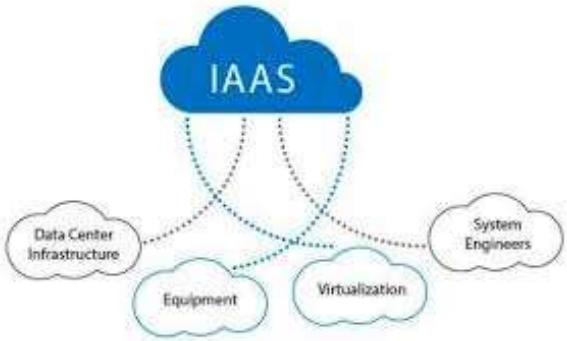
Academic Year: 2021-2022 **Semester: VIII**
Subject: Cloud Computing Lab **Class / Branch / Division: BE/CMPN A**
Name: Nithin Menezes **Roll Number: 56**

Experiment No:3

Aim: To demonstrate and implement IAAS service using AWS (Use t2.Micro (Free tier eligible) (instance only).

Theory:

Prepare a detailed study of Infrastructure as a Service



Iaas is also known as **Hardware as a Service (HaaS)**. It is one of the layers of the cloud computing platform. It allows customers to outsource their IT infrastructures such as servers, networking, processing, storage, virtual machines, and other resources. Customers access these resources on the Internet using a pay-as-per use model.
In traditional hosting services, IT infrastructure was rented out for a specific period of time, with pre-determined hardware configuration. The client paid for the configuration and time, regardless of the actual use. With the help of the IaaS cloud computing platform layer, clients can dynamically scale the configuration to meet changing requirements and are billed only for the services actually used.
IaaS cloud computing platform layer eliminates the need for every organization to maintain the IT infrastructure.
IaaS is offered in three models: public, private, and hybrid cloud. The private cloud implies that the infrastructure resides at the customer-premise. In the case of public cloud, it is located at the cloud computing platform vendor's data center, and the hybrid cloud is a combination of the two in which the customer selects the best of both public cloud or private cloud.21.

IaaS provider provides the following services -

1. **Compute:** Computing as a Service includes virtual central processing units and virtual main memory for the Vms that is provisioned to the end- users.
2. **Storage:** IaaS provider provides back-end storage for storing files.
3. **Network:** Network as a Service (NaaS) provides networking components such as routers, switches, and bridges for the Vms.
4. **Load balancers:** It provides load balancing capability at the infrastructure layer.

Advantages and Limitation of IaaS

Advantages of IaaS cloud computing layer

There are the following advantages of IaaS computing layer -
1. Shared infrastructure
IaaS allows multiple users to share the same physical infrastructure.
2. Web access to the resources
Iaas allows IT users to access resources over the internet.
3. Pay-as-per-use model
IaaS providers provide services based on the pay-as-per-use basis. The users are required to pay for what they have used.
4. Focus on the core business
IaaS providers focus on the organization's core business rather than on IT infrastructure.
5. On-demand scalability
On-demand scalability 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.

Disadvantages of IaaS cloud computing layer

1. Security
Security is one of the biggest issues in IaaS. Most of the IaaS providers are not able to provide 100% security.
2. Maintenance & Upgrade
Although IaaS service providers maintain the software, but they do not upgrade the software for some organizations.
3. Interoperability issues
It is difficult to migrate VM from one IaaS provider to the other, so the customers might face problem related to vendor lock-in.

Study security issues in IaaS

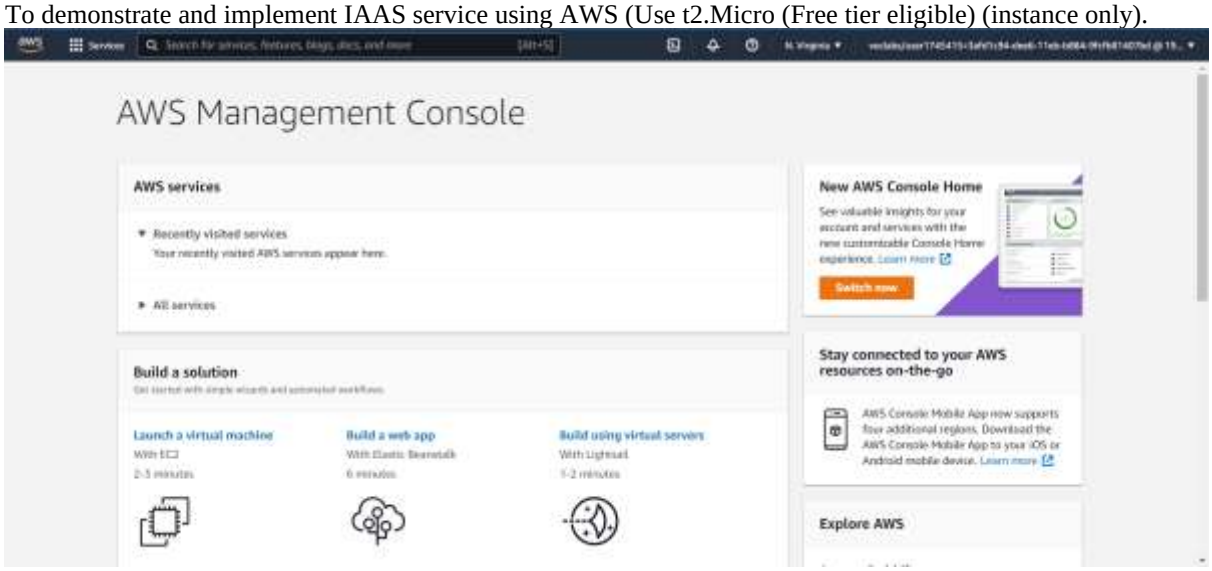
- **Misconfiguration.**
- In my experience, this is one of the most common cloud security missteps around: when setting up a new cloud server or even a simple storage bucket, IT staffers often don't properly configure their authentication or security standards, leaving potentially sensitive information vulnerable to unauthorized access. This is almost always a question of user error, typically on the part of the client – so always remember to double-check all security settings with your new IaaS provider for optimal cloud data protection… and if you're not sure if you've properly configured things? Ask an expert.
- **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. I recommend protecting your organization by partnering with a cloud service provider with a proven track record of rapid response to newly-found threats and vulnerabilities.
- **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. Mitigate this risk by having additional control measures in place to monitor the use of privileged accounts and movement of data outside of an established baseline.
- **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. I can count scores of times recently where emails that clearly should have never made it to my inbox ends up with me having to report it to the cloud email provider as a phishing email.
- **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. This is common because it is cheaper to use extant solutions rather than adopt or develop new ones. It also results in fewer interruptions to productivity as employees can continue using tools to which they're accustomed. 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.
- **Physically different locations.**
- Every single interaction from a team working in an IaaS environment goes over the Internet. An environment can become exponentially more complex if the cloud servers aren't in the same data center. For example, suppose an enterprise expects a sudden need for extra capacity and purchases more from their platform provider, but there is no more room in their extant data center so the new applications and computers must be located in a physically different one. In theory, employees should notice little to no difference, 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, especially given point

- **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. For example, certain nations require the use of sovereign crypto algorithms that aren't in use elsewhere. Does your IaaS provider support them?
- **You're responsible for your IaaS provider's mistakes.**
- This isn't so much one of our cloud security challenges as it is a closely related PR problem. In the event that a cloud provider security breach that puts your business' data at risk – more specifically, your customers' data at risk – then the fact that it wasn't your fault may be cold comfort. Your customers will be angry at you for exposing them to potential fraud, and regulatory bodies aren't likely to care much whose fault it was, only that the data that you were supposed to protect has been exposed. Thus, it is critical that in each step in the process, you focus on IaaS cloud data protection as much as is feasible.

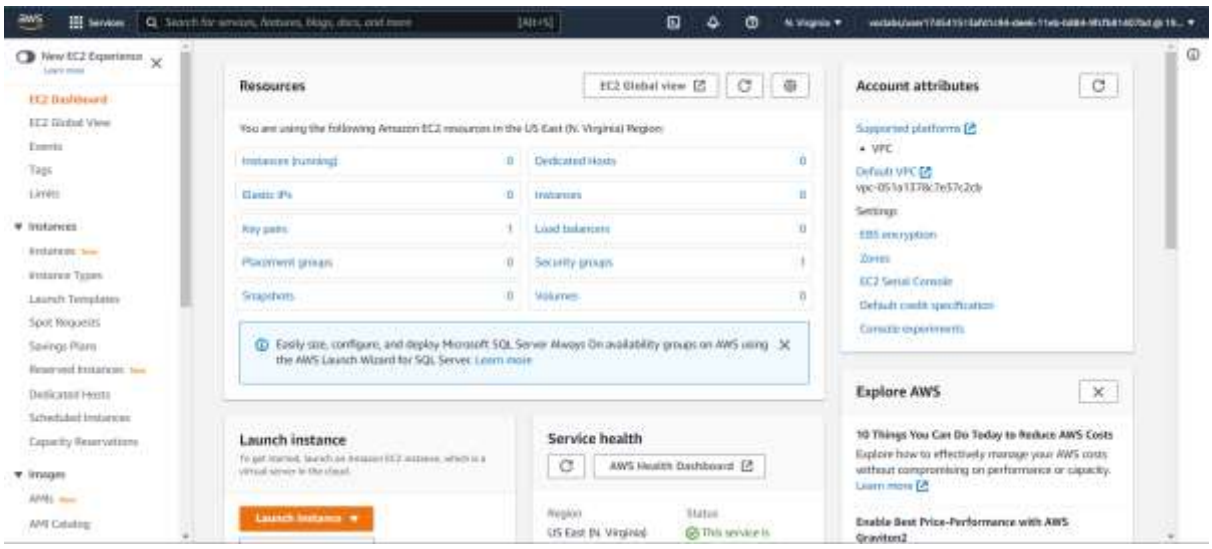
- **Activity**
    1. Use AWS, to create a VM and configure it.
    2. Access the created machine remotely

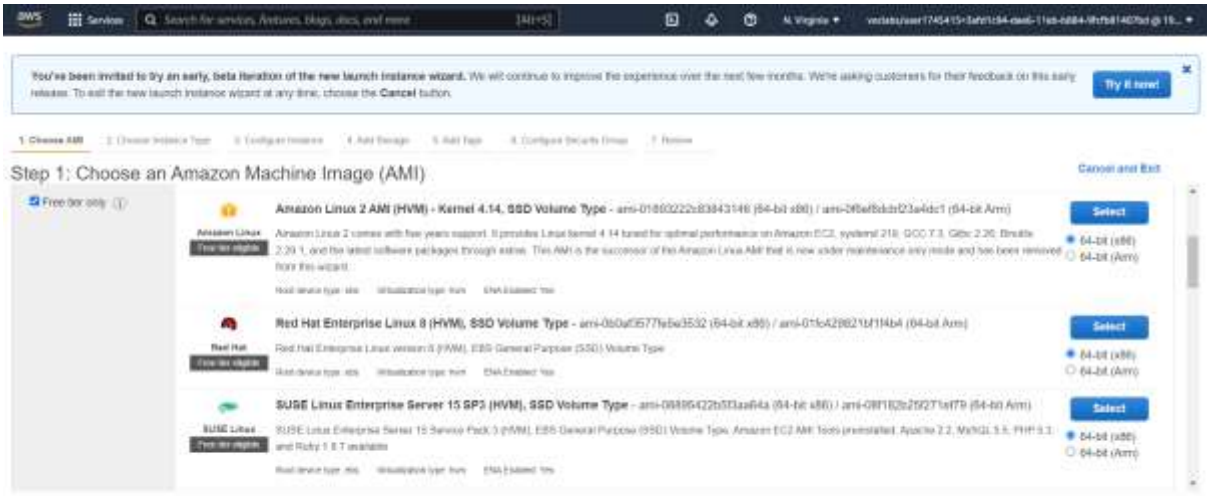
Implementation

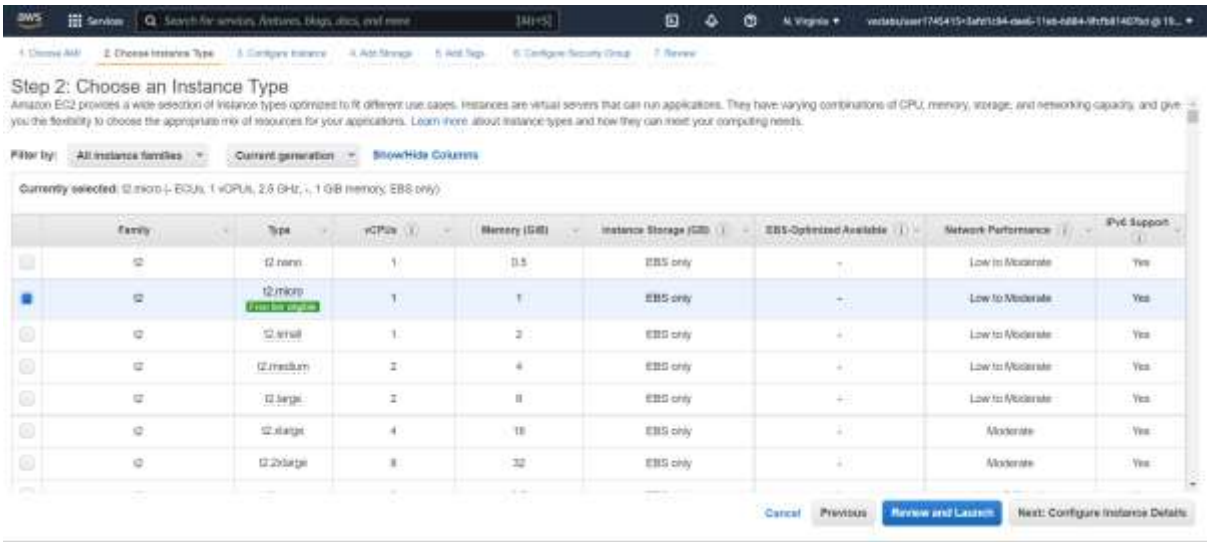
1. To demonstrate and implement IAAS service using AWS (Use t2.Micro (Free tier eligible) (instance only).

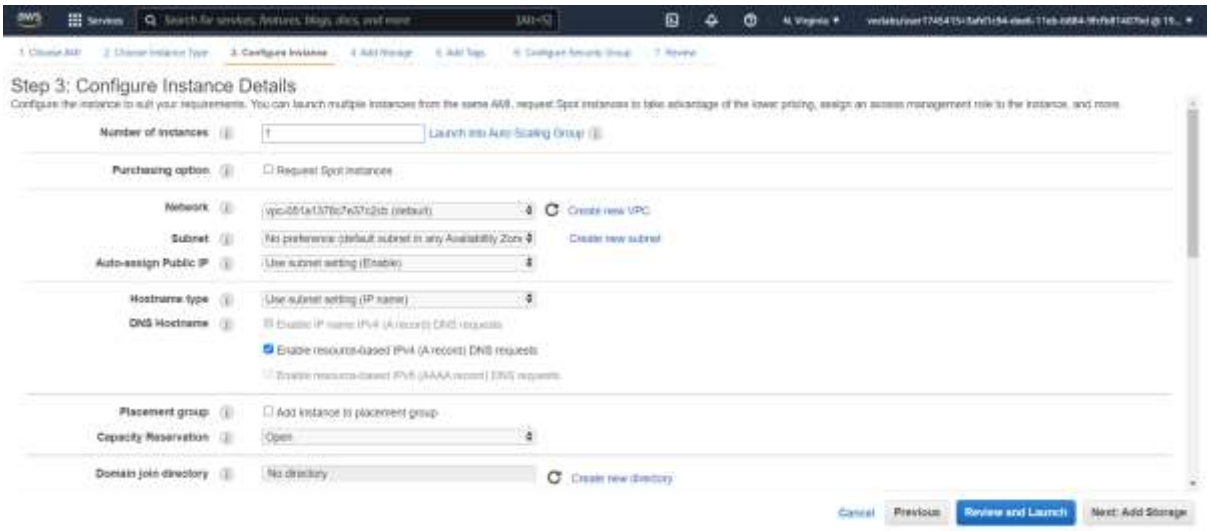


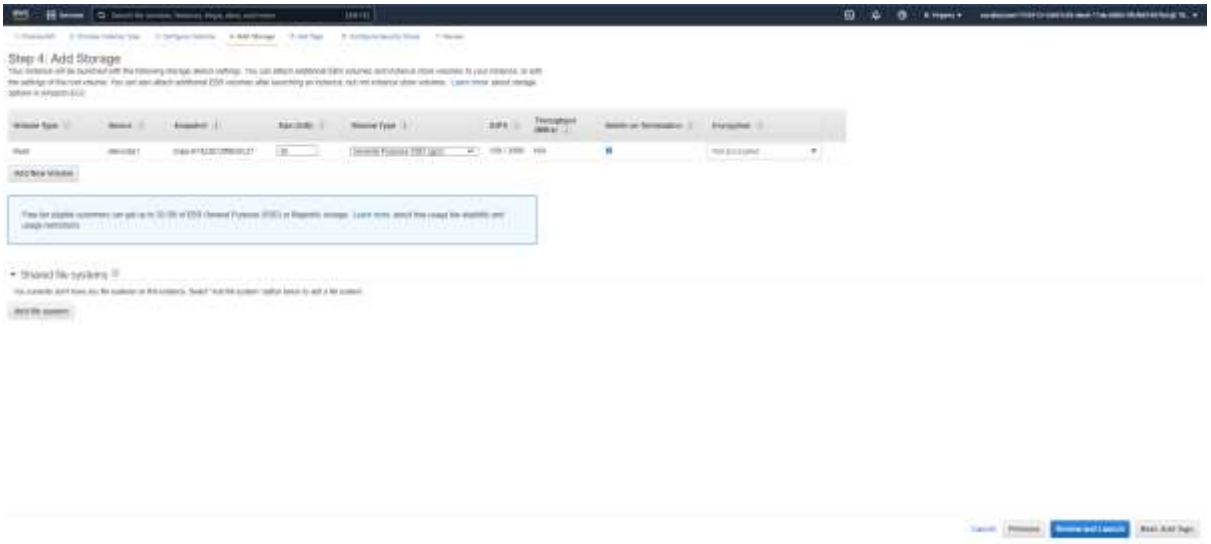
2. Choose Msft windows server base 2019

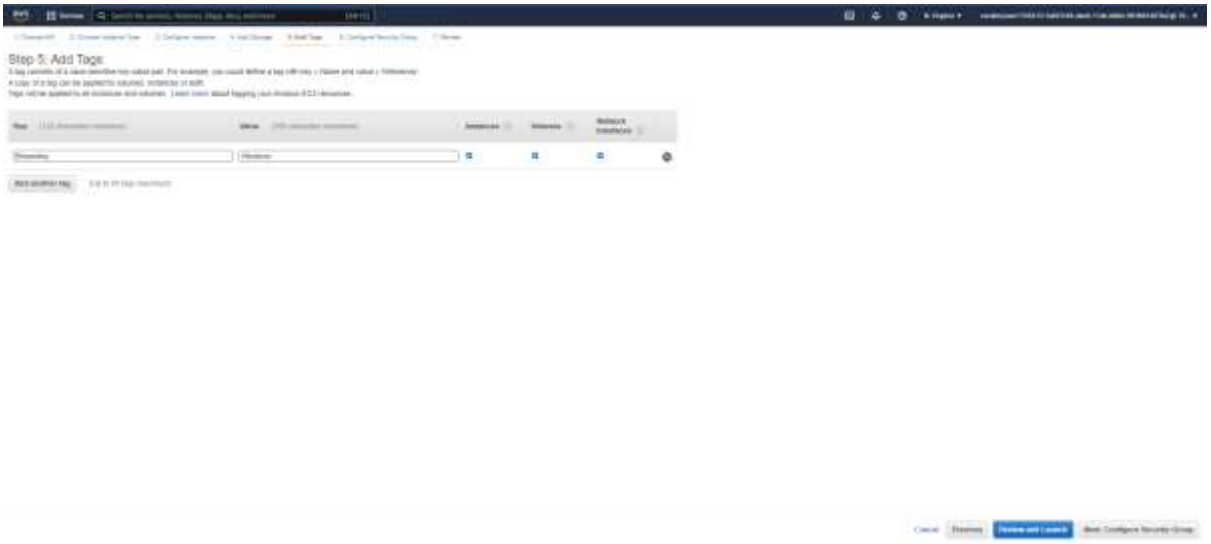


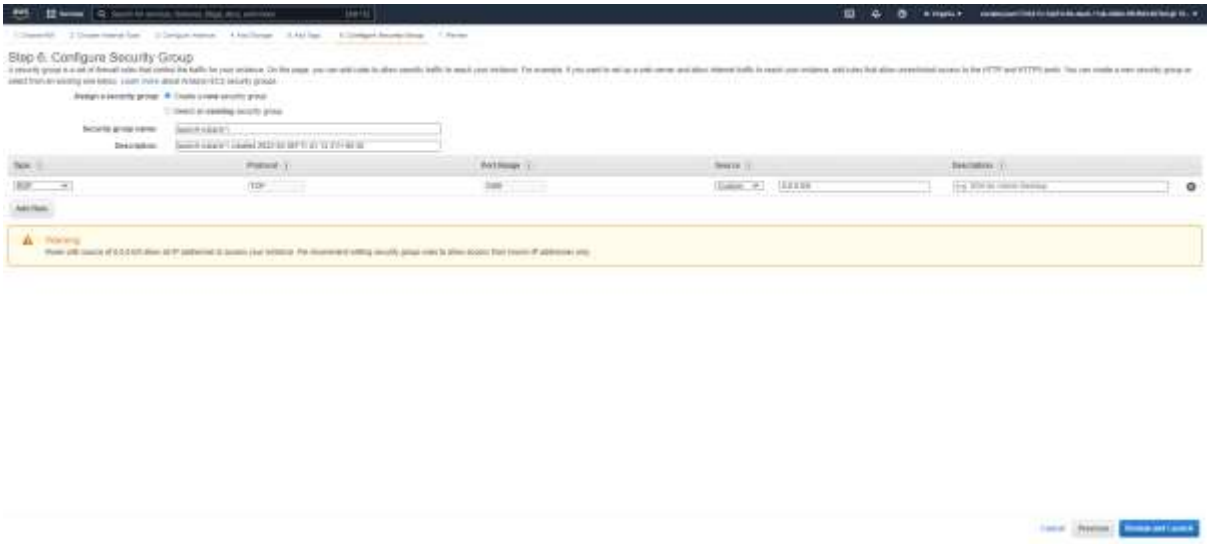

You're been invited to try an early, beta iteration of the new launch instance wizard.
Try it now!
Step 1: Choose an Amazon Machine Image (AMI)
Free tier only
Amazon Linux 2 AMI (HVM) - Kernel 4.14, SSD Volume Type
Select
Red Hat Enterprise Linux 8 (HVM), SSD Volume Type
Select
SUSE Linux Enterprise Server 15 SP3 (HVM), SSD Volume Type
Select

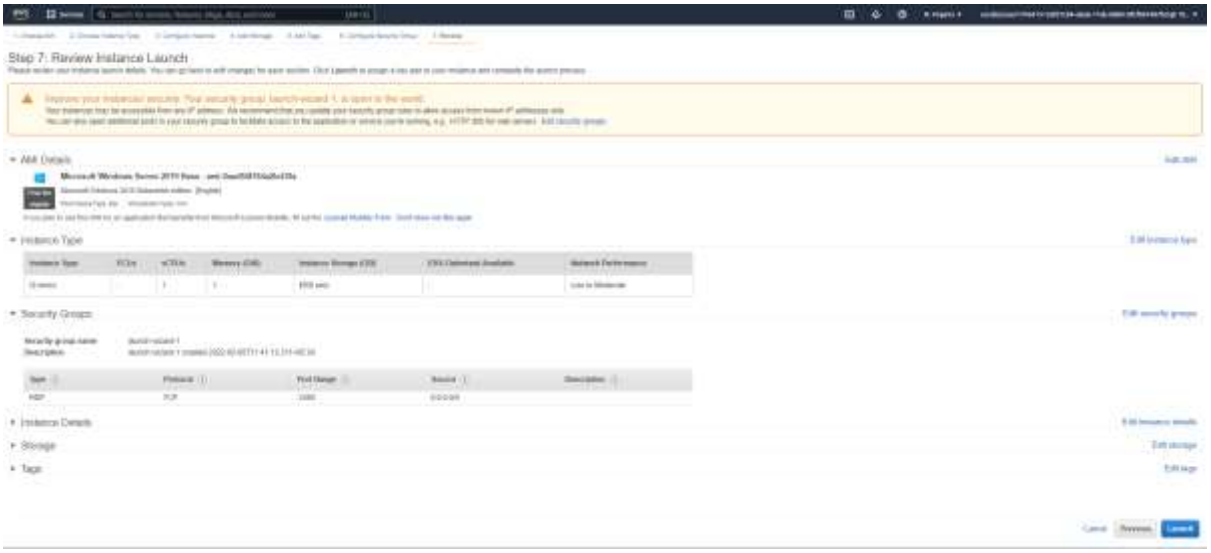

Step 2: Choose an Instance Type
Filter by:
All instance families
Current generation
Show/Hide Columns
Currently selected: t2.micro (- ECUs, 1 vCPUs, 2.5 GHz, -, 1 GiB memory, EBS only)
Cancel
Previous
Review and Launch
Next: Configure Instance Details

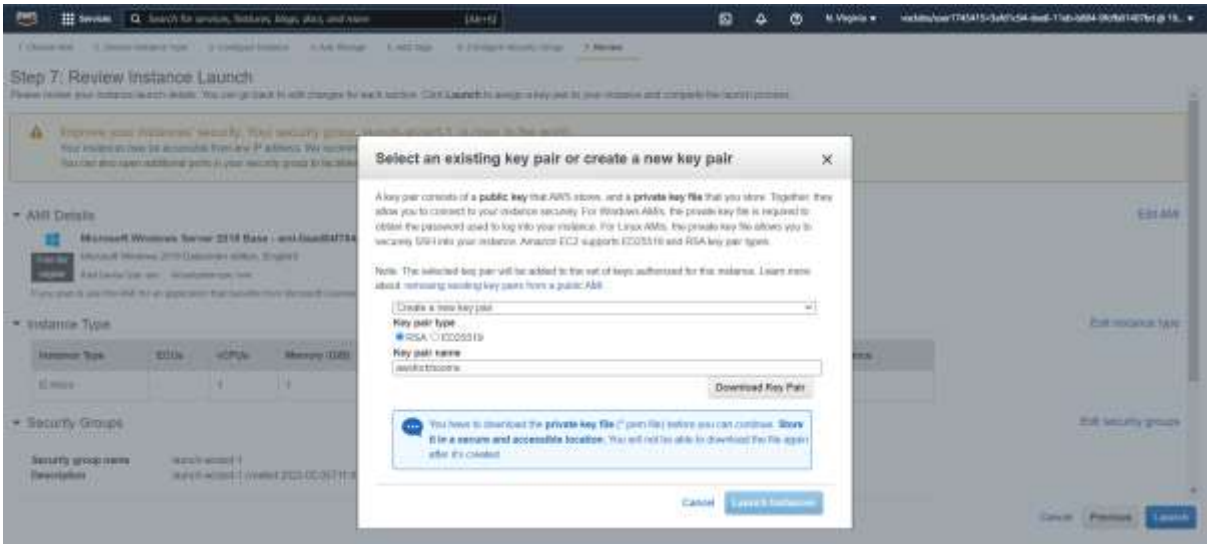

Step 3: Configure Instance Details
Number of instances
Launch into Auto Scaling Group
Purchasing option
Request Spot instances
Network
Create new VPC
Subnet
Create new subnet
Auto-assign Public IP
Hostname type
DNS Hostname
Enable resource-based IPv4 (A record) DNS requests
Placement group
Add instance to placement group
Capacity Reservation
Domain join directory
Create new directory
Cancel
Previous
Review and Launch
Next: Add Storage

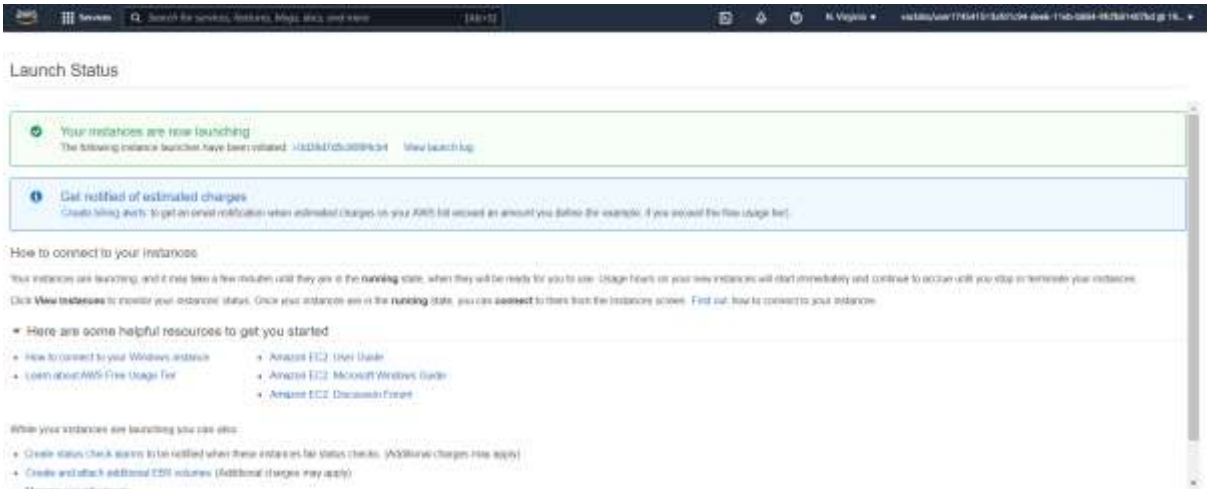

Step 4: Add Storage
Shared file systems

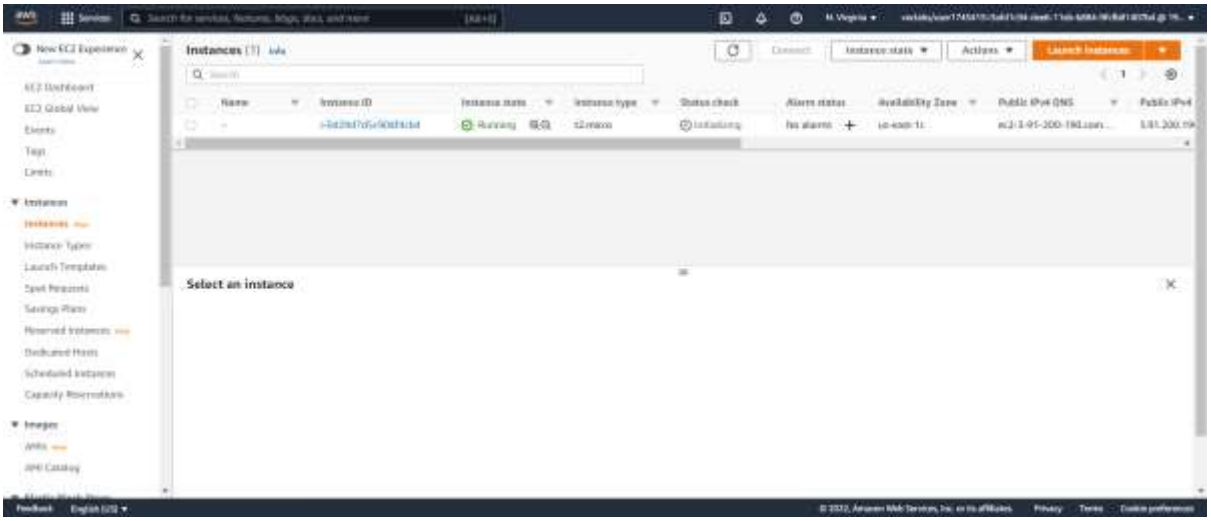

Step 5: Add Tags

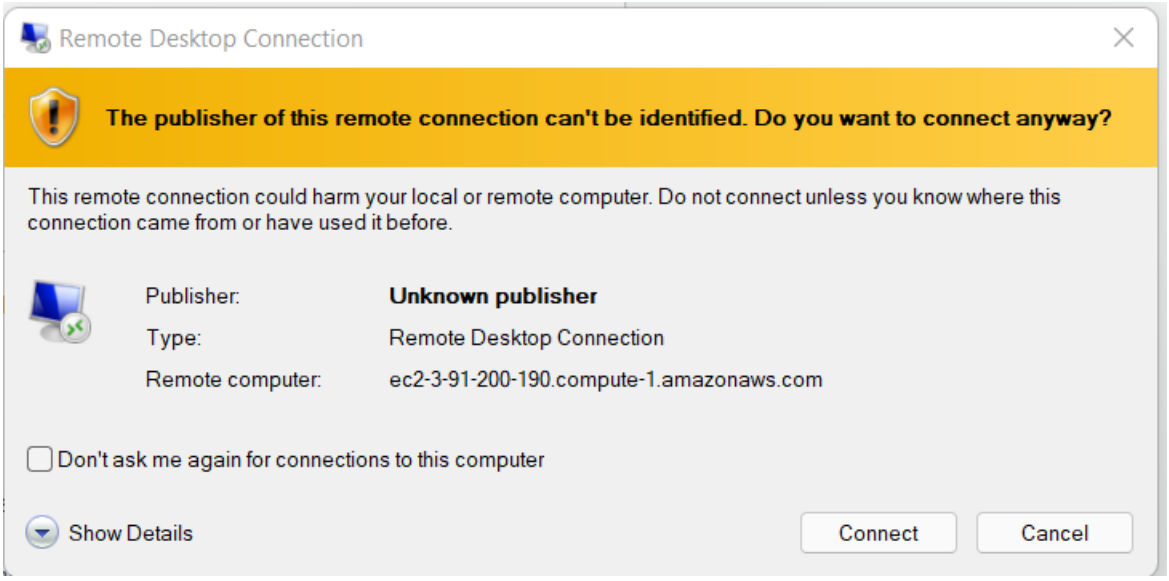

Step 6: Configure Security Group

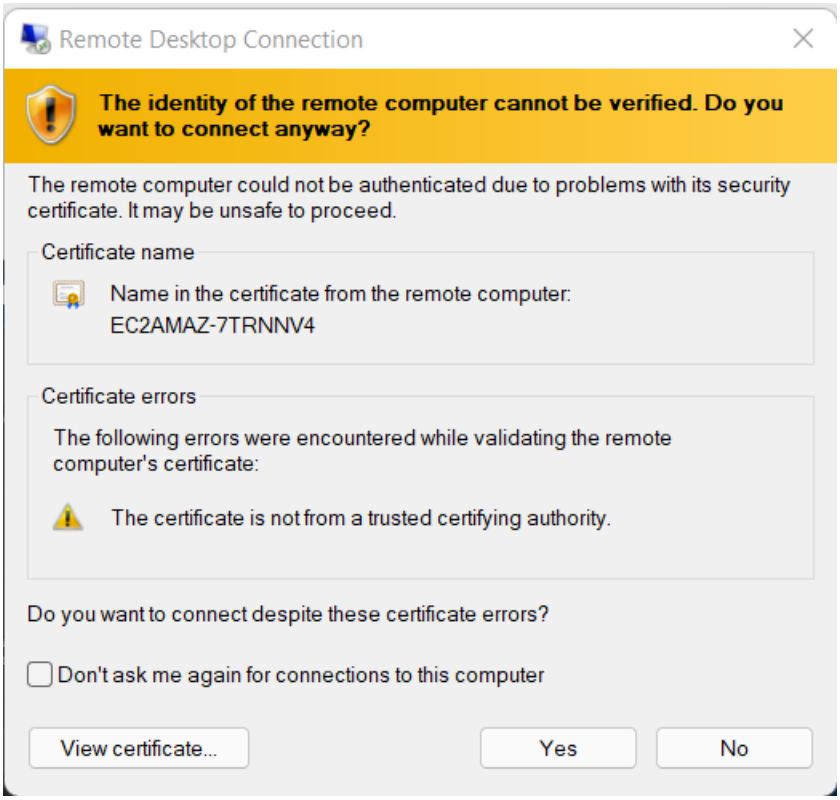

Step 7: Review Instance Launch
AMI Details
Instance Type
Security Groups
Instance Details
Storage
Tags

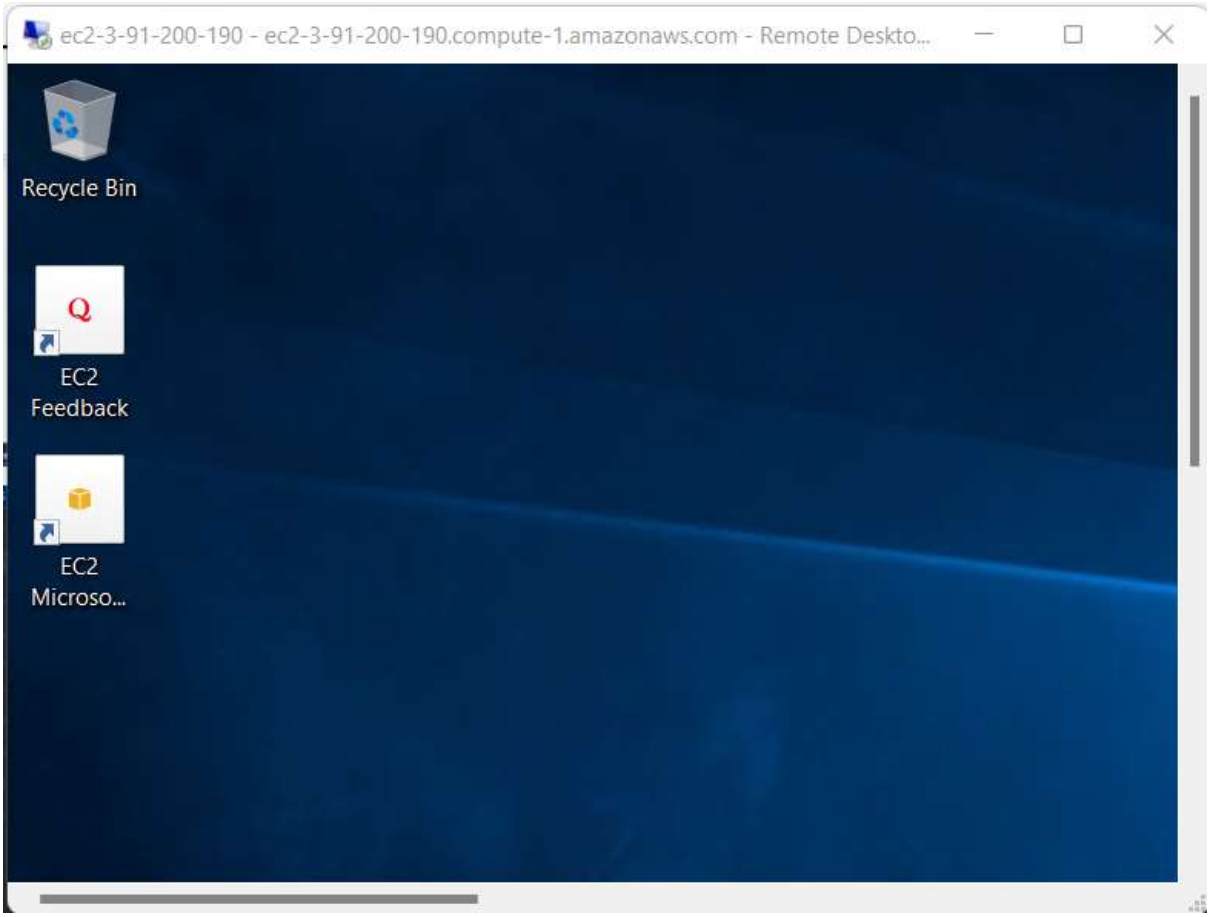

Step 7: Review Instance Launch
Select an existing key pair or create a new key pair
A key pair consists of a public key that AWS stores, and a private key file that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance. Amazon EC2 supports ED25519 and RSA key pair types.
Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.
Create a new key pair
Key pair type
RSA
ED25519
Key pair name
awsbotocore
Download Key Pair
You have to download the private key file (*.pem file) before you can continue. Store it in a secure and accessible location. You will not be able to download the file again after it's created.
Cancel
Launch Instances


Launch Status
Your instances are now launching
Get notified of estimated charges
How to connect to your instances
Here are some helpful resources to get you started
How to connect to your Windows instance
Learn about AWS Free Usage Tier
Amazon EC2 User Guide
Amazon EC2 Microsoft Windows Guide
Amazon EC2 Discussion Forum
While your instances are launching you can also
Create status check alarms to be notified when these instances fail status checks. (Additional charges may apply)
Create and attach additional EBS volumes (Additional charges may apply)


Instances (1)
Select an instance


Remote Desktop Connection
The publisher of this remote connection can't be identified. Do you want to connect anyway?
This remote connection could harm your local or remote computer. Do not connect unless you know where this connection came from or have used it before.
Publisher: Unknown publisher
Type: Remote Desktop Connection
Remote computer: ec2-3-91-200-190.compute-1.amazonaws.com
Don't ask me again for connections to this computer
Show Details
Connect
Cancel


Remote Desktop Connection
The identity of the remote computer cannot be verified. Do you want to connect anyway?
The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.
Certificate name
Name in the certificate from the remote computer:
EC2AMAZ-7TRNNV4
Certificate errors
The following errors were encountered while validating the remote computer's certificate:
The certificate is not from a trusted certifying authority.
Do you want to connect despite these certificate errors?
Don't ask me again for connections to this computer
View certificate...
Yes
No



Conclusion

What are the benefits of using IaaS

Infrastructure-as-a-Service (IaaS) is one of the biggest trends in cloud computing. Dataprise helps businesses uncover the many benefits of IaaS cloud computing, including enhanced performance, security, scalability, and support. The International Data Corporation (IDC) released its Quarterly Cloud IT Infrastructure Tracker, which forecasts that total spend on IT infrastructure will grow 12.9% reaching roughly $74.6 billion in 2021. What does this mean? Infrastructure-as-a-Service isn't going away anytime soon.

Along with Software-as-a-Service (SaaS) and Platform-as-a-Service (PaaS), Infrastructure-as-a-Service (IaaS) is one of the key elements of the cloud-computing stack. The benefits of IaaS provides businesses on-demand virtual services such as networking, storage, and hardware.

But, how can utilizing IaaS technology help to grow and advance your business and IT environment? Here are a few of the main benefits of IaaS:

Benefits of IaaS Technology

- 1. Increased Performance, Decreased CapEx
- 2. Increased Security
- 3. Increased Scalability and Flexibility
- 4. Increased Support for Disaster Recovery and Business Continuity

Advantages of Infrastructure-as-a-Service

1. Increased Performance, Decreased CapEx
2. Increased Security
3. Increased Scalability and Flexibility
4. Increased Support for Disaster Recovery and Business Continuity

References

1. https://drive.google.com/file/d/1lBM3IoFx1MHm4_bDvntqGmAJRafriGcU/view?usp=sharing
2. https://www.javatpoint.com/infrastructure-as-a-service
3. https://www.lastline.com/blog/8-iaas-cloud-security-challenges-you-should-be-aware-of/