Configuration Manual

MSc Industrial Internship
Msc. Cybersecurity

Oluwasefunmi Alabi
Student ID: x21130094

School of Computing
National College of Ireland

Supervisor: Vikas Shani

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	OLUWASEFUNMI MOYINOLUWA ALABI		
Student ID:	X21130094		
Programme:	MSc CYBERSECURITY	**Year:**	2022
Module:	MSc INTERNSHIP		
Supervisor:	VIKAS SHANI		
Submission Due Date:	6TH JANUARY, 2023		
Project Title:	THE HYPERAUTOMATION OF SOFTWARE SECURITY PATCH MANAGEMENT IN ENTERPRISE NETWORKS: A CASE STUDY AT THE CENTRAL BANK OF IRELAND.		
Word Count:	2202	**Page Count** 28	

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: OLUWASEFUNMI MOYINOLUWA ALABI

Date: 5TH JANUARY, 2023

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	☐
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	☐
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	☐

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Oluwasefunmi Alabi
Student ID: x21130094

Use Case: As an administrator of an IT tenant consisting of a large number of EC2 instances that must be patched on a continuous basis. Rather than waste labour hours manually patching each instance, organizations should automate and hyperautomate already automated processes with AWS Systems Manager.

1.1 Systems Manager

Systems Manager (SSM) provides visibility and control over any AWS infrastructure. SSM allows you to manage inventories by grouping resources together by software or environment, as well as integrate with CloudWatch to monitor analytics and operational data. SSM helps automate operational operations such as executing pre-defined commands on one or more EC2 instances, altering the instance state, attaching/detaching EBS volumes, making snapshots, and deploying patches and upgrades to increase efficiency. In this project the focus is on how to automatically patch several EC2 instances.

1.2 Create VPC

A basic VPC in a single AZ with a public and private subnet should be established for this project. For protection, install servers in a private subnet and an AWS bastion server in the public network. This design will allow the administrator to interface with the servers while without exposing them to the outside world.

a. Go to **VPC** Services > VPC > Your VPCs.

b. Give your VPC a name.

c. Select a CIDR block. Recopmmended to chose 10.0.0.0/16, which gives far more IP addresses than needed.

d. The remaining defaults are acceptable. Select Create VPC.

1.3 Create Subnets

a. Select Subnets from the browser's left sidebar.

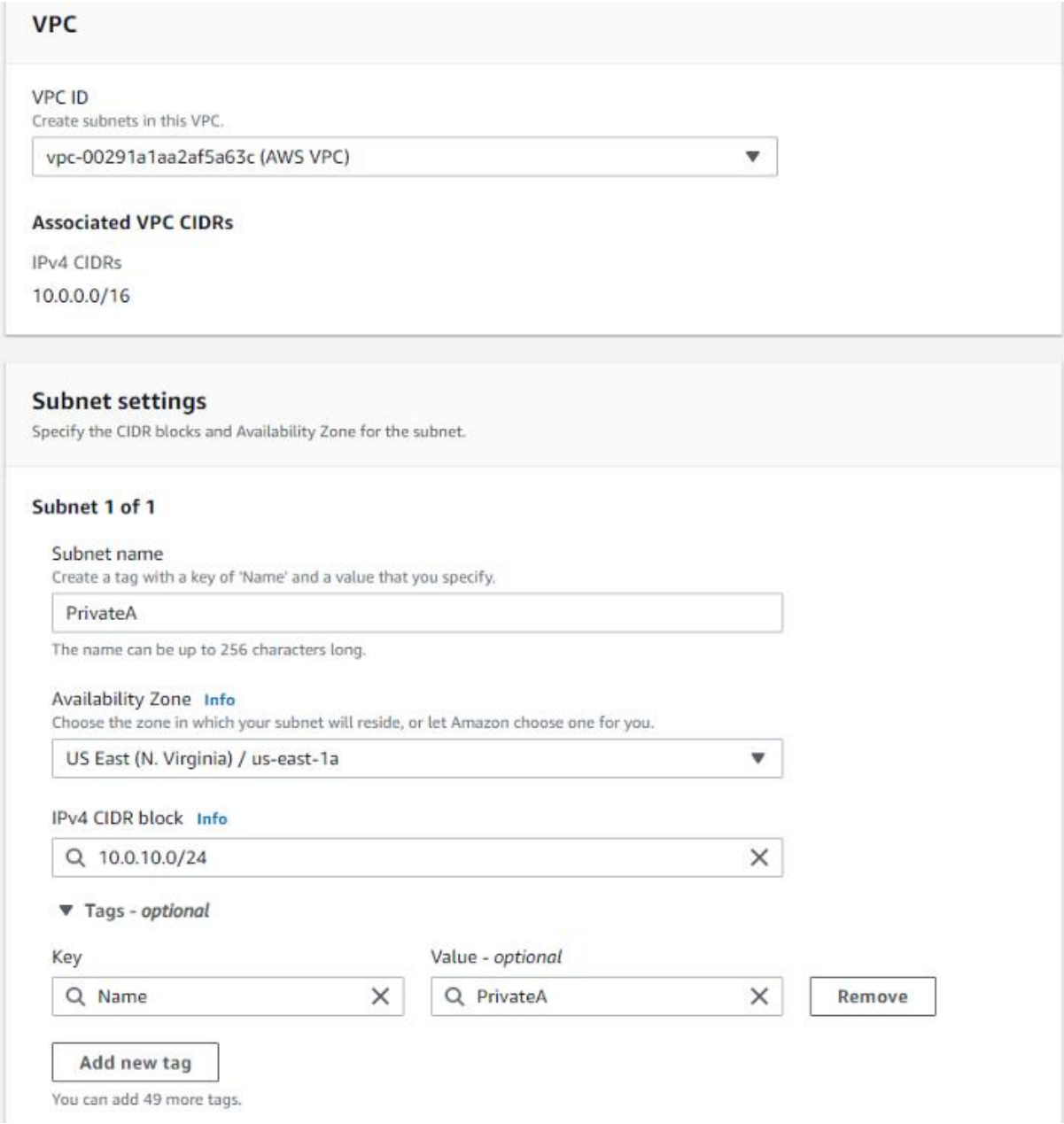
b. Select Create subnet.

c. Select the VPC you just established as the VPC ID. This is why, when you construct your VPC, you should give it a name tag so that it can be easily identified.

d. PrivateA is the name of the subnet.

e. Zone of availability: us-east-1a IPv4 CIDR block: 10.0.10.0/24

f. Select Create Subnet.



Create a public subnet now. Click the Create Subnet button.

g. Fill in the blanks with the following information:

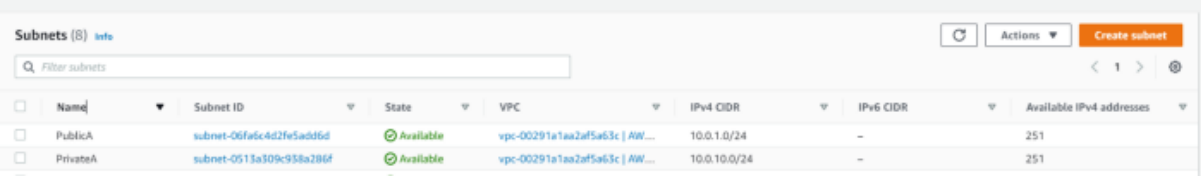
   VPC ID: Choose your VPC

   Name of the subnet: PublicA

   Zone of Availability: us-east-1a

   10.0.1.0/24 IPv4 CIDR block

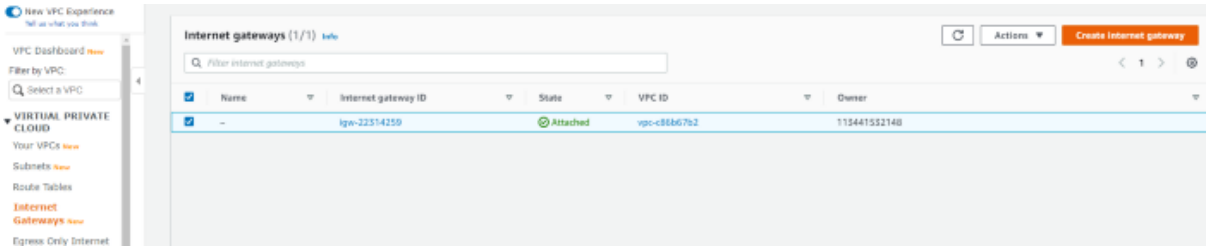
h. Your VPC should now have two subnets linked with it.



1.4 Create Internet Gateway

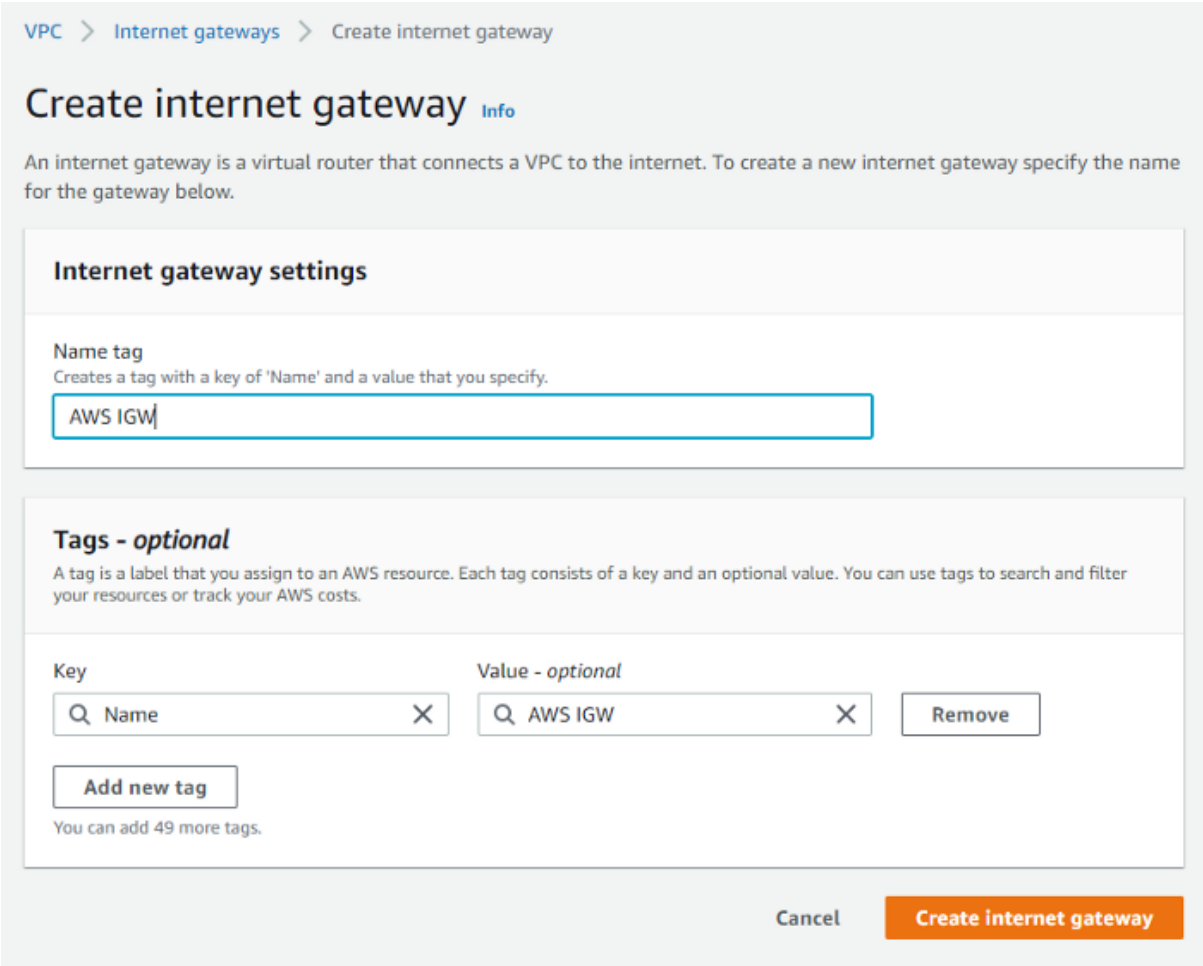
To make our public subnet available to the internet, an internet gateway would be built.

a. Select Internet Gateways from the Virtual Private Cloud menu.
b. Select Create Internet Gateway from the drop-down menu.



c. AWS IGW is the Name Tag chosen

d. Click the Create Internet gateway button**.**



e. Click **Actions** button and select **Attach to VPC**.

f. Select your VPC and click **Attach internet gateway**.

g. Attach your VPC after selecting it.

1.5 Create NAT gateway

The NAT gateway will permit the private servers access to connect to the internet in order to get updates and fixes.

a. Navigate to Virtual Private Cloud > NAT Gateways.

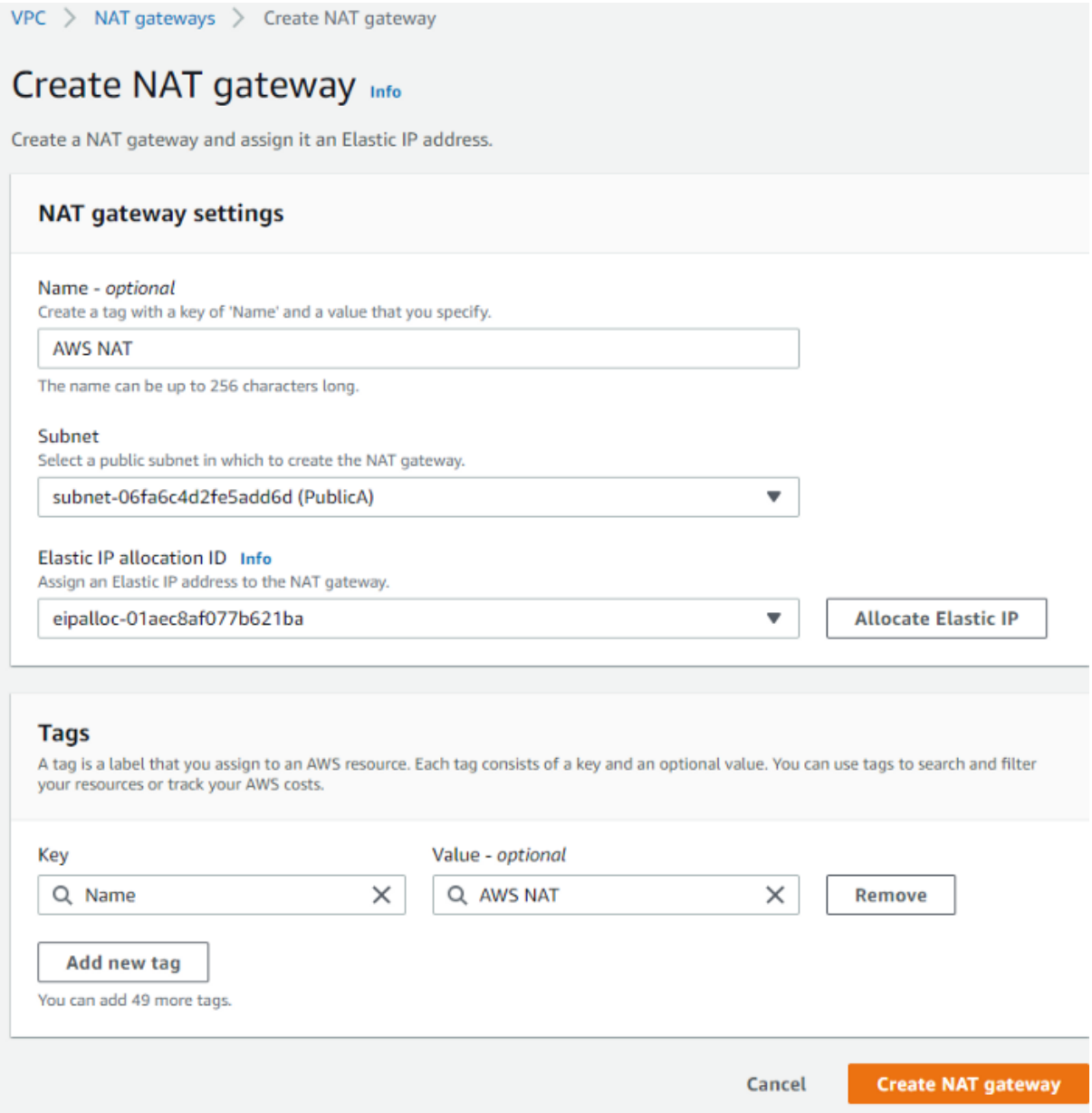
b. Select Create NAT gateway from the drop-down menu.

c. Give your NAT gateway a name.

d. Choose your public subnet (PublicA).

e. Select the Allocate Elastic IP option.

f. Select Create NAT gateway from the drop-down menu.



1.6 Configure Public Route Table

Currently, there is only one route table linked with the VPC, which facilitates connectivity across our subnets. Making the default route table public is not a smart idea since all new subnets will be automatically associated with the default, necessitating the creation of a new route table.

a. Navigate to VIRTUAL PRIVATE CLOUD and choose Route Tables.
b. Select Create route table from the drop-down menu.
c. Give your route table a name and choose a VPC. Preferably to make the name obvious, so to generally attach it to the VPC and specify whether it's public or private.

d. Select Create.

e. Select your newly created public route table. Options should show at the bottom of the browser once selected. You may enlarge it by dragging it.
f. Navigate to the Subnet Associations tab.
g. Select Edit subnet associations from the menu.
h. Choose your public subnet and then click Save.
i. Navigate to the Routes tab.
j. Select Edit Routes from the menu.
k. Select the Add route option.
l. 0.0.0.0/0 as the destination

m. Select Internet Gateway as the Target, then your Internet Gateway.

n. Select Save Routes.

NB: Remember to change the auto ip settings now that your public subnet is actually public.

a. Select Subnets from the VIRTUAL PRIVATE CLOUD menu.

b. Determine your public subnet.

c. Select Modify auto-assign IP settings from the Actions menu.

d. Select Enable auto-assignment of public IPv4 addresses and save.

1.7 Configure a Private Route Table

a. Choose the primary route table.

b. Go to the Routes tab and update the routes.

c. Replace Destination: 0.0.0.0/0 with the IP address of your NAT Gateway.

1.8 Create Bastion Security Group

a. Under SECURITY, choose Security Groups.

b. Select Create security group from the drop-down menu.

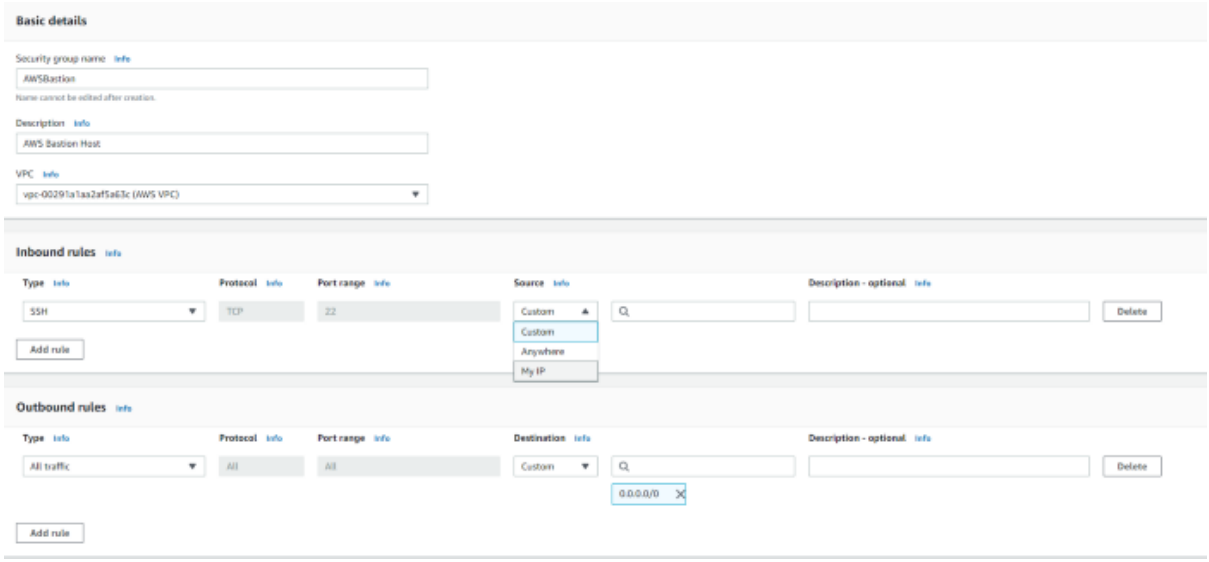
c. Give your security group a name. I picked AWSBastion so that I know which VPC it is affiliated with and what it is used for on my bastion server.

d. Choose your VPC.

e. Click Add rule to add an inbound rule.

f. SSH, My IP as the source. This restricts SSH access to your machine.

g. Select Create security group from the drop-down menu.

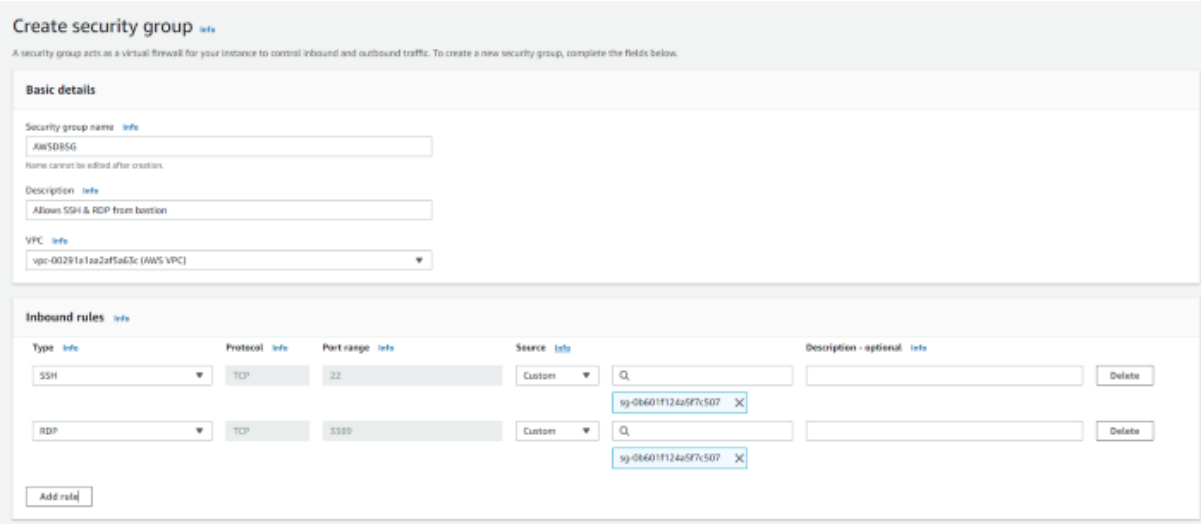


1.9 Create DB Security Group

1. Select Create security group from the drop-down menu.
2. Name of the security group: AWSDBSG

    - VPC: AWS VPC
    - Type: SSH, Source: Custom, and then choose the Bastion Security Group

    - Type: SSH, Source: Custom, and then choose the Bastion Security Group



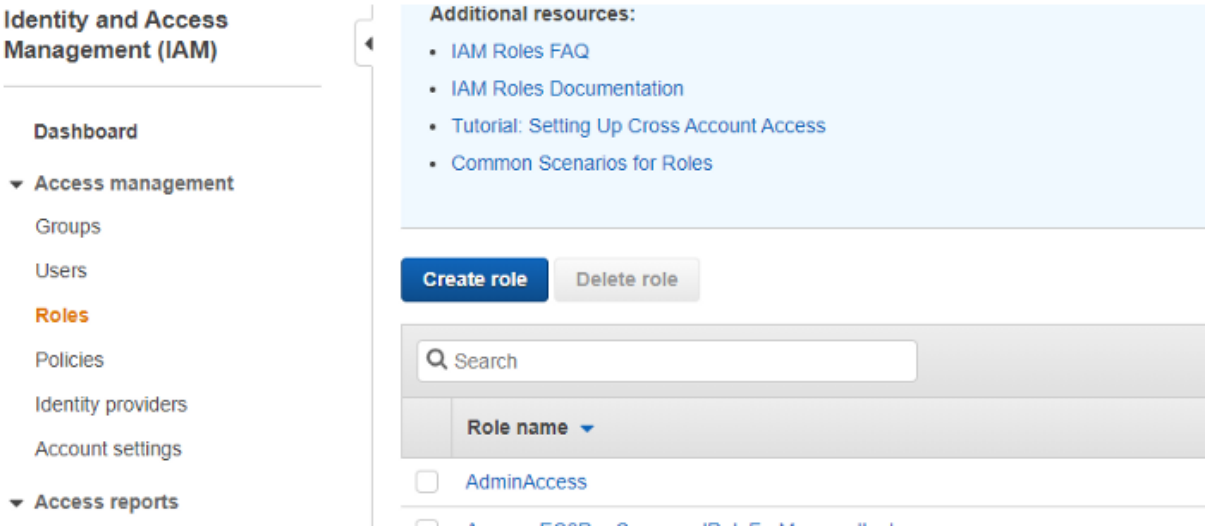
1.10 Create Systems Manager Role

For the EC2 instances to be monitored by Systems Manager, there's the need to define a role.

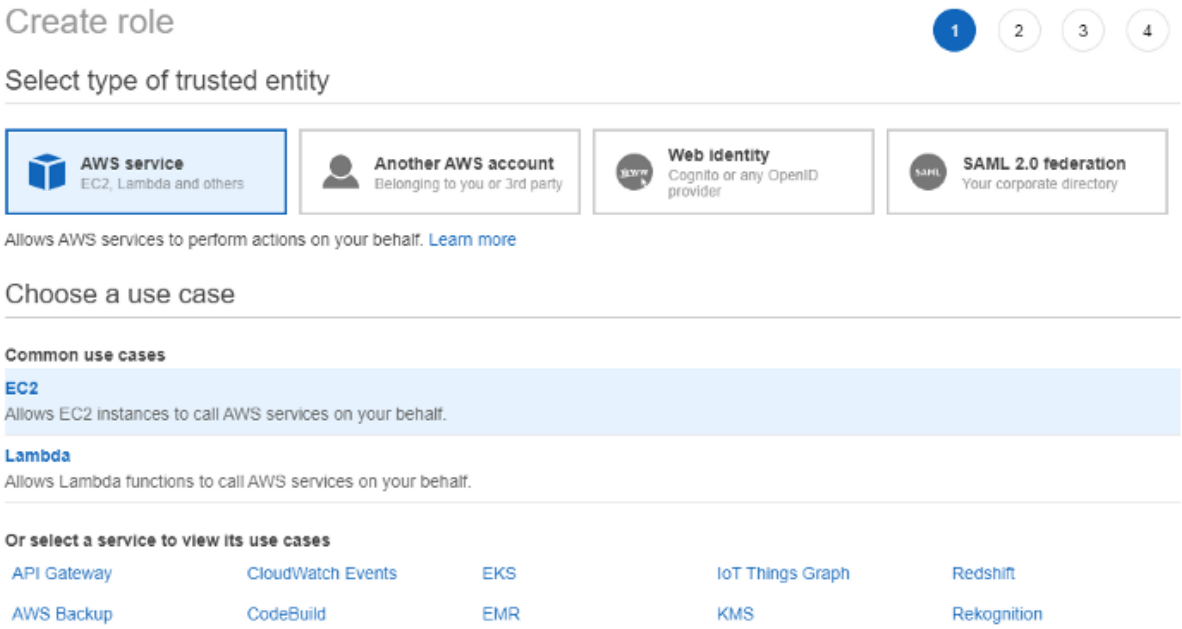
a. Select Identity and Access Management. IAM Services

b. Select Roles from the Access Management menu.

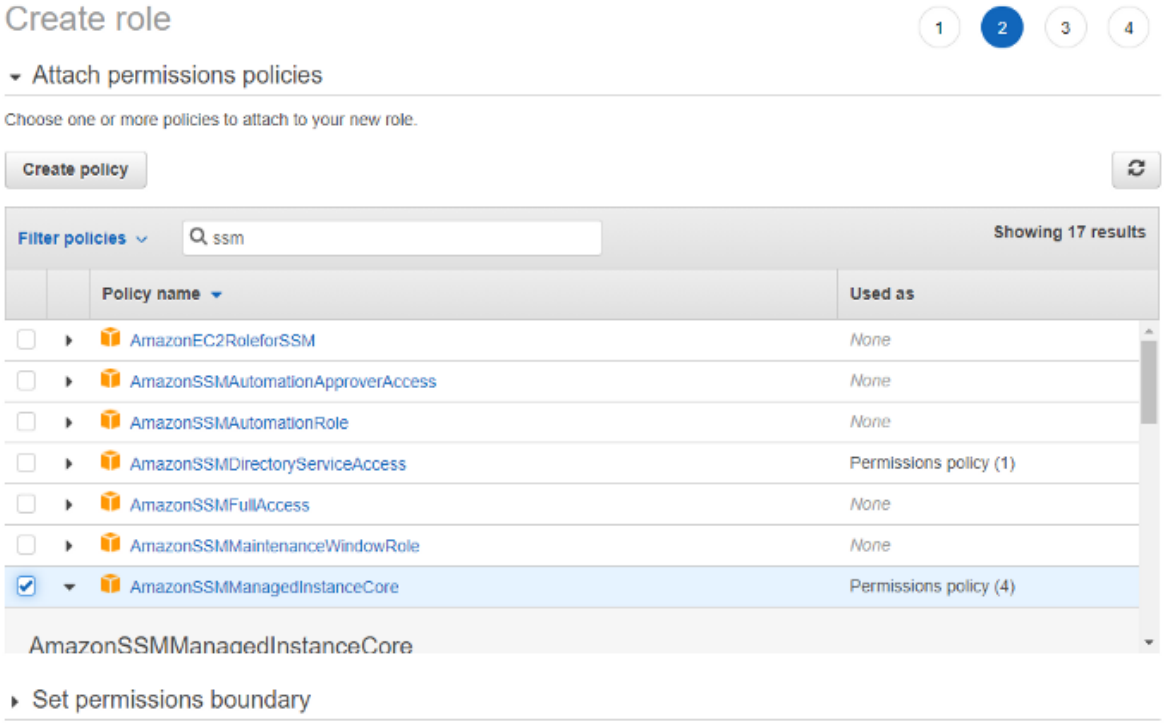
c. Select Create role.



d. Select AWS service, then EC2, and then click Next.



e. Look for and choose AmazonSSMManagedInstanceCore. Next, click.



f. Press the Next button.

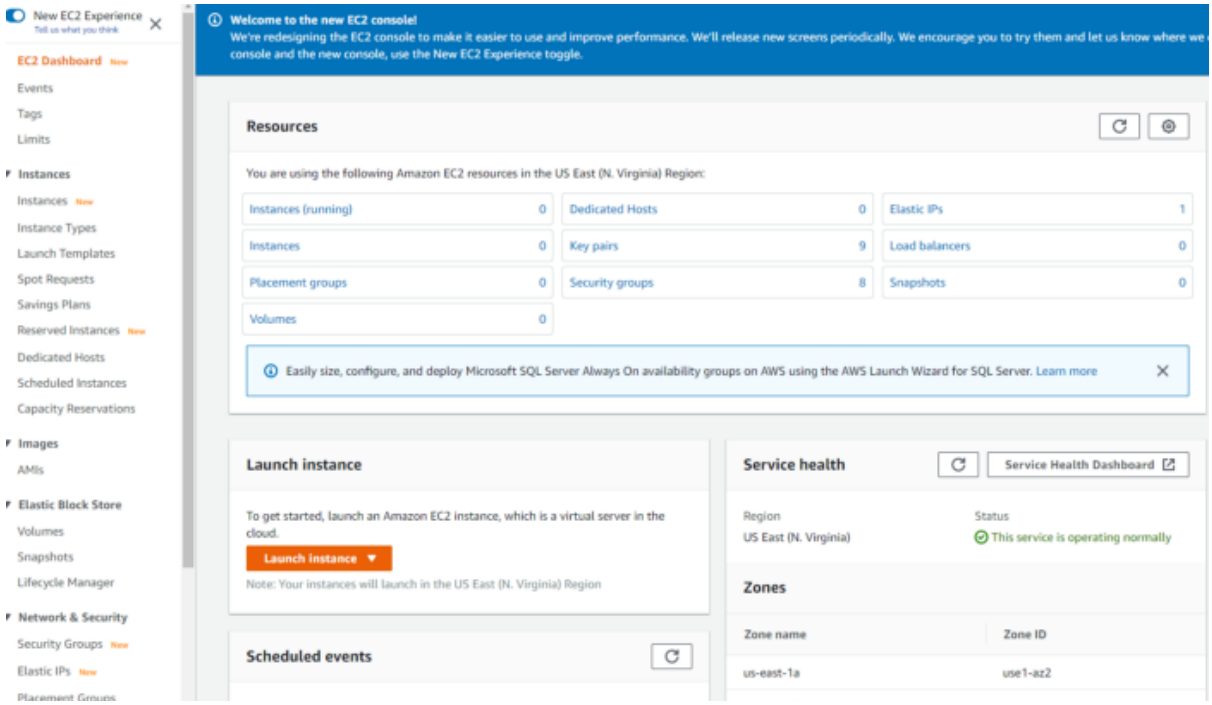
g. Give the role a name and click Create role.

1.11 Creating Bastion Host Instance

First, we'll set up our bastion server in our public subnet. A Bastion Host allows us to interact with the private instances that are not visible to the public. Then set up three instances in our own subnet. One instance of Ubuntu, one instance of Red Hat, and one instance of Windows. One may always add more if desired, but having a range of instances is essential for this project.

a. Go to EC2. Services > EC2

b. Select Launch Instance from the drop-down menu.



c. Choose Amazon Linux 2 AMI. Next, click.

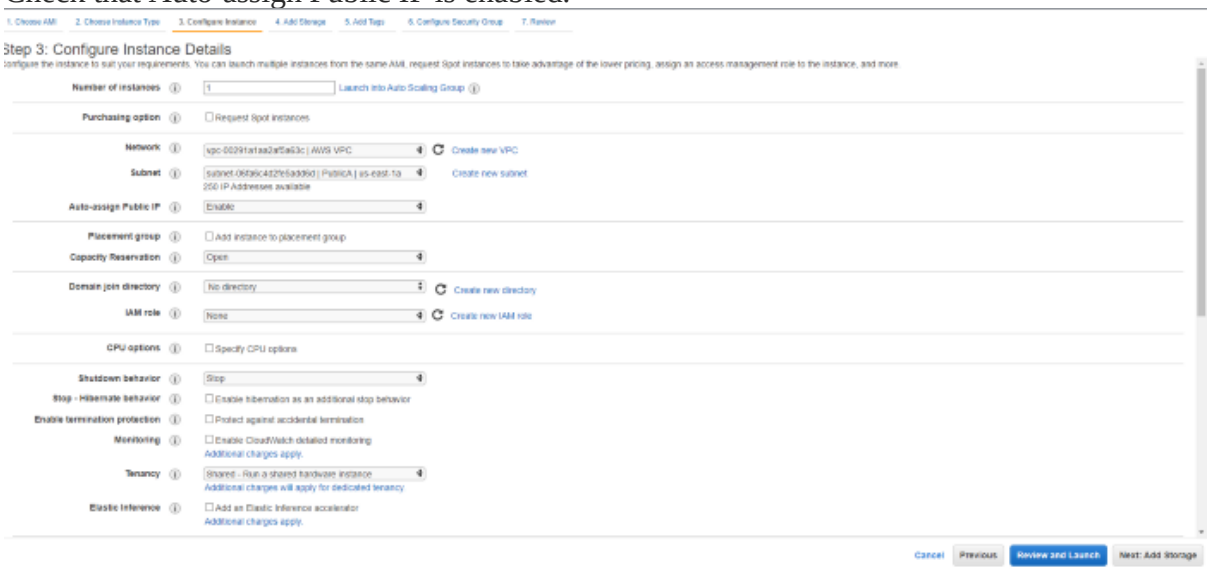
d. Choose t2.micro. Next, click.

e. Select Configure Instance Details from the drop-down menu.

Network: Choose the VPC

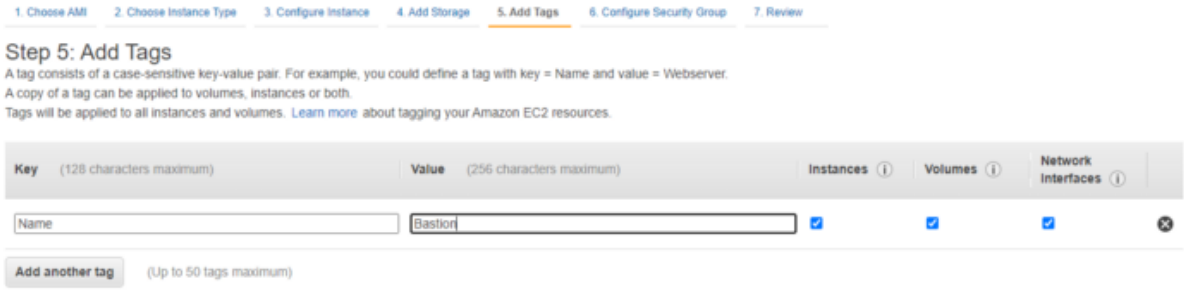
Subnet: Choose the public subnet.

Check that Auto-assign Public IP is enabled.



f. Maintain default storage. Next, click.

g. Include a tag. Name is the key, and Bastion is the value. Select Next.



h. Choose the Bastion Security Group.

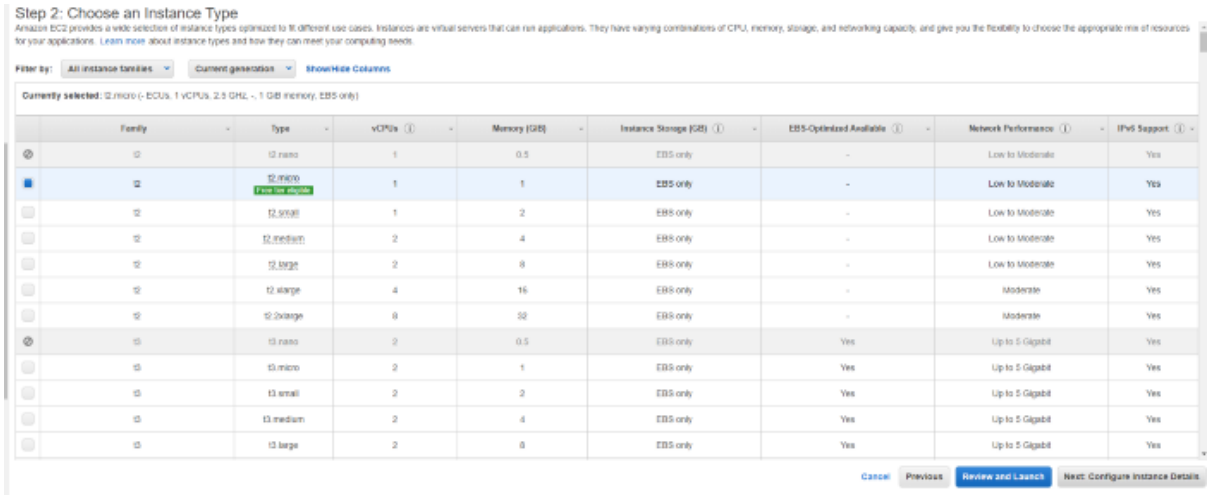
i. Review and release. Make sure that either the key pair is downloaded or utilise an existing key pair to which access is granted to.

1.12 Create Private Instances

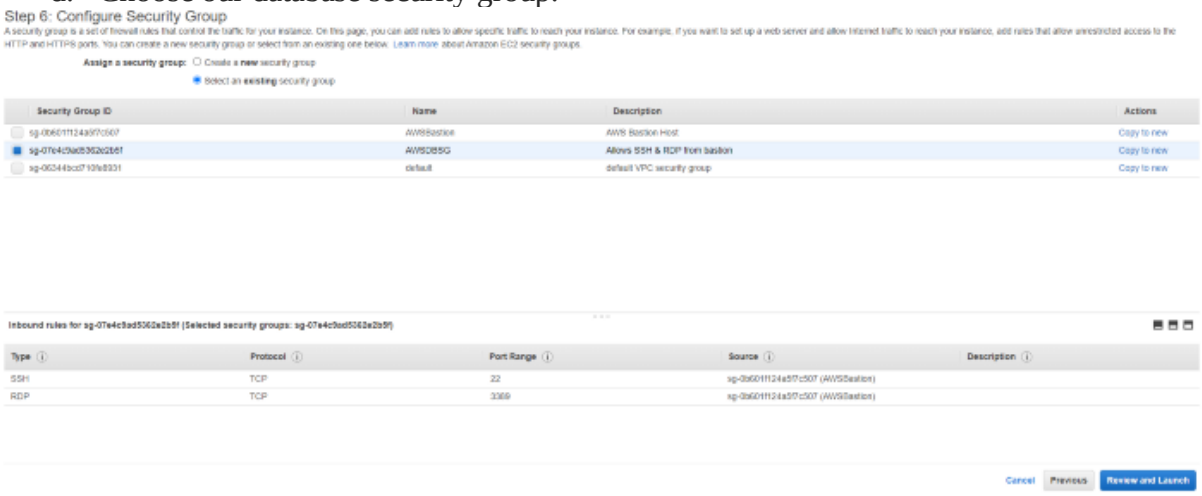
a. Click the Launch Instance button.

b. Decide on Red Hat Enterprise Linux.

c. Choose **t2.micro**.



d. Choose our database security group.

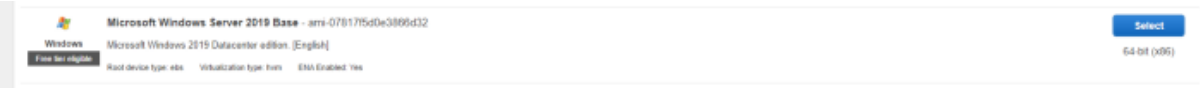


e. Finally, click Review and Launch.

f. Enter the same key combination as the Bastion Host.

g. Repeat the instructions for the RHEL instance, but this time build an Ubuntu Server LTS instance.

h. Repeat the instructions for the RHEL instance, but this time construct a Microsoft Windows Server 2019 Base instance.

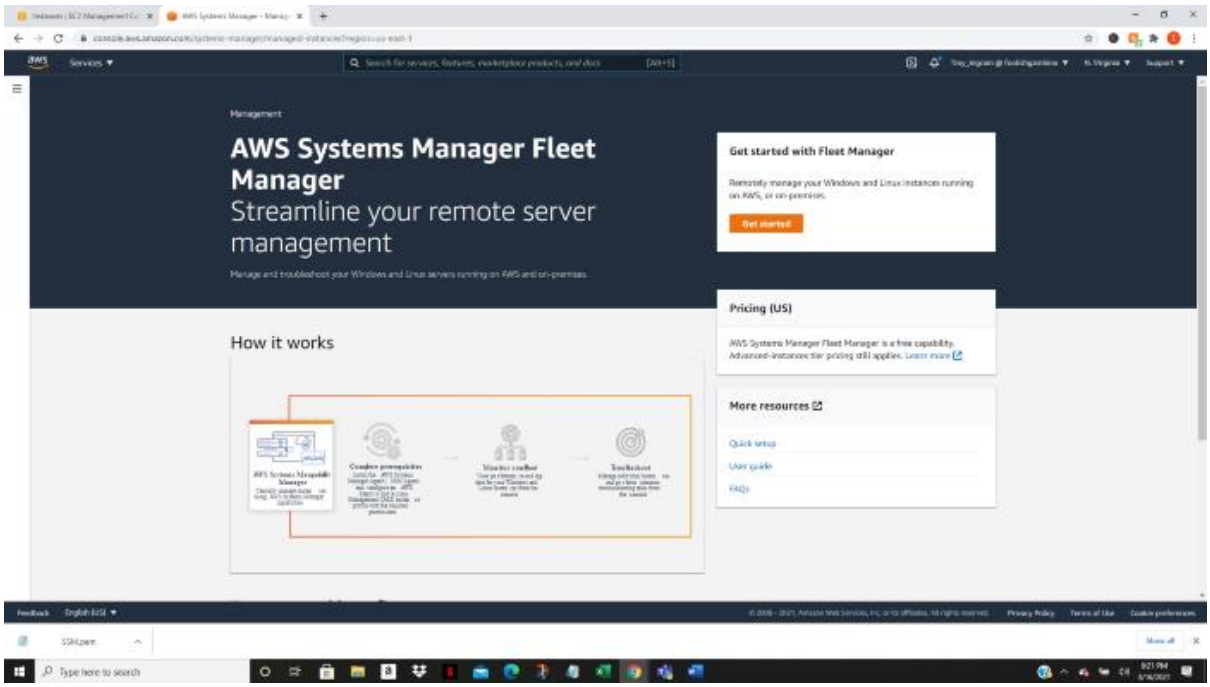


2 Systems Manager

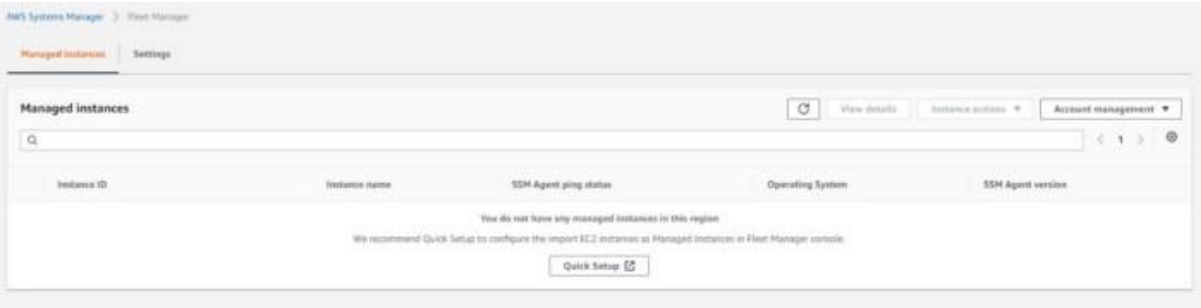
2.1 Managed Instances

a. Go to AWS Systems Manager by navigating to Services > AWS Systems Manager.
b. On the left, select Fleet Manager.

c. Select Get started.

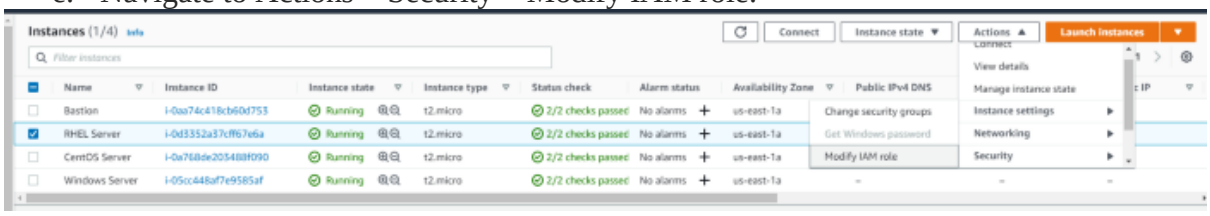


There are no instances listed in the Managed instances section. This is due to the fact that we have yet to assign the SSM role that was generated to the instances.



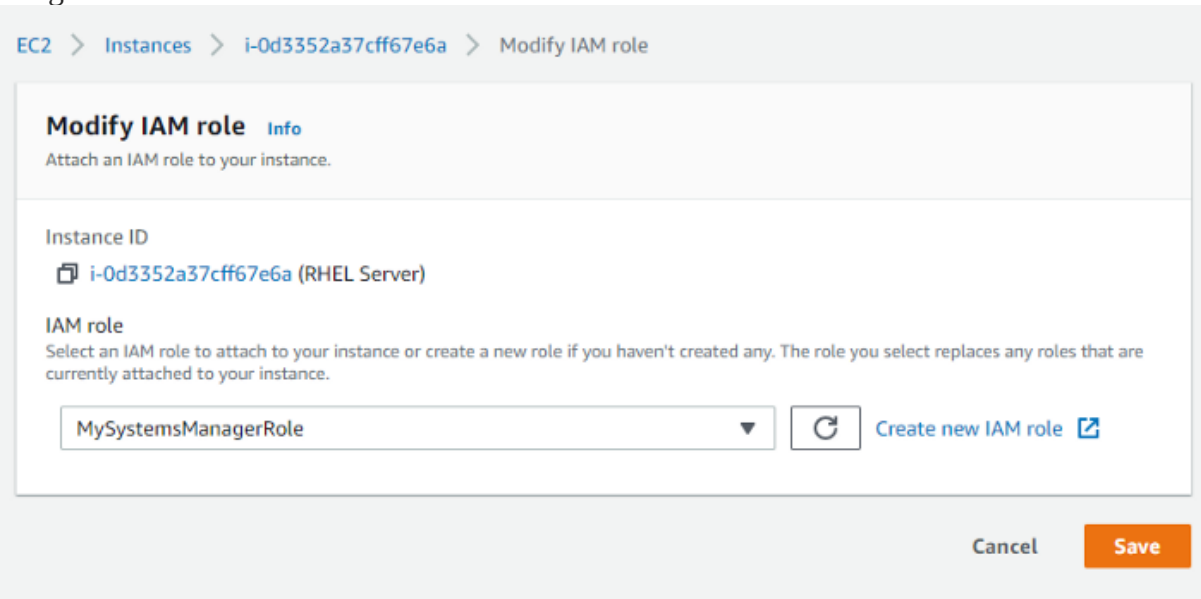
d. Go to EC2 and choose the RHEL instance.

e. Navigate to Actions > Security > Modify IAM role.

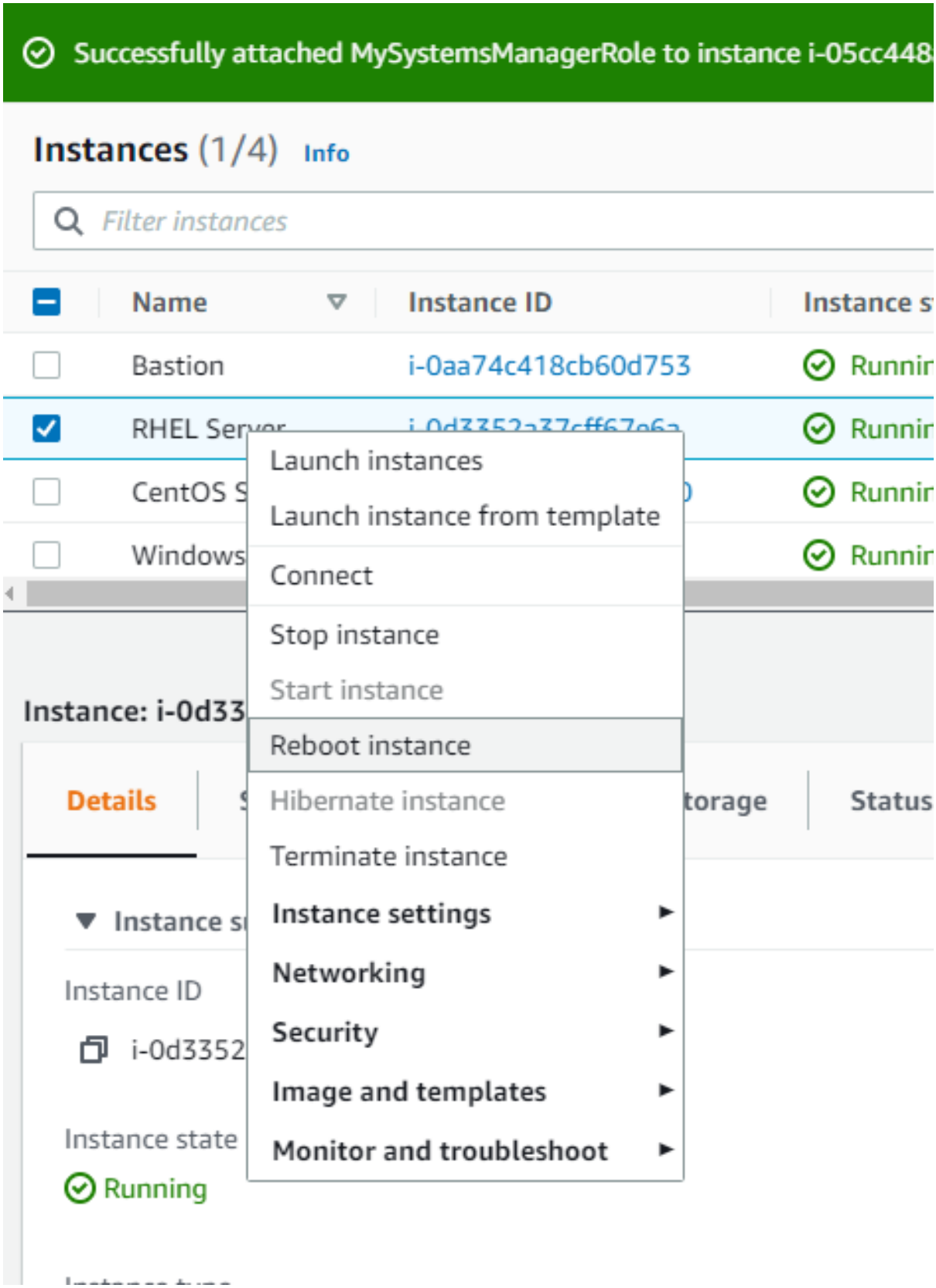


f. Select the SSM role previously generated for the IAM role.

g. Click the Save button.

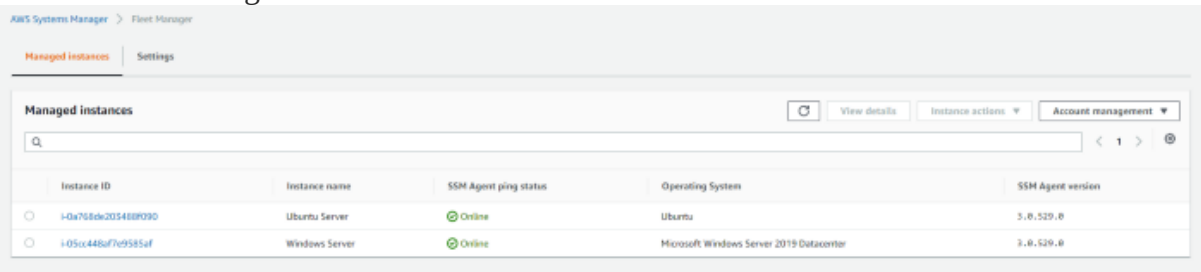


h. Select Reboot instance from the context menu when you right-click the RHEL instance.



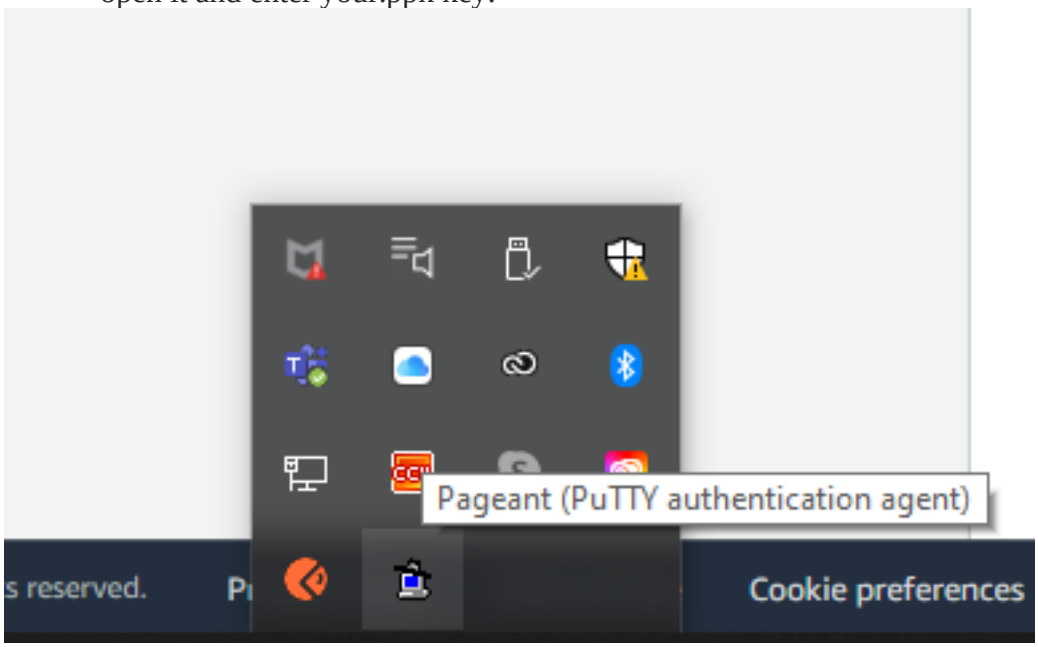
i. Repeat the preceding procedures for the Ubuntu and Windows instances.

When you return to the Managed instances, one will notice that some instances have populated since they now have the agent and permissions, but the RHEL instance does not. This is because the RHEL AMI does not include the agent. This instance will require manual installation of the agent.



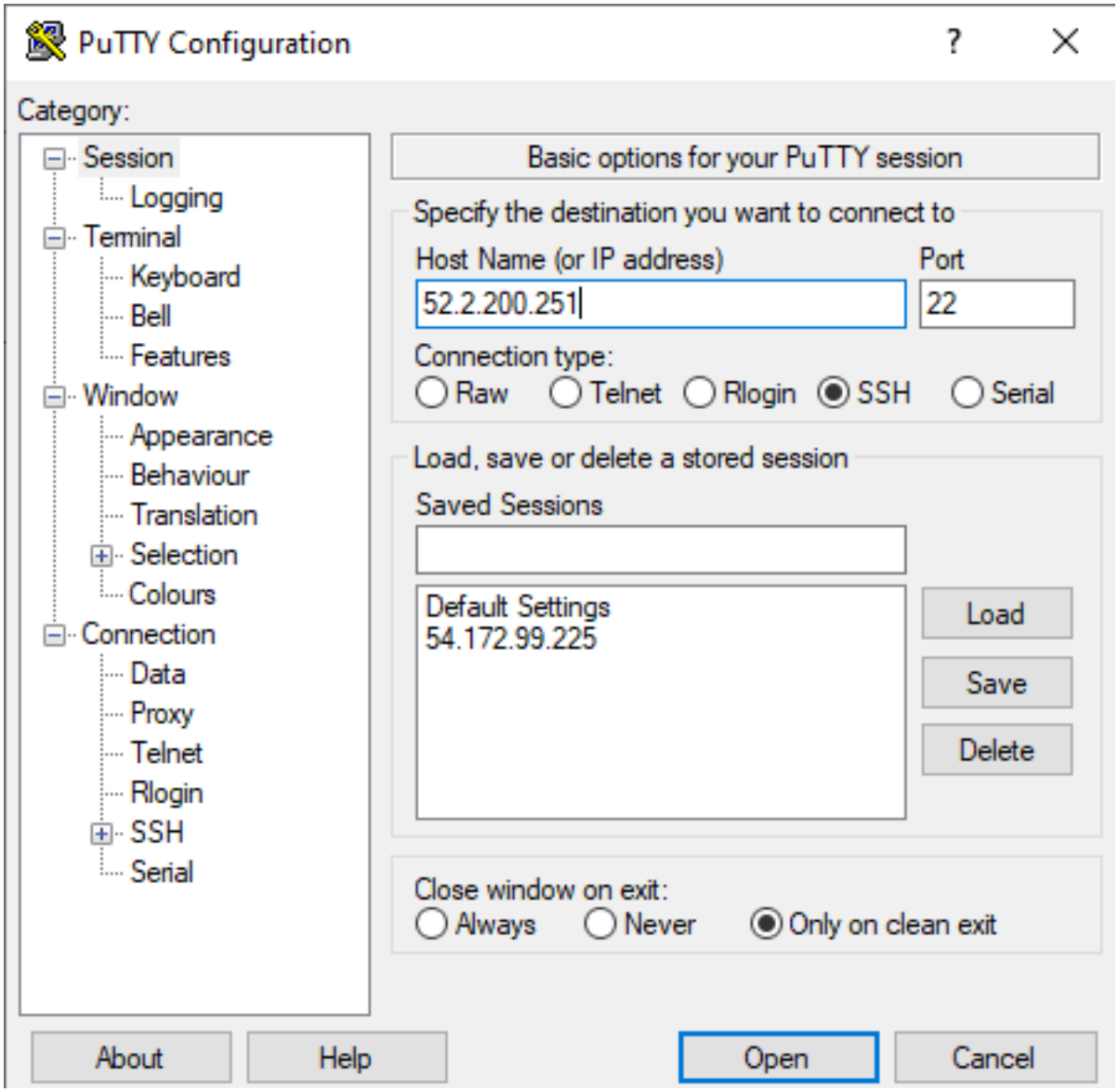
Putty is being used to SSH into the bastion and then into the RHEL instance. The procedure for various operating systems may be found here.

j. To enable agent forwarding, one must first download Pageant. upon first launch of Pageant, it will appear at the bottom right corner of the screen. Click Pageant to open it and enter your.ppk key.



k. Open Putty.

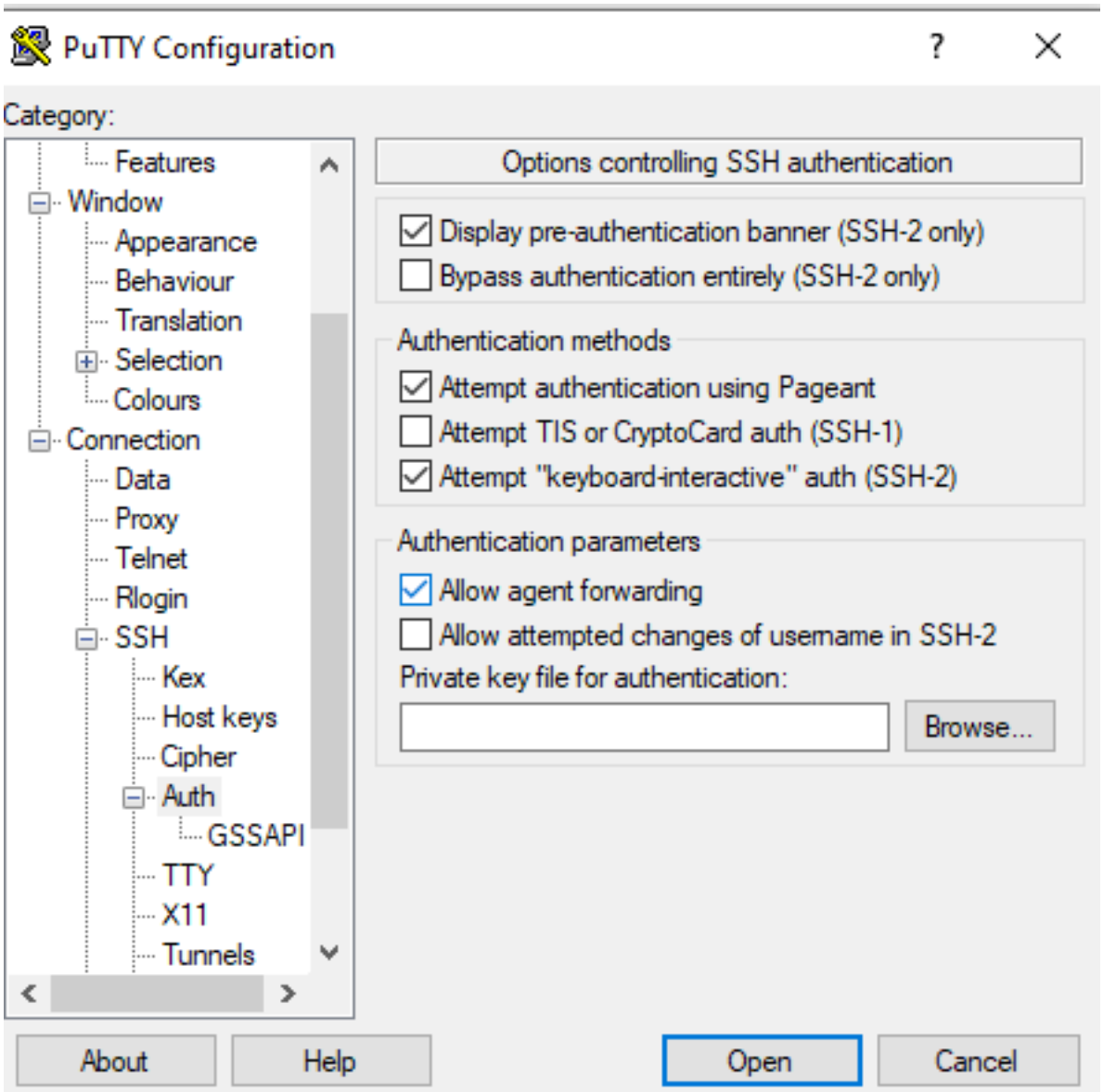
l. Enter the bastion's public IP address.



m. Expand Connection, then SSH, and finally Auth.

n. Check the Allow agent forwarding box.

o. Select your.ppk private key by clicking Browse. Then click the Open button.



p. This will launch your terminal. Following that, run:

```
ssh ec2-user@<private ip of RHEL instance>
```

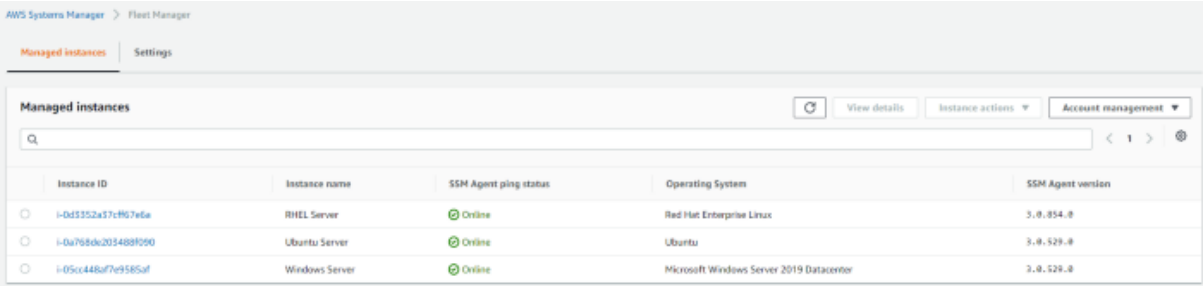
q. Run the following command:

```
sudo dnf install -y https://s3.us-east-1.amazonaws.com/amazon-ssm-us-east-1/latest/linux_amd64/amazon-ssm-agent.rpm
```

r. Then runthis commands:

```
sudo systemctl enable amazon-ssm-agent
sudo systemctl start amazon-ssm-agent
```

s. Return to the Systems Manager Managed instances and you should now see the RHEL instance.



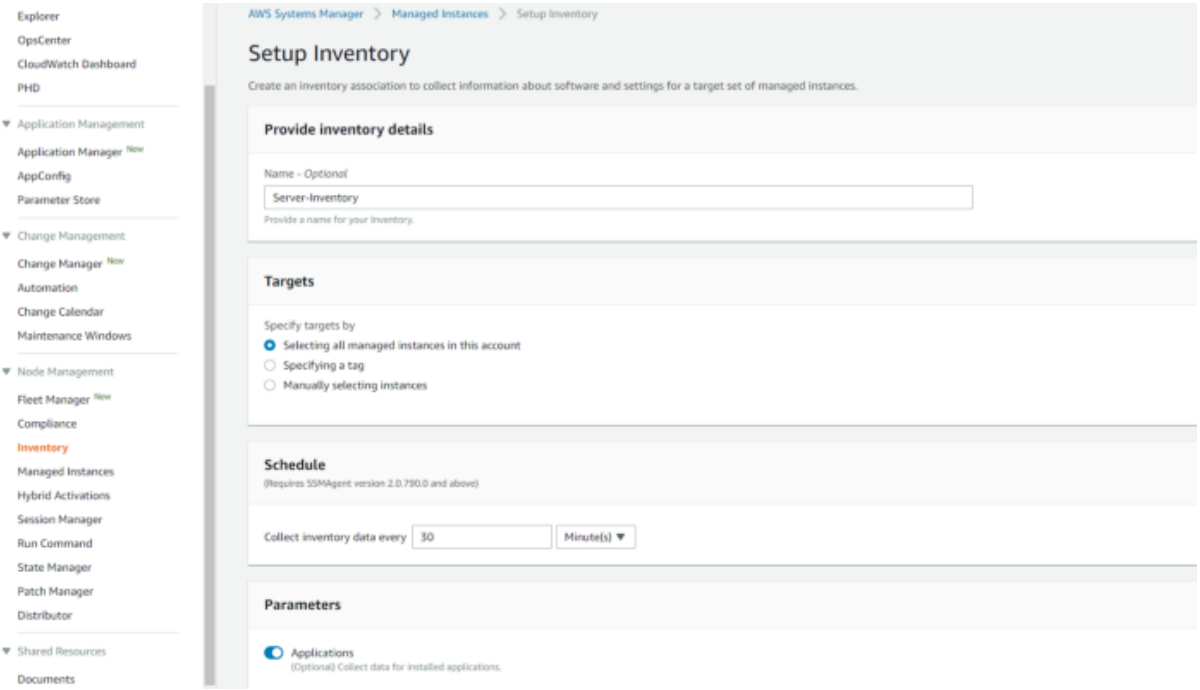
2.2 Configure Inventory

a. As there is a need to configure inventory. Go to AWS Systems Manager > Managed Instances > Inventory Setup.

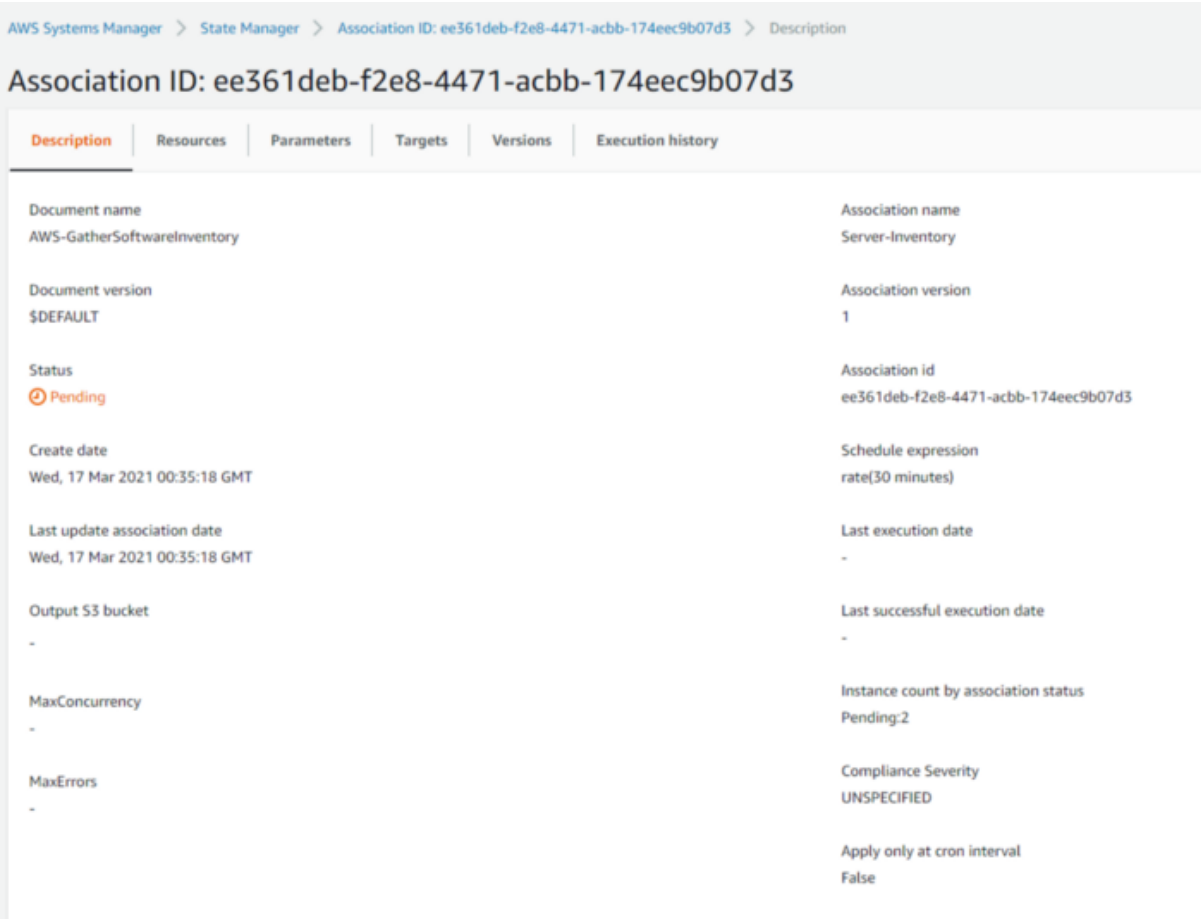
b. Come up with a name. This project made use of Server-Inventory.

c. Check the box next to Selecting all managed instances in this account.

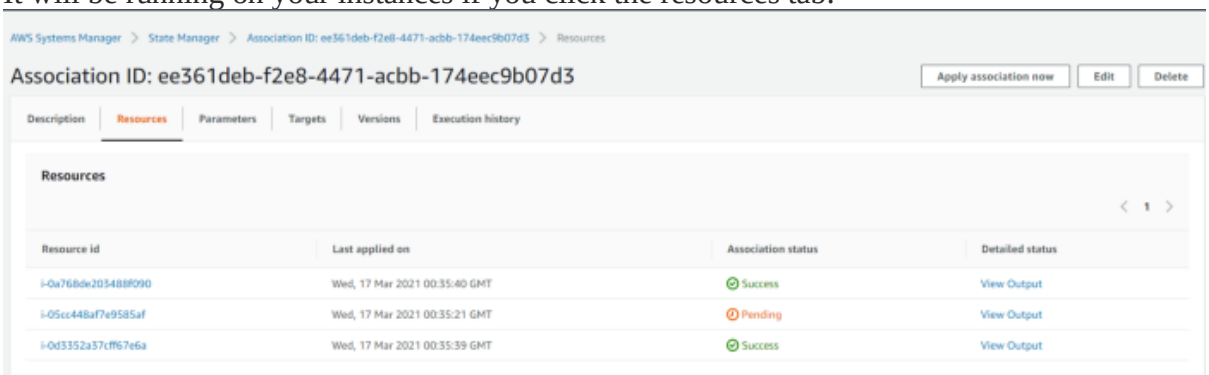
d. Program the Schedule to run every 30 minutes.



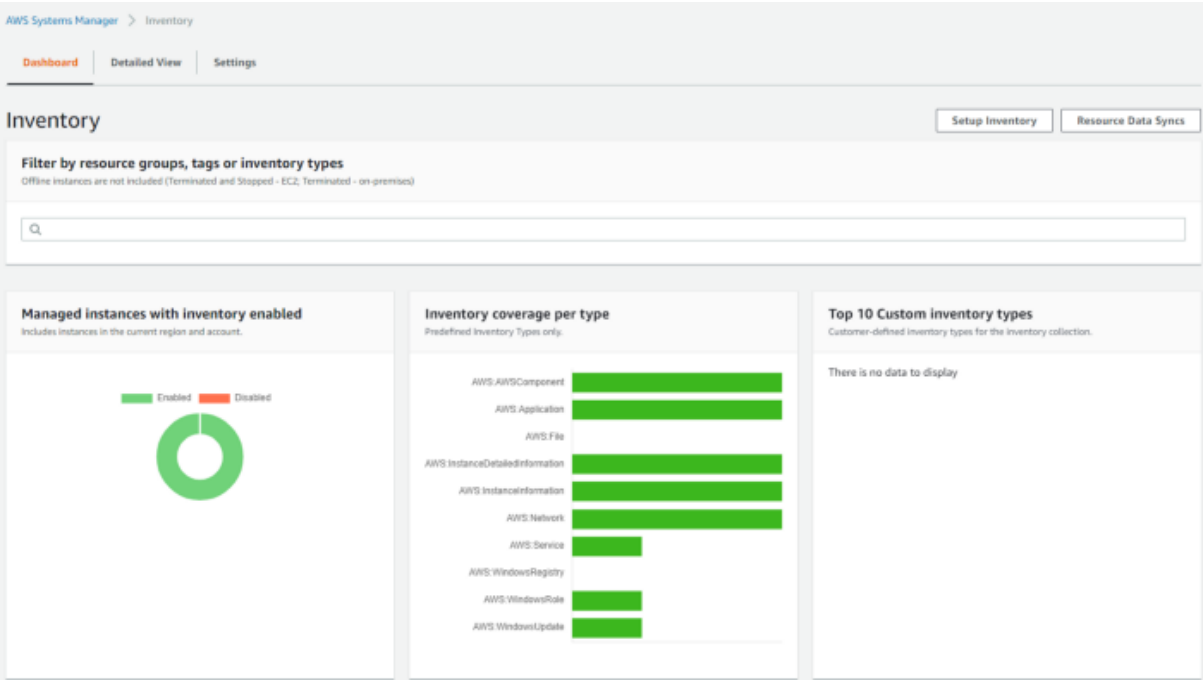
This will execute the AWS-GatherSoftwareInventory task on all managed instances every 30 minutes.



It will be running on your instances if you click the resources tab.



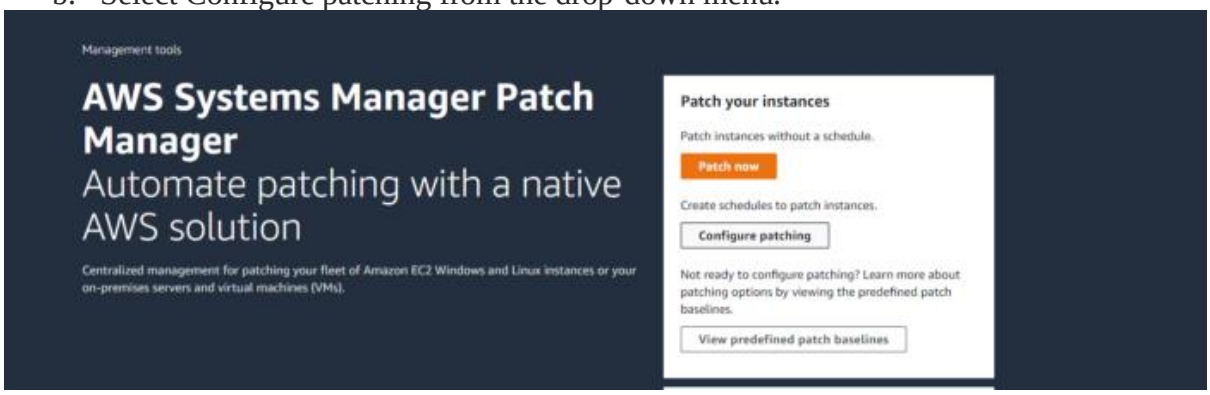
To get information about the managed inventory, go to AWS Systems Manager > Inventory > Dashboard tab.



2.3 Patch Manager

a. Select Patch Manager from the Node Management menu.

b. Select Configure patching from the drop-down menu.



c. Select instances manually by clicking the button.

d. Navigate to the RHEL instance. We could choose all RHEL instances if we had more.

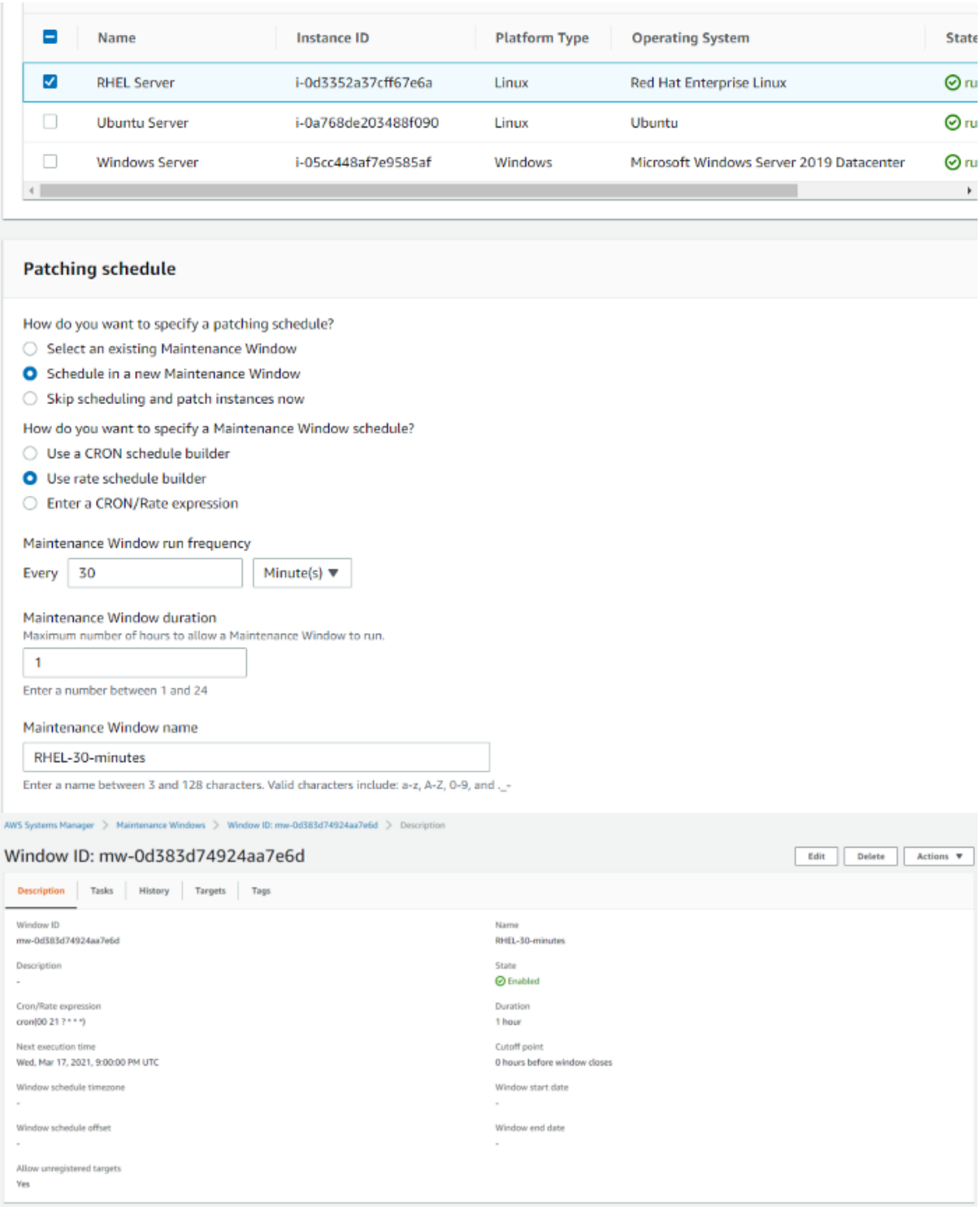
e. In a new Maintenance Window, select Schedule.

f. Choose Use rate schedule builder.

g. Every thirty minutes**.**

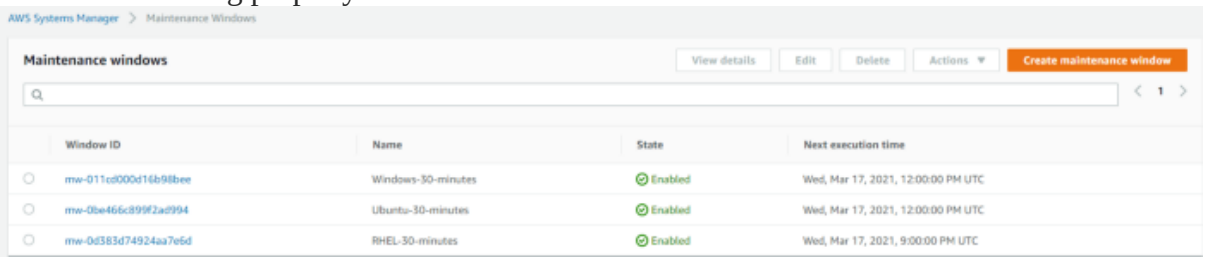
Maintenance RHEL-30-minutes is the name of the window.

h. Select Patching Configuration.

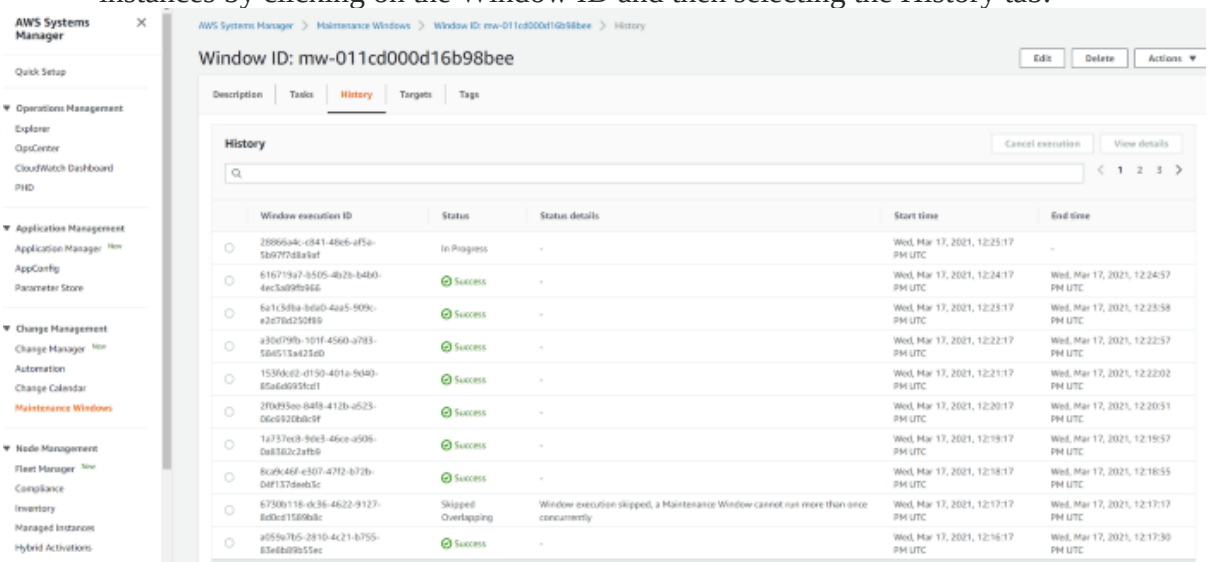


j. Repeat steps 5-8 to build a schedule for both Ubuntu and Windows instances.

k. Go to AWS Systems Manager and then to Maintenance Windows. Take note of the time of the next planned execution. Check back in 30 minutes to ensure everything is functioning properly.



l. After the patching has been completed, one can check that patching has begun on the instances by clicking on the Window ID and then selecting the History tab.



Using AWS Systems Manager, this project successfully generated a hyperautomated patching task.

3. References

Anon, (2022). AWS Systems Manager Patch Manager for orchestrating patching at scale - Mobilise Cloud. [online] Available at: https://www.mobilise.cloud/aws-systems-manager-patch-manager/ [Accessed 5 Jan. 2023].

AWS, A. (n.d.). Patch Manager :: AWS Management and Governance Tools Workshop. [online] mng.workshop.aws. Available at: https://mng.workshop.aws/ssm/use-case-labs/inventory_patch_management/patch.html.

CloudThat Resources. (n.d.). A Step-by-Step Guide: Centralized Multi-Account OS Patching using AWS Systems Manager | CloudThat. [online] Available at: https://www.cloudthat.com/resources/blog/a-step-by-step-guide-centralized-multi-account-os-patching-using-aws-systems-manager [Accessed 5 Jan. 2023].

www.youtube.com. (n.d.). Schedule Patching Across Multiple Accounts Using AWS Systems Manager Automation. [online] Available at: https://www.youtube.com/watch?v=dcJDvoUfboA [Accessed 5 Jan. 2023].

Monthly Internship Activity Report

The Internship Activity Report is a 1-page monthly summary of the activities performed by you and what you have learned during that month. The Internship Activity Report must be signed off by your Company and included in the configuration manual as part of the portfolio submission.

Student Name: Oluwasefunmi Alabi Student number: x21130094

Company: Central Bank of Ireland Month Commencing: September 2022

In my role as an Intern for 3 months in the Security department of the Central Bank of Ireland, I provided IT security support on planning, analysis and design of Information security systems and frameworks, for all operations in the organisation.

Responsibilities of the job function entailed:

• Software asset and patch management
• Reviewing and maintaining CMDB to get visibility of IT estate
• Maintaining and reviewing security vulnerabilities and systems
• Reviewing mailbox security and conducting phishing simulations
• Analyzing, improving, implementing and executing security controls proactively to prevent external threat actors from infiltrating
• company information systems.
• Research more advance and complex attempts/efforts to compromise security protocols.
• Vulnerability assessments and management
• Conducting cyber awareness trainings
• Supporting Incidence response operations
• Supporting IT security risk and compliance operations
• Performing other task as the business need requires

Employer comments

Oluwasefunmi has settled into the Service Lifecycle team well. He splits his time between my team (Service lifecycle) and the Information Security Operations team.

Oluwasefunmi is doing very well against the principal accountabilities. He works well with others in the bank both in my team and securioty operations.
Oluwasefunmi i s learning the principle accoubntabilities for the Software Assset Management and Information Security role.
This has been a huge bonus for the lifecycle team as a member of my team who normally looks after this role is currently on sick leave so Oluwasefunmi has had to step up earlier than expected and has done so convincingly.

Student Signature: _____ Date: 20th December, 2022

Industry Supervisor Signature: Martin Doyle _____ Date: 20th December, 2022