**23. Introduction to AWS Inspector**

* AWS Inspector is similar to a vulnerability scanner that will scan the system for specific assessment rules and provide the results.
* It relies on the agent installed on the server to scan the server.
* AWS Inspector has certain pre-defined templates based on which we can scan.
* CVE (Common Vulnerabilities & Exposure)
* CIS Benchmarks
* Security Best Practices
* Network Reachability

**Inspector Rule - CVE**

* As the name suggests, this rule will scan for all the packages in the OS to see if there are any vulnerabilities associated with the version of packages installed.

**Inspector Rule - CIS Benchmarks**

* This rule will check the OS against the CIS benchmarks to verify whether the server is following all the best practices mentioned in the CIS Benchmarks.

**Inspector Rule - Security Best Practices**

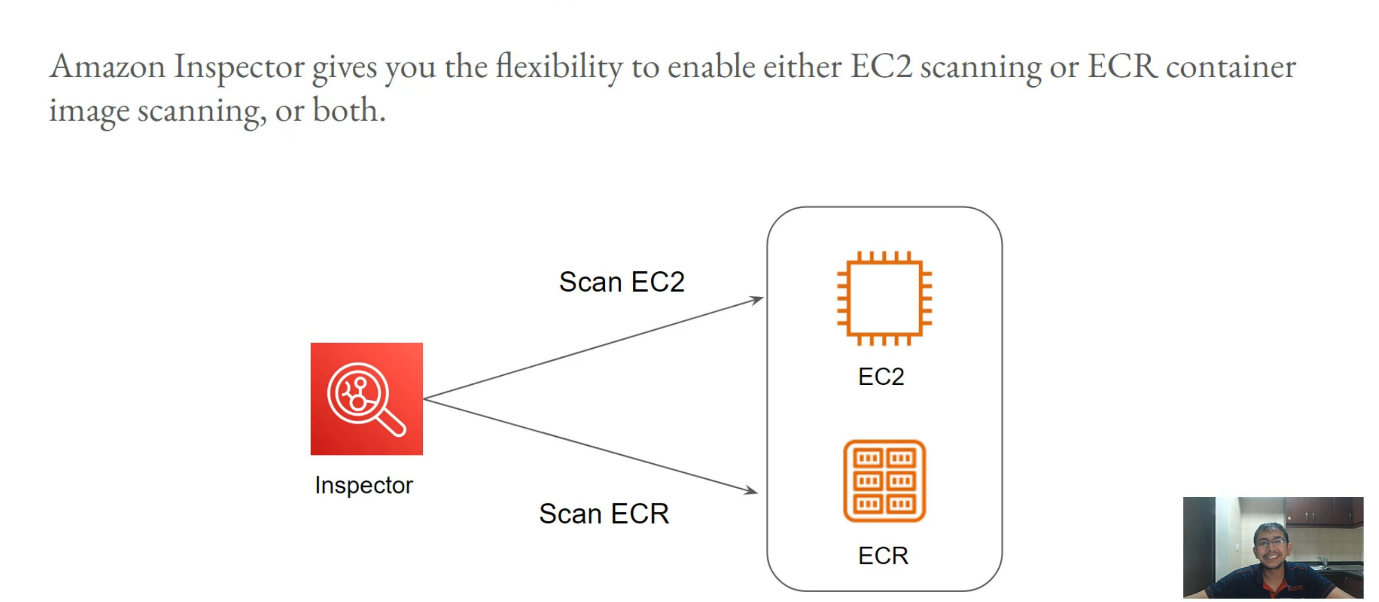
This is a set of certain rules which the Inspector will check against and report.

* Disable Root Login via SSH
* Support SSH V2 only.
* Disable Password Authentication via SSH
* Configure maximum password age and minimum length.
* Configuring password complexity.
* Enable ASLR and DEP
* Configure permissions for system directories.

**Inspector Rule - Network Reachability**

* Shows findings of the ports that are reachable from the internet through an internet gateway
* It can help if ports are misconfigured at the security group level.
* AWS Inspector Agent is not required for this scan.

**Supported scans**



--- **note** – we will be using inspector to scan EC2 instance, as well as the docker image with in the ECR repository.

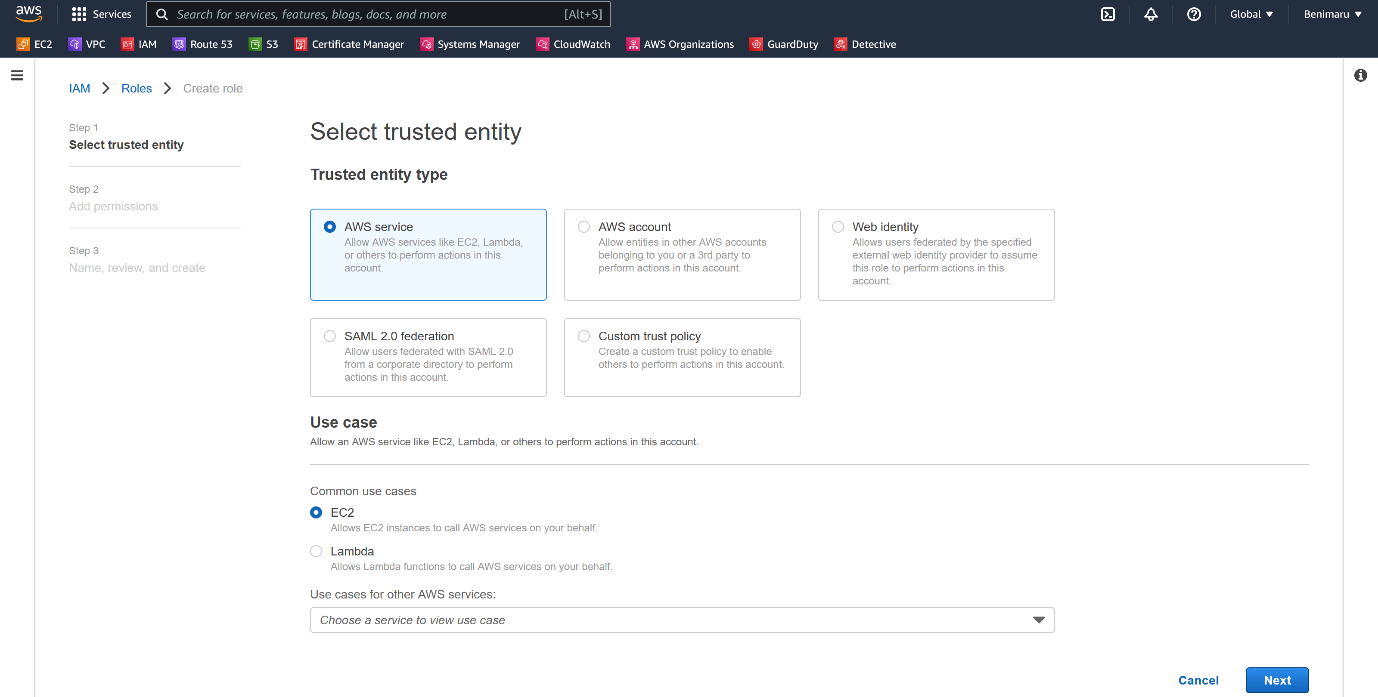
--- **prerequisites**

* if you are using Amazonlinux2, you do not really need to worry because it comes with SSM agent.
* if you are using some older operating system, you will have to manually install the SSM agent.
* Create a IAM rule with **AmazonSSMManagedInstanceCore** policy and attach the role to instance.
* Create private ECR repository and push cento6 image to the repository. So that you can see more vulnerabilities.

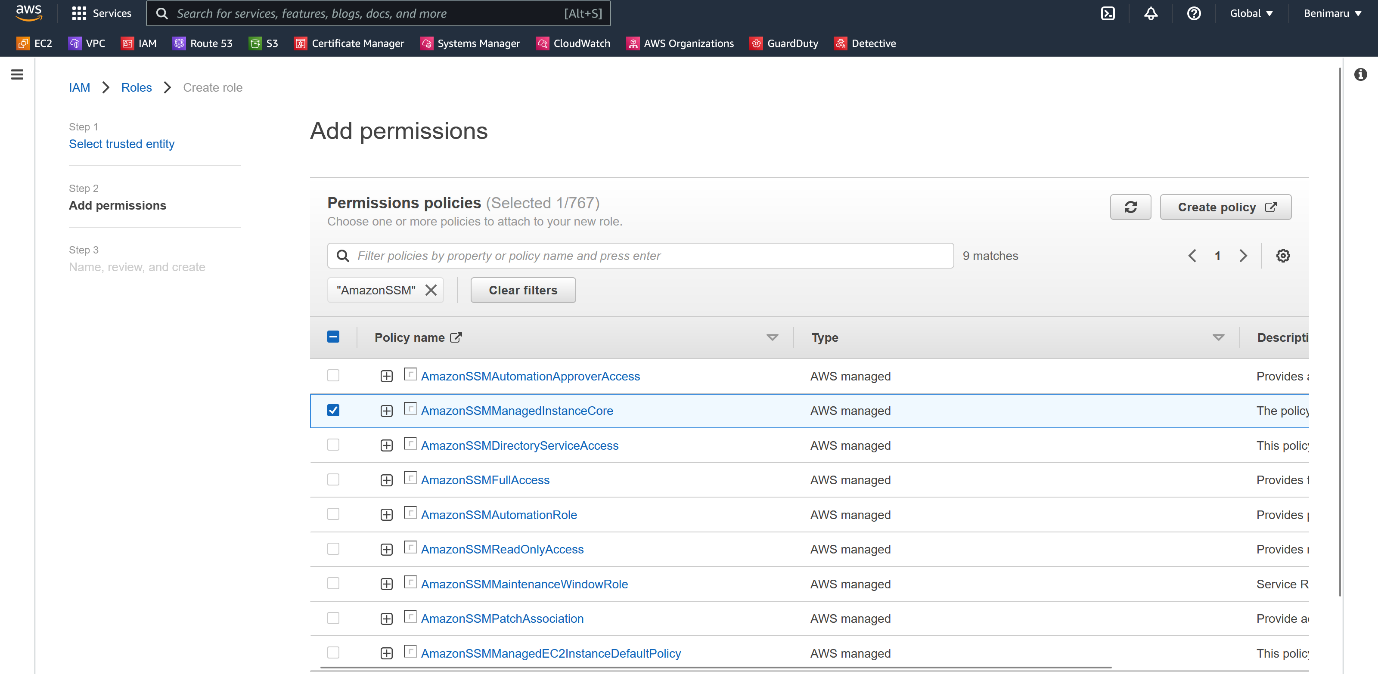
**Create IAM role**

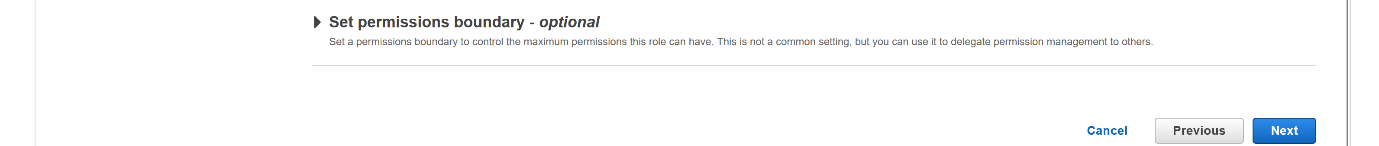
--- go to IAM and click on roles.

--- click on crater role.

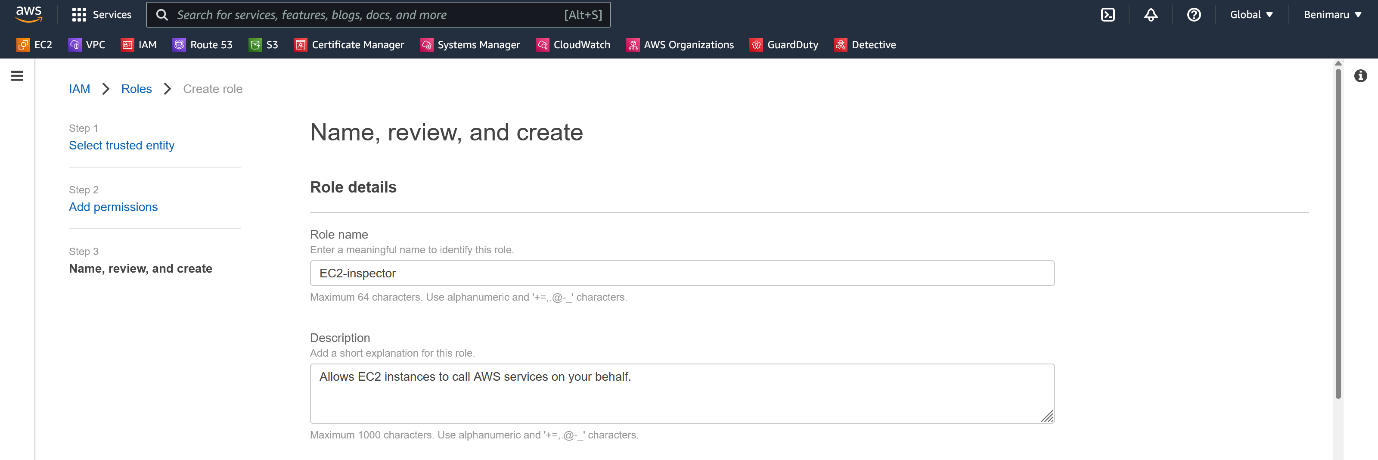


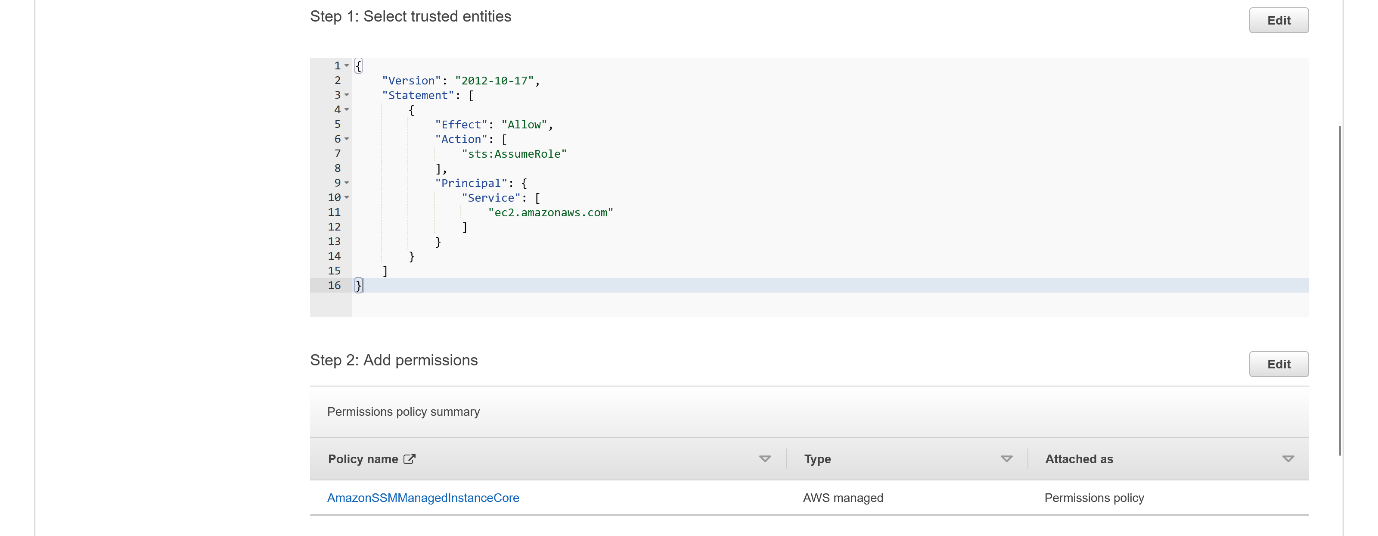
--- Click on next.

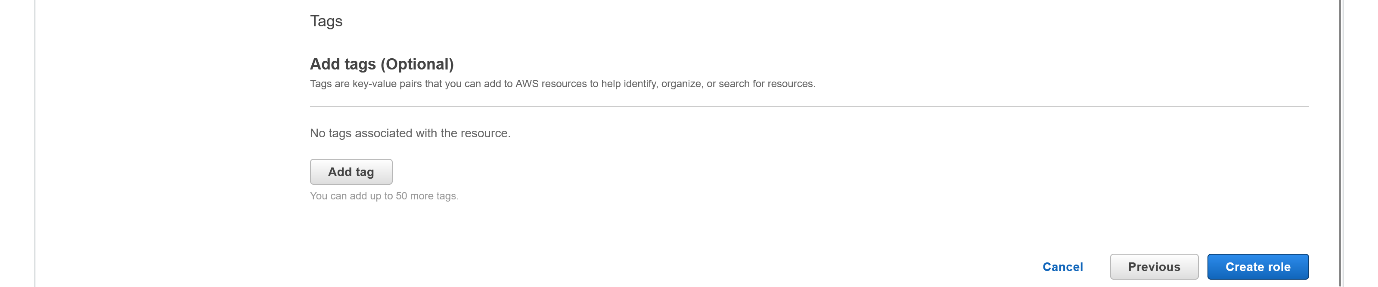




--- click on next.

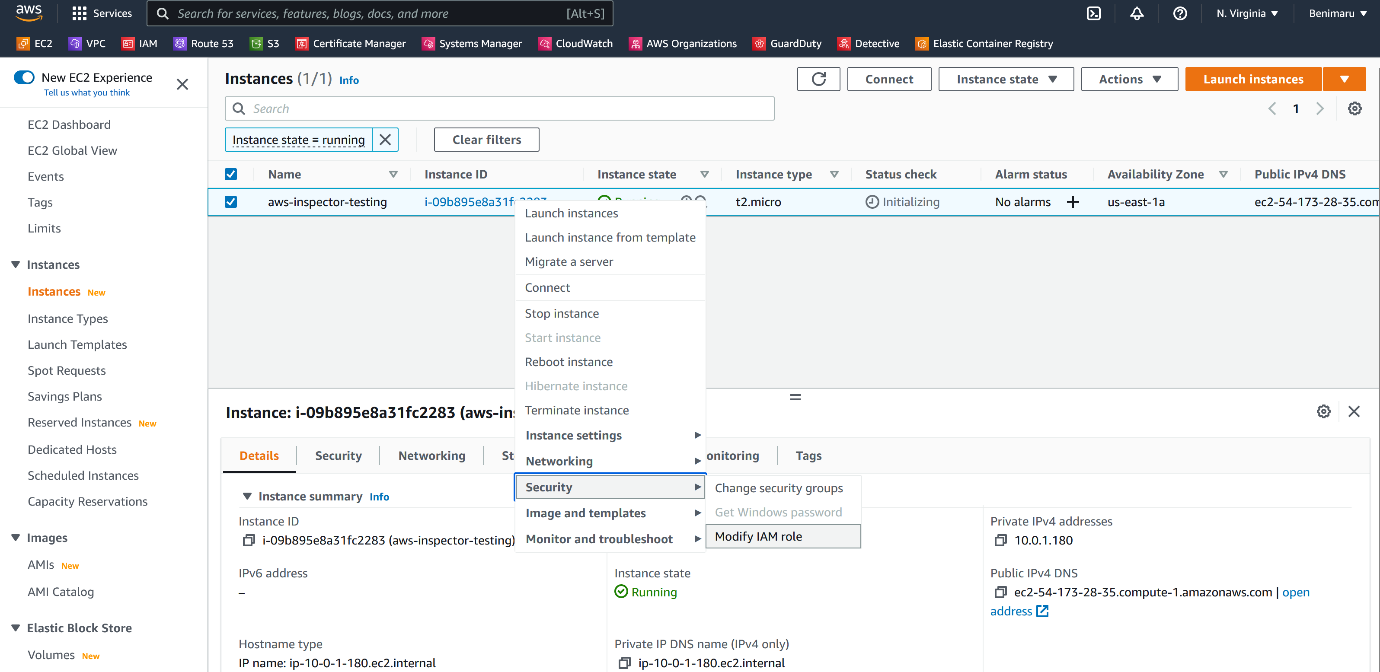




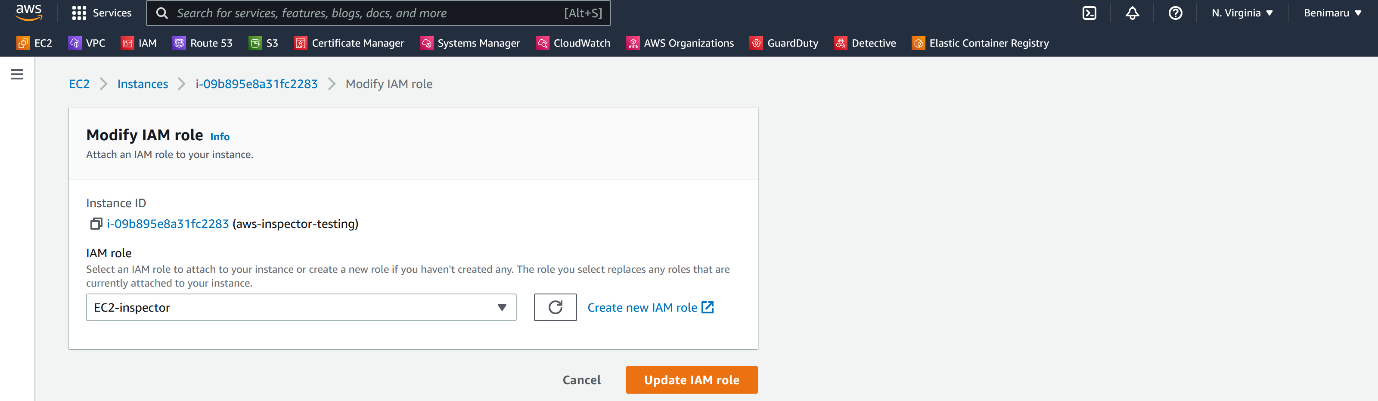


--- click on create role.

**Attach the role to instance**

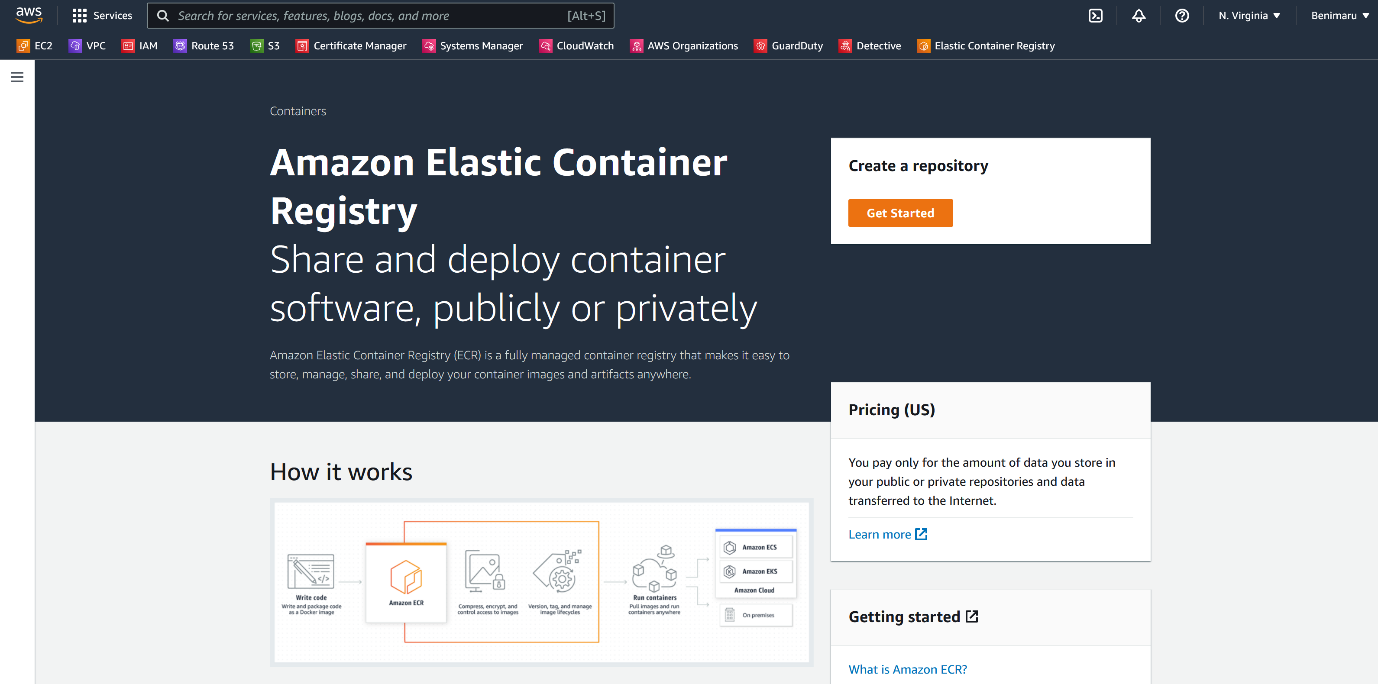


--- click on security and click on modify IAM role.

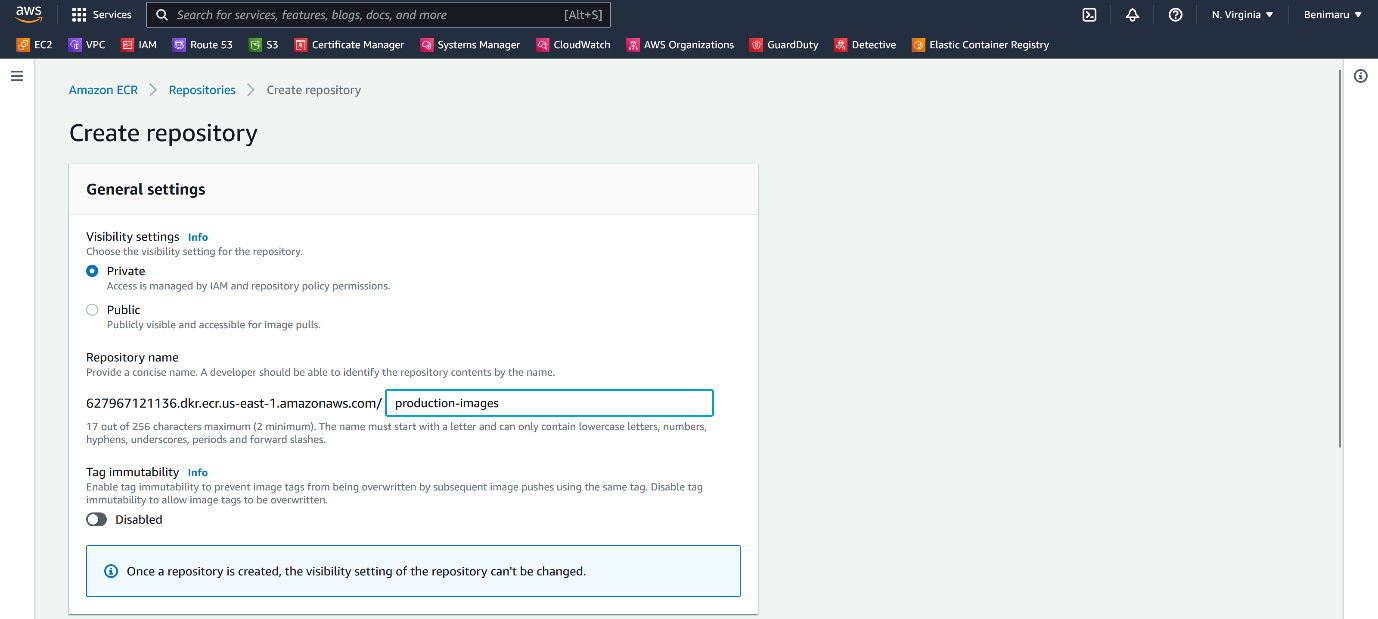


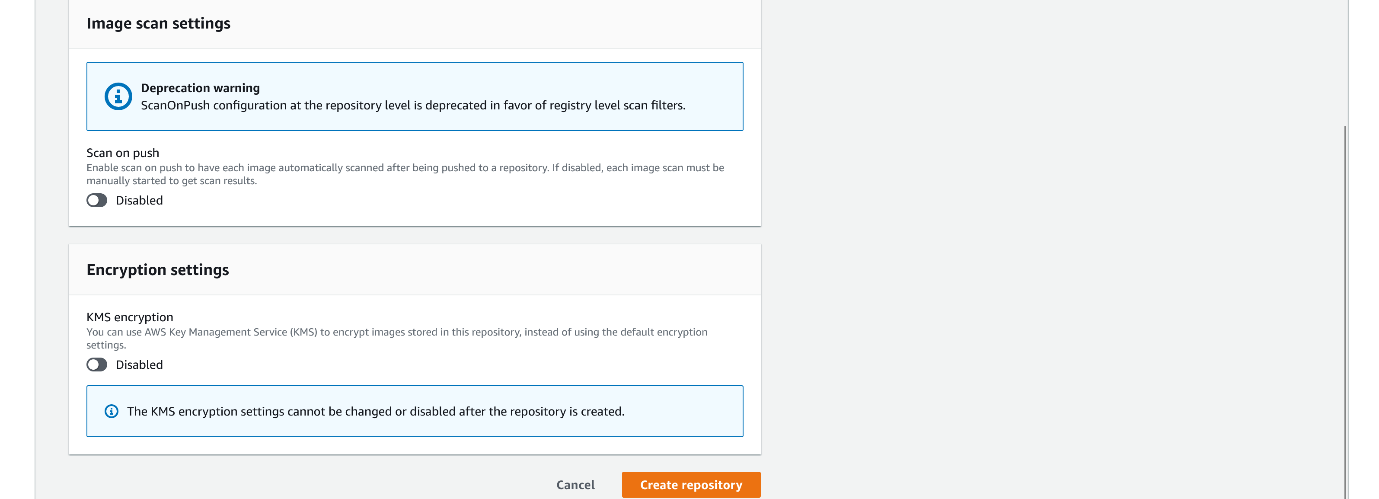
--- click on update IAM role.

**Create ECR repository**

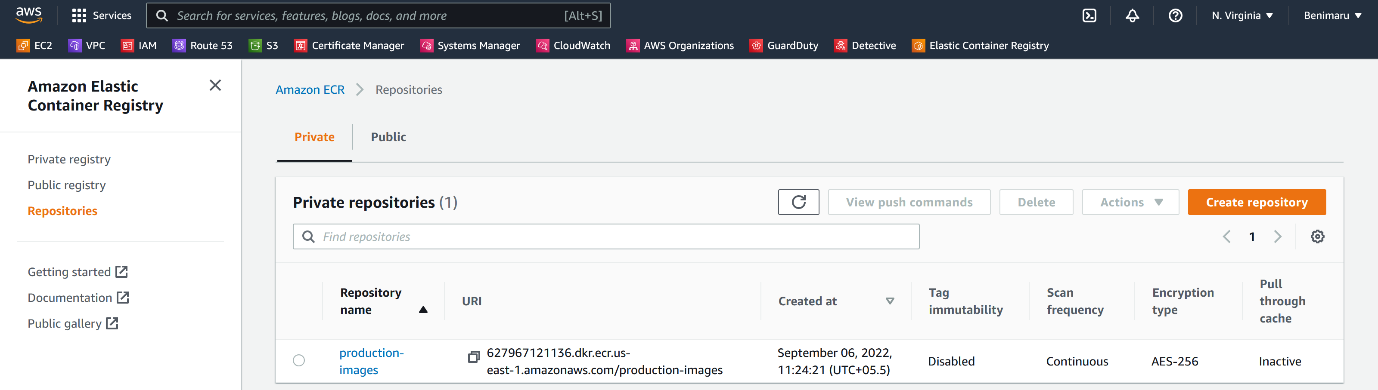


--- click on get started.





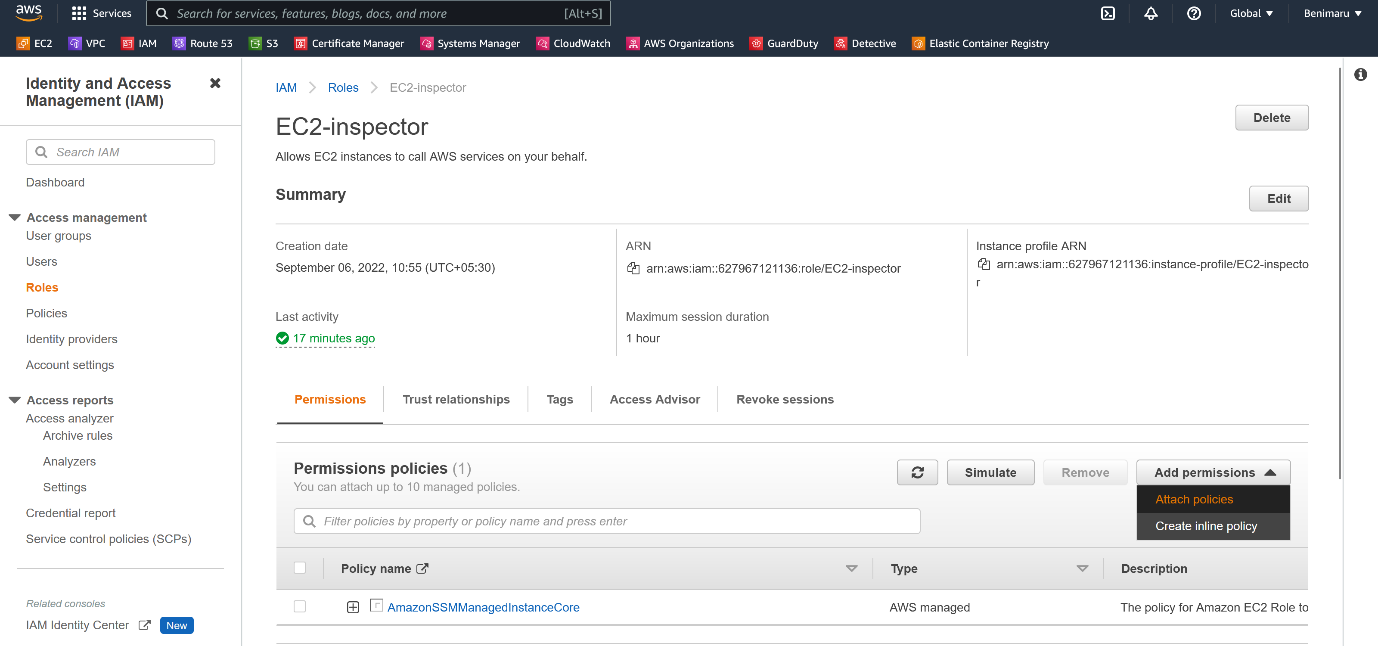
--- click on create repository.



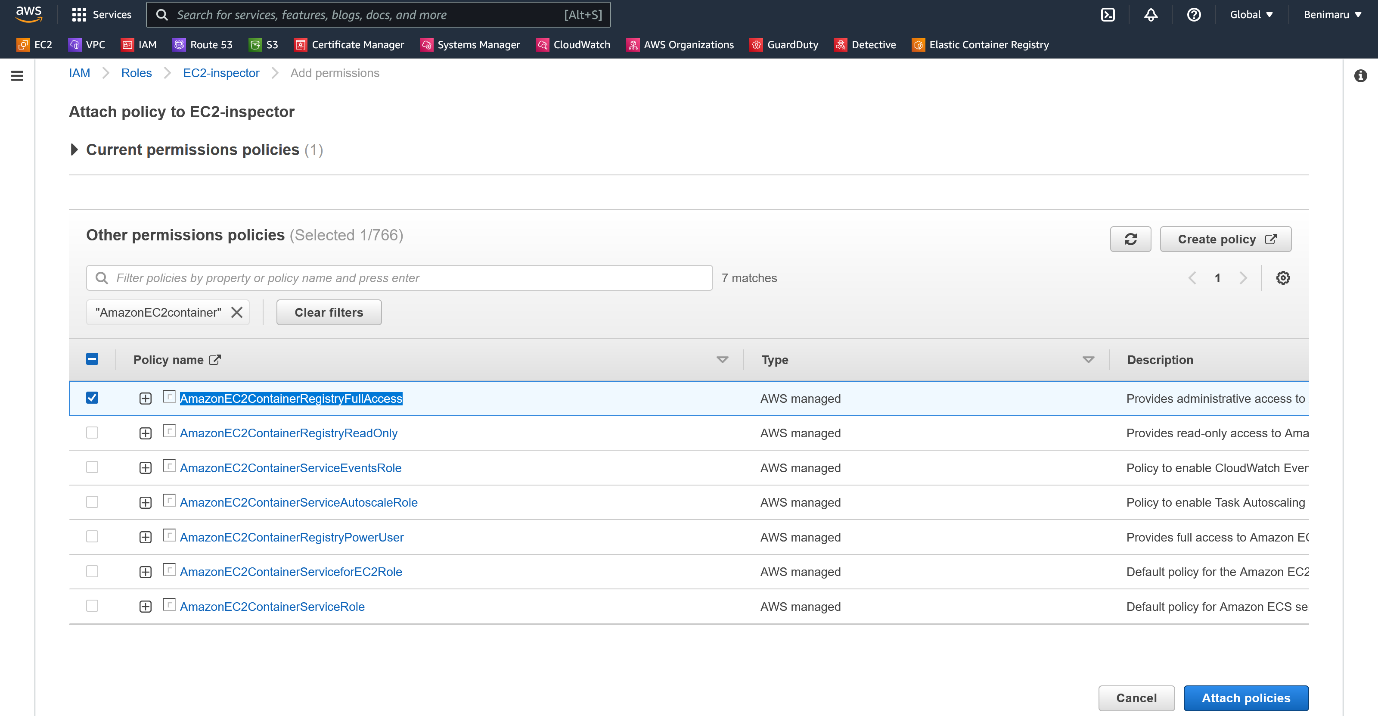
--- our private repository got created.

**Push image to aws ECR private repository**

--- **important** – in order push the image to ECR private repository, the instance should proper permissions so create policy with [AmazonEC2ContainerRegistryFullAccess](https://us-east-1.console.aws.amazon.com/iam/home#/policies/arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryFullAccess)



--- click on attach policy.



--- click on attach policies.

**# Pull centos image**

--- docker pull centos:6

**# Retrieve an authentication token and authenticate your Docker client to your registry.**

--- aws ecr get-login-password --region us-east-1 | docker login --username AWS --password-stdin 627967121136.dkr.ecr.us-east-1.amazonaws.com

**# Tag your image so you can push the image to this repository**

--- docker tag centos:6 627967121136.dkr.ecr.us-east-1.amazonaws.com/production-images:latest

**# Run the following command to push this image to your newly created AWS repository**

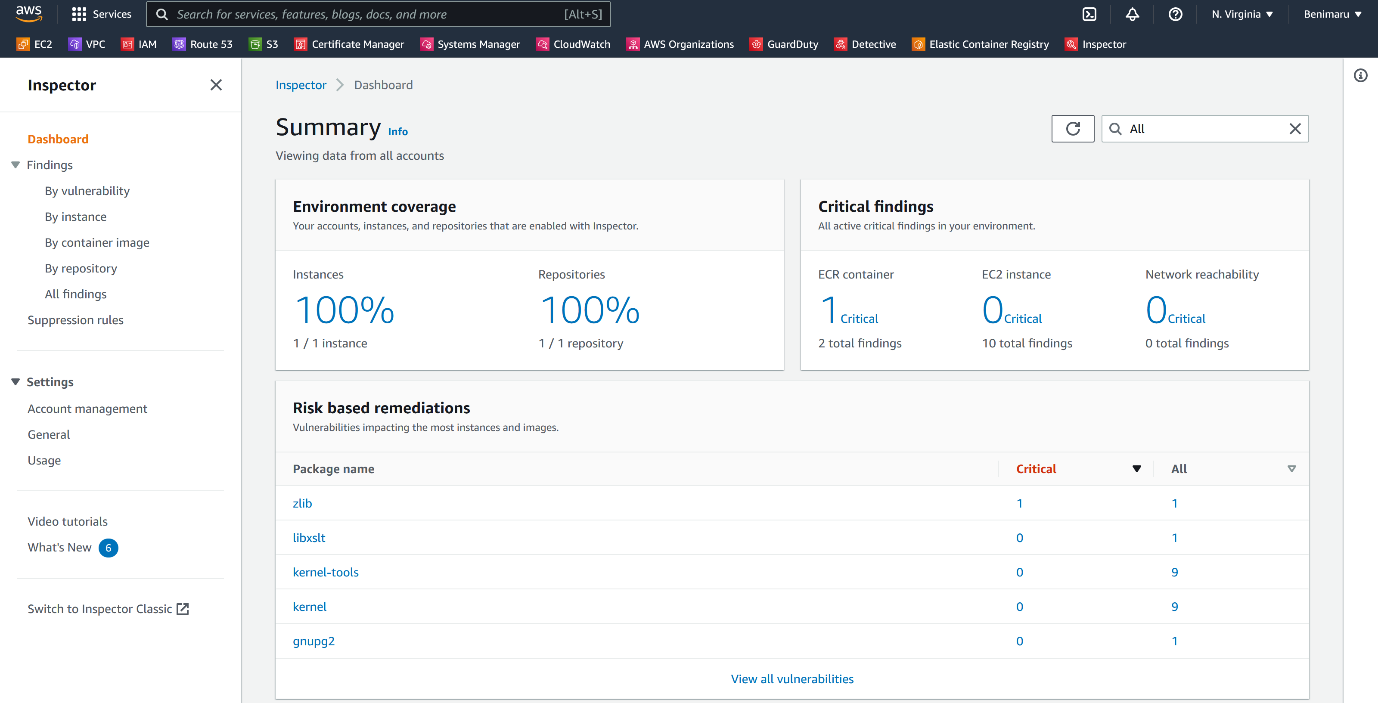
docker push 627967121136.dkr.ecr.us-east-1.amazonaws.com/production-images:latest

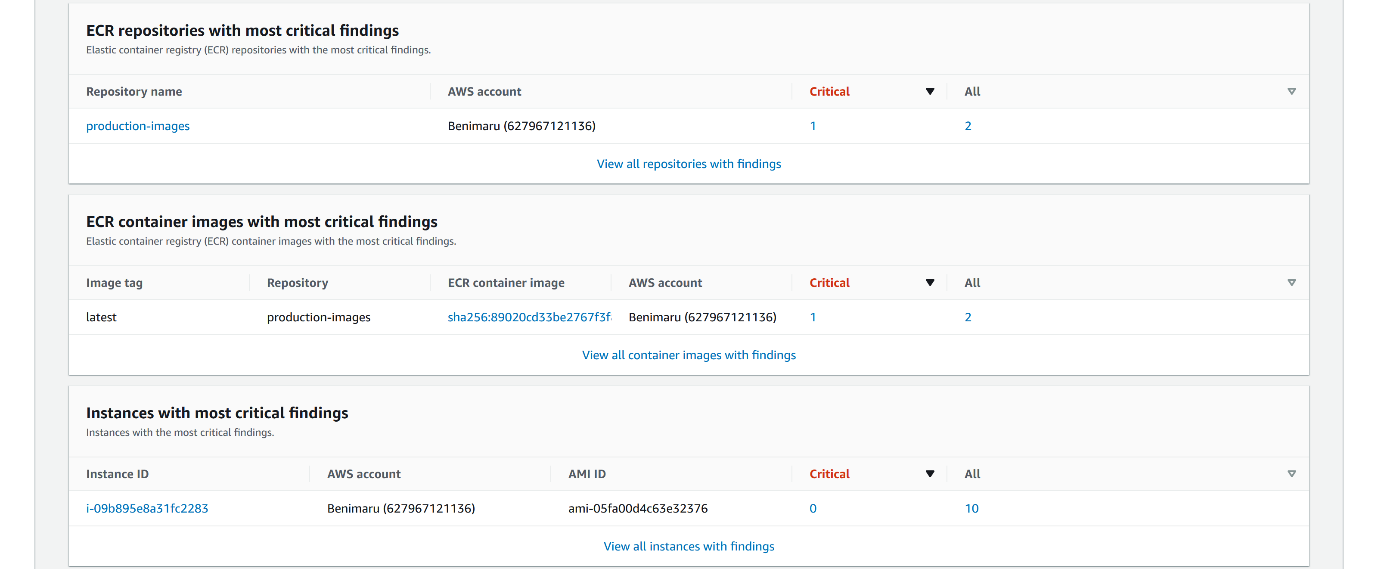
**# Verify the ssm agent is running on the instance**

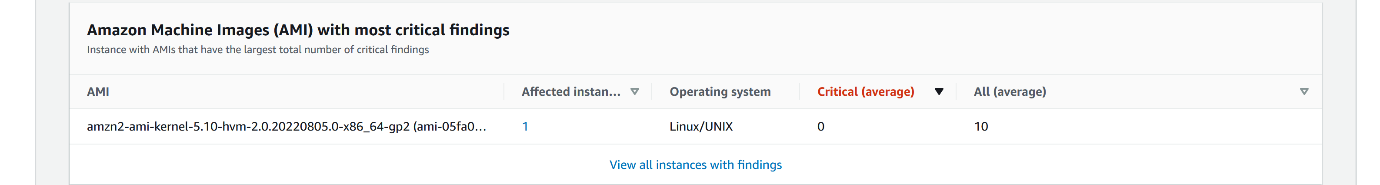
--- systemctl status amazon-ssm-agent

**AWS inspector dashboard**

--- go to Amazon ECR dash board.



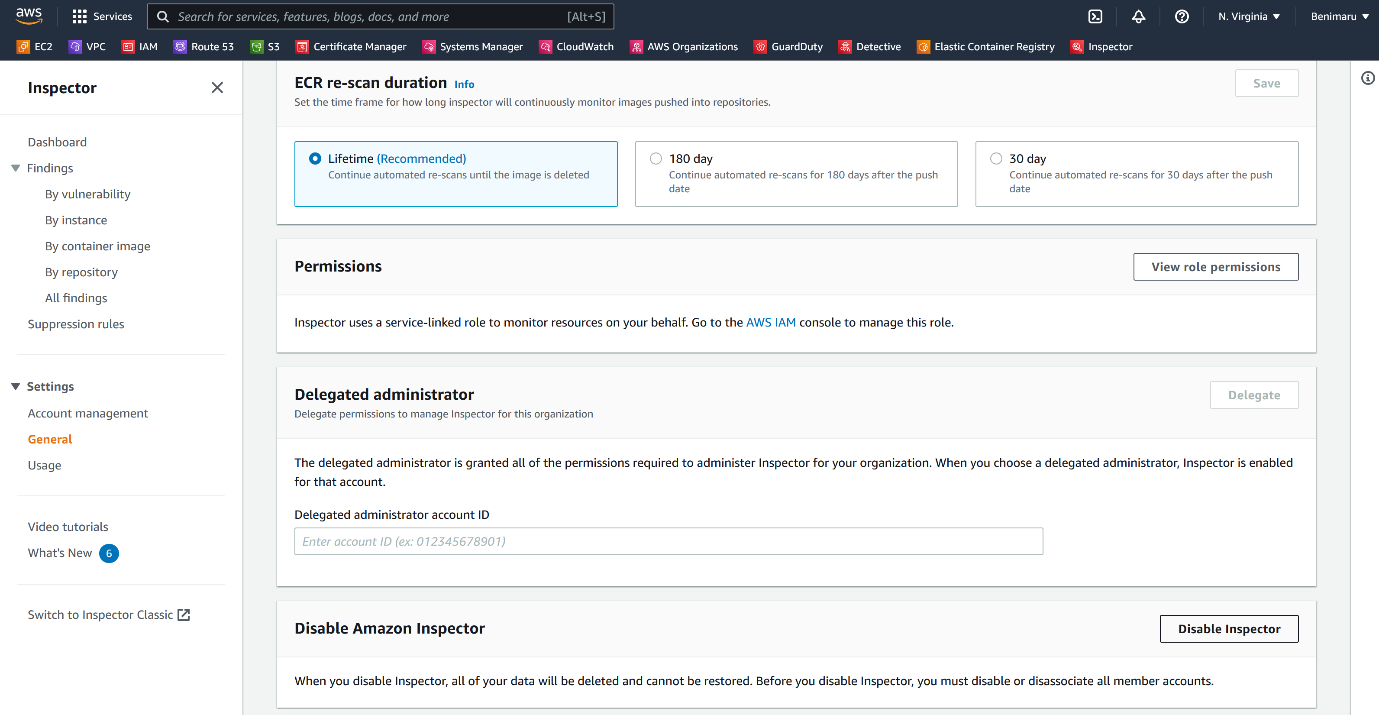




--- the instance and repositories are scanned. Now you can see the findings.

**Disable inspector**

--- click on general.



--- click on disable inspector.