

PROJECT : AWS EC2

Name : Vaishnavi Madhav Shinde

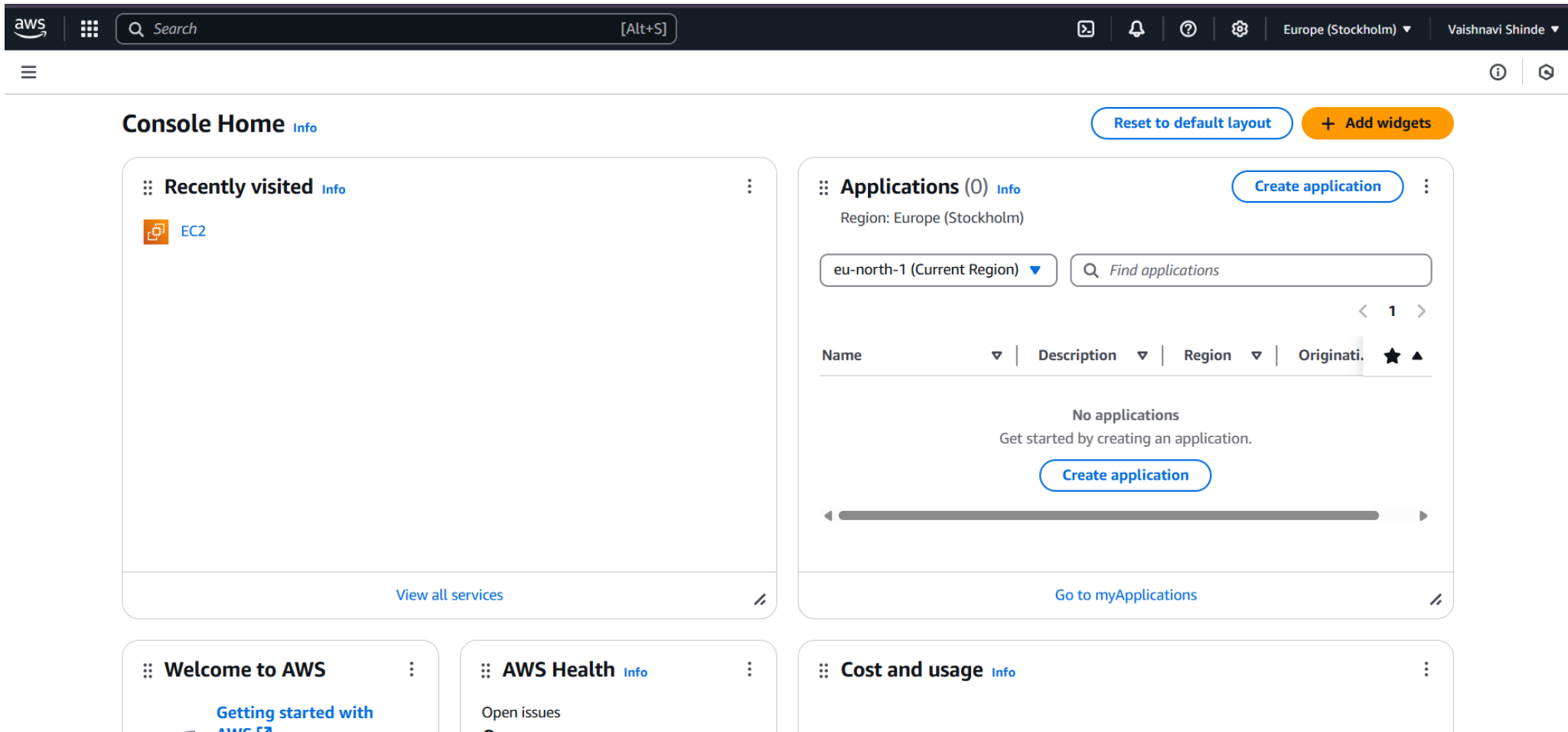
Roll No : MH-JM-24-07-0103

Course : Cyber Security Specialist

Guided By : Deepyesh Sir.

AWS EC2

Logging into the AWS Management Console and navigating to EC2.



Selecting Ubuntu 22.04 LTS as the operating system

EC2 > Instances > Launch an instance



Name and tags [Info](#)

Name

splunk

[Add additional tags](#)

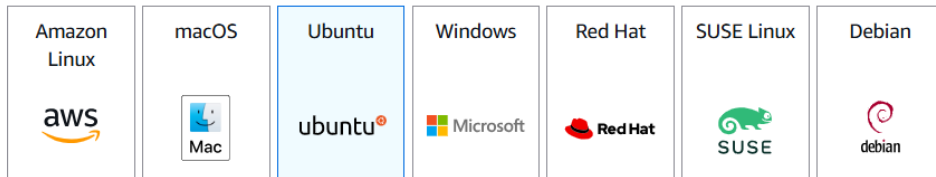
▼ Application and OS Images (Amazon Machine Image) [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Q Search our full catalog including 1000s of application and OS images

Recents

Quick Start



[Browse more AMIs](#)
Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Ubuntu Server 24.04 LTS (HVM), SSD Volume Type
ami-0c1ac8a41498c1a9c (64-bit (x86)) / ami-09fdd0b7882a4ec7b (64-bit (Arm))
Virtualization: hvm FFA enabled: true Root device type: ebs

Free tier eligible

▼ Summary

Number of instances [Info](#)

1

Software Image (AMI)

Canonical, Ubuntu, 24.04, amd64...[read more](#)
ami-0c1ac8a41498c1a9c

Virtual server type (instance type)

t3.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs. 750

[Cancel](#)

[Launch instance](#)

[Preview code](#)

Choosing an instance type (t3.micro or higher) for better performance

aws

Search

[Alt+S]

Europe (Stockholm)

Vaishnavi%20Shinde

EC2 > Instances > Launch an instance

Info

Refresh

Help

▼ Instance type [Info](#) | [Get advice](#)

Instance type

t3.micro

Free tier eligible

Family: t3 2 vCPU 1 GiB Memory Current generation: true
On-Demand Ubuntu Pro base pricing: 0.0143 USD per Hour
On-Demand RHEL base pricing: 0.0396 USD per Hour On-Demand SUSE base pricing: 0.0108 USD per Hour
On-Demand Linux base pricing: 0.0108 USD per Hour On-Demand Windows base pricing: 0.02 USD per Hour

☐ All generations

[Compare instance types](#)

Additional costs apply for AMIs with pre-installed software

▼ 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*

spl

▼

↻

Create new key pair

▼ Network settings [Info](#)

VPC - *required* | [Info](#)

vpc-0e39946fd0903a62d

172.31.0.0/16

(default) ▼

↻

Subnet | [Info](#)

No preference

▼

↻

[Create new subnet](#)

▼ Summary

Number of instances | [Info](#)

1

[Software Image \(AMI\)](#)

Canonical, Ubuntu, 24.04, amd64...[read more](#)
ami-0c1ac8a41498c1a9c

[Virtual server type \(instance type\)](#)

t3.micro

[Firewall \(security group\)](#)

New security group

[Storage \(volumes\)](#)

1 volume(s) - 8 GiB

❗ Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier

Cancel

Launch instance

[Preview code](#)

Configuring security group rules to allow access to ssh (22), splunk web (8000)

aws

Search

[Alt+S]

Europe (Stockholm)

Vaishnavi%20Shinde

EC2 > Instances > Launch an instance

launch-wizard-3

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;!\$*

Description - required [Info](#)

launch-wizard-3 created 2025-03-27T10:40:44.217Z

Inbound Security Group Rules

▼ Security group rule 1 (TCP, 22, 0.0.0.0/0) [Remove](#)

Type [Info](#)

ssh

Protocol [Info](#)

TCP

Port range [Info](#)

22

Source type [Info](#)

Anywhere

Source [Info](#)

Add CIDR, prefix list or security group

0.0.0.0/0

Description - optional [Info](#)

e.g. SSH for admin desktop

▼ Security group rule 2 (TCP, 8000, splunk web console) [Remove](#)

Type [Info](#)

Custom TCP

Protocol [Info](#)

TCP

Port range [Info](#)

8000

Source type [Info](#)

Custom

Source [Info](#)

Add CIDR, prefix list or security group

Description - optional [Info](#)

splunk web console

▼ Summary

Number of instances [Info](#)

1

Software Image (AMI)

Canonical, Ubuntu, 24.04, amd64...[read more](#)

ami-0c1ac8a41498c1a9c

Virtual server type (instance type)

t3.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier.

Cancel

Launch instance

[Preview code](#)

Splunk management (8089), and forwarder (9997)

aws

Search [Alt+S]

Europe (Stockholm)

Vaishnavi%20Shinde

EC2 > Instances > Launch an instance

▼ Security group rule 3 (TCP, 8089, splunk mgmt)

Type

Info

Custom TCP

Protocol

Info

TCP

Port range

Info

8089

Remove

Source type

Info

Custom

Source

Info

Q

Add CIDR, prefix list or security group

Description - optional

Info

splunk mgmt

▼ Security group rule 4 (TCP, 9997, forwarder)

Type

Info

Custom TCP

Protocol

Info

TCP

Port range

Info

9997

Remove

Source type

Info

Custom

Source

Info

Q

Add CIDR, prefix list or security group

Description - optional

Info

forwarder

⚠ 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.

×

Add security group rule

▼ Summary

Number of instances

Info

1

Software Image (AMI)

Canonical, Ubuntu, 24.04, amd6...[read more](#)

ami-0c1ac8a41498c1a9c

Virtual server type (instance type)

t3.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

ℹ Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier.

×

Cancel

Launch instance

🔗



Preview code





▼ Configure storage




Info

Advanced

Launching the instance and connecting via ssh

  [Alt+S]

    Europe (Stockholm) ▾ Vaishnavi%20Shinde ▾

 [EC2](#) > [Instances](#) > [i-098c5236686c0c042](#) > Connect to instance  

Connect to instance [Info](#)

Connect to your instance i-098c5236686c0c042 (splunk) using any of these options


EC2 Instance Connect



Session Manager

SSH client


EC2 serial console


Instance ID

 [i-098c5236686c0c042](#) (splunk)

1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is spl.pem
3. Run this command, if necessary, to ensure your key is not publicly viewable.
 `chmod 400 "spl.pem"`
4. Connect to your instance using its Public DNS:
 `ec2-13-60-66-81.eu-north-1.compute.amazonaws.com`

Example:

 `ssh -i "spl.pem" ubuntu@ec2-13-60-66-81.eu-north-1.compute.amazonaws.com`

 **Note:** In most cases, the guessed username is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.

[Cancel](#)

After downloading .pem file we have to open in kali linux and where there is .pem file is present we have to this following command on kali

> ssh -i your-key.pem ubuntu@your-aws-instance-ip

```
(root@kali)-[/home/kali/Downloads]
# ssh -i "spl.pem" ubuntu@ec2-13-60-66-81.eu-north-1.compute.amazonaws.com
The authenticity of host 'ec2-13-60-66-81.eu-north-1.compute.amazonaws.com (13.60.66.81)' can't be established.
ED25519 key fingerprint is SHA256:jcuVEtaBCDN4jkzdtuIaqFjfXvl8HZkXQtuAkLic9nU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-13-60-66-81.eu-north-1.compute.amazonaws.com' (ED25519) to the list of known hosts.
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.8.0-1024-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Thu Mar 27 12:51:32 UTC 2025

System load:  0.0           Temperature:   -273.1 C
Usage of /:   25.1% of 6.71GB Processes:    109
Memory usage: 23%          Users logged in: 0
Swap usage:   0%           IPv4 address for ens5: 172.31.32.38

Expanded Security Maintenance for Applications is not enabled.
```


Download splunk on ubuntu for log collection and security analysis

>wget -O splunk-9.1.2-b6b9c818539-linux-2.6-amd64.deb

<https://download.splunk.com/products/splunk/releases/9.1.2/linux/splunk-9.1.2-b6b9c8185839-linux-2.6-amd64.deb>

>sudo dpkg -i splunk-9.1.2-b6b9c818539-linux-2.6-amd64.deb

```
root@ip-172-31-32-38:/home/ubuntu# wget -O splunk-9.1.2-b6b9c8185839-linux-2.6-amd64.deb "https://download.splunk.com/products/splunk/releases/9.1.2/linux/splunk-9.1.2-b6b9c8185839-linux-2.6-amd64.deb"
--2025-03-27 13:16:50-- https://download.splunk.com/products/splunk/releases/9.1.2/linux/splunk-9.1.2-b6b9c8185839-linux-2.6-amd64.deb
Resolving download.splunk.com (download.splunk.com)... 3.164.230.7, 3.164.230.29, 3.164.230.43, ...
Connecting to download.splunk.com (download.splunk.com)|3.164.230.7|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 462049960 (441M) [binary/octet-stream]
Saving to: 'splunk-9.1.2-b6b9c8185839-linux-2.6-amd64.deb'

splunk-9.1.2-b6b9c8185839-linux-2.6-amd6 100%[=====>] 440.64M 178MB/s in 2.5s

2025-03-27 13:16:53 (178 MB/s) - 'splunk-9.1.2-b6b9c8185839-linux-2.6-amd64.deb' saved [462049960/462049960]

root@ip-172-31-32-38:/home/ubuntu# sudo dpkg -i splunk-9.1.2-b6b9c8185839-linux-2.6-amd64.deb
Selecting previously unselected package splunk.
(Reading database ... 70560 files and directories currently installed.)
Preparing to unpack splunk-9.1.2-b6b9c8185839-linux-2.6-amd64.deb ...
Unpacking splunk (9.1.2) ...
Setting up splunk (9.1.2) ...
complete
root@ip-172-31-32-38:/home/ubuntu# sudo /opt/splunk/bin/splunk enable boot-start
SPLUNK GENERAL TERMS

Last Updated: August 12, 2021

These Splunk General Terms ("General Terms") between Splunk Inc., a Delaware corporation, with its principal place of business at 270 Brannan Street, San
```

> /opt/splunk/bin/splunk start

```
root@ip-172-31-32-38:/home/ubuntu# /opt/splunk/bin/splunk start
```

```
Splunk> All batbelt. No tights.
```

```
Checking prerequisites...
```

```
Checking http port [8000]: open
```

```
Checking mgmt port [8089]: open
```

```
Checking appserver port [127.0.0.1:8065]: open
```

```
Checking kvstore port [8191]: open
```

```
Done
```

```
All preliminary checks passed.
```

```
Starting splunk server daemon (splunkd)...
```

```
Generating a RSA private key
```

```
.....+++++
```

```
.....+++++
```

```
writing new private key to 'privKeySecure.pem'
```

```
Signature ok
```

```
subject=/CN=ip-172-31-32-38/0=SplunkUser
```

```
Getting CA Private Key
```

```
writing RSA key
```

```
PYTHONHTTPSVERIFY is set to 0 in splunk-launch.conf disabling certificate validation for the http lib and urllib libraries shipped with the embedded Python interpreter; must be set to "1" for increased security
```

```
Done
```

```
Waiting for web server at http://127.0.0.1:8000 to be available..... Done
```

```
If you get stuck, we're here to help.
```

```
Look for answers here: http://docs.splunk.com
```

```
The Splunk web interface is at http://ip-172-31-32-38:8000
```

Once the setup is complete we see the splunk is running on <http://127.0.0.1:8000>

In the Instance summary we will get the **Auto-assigned IP address[public ip]**

Now we can login through that **public_ip** with port number [8000]

