**53. Overview of Amazon Macie**

--- AWS Macie can be used to recognize sensitive information like PII data, DB backups as well as data related to intellectual property.

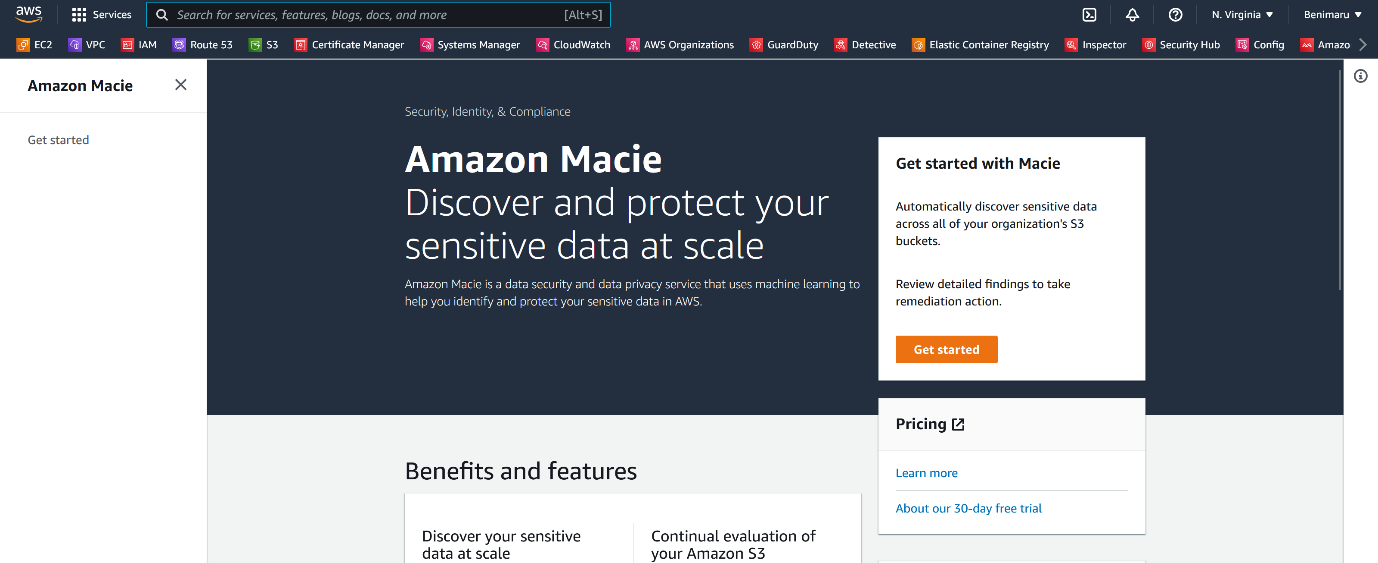
--- **example** - when you have terabytes of data in S3 and let us say, access key, a secret key in a text file in the S3 service. How will you quickly identify it? Because it is a little difficult to search terabytes of data to see if any data has been accidentally uploaded.

**Core feature of macie**

--- one of the core features of Macie is to go ahead and search and look for the sensitive data that is stored in the S3 service.

--- macie will also go ahead and give you various findings related to the bucket policies.

**AWS Macie**

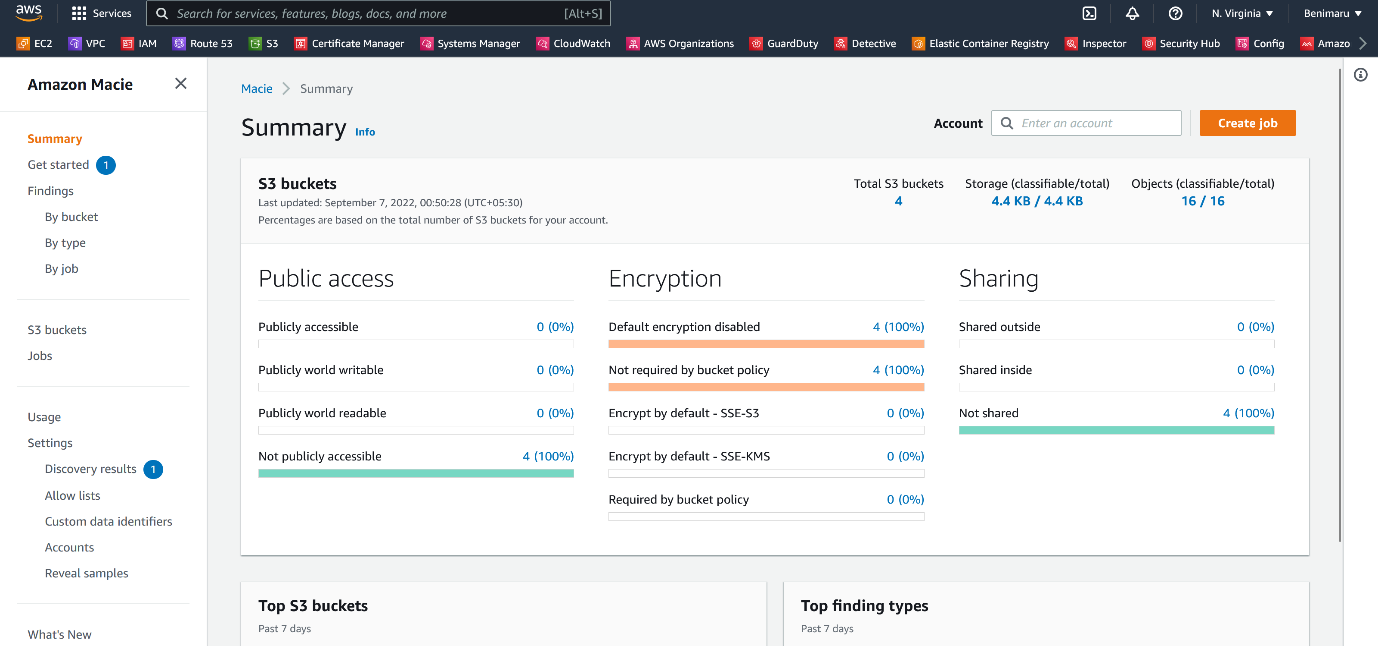


--- click on get stated.

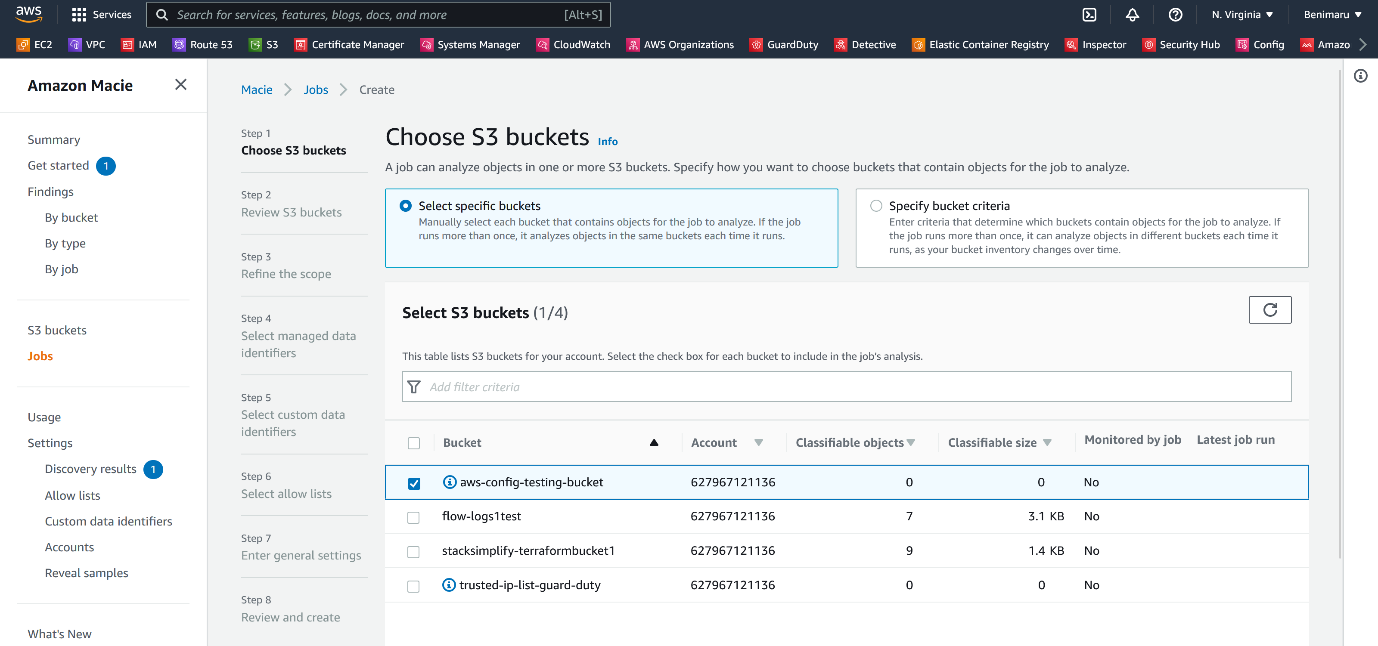
--- once you enabled macie then it will go and look into s3 configuration.

**Initiate a scan on bucket**

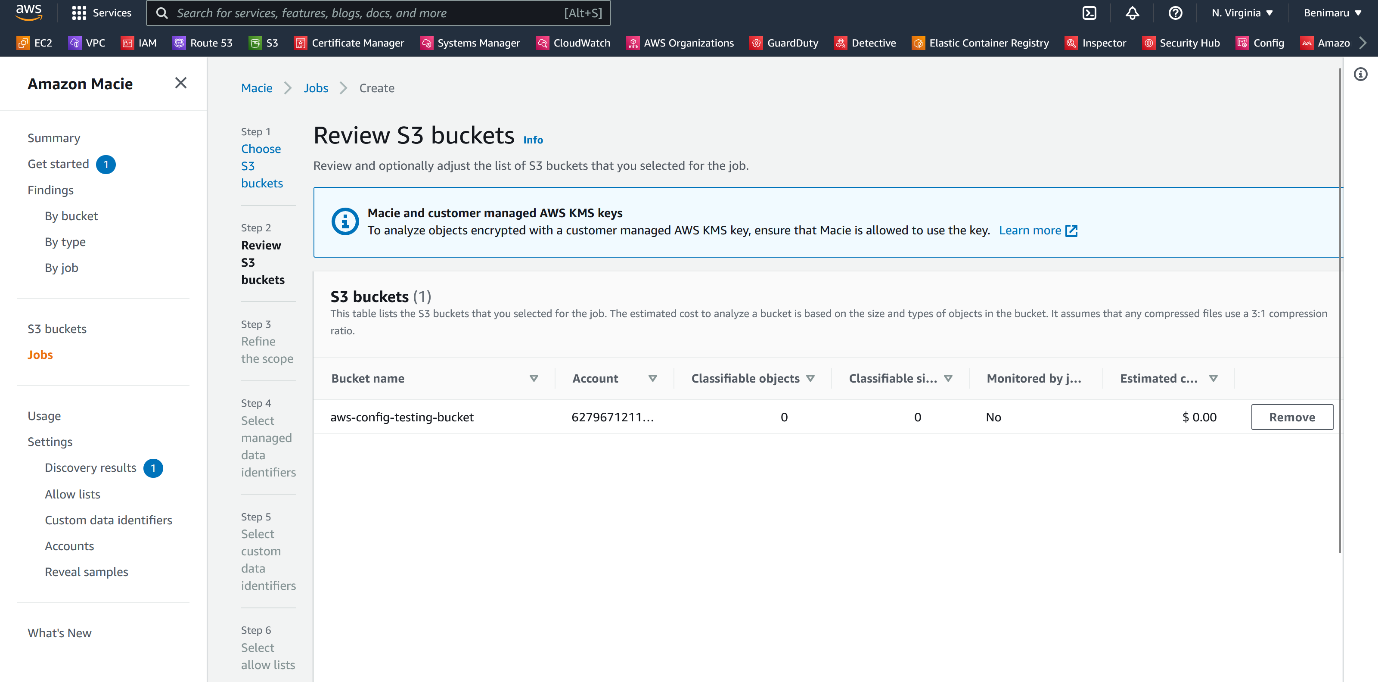
--- **important** – I have uploaded access and secret file in s3 bucket and I will scan the bucket using macie.



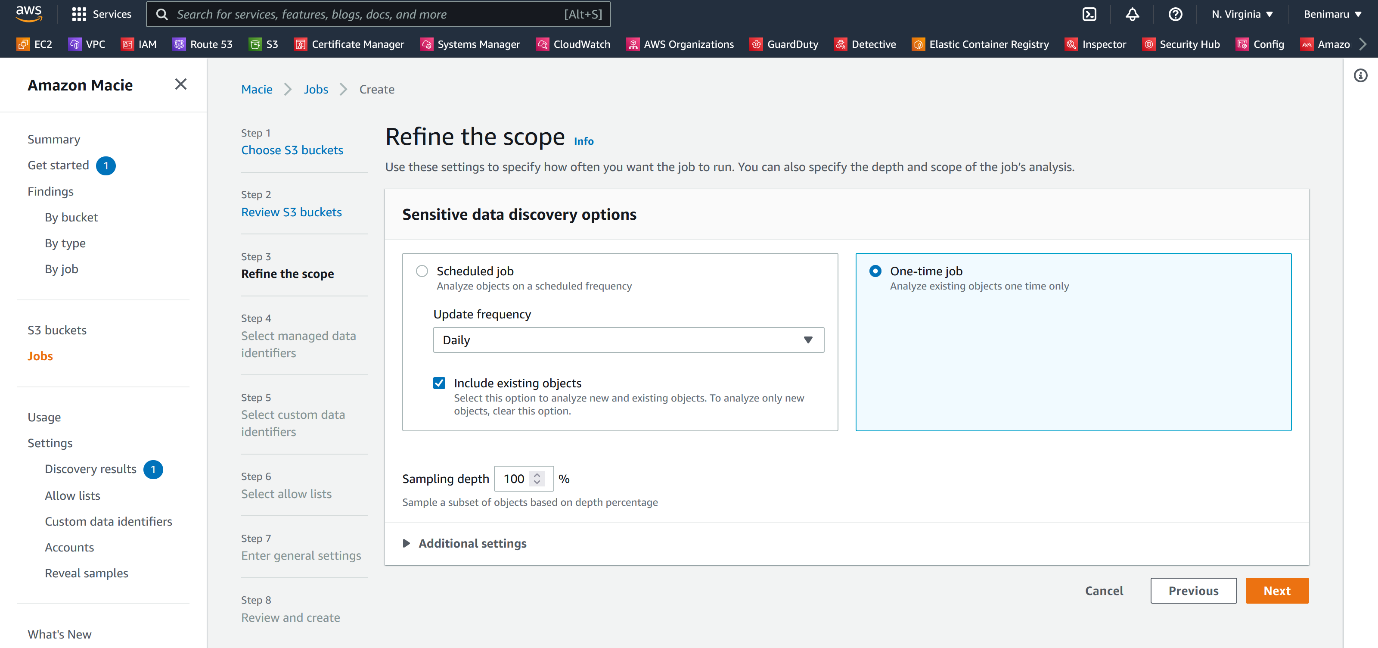
--- click on create a job.



--- click on next.

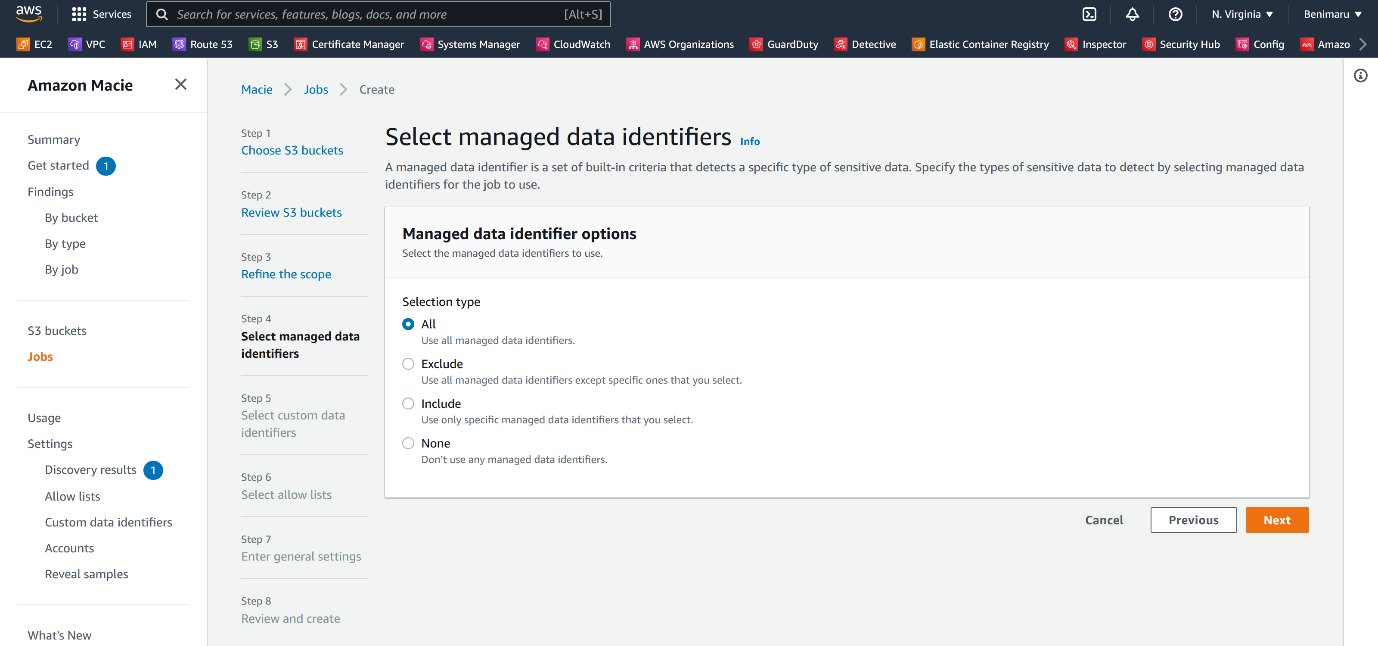


--- click on next.

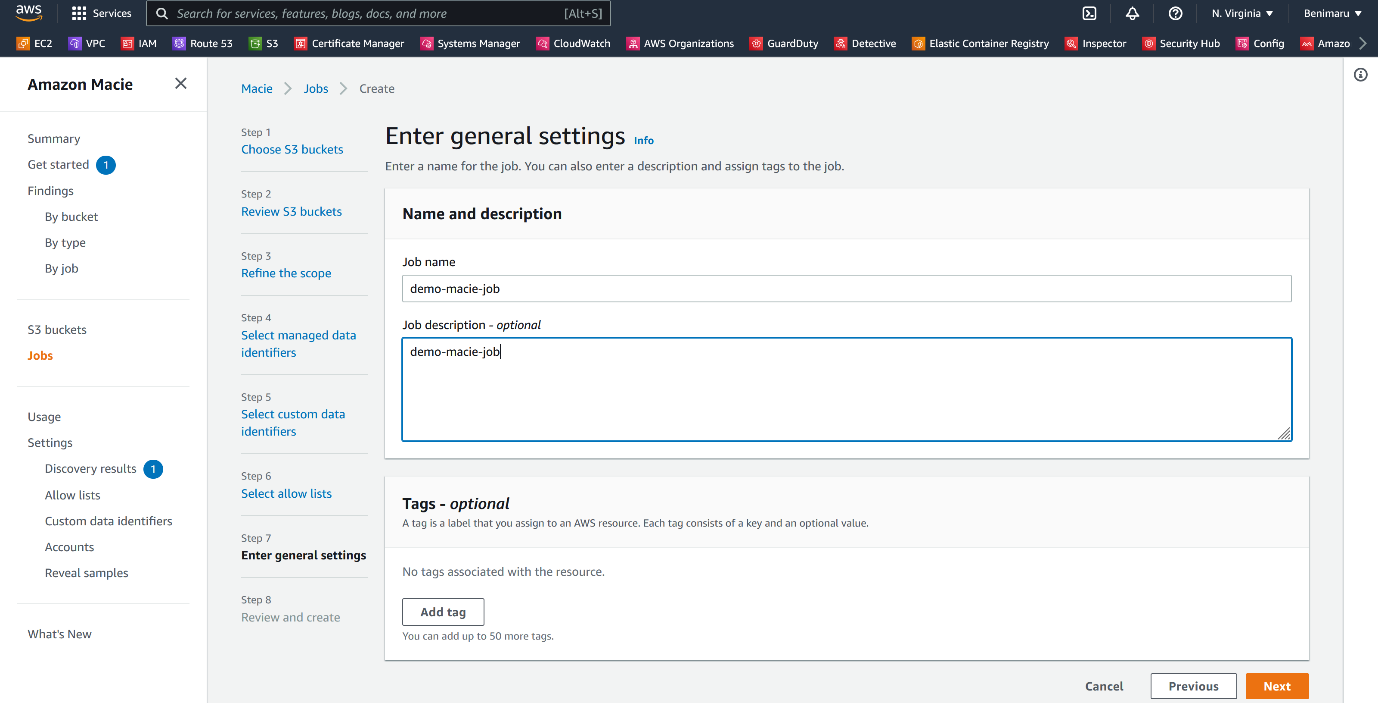


--- **note** – big organization will do monthly scan but I need only one time scan that is why I selected one-time job.

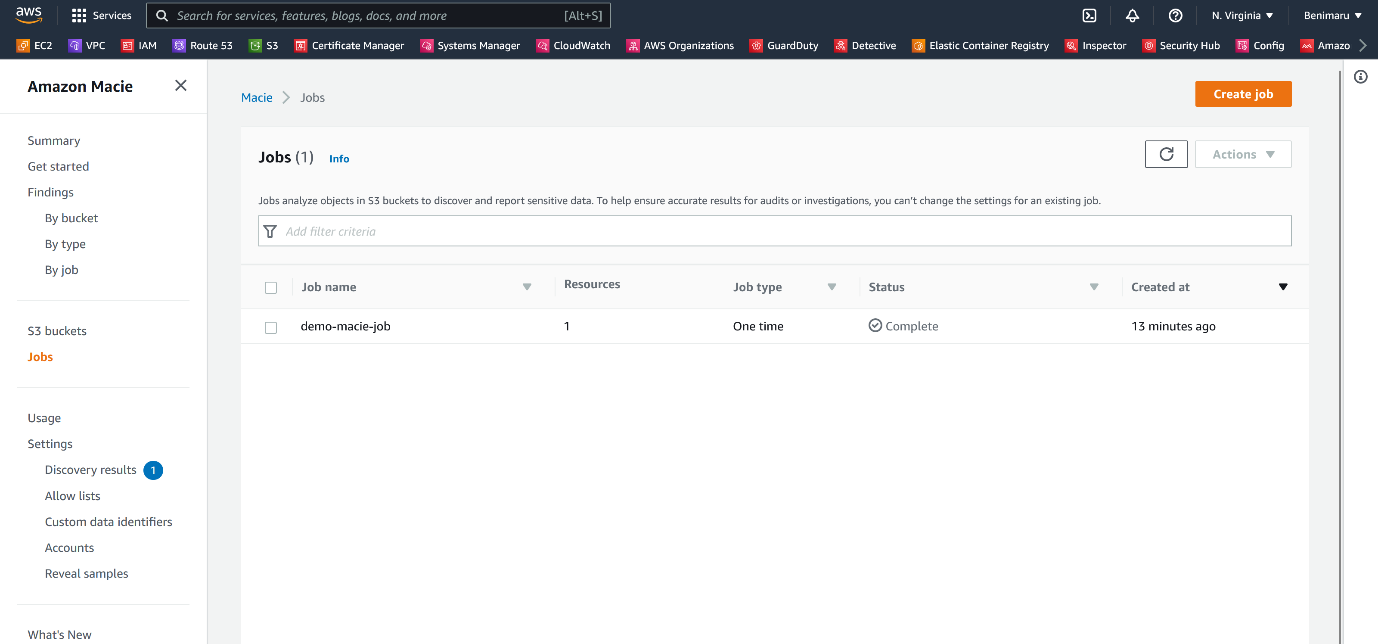
--- click on next.



--- click on next.



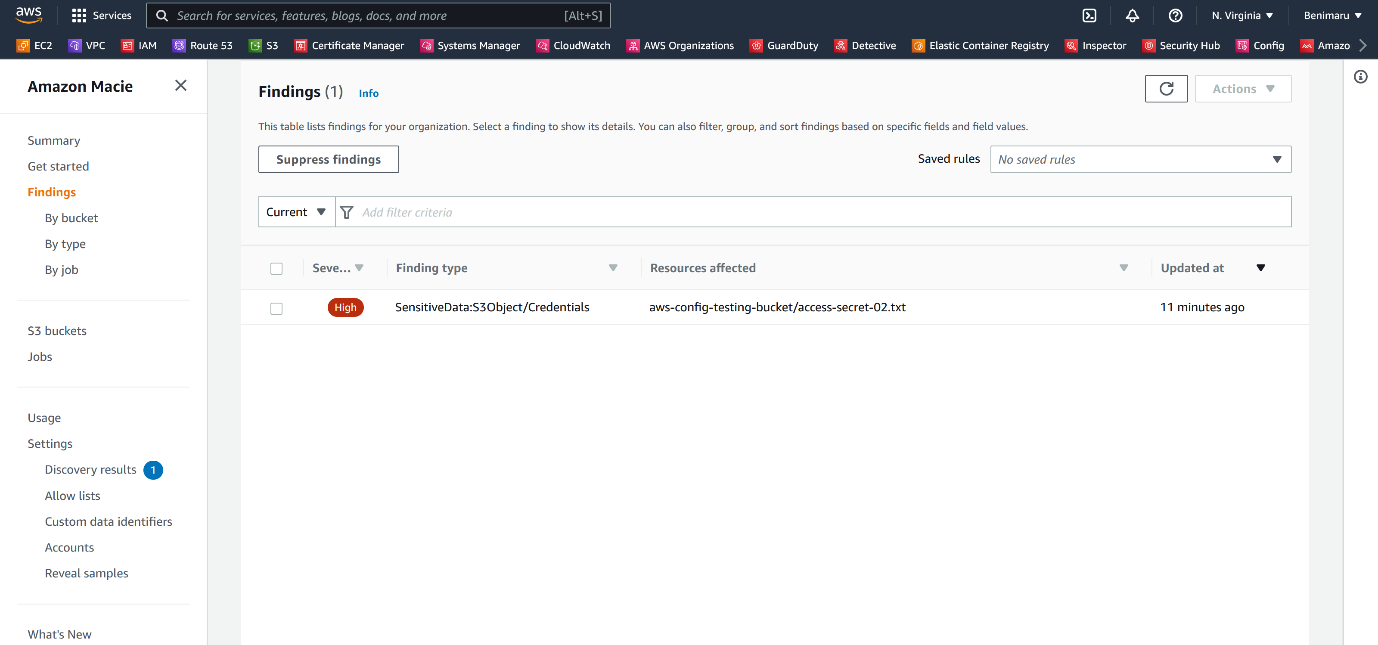
--- give the job name and click on next.



--- scan is completed after 13 minutes.

**Scan results**

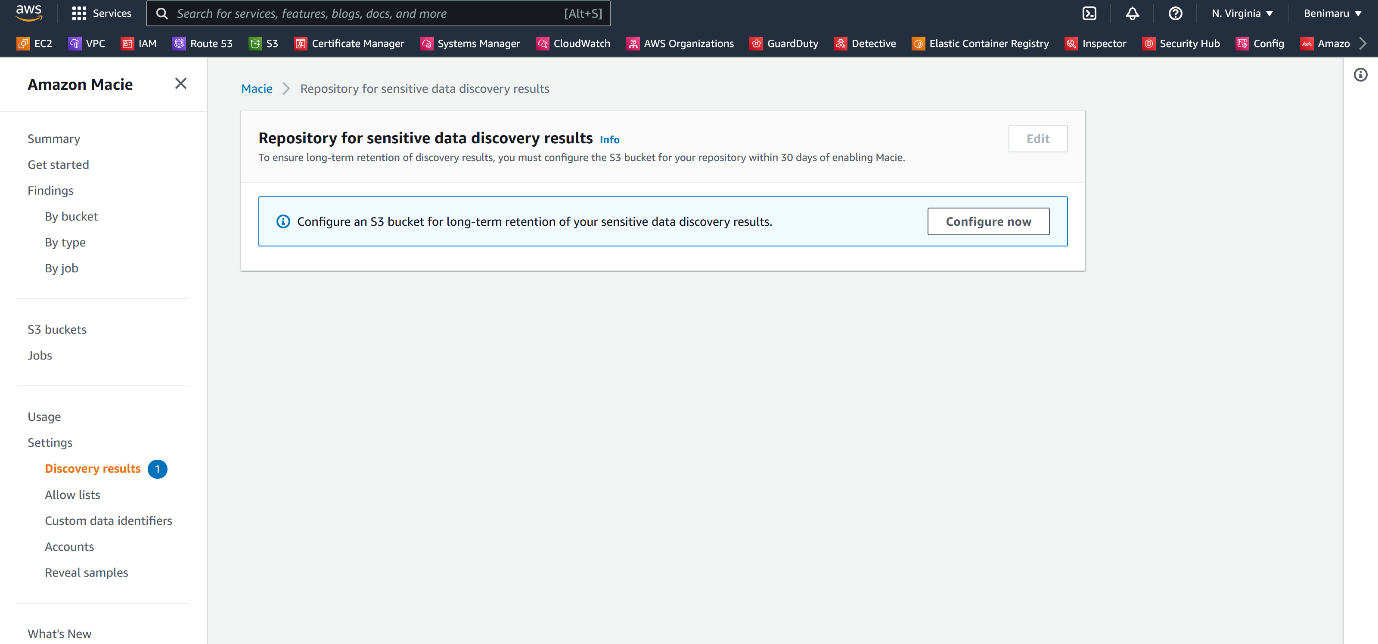
--- click on findings to see the scan results.



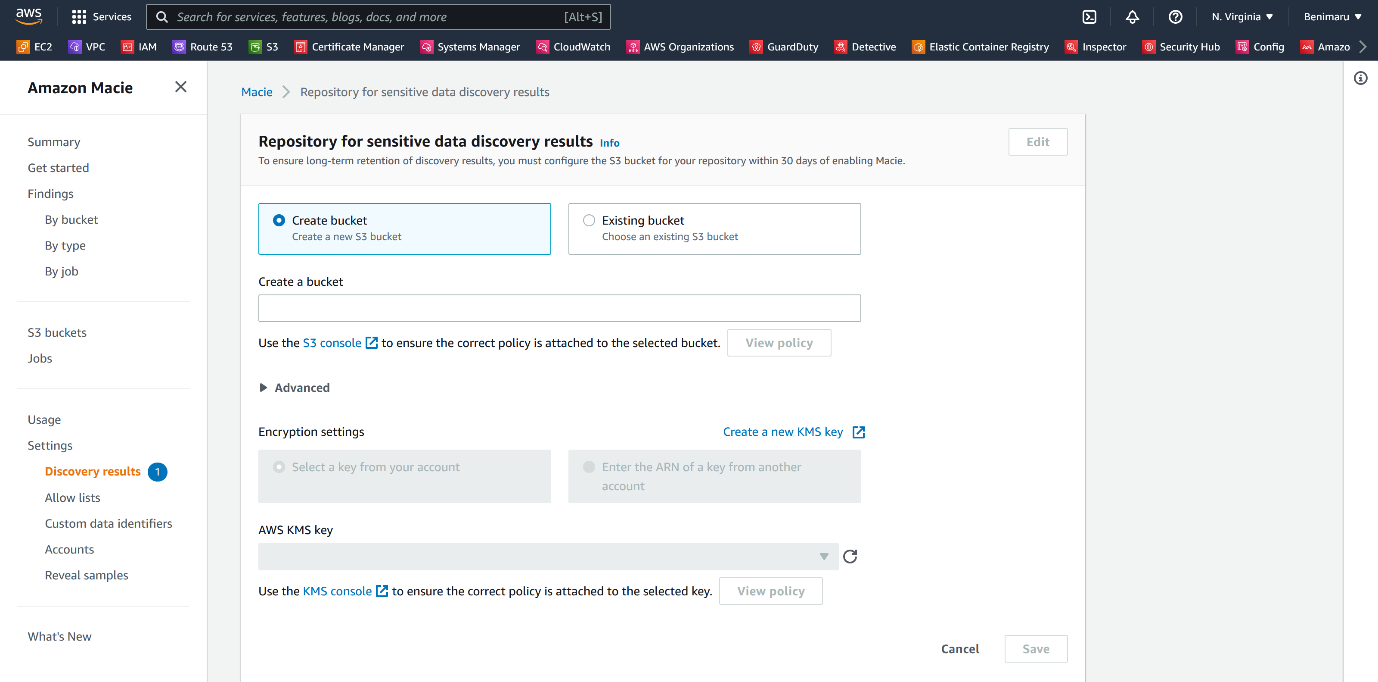
--- it founded the credentials file.

**Store your results in s3 bucket**

--- you can configure s3 bucket and store all your results. this is something we do in production level.

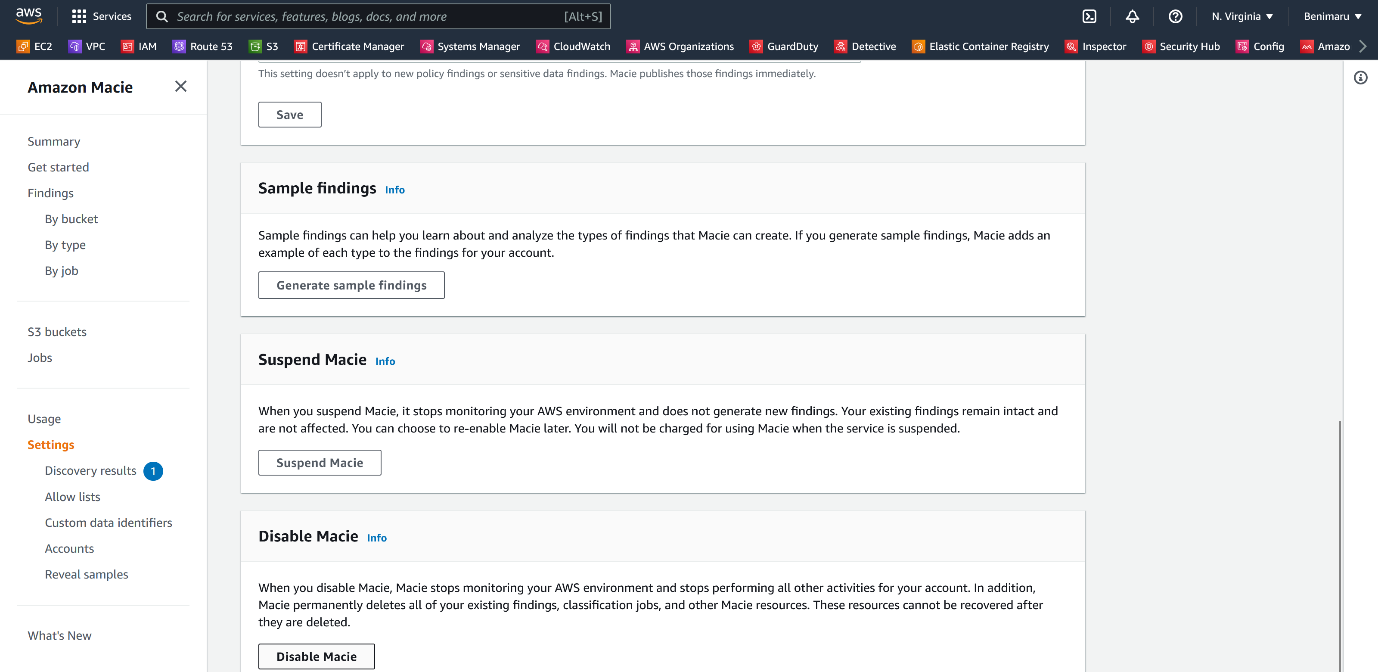


--- click on configure.



**Disable macie**

--- click on settings and scroll down.



--- we have the option to disable macie.