache Web Server and you should be able to access that webpage from your local web browser
- Create a Folder inside your “\var\www\html\” folder of your instance
- Name the folder by your SRN
- Create a simple html Page having your Name and SRN
- Access the Webpage from your local Browser using Your Instances PUBLIC DNS.

Sub Task5: Apache Benchmark and Cloudwatch

What is Apachebench?

ApacheBench is a single-threaded command line computer program for measuring the performance of HTTP web servers. Originally designed to test the Apache HTTP Server, it is generic enough to test any web server.

What is AWS Cloudwatch?

Amazon CloudWatch is a monitoring and management service that provides data and actionable insights for AWS, hybrid, and on-premises applications and infrastructure resources. With CloudWatch, you can collect and access all your performance and operational data in form of logs and metrics from a single platform.

Step

- In this task you are supposed to create load on your web server which you have setup on the ec2 Instance by using apachebench from your local computer.
- Then Monitor the load using Amazon cloudwatch(By enabling Detailed Monitoring)

- Identify the available metrics
- Vary the load using Apachebench,Following Load should be generated :
    - Users:10 Hits: 2000
    - Users: 20 Hits: 4000
    - Users: 30 Hits: 6000
    - Users: 40 Hits: 10000
- Identify the Metrics Whose values are changing and Take Screenshot of the Graphs.
- In order to monitor CPU Utilization Install stress-ng on your ec2 instance and then Create stress load of 60% and 80%. Take SS of CPU utilization curve.

Reference Link:

- Apachebencmark
- Cloudwatch your EC2 Instance (Look for enabling Detailed Monitoring for an existing EC2 Instance)

TASK B: Deploying Flask app On AWS Elastic Beanstalk

Objective:

In this task you'll be asked to create a AWS Elastic Beanstalk environment and deploy the flask application provided to you. You are required to configure a RDS along with your Beanstalk environment and create a few tables and databases.

Deliverables:

1) B1.png SS of Environment Health
2) B2.png SS of DB configuration(RDS)
3) B3.png Register User Request(Postman SS)
4) B4.png Verify User Request(Postman SS)

What is AWS Elastic Beanstalk?

AWS Elastic Beanstalk is an orchestration service offered by Amazon Web Services for deploying applications which orchestrates various AWS services, including EC2, S3, Simple Notification Service, CloudWatch, autoscaling, and Elastic Load Balancers.

AWS Elastic Beanstalk is an easy-to-use service for deploying and scaling web applications and services developed with Java, .NET, PHP, Node.js, Python, Ruby, Go, and Docker on familiar servers such as Apache, Nginx, Passenger, and IIS.

Flask is a lightweight Web Server Gateway Interface WSGI web application framework that was created to make getting started easy and making it easy for new beginners. With the tendency to scale up to complex applications.

FLASK?

Flask has its foundation around Werkzeug and Jinja2 and has become one of the most popular Python web application frameworks.

As a developer in developing a web app in python, you may be using a framework to your advantage. A framework is a code storage that should help developers achieve the required result by making work easier, scalable, efficient and maintainable web applications by providing reusable code or extensions for common operations.

References:

1. Elastic Beanstalk – Deploy Web Applications
2. Introduction to AWS Elastic Beanstalk

Note: In this Experiment you'll be provided with two files

a) **requirements.txt** having the list of libraries required by the flask app.
b) **application.py** Flask application file having two API's.

Steps:

1. Launch a AWS Beanstalk environment.
    a. Choose sample application code.
    b. Setup Application and Environment name (Application name should be your SRN).
    c. Select the environment type.

Reference for Step1.

2. Adding an Amazon RDS DB instance to your environment
    a. Setup Username(It should be your SRN) and Passwords
    b. Setup a MySQL Instance.
    c. After creating RDS, goto RDS instance info page
    d. Edit the securitygroup of your RDS Instance like you did in TASK A for EC2 Instance. Edit the Inbound rules to allow traffic from Anywhere.

Reference for Step2.

3. Write a Python Script to connect to RDS Instance Then you need to create a Database and Table in the RDS Instance.

a. Create a DB of your Name Make changes in the application.py based on it.
b. Create a table in that DB as follows:

i.
```
CREATE TABLE New_Users (
    Personid int NOT NULL AUTO_INCREMENT,
    username varchar(255),
    password varchar(255),
    age INT,
    mobile_number varchar(10),
    PRIMARY KEY (Personid)
);
```

4. Deploy the Flask App on Beanstalk.(Deploy using GUI)

   Watch this video to make your life simpler.

5. The Flask App has two REST API's One API is used to register Users And Another API is used to verify the registered user.

   i. API- Register User

      1. JSON Input

```
{
   "uname":"Ram",
   "pswd":"qwerty",
   "age":22,
   "mob": 8050569402
}
```

      2. Accepted Method: POST

   ii. API- Verify User

      1. JSON Input

```
{
   "uname":"UserName",
   "pswd":"Password"
}
```

      2. JSON Output (ID, Username, Password, Age, Mobile Number)

```
[
    6,
    "UserName",
    "Password",
    22,
    "8898734571"
]
```

3. Accepted Method: POST

6. Test the API's in the deployed Application Using POSTMAN. Create your own User and verify the user. SS needs to be taken.

   Reference for postman

Lab 3 - Virtual Private Cloud and migration of your existing application into the VPC.

a) Create Virtual Private Cloud Network, create subnets across availability zones, understand connectivity within and between subnets. Understanding NAT, ACLs and Routing Tables.

-70 points

- Deliverables: 5 screenshots (3a-3e).png

b) Migrate application developed earlier on elastic beanstalk to VPC. Use both public and private cloud (Hybrid Cloud): Load balancer in the public cloud and the application along with the database resides in the private cloud.Migrating your existing application on Beanstalk into the VPC -30 points

- Deliverables: 1 screenshot (3f)

Create Virtual Private Cloud and learn its features

- **Reading –** 20 mins
  - Virtual Private Cloud : Make sure to go through benefits and use cases
  - What is Amazon VPC? : Understand Key concepts for VPCs

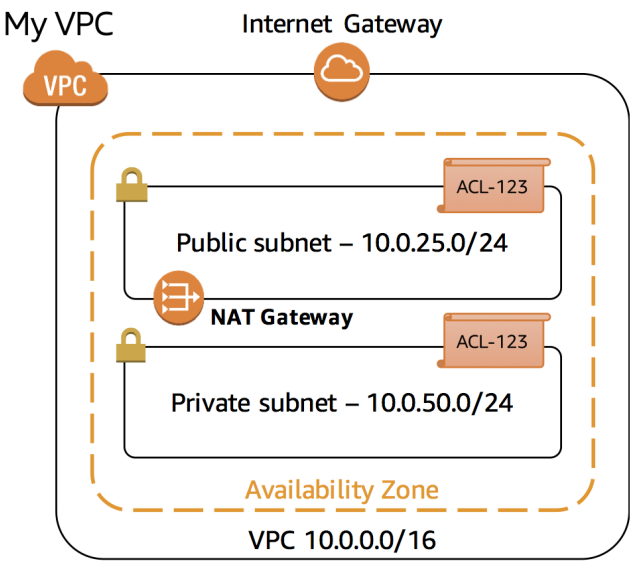
Task 1: Create an Elastic IP address - -5 min

- Under services in the AWS management console, click on VPC
- Allocate an elastic ip address with default settings.
- Take a screen shot with the allocated elastic ip address (3a.png)

Task 2: Create a VPC -35 mins

- Go to the VPC dashboard and launch the VPC wizard. The wizard makes your life much easier.
- Understand all the 4 VPC configurations

- Understand NAT gateways: NAT gateways - Amazon Virtual Private Cloud
- Create a **VPC with public and private subnets (Launch VPC wizard as shown in the demo video)**
- Configure the following:
    - VPC name: (your_name)_VPC
    - Public subnet IPv4 CIDR : 10.0.x.0 /24 (x: any number)
    - Private subnet IPv4 CIDR: 10.0.y.0/24 (y :any number)
    - Note: The availability zones should be the first in the list
    - Allocate the elastic ip address you created earlier.
- Create your VPC and click ok. Go to **Your VPCs** section and look at the details of the VPC you just created. Take a screenshot (3b.png)
- Internet gateway connects your VPC to the internet. Check if the gateway is attached to your VPC.
- Go to **subnets** and make sure to see if you have two subnets one public and one private.
- Take a screenshot of the subnets along with their ipv4 CIDR addresses. (3c.png)
- Go to the public network and take a screen shot(3d.png) and also analyse the details.



Task 3: Analyse your VPC -10 mins

- Each subnet is associated with a routing table which specifies the outbound traffic
- Routing tables for both your public and private networks
- The routing table for public network should have the following configuration:

- **Route 10.0.0.0/16** | **local** directs traffic destined for elsewhere in the VPC (which has a range of *10.0.0.0/16*) locally within the VPC. This traffic never leaves the VPC.
- **Route 0.0.0.0/0** | **igw-** directs all traffic to the Internet gateway.

- The routing table for your private network should look like this:

Route 10.0.0.0/16 | **local** directs traffic destined for elsewhere in the VPC (which has a range of *10.0.0.0/16*) locally within the VPC. This traffic never leaves the VPC.
Route 0.0.0.0/0 | **igw-** directs all traffic to the Internet gateway.

- Go to **Network ACL**:
- A network access control list (**ACL**) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets.
- Edit the inbound rule in your VPC to allow only http traffic Take a screen shot when done (3e.png)

Task b: -40 mins

Migrating your existing application on Beanstalk into the VPC

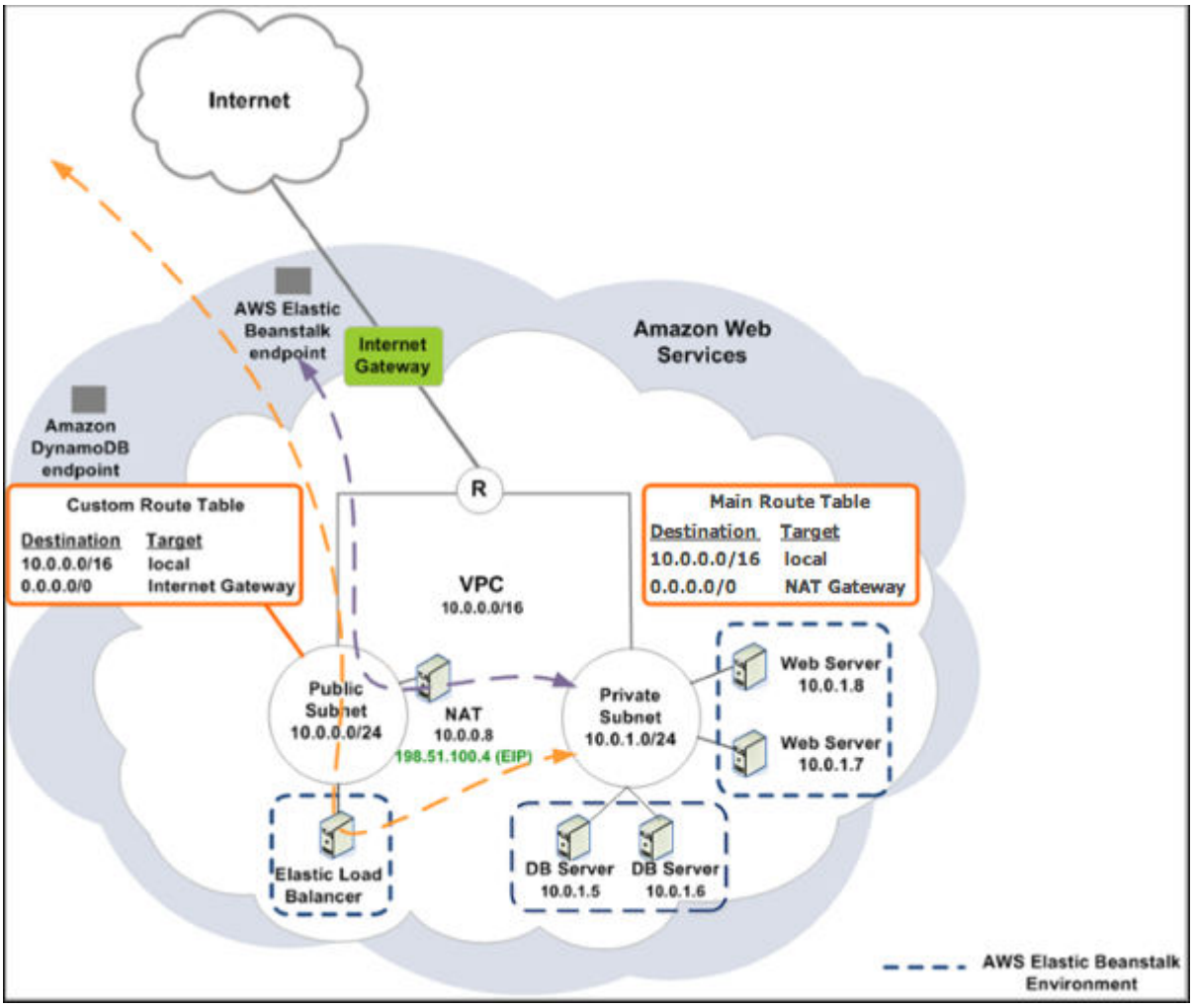
(Note: Refer the pictorial representation below)

- Create a snapshot of your elastic beanstalk environment by saving your environment's configuration as an object in Amazon Simple Storage Service (Amazon S3)
- Make sure you have a snapshot of the RDS database which works along with your application.
- Refer this to create a saved configuration of your environment in beanstalk.
- Now, go to your saved configurations under your web app and choose **Launch environment.**
- Note: We are now going to launch this environment into our VPC created earlier.
- Give the new environment name: pes[yourSRN]-env
- Upload your application code by importing from S3 or locally.
- Click configure more options and modify network so that the app sits on the VPC you created.
- Assign your load balancer to a subnet in each Availability Zone (AZ) in which your application runs.
- Choose a subnet in each AZ for the instances that run your application. To avoid exposing your instances to the Internet, run your instances in private subnets and load balancer in public subnets.
- Now that you have your elastic beanstalk application in your VPC, take a screenshot (3f) clearly showing your environment name and the network in which your application resides.
- Make sure you can access your application through the URL provided in the beanstalk dashboard.
- Try editing your database (in configuration) and restore an existing snapshot of the RDS SQL database.
- Validate that your VPC and the beanstalk application if it's configured properly.
- You are Done! But don't forget to delete your beanstalk application and your VPC.

Task 4: Delete your VPC -10 mins

- Terminate all your beanstalk environments and the application.
- Delete the NAT gateway (only the one associated with your VPC)
- Detach the internet gateway associated with your VPC after deleting the private and public subnet attached with the VPC.
- Delete the VPC (all subnets and routing tables are deleted in this process)
- Note: Make sure deletion is done in order to prevent any dependency errors.
- Release the elastic IP that you allocated.

Pictorial representation for your understanding



Reference: https://docs.amazonaws.cn/en_us/elasticbeanstalk/latest/dg/vpc-rds.html

Lab 4–AWS SQS and SNS

Introduction to message queues for communication using AWS Simple Message Queue Service(SQS) and understanding publisher-subscriber messaging using AWS Simple Notification Service(SNS).

- Deliverables: 5 screenshots 4a-4e

AWS SNS

- Amazon Simple Notification Service (Amazon SNS) is a fully managed messaging service for both application-to-application (A2A) and application-to-person (A2P) communication
- **SNS** is a distributed **publish-subscribe** system.
- Messages are **pushed** to subscribers as and when they are sent by publishers to SNS.
- Learn more here

Task 1 : Understand publisher subscriber pattern through application-to-person (A2P) messaging.

- Go to SNS from your console and create a topic
- Choose Standard as the type of your topic.
- Name the topic: [yourSRN]-[yourname] (eg: pes120180000-ram)
- Now, its time to create a subscription to the topic that you just created
- Create two subscriptions. Set the endpoint to your email and your friend's mail with the Email protocol. Make sure to confirm subscription from the mail inboxes. Once the subscriptions are confirmed, take a screen shot of all subscriptions. **(4a)**
- Now you need to publish messages to your topic.
- While publishing messages to your topic, set the header to "Hello this is [yourname] from SNS! " .
- Make sure to use Identical payload for all delivery, as your messages will be invariant of the different protocols.

- Send the message and check if you and your friend have received the mail. Take a screen shot of the mail received. **(4b)**

AWS SQS

- **SQS** is distributed **queuing** system.
- Messages are NOT pushed to receivers.
- Receivers have to **poll or pull** messages from **SQS**.
- Messages can't be received by multiple receivers at the same time. Any one receiver can receive a message, process and delete it.
- Other receivers do not receive the same message later.
- Polling inherently introduces some latency in message delivery in SQS unlike SNS where messages are immediately pushed to subscribers.
- Also note that SNS supports several end points such as email, SMS, http end point and SQS
- Learn in detail from here
- Learn about the basic architecture here
- SQS offers two types of message queues.:
    - Standard queues offer maximum throughput, best-effort ordering, and at-least-once delivery.
    - SQS FIFO queues are designed to guarantee that messages are processed exactly once, in the exact order that they are sent.

Task 2 : Play around with SQS queues

- Make a standard queue and name it [yourname]-queue. Take a screenshot **(4c)**
- Send any message to the queue with a delay of 10 seconds.
- Poll for messages. Notice that the receive count gets incremented, if you poll for messages multiple times. Take a screenshot after polling multiple times. **(4d)**
- Unless you delete the messages, it remains in the queue.
- Delete the message from the queue.
- Send another message, and poll for messages.
- Try changing the queue to FIFO and experiment with it. Do you find any difference ?

Fanout to Amazon SQS queues

- Using Amazon SNS and Amazon SQS together, messages can be delivered to applications that require immediate notification of an event, and also persisted in an Amazon SQS queue for other applications to process at a later time.

- When you subscribe an Amazon SQS queue to an Amazon SNS topic, you can publish a message to the topic and Amazon SNS sends an Amazon SQS message to the subscribed queue.
- The Amazon SQS message contains the subject and message that were published to the topic along with metadata about the message in a JSON document.

Task 3 : Using Amazon SNS and Amazon SQS together

- Subscribe the queue which you created to the topic previously created.
- Publish a message to the topic and select custom payload for each delivery protocol.
- Go to your SQS queue and poll for messages. Take a screenshot of the json object which you received. **(4e)**

DELETE all topics, subscription and queues. You are done!!

Questions: (Optional to submit the answers)

- Why do you generally couple SNS and SQS together?
- What's the point of having two different types of queues?

Lab 5 - Docker

Week 4 Tasks: (10 points each)

1. Installing Docker Engine on AWS EC2 instance

a. Screenshot of running docker hello-world

2. Docker images and Dockerfiles

a. Screenshot of C Program successfully run inside container.

3. Exposing ports,docker networks

a. Sample.html showing the web page on the browser. Screenshot should show public dns of the EC2 host of docker.

b. Screenshot of docker container running nginx (terminal of EC2 host)

c. Screenshot of python application successfully writing and reading from the MongoDB database

d. Screenshot showing mongodb being run within network(docker command has to be clearly highlighted)

e. Screenshot showing python file being run within network and successfully writing and reading from MongoDB(docker command has to be clearly highlighted)

4. Docker compose

a. Screenshot of python-mongodb application running as a docker compose application(logs of the application)

b. Screenshot of 3 python application writes and reads from MongoDB after scaling the python application.

5. Docker volumes (This task is optional, No bonus marks will be given for submitting this screenshot)

a. Screenshot clearly showing command run to mount the host volume and manually running the python application inside the container

Few key points to note:

1. All required files **except** Dockerfile(s) have been given in the drive folder(task wise) where this manual is uploaded.
2. It is very important to go through all reference material attached in this manual , as this will help you understand and debug the lab tasks.

3. Most of this lab focuses on 2 aspects building the right Dockerfile and running the right command.
4. Apart from the attached resources, you can always refer to the official docker documentation. The docker documentation is well maintained and should help you through all your tasks.https://docs.docker.com/
5. Additional resources have been given at the end of the manual.
6. When you run docker commands in the foreground, you cannot access the command prompt in which case press **[Ctrl+C]** and continue with the next step or run docker in the background mode by using –d option as explained in the demo video. https://www.tecmint.com/run-docker-container-in-background-detached-mode/

Understanding containers and Docker

Please watch the below youtube tutorial **mandatorily** before starting the lab, this will help kickstart your understanding of Docker and the commands.

Docker Basic Commands | Docker Commands with Examples | Docker Commands Tutorial | Intellipaat

Containers are the de-facto standard for creating,maintaining and deploying microservices. A container is a standard unit of software that packages up code and all its dependencies so the application runs quickly and reliably from one computing environment to another.

Container engines are the technology/software that are used to run the containers. There are many container engines available, but the most popular and easy to use CE is *Docker.*

The following links will help you get started on why we need containers, how they are different from VMs and why Docker:

What is a Container? | App Containerization - **Must Read!**

What is Docker?

Task 1: Installing Docker Engine on EC2

Sub-tasks are:

1. Create an EC2 instance with the following specs:

AMI	Ubuntu Server 20.04 LTS (HVM), SSD Volume Type
Instance Type	t2.medium
Instance Details	Default values
Storage	Default values

2. Get keypair(pem) file and SSH into the instance.
3. Install docker engine on the instance , instructions are in the given link:
    a. Install Docker Engine on Ubuntu
4. Use the following link to make docker a “sudo-less” command:
    a. Post-installation steps for Linux
5. Verify that Docker Engine is installed correctly by running : docker run hello-world

Task 2: Docker images and docker files

In AWS EC2 instances we saw *AMI(Amazon Machine Images)*, which was basically the operating system and in case of snapshots, the current *state* of the VM. Docker images are similar, but are not the same. Docker images are “ready to go” meaning everything that needs to be installed(requirements) has already been taken care of when building the image and they don't need to be installed/taken care of again.

Docker files are used to create Docker images. Dockerfile are a series of steps that specify which base image to use, which files/folders to copy into the container, run which commands while starting up the container and which will be the main process of the container. We need to create dockerfiles, then build it into an actual runnable docker image.

Sub tasks:

1. Docker hub is a central public repository containing Docker images and documentation on how to use these base images. Explore the different images at : https://hub.docker.com/
2. The images in docker hub, need to be *pulled* into our EC2 instance in order to use them(Pulling is the equivalent of downloading the images onto you docker host).
    a. docker pull

    Pull the following images onto your docker instance:

    - Ubuntu 18.04
    - Nginx
    - Python
    - MongoDB

    Stick to the latest images. To find the images that exist on your instance you can run the docker images command. This shows the image name, when you pulled the image, the tags(versions) of the images.

3. Now that we have the images we need to actually run the containers,
    a. We can run a container using the docker run command.
    b. To list the *currently running* container we use the docker ps command
    c. To stop a running container safely we use docker stop

d. Usually after a container is stopped it goes into a “exited state”, this can block some I/O operations needed by future containers and you will not be able to use the name of the exited container. What are the possible states for a docker container?

   To safely and cleanly remove a container, use the docker rm command.

4. *Containers are light weight VMs*, this means we should be able to somehow interact with a running container, like a terminal.
   a. Start an interactive bash(shell) session with an ubuntu:18.04 as a base image. Explore around the container using the shell. **What is different and what is same as an ubuntu VM?**
      i. Docker 'run' command to start an interactive BaSH session
   b. Get a shell into an already running container
5. Let us now create our own Docker image using Ubuntu:18.04 as a base image. The image you will create will run a simple C program, after installing the GCC compiler. The Dockerfile must:
   a. Specify the base image as **Ubuntu:18.04**
   b. Copy the program.c file from your instance to the docker image.
   c. Update the “apt” repository and install the GCC compiler
   d. Compiler the C program.
   e. Run the ./a.out *command*

   Hint: What should the name of the dockerfile you are creating?

   Use the following C program as a base, only modify your SRN:

```c
#include<stdio.h>

int main()

{

    printf("Running this inside a container !\n");

    printf("My SRN is <YOUR SRN HERE>\n");

}
```

6. After you have your Dockerfile, build the image using docker build and run the container.

References to help you get started:

- How do you write a Dockerfile?
- Docker Build: A Beginner's Guide to Building Docker Images
- How to Create a Docker Image From a Container

Task 3: Exposing ports,docker networks

Containers are also used to run web applications , they can be web servers such as Apache or Nginx, or web applications using REST APIs or any other web application. Similar to *Security Groups* for EC2 instances, we need to *expose* the right ports to access the container's web apps.

1. Download the sample HTML file from the Lab 5 drive folder , and modify your SRN.
2. Create a Dockerfile and then a docker image having an **nginx:latest** base image, and copying the html file into the default folder in the container. Build the docker image and **tag/name it your SRN**.
3. Run the docker container using the previously created docker image. Expose the HTTP port and check connectivity.
    a. Publishing/Exporting ports in a docker container
    b. Docker Container Tutorial #8 Exposing container ports

Hint: You are running a container on an EC2 instance. After exposing the port on the container , you might be able to access the nginx web server from within the EC2 instance, but not from the internet(your system). What needs to be configured for the AWS EC2 instance running your container?

In lab 3 , we saw VPC networks and how we can create a virtual network connectivity between virtual machines(EC2 instances). Similar networks need to be created for containers. We will explore connectivity without docker networks and see how docker networks make it much easier to connect within containers. To demonstrate this we will create a simple application using a python client and a MongoDB NoSQL server.

Note: You don't need to know how to use mongodb, code to use mongodb has been provided to you.

1. Run the mongodb container in a detached mode, exposing the default port(27017) of mongodb.
    a. Use the **mongo:latest** image.
    b. Name the container as **mongodb** while running the container. Naming a container
    c. Docker detached mode
2. Download sample.py from the drive folder. Modify the SRN wherever mentioned.
3. The MongoDB container is running, but we need to find out the *IP address* of the mongodb container. Find this IP using the docker inspect command. Modify this IP address in the sample.py file.
    a. Get a containers IP address

4. Create a Dockerfile, which:
    a. Uses **python** base image
    b. Updates the apt-repository
    c. Installs **pymongo** using pip (pymongo 3.11.2).
    d. Copies the sample.py from the instance to the container.
    e. Runs the python *command* , to run the python file.
5. Build the docker image using the above Dockerfile and run the container.
6. You should see that the data was correctly inserted and fetched from the database container.

The above tasks showed the connectivity between 2 containers *without* a network. This can cause problems as every time a container is created it *could possibly* have a different IP address. This is the issue *docker networks* tries to solve.

Docker Networking Options

Docker Networking | Docker bridge network deep dive | Container bridge drive

1. Create a docker bridge network , called **my-bridge-network.**
2. Stop the mongodb container you had created before and delete(rm) it. Run a mongodb container again, but now with the following parameters;
    a. network : **my-bridge-network**
    b. name: **mongodb**
    c. Exposed ports: **27017**
    d. Image: **mongo:latest**
3. Go back to sample.py , comment line 3 and uncomment line 4. We are now going to use the name of the database containers as the host name, leaving the ip address resolution to docker.
4. Build the python app docker image again as you did previously and run the container using the built image. You should see that insertion and retrieval have been done successfully.

Task 4: Docker compose

Till now, we have been using docker commands to start and stop containers,create docker networks etc. But this becomes challenging in a real environment when a single application may have 100s of containers(microservices) that need to talk to each other within a single network. While docker networks solve this problem partially, it still doesn't solve the issue of having to run multi-container applications and to automatically bootstrap these containers into the same application, this is where *Docker Compose* comes into the picture.

Docker compose helps bootstrap complex multi container applications, helps maintain the dependencies between them , create a network among these containers and even help scale the entire application entirely or particular containers within the application.

Overview of Docker Compose

"What, Why, How" Docker Compose?

We will use the same python-mongodb application to use docker compose and even scale containers within the application automatically. Docker compose uses YAML Files to specify the different *pieces(containers)* of the application, along with the required configurations. YAML files are EXTREMELY popular when it comes to bootstrapping complex applications not only in Docker!

Docker Compose in 12 Minutes

1. For the purposes of this lab make sure all the following files are in the same directory
    a. docker-compose.yml
    b. Dockerfile
    c. sample.py
2. Install docker compose using the following link:
    a. Install compose on linux systems
3. Go to the docker-compose.yml file and try to understand the syntax and what each line does.
4. Within the same directory, run: **docker-compose up**.
    a. Docker Compose command-line reference

    What you see is that Docker compose has built your python application, started the mongodb server , created links internally between the containers (network) and started both the containers together as a *unified application*.

    The python container exits, since its done with its utility of writing and reading to the database.

5. Now we will scale the python application, so that we have 3 containers of the python application, but keep only one container of the mongodb.
    a. docker-compose scale - Use this link as a reference and scale **only the python application. Use the correct "service" to scale**

Task 5: Docker volumes This task is for you to practice, No bonus marks will be given for submitting this screenshot

Docker volumes are an important and crucial concept. Volumes are the preferred mechanism for persisting data generated by and used by Docker containers. Volumes are either created dynamically by Docker or you can mount the host directory. In this task,we will focus on mounting a host volume.

Docker bind mount | Sharing data between host and Container

1. Create a new directory on the EC2 host , with the name as your SRN.
2. Add the following folders inside it:
    a. sample.py (A simple python application which reads from a text file called details.txt and prints them line by line)
    b. A text file called details.txt containing your name,srn,section,semester.
3. We will be using **Ubuntu:18.04** as a base image.
4. For the ubuntu container, mount the host volume you have created and create a bash shell into the container.
    a. Start a container with a bind mount
5. Inside the container run the python program to display contents of the list.

Additional Resources/Common bugs you might encounter:

1. What is Docker?
2. docker command not found even though installed with apt-get
3. docker CLI & Dockerfile Cheat Sheet
4. docker cheat sheet
5. Not able to reach the container(for web apps)? Think about EC2 security groups.
6. 9 Common Dockerfile Mistakes - Runnablog
7. How to debug and fix common docker issues.
8. Not able to build/run docker containers due to insufficient space on EC2: How To Remove Docker Images, Containers, and Volumes
9. Docker - Container is not running
10. exited with code 0 docker
11. Docker container has a name conflict? Remove all stopped containers
12. Curious about MongoDB and what it is ?
    a. What is NoSQL? NoSQL Databases Explained
    b. What Is MongoDB?
    c. Tutorial — PyMongo 3.11.2 documentation

Lab 6 - RabbitMQ and Docker-Compose

Introduction:

Welcome to Lab 6! In this lab you'll learn how RabbitMQ message brokering works. you'll also try out how you can use Message brokering with docker.

General Instructions:

- **Preparation**: Watch the **demo video** and read the instructions in this document carefully before you go to the lab or start doing the experiment.
- You do **not** need AWS for this experiment. You can use the lab machines with ubuntu installed.
- You should complete **TASK-1 (Work Queues)** in the lab and submit the SS to Edmodo on the same day.
- You can complete **TASK-2 (Publish/Subscribe)** and submit SSs to Edmodo on the same day or within 2 days of your lab.

RabbitMQ

RabbitMQ is an open-source message-broker software that originally implemented the Advanced Message Queuing Protocol and has since been extended with a plug-in architecture to support Streaming Text Oriented Messaging Protocol, MQ Telemetry Transport, and other protocols.

What can RabbitMQ do for you?

Messaging enables software applications to connect and scale. Applications can connect to each other, as components of a larger application, or to user devices and data. Messaging is asynchronous, decoupling applications by separating sending and receiving data.

You may be thinking of data delivery, non-blocking operations or push notifications. Or you want to use publish / subscribe, asynchronous processing, or work queues. All these are patterns, and they form part of messaging.

RabbitMQ is a messaging broker - an intermediary for messaging. It gives your applications a common platform to send and receive messages, and your messages a safe place to live until received.

Docker-Compose

Compose is a tool for defining and running multi-container **Docker** applications. With **Compose**, you use a YAML file to configure your application's services. Then, with a single command, you create and start all the services from your configuration.

Objective

In this lab experiment we will observe how two of the important messaging technique from RabbitMq work, Namely:

1. Work Queues
2. Publish/Subscribe

We will run the messaging application's and the RabbitMq server as the microservices using docker-compose.

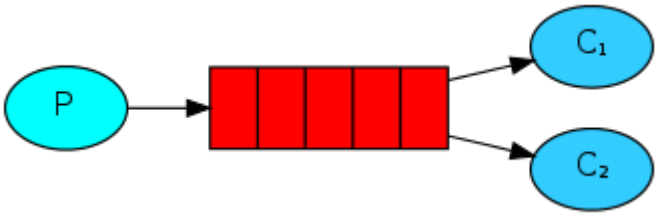
Prerequisites:

- Docker Installed on your system. (Refer to Task1 steps in the Lab5 manual)
- Understand how to write yaml files.

TASK-1 (Work Queues)

In this task we will implement the "Work Queues" Message brokering service. We are going to have three services running using Docker compose.

The main idea behind Work Queues (aka: Task Queues) is to avoid doing a resource-intensive task immediately and having to wait for it to complete. Instead we schedule the task to be done later. We encapsulate a task as a message and send it to the queue. A worker process running in the background will pop the tasks and eventually execute the job. When you run many workers the tasks will be shared between them.

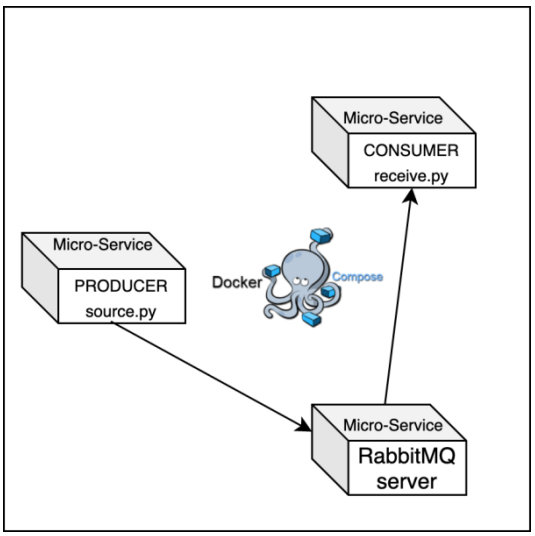


Background:

We will build a multi-container application having **three services**. One service will run your RabbitMq Server, Other two will be your Producer service and worker service(consumer).

The Architecture:

1. The producer will Run a Python Application which will push the message to the Queue.
2. The producer will push a certain amount of messages on the Queue.
3. The consumer will run a Python Application which will pop a message from the Queue and print it.
4. Scaling Multiple workers (consumers), the messages will be shared among the workers(consumers).



You are already provided with the application file for the producer service. A producer service run's an application "source.py". The producer service will push the message into the queue by connecting to the RabbitMq service running in the same docker-compose network.

What will you be doing:

- Build the python application for the worker service (consumer service).
- Write the YAML file to build the services.
- Scale the Number of workers while you do docker-compose.

Deliverables SS:

- **1A.png (SS of the docker compose output)**
- **1B.png (SS of the docker ps output) (showing what containers are running)**
- **1C.png (SS of the yaml file)**

Note:

- please download the source folder given to you
- The source folder will have two directories namely “send” and “receive’. It will also consist of one empty yml file. Please maintain the directory structure given to you.
- The “send” and “receive” folder will have a Dockerfile.
- The “send” folder has “source.py” file.
- The “receive” folder does not has the “receive.py” file.
- We are gonna use the terms “consumer” and “workers” Interchangeably.

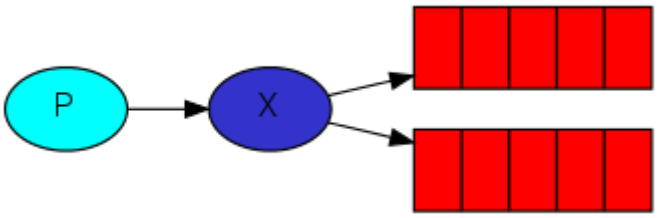
Steps:

- Build the python application for workers(consumer service).
- The worker (consumer) application should pop the message available in the queue and print it.
- The idea is when we will have multiple workers running(consumers) the messages will be shared among the workers.
- You can get the code for the worker application from here. Make sure you name the file as ‘receive.py” and change the queue name according to what’s given in “source.py” file. Also change the hostname by looking into “source.py”.
- Add the “receive.py” file to receive folder.
- Edit your yml file and add the below mentioned requirements. yaml file will have the skeleton code for you to begin with.
- You need to have three services one service is your rabbitmq server, other two are your producer and consumer. Below you can find the service specifications.
    - RabbitMQ service
        - Service Name: rmq
        - image: rabbitmq:3.8.3-alpine
    - Producer service
        - Service Name: producer
        - build context: “send”
        - Dockerfile: Use the dockerfile inside the send folder
        - command: sh -c "sleep 20 && python source.py" (would suggest to use the exact same command)
        - links: rmq
        - dependency: rmq
    - Consumer service
        - Service Name: consumer
        - build context: “receive”
        - Dockerfile: Use the dockerfile inside the receive folder
        - command: sh -c "sleep 15 && python receive.py" (would suggest to use the exact same command)
        - links: rmq

- dependency: rmq

- The producer service should use the Dockerfile present inside the send folder.
- The consumer service should use the Dockerfile present inside the receive folder.
- Understand the concept of context.
- Also edit the message being sent as the Message should Include your **SRN** in "source.py".
- Now run your docker services by scaling the number of consumers to **4.**
- Identify what command to run in order to scale the services while you start them.
- We are scaling the consumer service to create 4 workers. You can observe that the message sent by the sender is shared by the workers(consumers). Take the required SS.

TASK-2 (Publish/Subscribe)



The core idea in the messaging model in RabbitMQ is that the producer never sends any messages directly to a queue. Actually, quite often the producer doesn't even know if a message will be delivered to any queue at all.

Instead, the producer can only send messages to an exchange. An exchange is a very simple thing. On one side it receives messages from producers and the other side it pushes them to queues. The exchange must know exactly what to do with a message it receives. Should it be appended to a particular queue? Should it be appended to many queues? Or should it get discarded. The rules for that are defined by the exchange type.

Background:

We will build a multi-container application having **three services** just like the previous task. One service will run your RabbitMq Server, Other two will be your Producer service and worker service(consumer).

The Architecture:

1. The producer will publish messages to the exchange on the RabbitMq server.
2. The producer will Run a Python Application which will publish the message to the exchange.
5. The consumer will run a Python Application which is subscribe to the exchange using Queues.
6. Scaling to Multiple workers (consumers), All the messages will be received by all the consumers.

Deliverables SS:

- **1A.png (SS of the docker compose output)**
- **1B.png (SS of the docker ps output) (showing what containers are running).**

Steps:

- Please find the “emit_log.py” and ”receive_log.py” from this link.
- Understand what each of the applications does.
- Your producer service should run the “emit_log.py” Application.
- Your consumer service should run the ”receive_log.py” Application.
- You can use the previous yaml file for this task.
- Just replace the old application files with the new application files.
- Modify the yaml file to run the new application’s.
- Modify the application’s to connect to the RabbitMq server. The producer application should push your “SRN'' as the message.
- You need to start the services and make sure you scale the consumer service while you start.
- you need to scale the consumer service to **5**.
- Take appropriate SS.
- If you are using the same “Source” directory for this task, then make sure you delete your Images and Containers because if you run the service after modifying the application files it won’t build the new image for your services. Or you can refer to this process.

Reference:

- Hint: We will be using the same application files provided in this link: https://www.rabbitmq.com/tutorials/tutorial-two-python.html
- Docker-compose and scaling: https://medium.com/@karthi.net/how-to-scale-services-using-docker-compose-31d7b83a6648

Lab 7 – Jenkins (DevOps, CI/CD tool)

Introduction:

Welcome to Lab 7! This simple exercise is designed to introduce you to Jenkins and continuous integration.

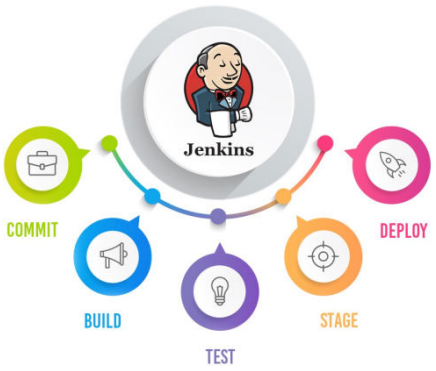
General Instructions:

1. All the screenshots must be uploaded to Edmodo before the stipulated deadline.
2. For each lab, screenshots need to be uploaded as mentioned under the "deliverables" section for each task **exactly** as mentioned.
3. If a task has some questions, these will not be evaluated but are extremely important in understanding the concepts.
4. Try to solve the tasks by yourselves, all relevant information to complete the tasks has been provided. In case you are stuck and not able to solve the issue, feel free to send email to pesu_cc_lab_support@googlegroups.com

What is Jenkins?

Jenkins is an extensible, open source continuous integration server. It builds and tests your software continuously and monitors the execution and status of remote jobs, making it easier for team members and users to regularly obtain the latest stable code.

What is Jenkins Pipeline?



In simple words, Jenkins Pipeline is a combination of plugins that support the integration and implementation of continuous delivery pipelines using Jenkins.The pipeline as Code describes a set of features that allow Jenkins users to define pipelined job processes with code, stored and versioned in a source repository.

Overview of the Experiment

- Setup jenkins Using Docker.
- Set up a job in Jenkins to connect to your repository and build C++ hello.cpp.
- Set up second job to run the program after the build completes.

Prerequisite:

- Docker Installed on your system. (Refer to Task1 steps in the Lab5 manual)

Task-1

Aim: Set up Jenkins using Docker.

Deliverables:

1. 1A.png (SS of the running Docker Container)

Steps:

- You will be given a Dockerfile.
- Put that Dockerfile in a folder and open a terminal in that folder.
- Build the dockerfile using this command: `"sudo docker build -t jenkins:lab7 . "`
- Run your container using this command `"sudo docker run -p 8080:8080 -p 50000:50000 -it jenkins:lab7" (Note down the password shown on the terminal)`
- Open URL: localhost:8080 on your browser.
- Enter the password shown on your terminal after running the container (You can set the password to ADMIN later).
    - In case you did not note down the password displayed on the terminal, you can find the password by connecting to the container (via "sudo docker exec –it <container_id> /bin/bash") and checking the file /var/Jenkins_home /secrets/initialAdminPassword inside the container
- **Integrate GitHub to Jenkins**: When prompted for plugin installation, click on "Select Plugins to Install" and then search for Github and check the github option. (This step may take a few minutes to complete)
- Take the necessary SS.

Task-2

Aim: Set up a job in Jenkins to connect to your repository and build C++ hello.cpp.

Deliverables:

1. 2A.png (picture showing the console output after the build is successful)
2. 2B.png (picture showing the Stable state of the task in Build History of Jenkins)

Steps:

- Navigate to Jenkins server. Click ***New Item***.
- Enter a name for your project, click *Freestyle Project*, then *OK*. *Note*: Please do not include a space.
- Name this something unique so there are no collisions.
- Select github project and Enter the repository URL. Use this repository link: https://github.com/sujeeth-cc/Lab7-Jenkins.git
- Set up *Source Code Management*, Select *git*. Enter the URL of git repository.
- Add "`*/main`" in **Branches to build** (Do not delete the existing */master branch)
- Setting up *Build Triggers.* Select *Poll SCM*.
- Set up cron job by putting in "`H/2 * * * *`" in the Schedule box
- Set up *Build*. In **Add build step** pull-down menu, select *Execute Shell*.
- Enter "`make -C original`"(This will run the Makefile).
- Click *Save*.
- Click on build now.
- Take the required SS.

Task-3

Aim: The final step to this exercise is to set up a second job that automatically runs after the project builds. This is different from the other job because this will not have a git repository - it doesn't even build anything.

Just a note: In a real-life scenario you wouldn't run a program through a build job just like this because I/O is not possible via this console. There are other tools people use at this step like SeleniumHQ, SonarQube, or a Deployment. The point of this is to show downstream/upstream job relationships.

Deliverables

1. *3A.png (Console output of second job)*
2. *3B.png (Status page of first job)*
3. *3C.png (Build History of jenkins)*
4. *3D.png (Jenkins Dashboard)*

Steps:

- Create a new Job in Jenkins, Click *New Item* in the left panel
- Enter a name for your second job, click *Freestyle Project*, then *OK*.

- Go immediately to build step and select *Execute Shell*.
- Enter the following Command `/var/jenkins_home/workspace/<the name of your first project>/original/hello_exec`
- Save
- Set your first job to call the second.
- Go to your first job (i.e item) and open the *Configure* page in the pull down menu
- Scroll to bottom and add a Post-Build Action. Select ***Build other projects***.
- Enter the name of your second job.
- Save.
- Run your first job.
- Do this by clicking build now on the main page.
- After that successfully builds, go and check your second job. You should see it successfully run.
- Select a Build Job from History and go to the console log to see your program output. If you program has run there then you successfully set up a basic pipeline.
- Take the required SS.

Lab 8 - Kubernetes

Week 8 Tasks:

1. Create a Kubernetes cluster using minikube
    a. 1a.png Screenshot of kubectl get nodes showing minikube is running properly
2. Kubernetes pods
    a. 2a.png Screenshot showing:
        i. nginx pod in running status
        ii. port-forwarding of the pod using port 80
    b. 2b.png Nginx home page access through localhost
3. Kubernetes Deployments and Kubernetes services
    a. 3a.png Screenshot showing deployment running and replicas as 2/2. Also, show the service
    b. 3b.png port-forwarding of the service using port 80 and accessing the web page using localhost
4. Scaling Kubernetes
    a. 4a.png showing 10 pods (either running/pending state)

Introduction to Kubernetes

https://kubernetes.io/docs/concepts/overview/what-is-kubernetes/

Kubernetes makes it easy to deploy and operate applications in a microservice architecture. It does so by creating an abstraction layer on top of a group of hosts so that development teams can deploy their applications and let Kubernetes manage:

- Controlling resource consumption by application or team
- Evenly spreading application load across a hosting infrastructure
- Automatically load balancing requests across the different instances of an application
- Monitoring resource consumption and resource limits to automatically stop applications from consuming too many resources and restarting the applications again
- Moving an application instance from one host to another if there is a shortage of resources in a host, or if the host dies
- Automatically leveraging additional resources made available when a new host is added to the cluster
- Easily performing canary deployments and rollbacks

Important Kubernetes Terminologies:

1. Kubernetes Namespace
    a. Kubernetes Documentation: Namespaces
2. Pod
    a. Pods – Kubernetes Documentation
    b. What is a Pod.
3. Replica Set
    a. ReplicaSet
4. Deployment
    a. Deployments
5. Service
    a. Kubernetes Service
6. LoadBalancer Service
    a. Kubernetes LoadBalancer Service
7. NodePort Service (Not needed for this lab, but must know)
    a. Kubernetes NodePort Service
8. Ingress Controller (Not needed for this lab, but must know)
    a. Ingress
9. Horizontal Pod Autoscaler (Not needed for this lab, but must know)
    a. Kubernetes Horizontal Pod Autoscaler

Quick Points:

1. Ensure Docker is installed, up and running before using minikube.
2. Pods may take some time (a few minutes in a bad network) initially to start up, this is normal.
3. All resources mentioned in all the tasks must be created only in the **default Kubernetes namespace**, modifying other namespaces such as kube-system may cause Kubernetes to stop working.

4. If you are unable to show the results to your respective lab faculty, you can submit the screenshots to Edmodo but only in PDF or WORD format (and not in ZIP format)

TASK-1 (Create a Kubernetes cluster using minikube)

The first task is to set up a Kubernetes cluster and a command-line tool called “kubectl” to interact with this cluster. For this lab, we will be using *minikube* which is a VM/Docker-based tool that helps to create a Kubernetes cluster quickly to either test applications/learn Kubernetes.

Kubernetes being a container-orchestration service needs an engine to create/destroy containers and uses Docker for this purpose.

A real Kubernetes cluster runs pods natively on the host machine using the docker engine. So all container processes are run natively on the host machine. Some examples of popular Kubernetes clusters are AWS Elastic Kubernetes Service(EKS), Google Kubernetes Engine(GKE), and kubeadm which is used to create clusters manually.

Minikube is slightly different from the real Kubernetes cluster, it creates a virtual machine/docker container and runs the pods inside the VM/container. This is done so that we can get a quick Kubernetes cluster up and running without bothering about the details of setting up one or to avoid cloud services. Details about how this impacts deployments/services will be clearly explained as we go on in the lab.

To set up minikube Kubernetes cluster, follow the following steps:

1. Install Docker/Ensure docker is already installed on the host machine. Make sure docker is up and running
2. Install Kubectl, the CLI tool used to interact with the Kubernetes cluster by following **Steps 1 to 4** under "**Install kubectl binary with curl on Linux**" in the following link:
   https://kubernetes.io/docs/tasks/tools/install-kubectl-linux/ **or**
   https://kubernetes.io/docs/tasks/tools/install-kubectl/
3. Download and install minikube by running the following 2 commands (each is a complete line of command:

```
curl -LO
https://storage.googleapis.com/minikube/releases/latest/minikube-linux-amd64

sudo install minikube-linux-amd64 /usr/local/bin/minikube
```

   Ref Link - https://minikube.sigs.k8s.io/docs/start/#binary-download

4. Startup the minikube cluster by running: `minikube start`
   a. This might take a while initially as it needs to pull the docker image and set up kubectl
5. Test your kubectl is configured and correctly running, by running: `kubectl get node`

You should see a similar output:

```
NAME       STATUS   ROLES    AGE   VERSION
minikube   Ready    master   65m   v1.18.3
```

TASK-2 (Create a Kubernetes pod)

All resources such as pods, deployments, services etc are created using YAML files. For this task and the following tasks, we will see how we can use Kubernetes to orchestrate Nginx web servers.

Pods are the smallest deployable units of computing that you can create and manage in Kubernetes. Open the **pod.yaml** file and examine the contents of the YAML and what each property/field does.

1. To run the pod, run:
    a. `kubectl create -f pod.yaml`
2. To find out whether the pod is running successfully, you can run:
    a. `kubectl get all` (This command fetches all the resources in the default namespace)
    b. `kubectl get pods`(This command shows only the pods in the default namespace)
3. The pod we are running is a web server, and we must be able to connect to the server.
    a. Since we have only a single pod, we want to just access THAT pod, and not a deployment (as we will see in the next task).
    b. Run. `kubectl port-forward pod/nginx 80:80`
        i. What this command does is, say "I have a pod called Nginx, expose it such that if any HTTP request is coming for port 80 of the host machine, redirect it to me(Nginx pod), I (pod) will handle that request"
        ii. Note: You may see "Unable to Create Listener" errors if port 80 is already being used on the host system. To resolve this, you can use a different port. In the above command, the following is the format: <port_on_host>:<default_container_port>. The default container port here is the default Nginx port i.e 80. Therefore to expose another port say 8080, use 8080:80 . This is important to note every time you try to port-forward.
    c. Access your webserver through http://localhost:80 (Or the port you changed to , if port 80 was not available)
    d. Press Ctrl+C to stop the port-forwarding.
4. Delete the pods by either:
    a. Deleting every pod in the default namespace, by running:
        i. `kubectl delete pods --all`
    b. Deleting the specific pod, by :
        i. Finding the pod name, using:
            1. `kubectl get pods`
        ii. Deleting the specific pod by running
            1. `kubectl delete pod/<pod_name>`

TASK-3 (Create a Kubernetes Deployment and create a Load Balancing Service)

A pod is only a single instance(the smallest part) in a Kubernetes “deployment”. A Kubernetes deployment refers to a collection of pods called replica sets, and configuration parameters for the replica sets. Deployment is used to tell Kubernetes how to create or modify instances of the pods that hold a containerized application. Deployments can scale the number of replica pods, enable the rollout of updated code in a controlled manner, or roll back to an earlier deployment version if necessary.

A Service in Kubernetes is an abstraction that defines a logical set of Pods and a policy by which to access them. What this means is, it defines an abstract layer on top of a logical set of pods, essentially a “micro-service”-layer. A microservice can be complex and also be horizontally scaled, as a user/caller of the micro-service, I am not bothered by which specific pod services my request but I only care of the “service”, this is essentially what kubernetes service does.

There are many types of Kubernetes services such as LoadBalancer, NodePort, Ingress etc.

This task involves creating a deployment and then a service for it.

1. Download the deploy.yaml file which defines the deployment. Go through the deployment YAML file to understand what each field is and how it affects the deployment. **Ref links to understand resource limits used in the YAML file and their meaning :** https://jamesdefabia.github.io/docs/user-guide/compute-resources/ or https://medium.com/@betz.mark/understanding-resource-limits-in-kubernetes-cpu-time-9eff74d3161b
2. Just like a pod, run the deployment using the following command:

   ```
   kubectl create -f deploy.yaml
   ```

3. This deployment creates 2 pods of NGINX web server and a replica set to manage these pods. To view all the aspects of the deployment(pods, replica sets etc), run:

   ```
   kubectl get all
   ```

4. Once you see all the pods up and running, your deployment is complete. The newly created replica set should show 2/2.
5. To create a service for this deployment, we can either use:
   a. `kubectl expose deploy mynginx --port=80 --target-port=80`
   b. Or use a YAML specification which **we will do now**.
6. Delete the previous deployment and service by running:

   ```
   kubectl  delete deploy mynginx
   ```

   ```
   kubectl delete service mynginx
   ```

7. Download the deploy_service.yaml file.
8. Create the deployment **and its service** by running:

```
kubectl create -f deploy_service.yaml
```

9. Once the pods are up and running, expose the service using:

```
kubectl port-forward service/nginx 80:80
```

10. Access the webserver on http://localhost:80
11. Keep the deployment and service running for the next task

TASK-4 (Scaling deployments)

Replica sets are what control the pods in a deployment, they are what allow for creating rolling updates, config changes etc but more importantly scaling. Replica sets scale the pods in the deployment without affecting the micro-service availability.

1. To scale the deployment done before, run the following command:

```
kubectl scale deploy mynginx --replicas=10
```

2. The above command scales the pods to 10 pods. (You may see pods in a pending state, this is because we are using minikube which has resource restrictions, on a real cluster having sufficient resources we would see the scaling successfully done)
3. Delete the deployment and the service:
    a. `kubectl delete service nginx`
    b. `kubectl delete deploy mynginx`

TASK-5 (Shutdown minikube)

This task ensures all resources are stopped:

1. Ensure all resources are stopped and not seen when running the Kubernetes commands.
2. Stop minikube by running:

```
minikube stop
```

Lab 9 - AWS EMR

Introduction:

Welcome to Lab 9! This simple exercise is designed to introduce you to AWS EMR

General Instructions:

1. **Watch the demo video before starting the experiment**
2. **Execute all 3 Tasks by referring to "AWS getting started with EMR" tutorial (link provided after EMR Workflow diagram below).**
3. Evaluation for the labs will be mixed, few labs will involve uploading screenshots and few might be auto-evaluated.
4. All screenshots must be uploaded to Edmodo before stipulated deadlines and as mentioned under the "deliverables" section for each task.
5. If a task has some questions, these will not be evaluated but are extremely important in understanding the concepts.
6. Try to solve the tasks by yourselves (by watching the demo video), all relevant information to complete the tasks have been provided. In case you are stuck and not able to solve the issue, feel free to send an email to **pesu_cc_lab_support@googlegroups.com**

Deliverables: 4 screenshots and 1 csv file (9a-9d and 9e.csv)

Reading - 30 mins

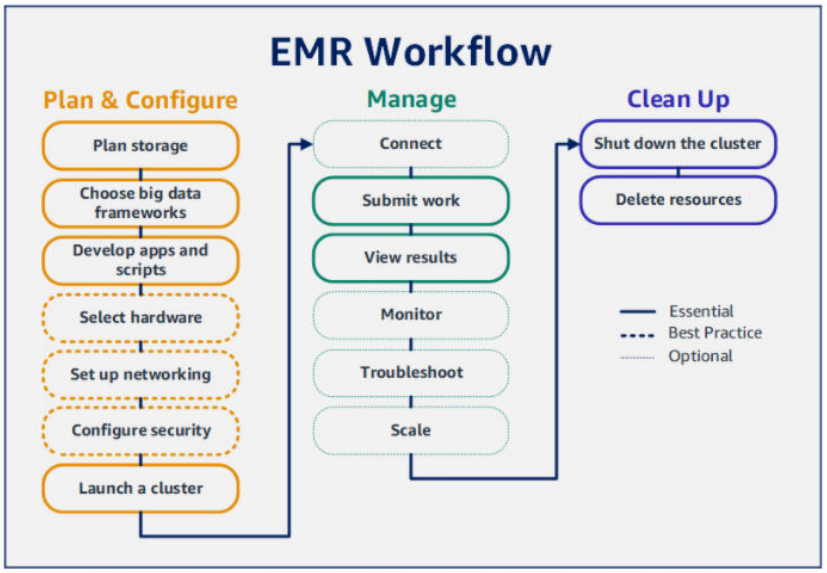
What is AWS EMR?

Amazon EMR is the industry-leading cloud big data platform for processing vast amounts of data using open source tools such as Apache Spark, Apache Hive, Apache HBase, Apache Flink, Apache Hudi, and Presto. Amazon EMR makes it easy to set up, operate, and scale your big data environments by automating time-consuming tasks like provisioning capacity and tuning clusters. With EMR you can run petabyte-scale analysis at less than half of the cost of traditional on-premises solutions and over 3x faster than standard Apache Spark. You can run workloads on Amazon EC2 instances, on Amazon Elastic Kubernetes Service (EKS) clusters, or on-premises using EMR on AWS Outposts.

Overview of AWS EMR :
https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-overview.html

Read about Spark : https://spark.apache.org/

EMR Workflow



LAB Reference: Please use this detailed reference for executing your lab keeping in mind the configurations mentioned below. **You do not have to perform the optional steps in this tutorial.**
https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-gs.html

Watching the demo video will help you to complete the following 3 tasks quickly: (This is the last experiment that will require or use your AWS Credit)

TASK 1: Plan and Configure an Amazon EMR Cluster

Name of s3 bucket: [your-srn-bucket]

Upload both .csv and .py files into S3 bucket and take a screenshot with uploaded files required (9a)

Launching cluster

Cluster name : my-cluster-[yoursrn]

Use the following configurations in your cluster:

Release label: emr-6.2.0

Application: Spark

Instance type: m5.xlarge

Instance count: 3 (1 master and 2 workers)

Screenshot of running cluster (9b)

TASK2: Managing Amazon EMR Clusters

Screenshot of spark job completed (9c)

Screenshot of output folder in S3 (9d)

Download the output csv to your local machine and upload csv (and NOT the screenshot of the csv) to the drive (9e.csv)

NOTE: In case "Add step" task in Cluster Management fails, make sure you have added both .csv file and .py file in your S3 bucket and then repeat the "Add step" task. At this point, you can add a new step or clone the existing (failed) step but make sure all the configurations are correct for the spark application before you re-run the step.

TASK3: Clean Up Amazon EMR Cluster Resources (Do not forget)

Go to EMR, select your cluster and click "Terminate".

Lab 10 - Serverless Computing With AWS Lambda and AWS API Gateway

In this lab you will learn how to:

- ***Create a microservice with AWS Lambda and AWS API Gateway***
- ***Create an AWS Lambda function***
- ***Create an Amazon API Gateway endpoints***

Week 10 Tasks:

1. AWS Lambda

a. 1a.png - Showing 2 S3 buckets created , one having the original image and another S3 bucket suffixed with -resized to store thumbnails

b. 1b.png - Showing the Designer tab diagram, showing that S3 will trigger the creation of the create-thumbnail function

c. 1c.png - Test run successfully (show test details also)

d. 1d.png - Thumbnail created in the *-resized* S3 bucket.

2. API Gateway with AWS Lambda

a. 2a.png - Showing the Designer tab diagram, showing that API Gateway will trigger the creation of the create-thumbnail function

b. 2b.png - Screenshot of accessing the API Endpoint URL on browser and getting successful response

c. 2c.png - Test run successfully (show test logs also)

Introduction to Qwiklabs

Qwiklabs is an online platform that provides end to end training in Cloud Services. This a platform where you can learn in a live environment anywhere, anytime and on any device. Qwiklabs offers training through various Labs which are specially designed to get you trained in Google Cloud Platform (GCP) as well as Amazon Web Services (AWS). Qwiklabs has joined hands with Google and now works as a part of Google Cloud. Every year Qwiklabs delivers thousands of labs and has happy learners all over the globe.

Points to remember:

1. **Although Qwiklabs uses AWS, you will NOT be using your AWS Educate Account. Qwiklabs will create a temporary AWS account with all the required permissions and access to complete the lab.**
2. **When using the Qwiklabs created AWS account, DO NOT change the default region/VPC or any other settings that are automatically created by Qwiklabs.**
3. **The Qwiklabs lab has a time limit within which the Qwiklab lab has to complete, after the timer hits zero, the AWS account will be removed and you will have to restart the lab from scratch.**
4. **All code and config for the Qwiklab labs have already been given, you need not code anything from scratch. However there may be instances where you need to change values of variables based on S3 bucket name etc.**
5. **To prevent conflicts with any AWS account that you have already signed into the browser, use Incognito/Private mode, to ensure you have a fresh browser with not previous logins.**
6. **Ensure that you have signed into Qwiklabs using your Google account.**

Introduction to Serverless Computing

Serverless computing is a method of providing backend services on an as-used basis. A serverless provider allows users to write and deploy code without the hassle of worrying about the underlying infrastructure. A company that gets backend services from a serverless vendor is charged based on their computation and do not have to reserve and pay for a fixed amount of bandwidth or number of servers, as the service is auto-scaling. Note that despite the name serverless, physical servers are still used but developers do not need to be aware of them.

What is serverless computing? | Serverless definition

What is Serverless?

Serverless Computing – Amazon Web Services

AWS Lambda Serverless Functions

AWS Lambda is a serverless compute service that lets you run code without provisioning or managing servers, creating workload-aware cluster scaling logic, maintaining event integrations, or managing runtimes. With Lambda, you can run code for virtually any type of application or backend service - all with zero administration.

Introduction to AWS Lambda - Serverless Compute on Amazon Web Services

In this lab task, you will be creating a serverless lambda function to automatically create thumbnails. Whenever an image is uploaded to the S3 bucket, it should automatically trigger the lambda function.

Point to keep in mind: When you start the lab, wait for "Open Console" button to appear on the left panel. While in AWS Lambda console, ensure that you have UNCHECKED using the new UI, make sure to use the old/former UI as Qwiklabs have not yet been updated for the new UI

TASK1: Click on the below link to go to Qwiklabs lab: Introduction to AWS Lambda - Qwiklabs Lab and Click "Join to Start This Lab"

AWS API Gateway

AWS API gateway is a fully managed service that makes it easy for developers to create, publish, maintain, monitor and secure APIs. API acts as a front door for the application to access data, business logic or functionality from the backend services. It handles all the task involved in accepting and processing up of hundreds or thousands of concurrent API calls, including traffic management, authorization, access control, monitoring and API management.

https://aws.amazon.com/api-gateway/

Building APIs with Amazon API Gateway

Five Reasons to Consider Amazon API Gateway for Your Next Microservices Project – The New Stack

This lab task will involve using your learnings from the previous task(Lambda). In this lab task you will create an AWS lambda function to return random Questions and answers(FAQs), and this lambda function will be exposed using a REST API endpoint created(and managed) using API Gateway.

Point to keep in mind: While in AWS Lambda console, ensure that you have UNCHECKED using the new UI, make sure to use the old/former UI as the Qwiklabs have not yet been updated for the new UI

TASK2: Click on the below link to go to Qwiklabs lab: Introduction to AWS API Gateway- Qwiklabs Lab and Click "Join to Start This Lab"

Lab 11 - Introduction to AWS Identity and Access Management (IAM)

Week 11 Tasks:

1. Explore the Users and Groups

a. 1a.png - list of groups showing that they have zero users in each group

b. 1b.png - Showing policy for EC2-Support group.

2. Add Users to the Groups

a. 2a.png - Showing each user with the groups they have been added to.

b. 2b.png - Showing each group having one user.

3. Testing User Access

a. 3a.png-Showing User-1 having access to view details S3-Bucket

b. 3b.png-Showing User-1 having NO access to view details EC-2 Instances

c. 3c.png-Showing User-2 having access view details EC-2 Instances, but not able to stop instance.

d. 3d.png-Showing User-2 having NO access view details S3-Bucket.

e. 3e.png-Showing User-3 having able to stop instance, since the user is a admin

4. 4a.png or 4a.jpg – Showing email confirmation from QWIKLABS for having completed the lab successfully. The SS should clearly show the timestamp in the received email.

Introduction to Qwiklabs

Qwiklabs is an online platform that provides end to end training in Cloud Services. This a platform where you can learn in a live environment anywhere, anytime and on any device. Qwiklabs offers training through various Labs which are specially designed to get you trained in Google Cloud Platform (GCP) as well as Amazon Web Services (AWS). Qwiklabs has joined hands with Google and now works as a part of Google Cloud. Every year Qwiklabs delivers thousands of labs and has happy learners all over the globe.

Points to Note:

1. **Although Qwiklabs uses AWS, you will NOT be using your AWS Educate Account. Qwiklabs will create a temporary AWS account with all the required permissions and access to complete the lab.**

2. **When using the Qwiklabs created AWS account, DO NOT change the default region/VPC or any other settings that are automatically created by Qwiklabs.**
3. **The Qwiklabs lab has a time limit (45 minutes) within which the Qwiklab lab has to complete, after the timer hits zero, the AWS account will be removed and you will have to restart the lab from scratch.**
4. **All code and config for Qwiklab labs is already given, you need not code anything from scratch.**
5. **To prevent conflicts with any AWS account that you have already signed into the browser, use Incognito/Private mode, to ensure you have a fresh browser with not previous logins.**
6. **Ensure that you have signed into Qwiklabs using your Google account.**

Introduction to IAM

AWS Identity and Access Management (IAM) enables you to manage access to AWS services and resources securely. Using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources.

IAM is a feature of your AWS account offered at no additional charge. You will be charged only for use of other AWS services by your users.

How it works?

IAM assists in creating roles and permissions. AWS IAM allows you to:

Manage IAM users and their access – You can create users in IAM, assign them individual security credentials (in other words, access keys, passwords, and multi-factor authentication devices), or request temporary security credentials to provide users access to AWS services and resources. You can manage permissions in order to control which operations a user can perform.

Manage IAM roles and their permissions – You can create roles in IAM and manage permissions to control which operations can be performed by the entity, or AWS service, that assumes the role. You can also define which entity is allowed to assume the role. In addition, you can use service-linked roles to delegate permissions to AWS services that create and manage AWS resources on your behalf.

Manage federated users and their permissions – You can enable identity federation to allow existing identities (users, groups, and roles) in your enterprise to access the AWS Management Console, call AWS APIs, and access resources, without the need to create an IAM user for each identity. Use any identity management solution that supports SAML 2.0, or use one of our federation samples (AWS Console SSO or API federation).

Click on the link below to go to Qwiklabs lab (and then click **Join to Start this Lab** followed by **Start Lab** after which you will see **Open Console** button appearing on the left panel after 1 to 2 minutes) **AWS IAM**

Note: Before you click **Start Lab**, make sure you review the following 3 Tasks and then execute all these tasks in **45 minutes**

Task-1: Explore the Users and Groups (You need to execute Steps 3-21 here)
Task-2: Add Users to Groups (Execute Steps 22-29)
Task-3: Sign-In and Test Users (Execute Steps 30-59)
Task-4: End Lab (Execute Steps 60-64)

During Task-3 you will be asked to logout and log in with a different user ID three times, so note down the Account ID and the user sign-in link (which will look similar to https://123456789012.signin.aws.amazon.com/console) displayed on IAM dashboard in a separate text file. In this link 123456789012 denotes the Account ID which you will need to login with a different user id.

If your lab time expires in the middle, you can start a new lab and go straight to Task-2 Step 22 (if you have saved SS of Task-1 already).