## Aim: Study Infrastructure as a Service

## Theory:

## 1. Prepare a detailed study of Infrastructure as a Service.

IaaS (Infrastructure as a Service) is a cloud service that gives customers access to an immediately usable, highly scalable IT infrastructure over the internet. Storing, running, and maintaining the hardware is the provider’s responsibility. The typical cost accounting model for IaaS is the pay-per-use method, in which customers only pay for what they have used.

A service provider rents out its own IT infrastructure and makes it available to use online. To do this, the cloud provider usually operates its own data centers where the corresponding hardware is stored, administered, and maintained. By doing this, IaaS providers can offer access to computing power (processor, memory, hard drive space) and complete network structures (including firewalls, routers, and security/back-up systems), the scope of which you, as a customer, can freely dispose of. You can choose which infrastructure you want to use, how many servers, routers, firewalls you want to use, and what performance data (CPU, RAM, etc.) the various network elements should have.

The rented IaaS resources can be scaled up or down at any time if you want to integrate an additional server or reduce the computing power. With most providers, however, you only pay for the components that you actually use.

Features that IaaS operators provides :

- Establish, maintain and keep data center infrastructure up-to-date
- Protect the data center against external influences
- Provide computing power (CPU, working memory) and storage space
- Provide server and network structures as well as databases
- Create a virtualization environment that customers can use to access the IaaS resources provided
- Provide software that enables customers to control and administer the virtualized IT infrastructure

Roles of Customers to use IaaS :

- Choose and structure the desired virtual infrastructure
- Install, configure, and regularly update operating systems and any application software required for your own purposes
- Run the IaaS network and configure the firewall
- Protect the operating systems and any other installed software (also applies to own applications, of course) using security software

- Encrypt data and data connections
- Set up authentication mechanisms, identity controls, and access controls

Types of IaaS:

1. Public IaaS : It is the basic version of the practical cloud service. The term “public” is derived from the fact that the resources offered are generally shared by all the provider’s customers and accessed via the internet. However, sharing hardware leads to conflicts, as all resources are virtualized and detached from a specific computer.
2. Private IaaS : The concept of private IaaS differs from the actual idea of infrastructure as a service in that it is not an external service provider, but an in-house IT department that provides the supplies and leases the resources. This way, the company benefits from the possibilities of IaaS technology without losing control over data and security. However, this means that the scalability is no longer flexible. In addition, the company itself is responsible for the physical environment.
3. Hybrid IaaS : It is a solution that combines public and private IaaS. With this solution, the resources are obtained both from an internal service provider and from an external provider. This makes it possible to manage sensitive company data on your own while the scalable external resources are used for other purposes.

Some IaaS providers are Amazon Web Services (AWS), Netmagic solutions,Rackspace,Etc.

## 2. Advantages and Limitation of IaaS.

Advantages:

- No hardware costs, easily controllable running costs.
- Quick to implement and provide new projects.
- High flexibility thanks to simple scalability of the required resources.
- No need to set up, maintain, or update the hardware.
- Easy to connect several company locations to the rented IaaS environment.

Limitations:

- Dependency on the provider, whose sole responsibility is to make sure the service is available and secure.
- Internet access is essential (problems with the internet connection also cause problems with the IaaS environment).
- Changing providers is very complicated.
- Possible privacy issues due to the provider’s server locations.

## 3. Study security issues in IaaS.

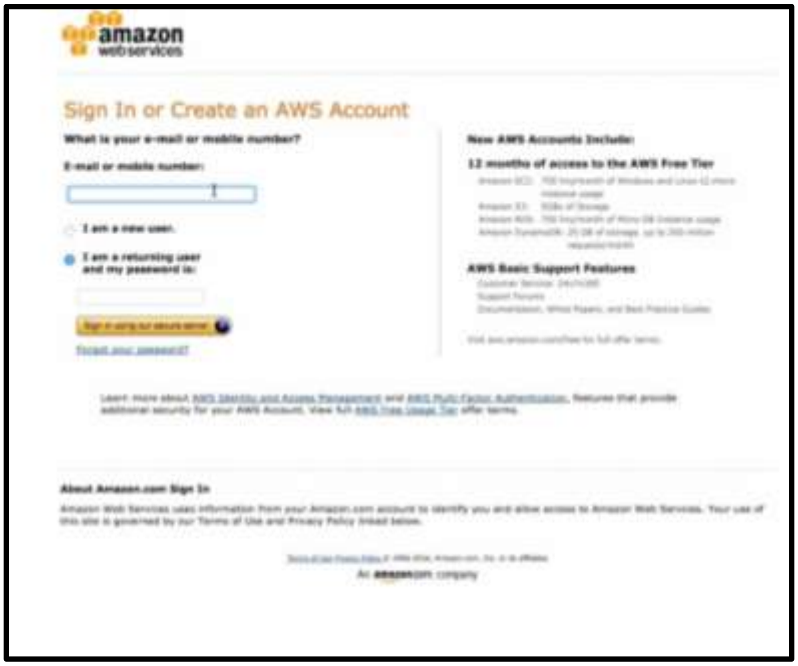
1. Misconfiguration : This is one of the most common cloud security missteps around: when setting up a new cloud server or even a simple storage bucket, IT staffers often don't properly configure their authentication or security standards, leaving potentially sensitive information vulnerable to unauthorized access.
2. Changes in visibility : This isn't necessarily a risk unto itself but is rather a compounder of other risks. For an IT team, you will never have as much visibility into an IaaS environment as an on-premises one that is completely controlled by your organization. Even the most transparent IaaS providers cannot offer the full visibility of an on-premises server, which means your ability to detect and respond to threats may be impaired or delayed.
3. Blocking data exfiltration : Because a client is not in full control of the server environment, it may be difficult to block exfiltration to someone without legitimate credentials – or who is using legitimate credentials illicitly.
4. Cloud email isn't as secure : Cloud email platforms have many of the same vulnerabilities as other email products – chief among them is a vulnerability for human error. These email platforms also typically offer less robust protection than secure email gateway products, which don't typically translate well to the cloud which can lead to phishing emails.
5. Different points of vulnerability : When transitioning to a cloud environment, it's very popular for developers to do what's called a "lift-and-shift," i.e., simply deploying all existing apps and solutions on the cloud as though it were the on-premises server. However, a lift-and-shift deployment neglects to account for there being different points of vulnerability in a cloud environment as opposed to an on-premises one. Specialized tools may not work as well, if at all. Consequently, any infosec team used to rely on a given set of tools may find themselves blindsided by things they didn't expect and scrambling to respond.
6. Physically different locations : Every single interaction from a team working in an IaaS environment goes over the Internet. In theory, employees should notice little to no difference when data centers are in different locations, but these additional locations mean that there must be additional firewall or routing rules to handle traffic accordingly. Complexity is the enemy of security – more points for failure.
7. Compliance and regulation differences : This is particularly true for business that does business internationally or with governments around the world and may be required to follow certain regulations or compliance protocols that their cloud providers might not be. If your IaaS provider isn't in compliance, you might not be in compliance, and so it's imperative to check.
8. Breaking Authentication : Access to the accounts used to provision (and terminate) virtual machines and other cloud services enables the attacker to simply use the cloud service's API or user interface to destroy services or grant additional access as desired.

The credentials to access the cloud service could be obtained by, e.g., installing a keylogger on an administrator's desktop as a part of a broader breach on the internal network.Obtaining any API credentials, database credentials, or private keys used by the cloud service could also provide an attacker free access to those services.

## Activity

## Use AWS to create a VM and configure it. Access the created machine remotely.

1. Use AWS to create a VM and configure it



Sign In or Create an AWS Account

What is your e-mail or mobile number?

E-mail or mobile number:

○ I am a new user.

● I am a returning user and my password is:

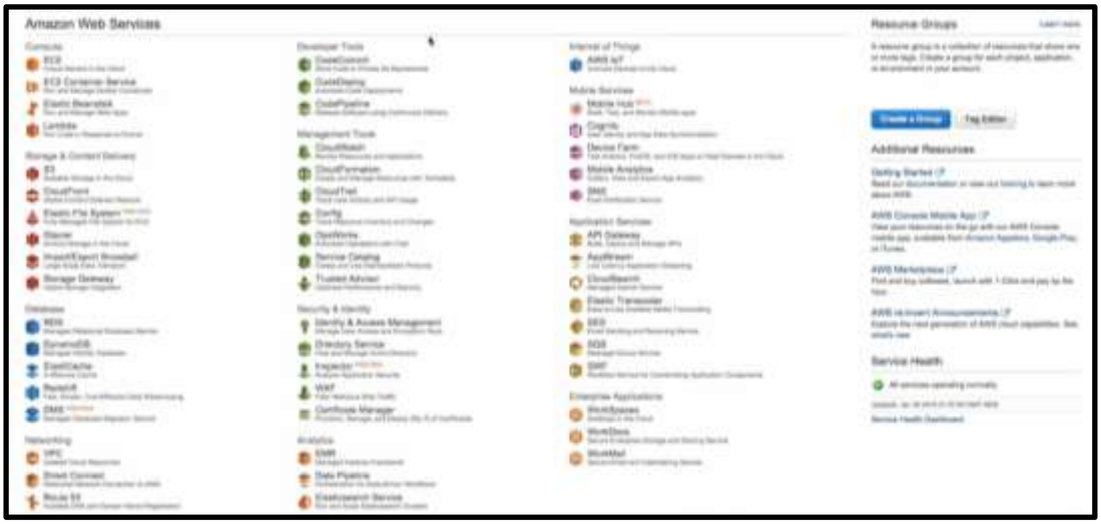
New AWS Accounts Include:

12 months of access to the AWS Free Tier

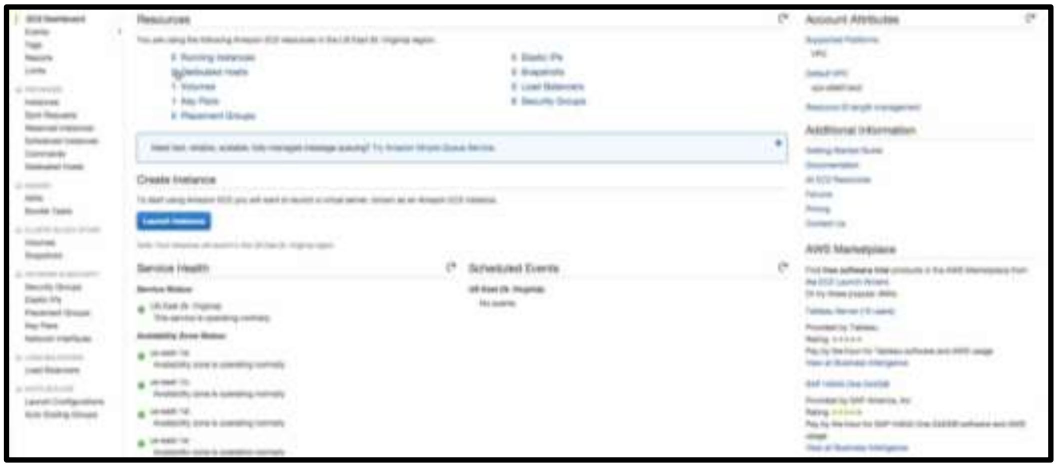
AWS Basic Support Features

About Amazon.com Sign In

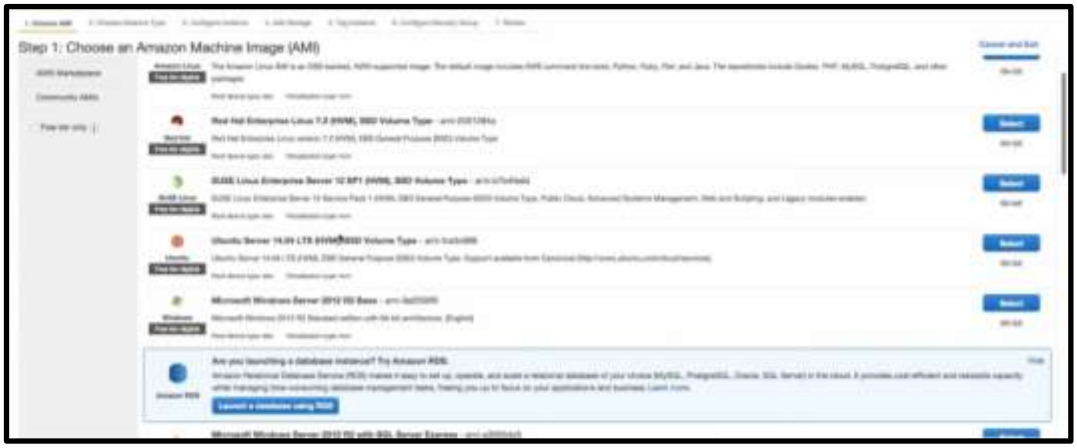
2. After logging into your account, AWS displays the AWS management console



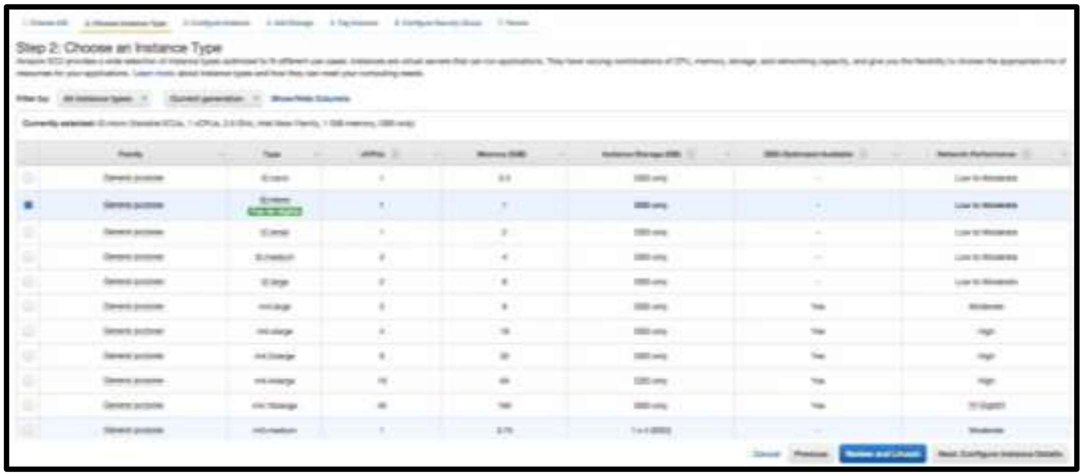
3. Click on the EC2 service which displays the EC2 dashboard



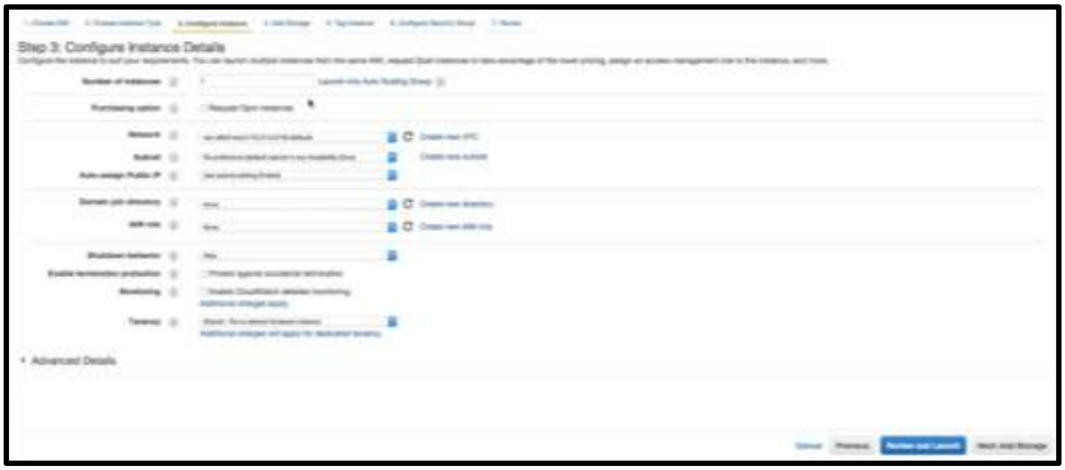
4. Click on the launch instance and choose an Amazon Machine Image (AMI). Windows server 2012 is chosen here.



5. Next, choose an instance type

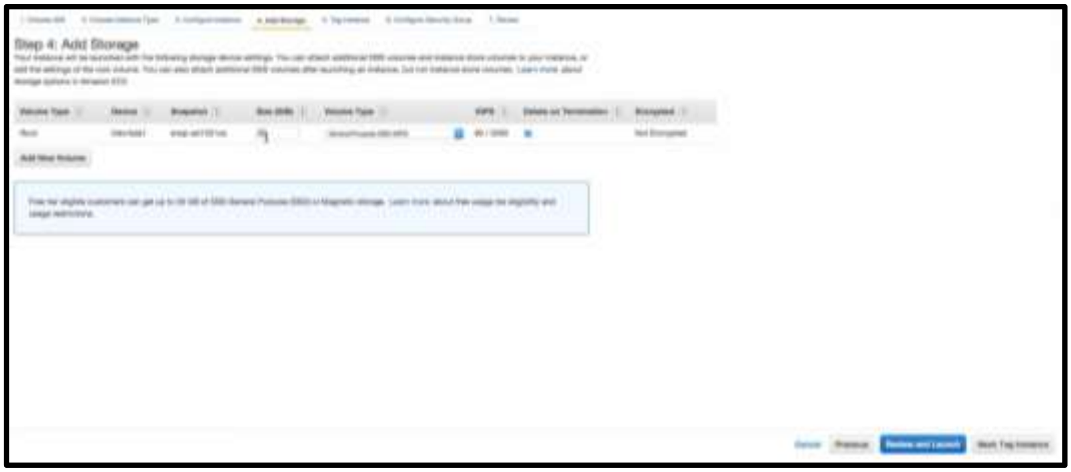


6. Configure the instance details



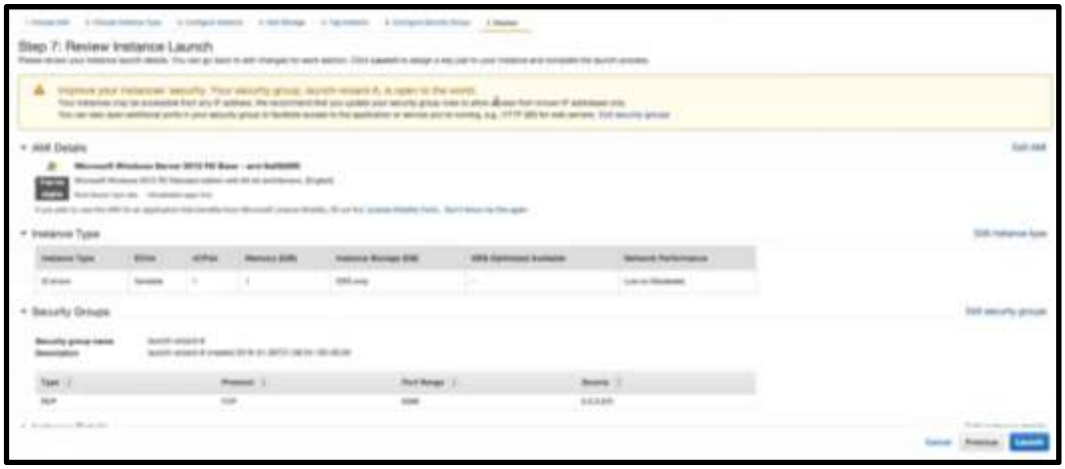
Step 3: Configure Instance Details

7. Choose the amount of storage



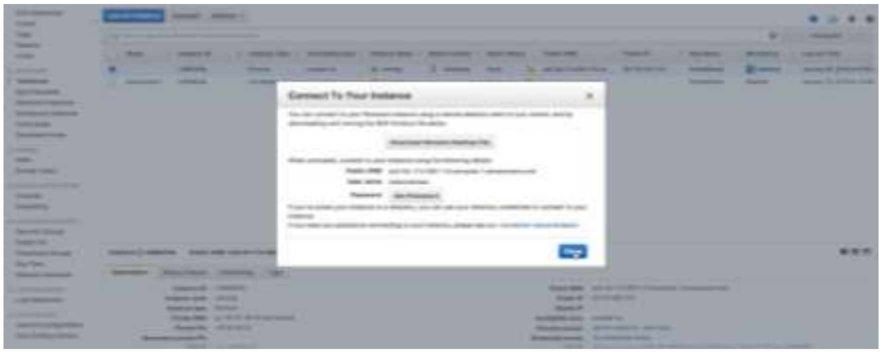
Step 4: Add Storage

8. Then, AWS displays the Review Instance Launch window to view all the launch parameters



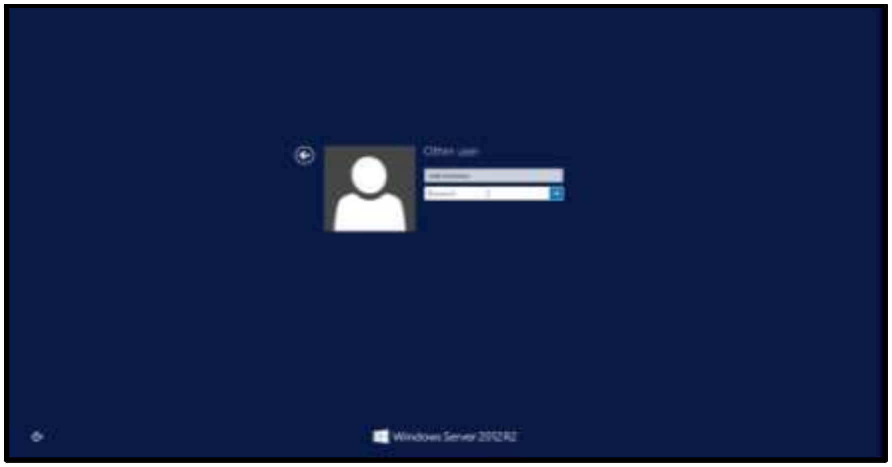
Step 7: Review Instance Launch

9. After clicking on Launch, the EC2 dashboard is displayed and on the EC2 dashboard, click on the newly created VM and launch it by clicking on the Download Remote Desktop File (RDF)

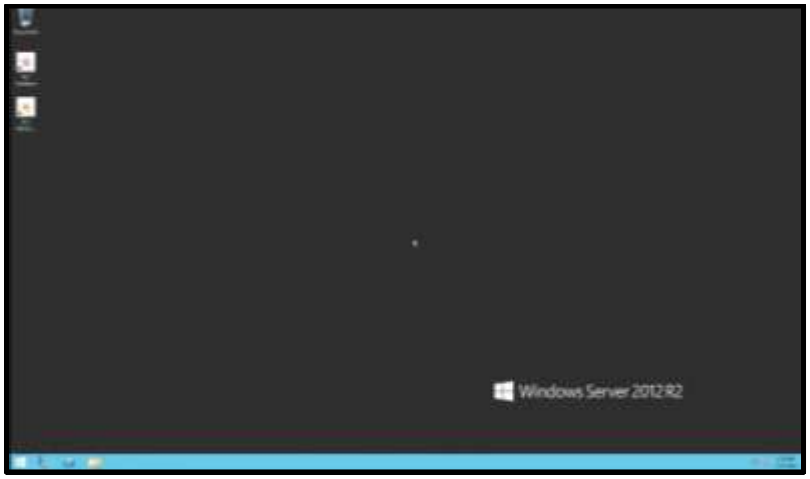


**Access the created machine remotely**

After the RDF file is downloaded, login into your VM



After logging in, use the VM



## CONCLUSION :

- From this experiment we learned about Infrastructure as a Service which is a cloud service that gives customers access to an immediately usable, highly scalable IT infrastructure over the internet.
- The benefits of using IaaS are it has Shared infrastructure which will allow multiple users to share a same physical infrastructure, web access to the resources allowing users to access resources over the internet, Pay-as-per-use model, Focus on the core business rather on the IT infrastructure.
- It also allows On-demand scalability which is one of the biggest advantages of IaaS. Using IaaS, users do not worry about to upgrade software and troubleshoot the issues related to hardware components.
- We also performed an activity where we used Amazon Web Services (AWS) to create a VM using AWS EC2 where we configured the EC2 instance and then we used ssh to login into the created machine remotely.

## REFERENCES

1. https://www.ionos.com/digitalguide/server/know-how/iaas-infrastructure-as-a-service/

2. https://www.ssh.com/cloud/iaas/

3. https://www.lastline.com/blog/8-iaas-cloud-security-challenges-you-should-be-aware-of/

4. https://www.javatpoint.com/infrastructure-as-a-service

5. https://docs.aws.amazon.com/efs/latest/ug/gs-step-one-create-ec2-resources.html