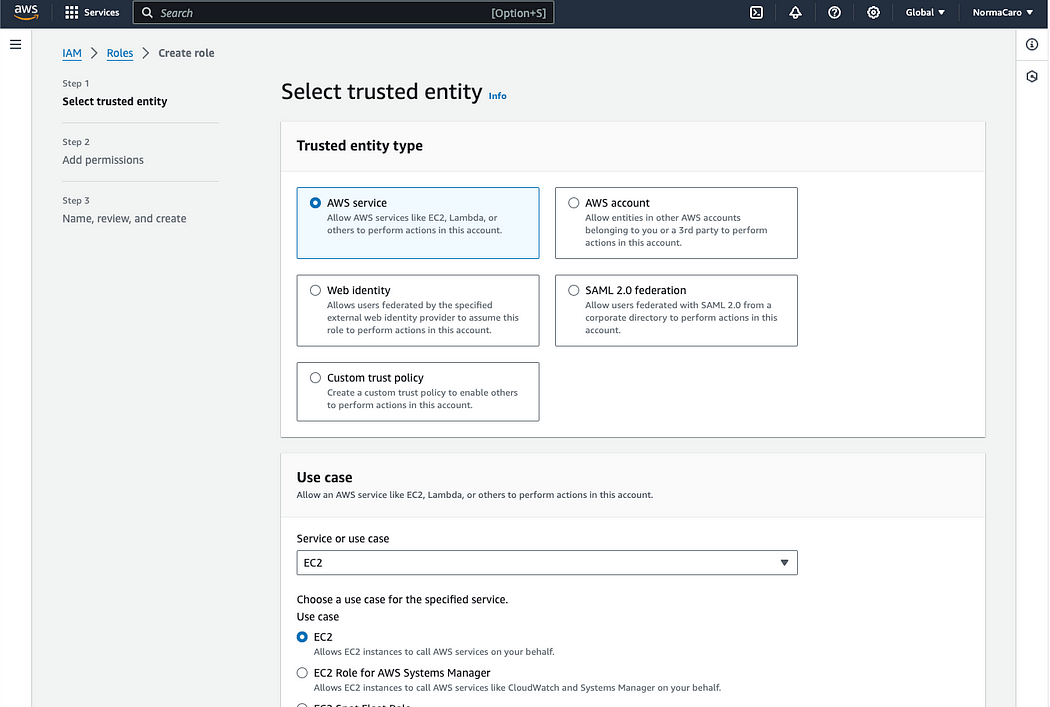
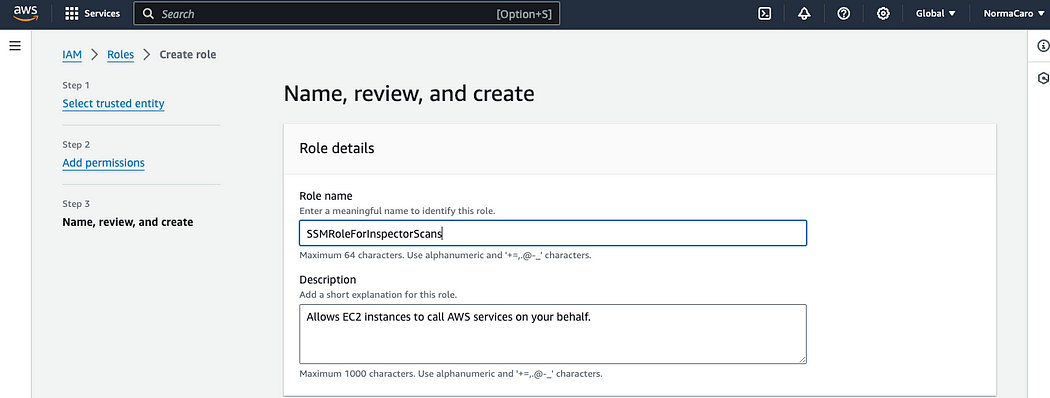
Navigate to IAM, click on Roles then click on the Create role button. You will be prompted to select an entity type, in our case select “AWS service”, and for service select EC2. This will create a trust policy that will allow EC2 to assume it.

Click Next

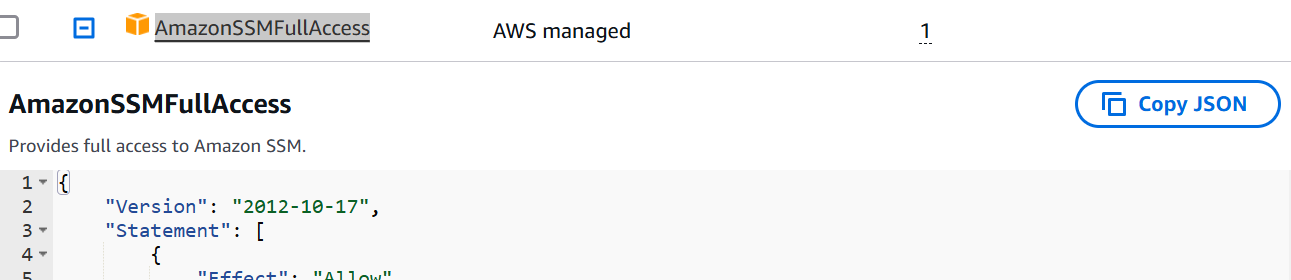


Now we must add permissions to the role that the EC2 will assume. Under the Add permissions config screen, search for AmazonSSMFullAccess, select it and click Next.

In the next window, give the role a name scanrole and click Create role.

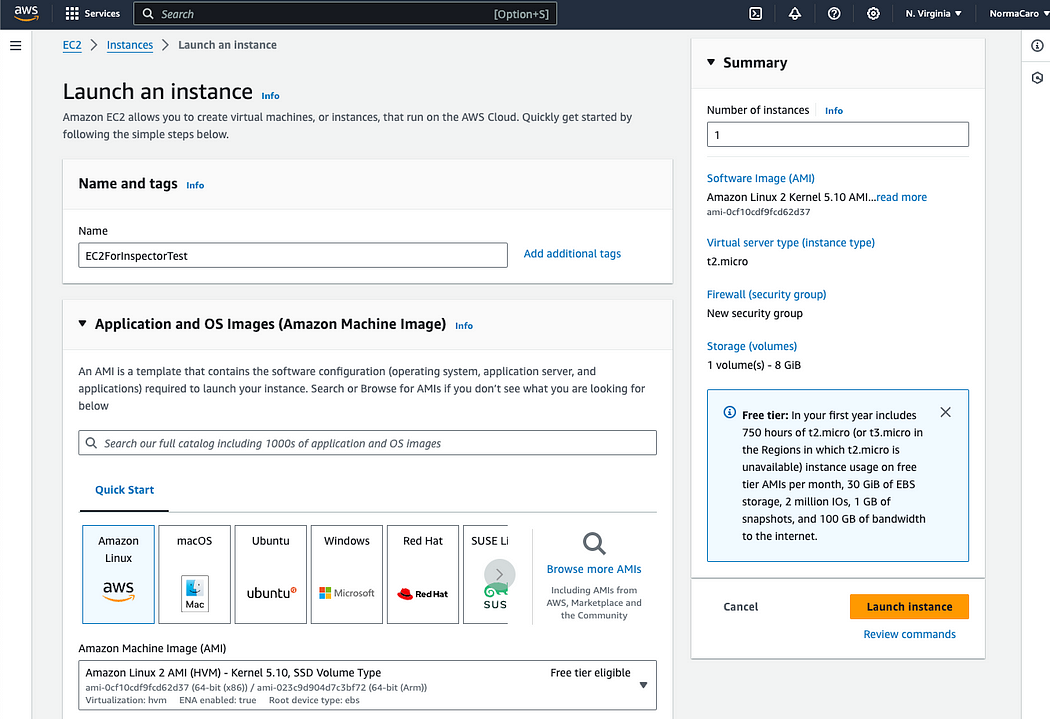


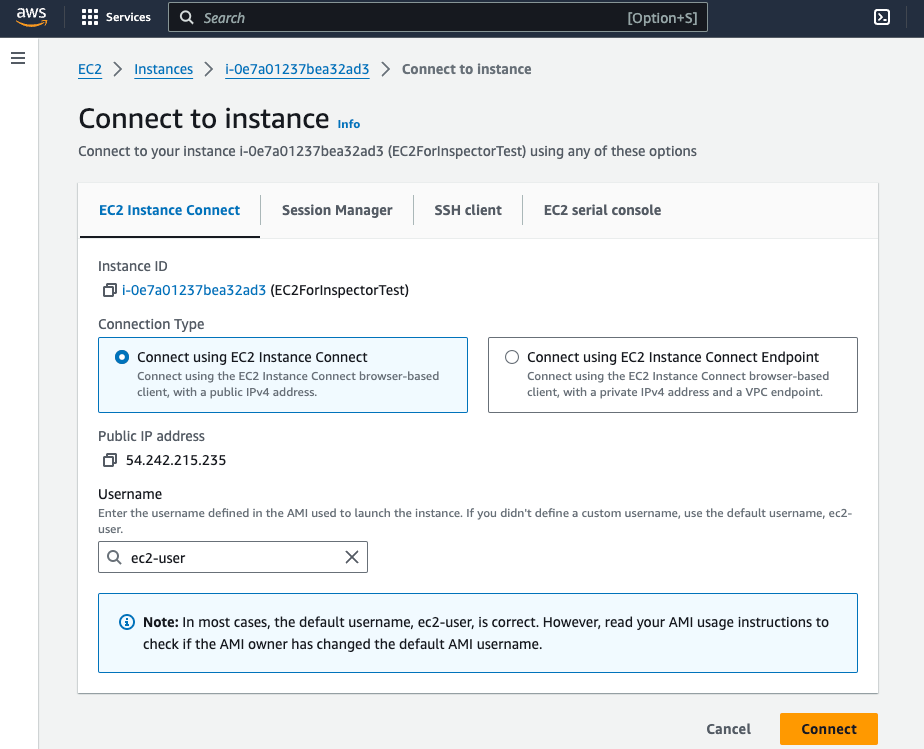
You should now see your role created.



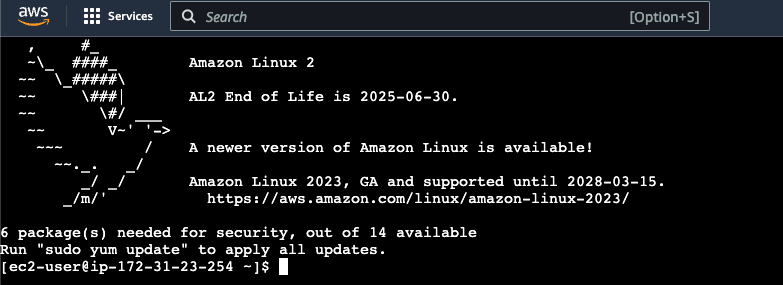
**Create an EC2 and confirm the agent is installed**

Let’s create an EC2 that we can use for our test.





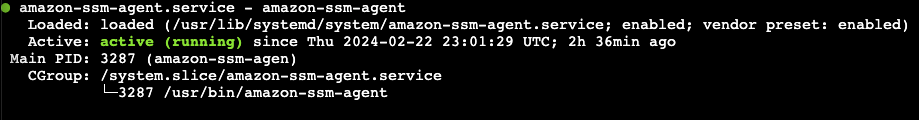
This will open a terminal on your browser and connect you directly to your instance.



At the command terminal type:

sudo systemctl status amazon-ssm-agent

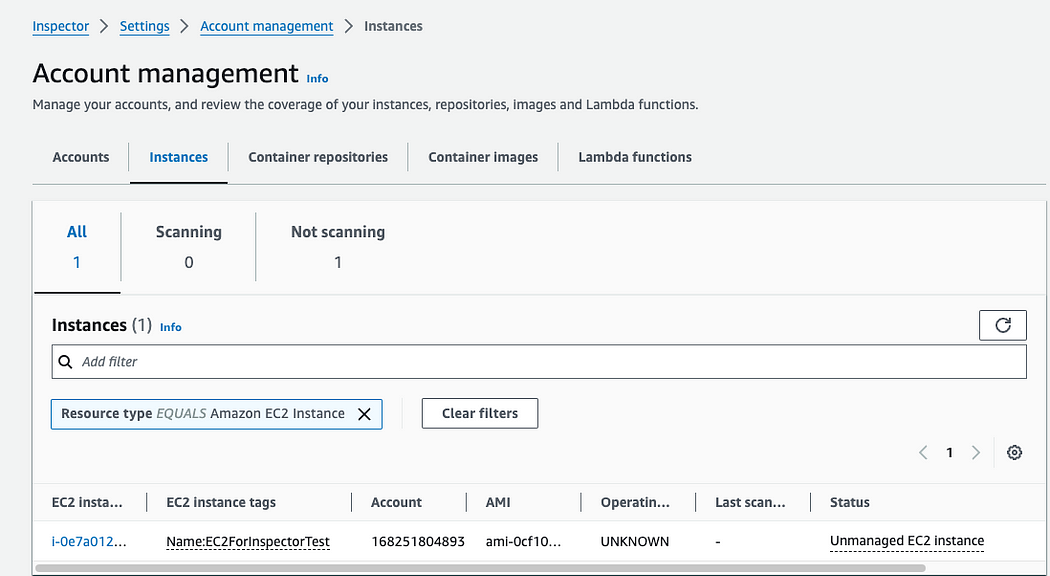
You should see a confirmation that the agent is “active (running)”



If you used a different AMI that did not have the agent installed, you can follow the instructions to install the agent for your respective OS here: <https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-manual-agent-install.html>

Go to inspector🡪 Check for scan report

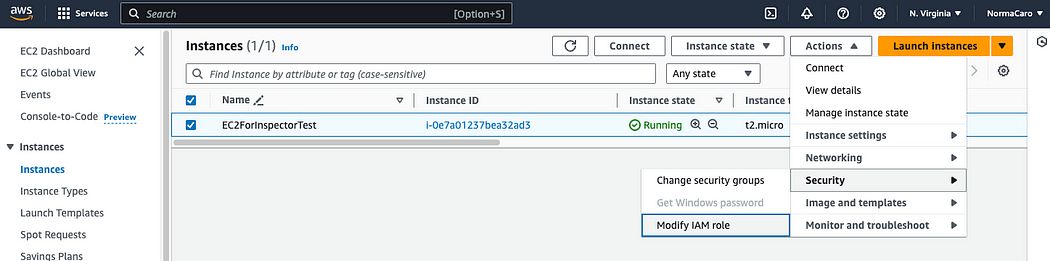
In my example, I only have one instance and it shows that the operating system is “UNKNOWN” and that status is “Unmanaged EC2 instance”.



**Attach the SSM agent role to the EC2 instance**

The reason we do not see any scans is because we have not yet attached the IAM Instance Profile role that will allow AWS Inspector to talk to the SSM agent. Let’s go back to our EC2 console and attach the role.

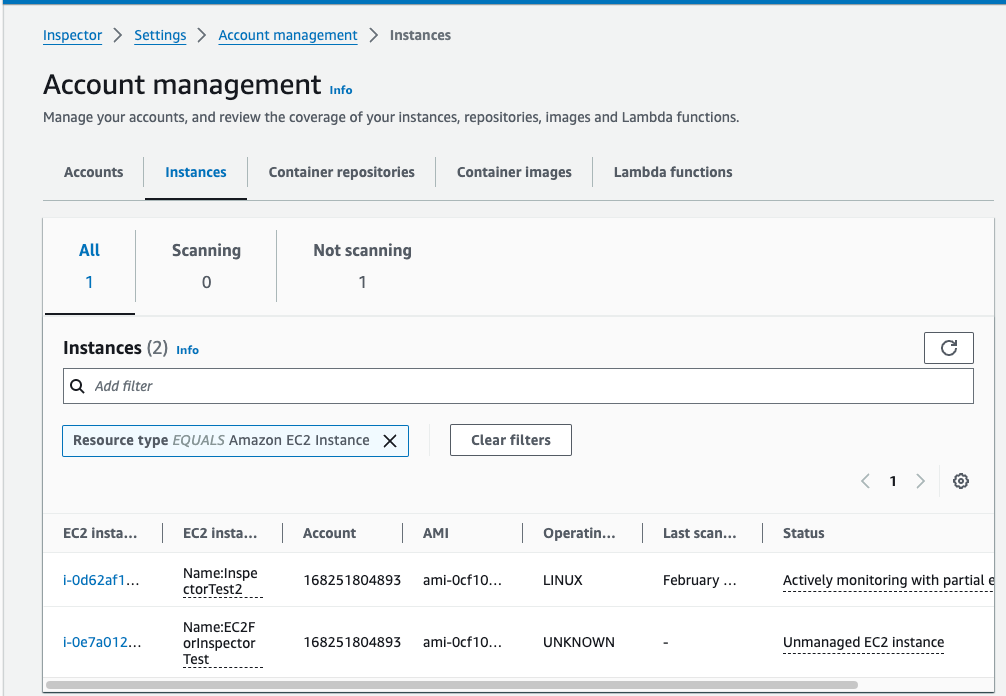
Select your instance, click on Actions, then click Security, and then click on Modify IAM role.



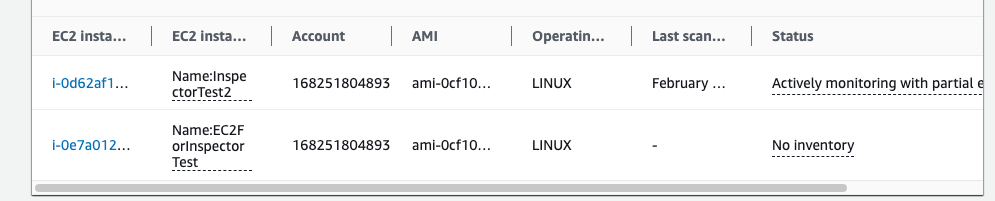
Within the Modify IAM role screen, select the role you created earlier. In my case, I am selecting scan role Click on Update IAM role.

**Review the scanned report in AWS Inspector and understand how to read it.**

Go to inspector🡪 Check for scan report



If you are eye-balling the status, you’ll see the Status change to “No inventory” and eventually to “Actively monitoring”.



Once your scans have completed, you can go back to your dashboard and navigate through the findings.

