CREATE EC2 INSTANCE FROM CUSTOM AMAZON MACHINE IMAGES (AMI)

PRESENTED BY GROUP 10
COMPRISING OF THE FOLLOWING

ENUGU STATE CYBER SECURITY LEARNING PROGRAM
(ECSL)

OCTOBER, 2022

OBJECTIVES OF THE STUDY

The general objective of this study is to empirically demonstrate how an EC2 instance can be created directly from the Amazon machine image (AMI) catalog. The specific objectives of the study include:

1. To examine its relationship with security and analyze some security best practices associated with the use of EC2 and the AMI.
2. To demonstrate with the use of screenshots, the processes involved in launching another EC2 instance from one of our privately owned or custom AMIs.
3. Analyze some of the significant benefits of the AMI to security, businesses and organizations that make use of it.

BACKGROUND OF THE STUDY

+ Learning the terminology in cloud computing can take a little time. The first step is realizing what the cloud itself can do for our businesses – mostly, it's about scaling computing services. The servers we use do not run locally in a data center but in a remote facility acquired, managed and delivered to us by the cloud service providers with the biggest being the Microsoft Azure, Google Cloud and our very own Amazon Web Service (AWS) which our project is limited to. There are options for cloud storage, compute performance on virtual servers, and running web applications.

Definition of some key terms related to our study;

Amazon Elastic Compute Cloud (EC2):

Provides scalable computing capacity in the Amazon web services (AWS) cloud. Using Amazon EC2 eliminates our need to invest in hardware upfront, so we can quickly develop and deploy applications faster. We can use the EC2 to launch as many or as few virtual servers as needed, configure security and networking and also manage storage. EC2 is incredibly popular in recent times because of its high scalability rate, growing as our business changes and evolves and also because the costs associated with the virtual infrastructure are based on actual usage.

Amazon Machine Image (AMI):

An Amazon machine image (AMI) is a template, pre-configured or customized for our computing needs. The configuration can be an operating system, an application server and applications. From an AMI, one can easily launch an instance or multiple instances, which is a copy of the AMI running as a virtual server in the cloud. Our instances keep running until it is stopped, hibernated, terminated or fails. AWS publishes many AMIs that contain common software configurations for public use. In addition, members of the AWS developer community have published their own custom AMIs. You can also create your own AMI or AMIs; doing so enables you to quickly and easily start new instances that have everything you need. In our example, our application is a website and upon its creation, our AMI included a web server, the associated static content, and the code for the dynamic pages. As a result, after we successfully launched our instance from the AMI, our web server started up and our application was ready to accept requests.

You can deregister an AMI when you have finished using it. After you deregister an AMI, you can't use it to launch new instances. Existing instances launched from the AMI are not affected. Therefore, if you are also finished with the instances launched from these AMIs, you should terminate them to avoid extra charges.

RELATIONSHIP TO SECURITY AND BEST PRACTICES

In cloud computing, security is treated as a high priority and AWS is no exception. As an AWS customer, one tends to benefit from a data center and network architecture that are built to meet the requirements of the most securely sensitive organizations. Security is a shared responsibility between AWS and their customers. The shared responsibility model describes this as “security of the cloud and security in the cloud”.

On the part of AWS, they provide protection and security of the infrastructure that runs their services such as the EC2 and AMI in the cloud while it is the responsibility of us being the cloud customers and users to secure our instances in the following areas:

- Controlling network access to our instances through configuring our VPC and security groups.
- Managing the credentials used to connect to our instances and restricting access by only allowing trusted hosts or networks to access ports on our instance. For example, restricting SSH access by restricting incoming traffic on port 22.
- Managing the guest operating system and software deployed to the guest operating system including updates and security patches.
- Configuring the IAM roles that are attached to the instance and those permissions associated with those roles.
- Review the rules in our security groups regularly and ensure that we apply the principle of least privilege – only open up permissions that we require. One can also create different security groups to deal with instances that have different security requirements.

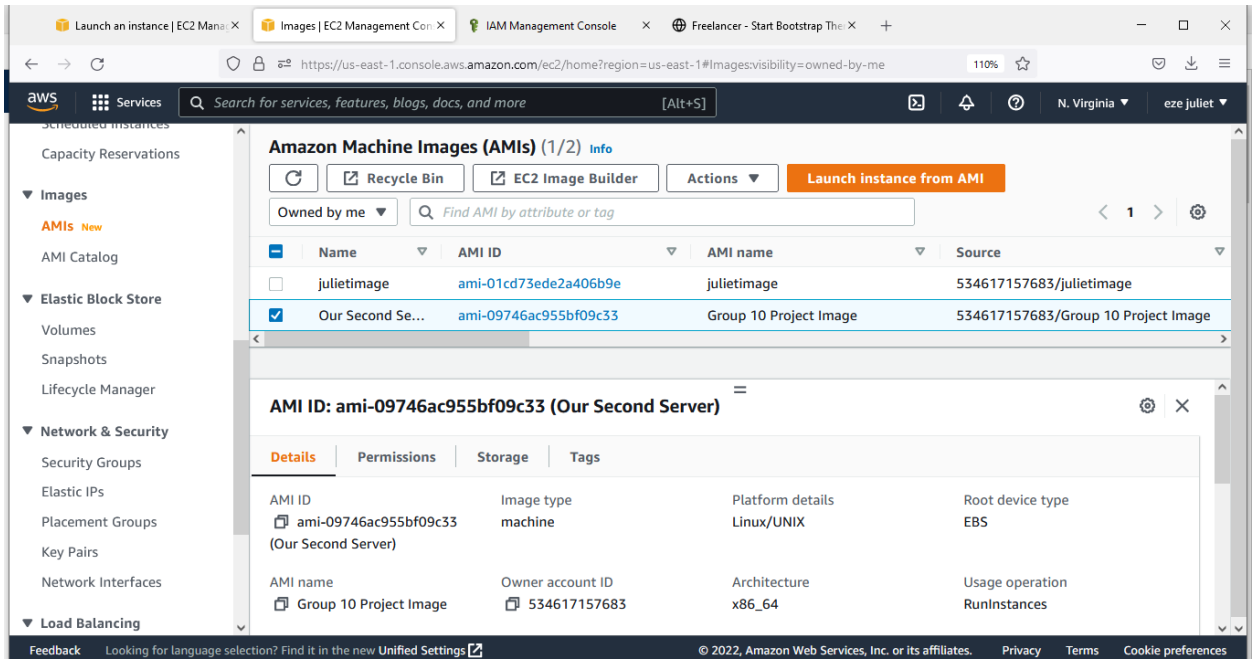
- Use AWS Identity and Access Management (IAM) to control access to our AWS resources including instances. One can also create IAM users and groups under our AWS account, assign credentials to each and control the access that each has to resources and services in AWS.
- Disable password-based logins for instances launched from our AMI. Passwords can be found or cracked and are a security threat.

HOW TO CREATE AN EC2 INSTANCE FROM A CUSTOM AMI

To launch a new EC2 instance from an AMI, do the following:

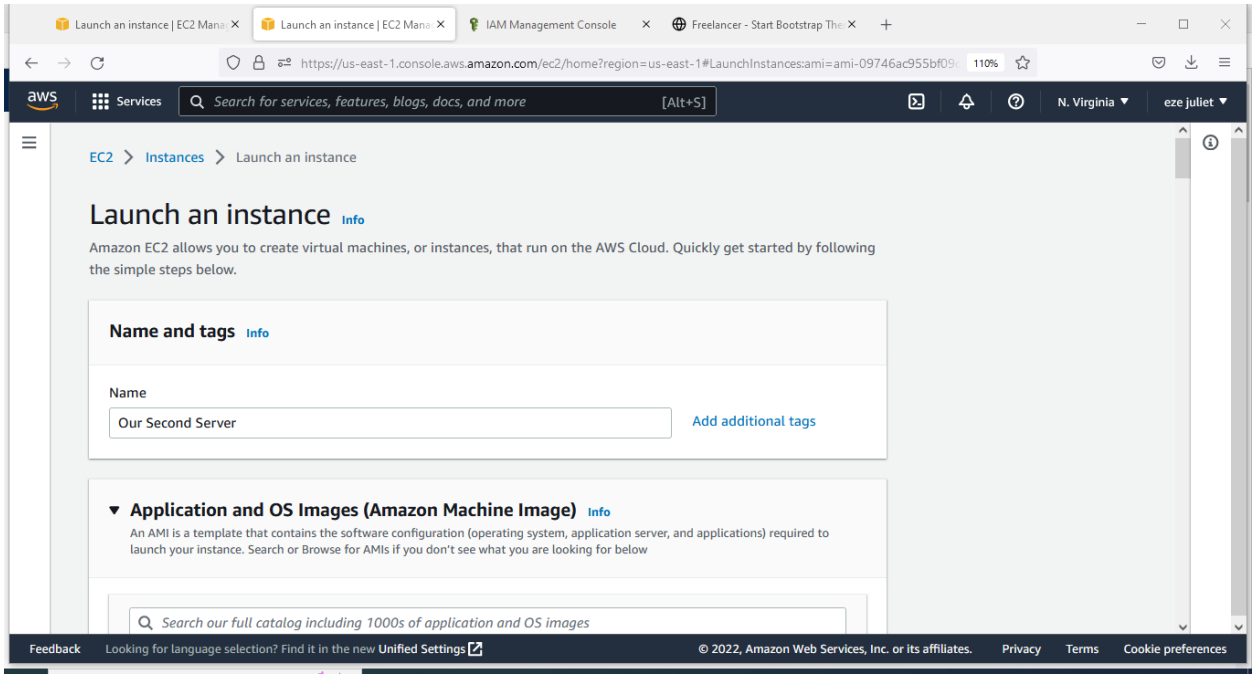
1. Open the EC2 console.
   Note: Be sure to select the AWS region that you want to launch the instance in.
2. From the navigation bar, choose AMIs.
3. Find the AMI that you want to use to launch a new instance. To begin, open the menu next to the search bar, and then choose one of the following:
   If the AMI that you are using is one that you created, select Owned by me.
   If the AMI that you are using is a public AMI, select Public images.

If the AMI that you are using is a private image that someone else

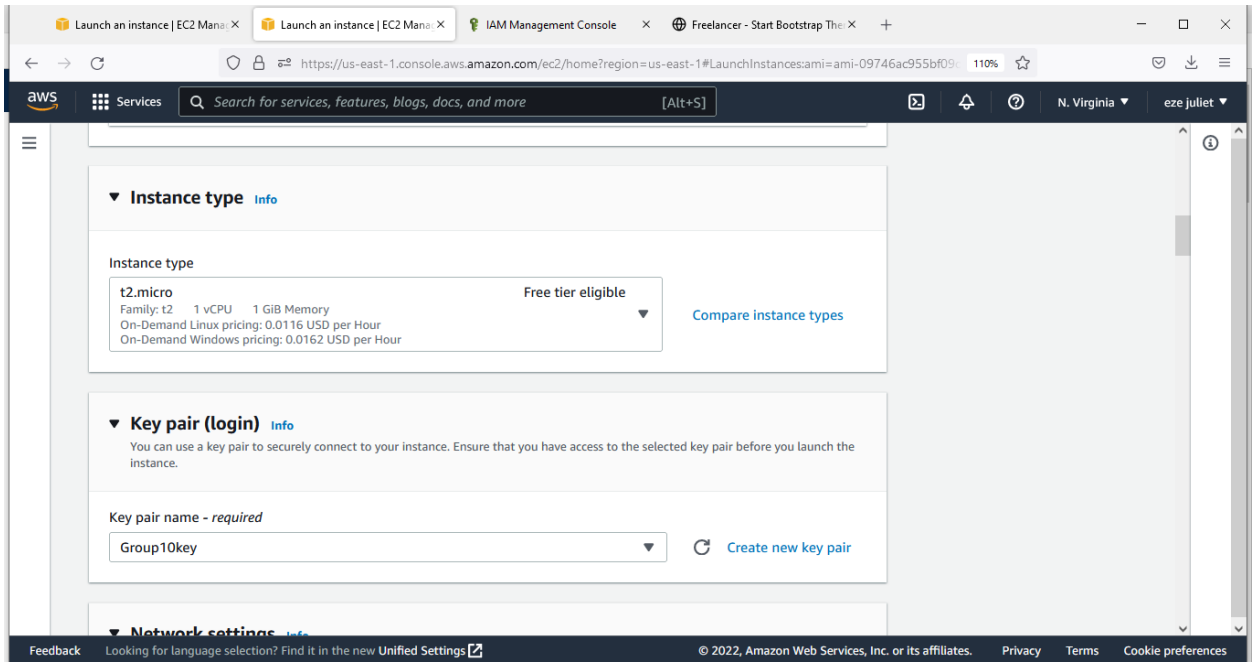


shared with you, select Private images. We selected the owned by me option because our task is limited on creating our own customized AMI instance.

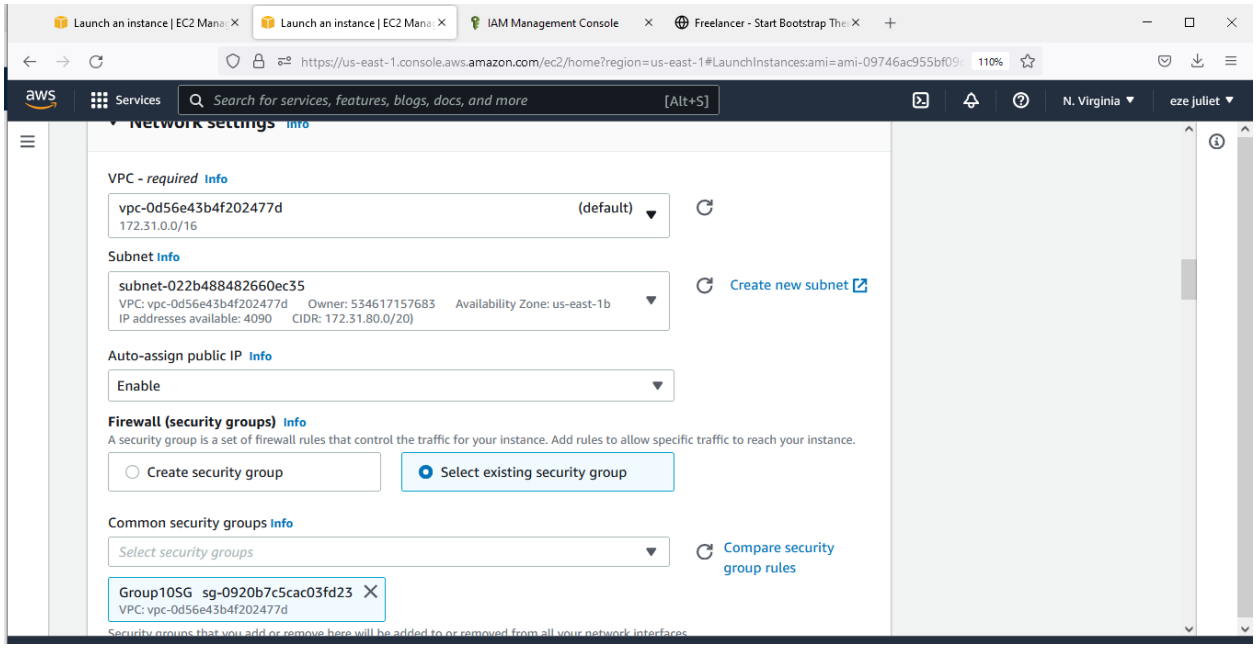
4. Select the desired AMI, and then click on Launch instance.
5. Give it a name for easy identification.



6. Create a Key pair to use to securely connect to our instance or use an existing one.



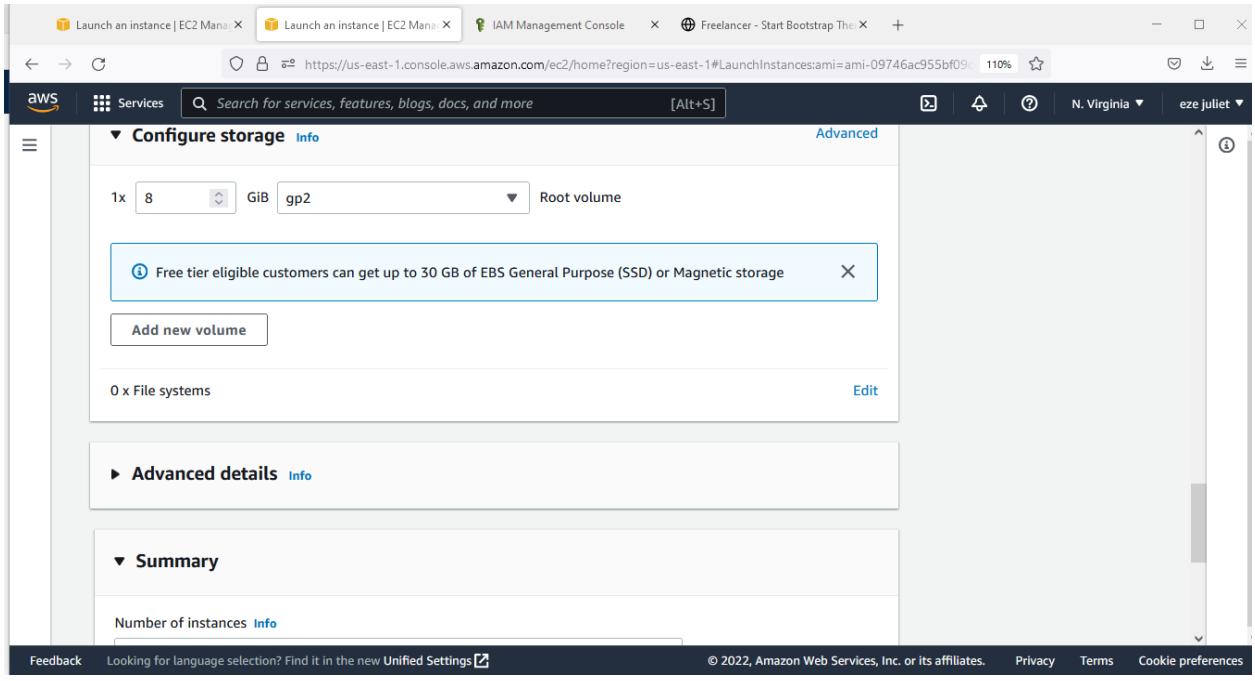
7. Configure network settings (security groups and availability zones) We used the 1b subnet to separate our custom AMI server from the availability zone of our first instance.



We attributed the same security group which we used to launch our first instance to this one because we want them to have the same security group parameters.

Note: We are creating our second web application server from our custom AMI.

8. Configure Storage: We will launch the EC2 instance using the default 8 GiB disk volume.

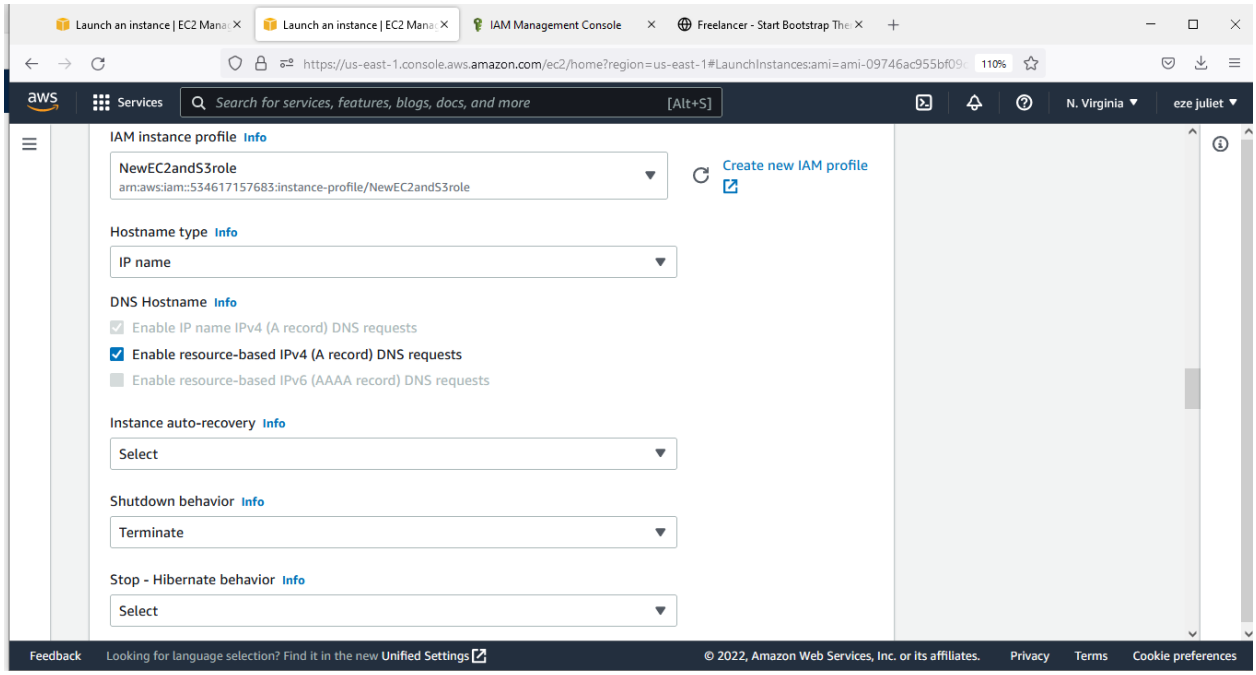


9. Configure the Advanced Details

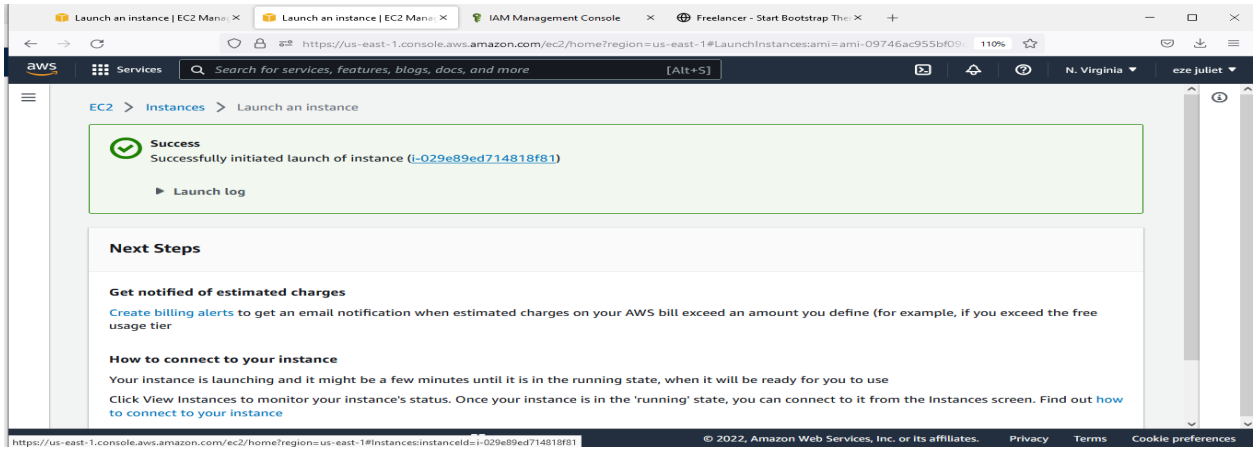
   Give it our created IAM role which allows EC2 to call up and execute our website code on S3.

   Shutdown Behavior: Terminate

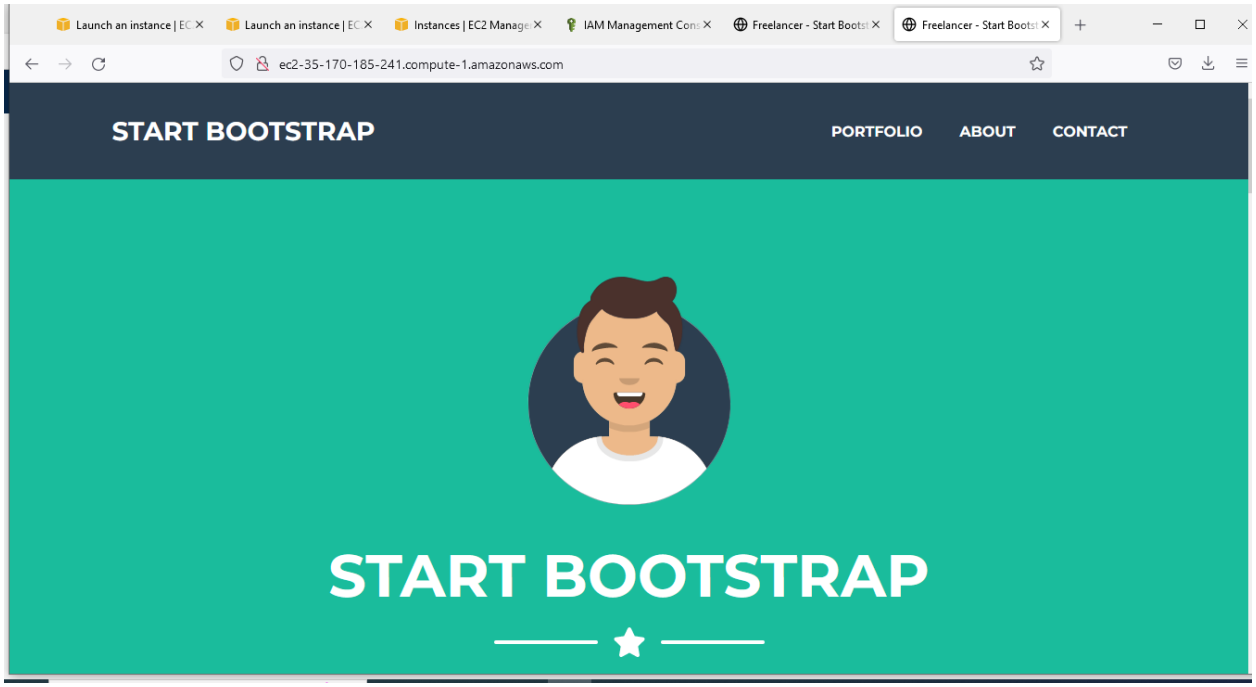
   Tenancy: Shared host



Review the summary and click on the launch instance button to create our instance.



10. Once it is up and running, copy the public ipv4 DNS number and try exploring on the browser to ensure it is working perfectly and our second website is up and running.



Viola!!!!!! Our website is up and running.

SIGNIFICANT BENEFITS OF USING AMI TO ORGANIZATIONS AND SECURITY

Like cloud computing itself, using an AMI has several important advantages.

Faster set-up

One of the key benefits of an AMI deployment is the fact that it also speeds up configuration and deployment because the templates are well-known and defined or customized for typical computing infrastructure needs. The alternative is much more complex. Developers would have to define the parameters they need on their own data center servers or architect the virtual servers and settings on their own. But with AMI, this is all accomplished in a more seamless way and it also aids the quick recovery of failed instances.

Aids Innovation and Invention

It helps new startup companies launching out new products or applications to be able to scale and experiment with new application features or by releasing additional apps without worrying about the infrastructure itself as a result of the pay-as-you-go cost structure and speed of deployment.

Integration with the AWS Marketplace, allowing software vendors to charge for the use of their AMIs

With products bought through the AWS marketplace, payment is made simple. All billing is contained within the marketplace platform and payments are taken using customers' existing AWS billing details. This

pricing is set by the vendor but is clearly stated on the marketplace page, along with the usage fees for related web services. The AMI is one of such customized services marketed and sold by third party software vendors on the AWS marketplace thereby providing them an additional source of income through an annual and hourly pricing structure.

Flexibility

Flexibility is another key benefit as well. It can run linux, unix, windows or website servers and can be augmented with other services. It is also compressed, encrypted, and secured no matter which operating system is used.

Lower cost advantage

An AMI is a virtual machine that runs in the cloud, and one can easily deploy and configure each one according to business needs. For massive Big Data Projects, an organization can easily deploy multiple instances on an AMI and pay for the higher usage, but even a small startup could deploy instances for a simple mobile app. There are no up-front costs. The pricing structure is based on a pay-as-you-go model.

CONCLUSION

With an AMI, we have the ability to quickly and efficiently determine what computing power, memory, storage, and other factors we need for our applications and also get to deploy them faster and easier.

Finally, working on this project was a little bit tedious as a result of the fact that we needed to research around the topic to deliver in a little time duration and coupled with the fact that we had other program activities lined up to complete at the same interval. Apart from this, it was fun working on this topic. Researching, running the hands-on and coming up with the final draft makes us feel like certified cloud practitioners already and I know that if we keep up with the pace, the sky would definitely be our stepping stone.

So in a special way, I would like to say a big thank you to our amazing trainer for the excellent work you did in taking us on this journey up to this very moment and the entire Cybersafe team for holding our hands and exposing us to this great path filled with amazing opportunities. This wouldn’t have been possible without you all. Thanks