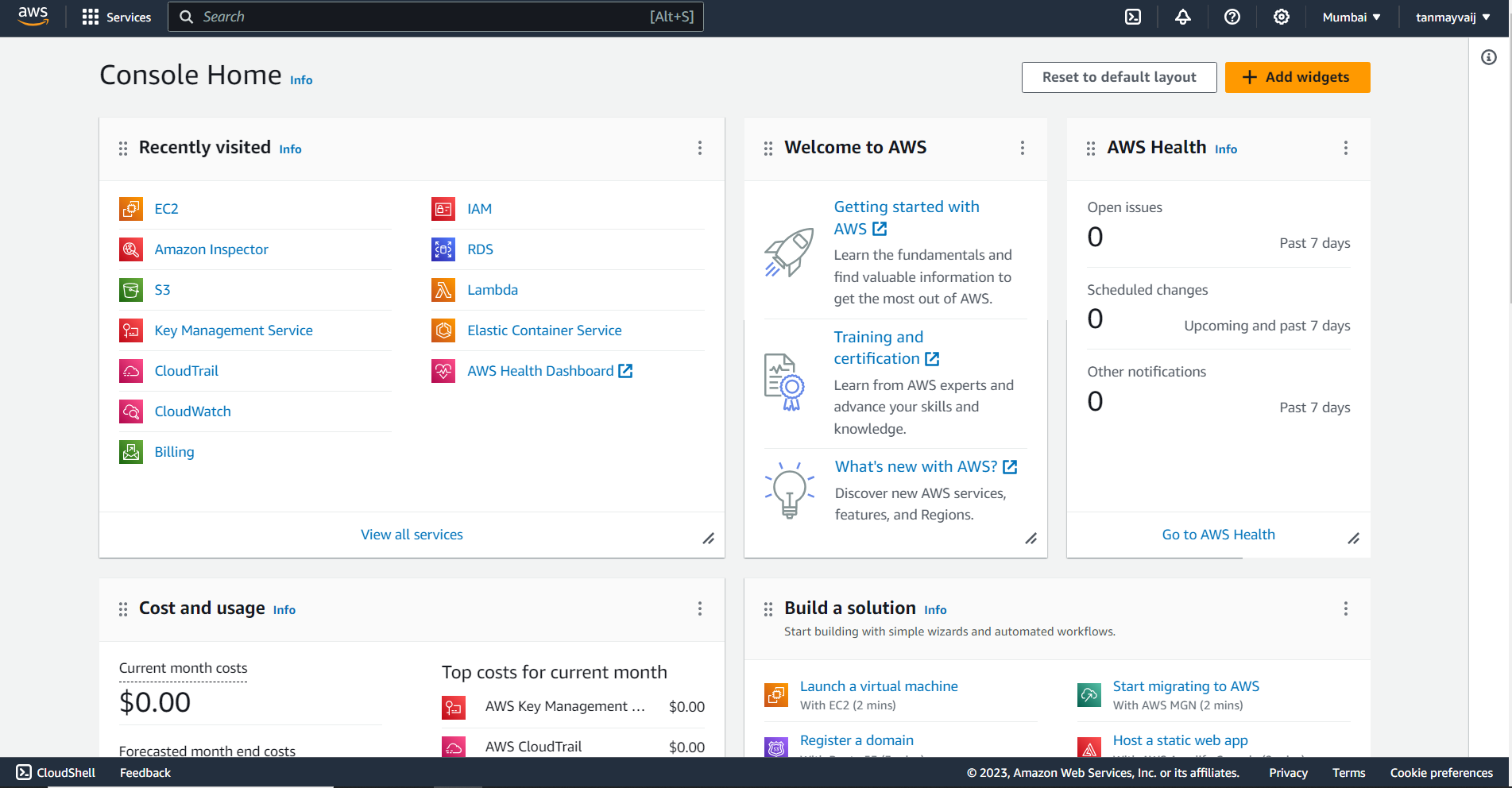
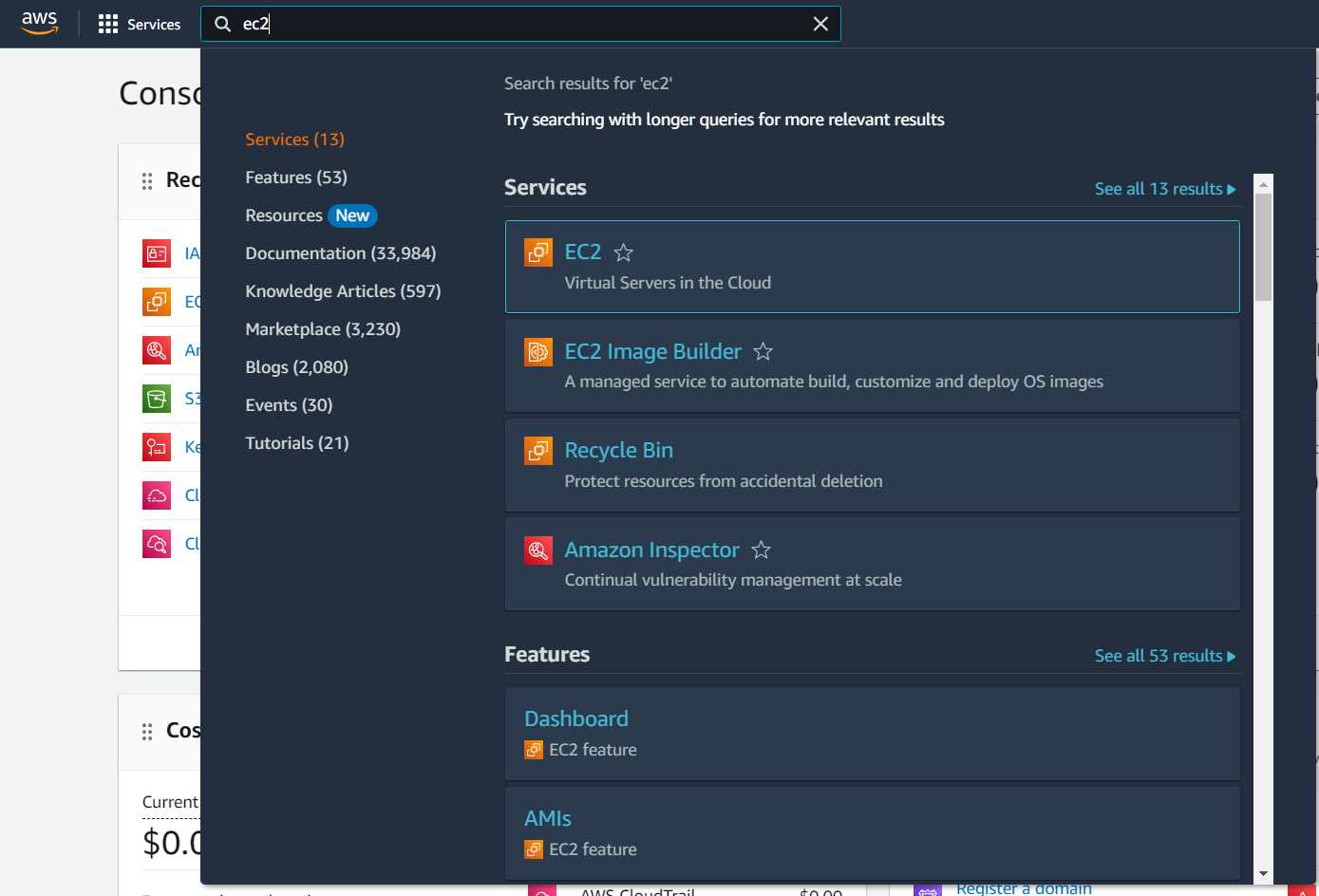
**Finding vulnerabilities on EC2 instance using Amazon Inspector**

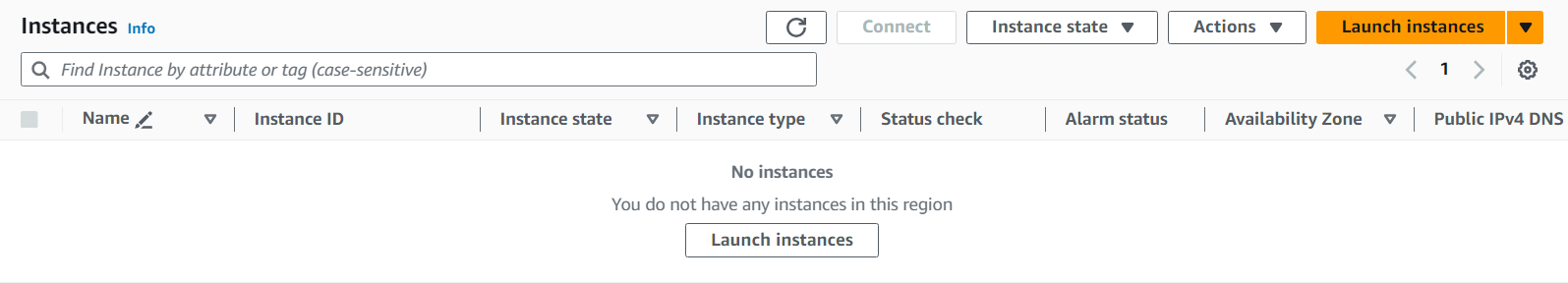
1. Sign in to AWS Console.

****

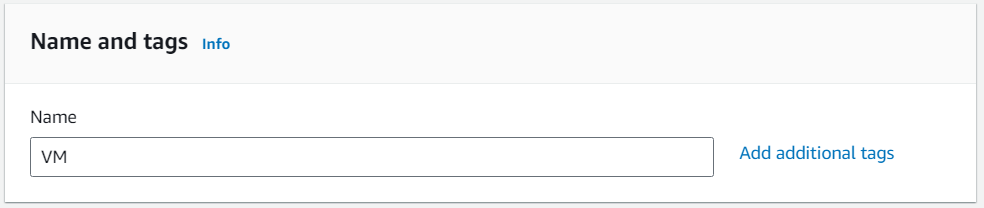
2. Search and click on Ec2.



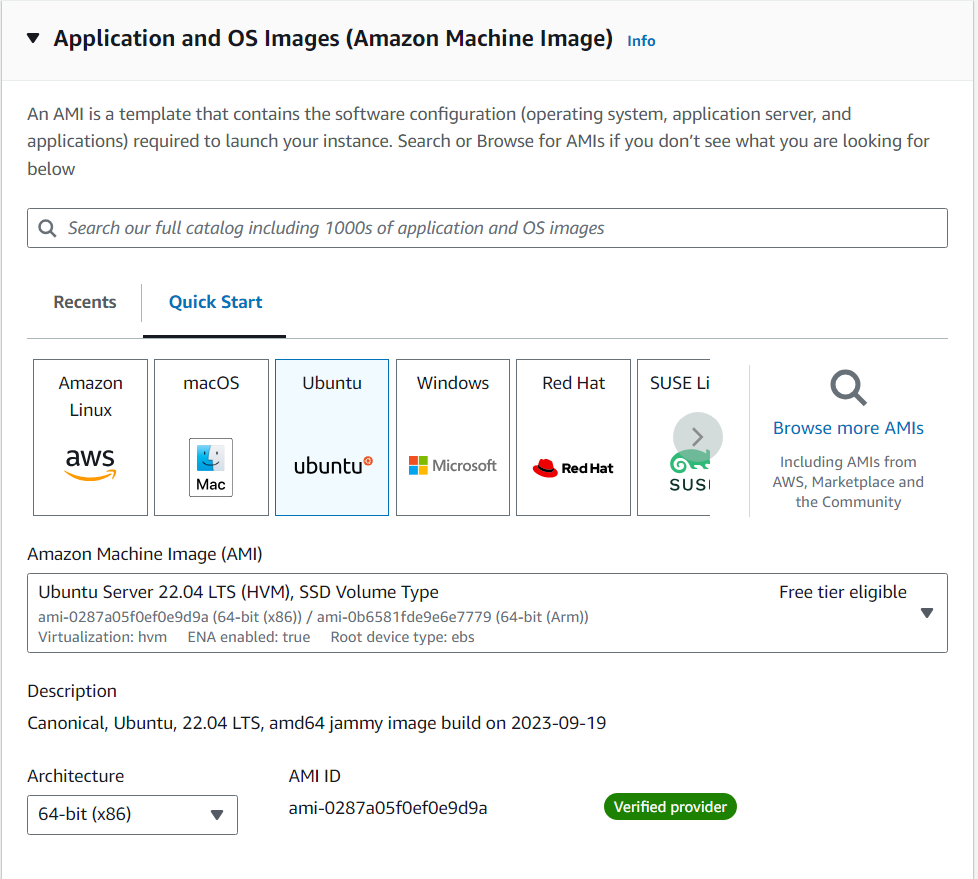
3. Click on “Launch instances”.

****

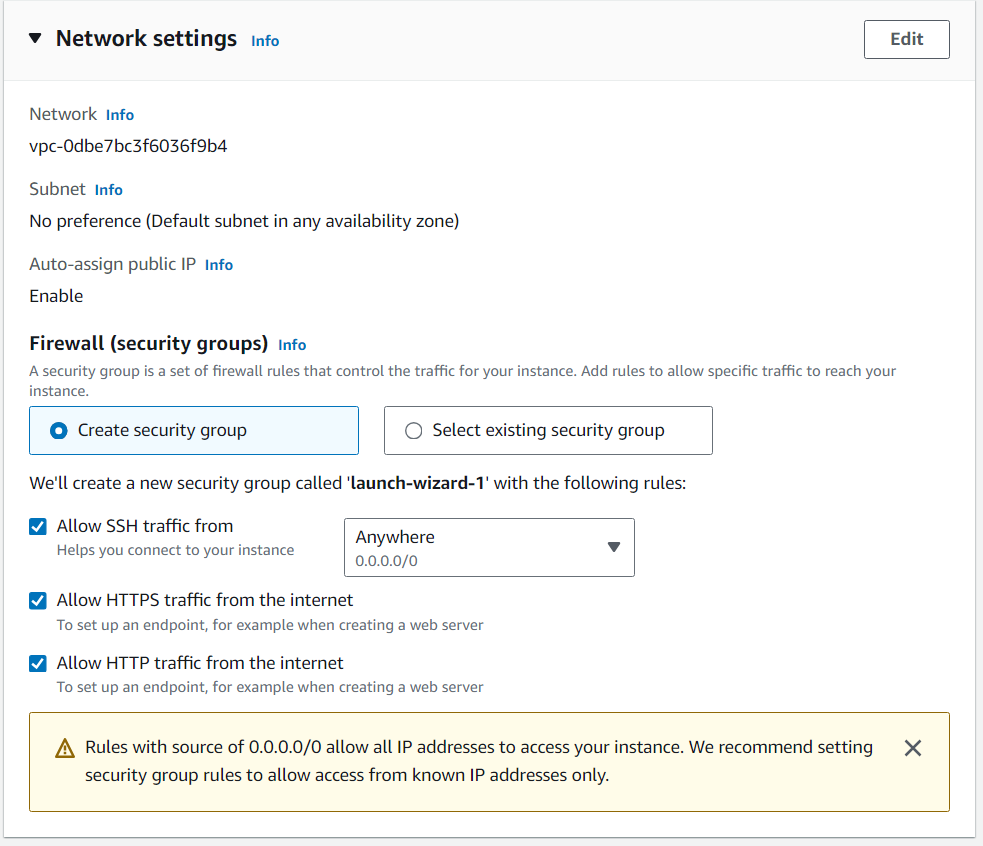
4. Give a name to the instance.

****

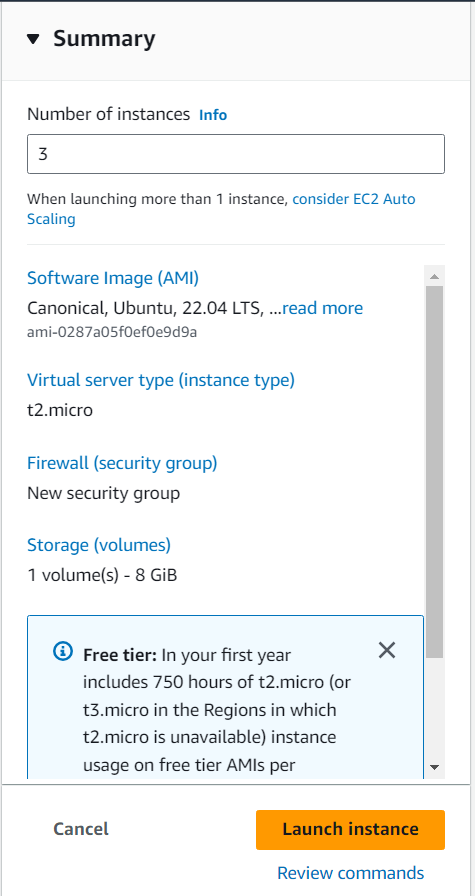
5. Select Ubuntu as the OS Image.

****

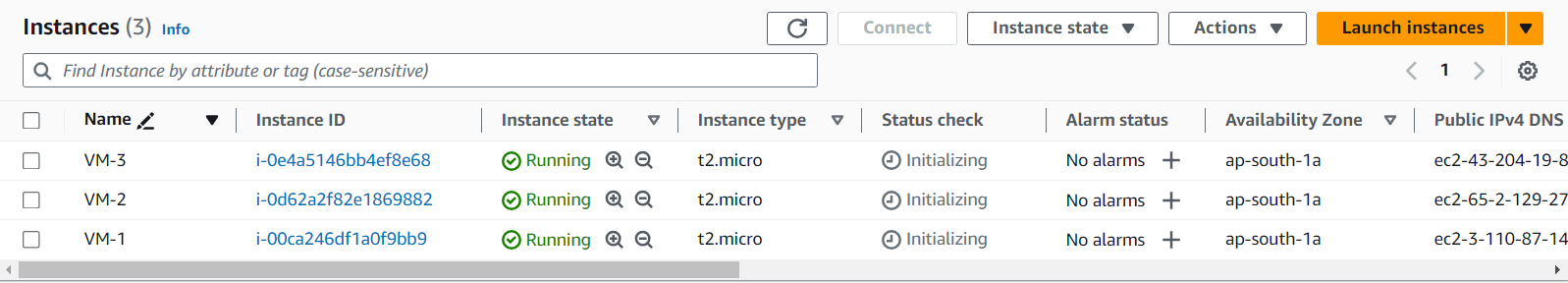
6. Create a security group or select an existing one.



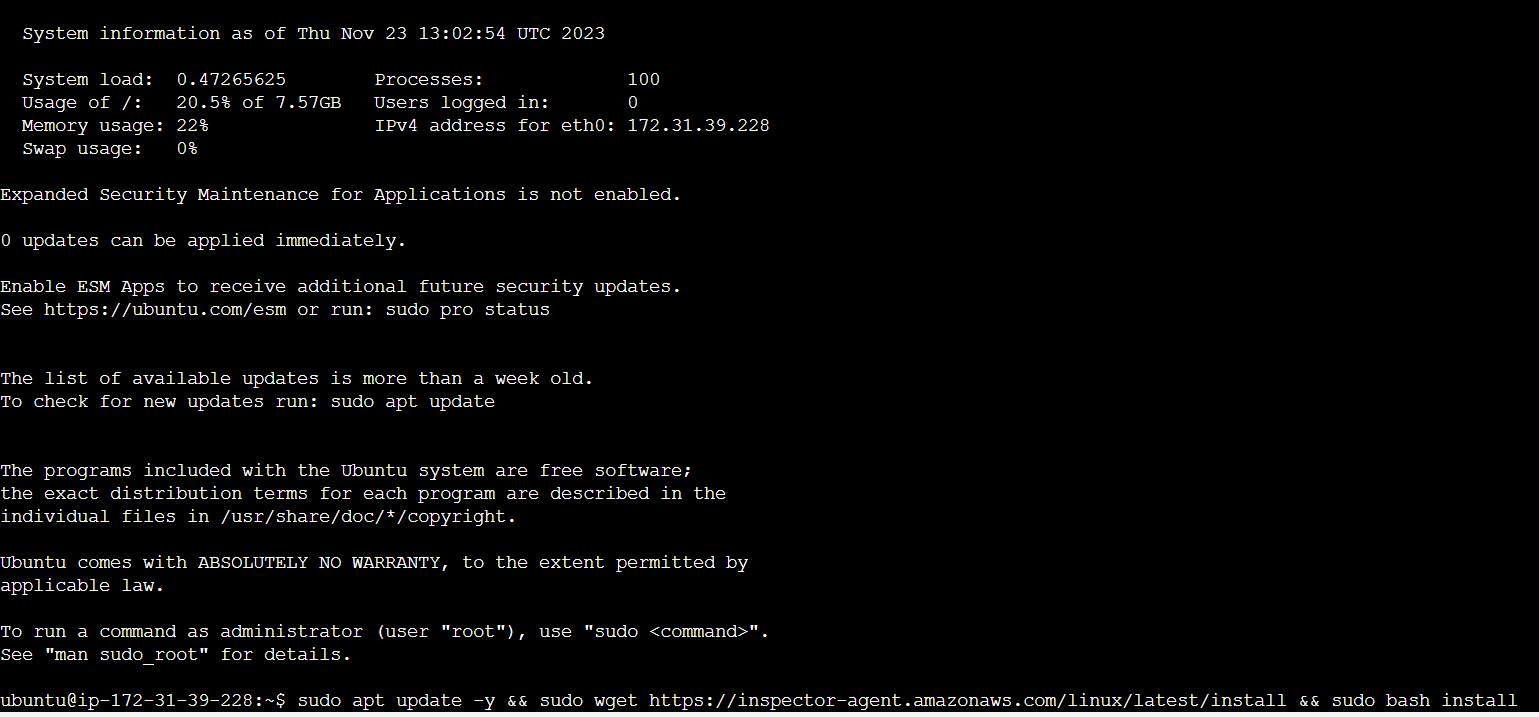
7. Set the number of instances to 3 and click on “Launch instance”.



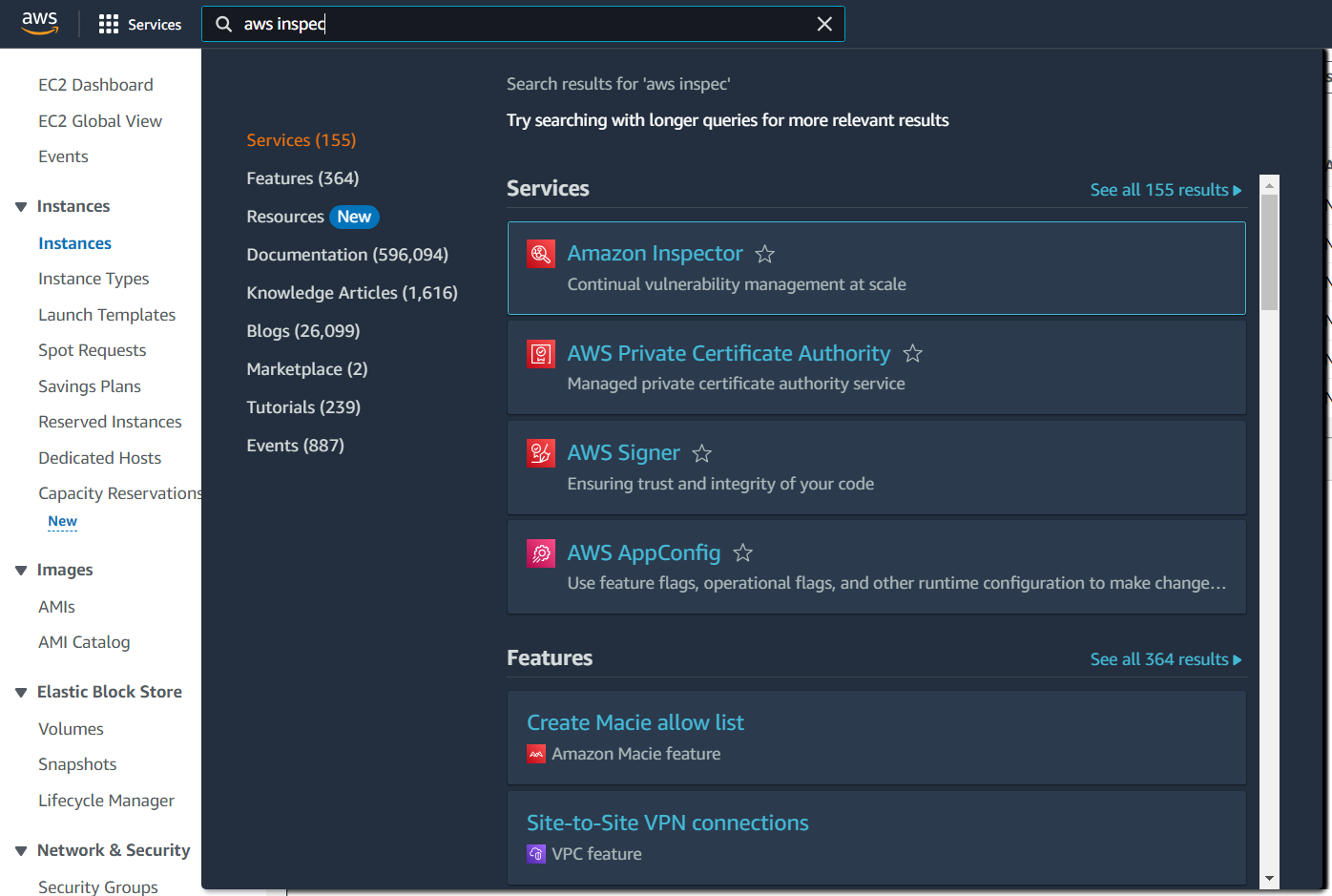
8. Rename the 3 instances to identify them uniquely.



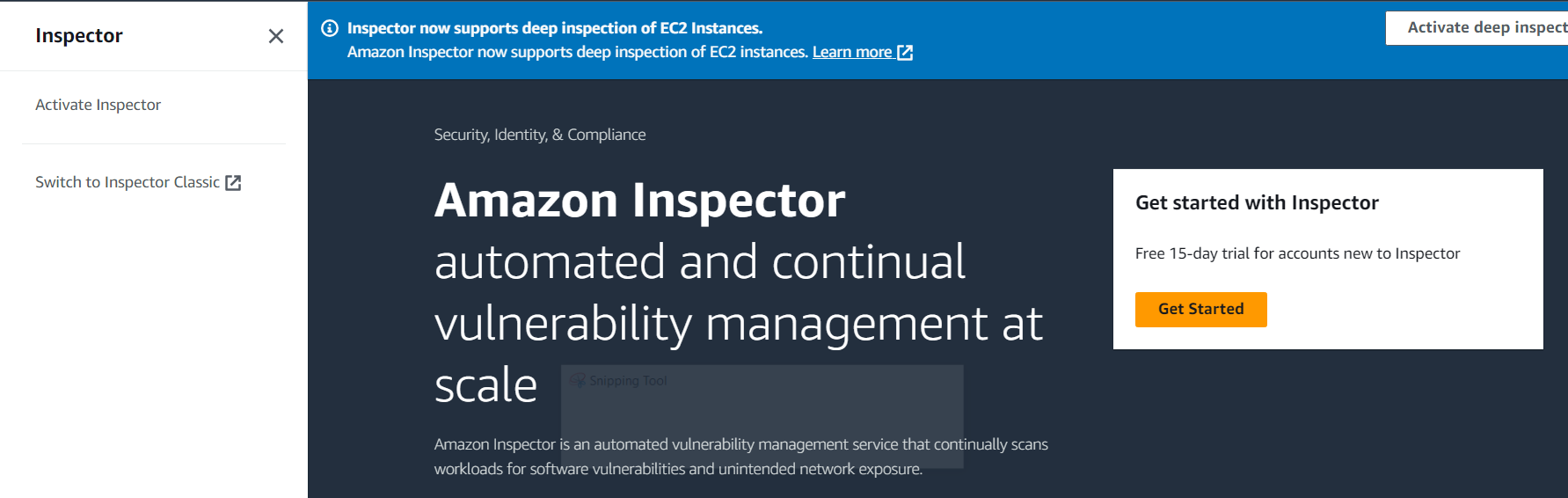
9. Connect one instance and fire the command “sudo apt update -y && sudo wget https://inspector-agent.amazonaws.com/linux/latest/install && sudo bash install”. Repeat the same for the other 2 instances.



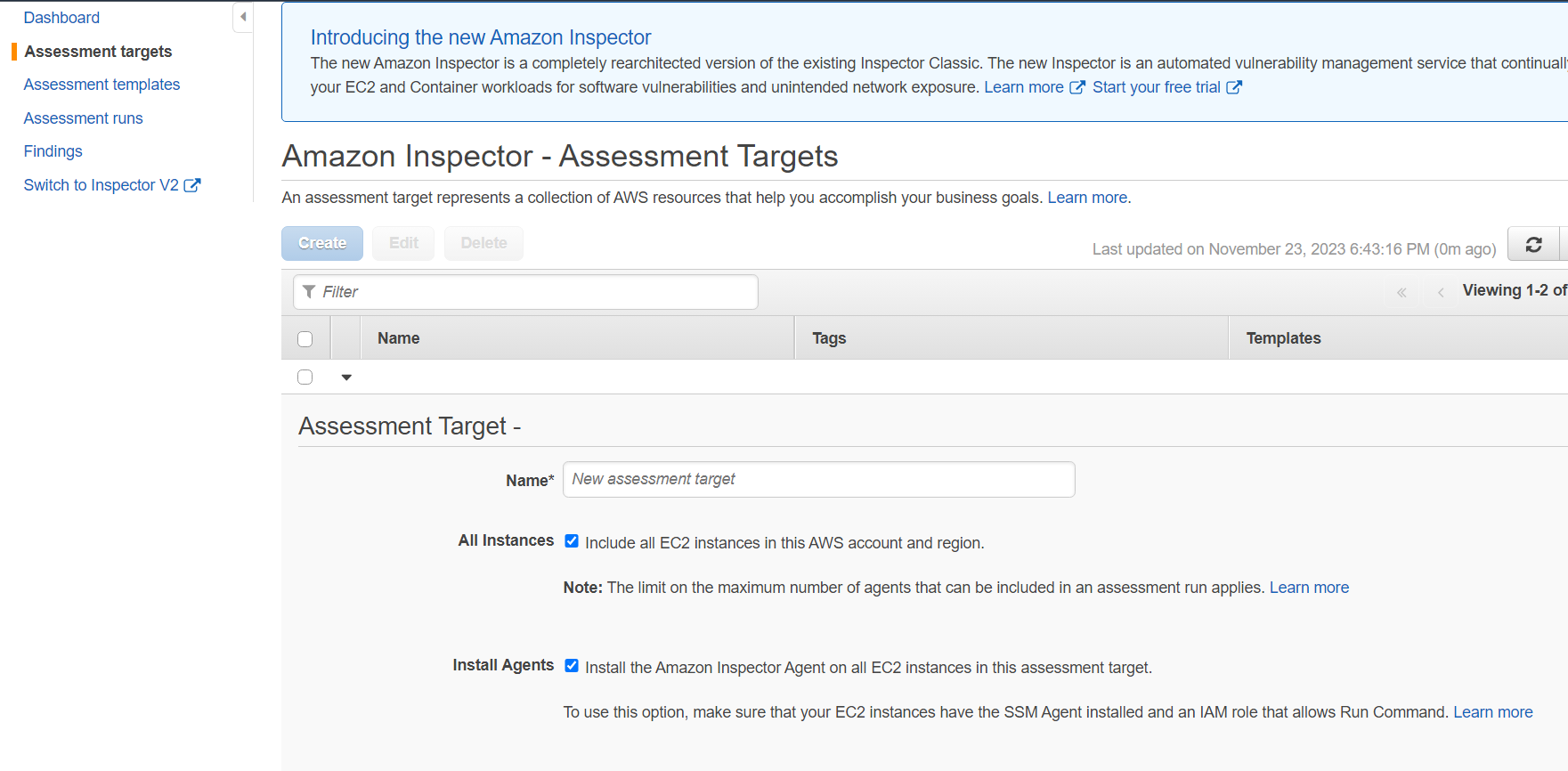
10. Now search for Amazon Inspector and click on it.



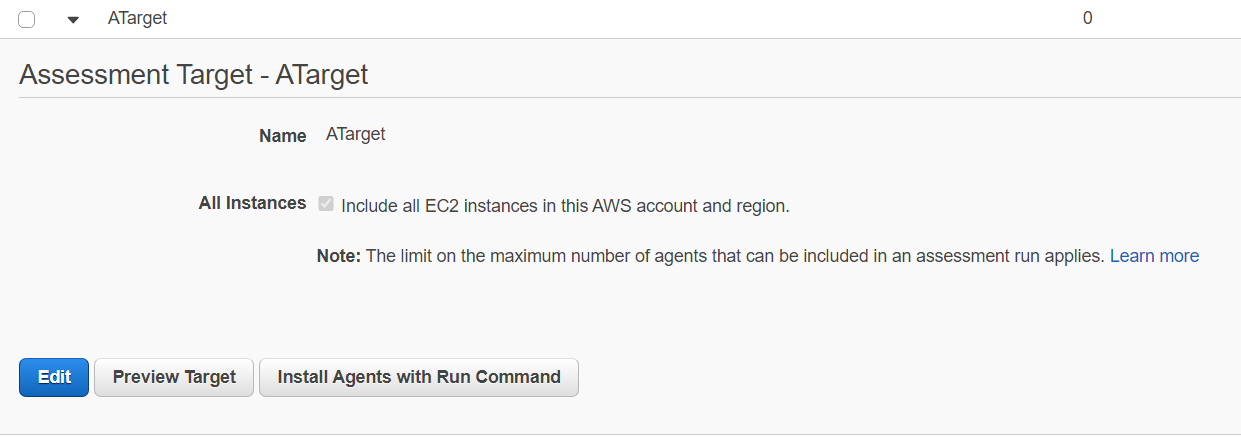
11. Click on the side menu icon and click on “Switch to Inspector Classic”.



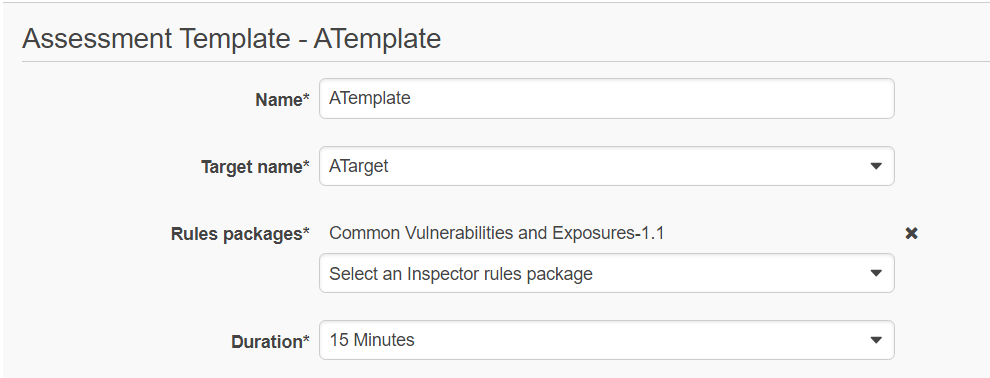
12. Create an assessment target, give a name to it, Check to “include all EC2 instances in this AWS account and region” and then click “Save” below.



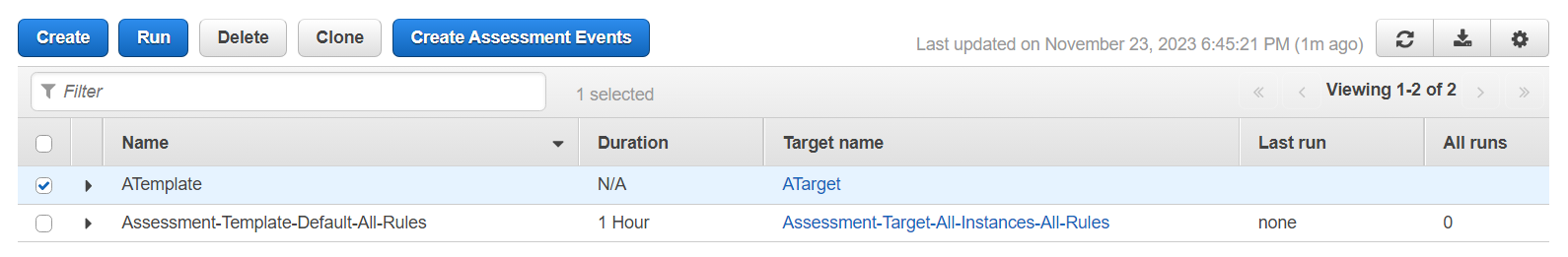
13. Then open the target by clicking on dropdown and click on “Install Agents with Run Command”.



14. Create an Assessment Template, give a name, select the target, select rules packages as “Common Vulnerabilities and Exposures-1.1”, set the Duration to 15 Minutes and then click on save.



15. Now select the template and click on run and then wait for 15 minutes.



16. After the set duration, in the Assessment runs, the report gets ready. Click on Download report



17. The pdf report will be opened in a new tab

