

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)	<input type="checkbox"/>
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	<input type="checkbox"/>
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.	<input type="checkbox"/>

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. Recommended to choose 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.

VPC

VPC ID
Create subnets in this VPC.

vpc-00291a1aa2af5a63c (AWS VPC) ▼

Associated VPC CIDRs

IPv4 CIDRs
10.0.0.0/16

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.

PrivateA

The name can be up to 256 characters long.

Availability Zone [Info](#)
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

US East (N. Virginia) / us-east-1a ▼

IPv4 CIDR block [Info](#)

Q 10.0.10.0/24 X

▼ **Tags - optional**

Key	Value - optional	
Q Name X	Q PrivateA X	Remove

Add new tag

You can add 49 more tags.

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

g. Fill in the blanks with the following information:

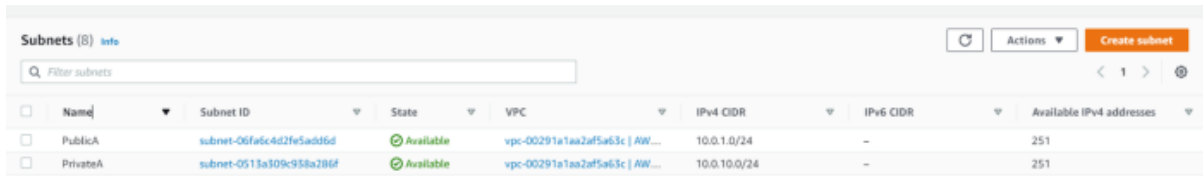
VPC ID: Choose your VPC

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.

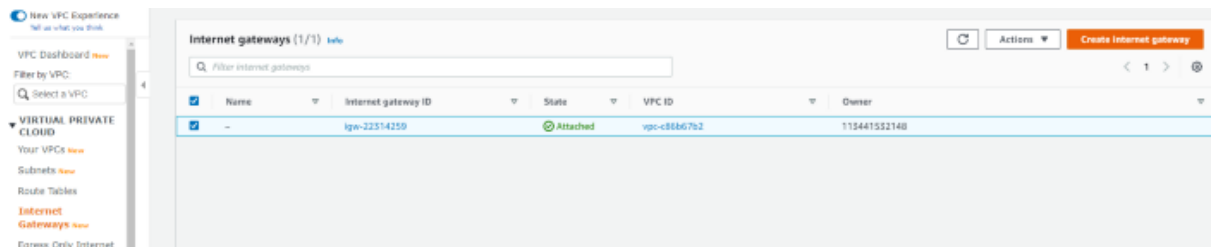


<input type="checkbox"/>	Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4 addresses
<input type="checkbox"/>	PublicA	subnet-06fa6c4d2fe5ad56d	Available	vpc-00291a1aa2af5a63c AW...	10.0.1.0/24	-	251
<input type="checkbox"/>	PrivateA	subnet-0513a509c958a286f	Available	vpc-00291a1aa2af5a63c AW...	10.0.10.0/24	-	251

1.4 Create Internet Gateway

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

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



<input checked="" type="checkbox"/>	Name	Internet gateway ID	State	VPC ID	Owner
<input checked="" type="checkbox"/>	-	igw-22514259	Attached	vpc-c84667b2	115441532148

- AWS IGW is the Name Tag chosen
- Click the Create Internet gateway button.

VPC > Internet gateways > Create internet gateway

Create internet gateway [Info](#)

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Internet gateway settings

Name tag
Creates a tag with a key of 'Name' and a value that you specify.

Tags - optional

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

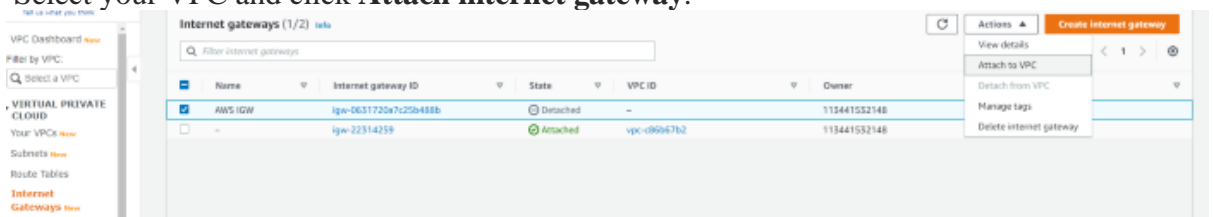
Key

Value - optional

You can add 49 more tags.

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.

VPC > NAT gateways > Create NAT gateway

Create NAT gateway [Info](#)

Create a NAT gateway and assign it an Elastic IP address.

NAT gateway settings

Name - optional
Create a tag with a key of 'Name' and a value that you specify.

The name can be up to 256 characters long.

Subnet
Select a public subnet in which to create the NAT gateway.

Elastic IP allocation ID [Info](#)
Assign an Elastic IP address to the NAT gateway.

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - optional	
<input type="text" value="Q Name"/>	<input type="text" value="Q AWS NAT"/>	<input type="button" value="Remove"/>
<input type="button" value="Add new tag"/>		

You can add 49 more tags.

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.

Route Tables > Create route table

Create route table

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Name tag: ⓘ

VPC*: ⓘ

Key	Value
This resource currently has no tags	

50 remaining (Up to 50 tags maximum)

* Required

- 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.

Basic details

Security group name [info](#)

Name cannot be edited after creation.

Description [info](#)

VPC [info](#)

Inbound rules [info](#)

Type info	Protocol info	Port range info	Source info	Description - optional info
SSH	TCP	22	Custom <input type="text" value="Q,"/> Custom Anywhere My IP	<input type="text"/>

Outbound rules [info](#)

Type info	Protocol info	Port range info	Destination info	Description - optional info
All traffic	All	All	Custom <input type="text" value="Q,"/> <input type="text" value="0.0.0.0/0"/>	<input type="text"/>

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

Create security group [info](#)

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name [info](#)

Name cannot be edited after creation.

Description [info](#)

VPC [info](#)

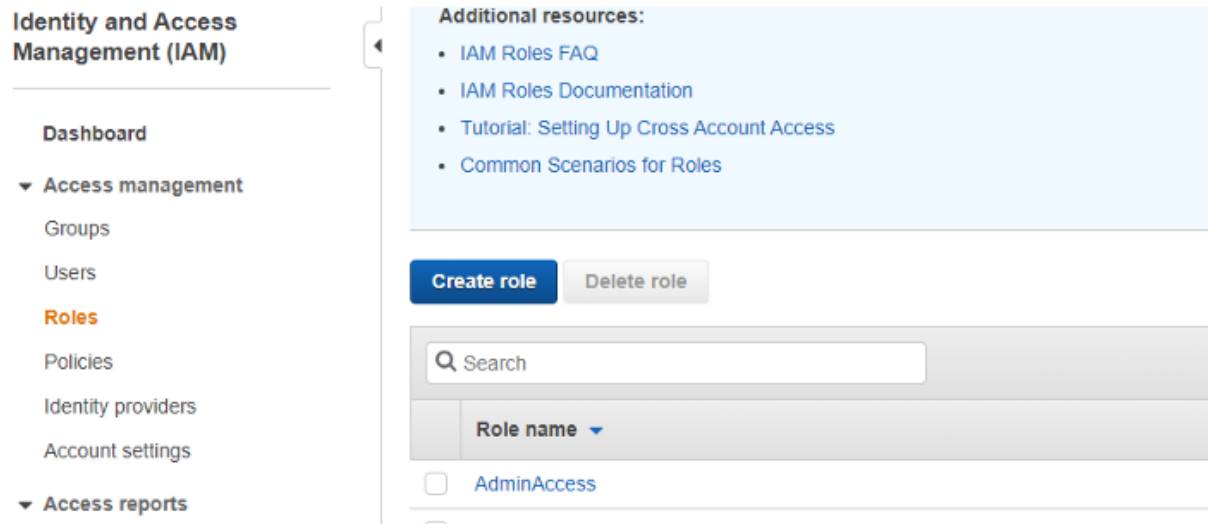
Inbound rules [info](#)

Type info	Protocol info	Port range info	Source info	Description - optional info
SSH	TCP	22	Custom <input type="text" value="Q,"/> <input type="text" value="sg-0b601f124a5f7c507"/>	<input type="text"/>
RDP	TCP	3389	Custom <input type="text" value="Q,"/> <input type="text" value="sg-0b601f124a5f7c507"/>	<input type="text"/>

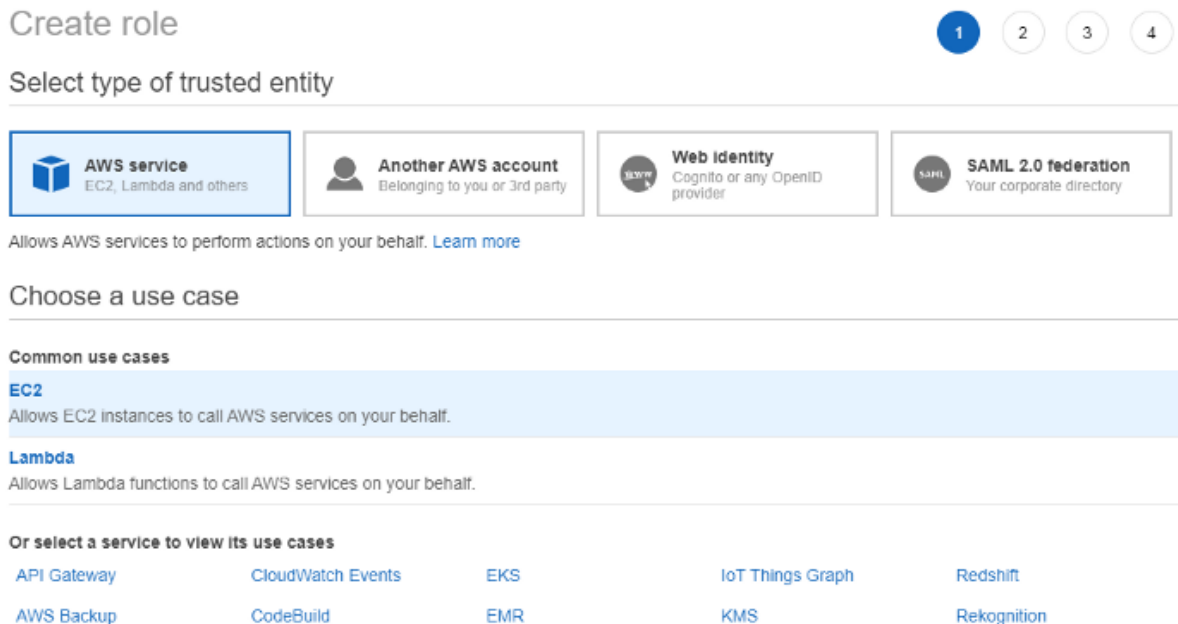
1.10 Create Systems Manager Role

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.

Create role



▼ Attach permissions policies

Choose one or more policies to attach to your new role.

Filter policies Showing 17 results

	Policy name ▼	Used as
<input type="checkbox"/>	▶ AmazonEC2RoleforSSM	None
<input type="checkbox"/>	▶ AmazonSSMAutomationApproverAccess	None
<input type="checkbox"/>	▶ AmazonSSMAutomationRole	None
<input type="checkbox"/>	▶ AmazonSSMDirectoryServiceAccess	Permissions policy (1)
<input type="checkbox"/>	▶ AmazonSSMFullAccess	None
<input type="checkbox"/>	▶ AmazonSSMMaintenanceWindowRole	None
<input checked="" type="checkbox"/>	▶ AmazonSSMManagedInstanceCore	Permissions policy (4)

AmazonSSMManagedInstanceCore

▶ Set permissions boundary

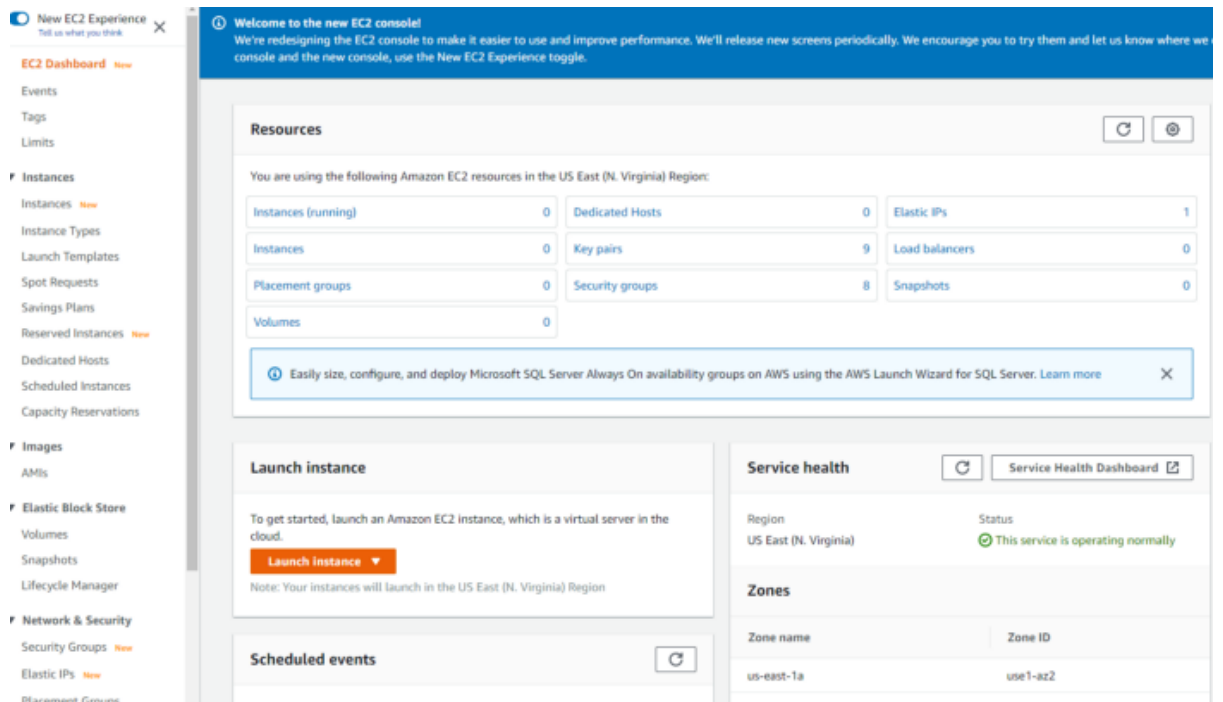
- f. Press the Next button.

- 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.

- Go to EC2. Services > EC2
- Select Launch Instance from the drop-down menu.

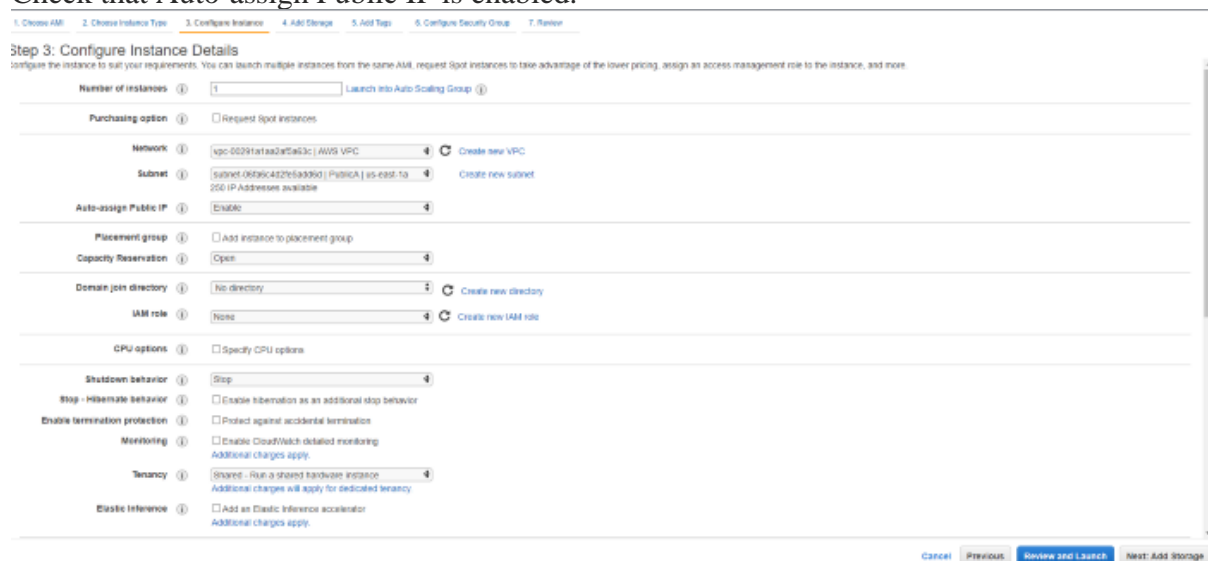


- c. Choose Amazon Linux 2 AMI. Next, click.
- d. Choose t2.micro. Next, click.
- e. Select Configure Instance Details from the drop-down menu.

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.

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.
A copy of a tag can be applied to volumes, instances or both.
Tags will be applied to all instances and volumes. [Learn more](#) about tagging your Amazon EC2 resources.

Key (128 characters maximum)	Value (256 characters maximum)	Instances (i)	Volumes (i)	Network Interfaces (i)
Name	Bastion	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

(Up to 50 tags maximum)

h. Choose the Bastion Security Group.

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic to your instances. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: Create a new security group
 Select an existing security group

Security Group ID	Name	Description	Actions
sg-0a601f12a4d7c557	AWSBastion	AWS Bastion Host	Copy to new
sg-07e4c3a5092e29f	AWSDBS	Allows SSH & RDP from bastion	Copy to new
sg-00344ec8710b0201	default	Default VPC security group	Copy to new

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.

Red Hat
Free trial available

Red Hat Enterprise Linux 8 (HVM), SSD Volume Type - ami-09615a3c22c1c990a (64-bit x86) / ami-0698190685a2d4d11 (64-bit Arm)

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

64-bit (x86)
 64-bit (Arm)

c. Choose **t2.micro**.

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 (ECU: 1 vCPUs, 2.5 GHz, ~ 1 GB memory, EBS only)

	Family	Type	vCPUs	Memory (GB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
<input checked="" type="checkbox"/>	t2	t2.micro	1	0.5	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	t2	t2.micro	1	1	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.xlarge	1	2	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.large	2	8	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.xlarge	4	16	EBS only	-	Moderate	Yes
<input type="checkbox"/>	t2	t2.xlarge	8	32	EBS only	-	Moderate	Yes
<input checked="" type="checkbox"/>	t3	t3.nano	2	0.5	EBS only	Yes	Up to 5 Gbps	Yes
<input type="checkbox"/>	t3	t3.micro	2	1	EBS only	Yes	Up to 5 Gbps	Yes
<input type="checkbox"/>	t3	t3.small	2	2	EBS only	Yes	Up to 5 Gbps	Yes
<input type="checkbox"/>	t3	t3.medium	2	4	EBS only	Yes	Up to 5 Gbps	Yes
<input type="checkbox"/>	t3	t3.large	2	8	EBS only	Yes	Up to 5 Gbps	Yes

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Configure Instance Details](#)

d. Choose our database security group.

Step 6: Configure Security Group
 A security group is a set of firewall rules that control the traffic to your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more about Amazon EC2 security groups.](#)

Assign a security group: Create a new security group Select an existing security group

Security Group ID	Name	Description	Actions
<input type="radio"/> sg-0b601124a97c507	AWSDefault	AWS Default Host	Copy to new
<input checked="" type="radio"/> sg-07e4c9a0535262b0f	AWSDefault	Allows SSH & RDP from bastion	Copy to new
<input type="radio"/> sg-003443c0712b8331	default	default VPC security group	Copy to new

Inbound rules for sg-07e4c9a0535262b0f [Selected security groups: sg-07e4c9a0535262b0f]

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	sg-0b601124a97c507 (AWSDefault)	
RDP	TCP	3389	sg-0b601124a97c507 (AWSDefault)	

[Cancel](#) [Previous](#) [Review and Launch](#)

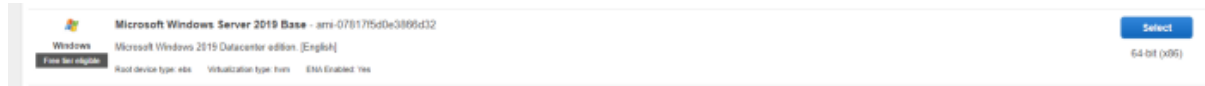
e. Finally, click Review and Launch.

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.

	SUSE Linux Enterprise Server 15 SP2 (HVM), SSD Volume Type - ami-05e503c48217 (54-bit x86) / ami-0529575d803132b (54-bit Arm)	Select
	SUSE Linux Enterprise Server 15 Service Pack 2 (HVM), EBS General Purpose (SSD) Volume Type - Amazon EC2 AMI Tools preinstalled, Apache 2.2, MySQL 5.5, PHP 5.3, and Ruby 1.8.7 available.	Select
	Ubuntu Server 20.04 LTS (HVM), SSD Volume Type - ami-042e020730845d03 (54-bit x86) / ami-0b75966a97c952252 (54-bit Arm)	Select
	Ubuntu Server 20.04 LTS (HVM), EBS General Purpose (SSD) Volume Type - Support available from Canonical (http://www.ubuntu.com/cloud/services).	Select
	Ubuntu Server 18.04 LTS (HVM), SSD Volume Type - ami-01317f30f8b1efb (54-bit x86) / ami-02e8023a38300e0f (54-bit Arm)	Select
	Ubuntu Server 18.04 LTS (HVM), EBS General Purpose (SSD) Volume Type - Support available from Canonical (http://www.ubuntu.com/cloud/services).	Select

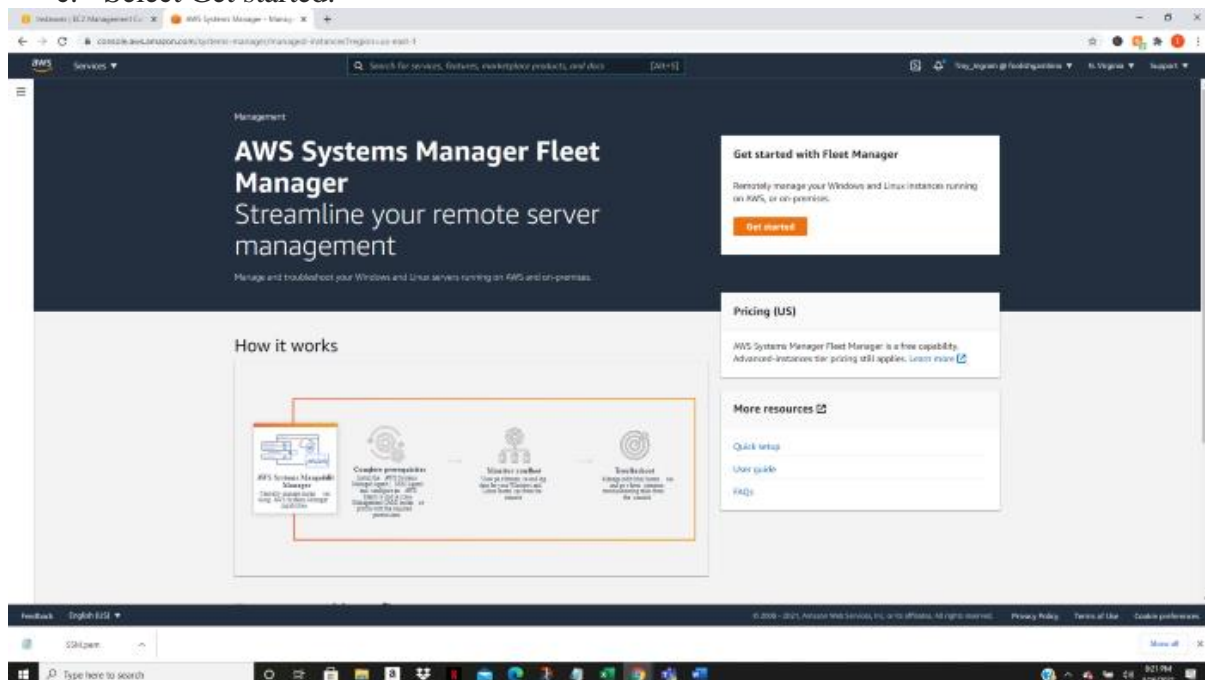
- h. Repeat the instructions for the RHEL instance, but this time construct a Microsoft Windows Server 2019 Base instance.



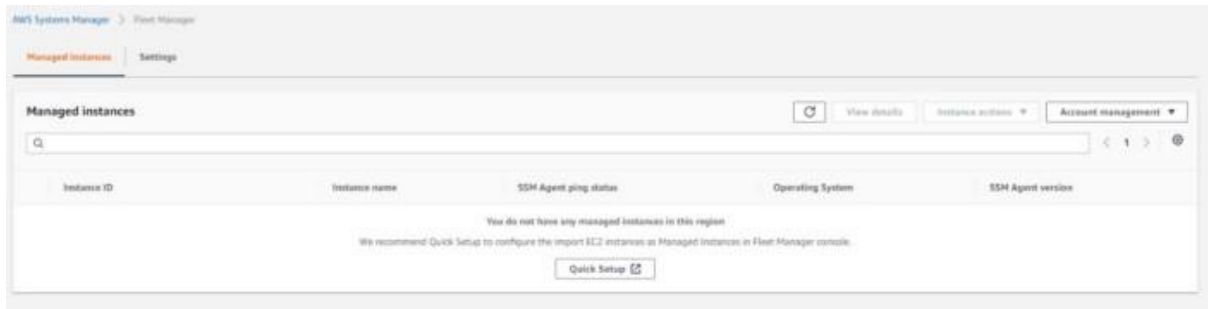
2 Systems Manager

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.

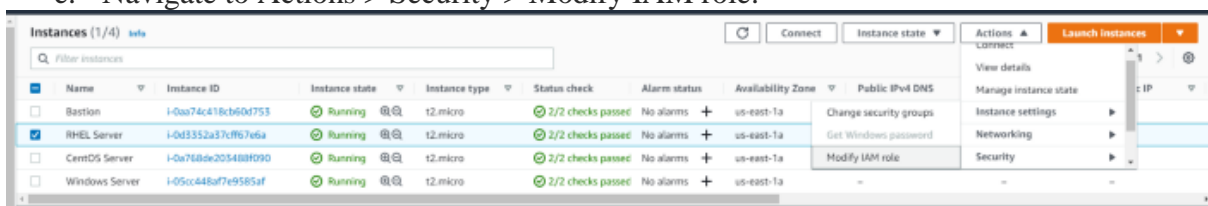


There are no instances listed in the Managed instances section. This is due to the fact that we have yet to assign the SSM role that was generated to the instances.



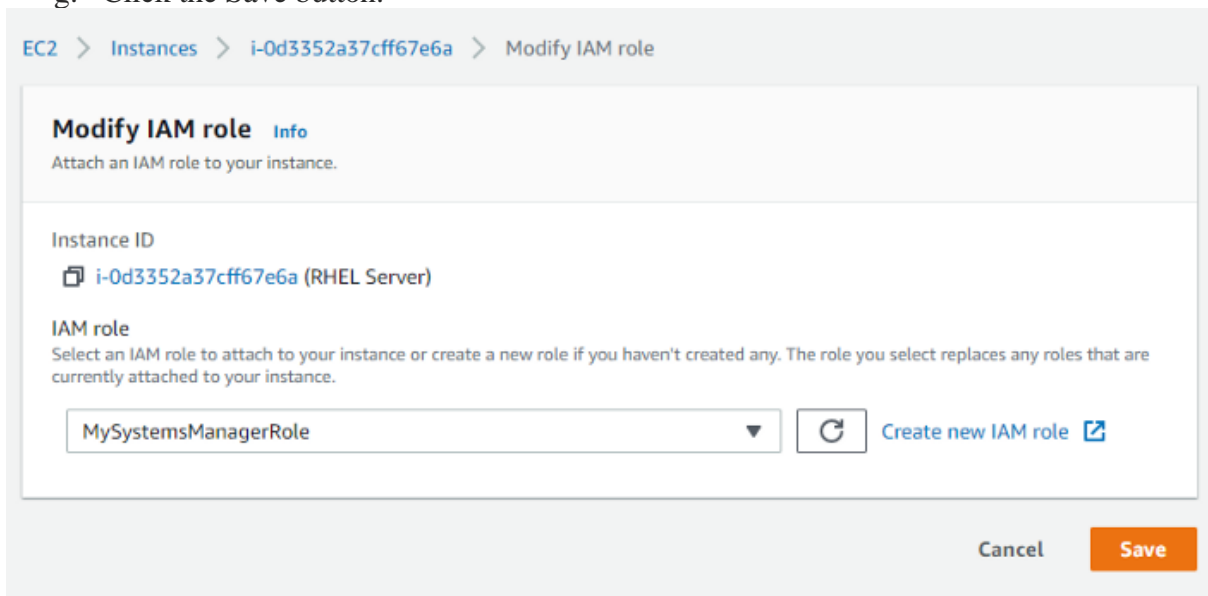
d. Go to EC2 and choose the RHEL instance.

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.

✔ Successfully attached MySystemsManagerRole to instance i-05cc448

Instances (1/4) [Info](#)

🔍 *Filter instances*

<input type="checkbox"/>	Name	Instance ID	Instance s
<input type="checkbox"/>	Bastion	i-0aa74c418cb60d753	✔ Running
<input checked="" type="checkbox"/>	RHEL Server	i-0d3352a37c67e6a	✔ Running
<input type="checkbox"/>	CentOS S		✔ Running
<input type="checkbox"/>	Windows		✔ Running


- Launch instances
- Launch instance from template
- Connect
- Stop instance
- Start instance
- Reboot instance
- Hibernate instance
- Terminate instance
- Instance settings ▶
- Networking ▶
- Security ▶
- Image and templates ▶
- Monitor and troubleshoot ▶

Instance: i-0d3352a37c67e6a

Details

▼ Instance s

Instance ID

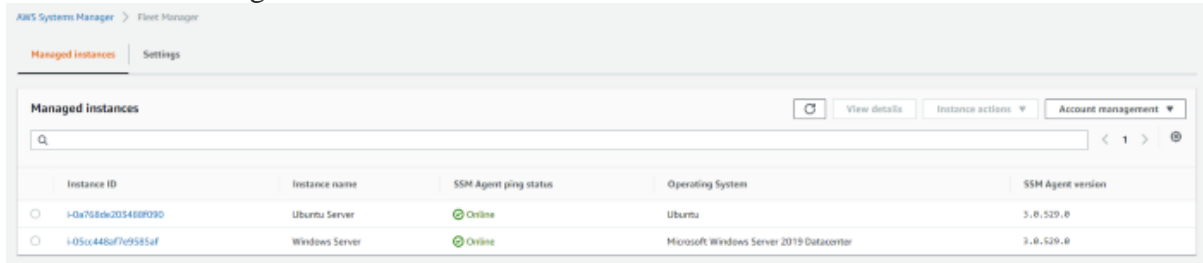
 i-0d3352a37c67e6a

Instance state

✔ Running

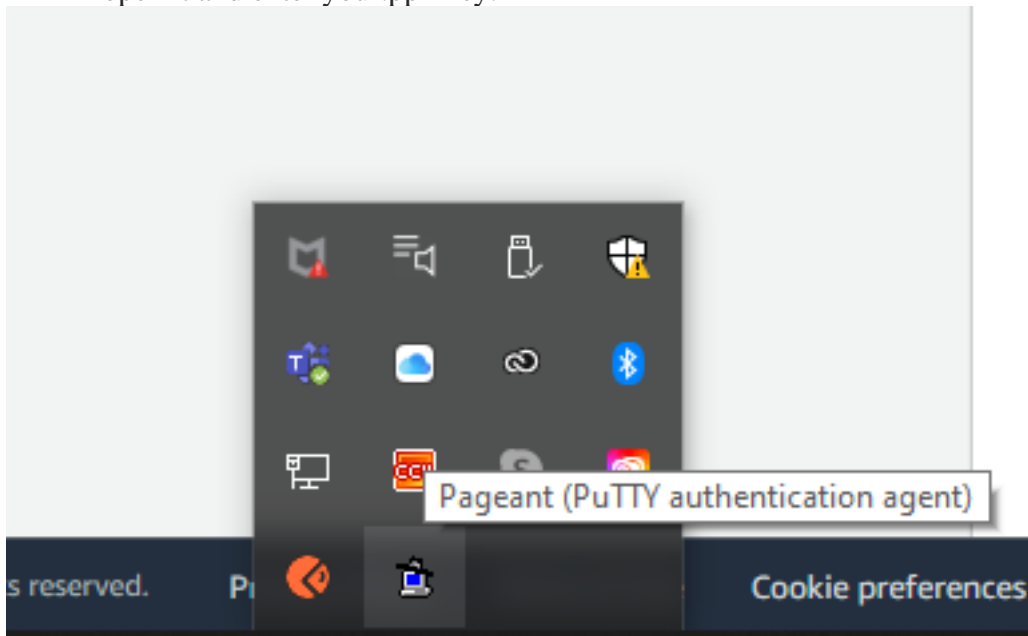
- i. Repeat the preceding procedures for the Ubuntu and Windows instances.

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.

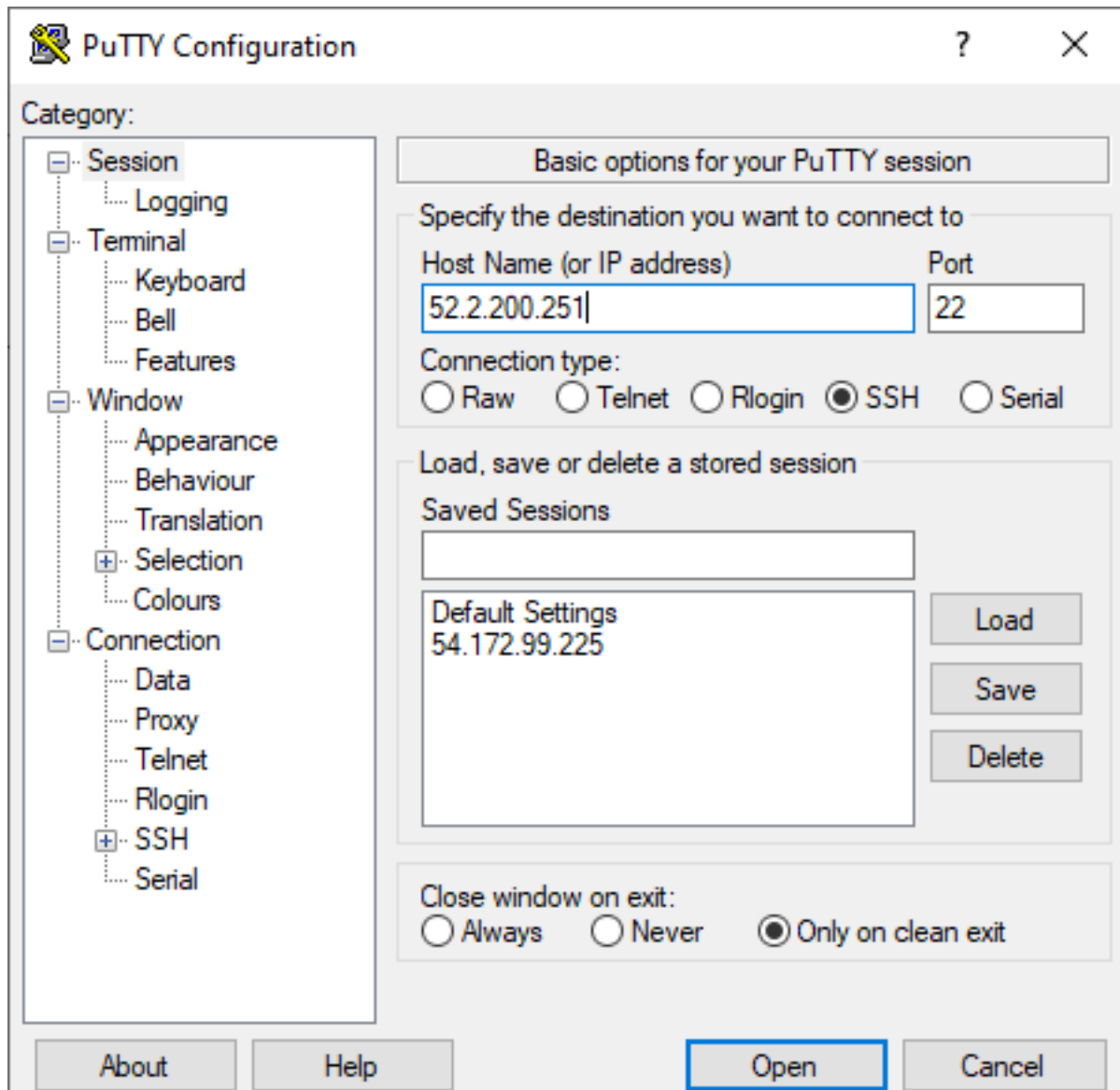


Putty is being used to SSH into the bastion and then into the RHEL instance. The procedure for various operating systems may be found [here](#).

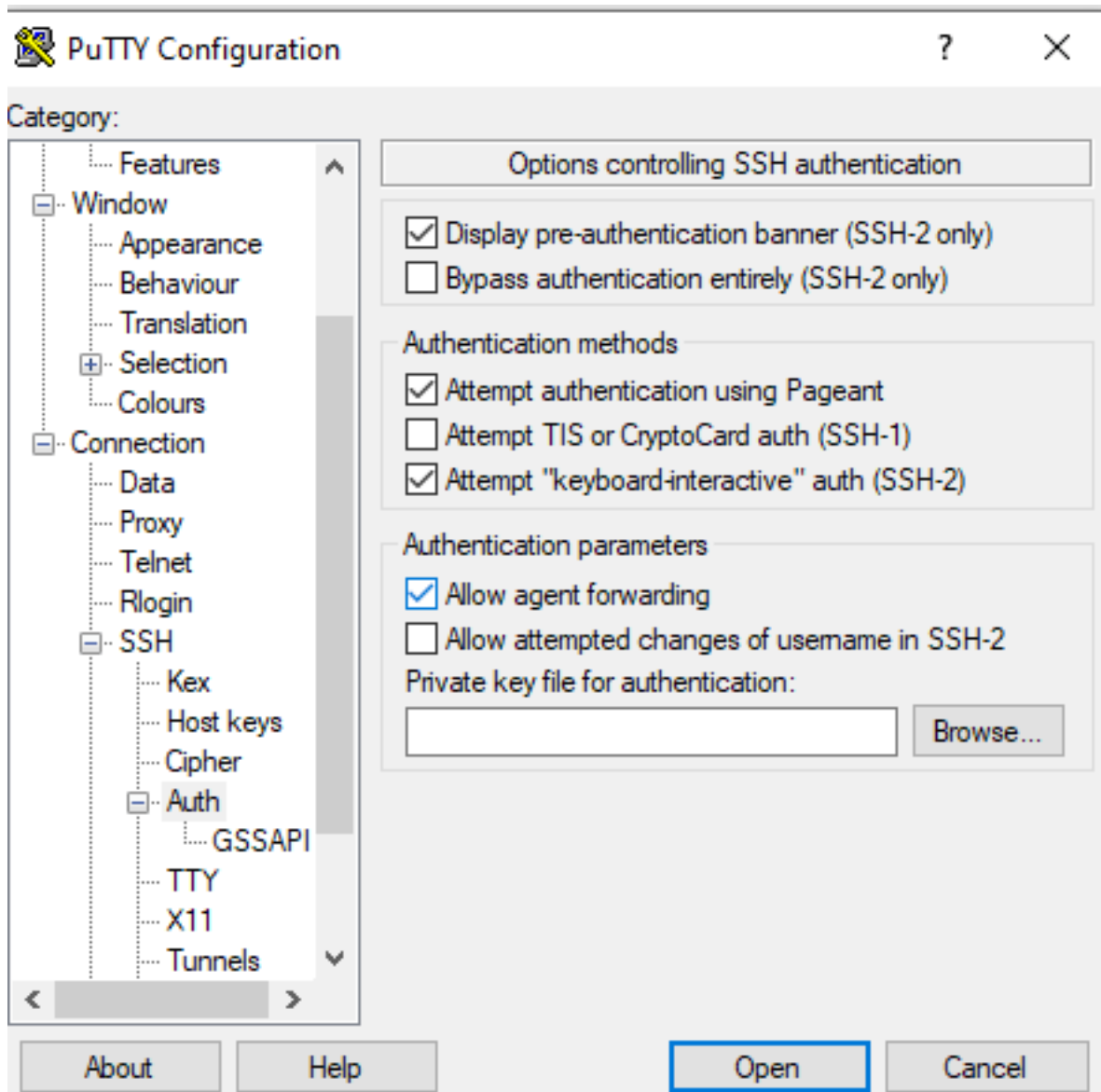
- j. To enable agent forwarding, one must first download Pageant. upon first launch of Pageant, it will appear at the bottom right corner of the screen. Click Pageant to open it and enter your.ppk key.



- 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 run these 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.

| Instance ID         | Instance name  | SSM Agent ping status | Operating System                         | SSM Agent version |
|---------------------|----------------|-----------------------|------------------------------------------|-------------------|
| i-0d3352a37c967e6e  | RHEL Server    | Online                | Red Hat Enterprise Linux                 | 3.0.854.0         |
| i-0a798dc203488f990 | Ubuntu Server  | Online                | Ubuntu                                   | 3.0.529.0         |
| i-05cc448af7e3585af | Windows Server | Online                | Microsoft Windows Server 2019 Datacenter | 3.0.529.0         |

## 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.

**Setup Inventory**  
Create an inventory association to collect information about software and settings for a target set of managed instances.

**Provide inventory details**

Name - Optional  
  
 Provide a name for your inventory.

**Targets**

Specify targets by

- Selecting all managed instances in this account
- Specifying a tag
- Manually selecting instances

**Schedule**  
(Requires SSM Agent version 2.0.790.0 and above)

Collect inventory data every

**Parameters**

- Applications  
(Optional) Collect data for installed applications.

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

AWS Systems Manager > State Manager > Association ID: ee361deb-f2e8-4471-acbb-174eec9b07d3 > Description

## Association ID: ee361deb-f2e8-4471-acbb-174eec9b07d3

Description | Resources | Parameters | Targets | Versions | Execution history

|                                                               |                                                        |
|---------------------------------------------------------------|--------------------------------------------------------|
| Document name<br>AWS-GatherSoftwareInventory                  | Association name<br>Server-Inventory                   |
| Document version<br>\$DEFAULT                                 | Association version<br>1                               |
| Status<br><span style="color: orange;">⏸ Pending</span>       | Association id<br>ee361deb-f2e8-4471-acbb-174eec9b07d3 |
| Create date<br>Wed, 17 Mar 2021 00:35:18 GMT                  | Schedule expression<br>rate(30 minutes)                |
| Last update association date<br>Wed, 17 Mar 2021 00:35:18 GMT | Last execution date<br>-                               |
| Output S3 bucket<br>-                                         | Last successful execution date<br>-                    |
| MaxConcurrency<br>-                                           | Instance count by association status<br>Pending:2      |
| MaxErrors<br>-                                                | Compliance Severity<br>UNSPECIFIED                     |
|                                                               | Apply only at cron interval<br>False                   |

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

AWS Systems Manager > State Manager > Association ID: ee361deb-f2e8-4471-acbb-174eec9b07d3 > Resources

## Association ID: ee361deb-f2e8-4471-acbb-174eec9b07d3

Apply association now | Edit | Delete

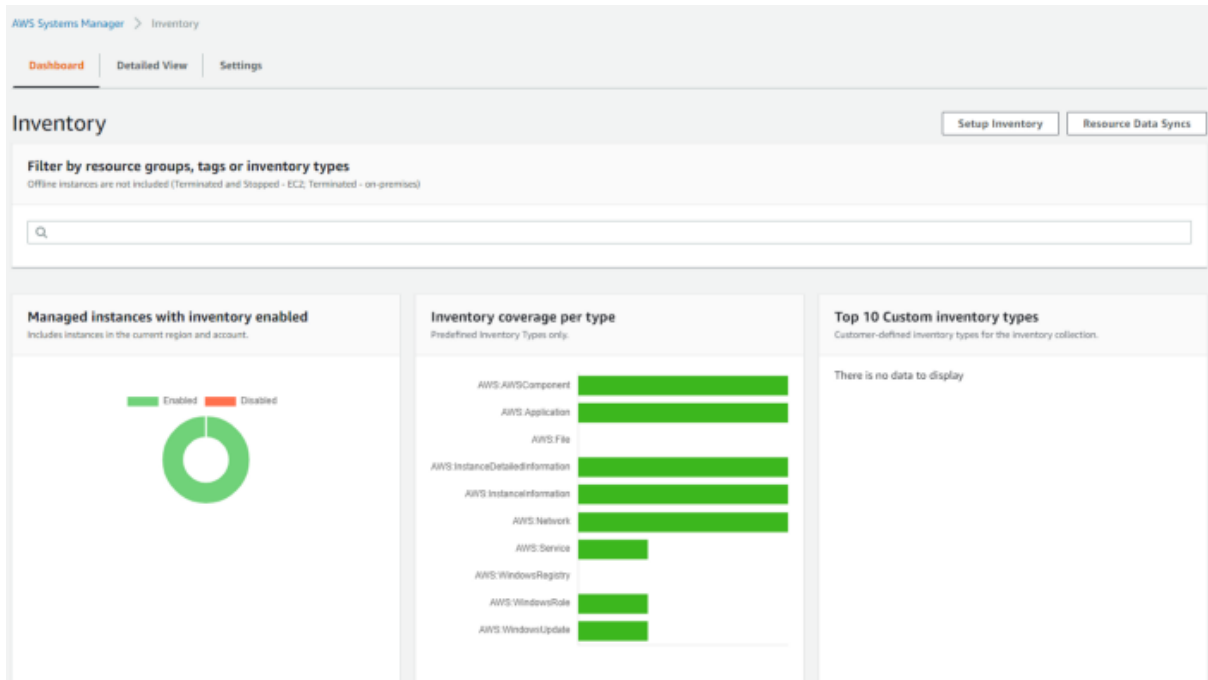
Description | Resources | Parameters | Targets | Versions | Execution history

**Resources** < 1 >

| Resource id                         | Last applied on               | Association status                            | Detailed status             |
|-------------------------------------|-------------------------------|-----------------------------------------------|-----------------------------|
| <a href="#">i-0a768de203488f090</a> | Wed, 17 Mar 2021 00:35:40 GMT | <span style="color: green;">✔ Success</span>  | <a href="#">View Output</a> |
| <a href="#">i-05cc448af7e9585af</a> | Wed, 17 Mar 2021 00:35:21 GMT | <span style="color: orange;">⏸ Pending</span> | <a href="#">View Output</a> |
| <a href="#">i-0d3352a37cf67e6a</a>  | Wed, 17 Mar 2021 00:35:39 GMT | <span style="color: green;">✔ Success</span>  | <a href="#">View Output</a> |

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.

| <input type="checkbox"/>            | Name           | Instance ID         | Platform Type | Operating System                         | State                                   |
|-------------------------------------|----------------|---------------------|---------------|------------------------------------------|-----------------------------------------|
| <input checked="" type="checkbox"/> | RHEL Server    | i-0d3352a37cff67e6a | Linux         | Red Hat Enterprise Linux                 | <span style="color: green;">✔</span> ru |
| <input type="checkbox"/>            | Ubuntu Server  | i-0a768de203488f090 | Linux         | Ubuntu                                   | <span style="color: green;">✔</span> ru |
| <input type="checkbox"/>            | Windows Server | i-05cc448af7e9585af | Windows       | Microsoft Windows Server 2019 Datacenter | <span style="color: green;">✔</span> ru |

---

### Patching schedule

How do you want to specify a patching schedule?

Select an existing Maintenance Window  
 Schedule in a new Maintenance Window  
 Skip scheduling and patch instances now

How do you want to specify a Maintenance Window schedule?

Use a CRON schedule builder  
 Use rate schedule builder  
 Enter a CRON/Rate expression

Maintenance Window run frequency

Every  Minute(s) ▼

Maintenance Window duration

Maximum number of hours to allow a Maintenance Window to run.

Enter a number between 1 and 24

Maintenance Window name

Enter a name between 3 and 128 characters. Valid characters include: a-z, A-Z, 0-9, and .\_-

---

AWS Systems Manager > Maintenance Windows > Window ID: mw-0d383d74924aa7e6d > Description

### Window ID: mw-0d383d74924aa7e6d

[Edit](#) [Delete](#) [Actions](#) ▼

**Description** | [Tasks](#) | [History](#) | [Targets](#) | [Tags](#)

|                            |                                   |                   |                                              |
|----------------------------|-----------------------------------|-------------------|----------------------------------------------|
| Window ID                  | mw-0d383d74924aa7e6d              | Name              | RHEL-30-minutes                              |
| Description                | -                                 | State             | <span style="color: green;">✔</span> Enabled |
| Cron/Rate expression       | cron[00 21 ? * * ]                | Duration          | 1 hour                                       |
| Next execution time        | Wed, Mar 17, 2021, 9:00:00 PM UTC | Cutoff point      | 0 hours before window closes                 |
| Window schedule timezone   | -                                 | Window start date | -                                            |
| Window schedule offset     | -                                 | Window end date   | -                                            |
| Allow unregistered targets | Yes                               |                   |                                              |

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.

| Window ID            | Name               | State   | Next execution time                |
|----------------------|--------------------|---------|------------------------------------|
| mw-011cd000d16b98bee | Windows-30-minutes | Enabled | Wed, Mar 17, 2021, 12:00:00 PM UTC |
| mw-0be466c899f2ad994 | Ubuntu-30-minutes  | Enabled | Wed, Mar 17, 2021, 12:00:00 PM UTC |
| mw-0d383d74924aa7e6d | RHEL-30-minutes    | Enabled | Wed, Mar 17, 2021, 9:00:00 PM UTC  |

- 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.

| Window execution ID                   | Status              | Status details                                                                        | Start time                         | End time                           |
|---------------------------------------|---------------------|---------------------------------------------------------------------------------------|------------------------------------|------------------------------------|
| 2886e94c-c841-486e-af5a-5ba97788a8af  | In Progress         | -                                                                                     | Wed, Mar 17, 2021, 12:25:17 PM UTC | -                                  |
| 616779a7-8595-4b2b-8460-4ec3a8989666  | Success             | -                                                                                     | Wed, Mar 17, 2021, 12:24:17 PM UTC | Wed, Mar 17, 2021, 12:24:57 PM UTC |
| 6a1c3f8a-9da0-4aa5-909c-a2676d250889  | Success             | -                                                                                     | Wed, Mar 17, 2021, 12:23:17 PM UTC | Wed, Mar 17, 2021, 12:23:58 PM UTC |
| a30d79fb-101f-456a-a783-5ba6513a421eb | Success             | -                                                                                     | Wed, Mar 17, 2021, 12:22:17 PM UTC | Wed, Mar 17, 2021, 12:22:57 PM UTC |
| 1530ca82-d150-401a-9d40-85a6d6995c0f  | Success             | -                                                                                     | Wed, Mar 17, 2021, 12:21:17 PM UTC | Wed, Mar 17, 2021, 12:22:02 PM UTC |
| 2f0d95ee-8489-412b-a523-06c8920ba03f  | Success             | -                                                                                     | Wed, Mar 17, 2021, 12:20:17 PM UTC | Wed, Mar 17, 2021, 12:20:51 PM UTC |
| 1a737ec8-96c3-460e-a506-da8362c2af6b  | Success             | -                                                                                     | Wed, Mar 17, 2021, 12:19:17 PM UTC | Wed, Mar 17, 2021, 12:19:57 PM UTC |
| 8c9c46f-e307-47f2-b72b-d4f137ddeb5c   | Success             | -                                                                                     | Wed, Mar 17, 2021, 12:18:17 PM UTC | Wed, Mar 17, 2021, 12:18:55 PM UTC |
| 67300118-dc36-4622-9127-8d0ca1580ba2  | Skipped Overlapping | Window execution skipped, a Maintenance Window cannot run more than once concurrently | Wed, Mar 17, 2021, 12:17:17 PM UTC | Wed, Mar 17, 2021, 12:17:17 PM UTC |
| a059a7b5-2810-4c21-b755-83a88d9ba55e  | Success             | -                                                                                     | Wed, Mar 17, 2021, 12:16:17 PM UTC | Wed, Mar 17, 2021, 12:17:30 PM UTC |

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](https://mng.workshop.aws). Available at: [https://mng.workshop.aws/ssm/use-case-labs/inventory\\_patch\\_management/patch.html](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 security operations. Oluwasefunmi is learning the principle accountabilities for the Software Asset 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