

EXPERIMENT 1

AIM: Windows EC2

THEORY:

1) What is DevOps ?

--> DevOps is a software development approach that emphasizes collaboration and communication between development (Dev) and operations (Ops) teams. It aims to shorten the software development lifecycle and improve the quality and reliability of software releases. DevOps will remove the “siloes” conditions between the development team and operations team. In many cases these two teams will work together for the entire application lifecycle, from development and test to deployment to operations, and develop a range of skills not limited to a single function.

Teams in charge of security and quality assurance may also integrate more closely with development and operations over the course of an application’s lifecycle under various DevOps models. DevSecOps is the term used when security is a top priority for all members of a DevOps team.

2) What is AWS EC2? Why EC2?

-->EC2 Instance storage is the temporary block storage service provided by AWS. EC2 instance storage, in itself, is not a storage service, but essentially it is a part of the EC2 service. These storage devices physically lie on the same host that provides the EC2 instance and are essentially useful to store temporary data associated with the EC2 instances.

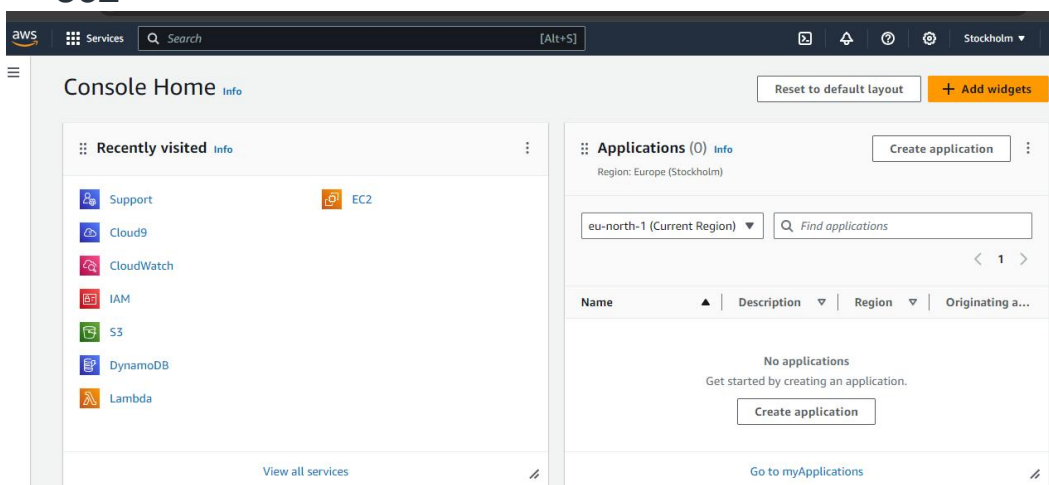
Features of EC2 instance storage:

- **Temporary storage:** EC2 instance storage provides temporary storage for EC2 instances.
- **Cost:** The cost of these storage volumes is included in the cost of the EC2 instance. Different instances may have different storage volumes capacity, but the cost is always included in the price of the EC2 instance.
- **Data Transfer Rate:** Since these storage volumes physically reside on the same host as the EC2 server, the I/O speed offered by these storage volumes is *extremely high*. I/O speeds offered by these volumes far exceed other storage options on AWS.
- **Security:** Security on instance store volumes is the same as the security on the EC2 associated with them. The roles, users, and policies which have access to an EC2 instance will have access to the associated Instance Storage Volumes.
- **Not backed up as AMI:** If the user takes an AMI snapshot of an existing EC2 instance, and launches a new instance from that AMI, the instance storage data is not replicated onto the new EC2 instance machine.

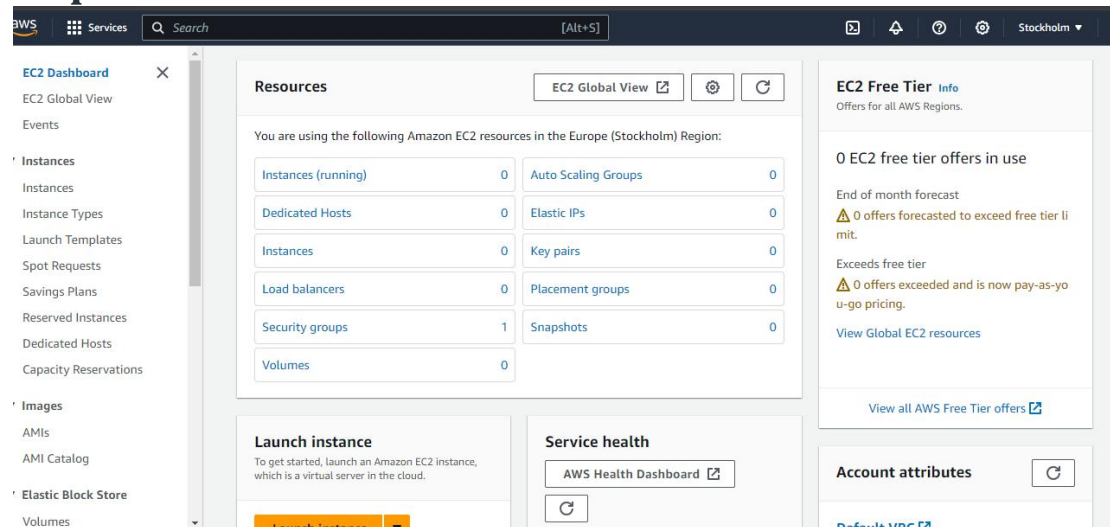
3)

-->

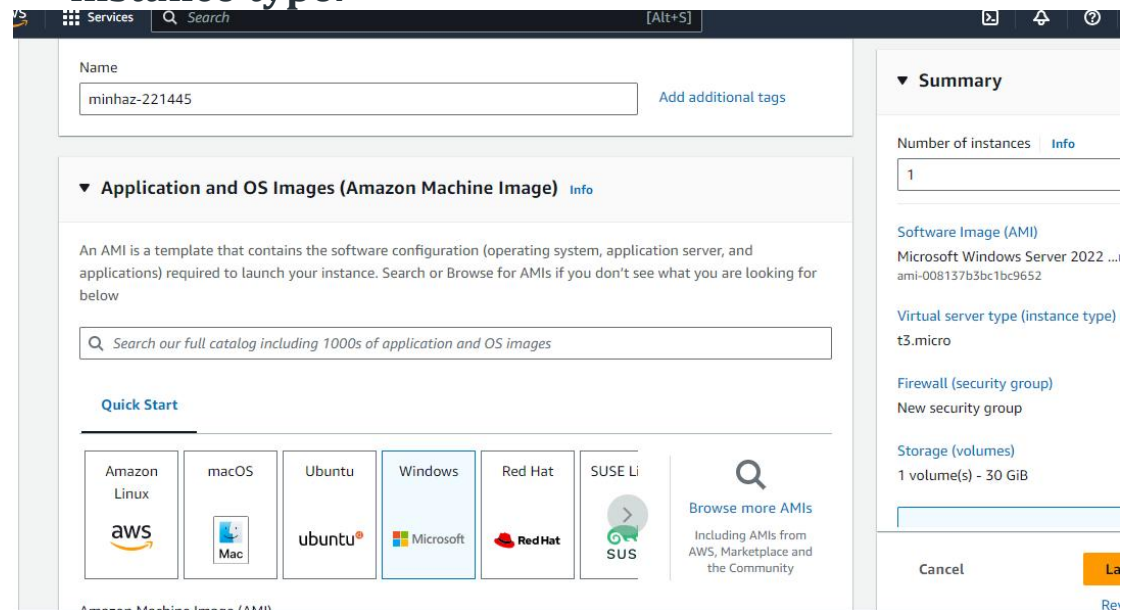
1. First we will login to our AWS account and locate ec2



2. After selecting EC2, EC2 dashboard will open and press launch instance.



3. Here we will give our server name and selecting windows as our OS and selecting free-tier eligible instance type.



4. Next we will generate a key pair.

▼ Key pair (login) Info

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

minhaz

Create new key pair

For Windows instances, you use a key pair to decrypt the administrator password. You then use the decrypted password to connect to your instance.

▼ Network settings Info Edit

Network Info

vpc-0e13cc18efe1fea4f

Subnet Info

No preference (Default subnet in any availability zone)

Auto-assign public IP Info

Enable

▼ Summary

Number of instances Info

1

Storage (optional)

1 volume(s) - 30 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Cancel Launch instance

Review command

5. In this step, we will enable allow RDP traffic , tick http and https traffic based on our requirement.

aws Services Search [Alt+S]

Firewall (security groups) Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☒ Create security group
 ☐ Select existing security group

We'll create a new security group called 'launch-wizard-1' with the following rules:

☒ Allow RDP traffic from
Helps you connect to your instance
Anywhere
0.0.0.0/0

☐ Allow HTTPS traffic from the internet
To set up an endpoint, for example when creating a web server

☒ Allow HTTP traffic from the internet
To set up an endpoint, for example when creating a web server

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

▼ Configure storage Info Advanced

1x 30 GiB gp2 Root volume (Not encrypted)

CloudShell Feedback © 2024

6. Our server is launched.

aws Services Search [Alt+S]

EC2 > Instances > Launch an instance

Success

Successfully initiated launch of instance (i-0aa1756a805b0f451)

Launch log

Stockholm

7. We will now open our RDP client to get RDP file, pressing on get password and uploading the key file which we have downloaded earlier.

aws Services Search [Alt+S]

EC2 > Instances > i-02559269e27dc5c76 > Connect to instance

Connect to instance [Info](#)

Connect to your instance i-02559269e27dc5c76 (minhaz-221445) using any of these options

Session Manager **RDP client** EC2 serial console

Instance ID
i-02559269e27dc5c76 (minhaz-221445)

Connection Type

- ☒ **Connect using RDP client**
Download a file to use with your RDP client and retrieve your password.
- ☐ **Connect using Fleet Manager**
To connect to the instance using Fleet Manager Remote Desktop, the SSM Agent must be installed and running on the instance. For more information, see [Working with SSM Agent](#)

You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:

[Download remote desktop file](#)

i-02559269e27dc5c76 (minhaz-221445)

Key pair associated with this instance
minhaz-45

Private key
Either upload your private key file or copy and paste its contents into the field below.

[Upload private key file](#)

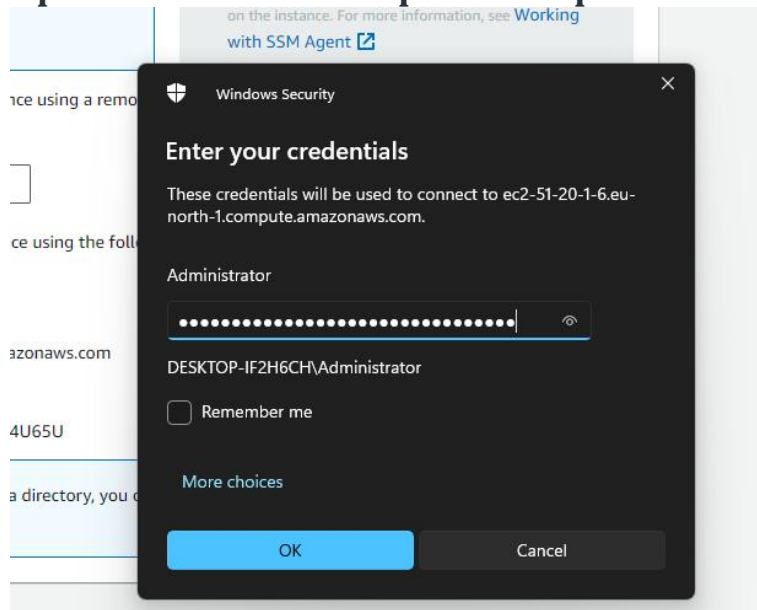
minhaz-45.pem
1.674KB

Private key contents - optional

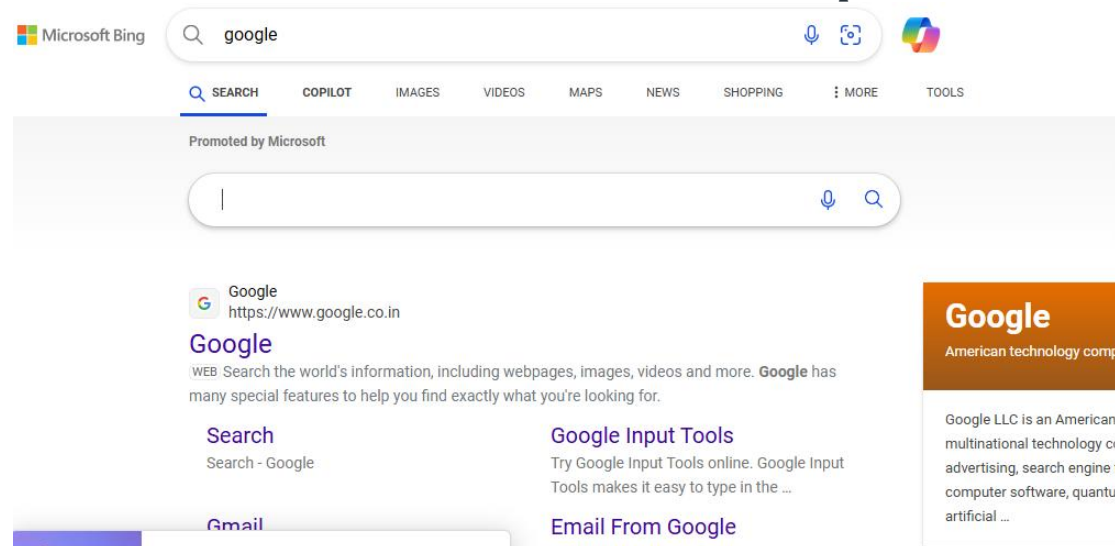
```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEA3IW4qRuQUwDupz7vySs2Uknp/rg7qJGW0zQO2peNGAay0NqM
GZb4eHAJ3iH/VwHIG5toYtbiQUVD8bKIPa4snEq3Jxo3BHiBjqCb25zm+TdjvcdG
BhTx+wC4oVXiW6XVn38sPwEboF27n+TRee6VUTqETgt+jiNUZ5vVdCwpxWizztEq
91x19A/H5+vrIY0t1MbPbBcU43258HwSNxFXSVrc8mYg9CuPfq1HIS8ZKhP3FjZW
Wk2fFSZLfBmvNSqqR/pyXGnLkZiY9JdfVAQmhePAetvNIH48ylWgSSJDjTjyGJ65
tBgbdwsvmnSH0rdoDZHa1KiO/63o87YluE3yQIDAQABAolBAD6E2rl2yw/9L6vS
uAB8c8YYlnJUoPVFcVEnbR6j4KhzhBcAfr+ygXcDrliBcvaj3uRYxtteuH5wuLaJ
-----
```

Cancel Decrypt password

8. Open the RDP file and paste the password.



9. Now we will connected to the remote desktop.



10. After the work we will terminate our instance.

