Module 2: Security Management in AWS

Demo Document 6

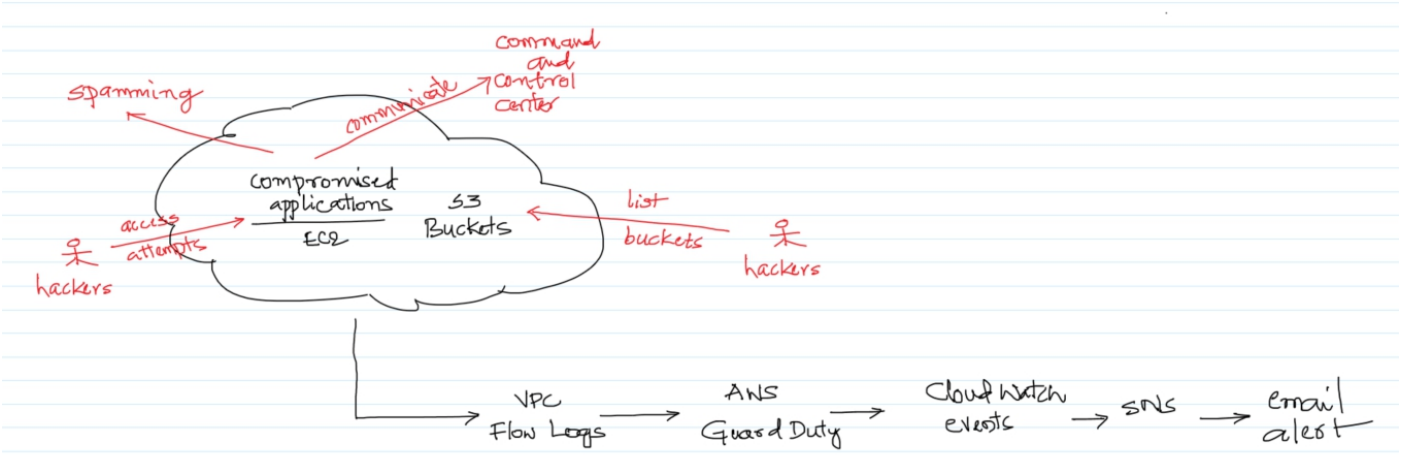
Title: Monitoring Malicious Activity or Unauthorized Behaviour via GuardDuty

Use Case

When we deploy any resources in AWS — whether it's public-facing or private —the hackers always attempt to break into the resources and steal the confidential data to exploit them to their advantages. These resource can be an EC2 instance, an S3 Bucket, an RDS instance, or anything else. While the hackers always look for loopholes to break into the systems, the onus is on the company to protect themselves before hackers can exploit the vulnerabilities to compromise your systems.

To address this challenge, AWS provides Amazon GuardDuty: A managed service that continuously monitors your resources for any malicious activity or unauthorized behavior, thus helping you protect your AWS accounts and workloads. Once Amazon GuardDuty is enabled, it automatically monitors for

- Anomalous API activity
- Potentially unauthorized deployments and compromised instances
- Reconnaissance by attackers



In this use case, we will perform the below activities and check if GuardDuty is able to identify them and alert us. These are the scenarios of a hacker attempting to break into a system or a compromised system.

- Create a Windows EC2 instance and make a connection to a TorGuard or an Authority node.

- Hacker performing some reconnaissance from Kali Linux on the S3 buckets.

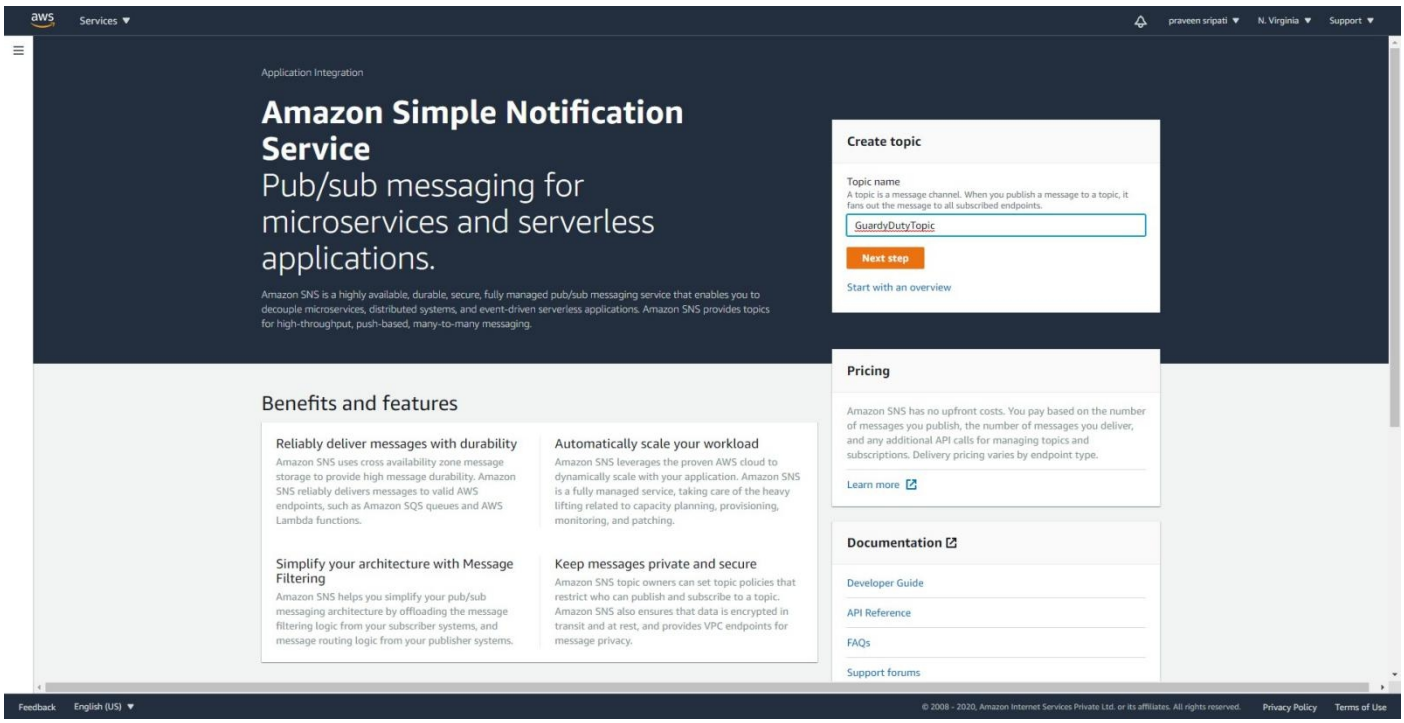
- Invoking AWS API using root credentials.

All of the above involve network traffic, which can be captured by the VPC Flows and which GuardDuty automatically analyzes and checks for any anomaly. In the event of an anomaly detected, it sends an event to CloudWatch, which in turn triggers an email via SNS service.

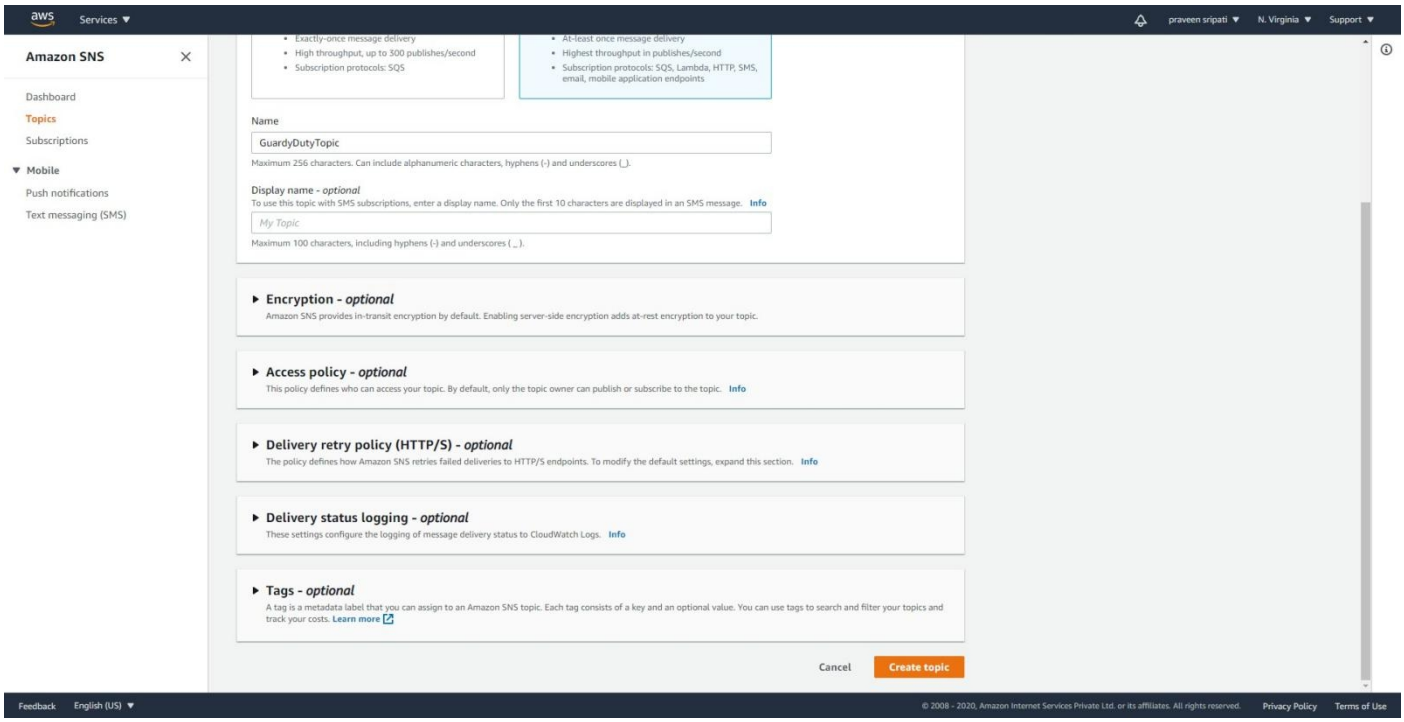
Note that in this use case, we will create an EC2 instance and an S3 bucket to perform some of the steps typically performed by hackers. We will also check if GuardDuty is able to identify them and notify us.

AWS Services: GuardDuty, EC2, S3, VPC, CloudWatch, SNS, SES

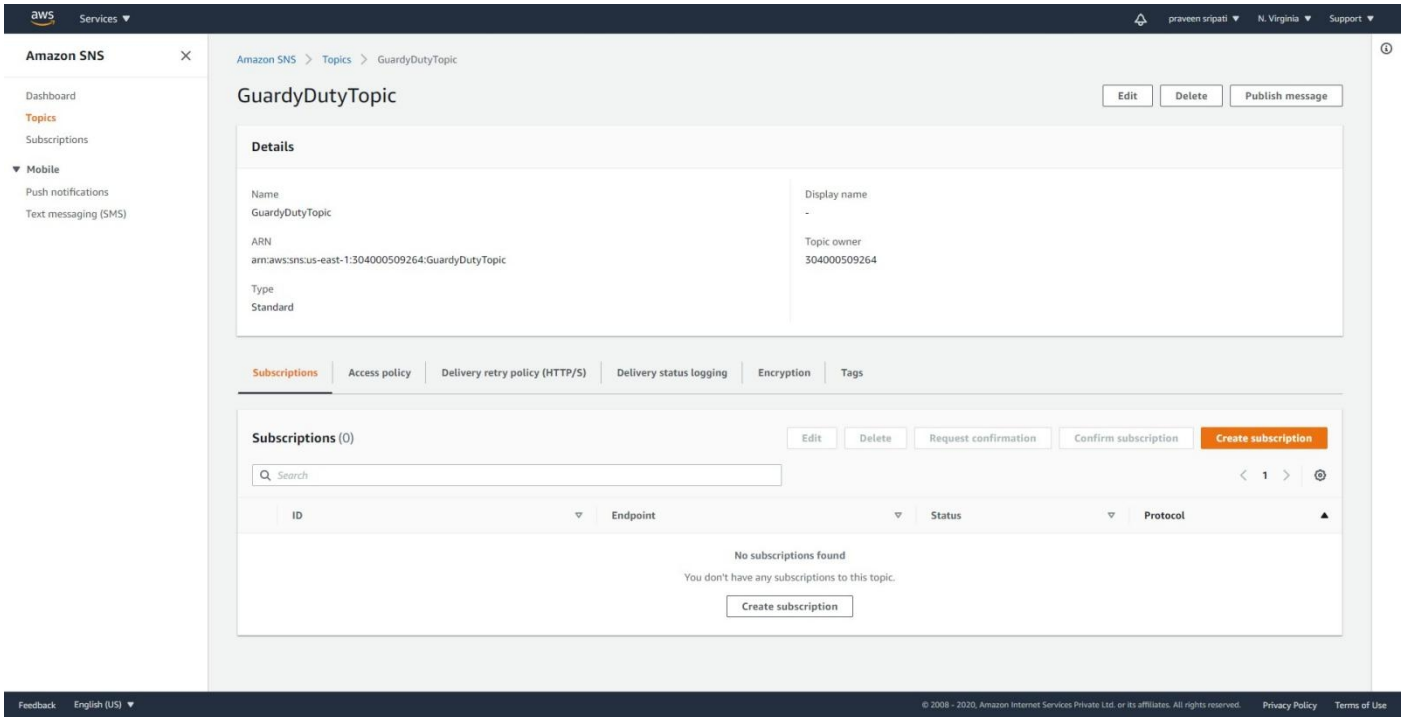
Step 1: Navigate to the SNS Management Console and enter the **Topic name** and click on **Next step**.



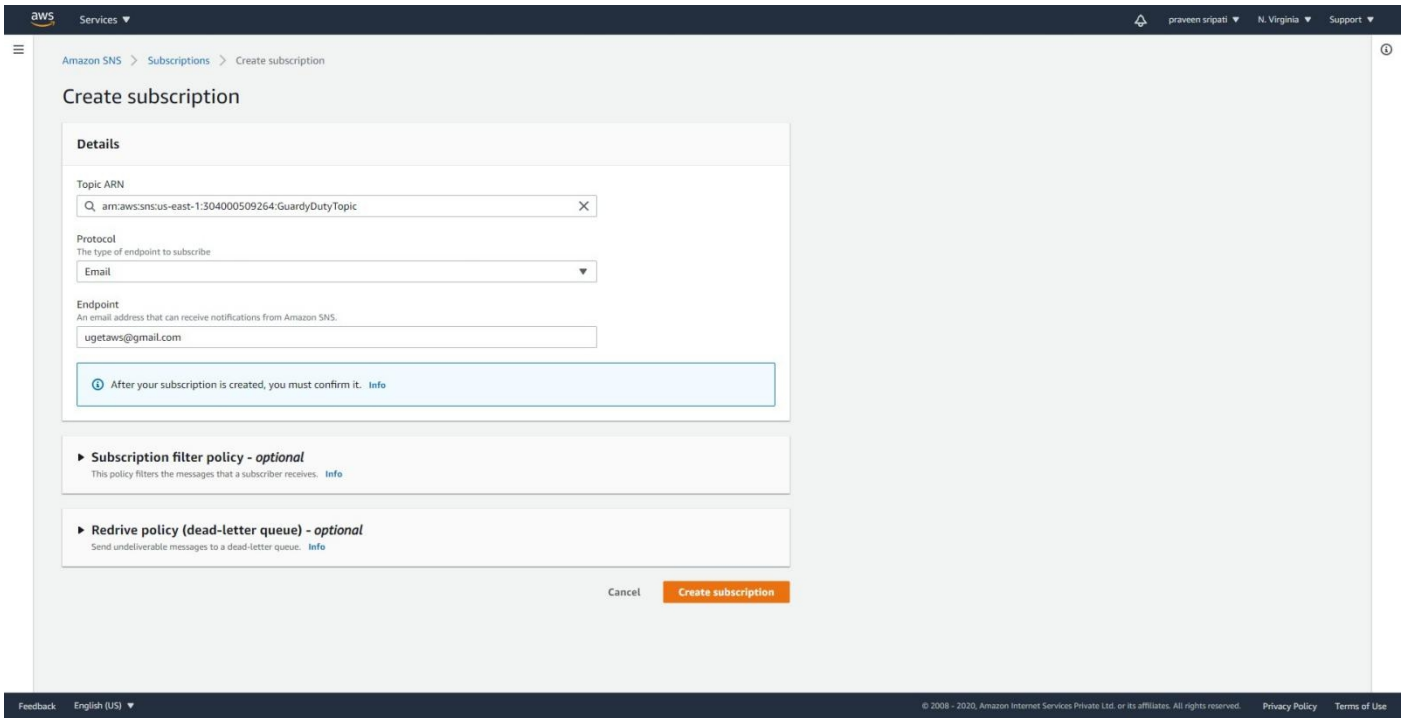
Step 2: Go with all the default options and click on **Create topic**.



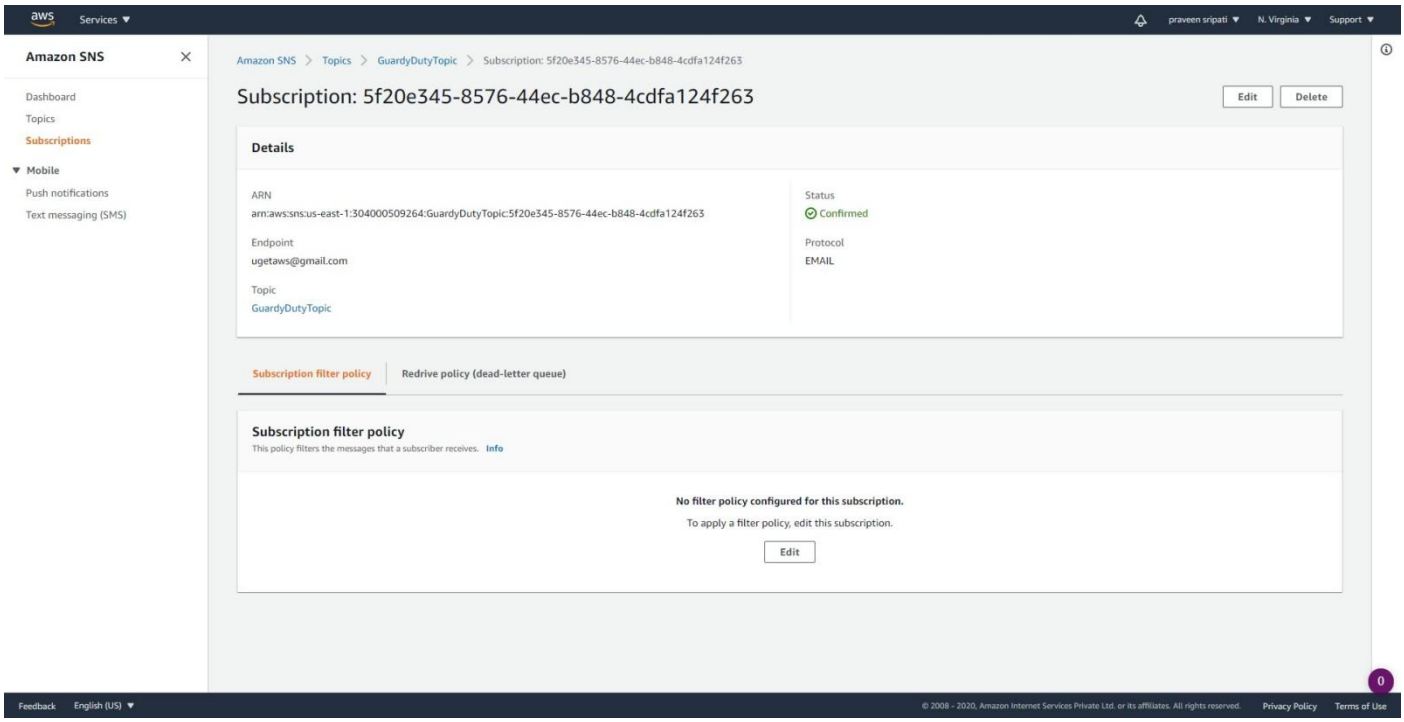
Step 3: Click on **Create subscription**.



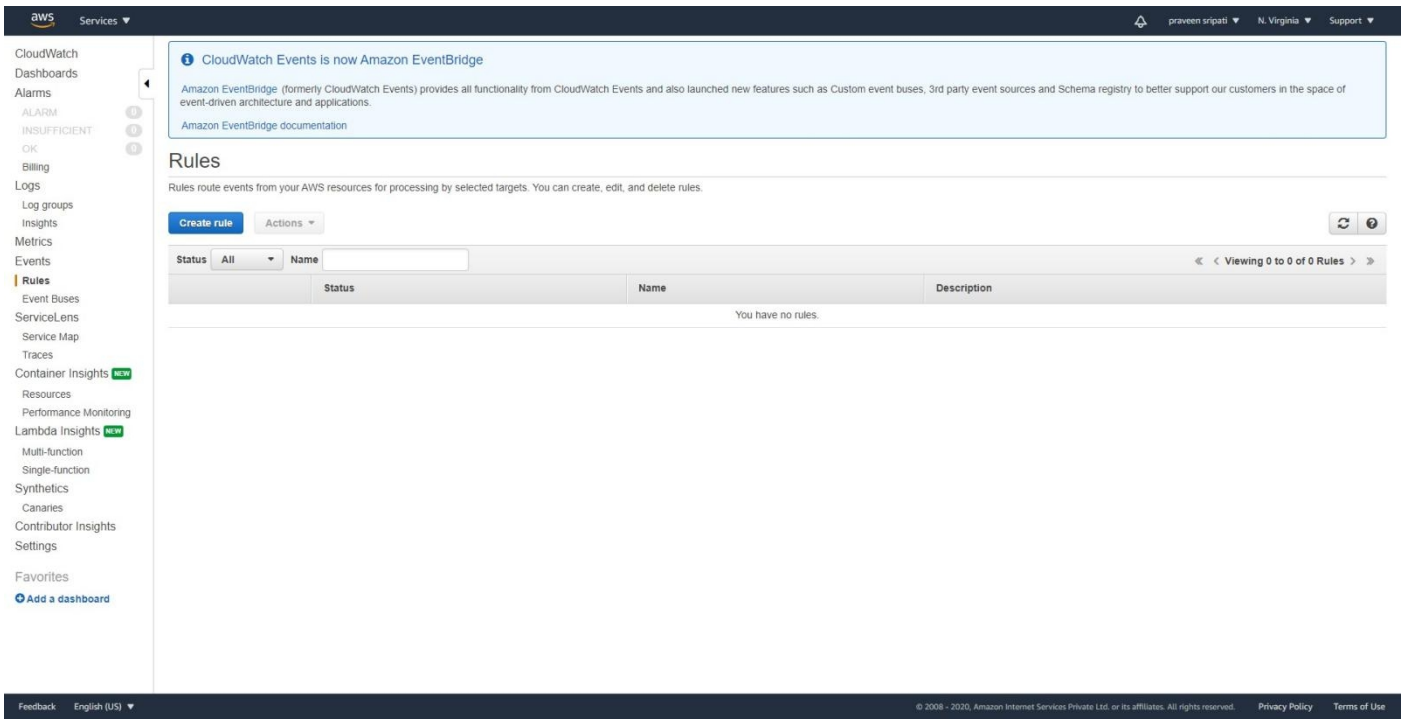
Step 4: Select Email for the Protocol and the email address for the Endpoint. Click on **Create subscription**.



Step 5: When SNS sends an email, open it and click on the link to change the status of the subscription: From **pending** to **confirmed** status. Once in a while, the email is marked as spam. So, ensure to check the spam folder every now and then.

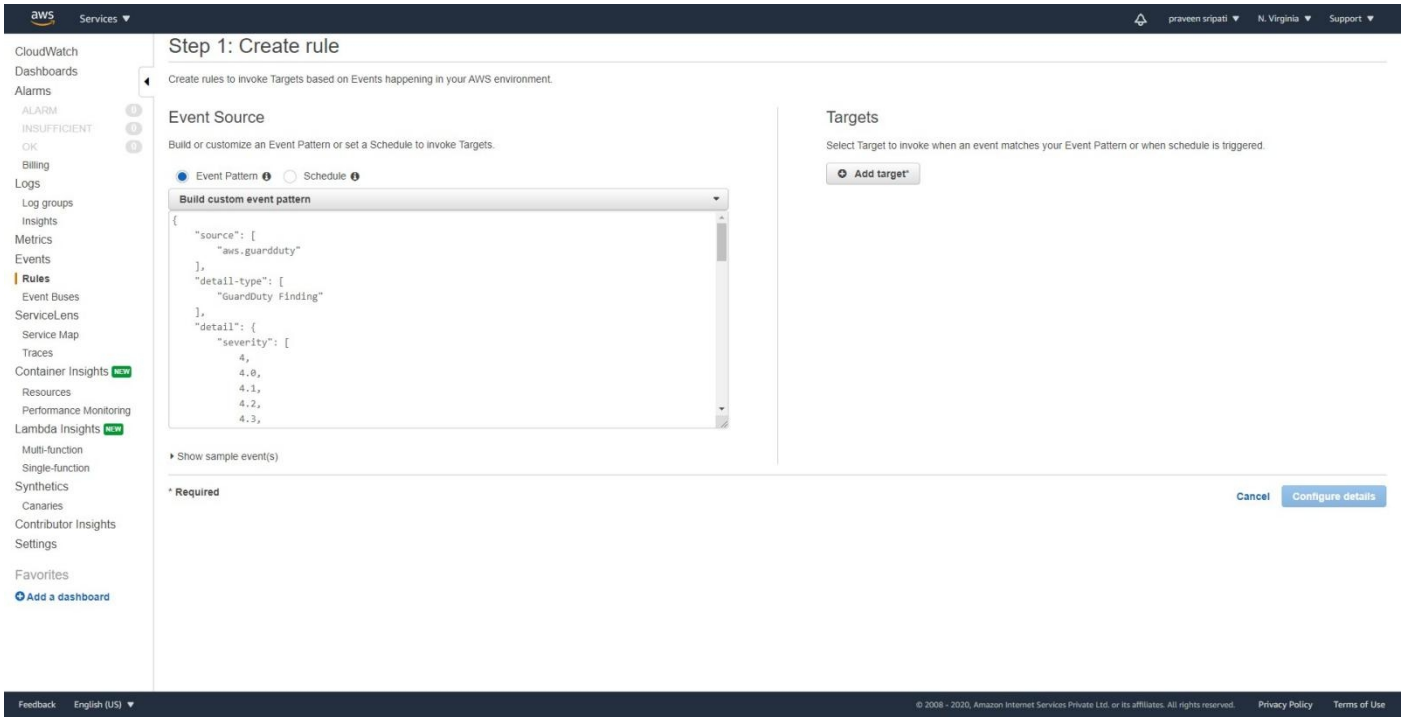


Step 6: Go to the CloudWatch Management Console and then to the **Rules** tab. Click on **Create rule**.



Step 7: Enter the attached event-pattern.json in the **Event Source**. Click on **Add target**.

event-pattern.json

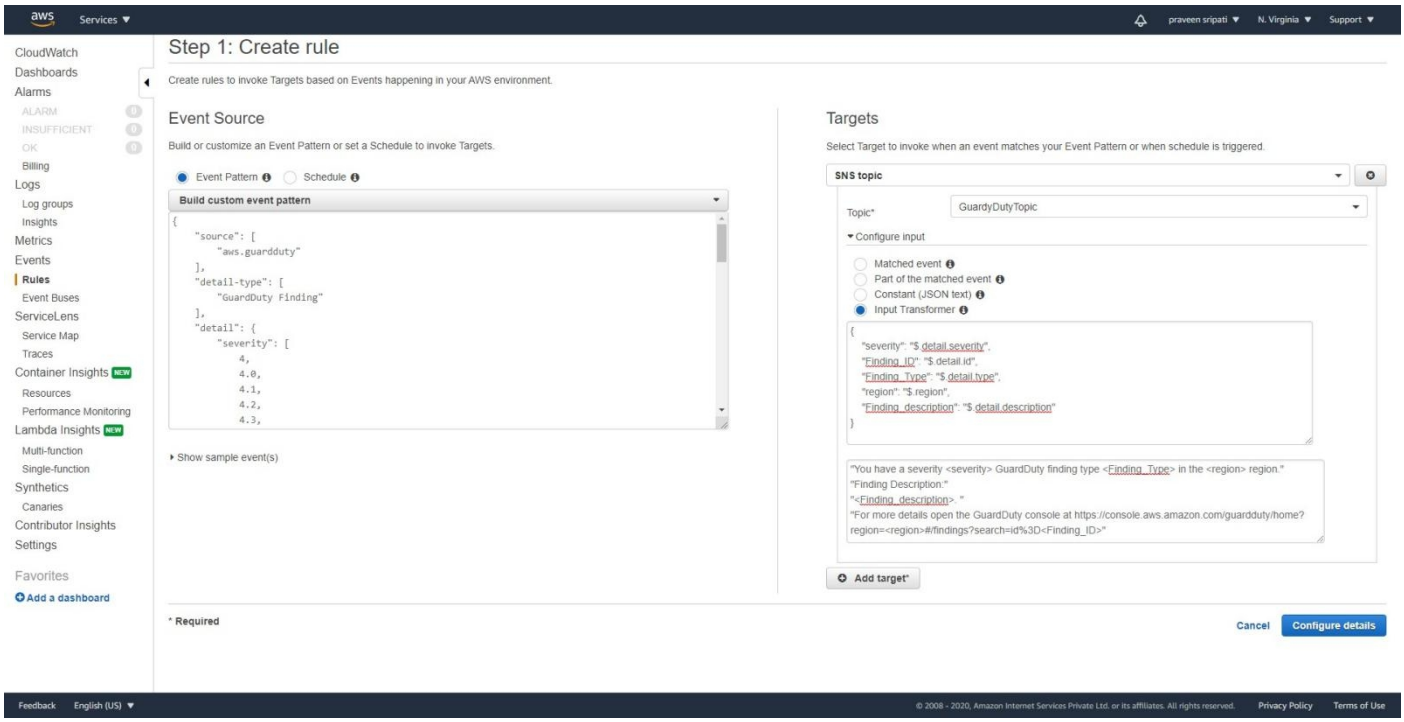


Step 8: Select the **SNS Topic** and the Topic created in the previous steps. Select **Input Transformer** and enter the below JSON.

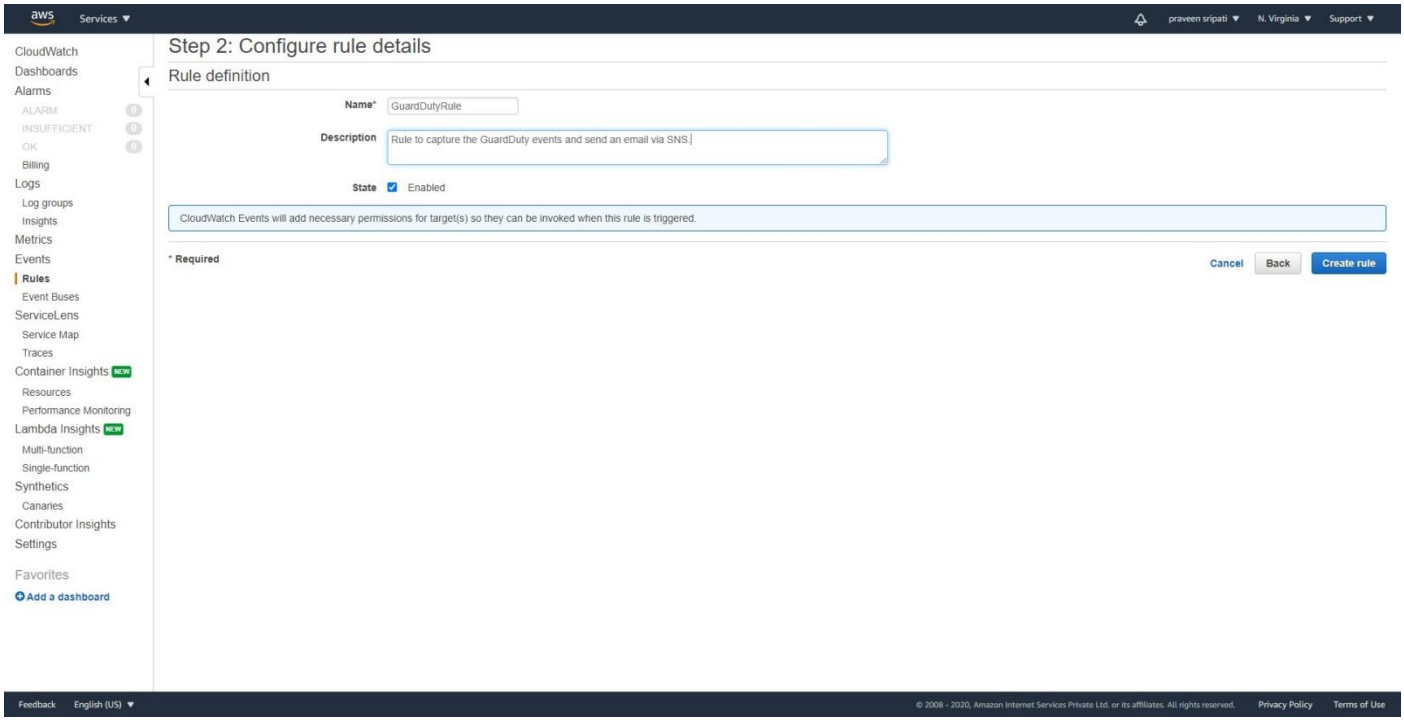
```
{
   "severity": "$.detail.severity",
   "Finding_ID": "$.detail.id",
   "Finding_Type": "$.detail.type",
   "region": "$.region",
   "Finding_description": "$.detail.description"
}
```

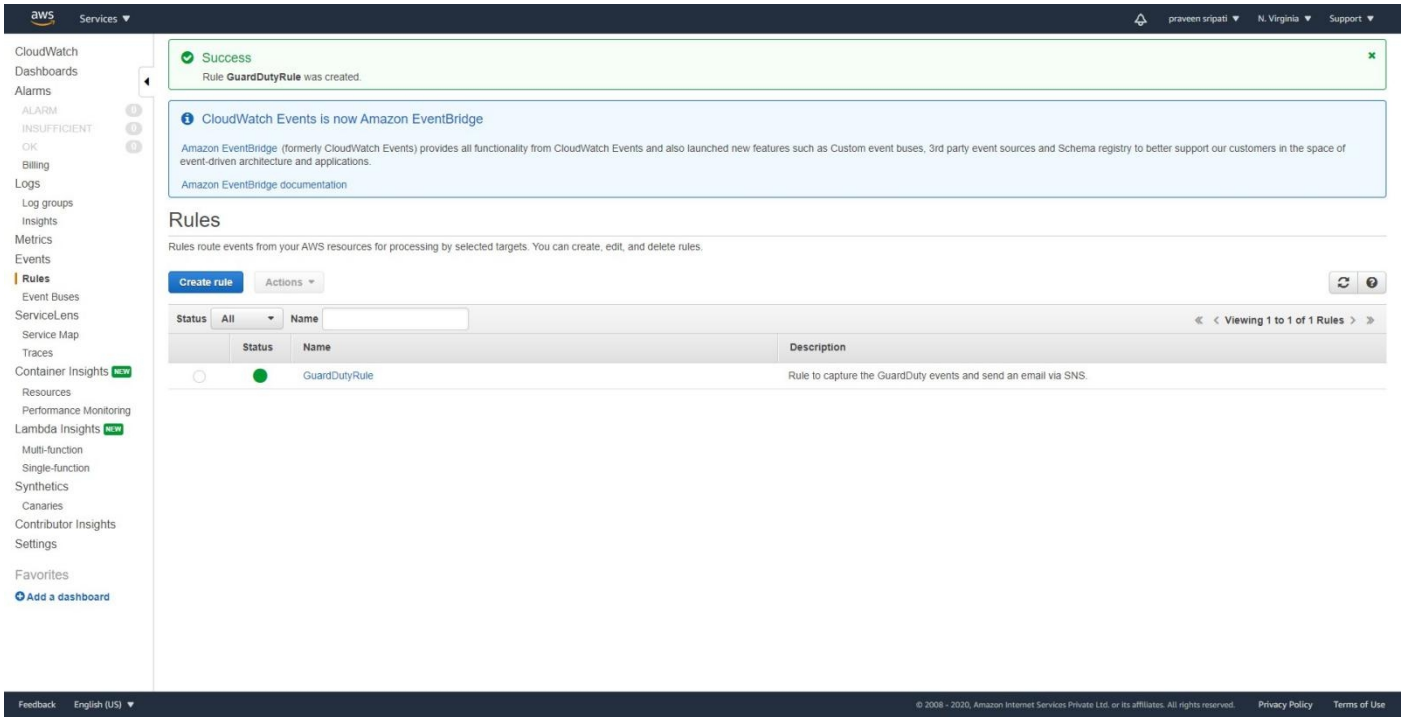
And for the **Input Template,** enter the below text and click on **Configure details**.

"You have a severity <severity> GuardDuty finding type <Finding_Type> in the <region> region."
"Finding Description:"
"<Finding_description>. "
"For more details open the GuardDuty console at https://console.aws.amazon.com/guardduty/home?region=<region>#/findings?search=id%3D<Finding_ID>"

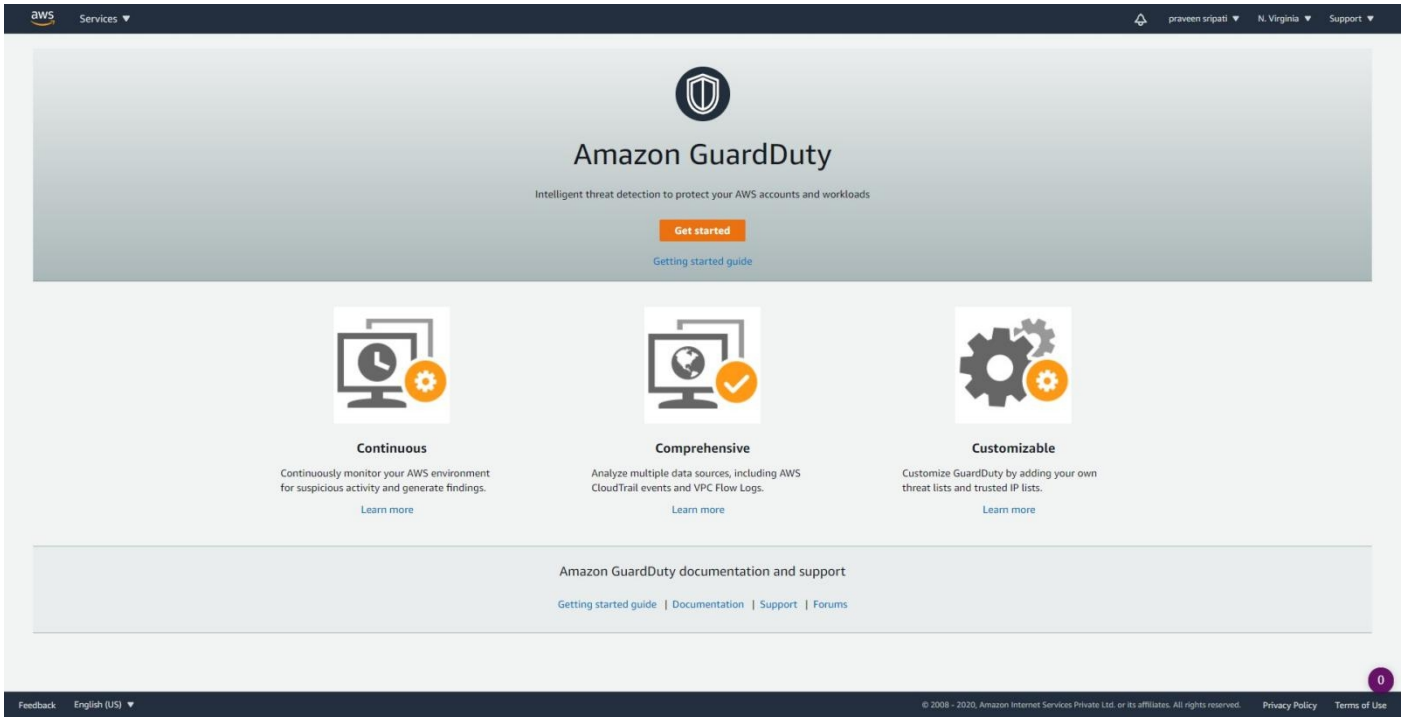


Step 9: Give the rule a name and enter some description. Click on **Create rule** to create the rule.

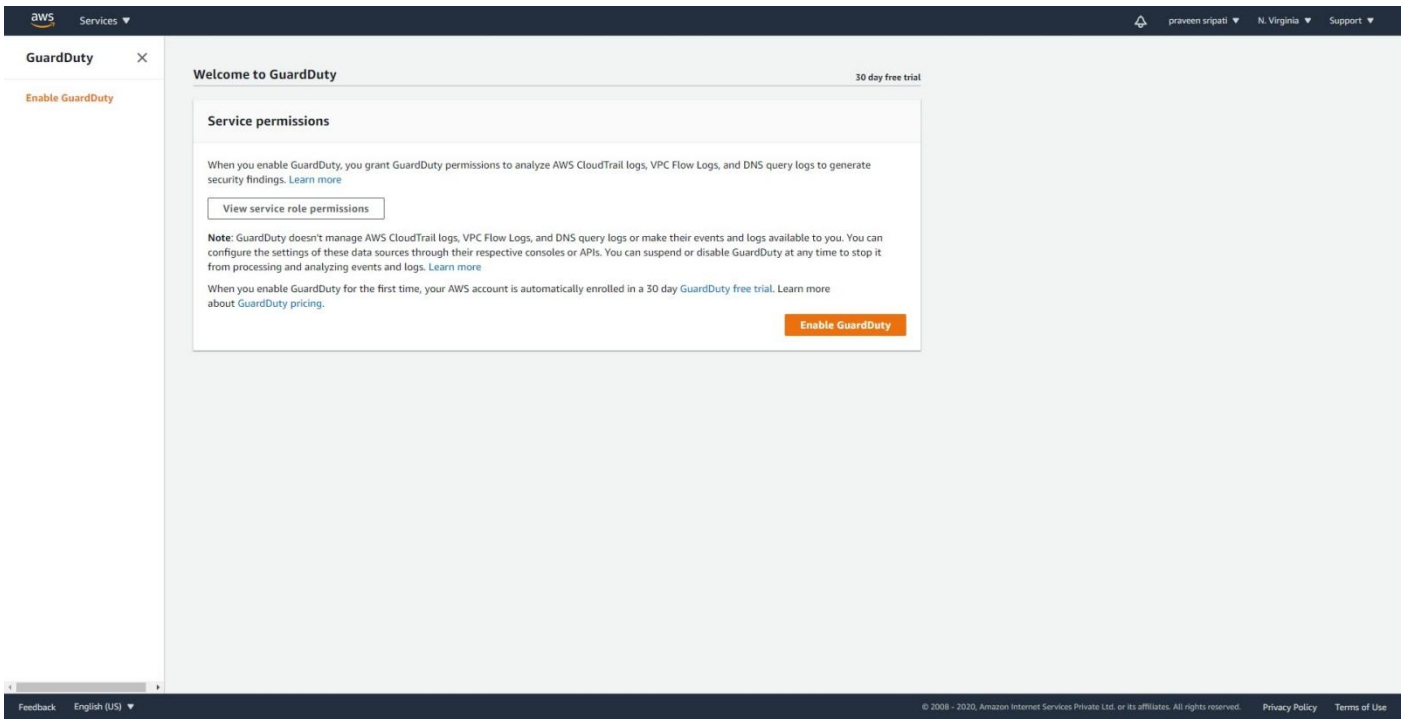




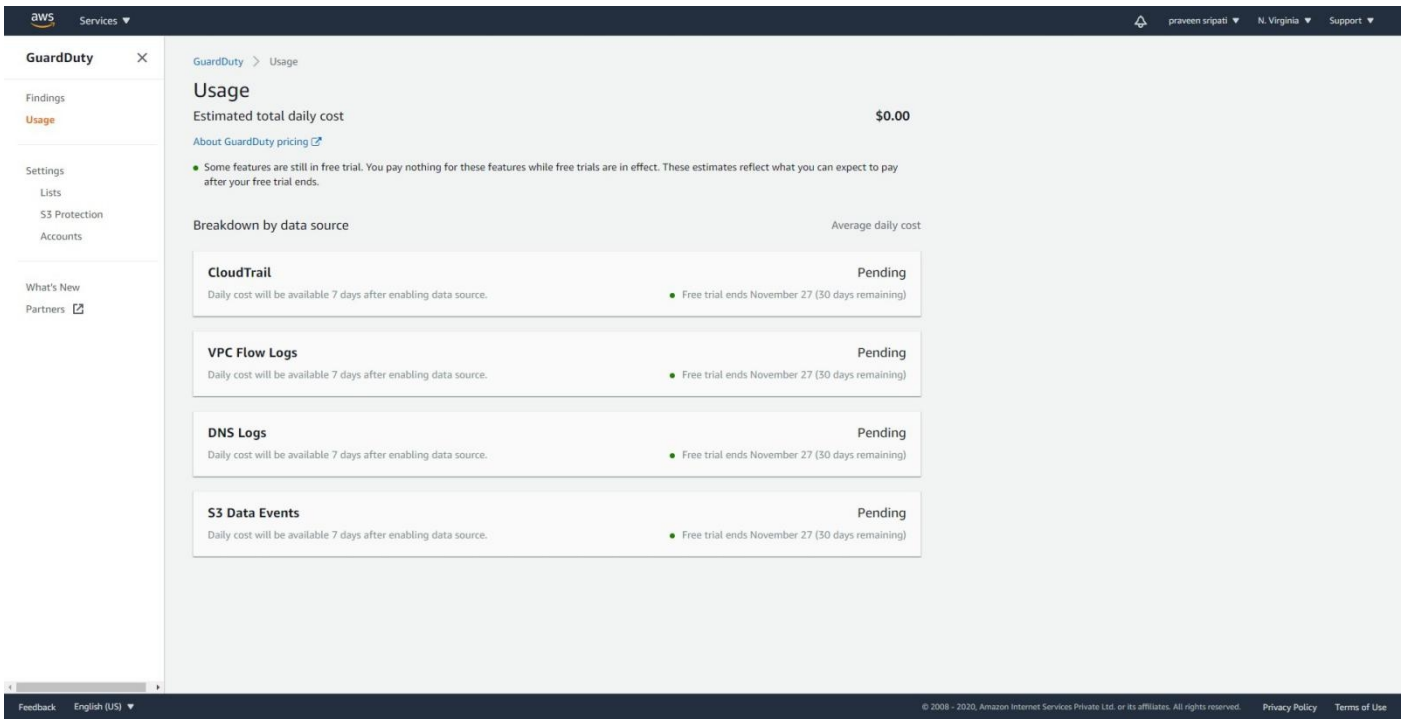
Step 10: Navigate to the GuardDuty Management Console and click on **Get started**.



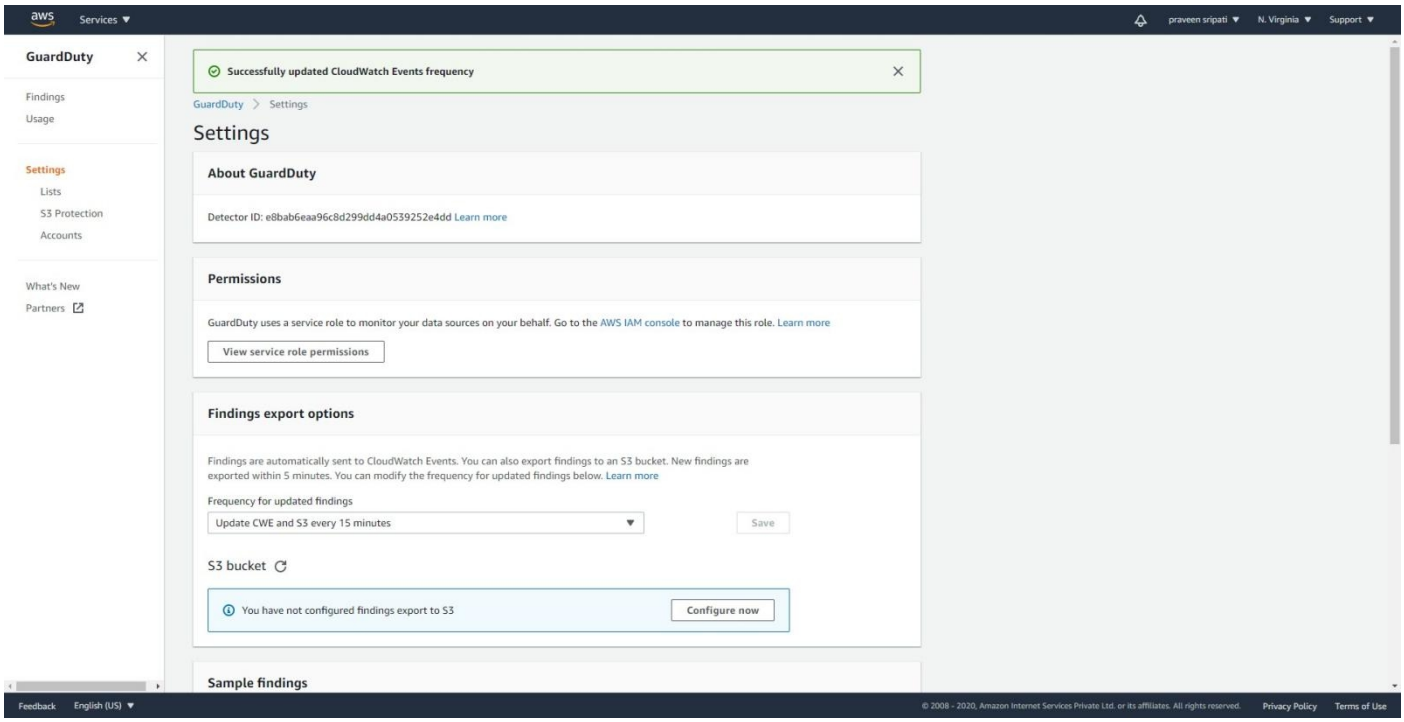
Step 11: Click on **Enable GuardDuty**.



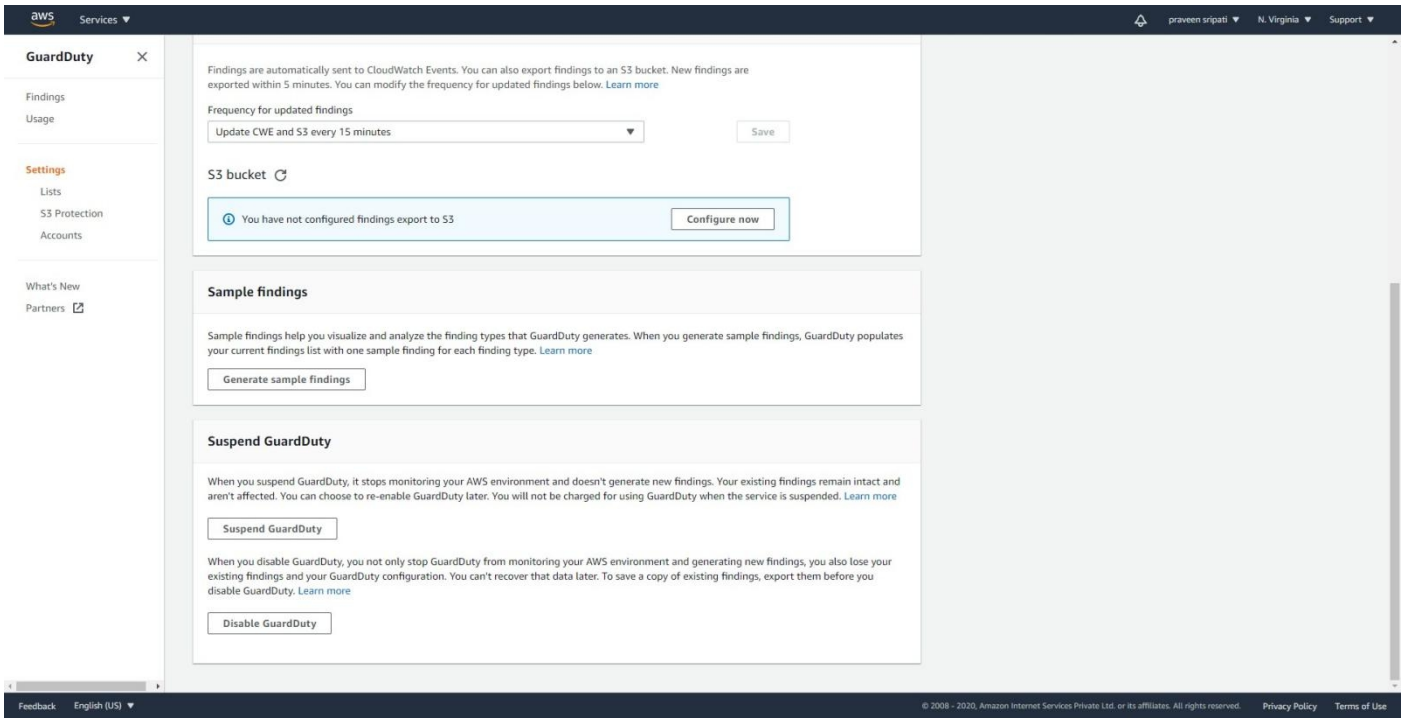
Step 12: GuardDuty is free for 30 days once we enable it. Go to the **Usage** tab to figure out how many days are left for free.



Step 13: Under the **Settings** tab, change the **Frequency for updated findings** to 15 minutes and click on **Save**.

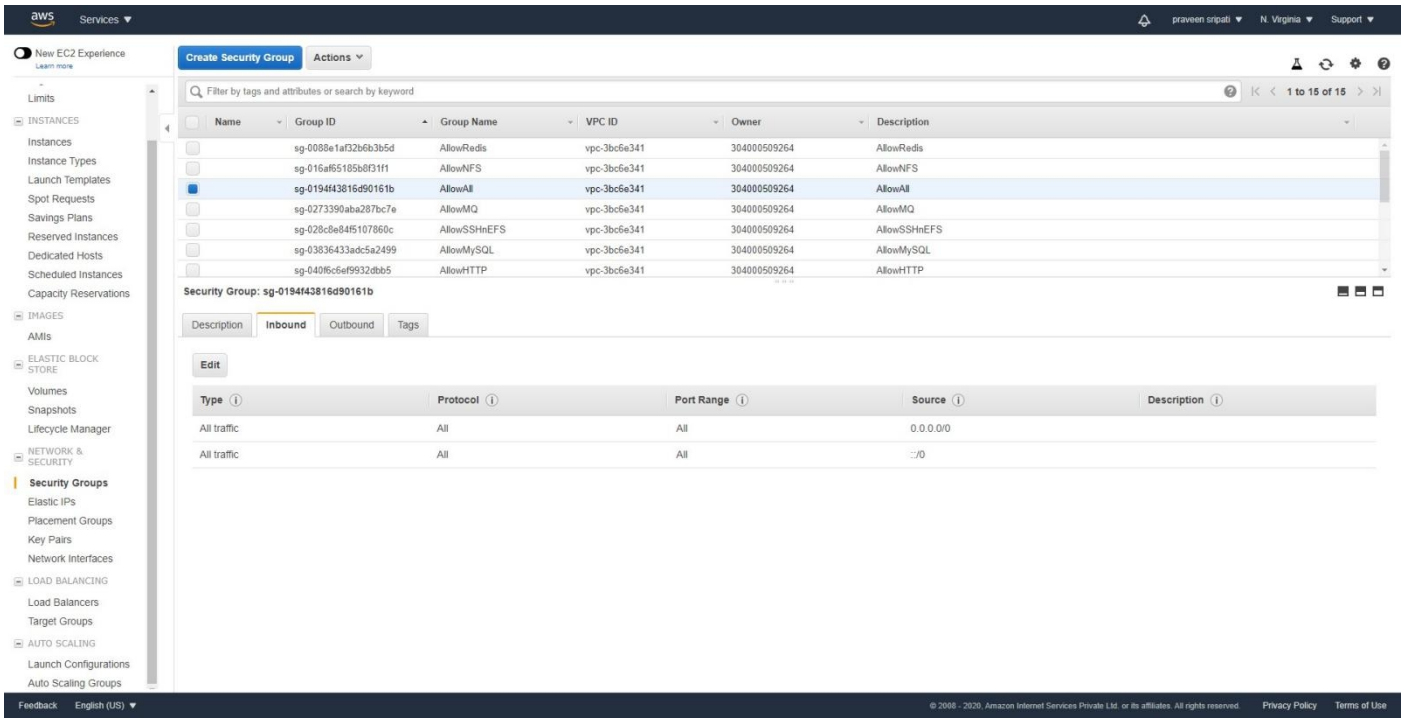


Step 14: For some reason, if we want to disable GuardDuty, you can use the option **Disable GuardDuty** in the same Settings tab. For now, keep it enabled, so there is no need to make any changes.

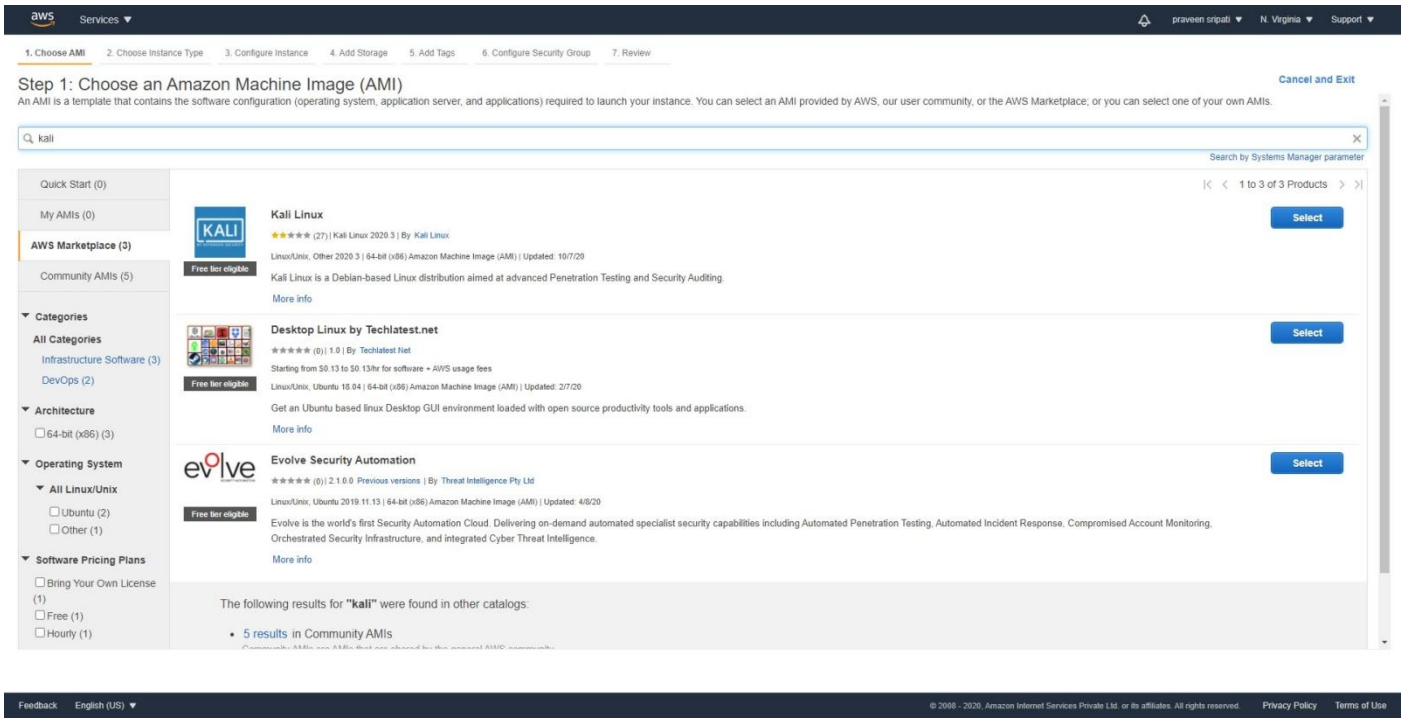


Step 15: In the EC2 Management Console, create a Security Group with all the traffic allowed inbound, as shown below.

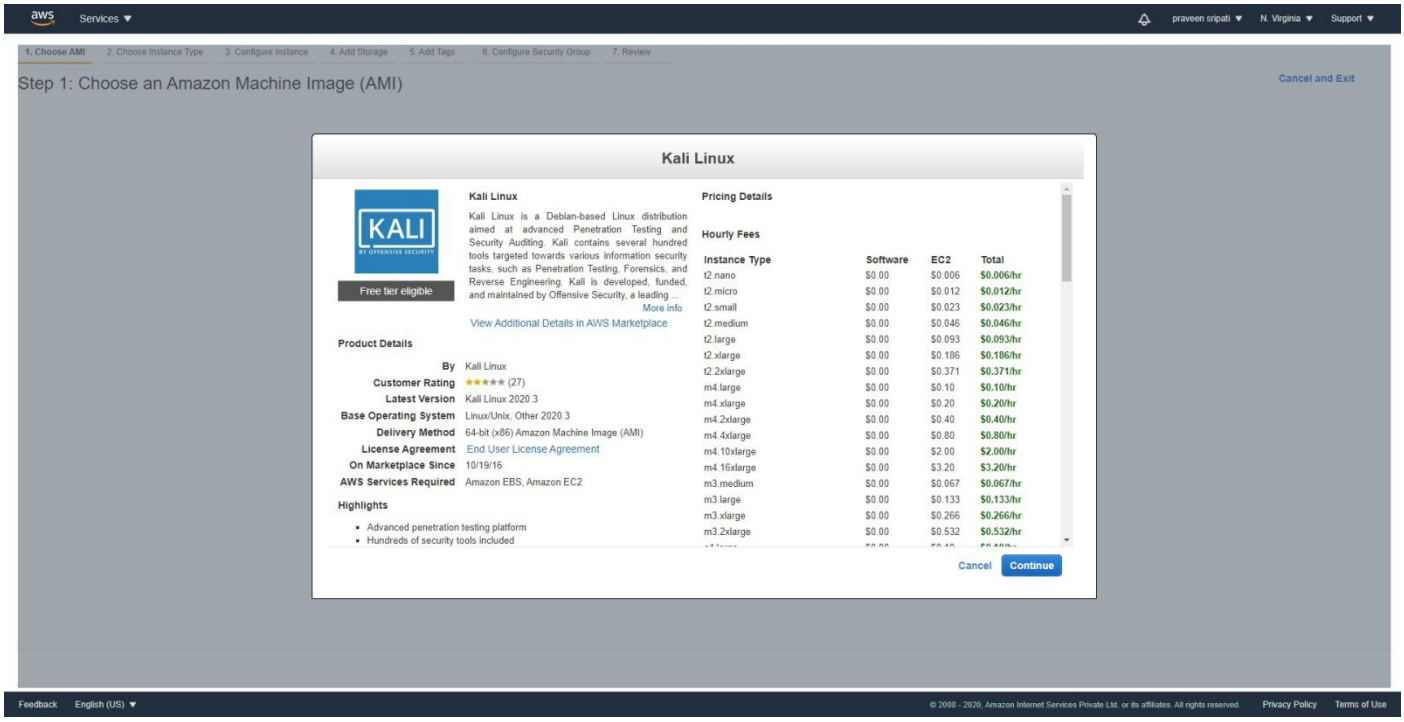
Note: We do not recommend this approach. This is only for demonstration.



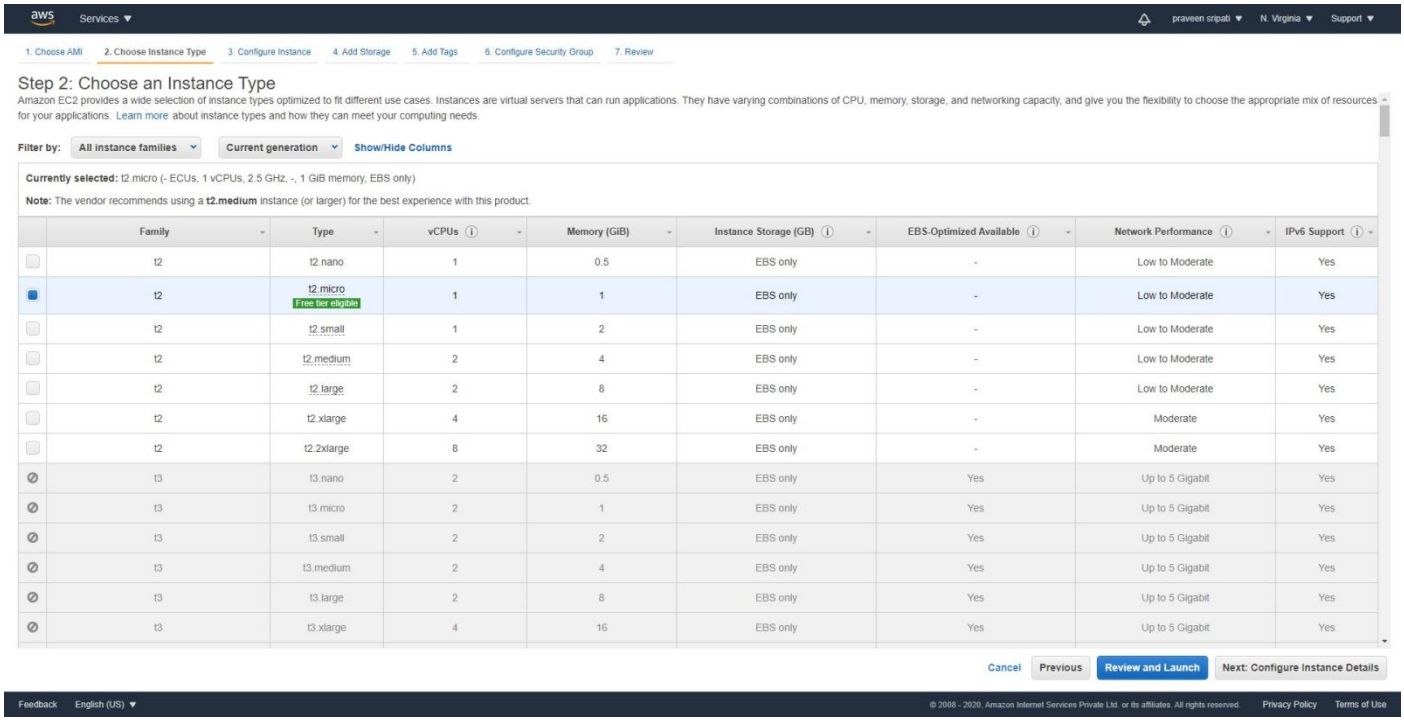
Step 16: Launch an EC2 instance and select **Kali Linux** under the AWS Marketplace. Kali Linux is mainly used for penetration testing and any action we take against AWS resources will be captured by GuardDuty as an anomaly.



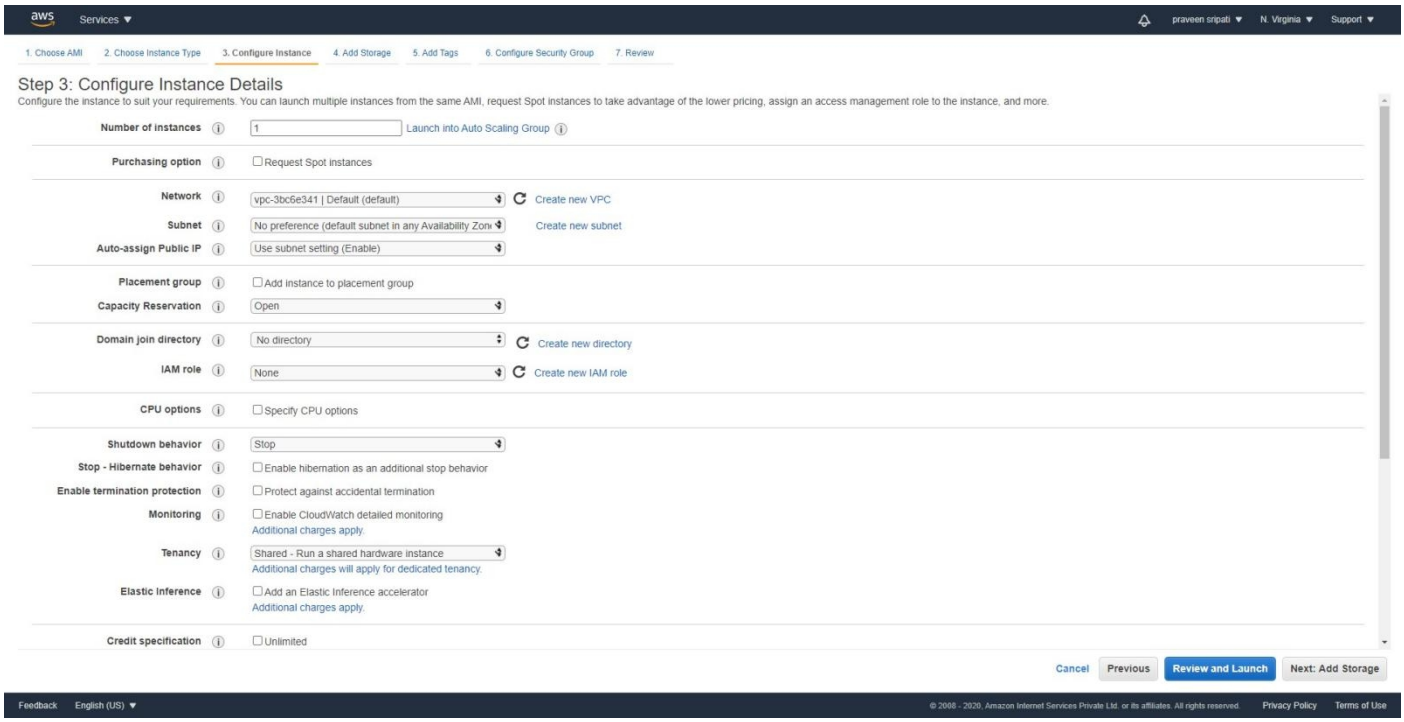
Step 17: Click on **Continue**.



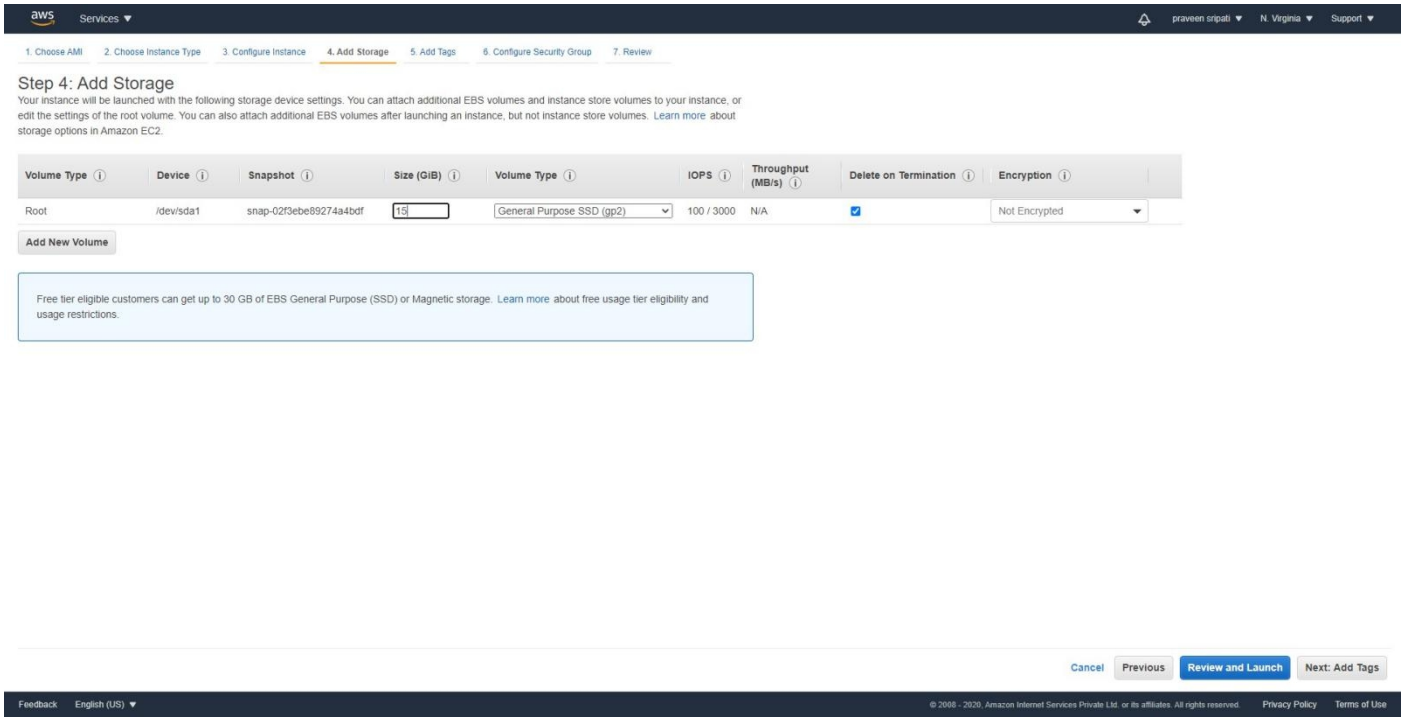
Step 18: Make sure to select **t2.micro** as it falls under the AWS free trial. Click on **Next**.



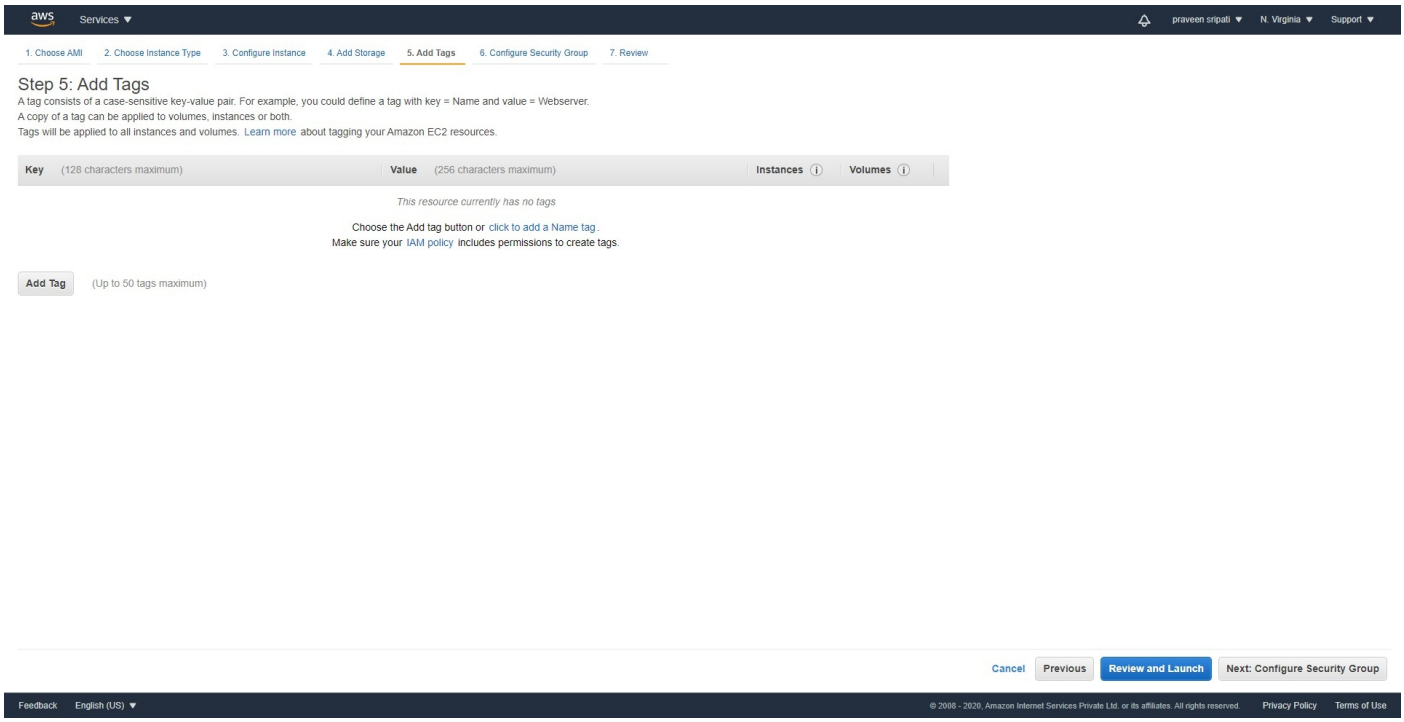
Step 19: Go with the default options under the **Configure Instance Details** and click on **Next**.



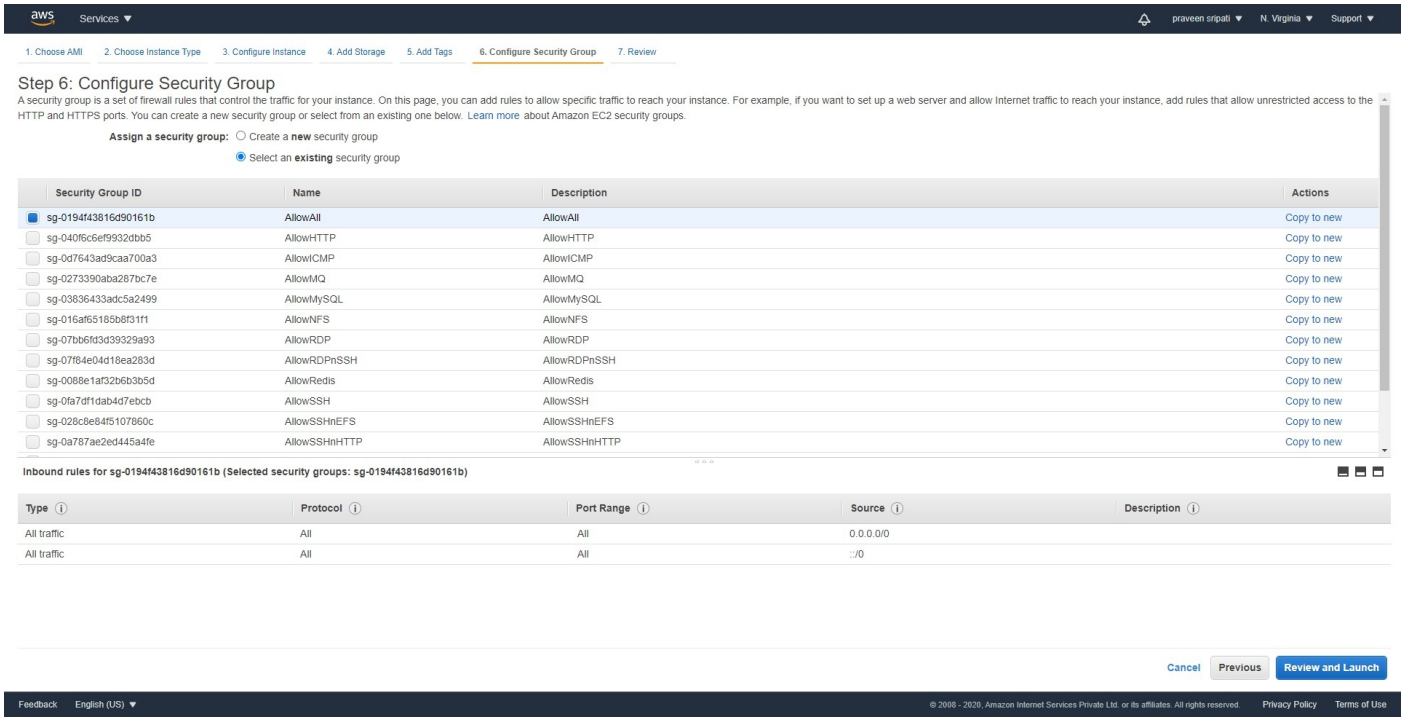
Step 20: On this EC2 instance, we will install a bunch of software applications to change the storage from the default 8GB to 15GB. Click on **Next**.



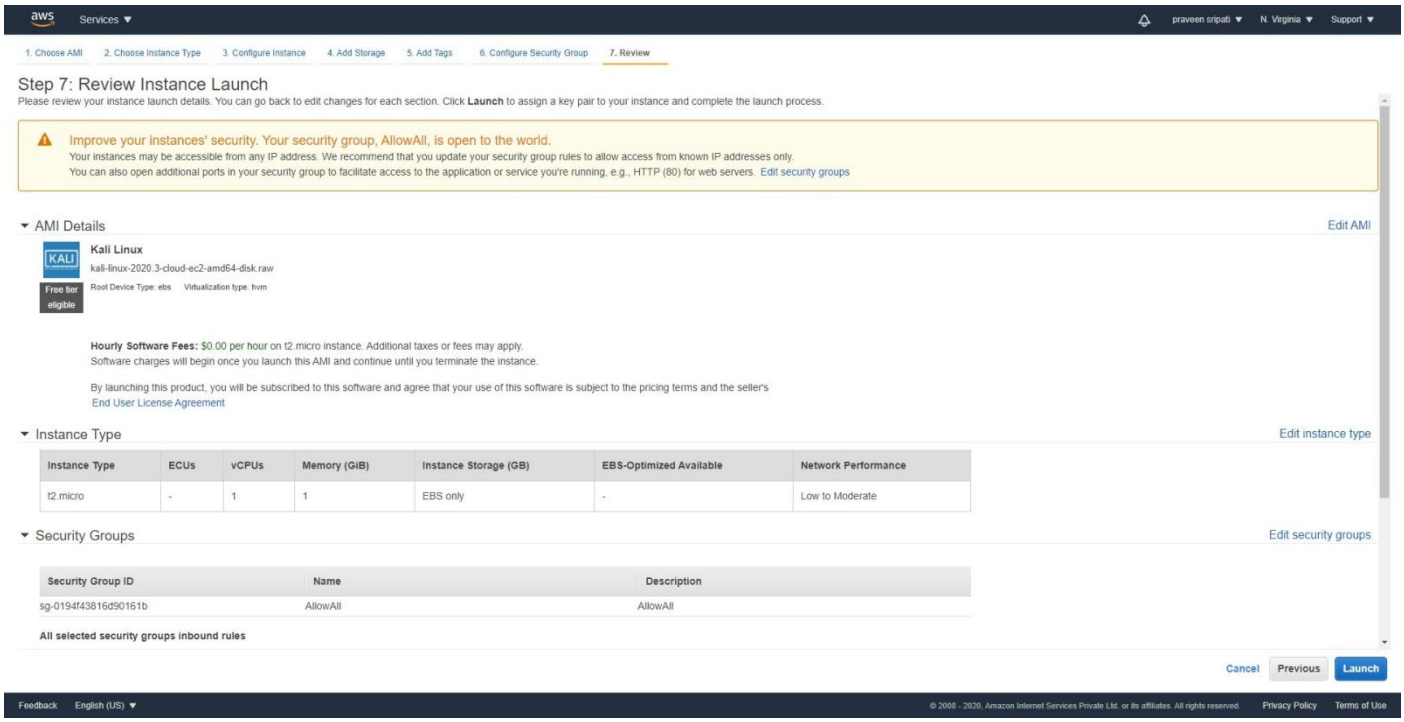
Step 21: Tags are optional. Click on **Next**.



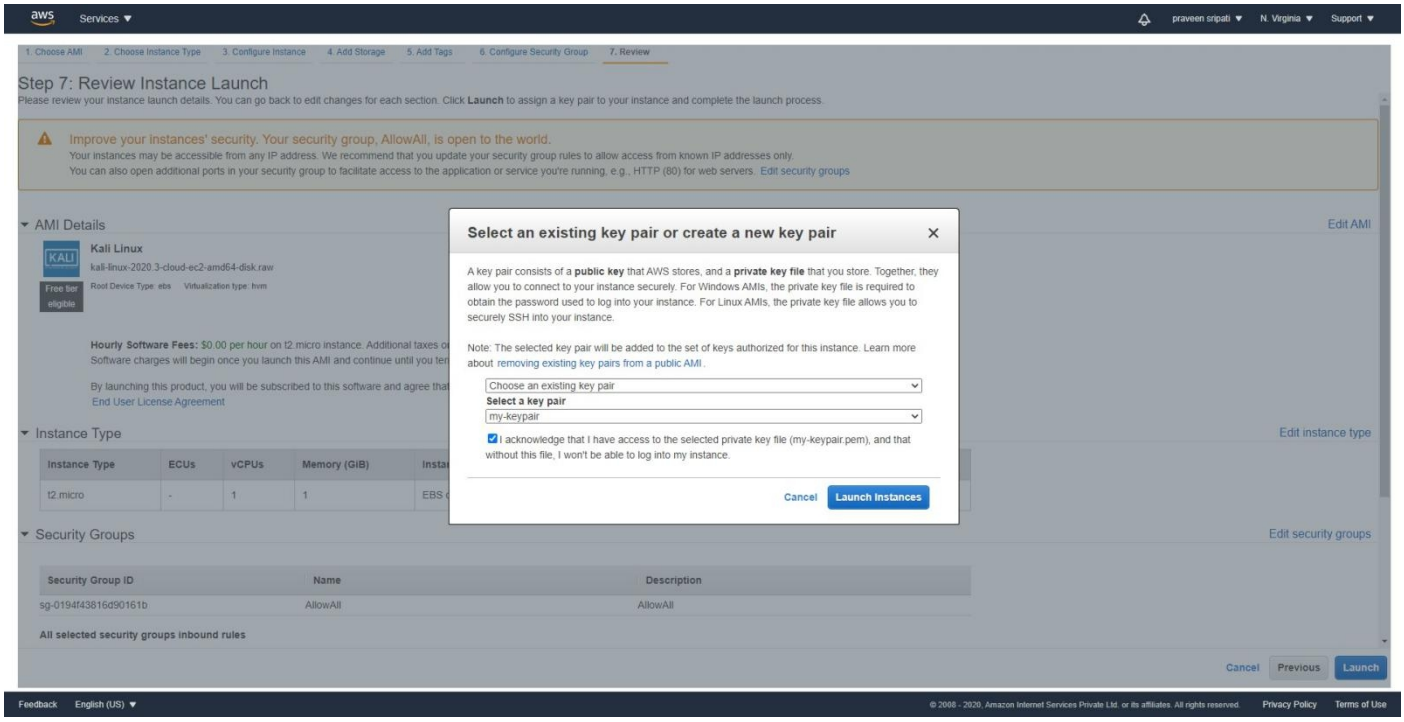
Step 22: Under the **Select an existing security group,** select the Security Group created in the previous step. Click on **Next**.



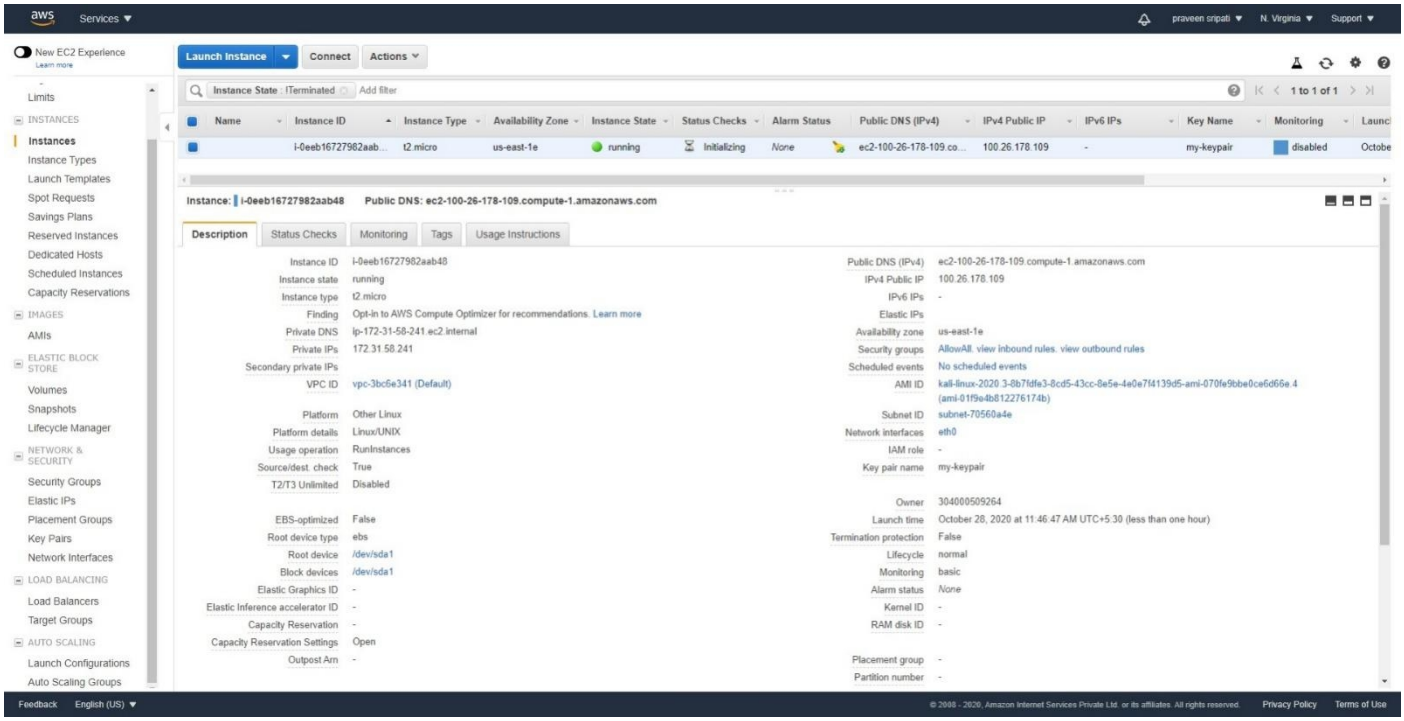
Step 23: Review all the details and click on **Launch**.



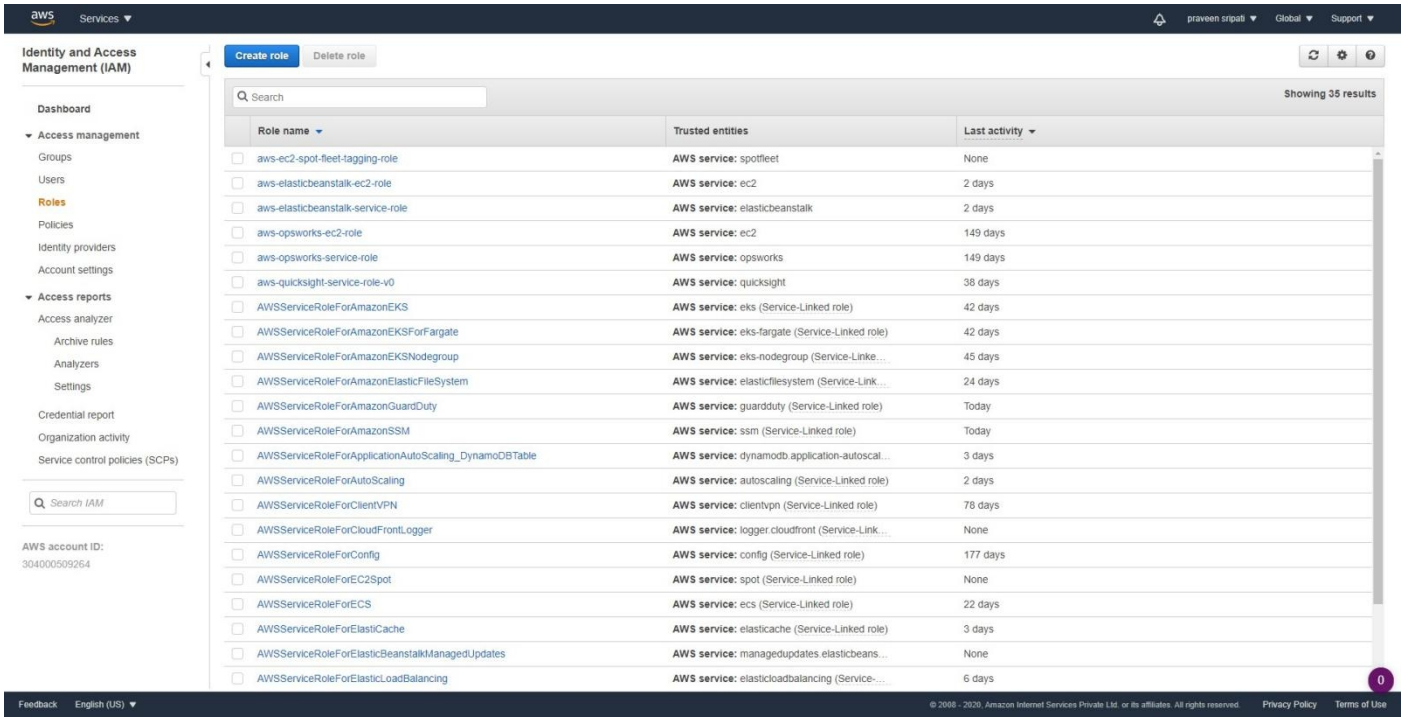
Step 24: Make sure to select the KeyPair, select **I acknowledge ….** and click on **Launch Instances**.



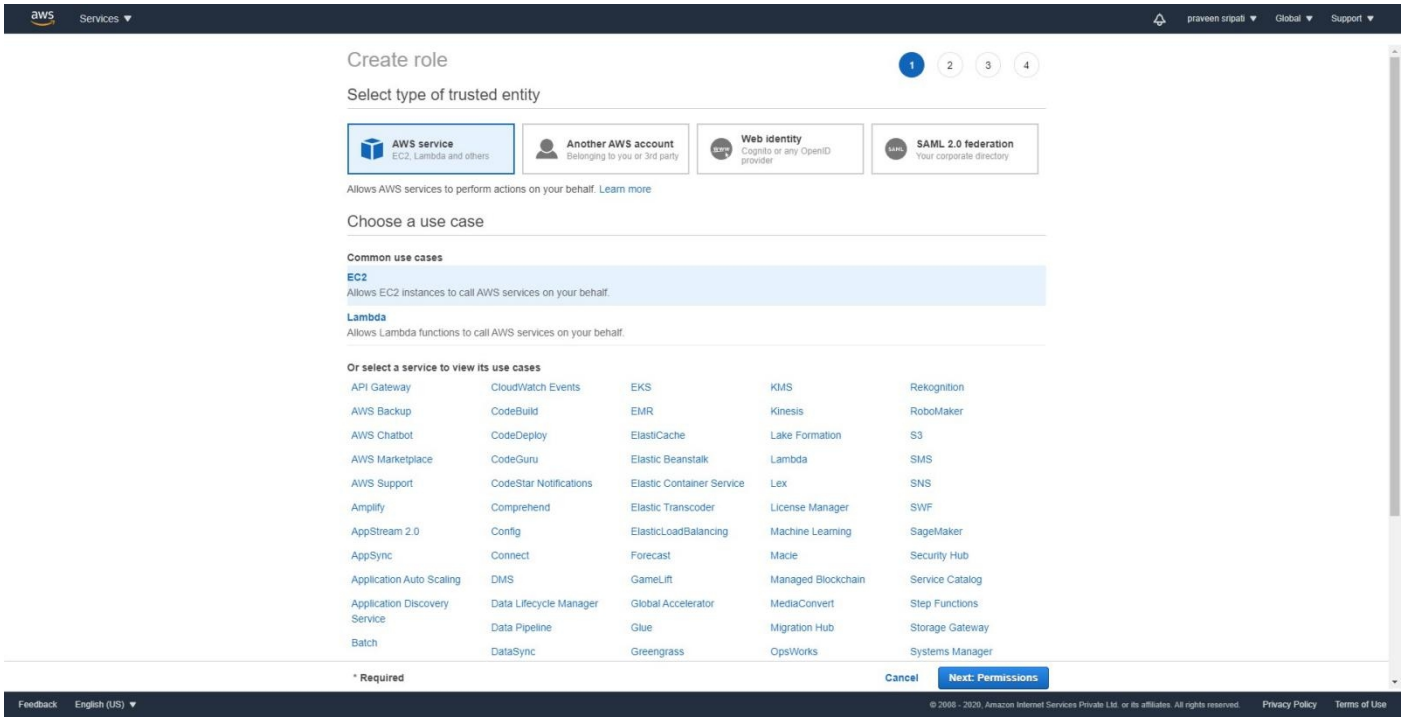
Step 25: The EC2 instances would in a **running** state in a few minutes.



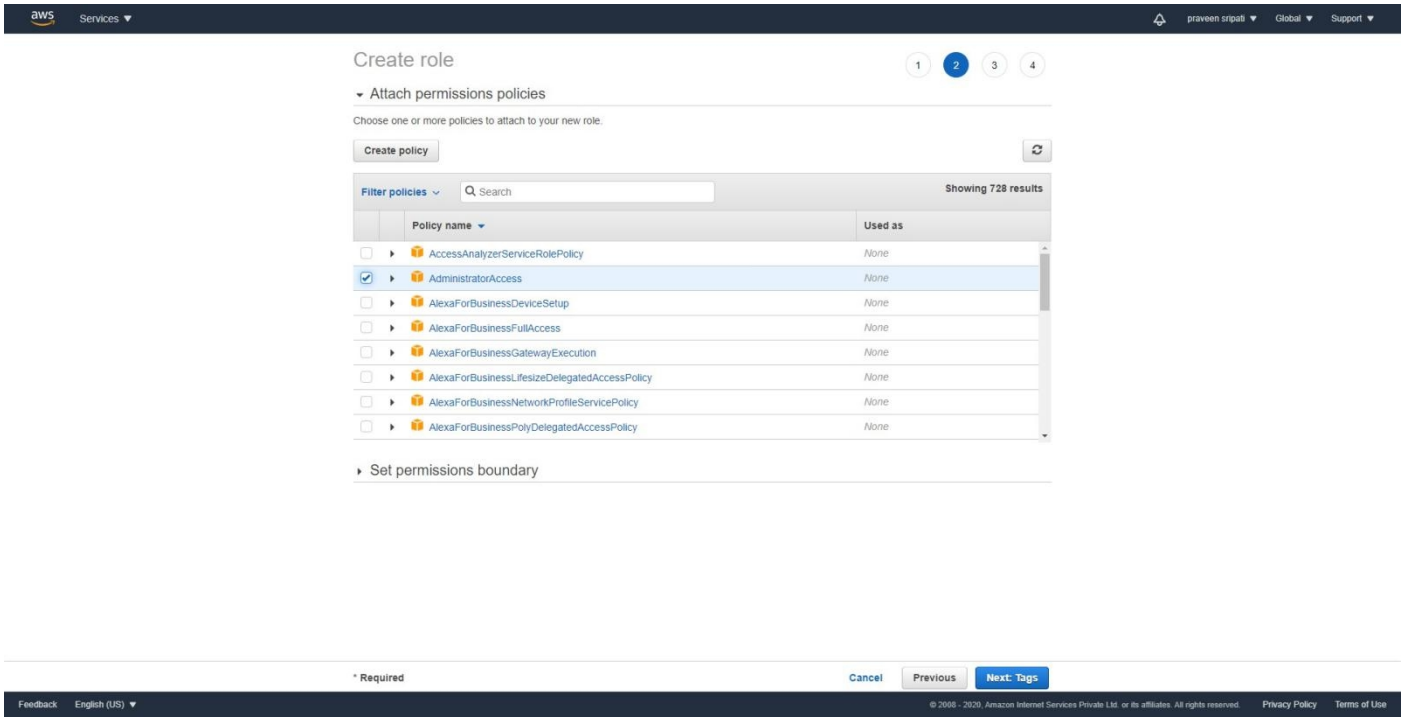
Step 26: Go to the IAM Management Console and then to the **Roles** tab. Click on **Create role**.



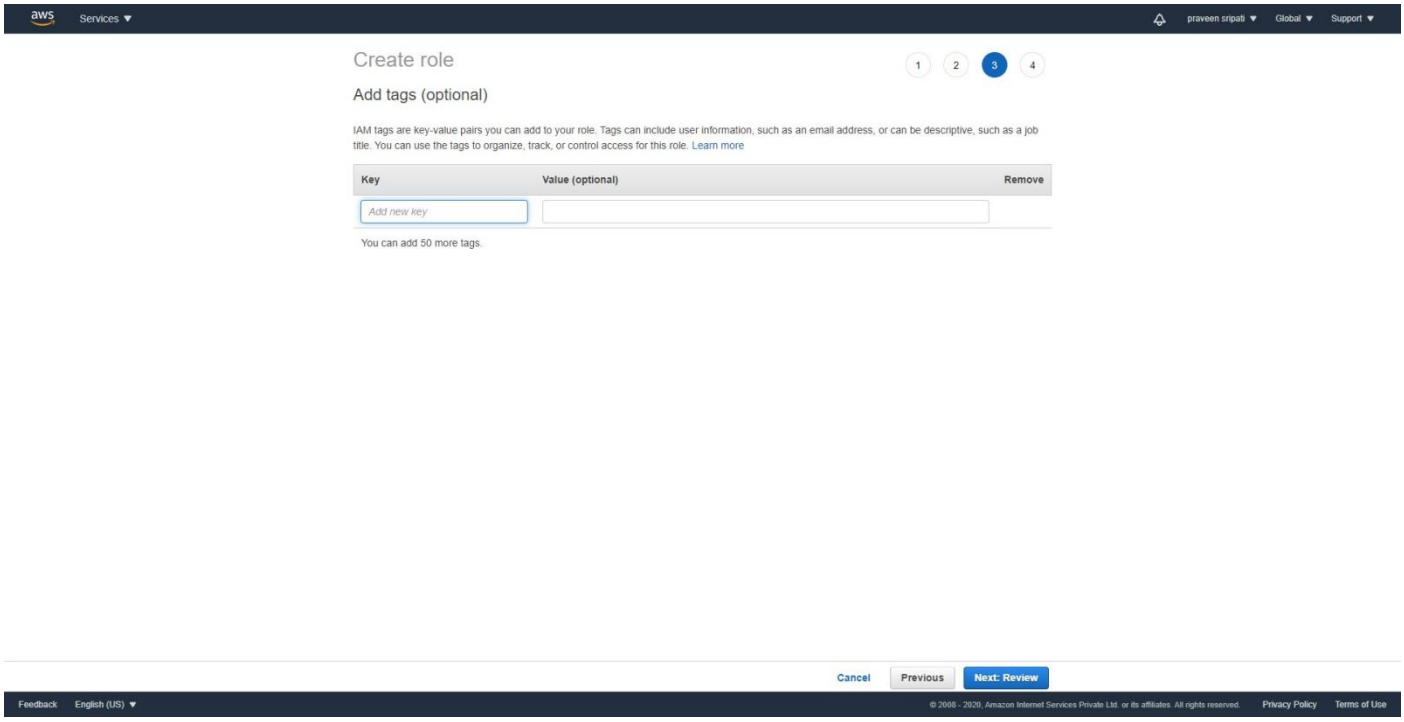
Step 27: Select EC2 under **Common use cases** and click on **Next**.



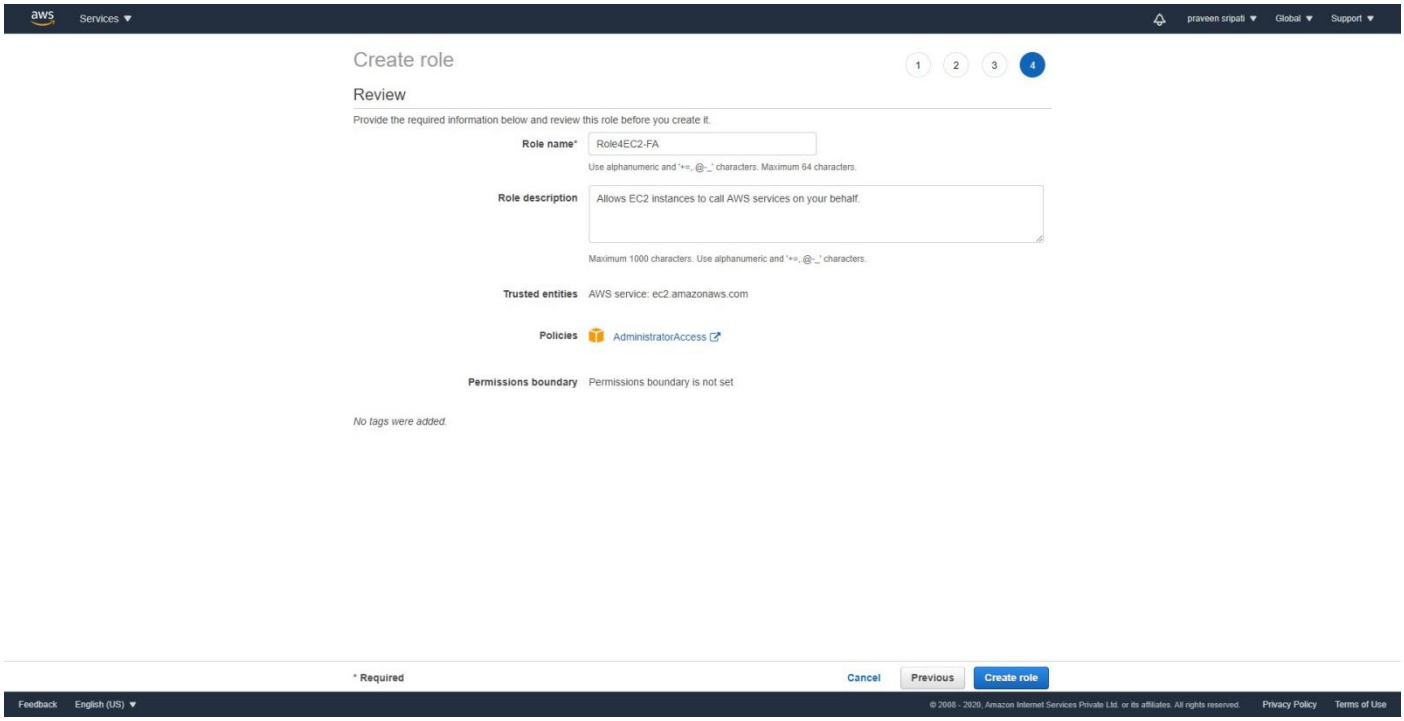
Step 28: Select **AdministratorAccess** Policy and click on **Next**.



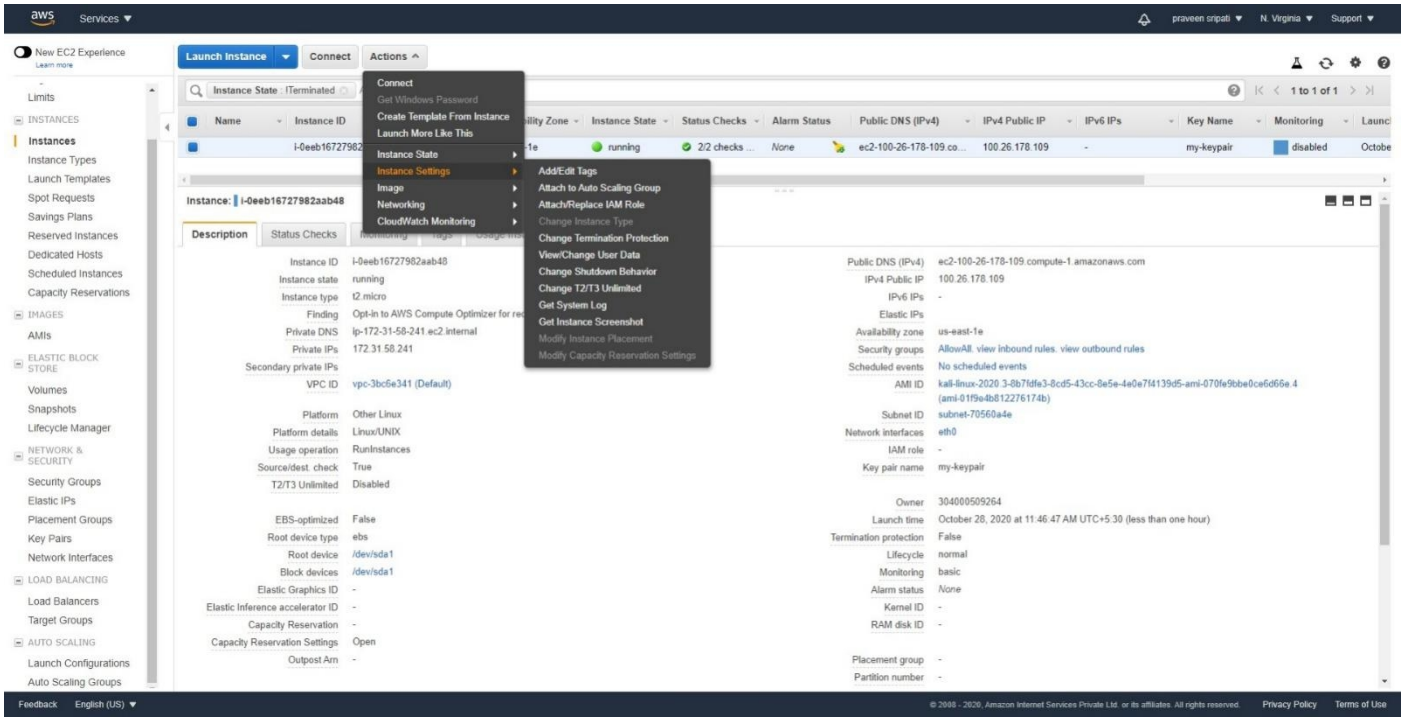
Step 29: Tags are optional. Click on **Next**.



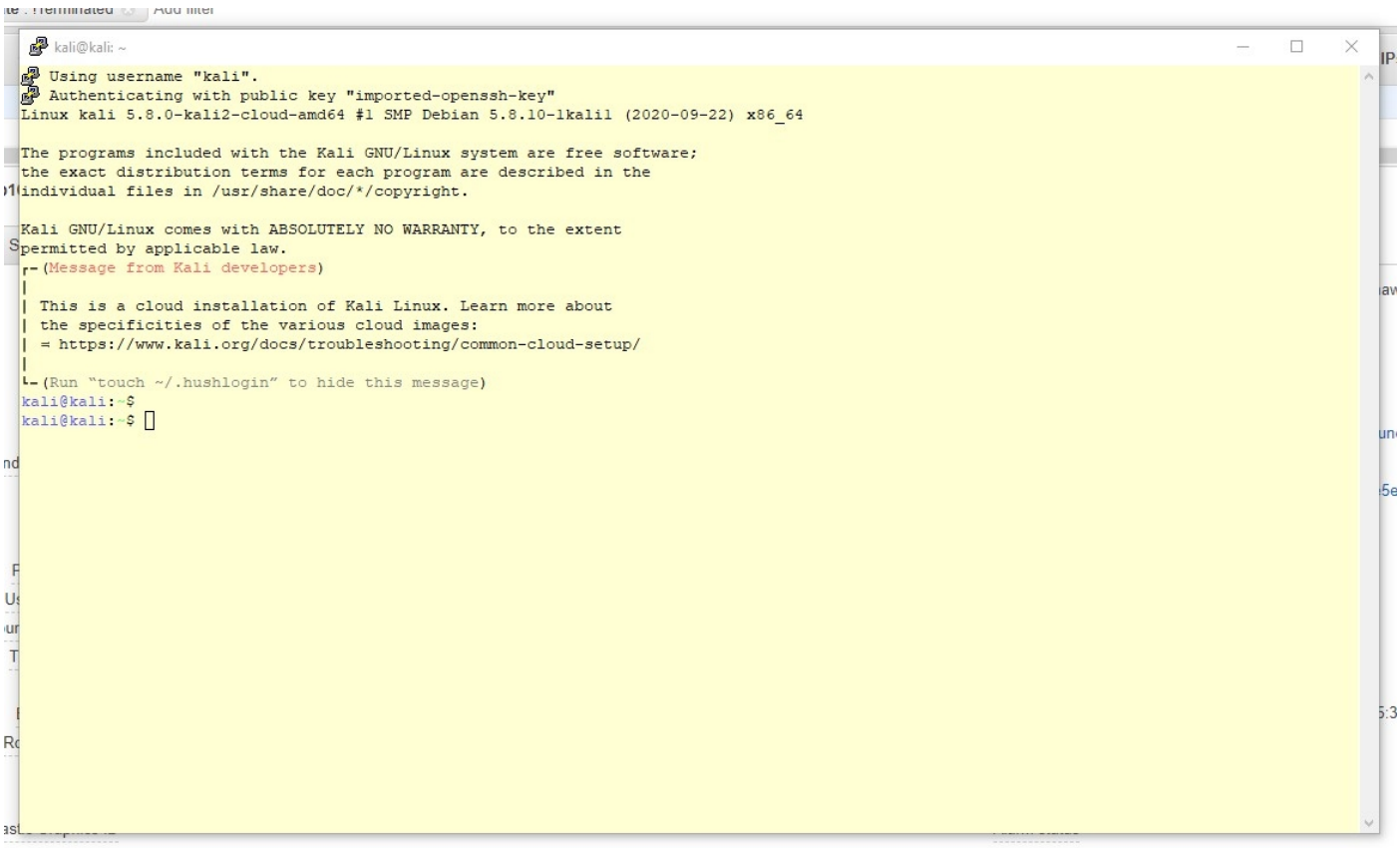
Step 30: Give the Role a name and click on **Create role**.



Step 31: Attach the IAM Role to the earlier created EC2 instance.



Step 32: Connect to the EC2 instance via PuTTY or some other SSH client. Note that the user name to connect to the EC2 instance is **kali**.



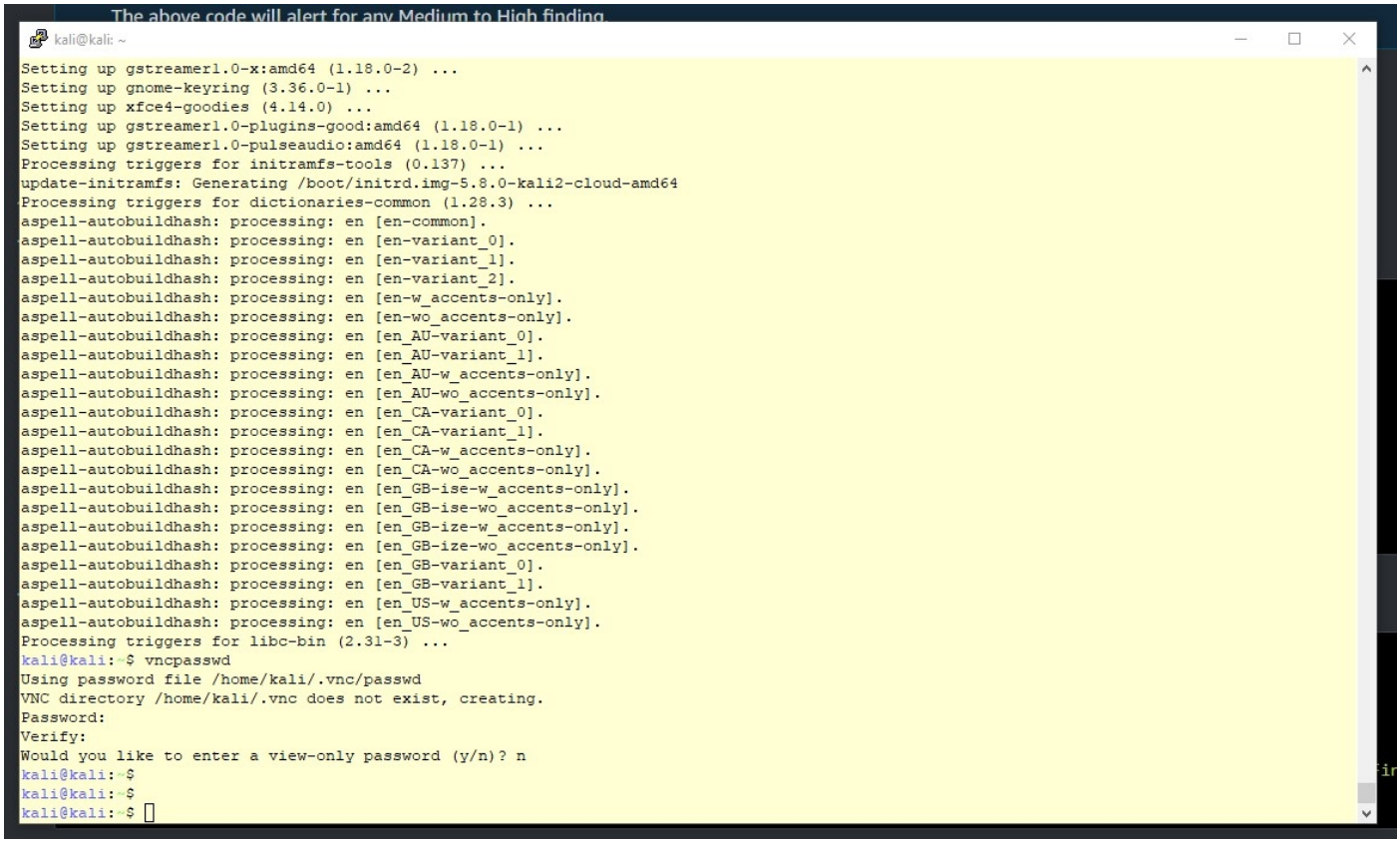
Step 33: The below actions have to be performed on the Kali Linux:

a) Execute the below commands.

sudo apt update
sudo apt install -y xfce4 xfce4-goodies tightvncserver midori python3 python3-pip
pip install awscli –upgrade
export PATH="$PATH:/home/ubuntu/.local/bin/"

b) Execute the **aws configure** command and enter **us-east-1** for the default Region and leave the rest of the fields without anything.

c) Execute the **vncpasswd** command and enter the **kali123** password thrice, as shown below at the end.



d) Create a file in the **~/.vnc/xstartup** path with the below content

#!/bin/bash
xrdb $HOME/.Xresources
startxfce4 &

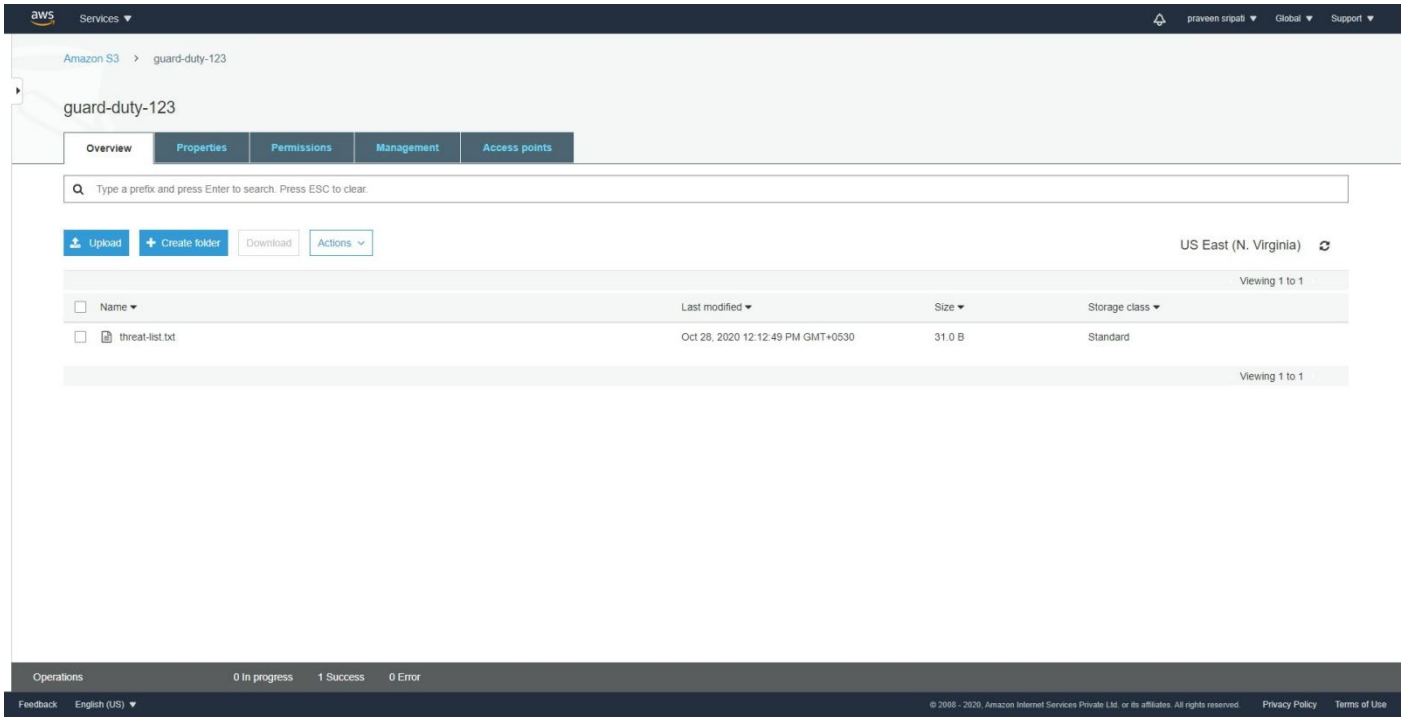
e) Change the permissions on the above file and execute the **vncserver** command.

chmod +x ~/.vnc/xstartup
vncserver

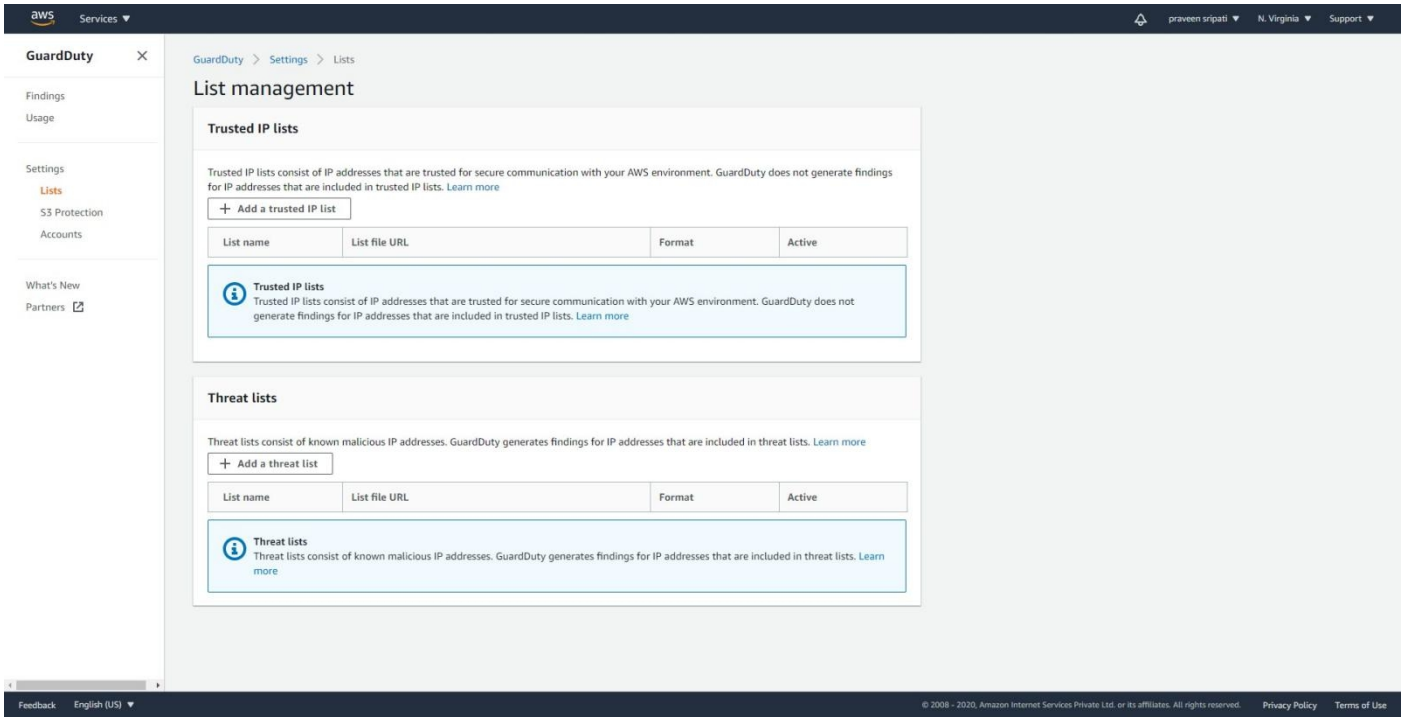
Step 34: Create a file named **threat-list.txt** with the IP address of Google and the Public IP of the EC2. One IP address per line, as shown below. The IP address of the Google can be obtained by executing **ping google.com** command from the Windows Command Prompt.

a.b.c.d
m.n.o.p

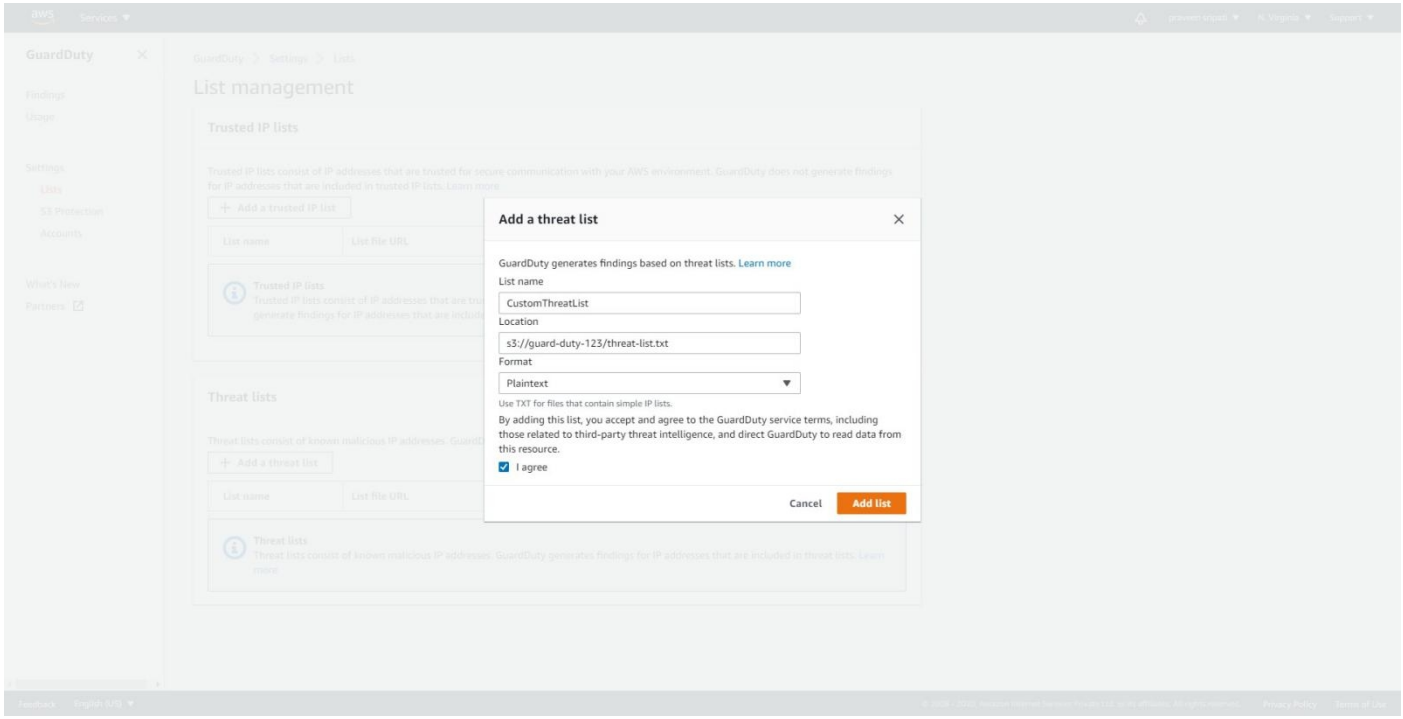
Now, create an S3 bucket and upload the file, as shown below.

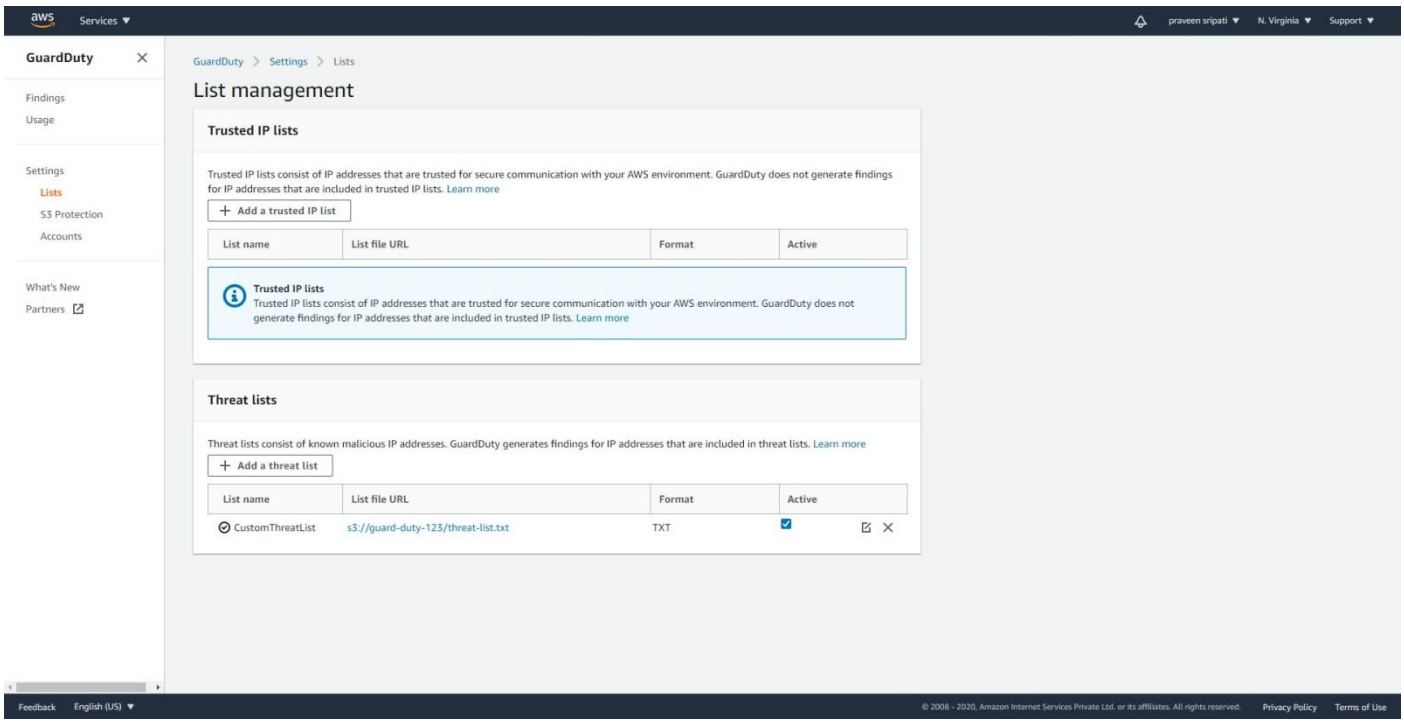


Step 35: Go back to the GuardDuty Management Console and click on **Lists** under **Settings**. Click on **Add a threat list**.


aws
Services
praveen sripati
N. Virginia
Support
GuardDuty
Findings
Usage
Settings
Lists
S3 Protection
Accounts
What's New
Partners
GuardDuty > Settings > Lists
List management
Trusted IP lists
Trusted IP lists consist of IP addresses that are trusted for secure communication with your AWS environment. GuardDuty does not generate findings for IP addresses that are included in trusted IP lists. Learn more
Add a trusted IP list
List name
List file URL
Format
Active
Trusted IP lists
Trusted IP lists consist of IP addresses that are trusted for secure communication with your AWS environment. GuardDuty does not generate findings for IP addresses that are included in trusted IP lists. Learn more
Threat lists
Threat lists consist of known malicious IP addresses. GuardDuty generates findings for IP addresses that are included in threat lists. Learn more
Add a threat list
List name
List file URL
Format
Active
Threat lists
Threat lists consist of known malicious IP addresses. GuardDuty generates findings for IP addresses that are included in threat lists. Learn more
Feedback
English (US)
© 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

Step 36: Give the list a name and enter the proper location of the file in S3 from the previous step. For the format, select **Plaintext**. And, finally, click on **I agree** and **Add list**.





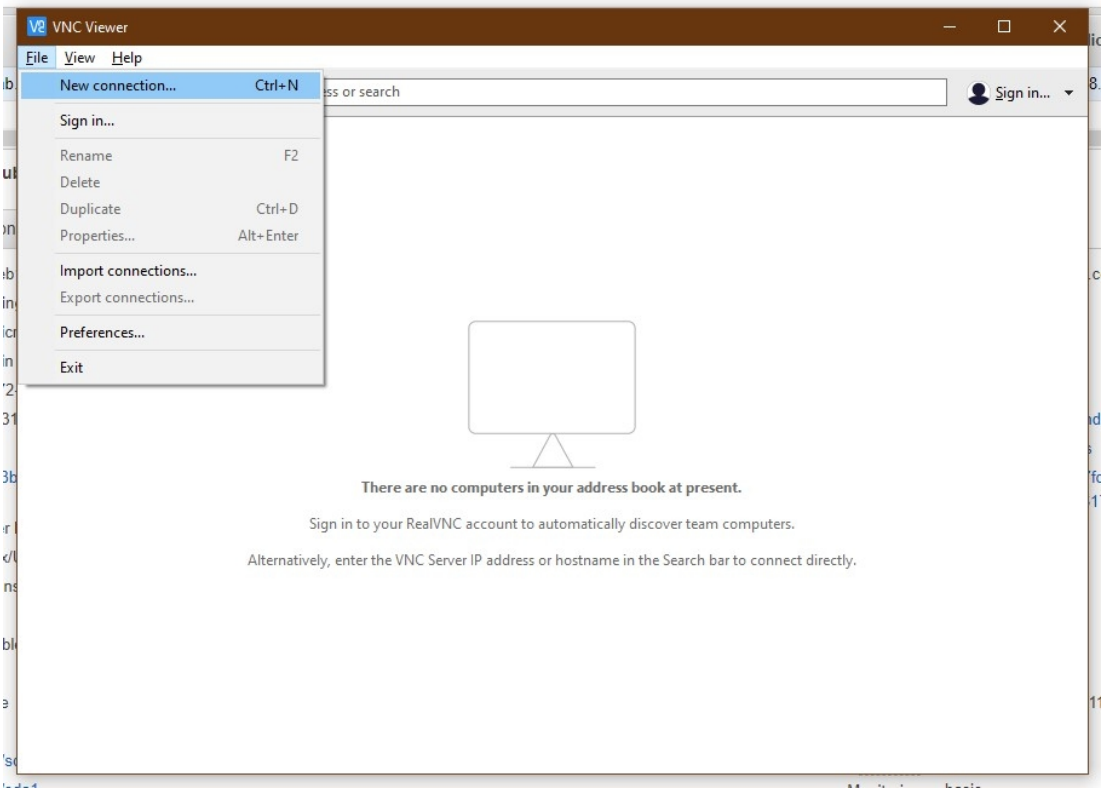
Step 37: From the PuTTY session connected to the Kali Linux, execute the below AWS CLI commands to get the S3 buckets and Security Groups list. This should be identified as an anomaly by the GuardDuty as the commands are run from Kali Linux, mainly used for penetration testing.

aws s3 ls
aws ec2 describe-security-groups

Step 38: Download the VNC Viewer from the below URL and install it as with any other software on the Windows OS. We would be using this later to get the GUI access to the Kali Linux EC2 instance.

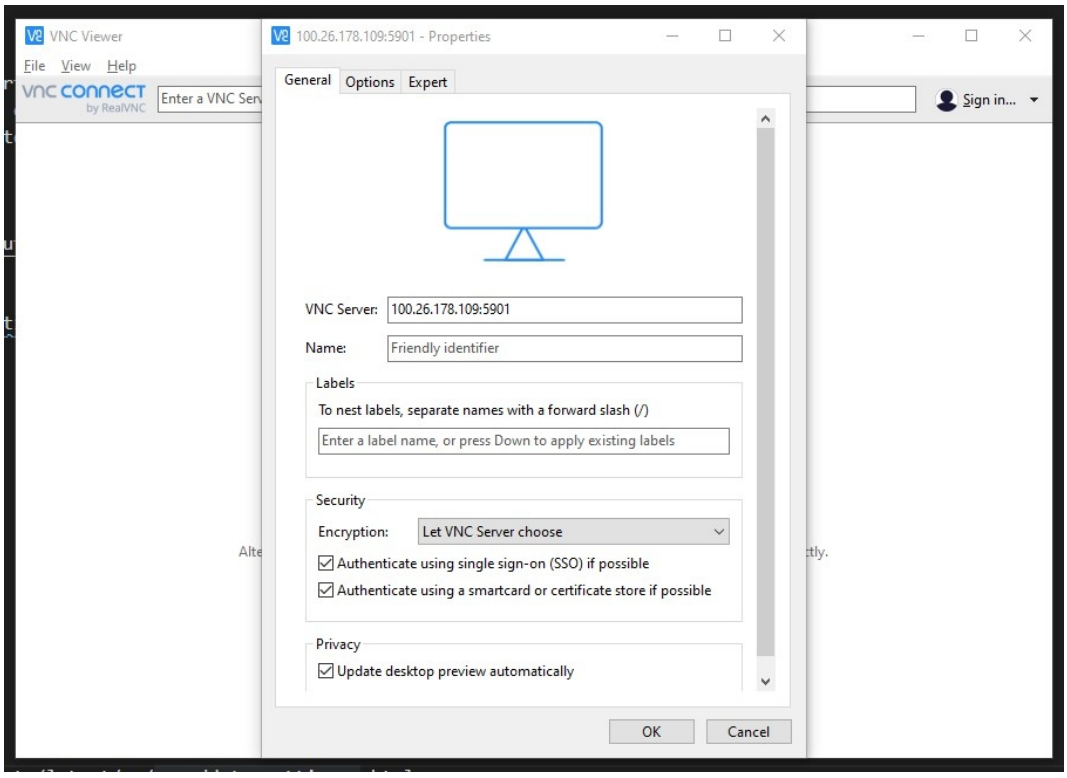
https://www.realvnc.com/en/connect/download/viewer/

Step 39: Start the VNC Viewer. Go to File -> New Connection.

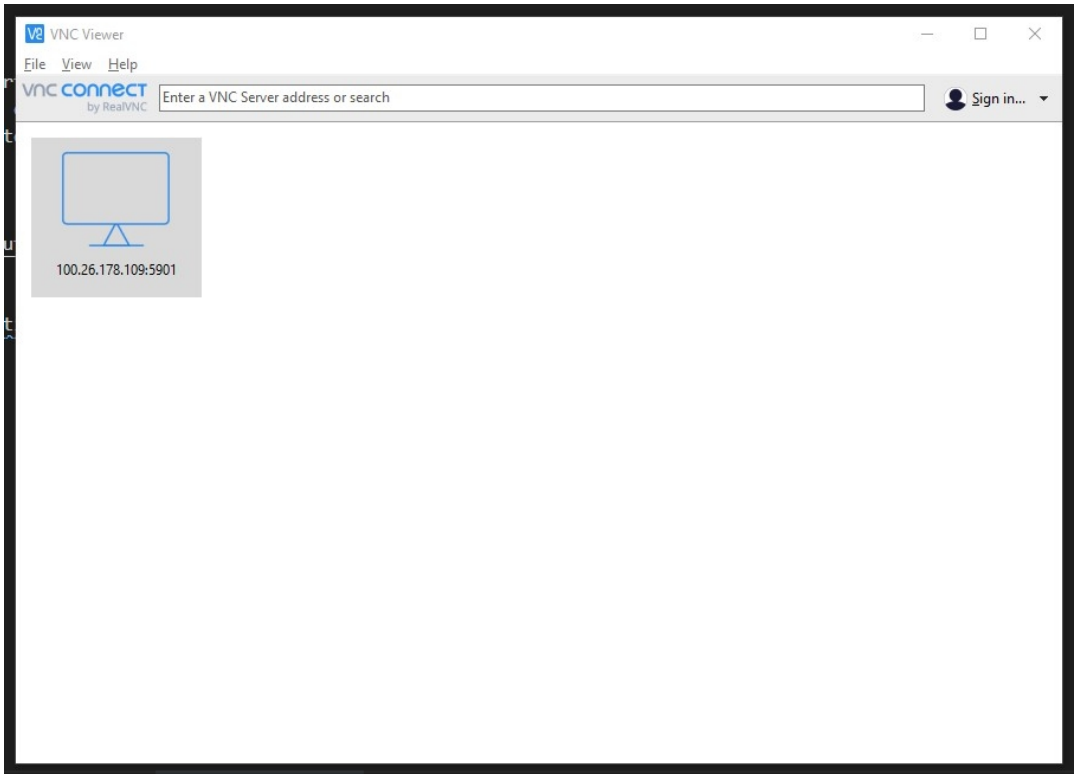


Step 40: Enter the VNC Server details in the below format and click on **OK**.

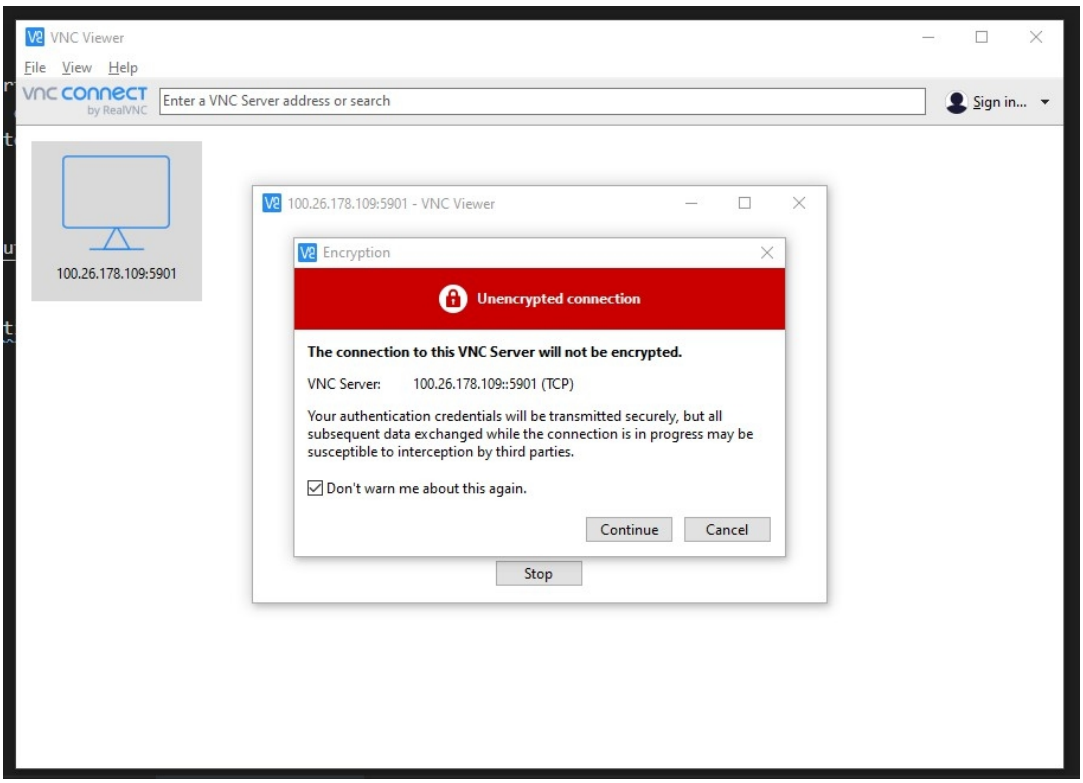
public-ip-of-ec2:5901



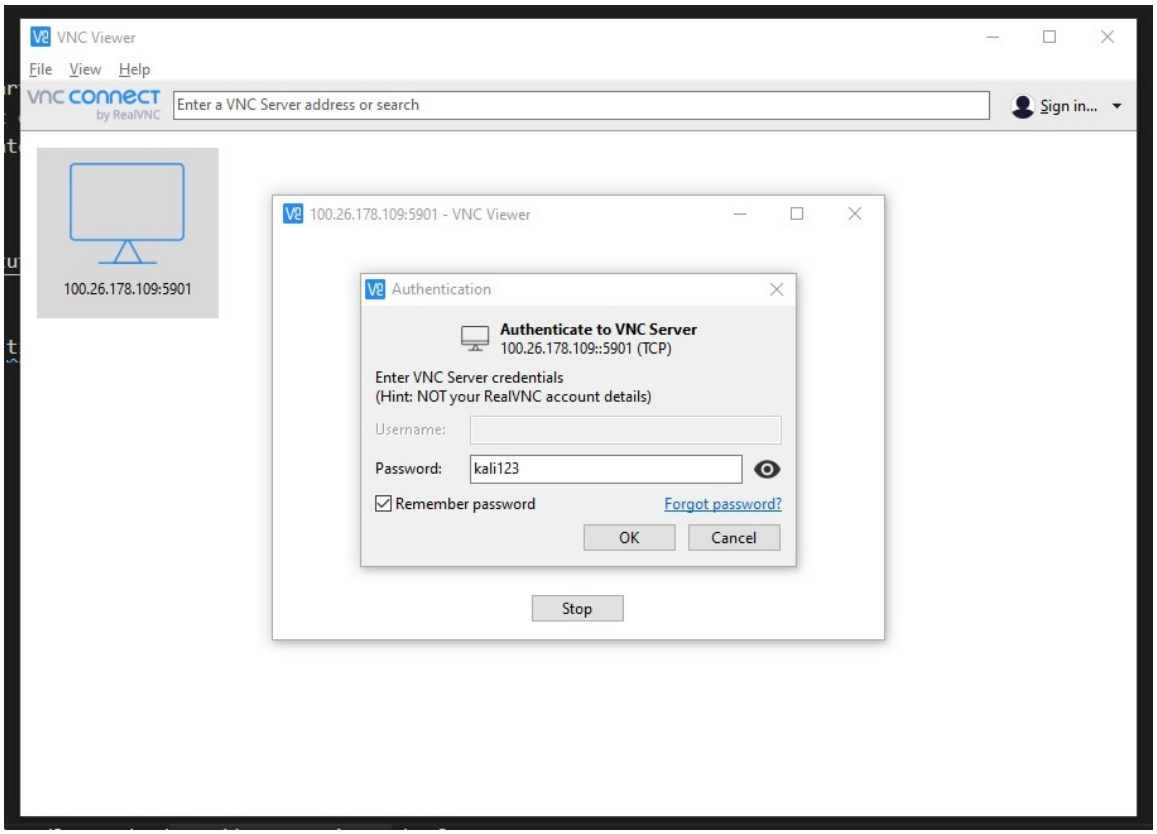
Step 41: An entry should be created, as shown below. Double click on it to connect to the Kali Linux.



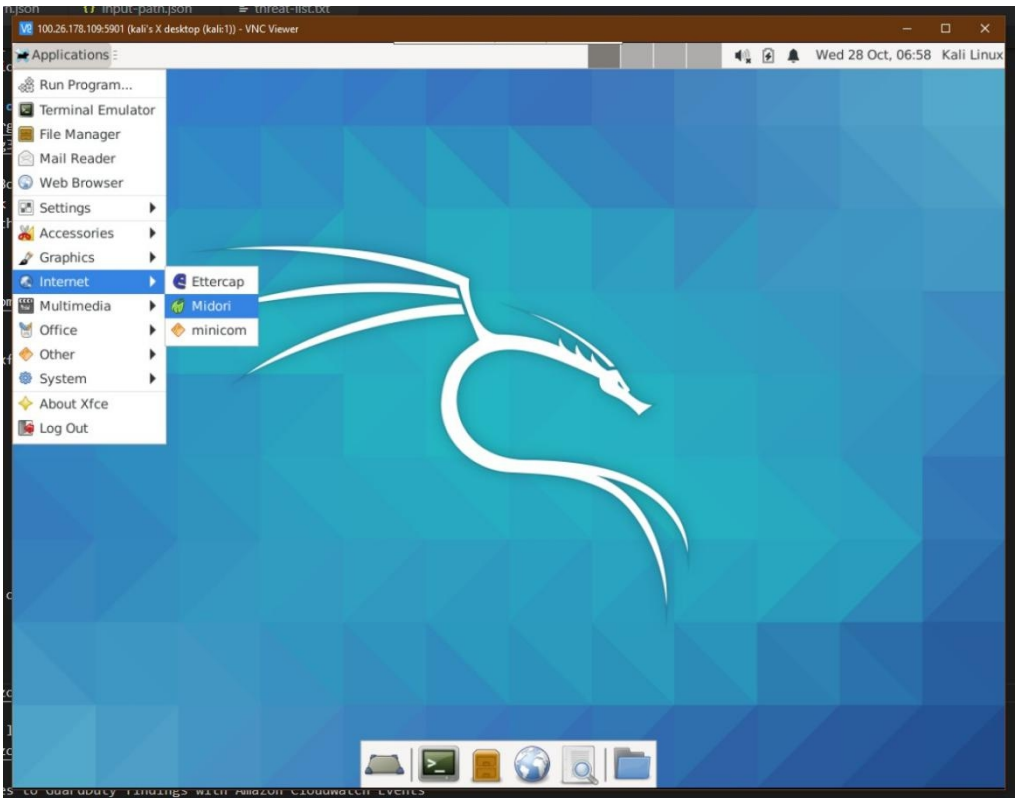
Step 42: When prompted with a warning on Unencrypted connection, select **Don't warn** …. and click on **Continue**.



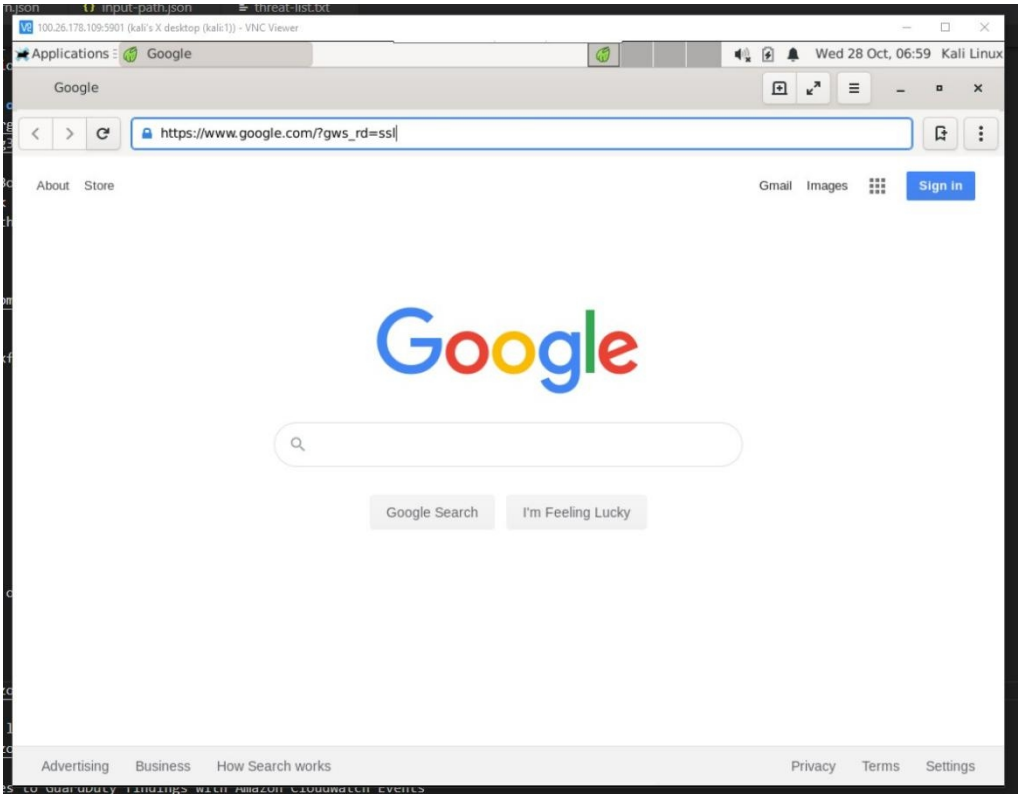
Step 43: Enter the password as **kali123**, select **Remember password** and click on **OK**.



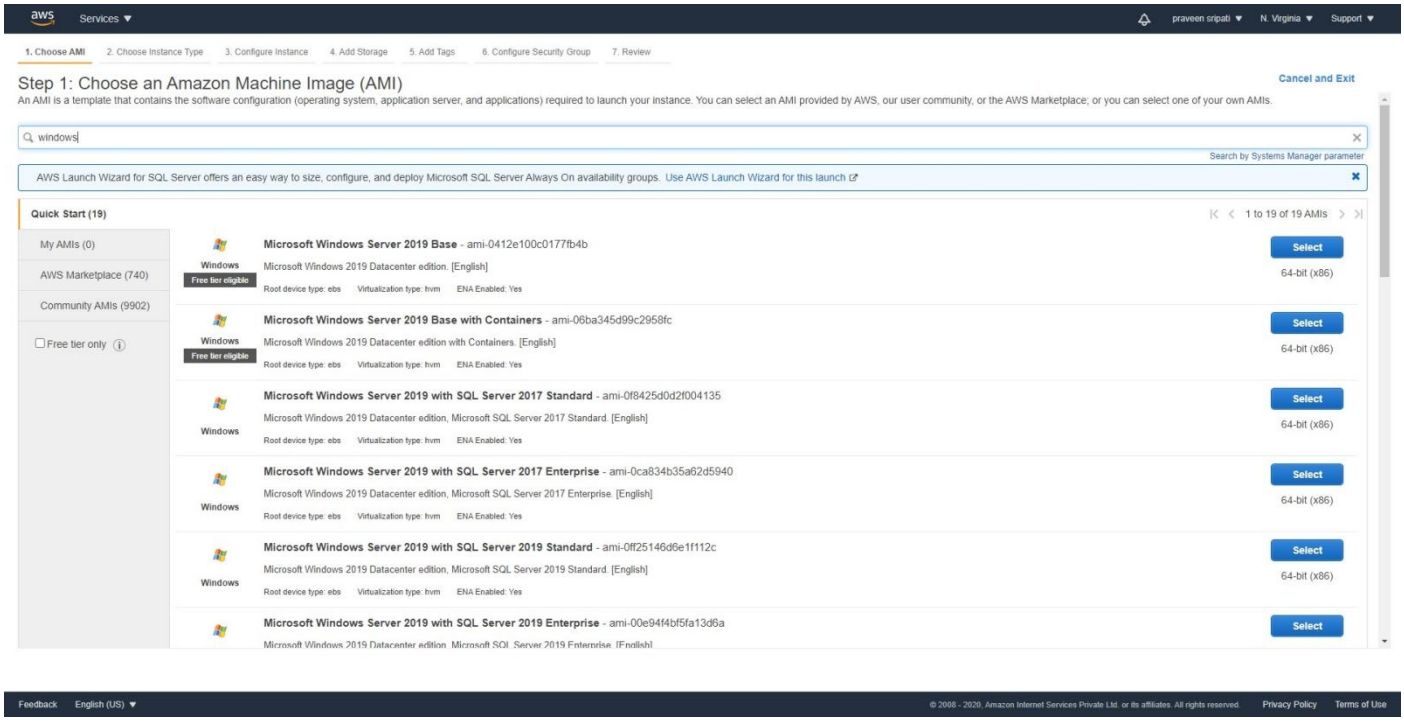
Step 44: The Kali Linux GUI will be displayed, as shown below. Navigate to Applications -> Internet -> Modori as shown below and start the browser.



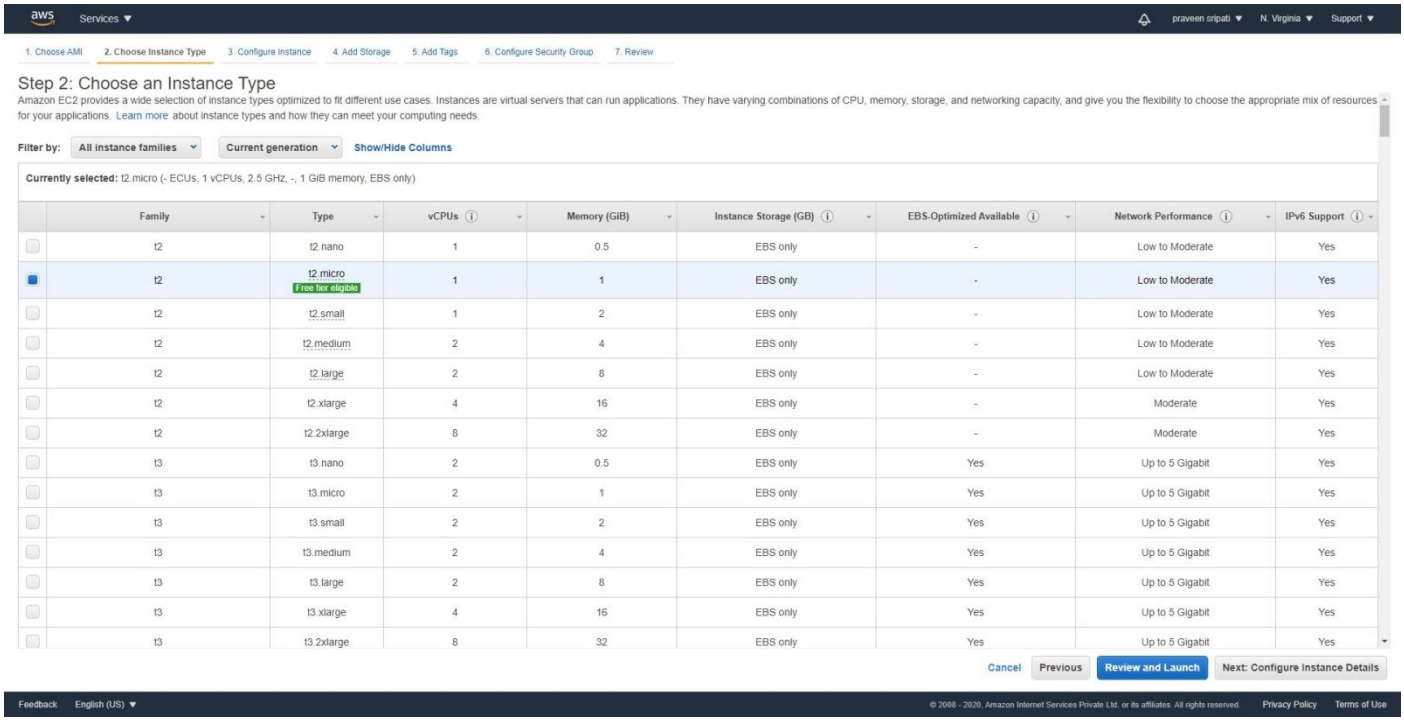
Step 45: Navigate to google.com using the IP we got from one of the previous steps and the one added to the `threat-list.txt` file in S3. It would redirect to the Google page automatically from the IP address, as shown below. This activity also should be triggered as an anomaly by GuardDuty as we have included the Google IP in the threat list for GuardDuty.



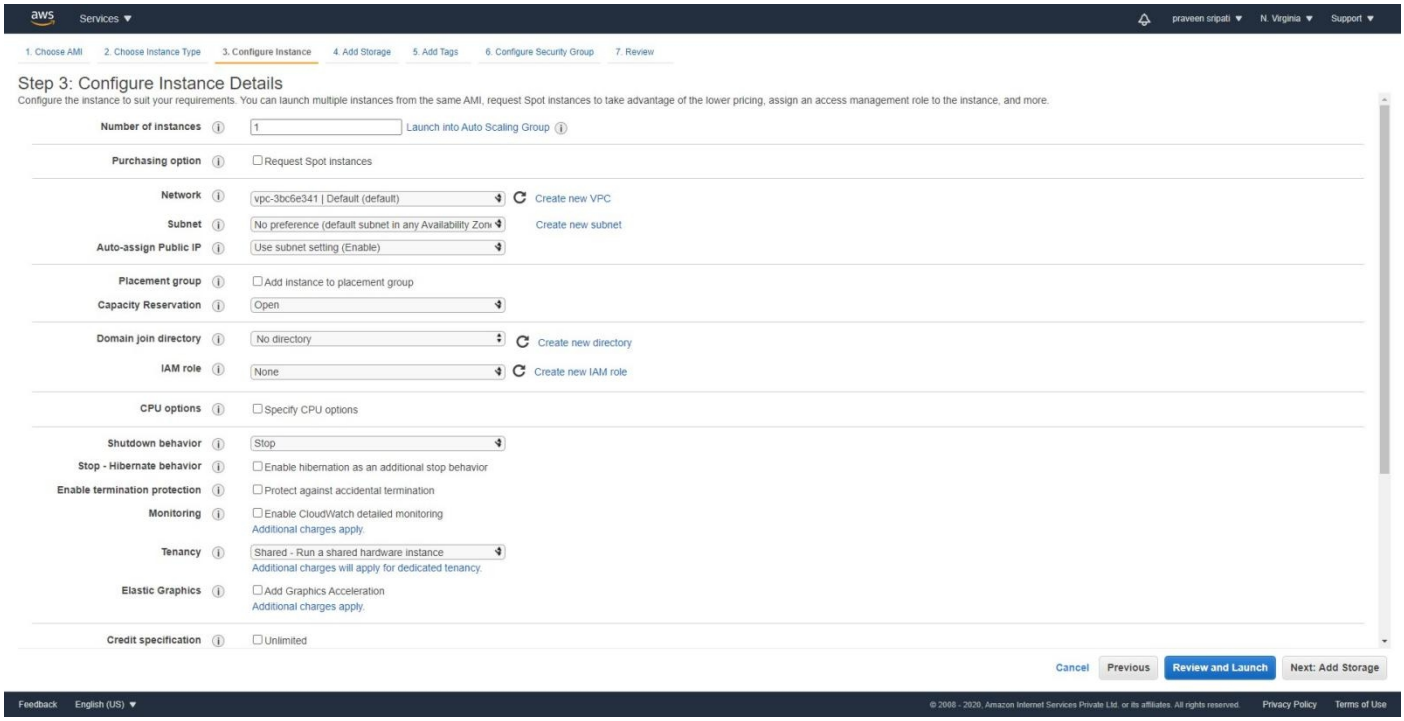
Step 46: From the EC2 Management Console, launch an EC2 instance and select **Microsoft Windows Server 2019 Base**.



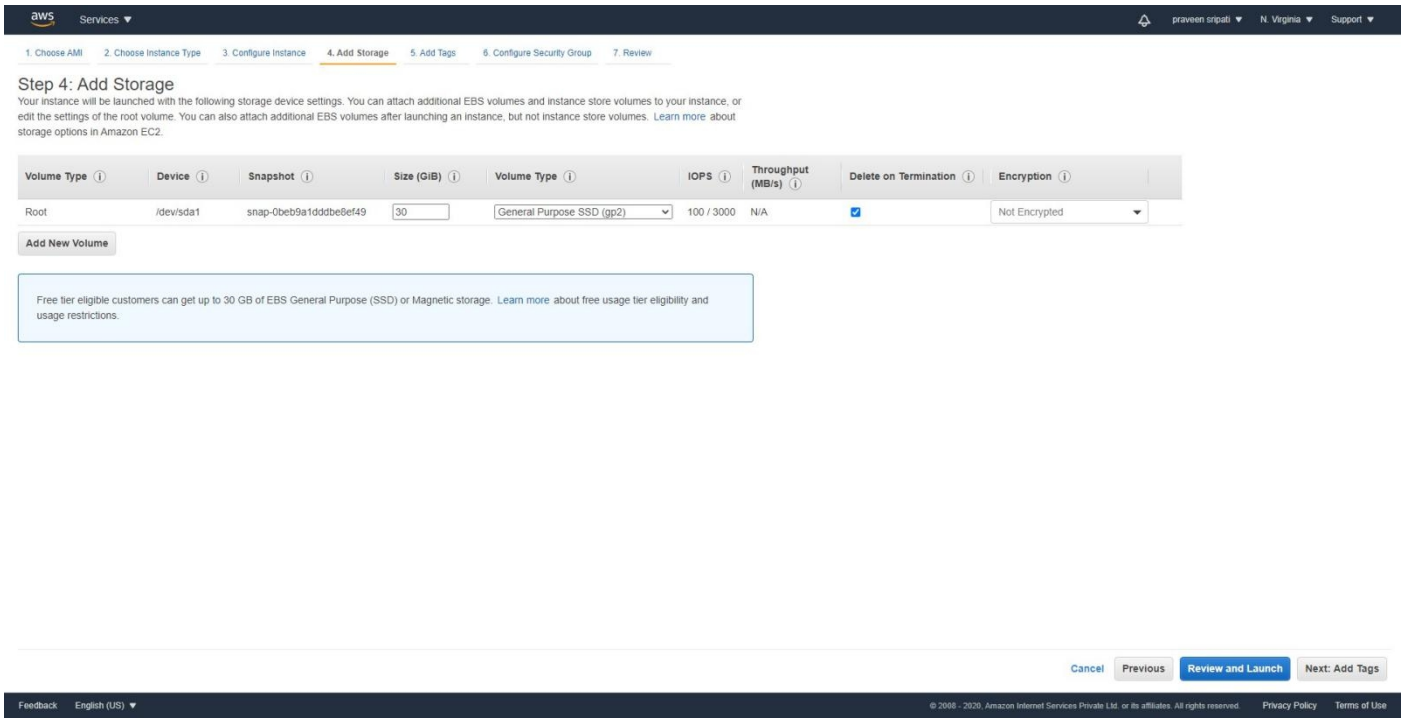
Step 47: Select **t2.micro** and click on **Next**.


aws
Services
praveen sripati
N. Virginia
Support
1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 2: Choose an Instance Type
Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. Learn more about instance types and how they can meet your computing needs.
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)
Family
Type
vCPUs
Memory (GiB)
Instance Storage (GB)
EBS-Optimized Available
Network Performance
IPv6 Support
t2 t2.nano 1 0.5 EBS only - Low to Moderate Yes
t2 t2.micro Free tier eligible 1 1 EBS only - Low to Moderate Yes
t2 t2.small 1 2 EBS only - Low to Moderate Yes
t2 t2.medium 2 4 EBS only - Low to Moderate Yes
t2 t2.large 2 8 EBS only - Low to Moderate Yes
t2 t2.xlarge 4 16 EBS only - Moderate Yes
t2 t2.2xlarge 8 32 EBS only - Moderate Yes
t3 t3.nano 2 0.5 EBS only Yes Up to 5 Gigabit Yes
t3 t3.micro 2 1 EBS only Yes Up to 5 Gigabit Yes
t3 t3.small 2 2 EBS only Yes Up to 5 Gigabit Yes
t3 t3.medium 2 4 EBS only Yes Up to 5 Gigabit Yes
t3 t3.large 2 8 EBS only Yes Up to 5 Gigabit Yes
t3 t3.xlarge 4 16 EBS only Yes Up to 5 Gigabit Yes
t3 t3.2xlarge 8 32 EBS only Yes Up to 5 Gigabit Yes
Cancel
Previous
Review and Launch
Next: Configure Instance Details
Feedback
English (US)
© 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

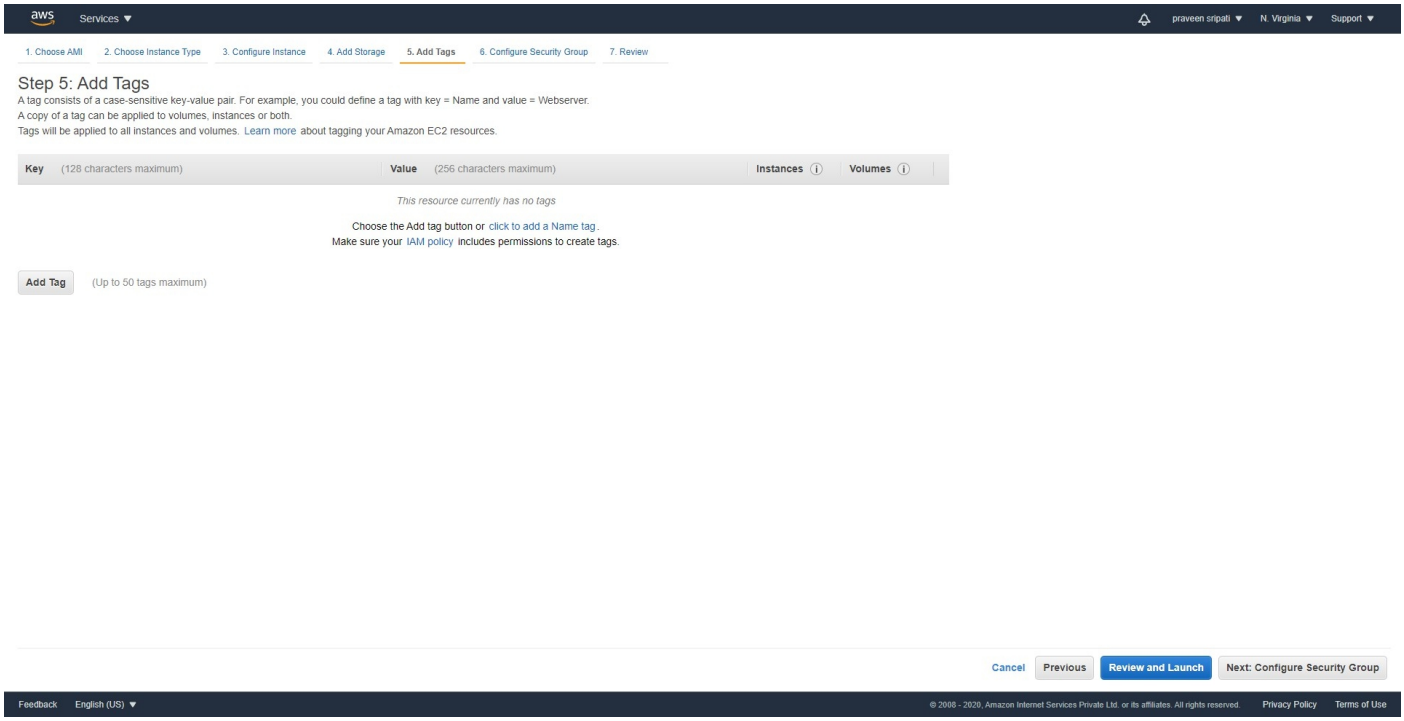
Step 48: Go with all the default options and click on **Next**.



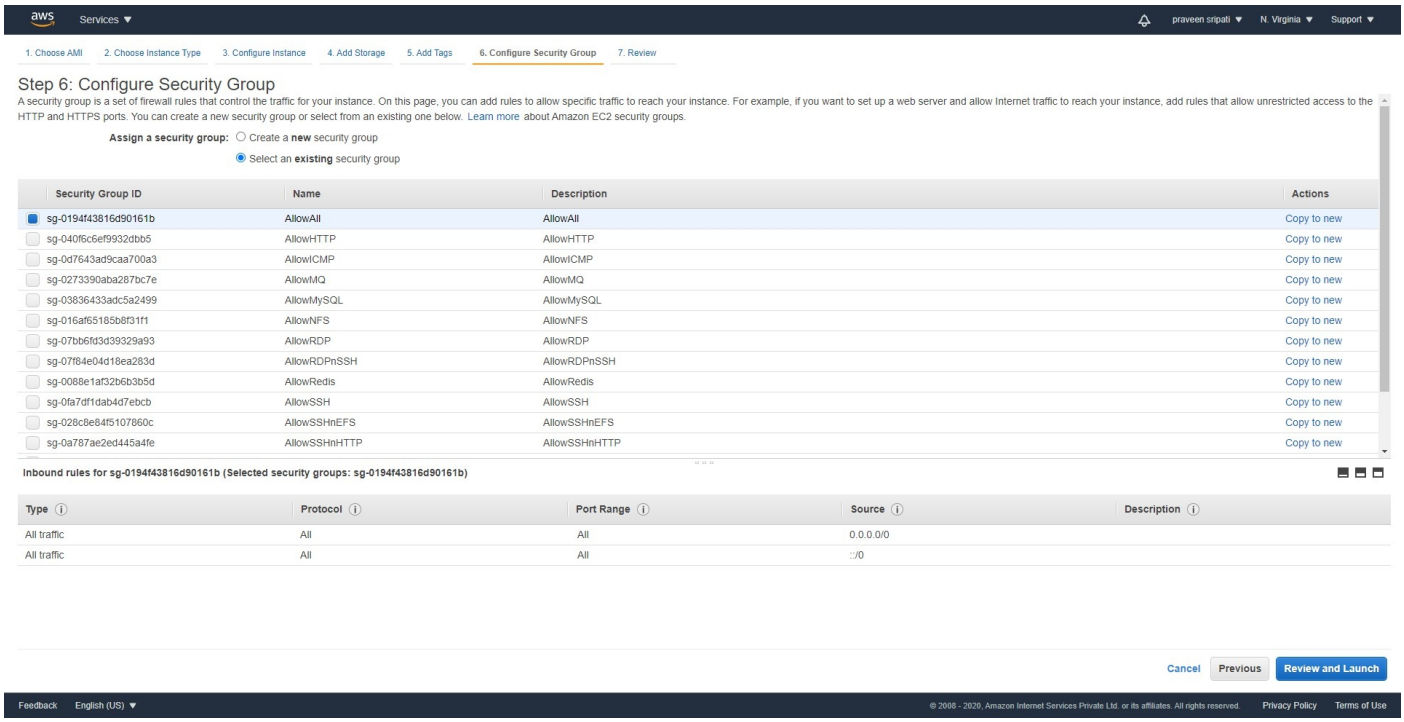
Step 49: Go with the default storage and click on **Next**.



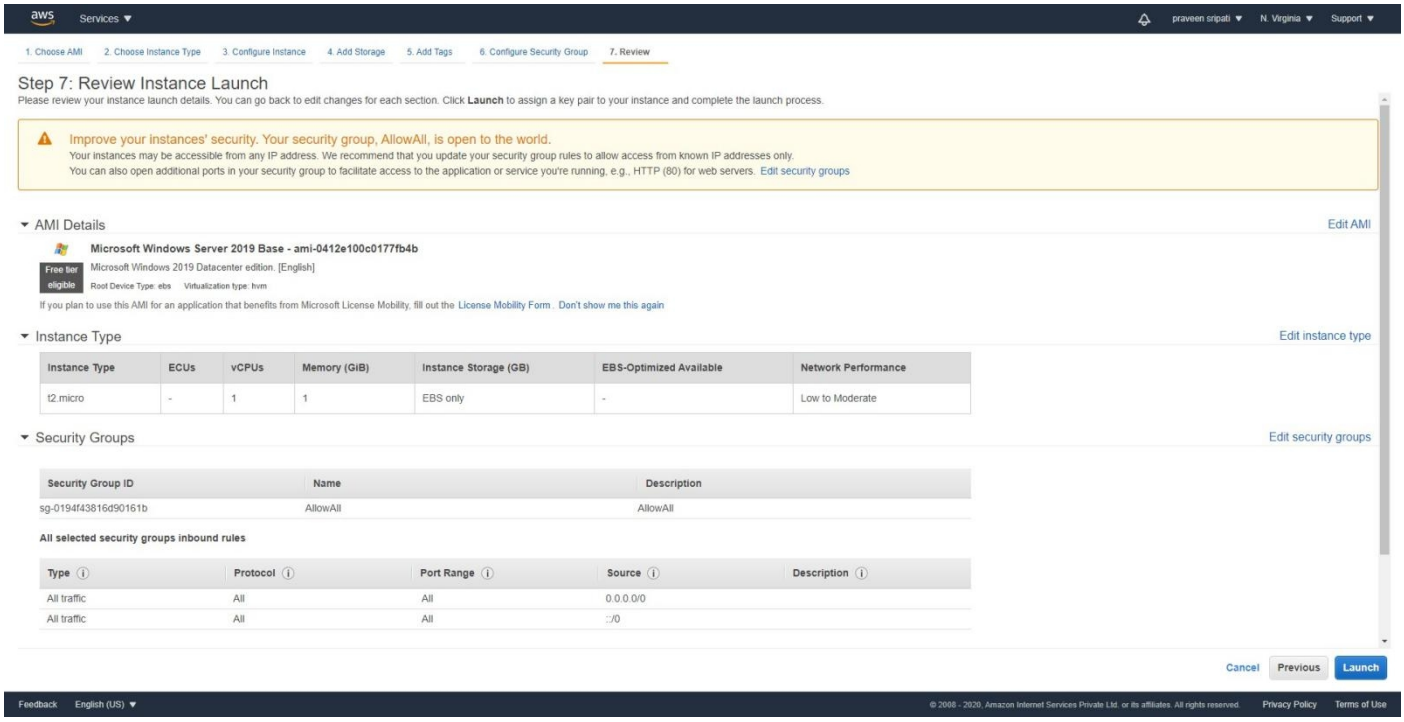
Step 50: Tags are optional. Click on **Next**.



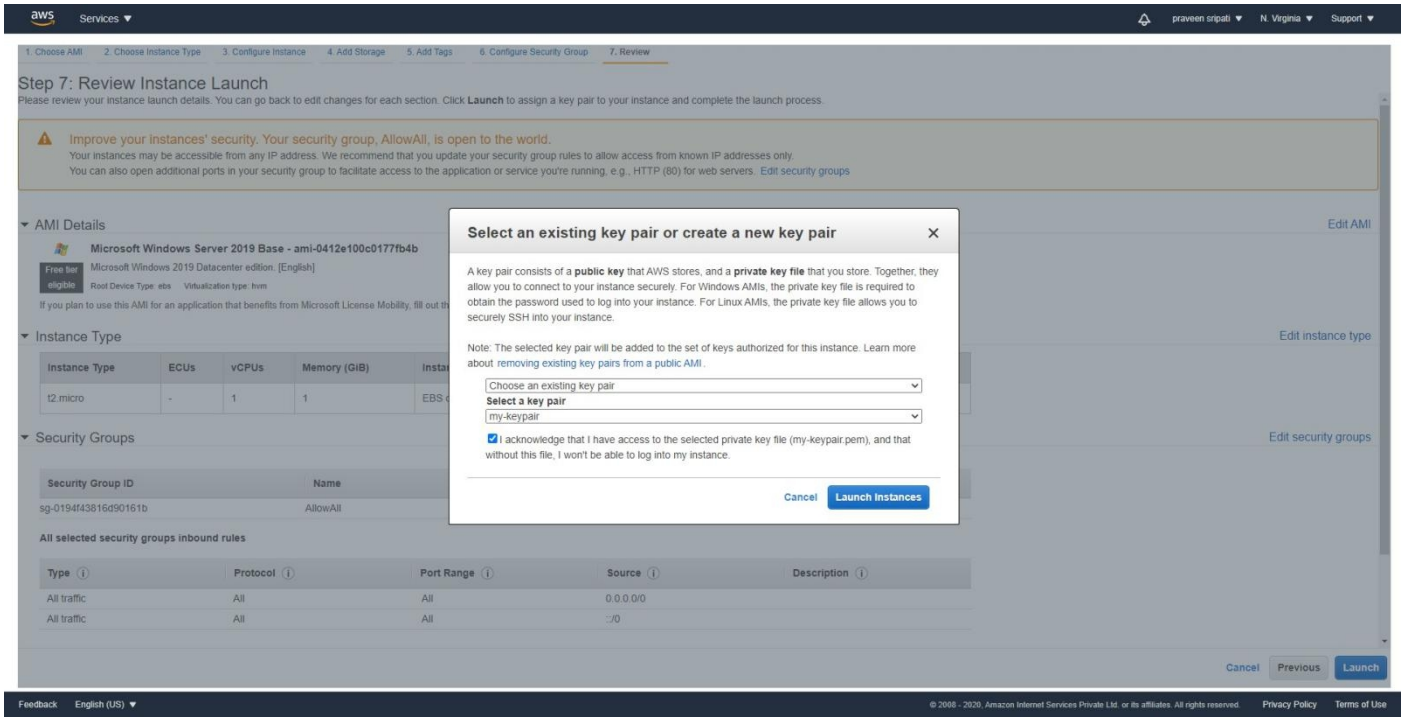
Step 51: Select the Security Group created in one of the previous steps. Then, click on **Next**.



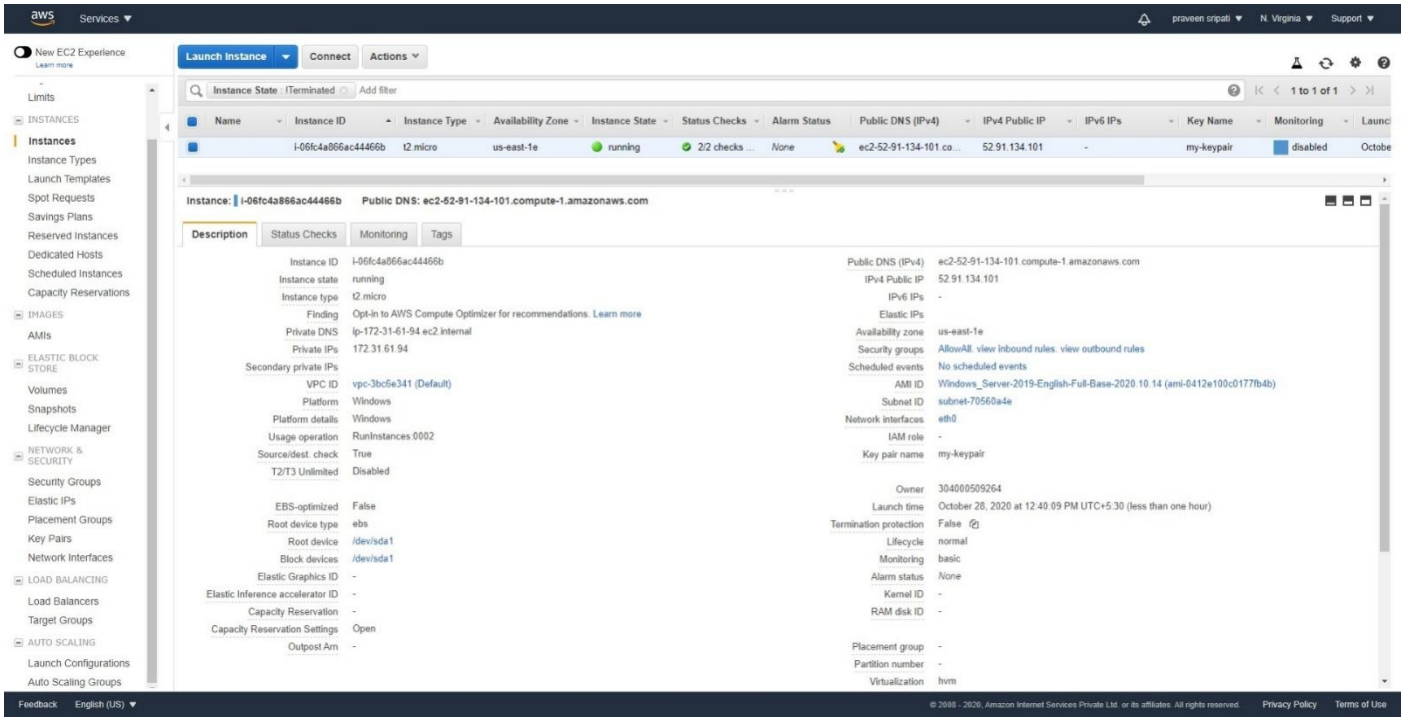
Step 52: Review all the details and click on **Launch**.



Step 53: Select the KeyPair, select **I acknowledge ….** and click on **Launch Instances**.



Step 54: In a few minutes, the EC2 would be in a **running** state.



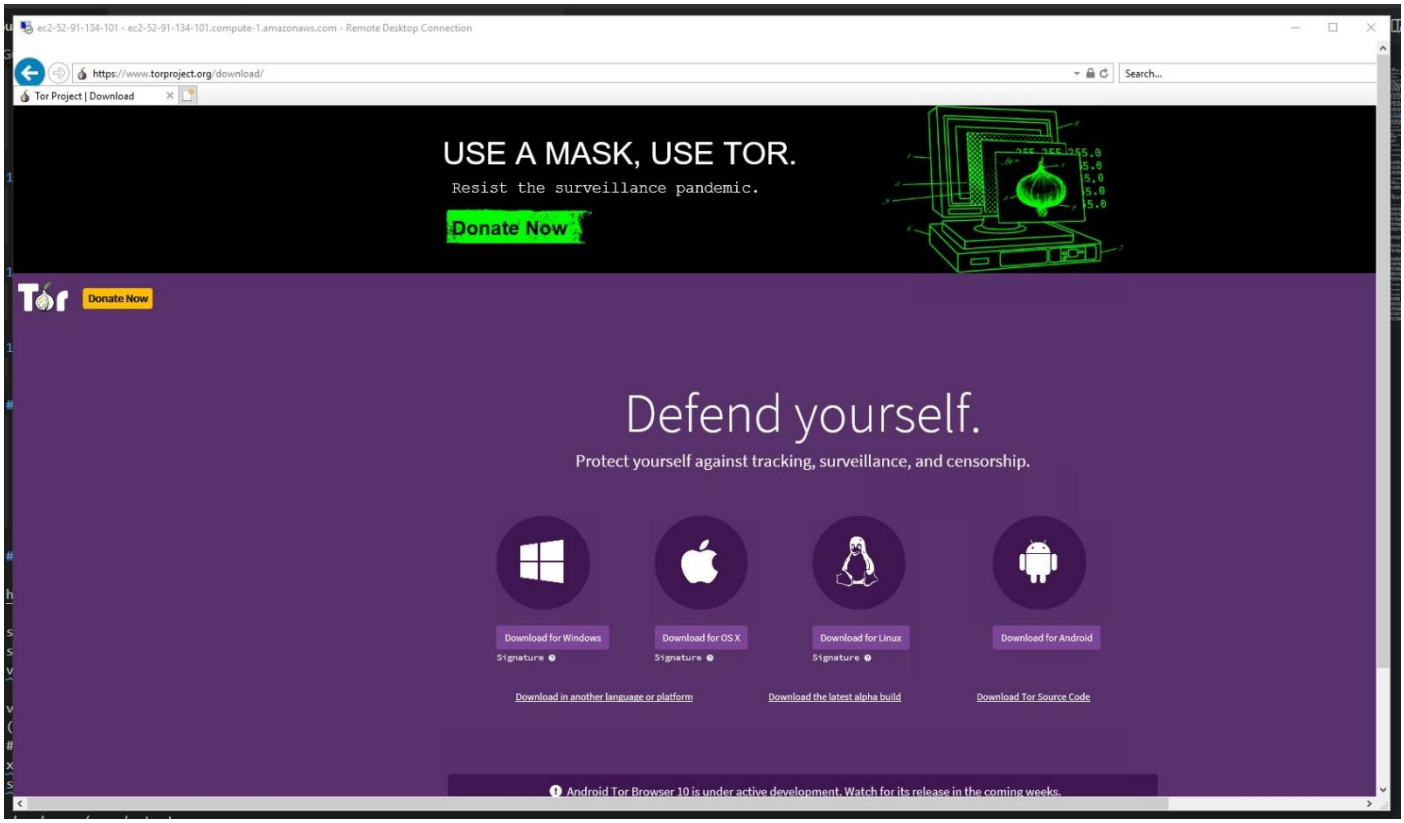
Step 55: Connect to the EC2 instance using the RDP protocol.

Step 56: Inside the EC2 instance, perform the below steps, which allows the software to be downloaded by IE.

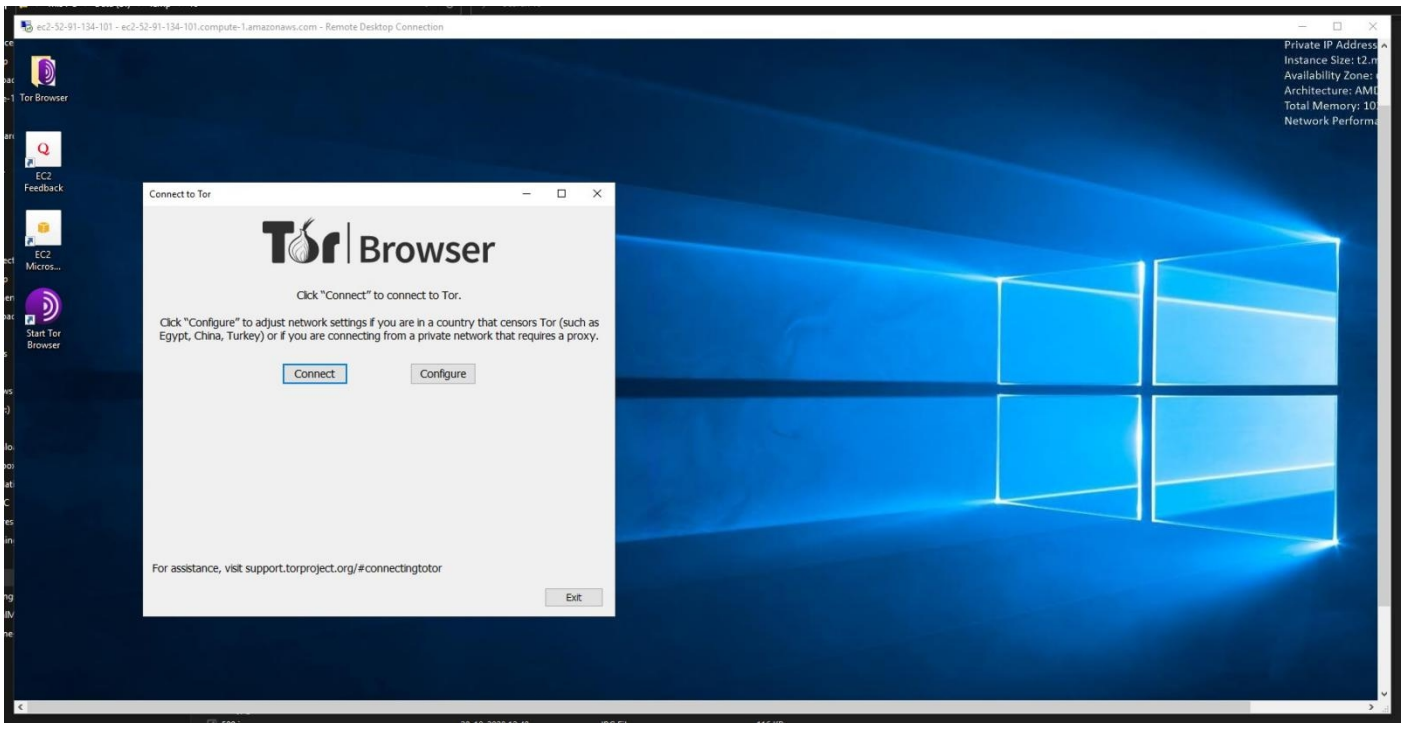
Go to Start > Server Manager > Local Server
Click on the link to the right of IE Enhanced Security Configuration
Navigate to the Administrators and Users section and Click on **OK**

Step 57: Download the Tor browser for Windows from the below URL and install it like any other application.

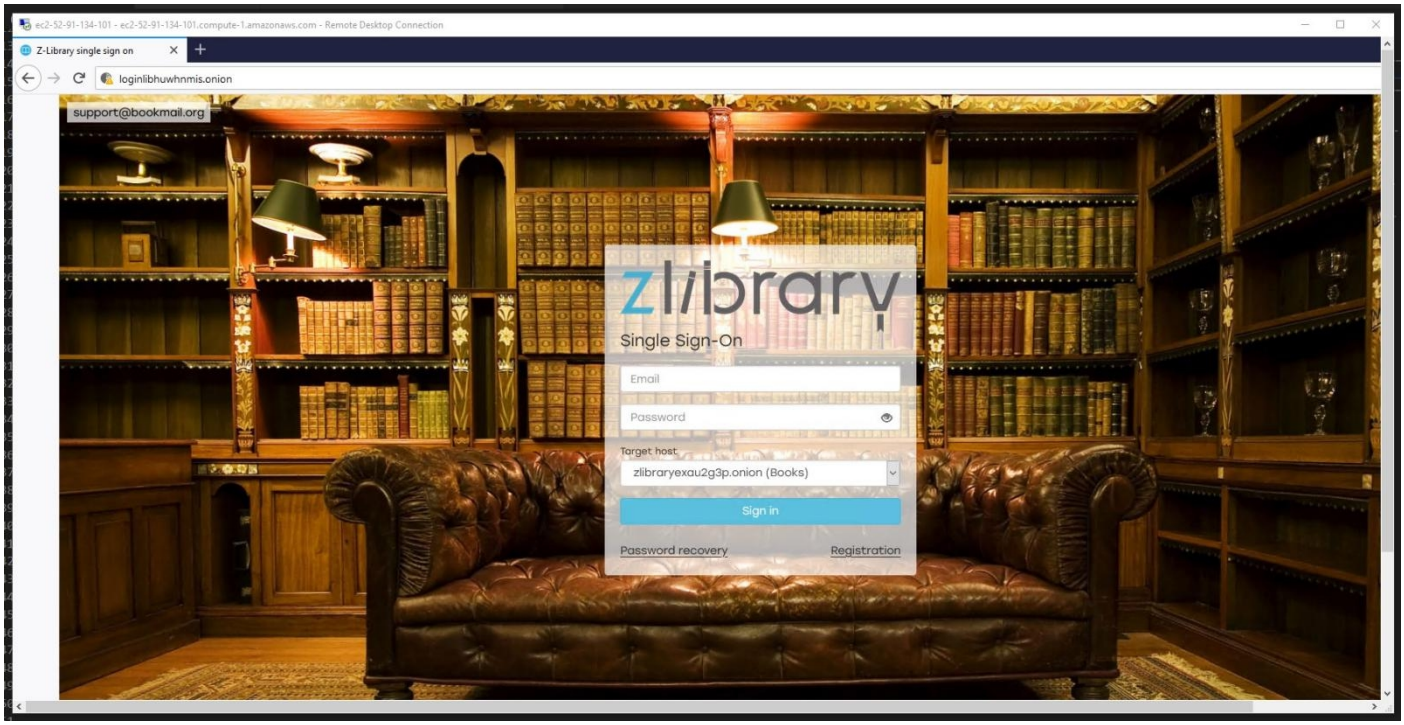
https://torproject.org/download



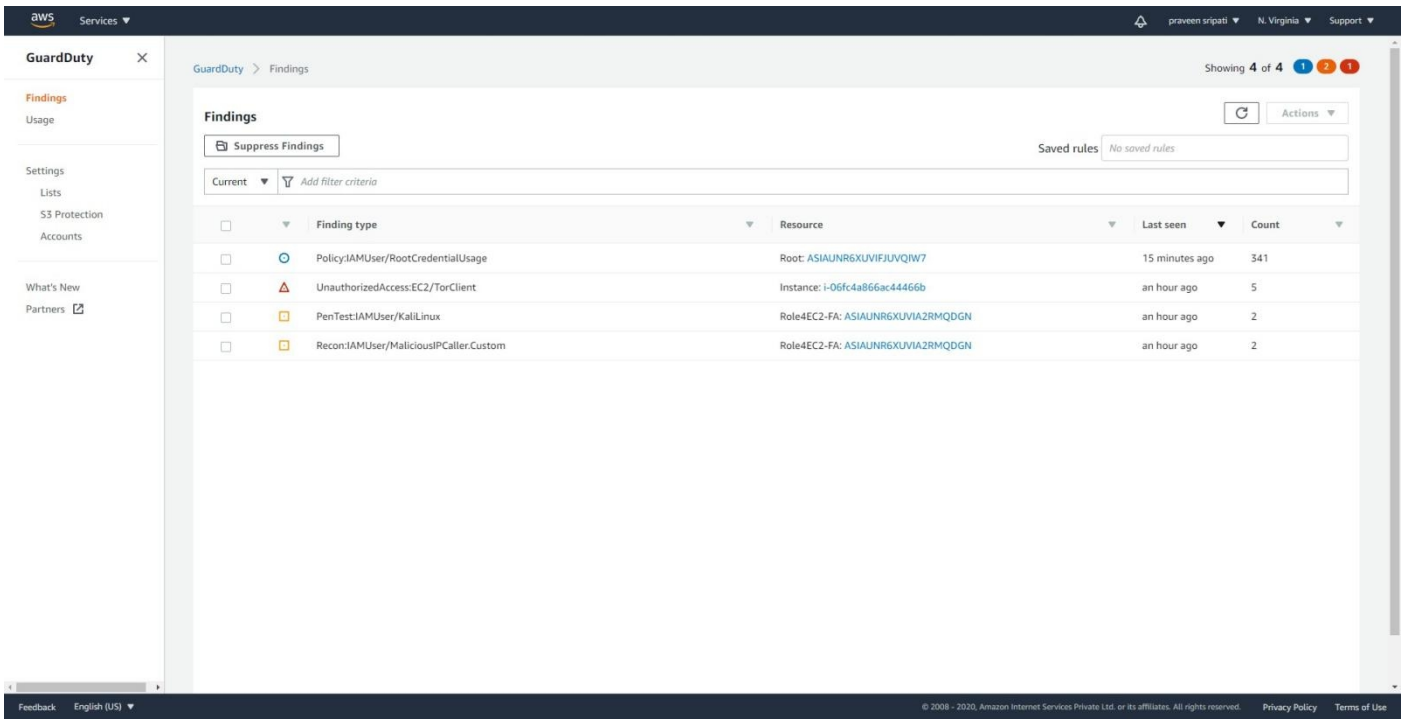
Step 58: Once the Tor browser has been installed, there would be an icon on the Desktop, as shown below. Use it to start the Tor browser. Click on the **Connect** button.



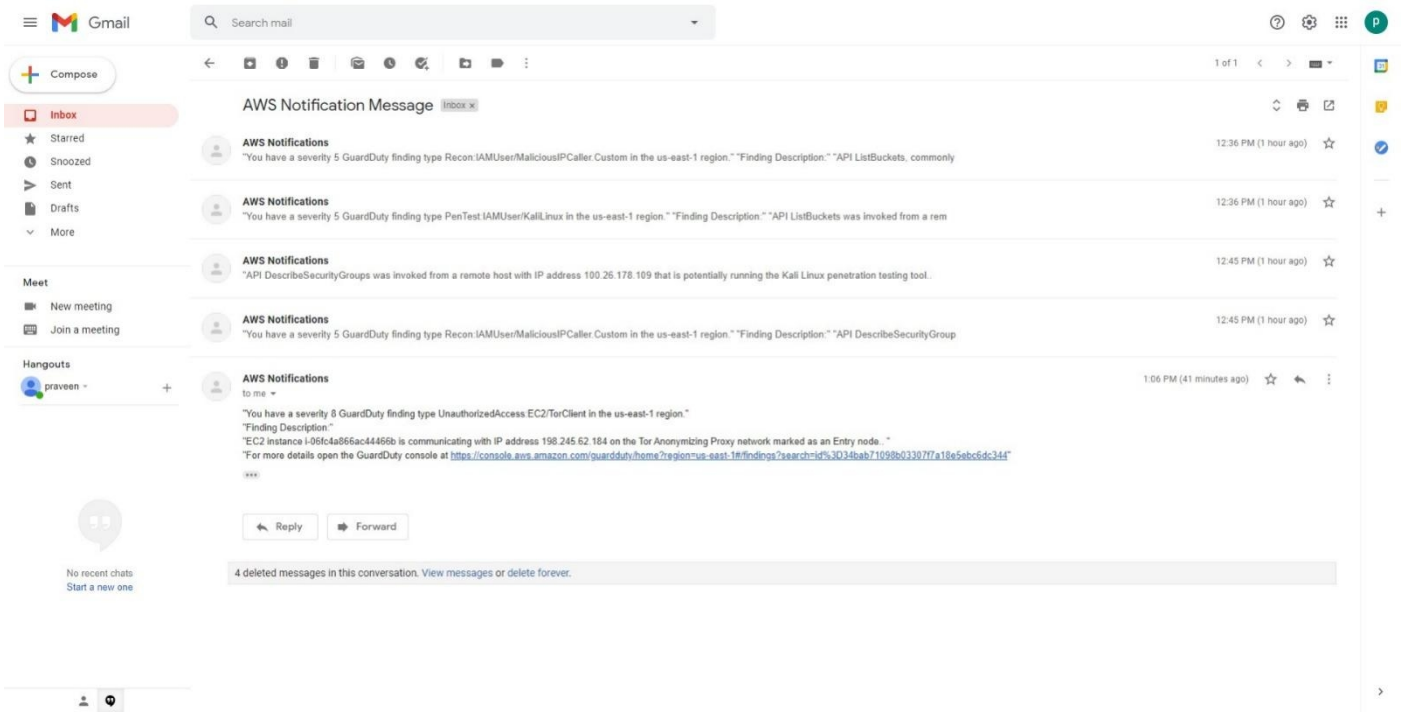
Step 59: In a few seconds, the Tor browser opens in the EC2 instance. Navigate to any onion site. Maybe to http://zlibraryexau2g3p.onion in the Tor browser. This should also trigger an anomaly in the GuardDuty as we are visiting a Tor site.



Step 60: Go back to the GuardDuty Management Console and you will find a bunch of findings. GuardDuty displays these findings as anomalies in different activities we performed.



Step 61: We will also get an email as shown below, since we have integrated GuardDuty events with SNS Notifications via the CloudWatch Rules.



Conclusion:

In this use case, we tried to perform a few actions which are typically performed by hackers

- Use Kali Linux to probe AWS resources
- Use Root IAM role to perform AWS activities
- Use a TOR Client on an EC2 instance
- Used a browser to reach a malicious IP address

In the above steps, we observed that the suspicious activities were immediately identified by GuardDuty as anomalies, and an email alert was also sent via SNS Topic.