AWS Security: Amazon Inspector

In this lab, we are going to implement Amazon Inspector in our environment. Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for vulnerabilities or deviations from best practices. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity. These findings can be reviewed directly or as part of detailed assessment reports which are available via the Amazon Inspector console or API.

Below is the list of tasks:

Task 1: Create IAM Role

Task 2: Launch & Configure EC2 Instances with SSM Agent

Task 3: AWS Systems Manager: Managed Instances

Task 4: Amazon Inspector Configurations

Task 5: Amazon Inspector Troubleshooting

Task 6: Amazon Inspector-Findings

Task 1: Create IAM Role

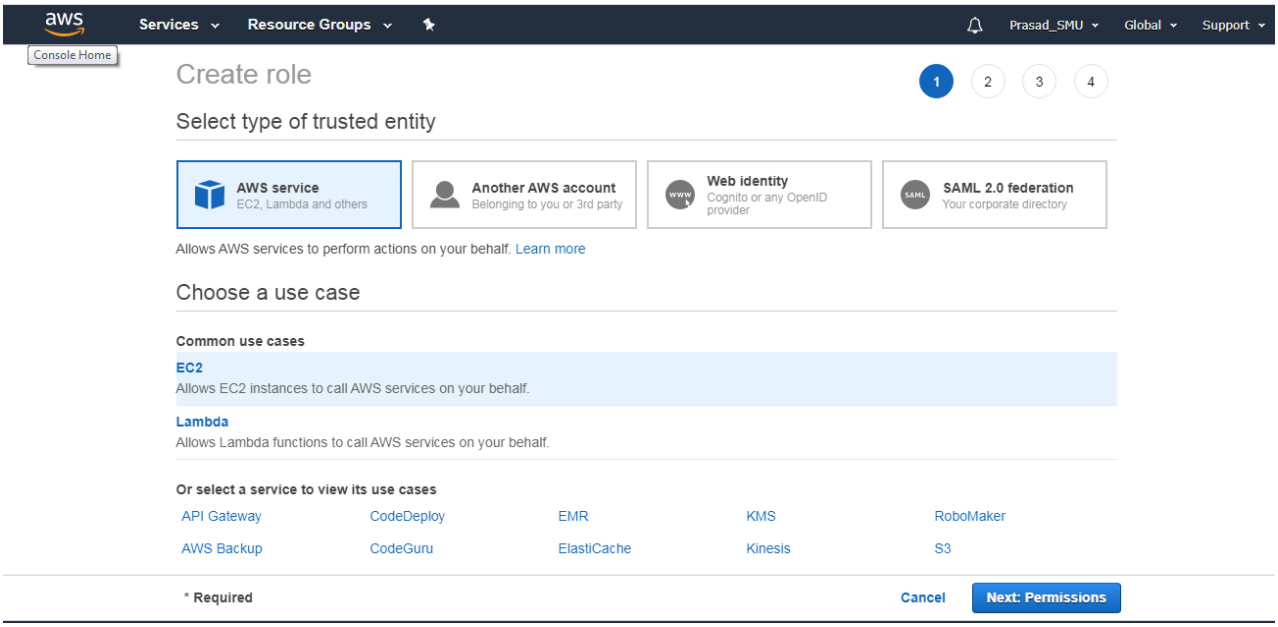
Login to the AWS Management Console.

Navigate to IAM Service and click on Roles.

Click on Create Role.

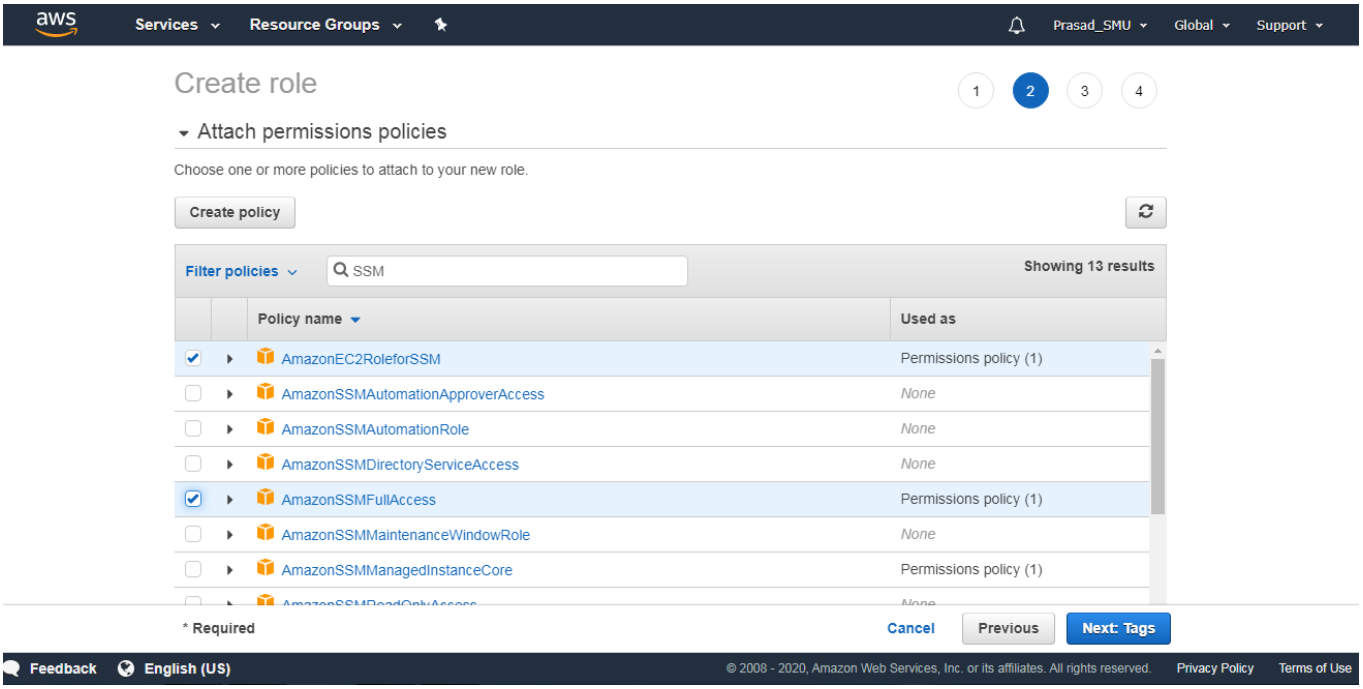
Make sure to select the Use Case as **EC2**.

Click Next: Permissions.

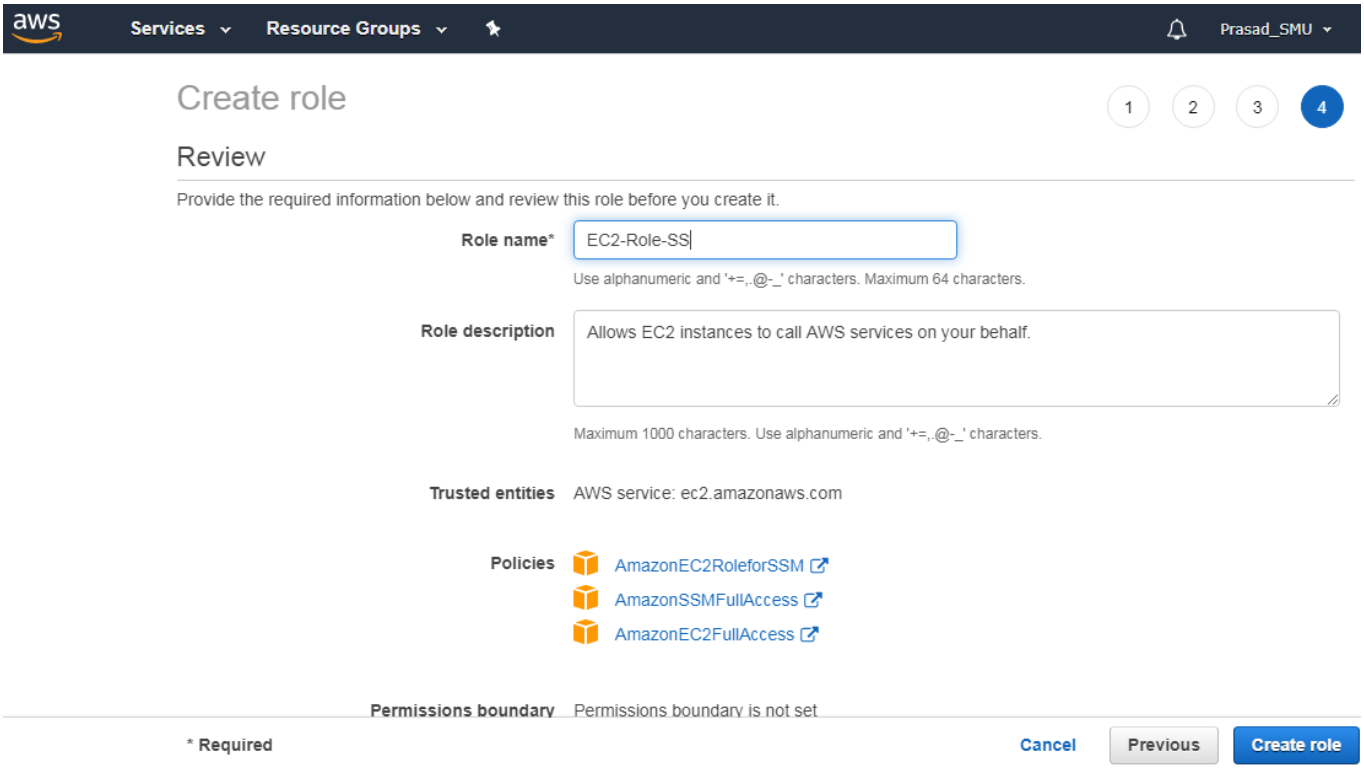


Select the below two Default IAM Policies:

1. **AmazonEC2RoleforSSM**
2. **AmazonSSMFullAccess**
3. **AmazonEC2FullAccess**



Give the Role Name as per your Choice and click on Create Role.

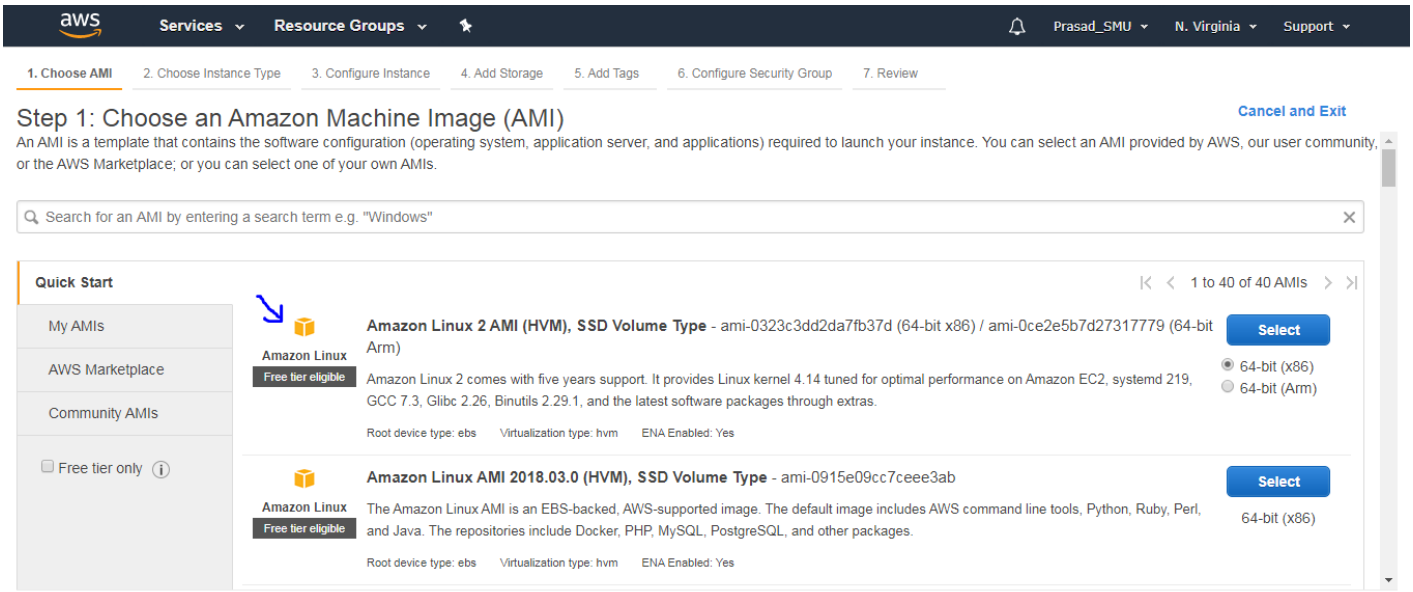


Task 2: Launch & Configure EC2 Instances with SSM Agent

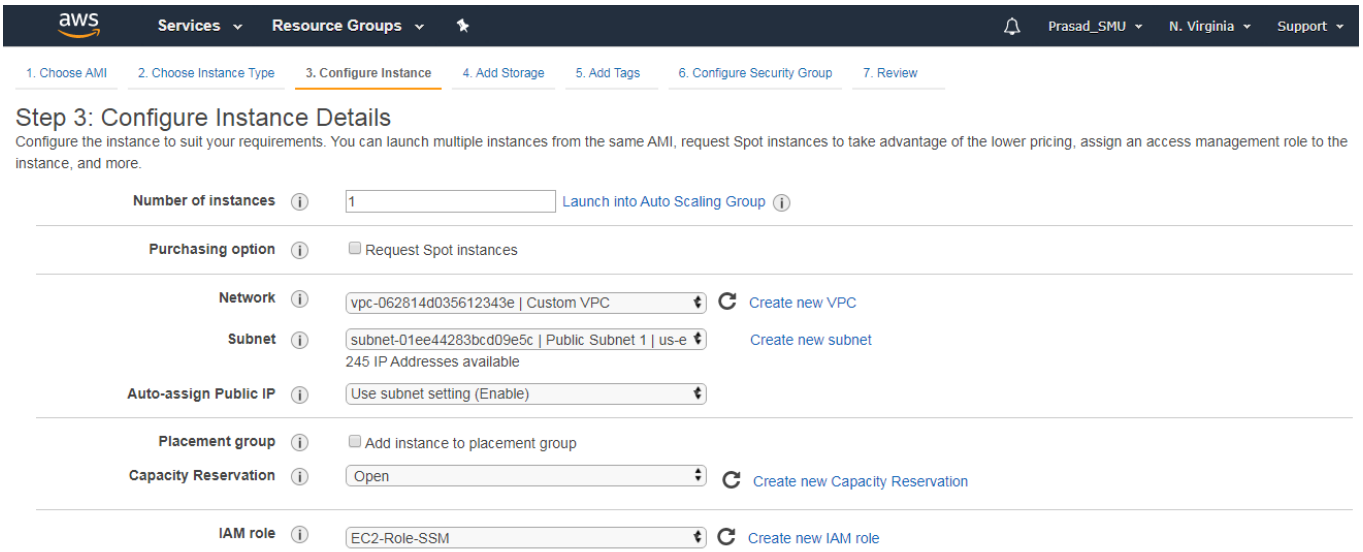
Login to the AWS Management Console.

Navigate to EC2 Service and click on Launch Instance.

Select the **Amazon Linux AMI**.



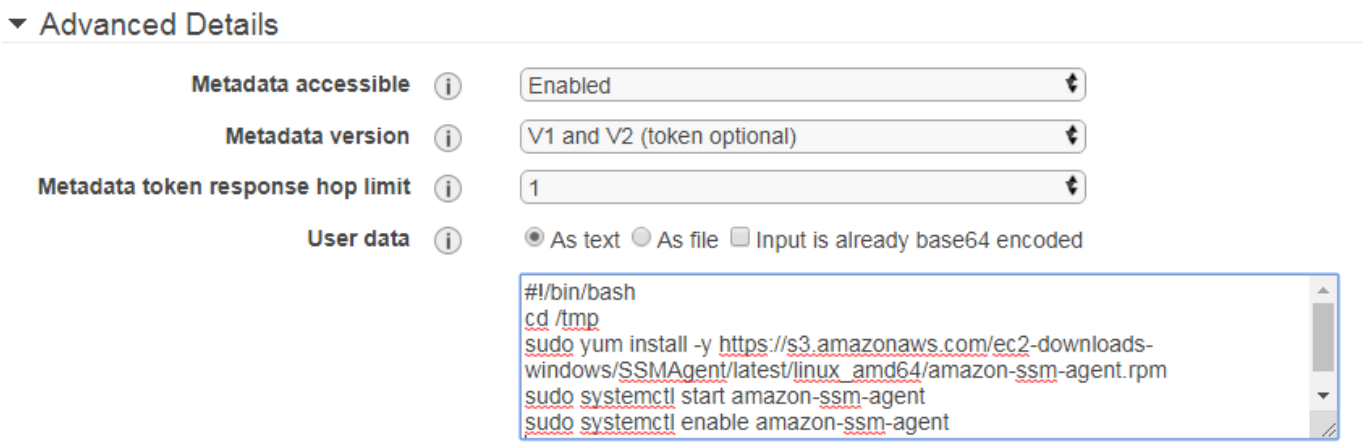
Select the Number of Instances as 1, select the Network as our Custom VPC, Select Subnet as Public Subnet 1 and select the IAM Role which you configured in the Task 1.



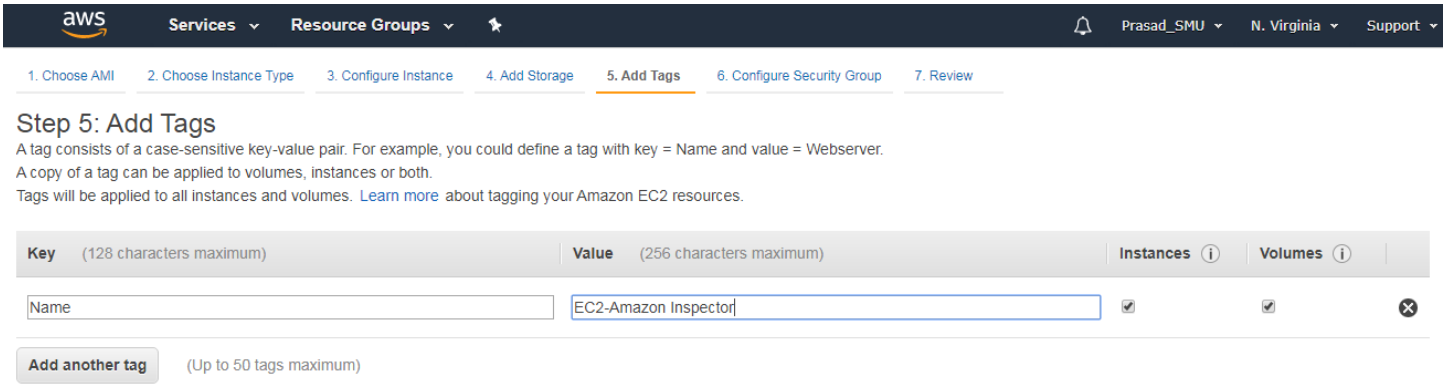
Since AWS Systems Manager is AGENTLESS, we need to install Packages for Systems Manager (SSM) to connect with Target Instances.

Scroll down on the same page, click on Advanced Details and in User Data field bootstrap the below commands.

I've provided the Commands in text file.

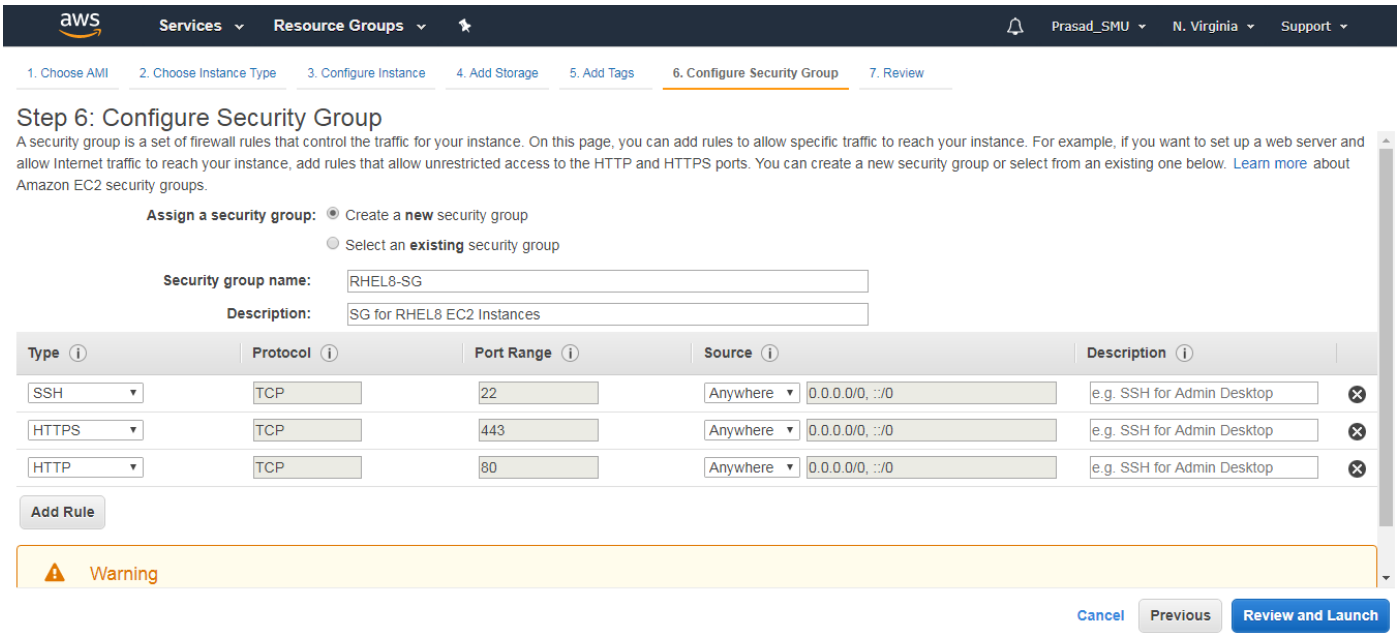


You can mention Tags as per your choice.



Click Next: Security Groups.

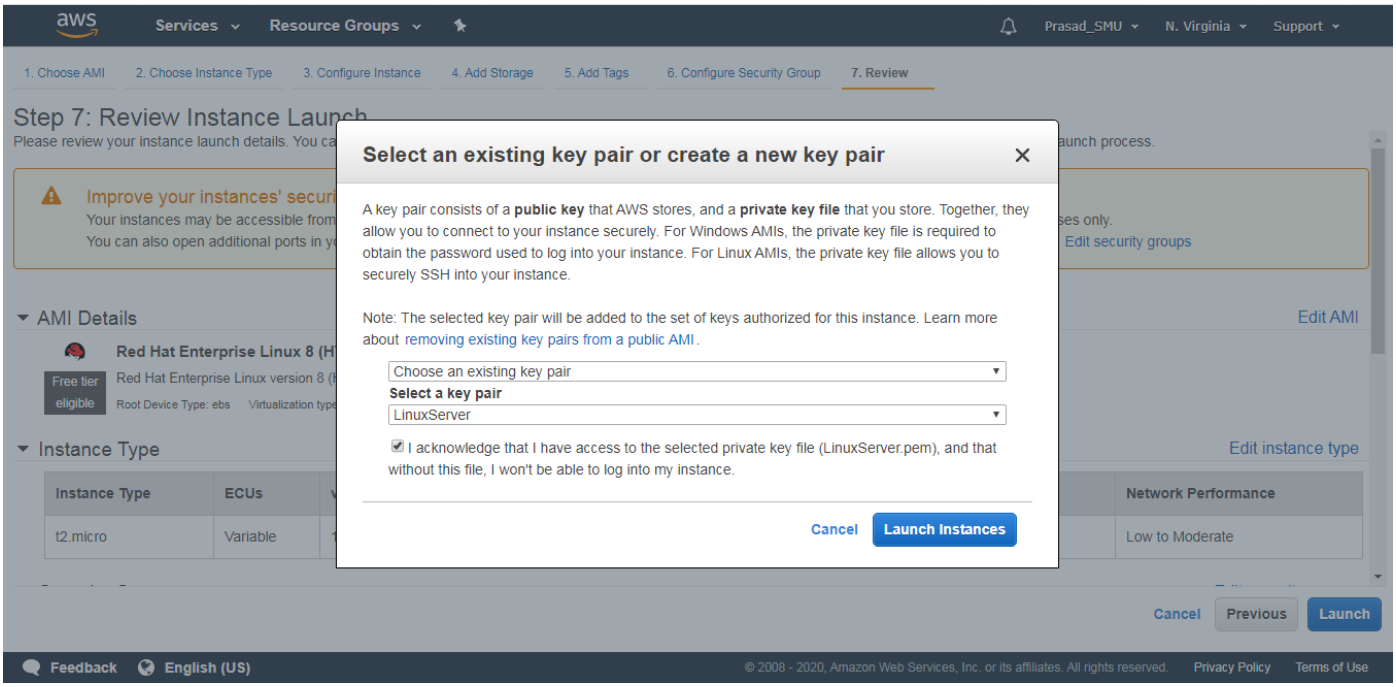
Create a new Security Group. Give the Name & Discription as per your choice. Allow SSH, HTTPS, HTTP Inbound traffic from Anywhere.



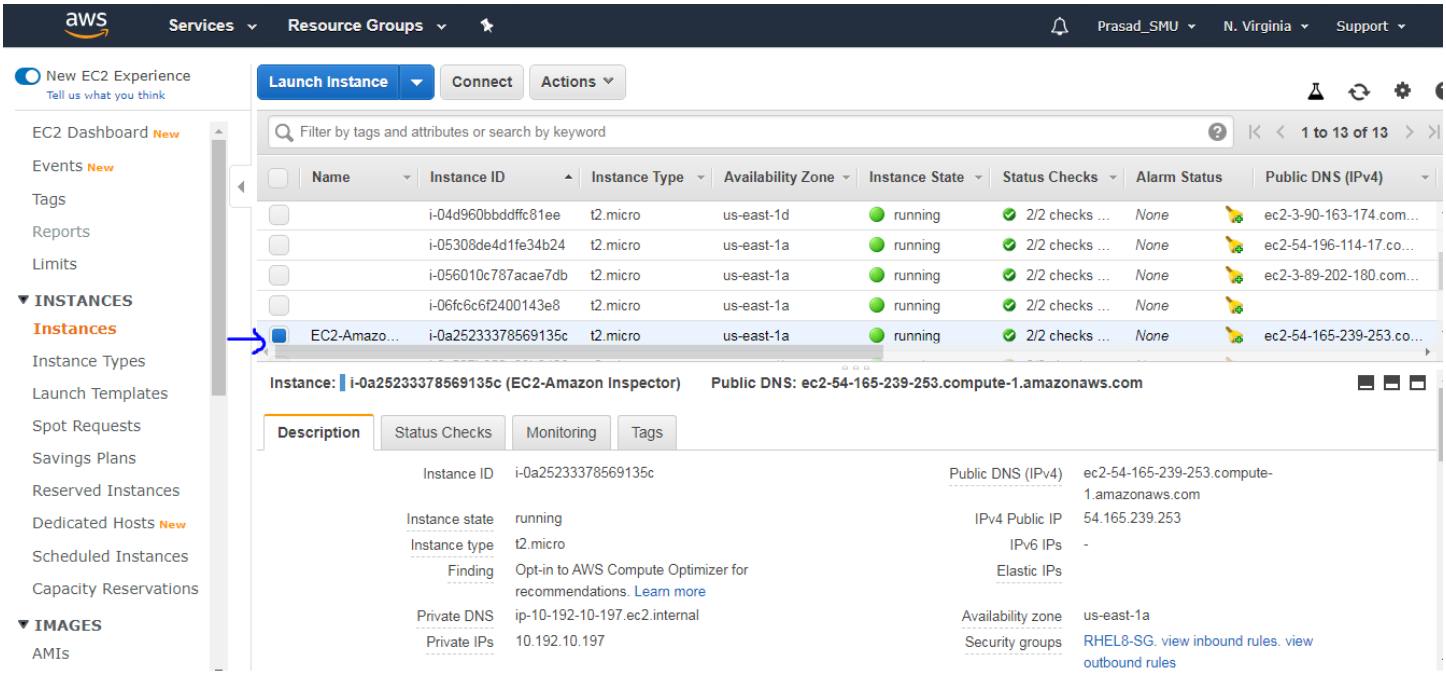
Click on Review and Launch.

Select the existing Key Pair which you've using for previous labs.

Click on Launch Instances.

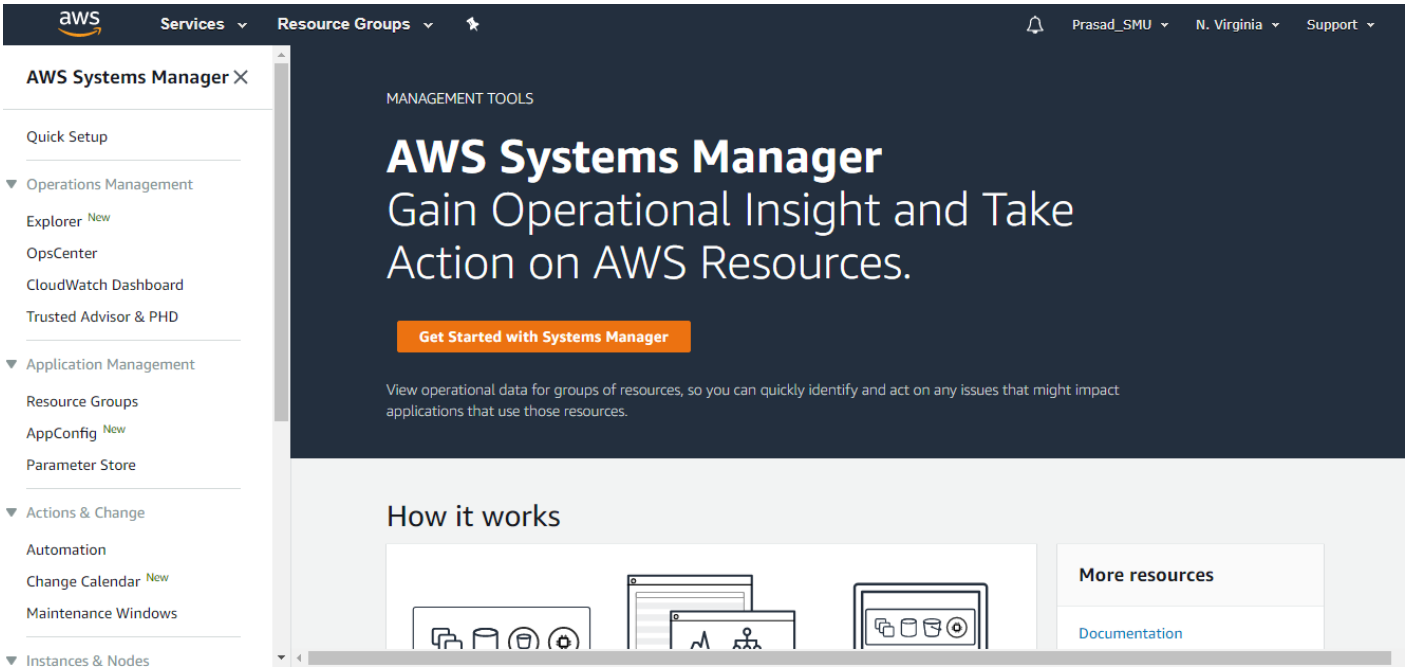


You can see that the Highlighted Instance has been launched Successfully!!!!!

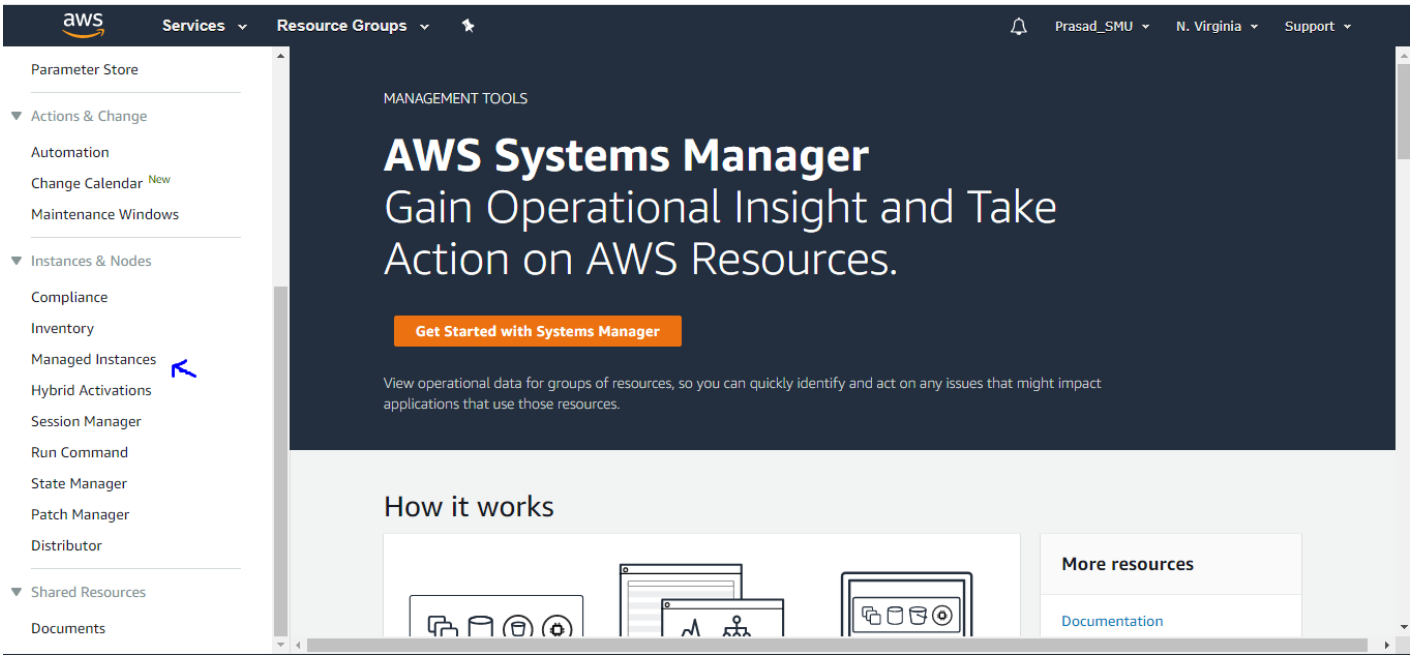


Task 3: AWS Systems Manager: Managed Instances

Navigate to AWS Systems Manager Service.

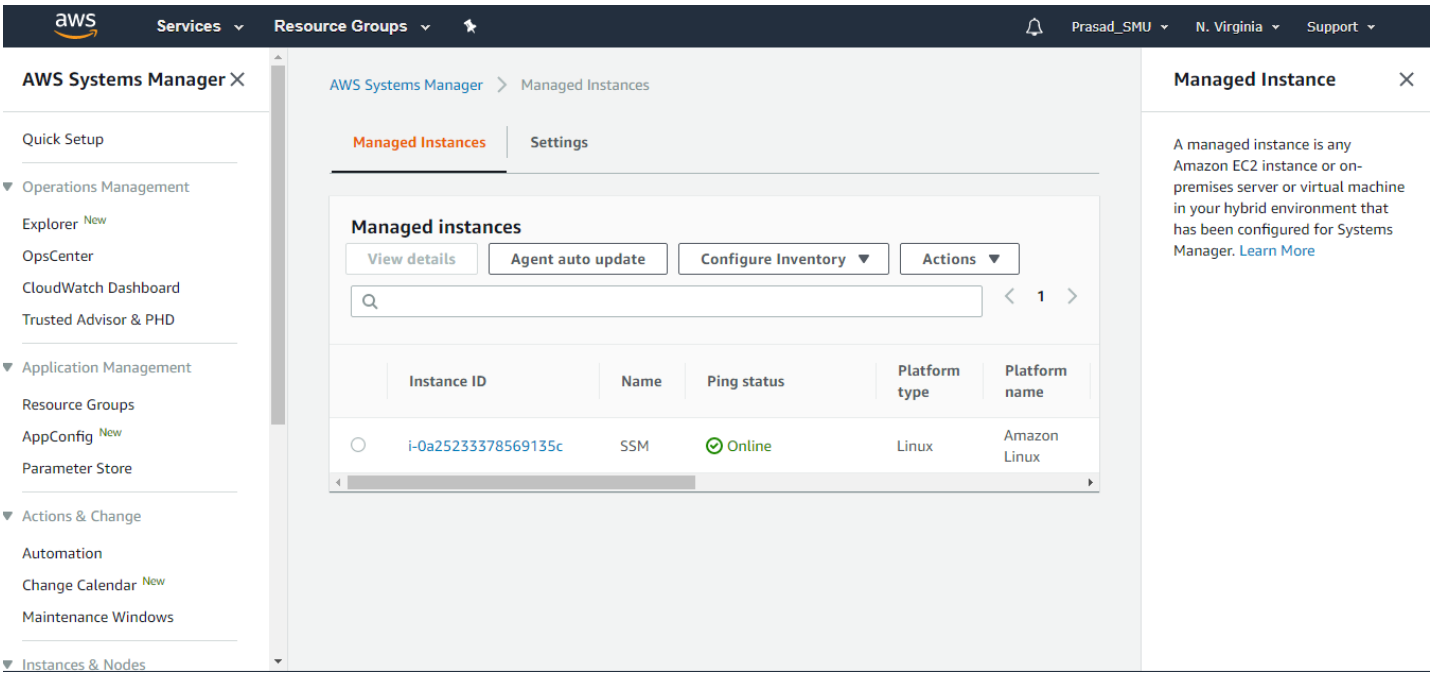


One the left-hand side, click on Managed Instances.

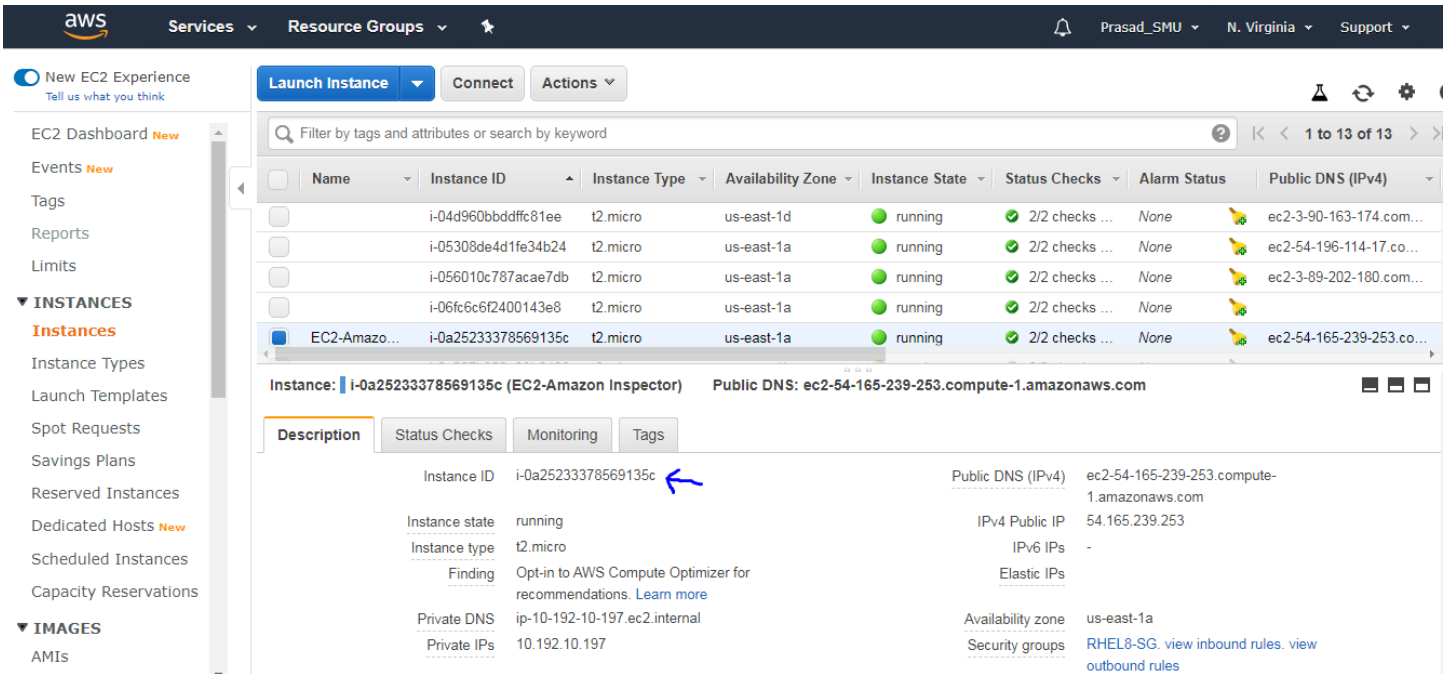


You should see the Instance which we launched in Task 2.

If you do not see any Instance in Managed Instances tab, it means Systems Manager Agent is not Installed on the EC2 Instance.

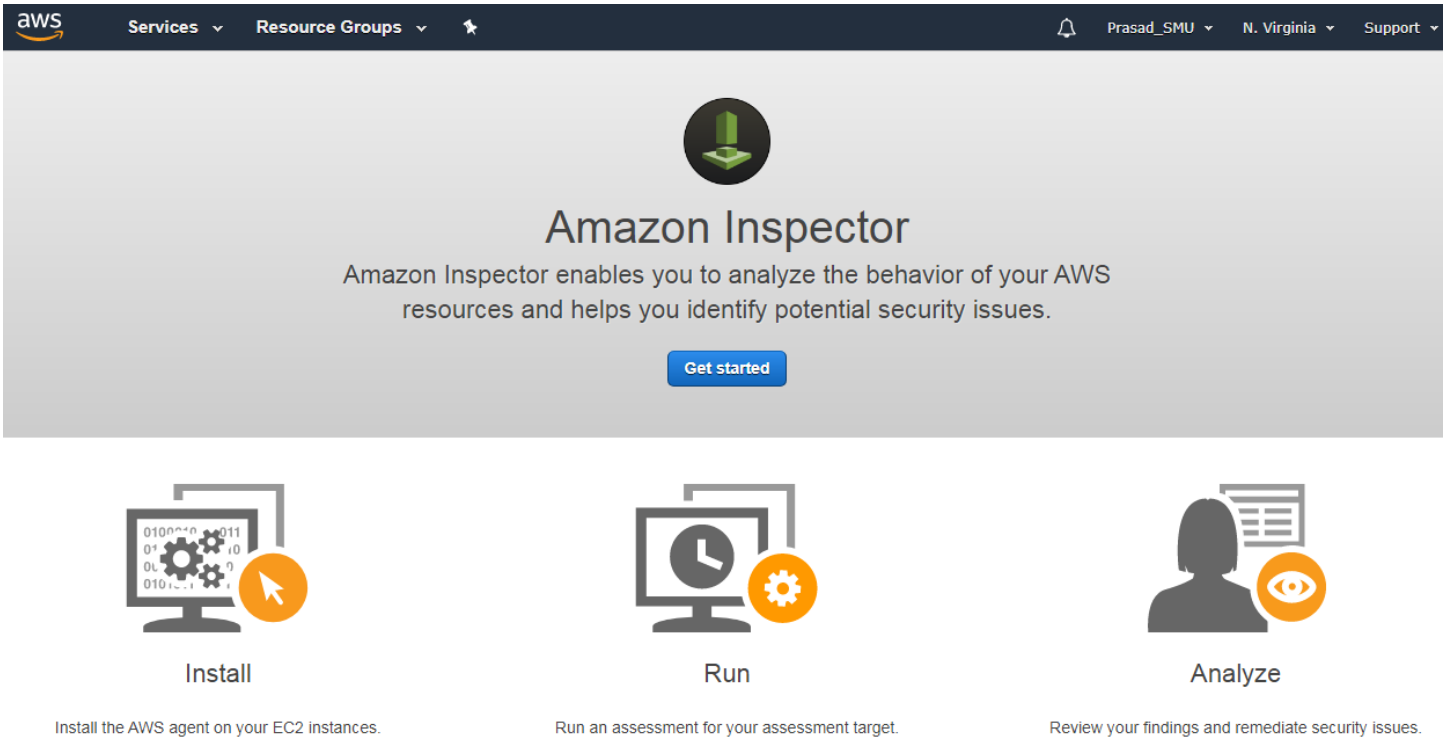


You can also verify the Instance IDs from EC2 Service Dashboard.

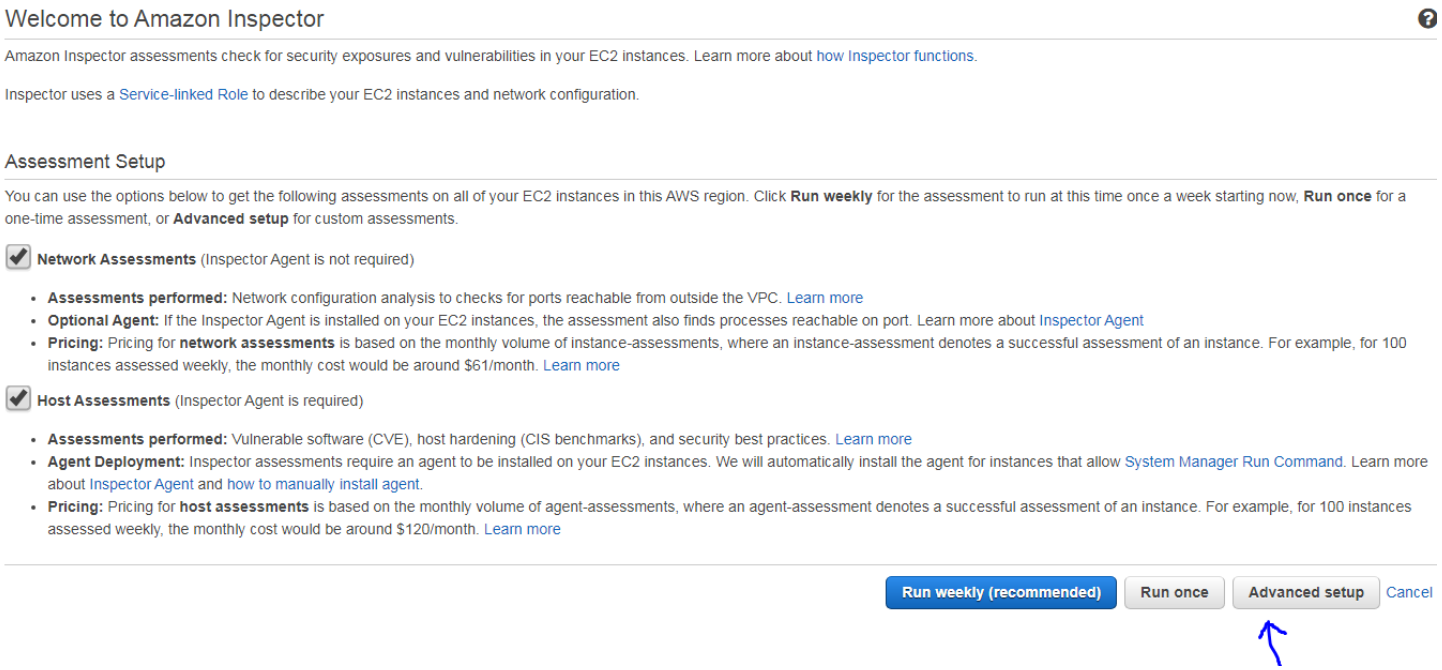


Task 4: Amazon Inspector Configurations

Navigate to Amazon Inspector Service.



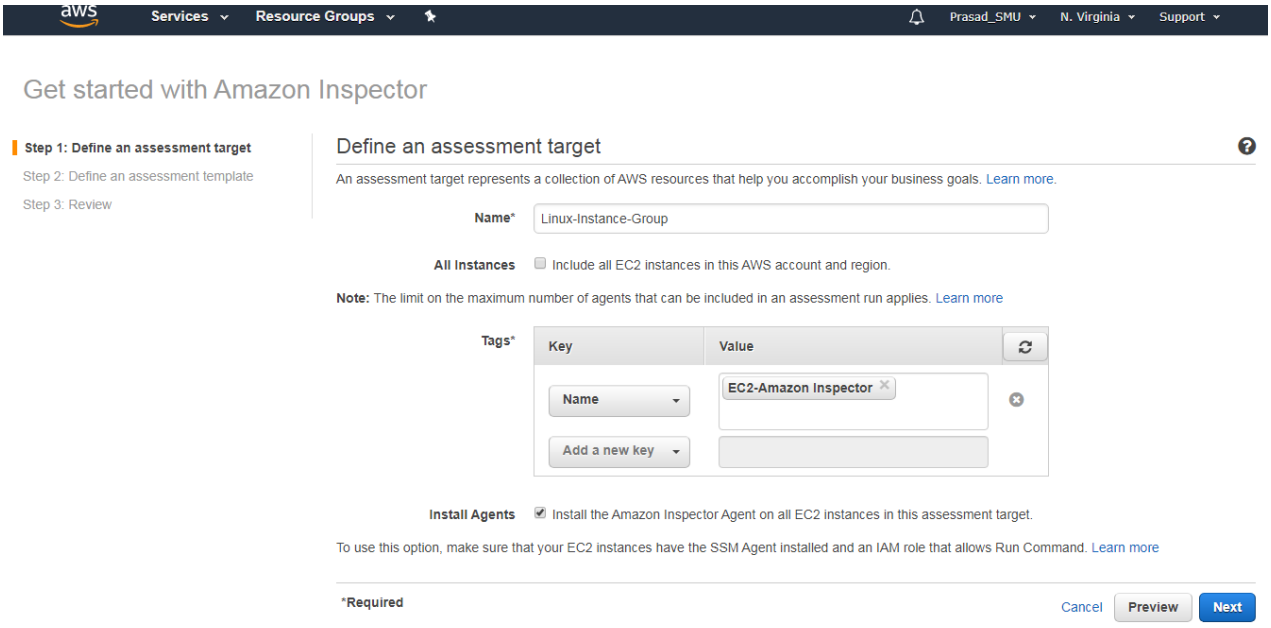
Go ahead and click on Get Started. Click on Advanced Setup.



Give the Assessment Target Name as per your choice.

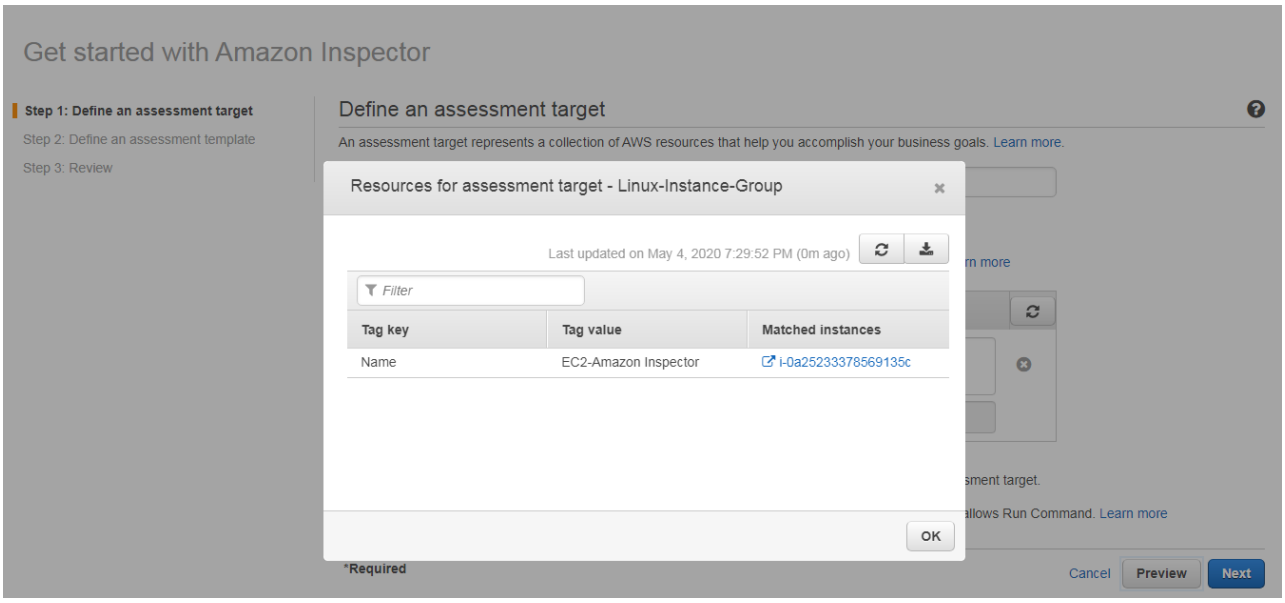
Unselect the All Instances and specify Tag of your EC2 Instance.

Check on Install Agents. Amazon Inspector will now Install Amazon Inspector Agent on Target Instances using Systems Manager Service-Run Command.



Click on Preview. You should see the Instance which you've configured in Task 2.

You can also verify the Instance ID from the EC2 Service Dashboard.



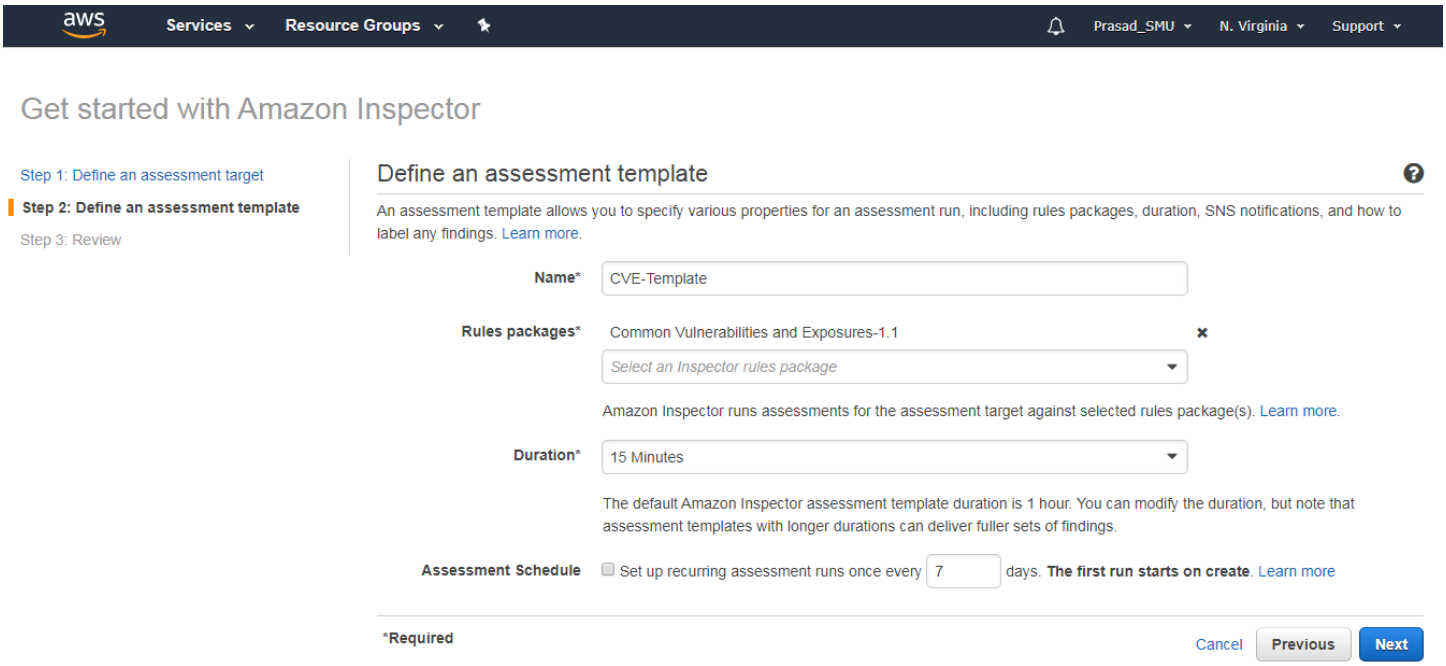
Click on Next.

Give the Assessment Template Name as CVE-Template.

Remove all the existing Rule Packages & from the dropdown select the **Common Vulnerabilities and Exposure-1.1** Rule Package.

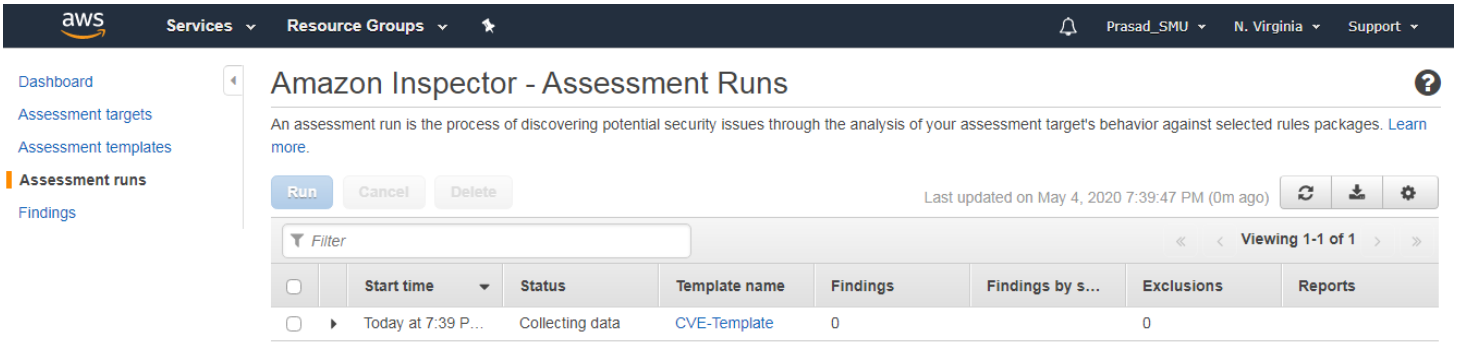
Set the scan duration to 15 Minutes. Amazon Inspector will scan the Target Instances for every 15 Minutes to detect the Vulnerabilities.

You can also set up the recurring schedule if you want. Click Next.



Finally review the configurations and click on Create.

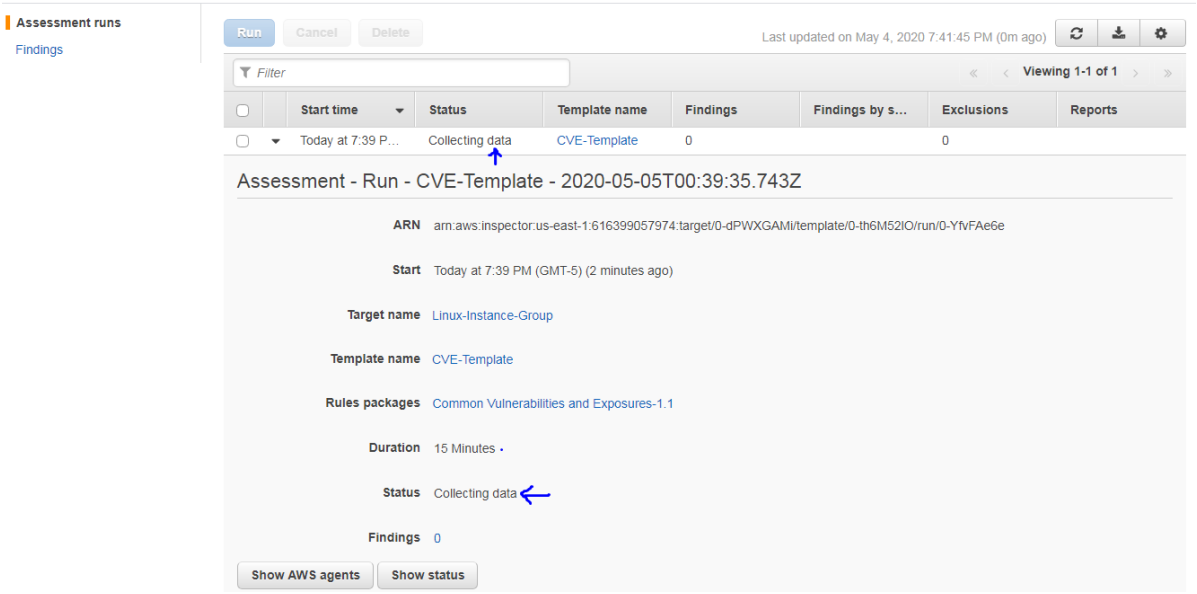
Assessment has been deployed successfully.



Click and expand the current Assessment.

You'll notice that the Scanning for the Vulnerabilities on the EC2 Instance has been started automatically. You can see the scanning Status as **Collecting Data**.

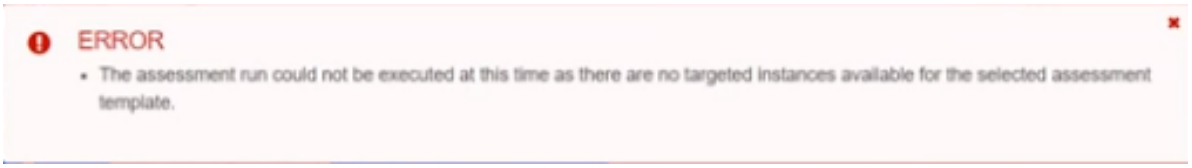
The entire scanning process will take approximately 15-30 Minutes.



Task 5: Amazon Inspector-Troubleshooting

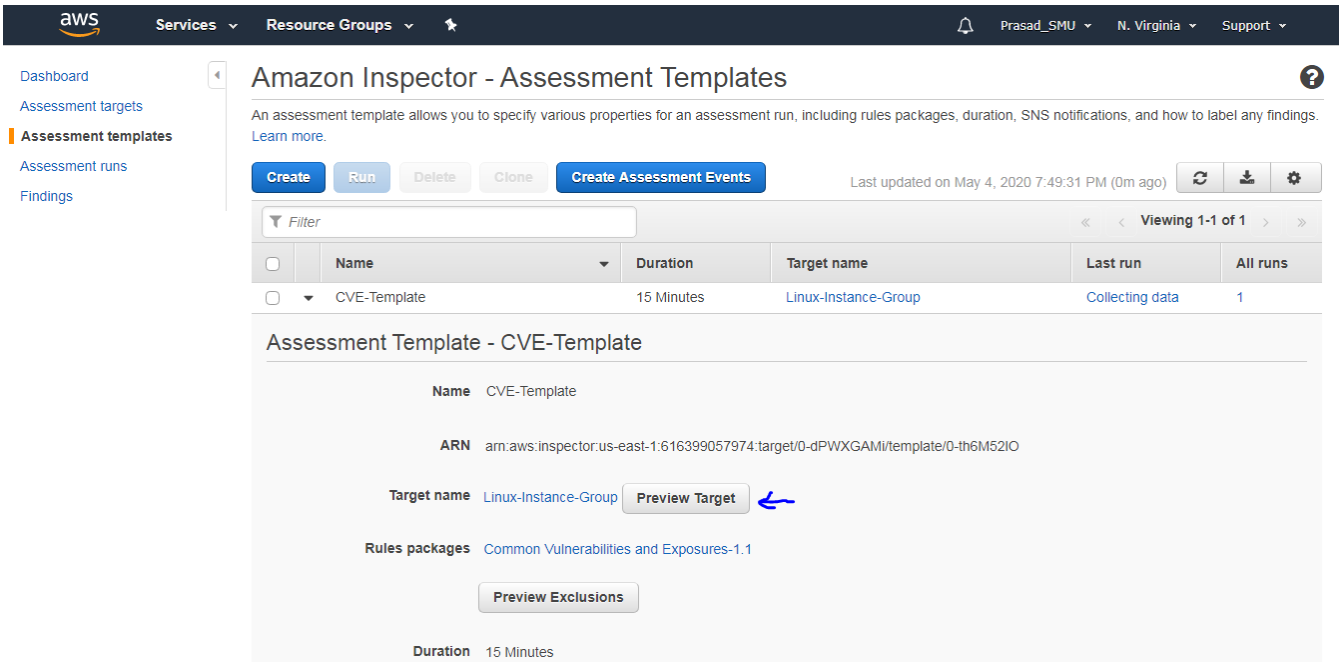
In some cases, the Inspector Agent may not get installed on the Target Instances successfully.

In-such cases, if you Run the Scanning Process, you may get the below error message.

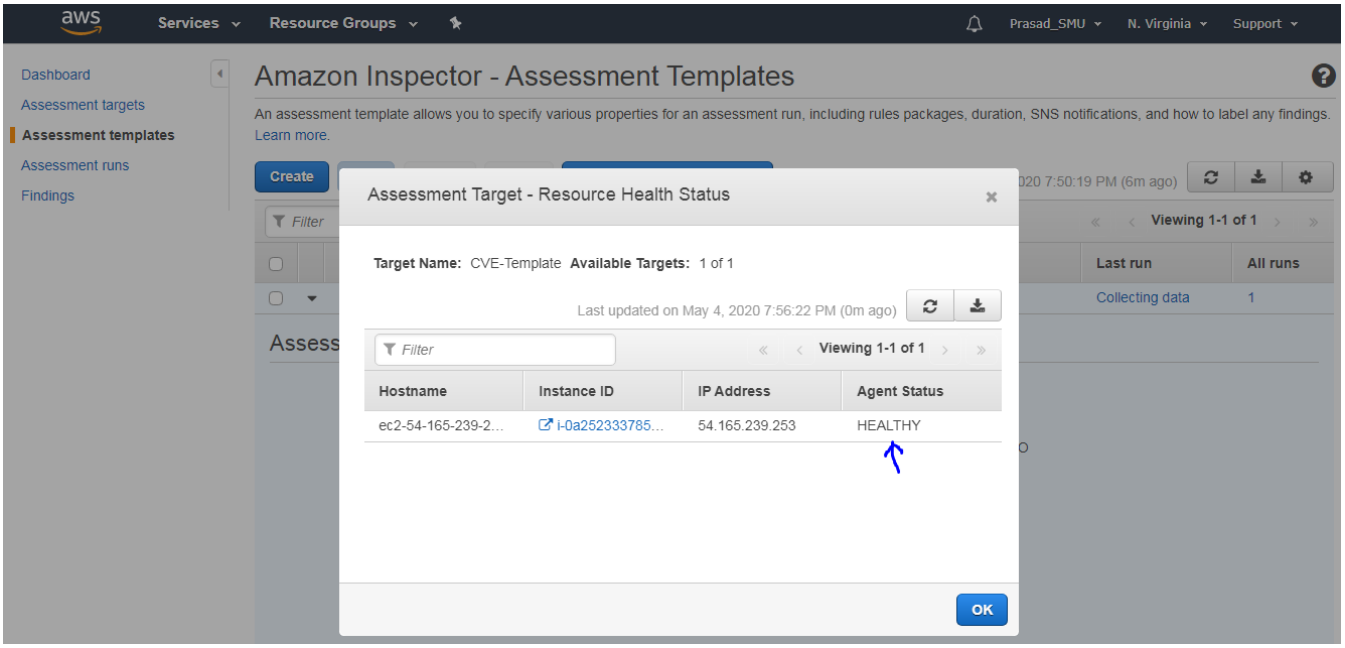


In this case, on the right-hand side, click on Assessment Template.

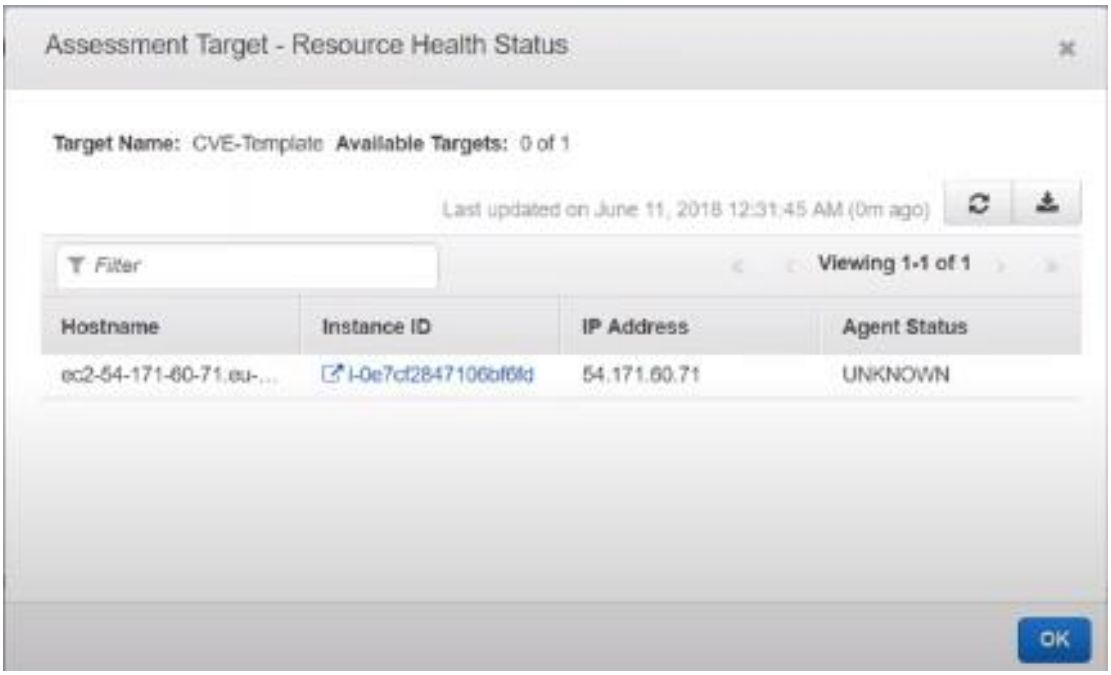
Expand the Assessment Template and click on Preview Targets.



Agent Status is currently Healthy, you do not have to worry about it.



But in-case of above error, the Agent Status will be Unknown.

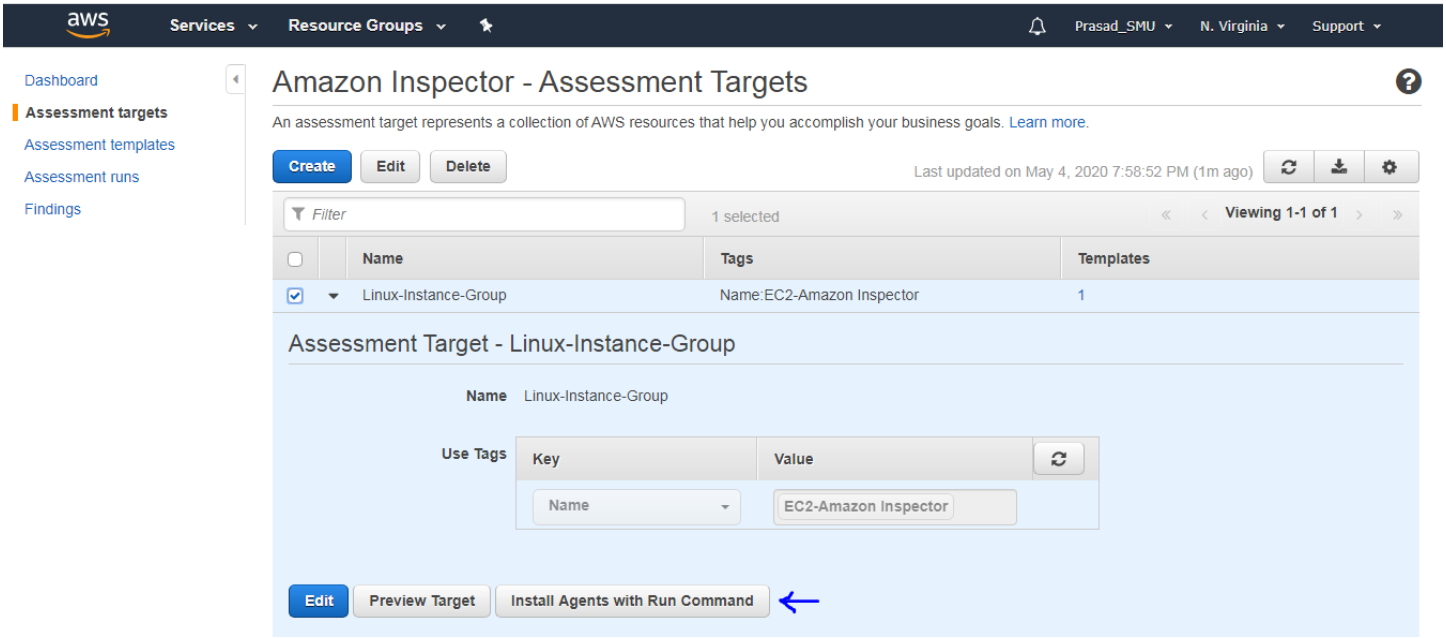


If the Agent Status is Unknown, then it is possible to Install the Inspector Agent Remotely on the EC2 Instances.

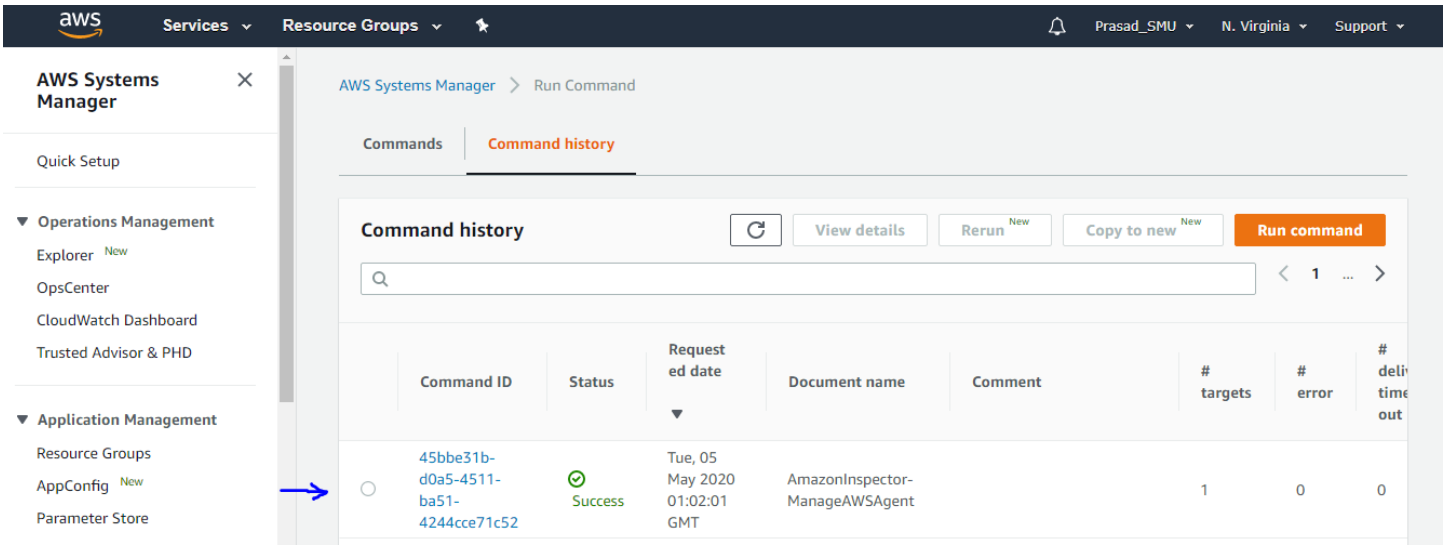
On right-hand side. Click on Assessment Targets.

Select the Assessment Target and click on **Install Agents with Run Command**.

This will Install the Amazon Inspector Agent on EC2 Instances remotely.



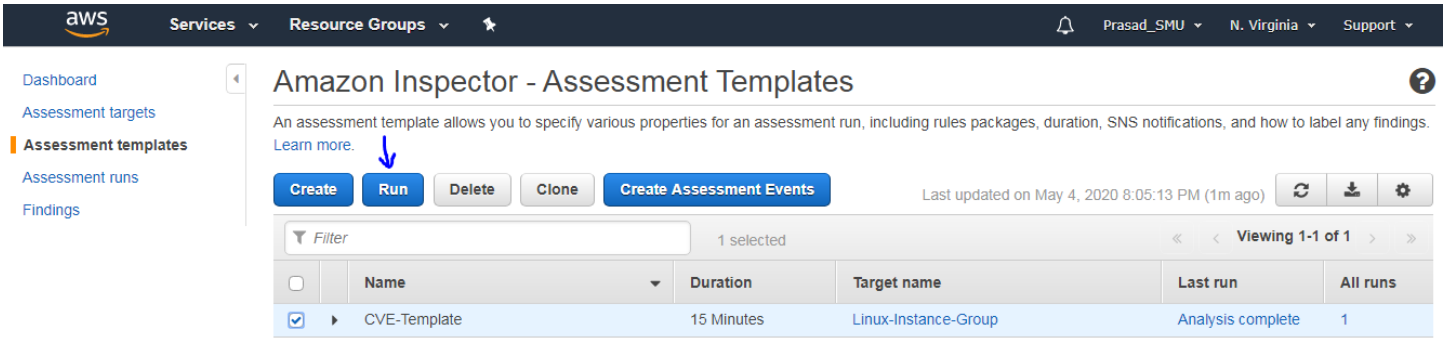
Now if you navigate to AWS Systems Manger Service, click on Run Command and click on Command History, you'll observe the Command has been executed successfully.



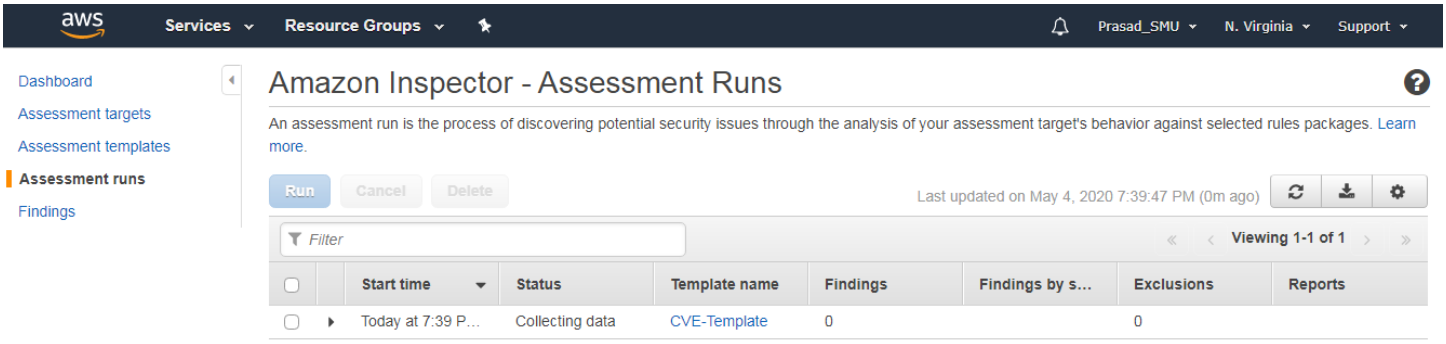
Now if you click on Assessment Template, expand the Assessment Template and click on Preview Targets, the Agent Status will be HEALTHY.

Now again click on Assessment Templates.

Select the Template and click on Run.

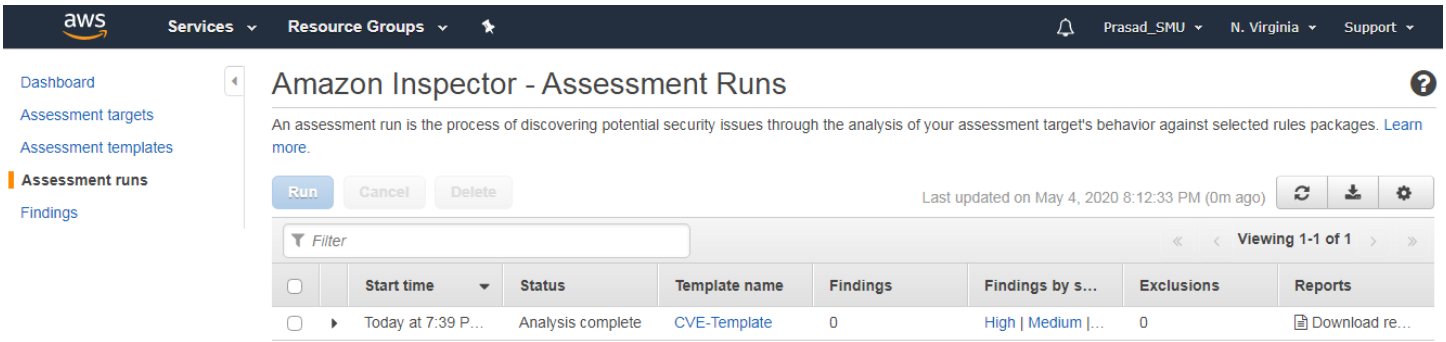


Scanning Process will get started.



Task 6: Amazon Inspector-Findings

Now you can see that the Assessment analysis has been completed.

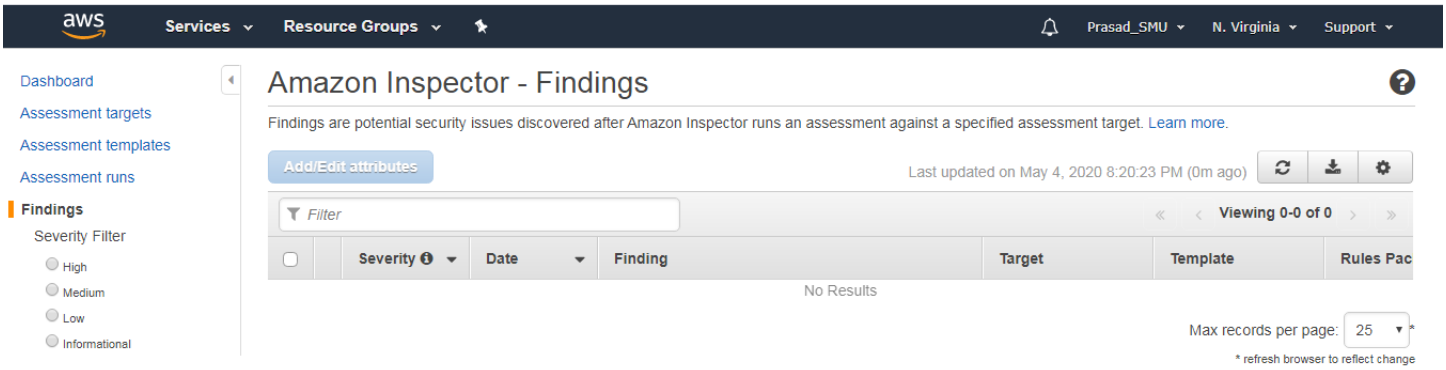


You can download the Vulnerability Report if you want.

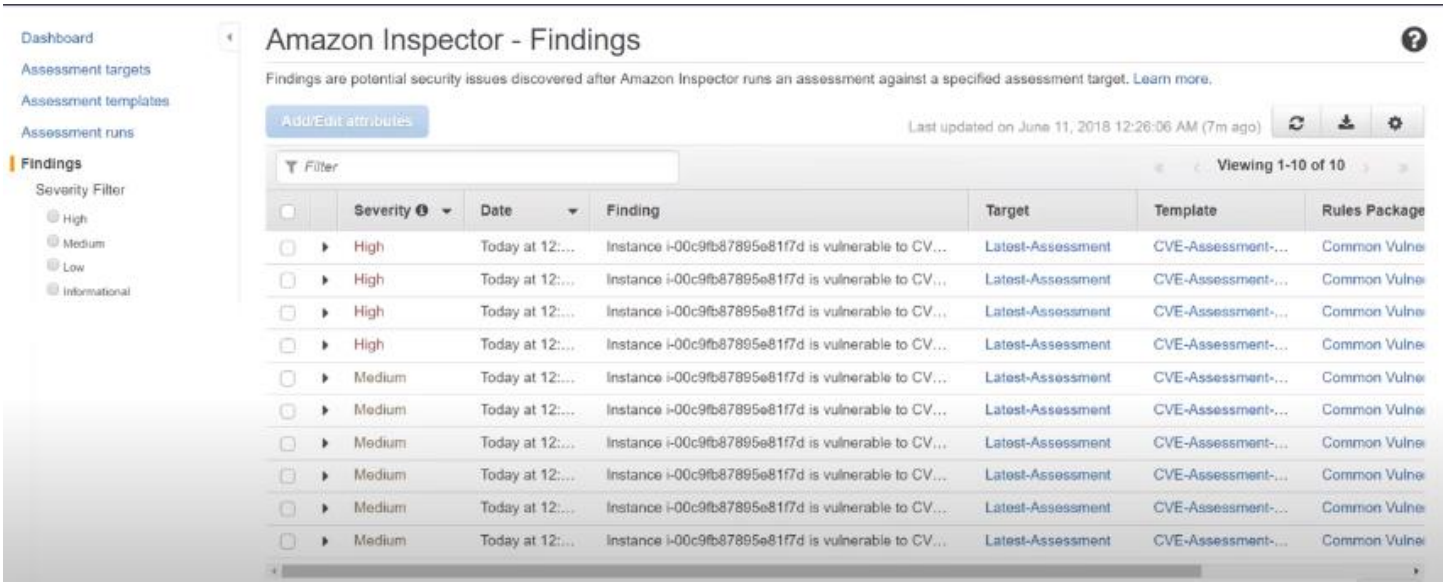
Now click on Findings.

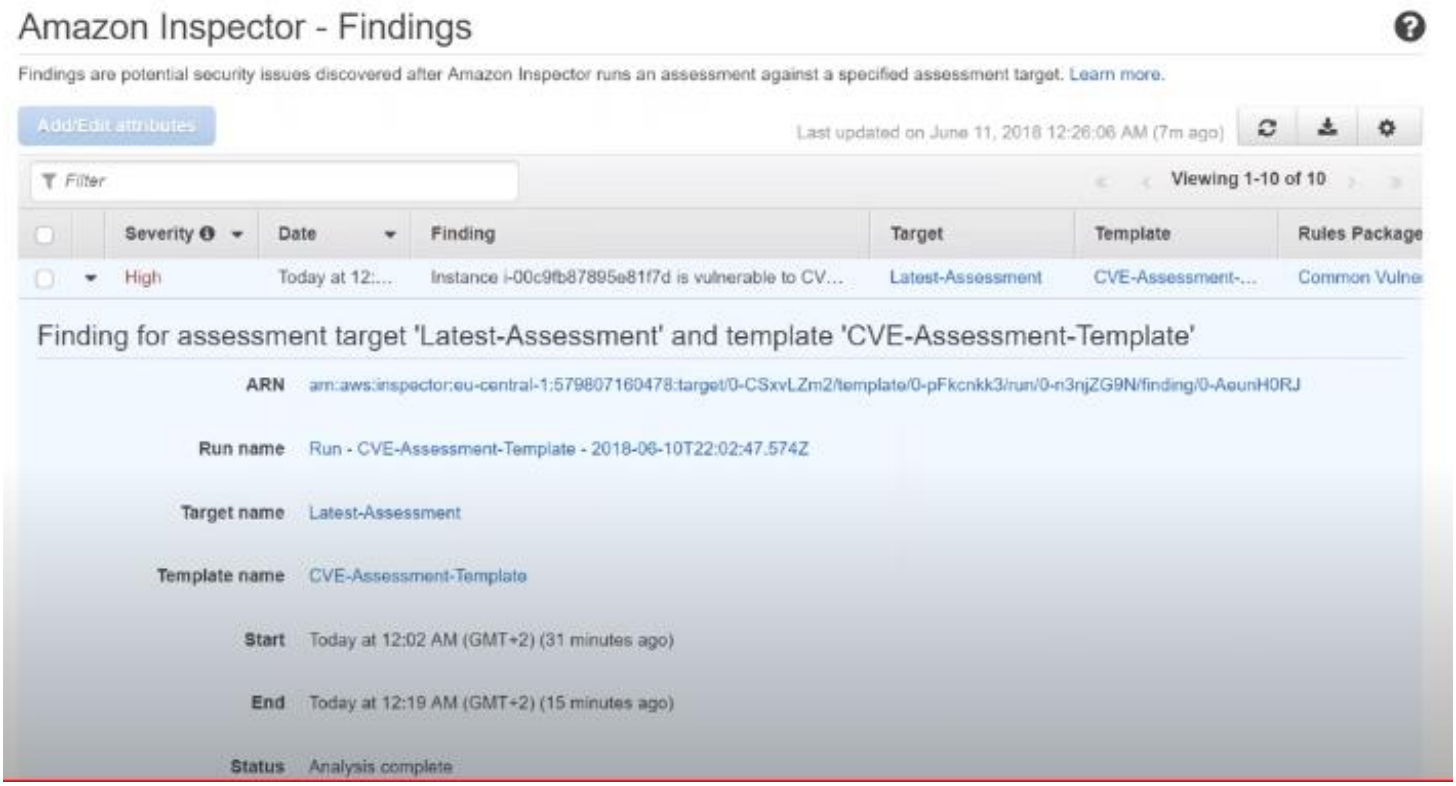
You'll observe the list of Vulnerability exists in your EC2 Instance.

I do not have any findings for my EC2 Instance, it means my EC2 Instance is 0% vulnerable and highly secured.



Below is the list of Findings & example of Amazon Inspector Finding which provides Description of the Vulnerability and Steps or recommendations to remove the **Vulnerability**.





Target name	Latest-Assessment
Template name	CVE-Assessment-Template
Start	Today at 12:02 AM (GMT+2) (31 minutes ago)
End	Today at 12:19 AM (GMT+2) (15 minutes ago)
Status	Analysis complete
Rules package	Common Vulnerabilities and Exposures-1.1
AWS agent ID	i-00c9fb87895e81f7d
Finding	Instance i-00c9fb87895e81f7d is vulnerable to CVE-2018-1068
Severity	High
Description	A flaw was found in the Linux 4.x kernel's implementation of 32-bit syscall interface for bridging. This allowed a privileged user to arbitrarily write to a limited range of kernel memory.
Recommendation	Use your Operating System's update feature to update package kernel-0:4.14.33-59.37.amzn2. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1068

Show Details

This completes the Lab on AWS Security-AWS Inspector.

For questions. Contact me on pbhavsar@smu.edu .