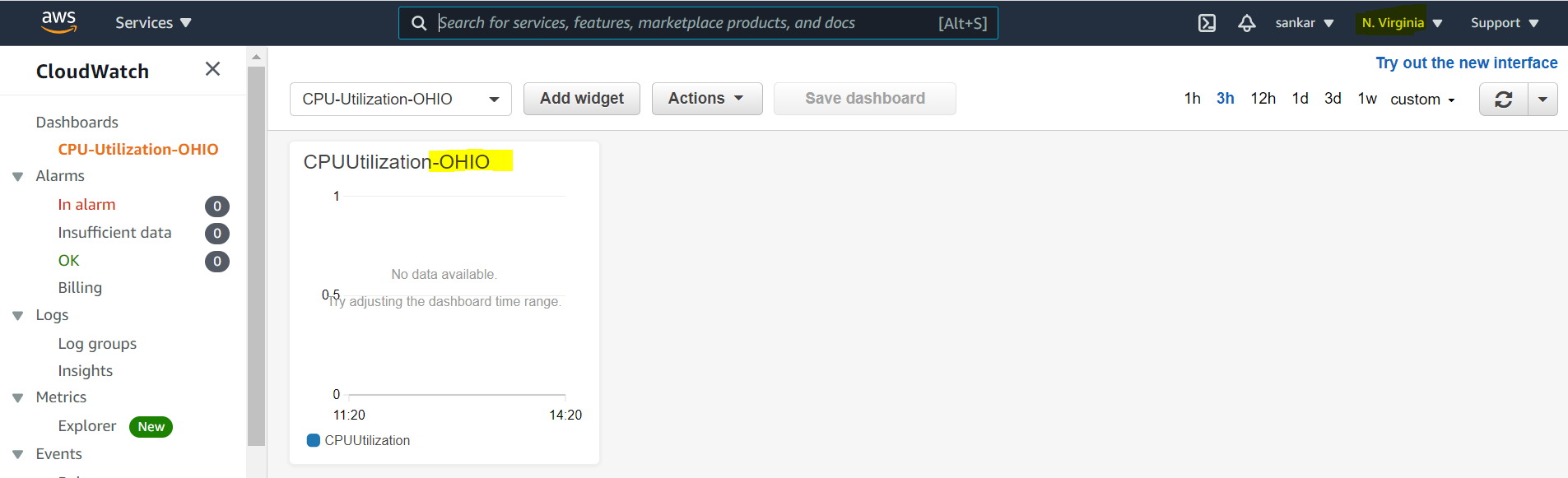
Cloud watch Dashboards are global not specific to region:



Created in OHIO region and dashboard can be checked in N.V region.

Application will send logs to cloudwatch using SDK’s

Logs will collect from :

Elastic Beanstalk: collection of logs from application

ECS : collection from containers

AWS Lambda : collection from function logs

VPC Flow Logs : VPC specific logs

Cloud watch log agents : EC2 machines

Route 53 : Log DNS Queries

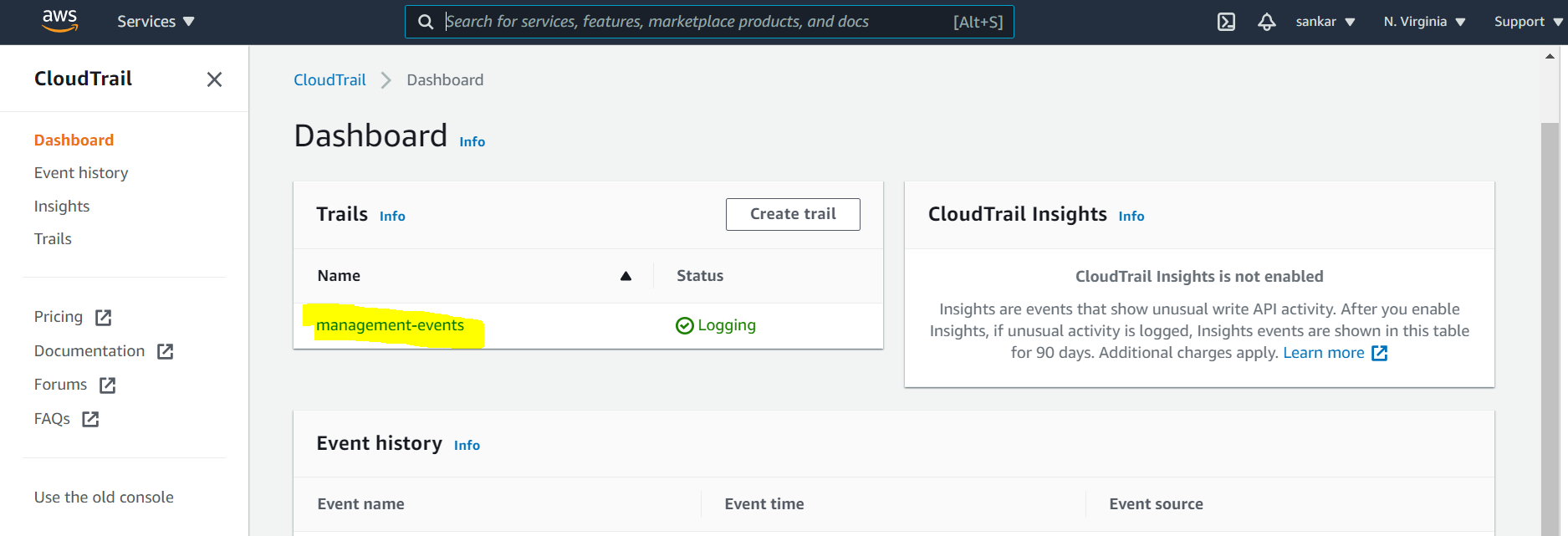
Cloud watch can send logs

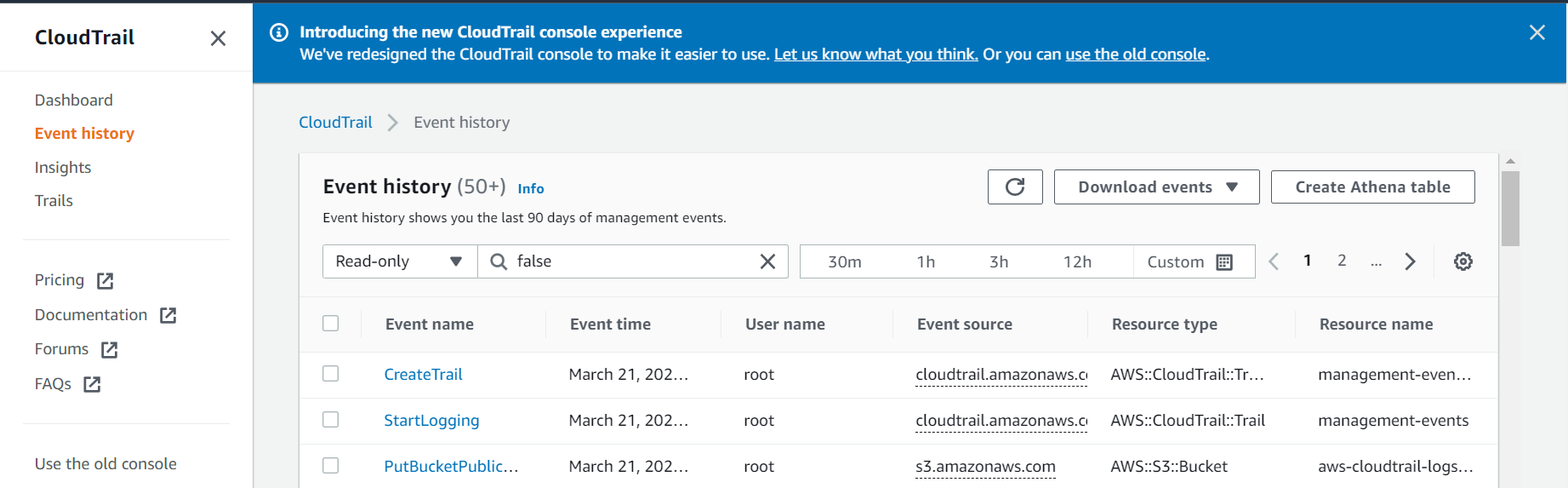
S3 : For archival

Elastic Search for analysis

CloudTrail:

Capture all the events of resources to cloudtrail

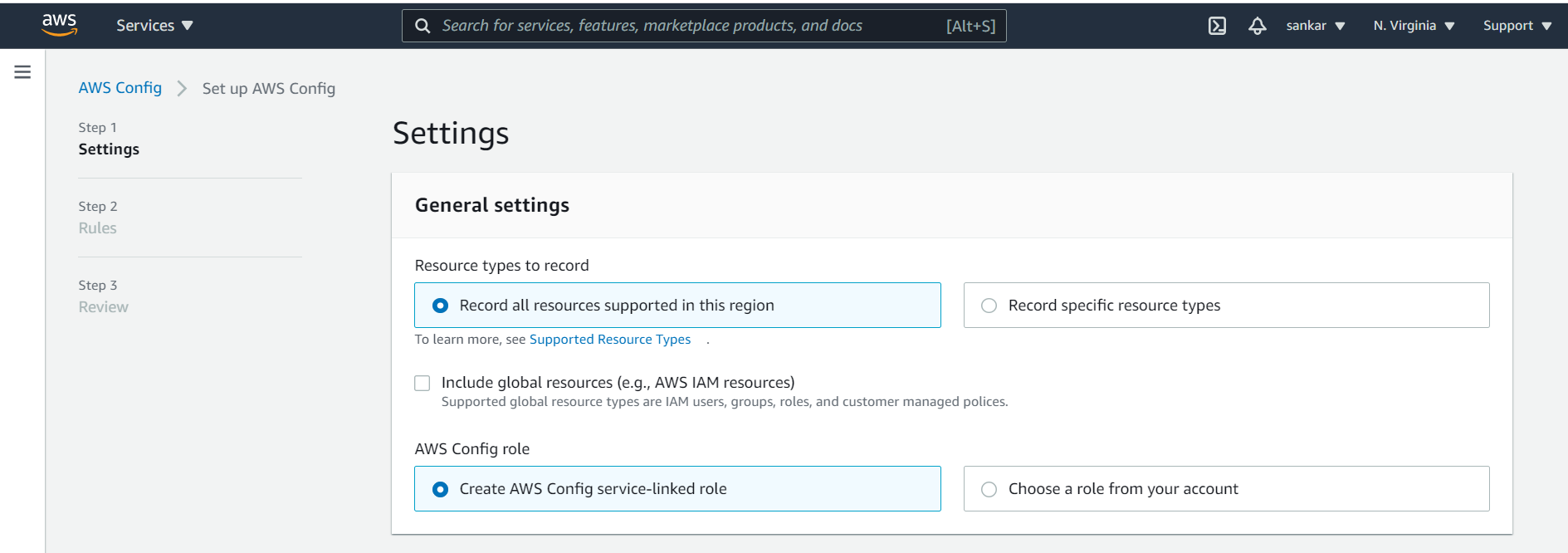




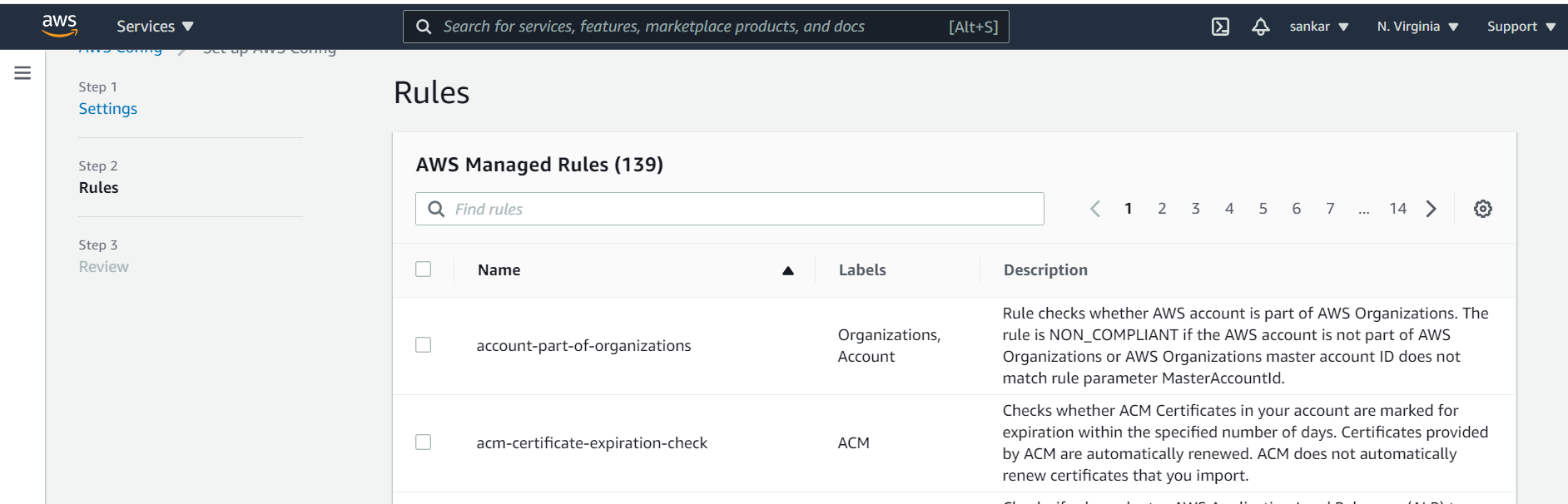
We can verify events also filter the events.

AWS Config:

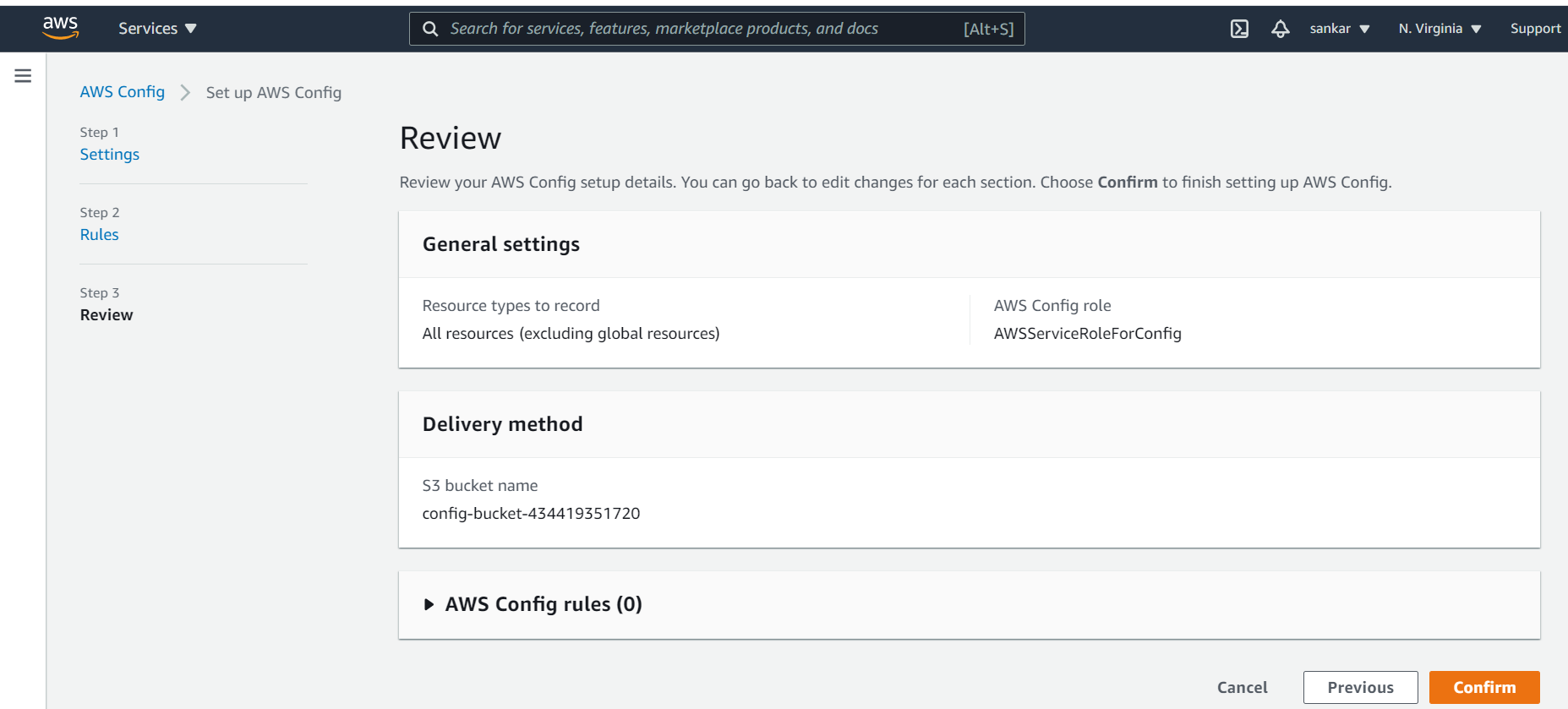
Monitor resources configurations, any changes it will alert an make it non compliance with time and date.



Leave all defaults and create config. (it will monitor all the resources)

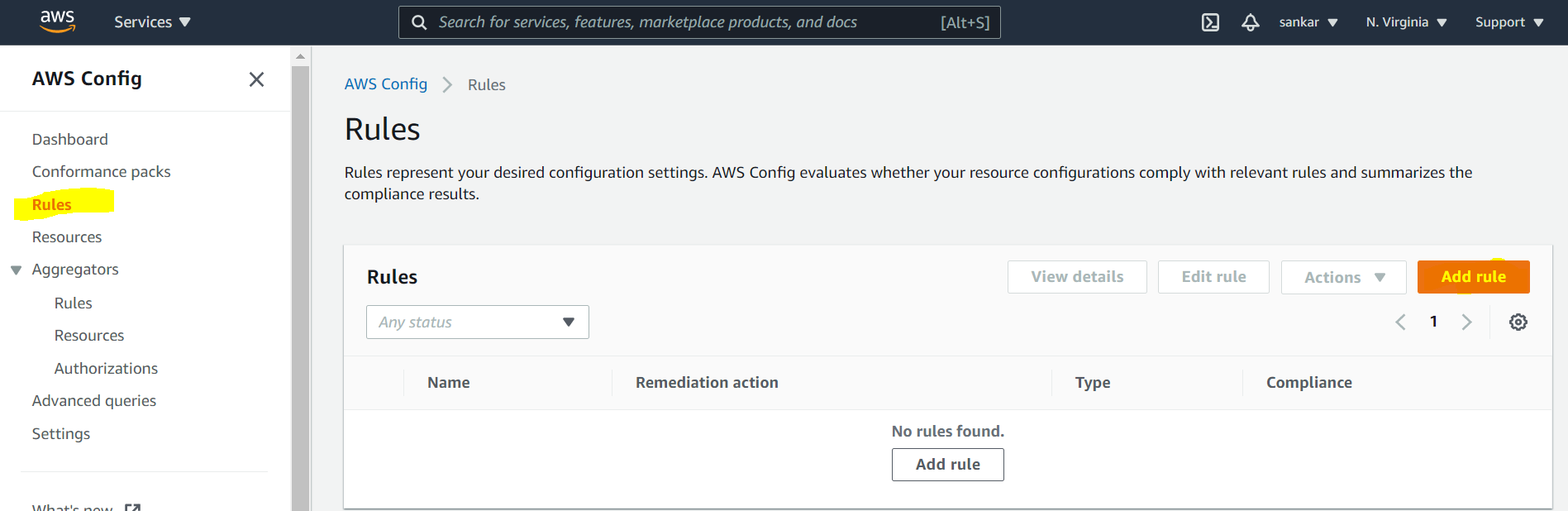


Leave default and click on next

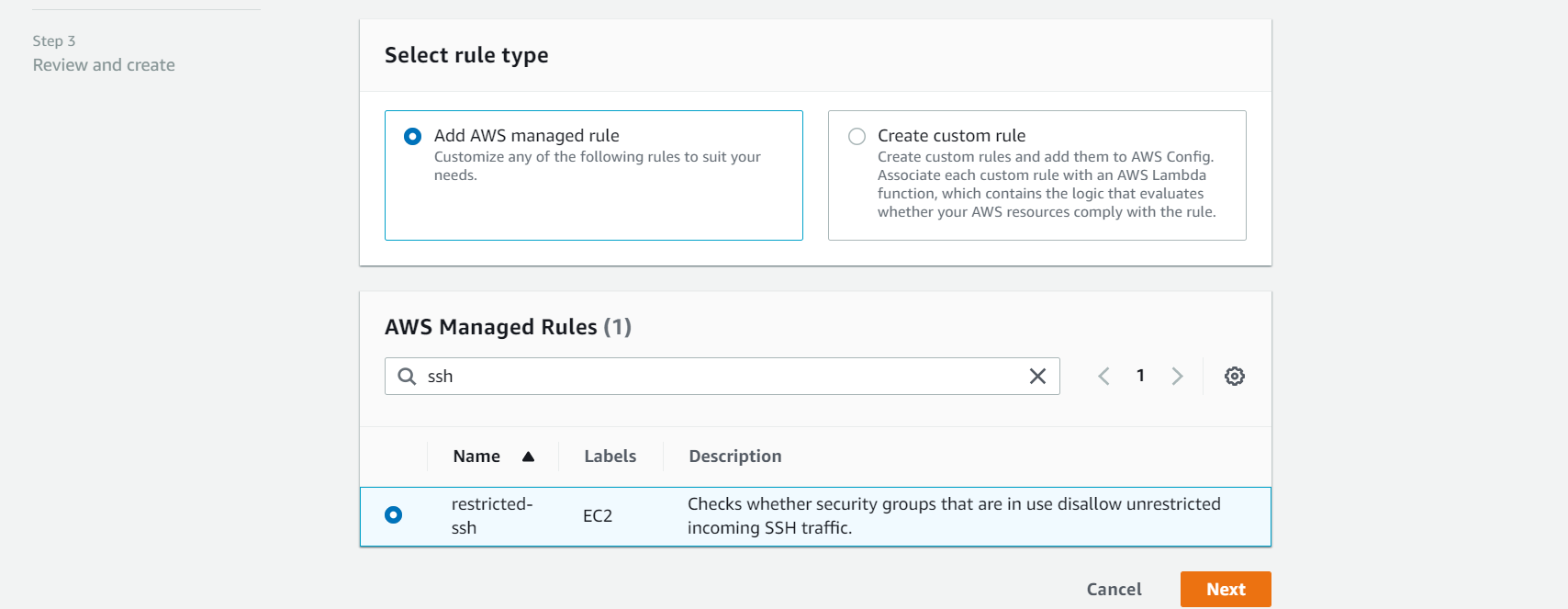


Click on confirm.

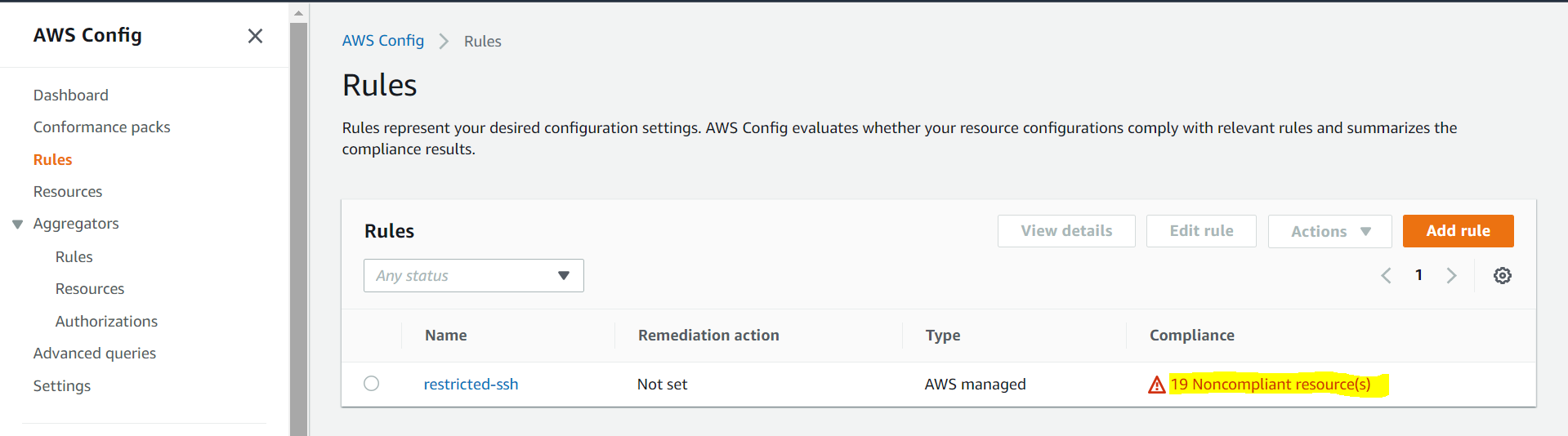
To create Rule, go to rules and click on rule



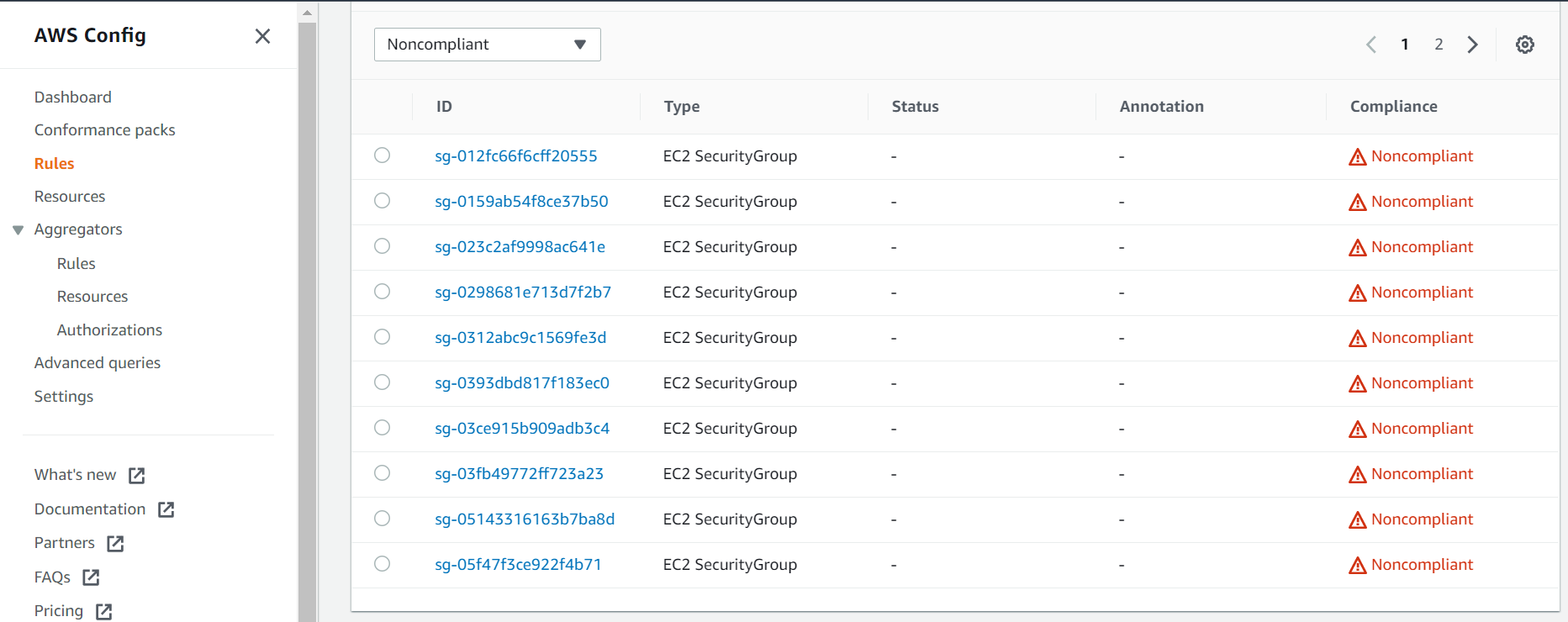
Search for specific rule to apply



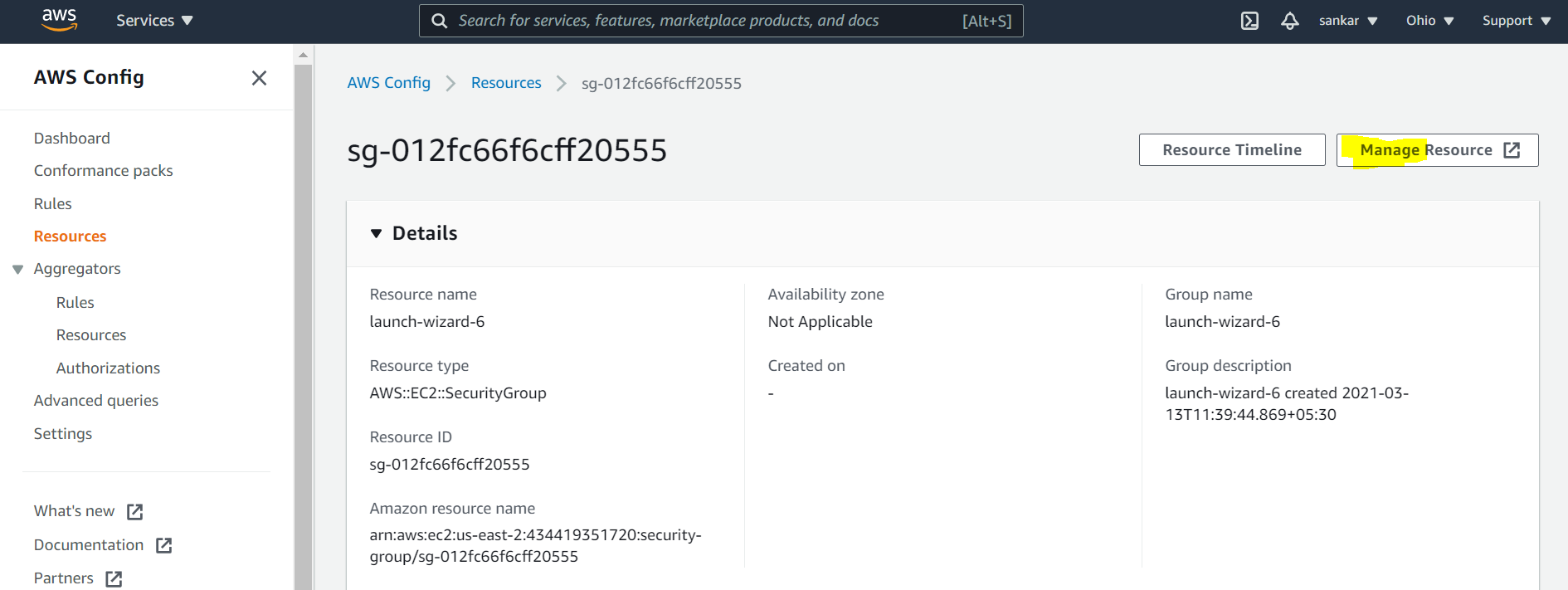
Once after rule is created, after some time we can check the non compliant resources.



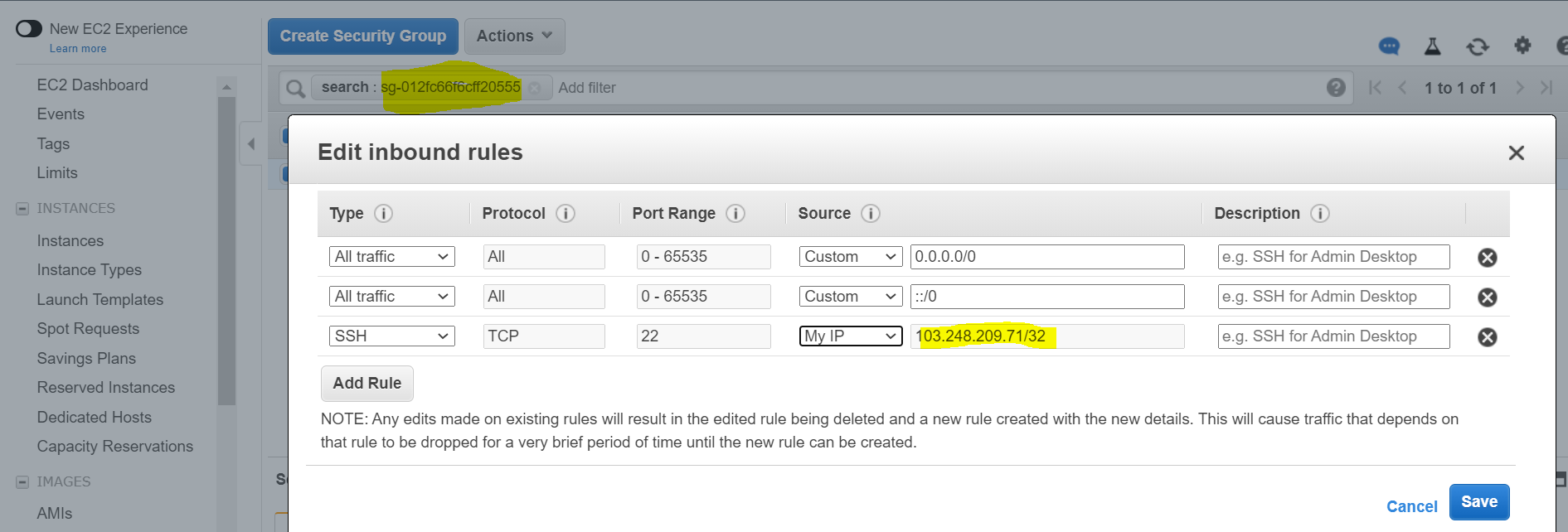
**Click on** the resources to get more details.



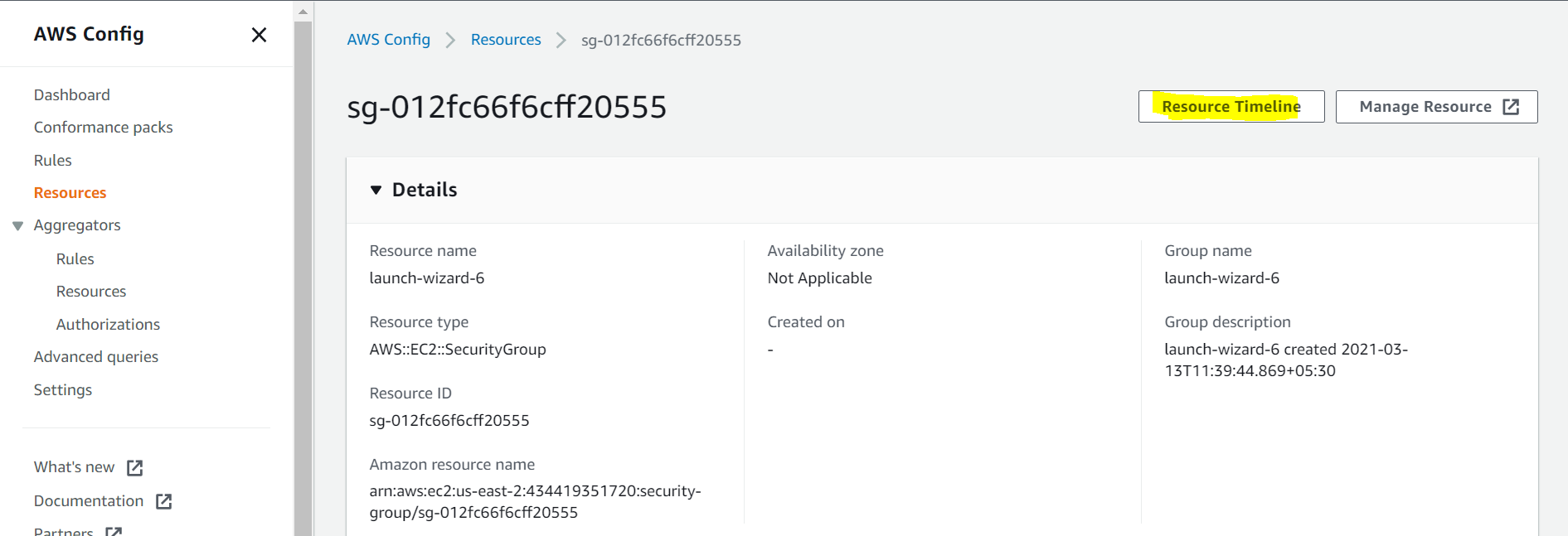
To go to the particular resource , click on the security group then click on managed resources.

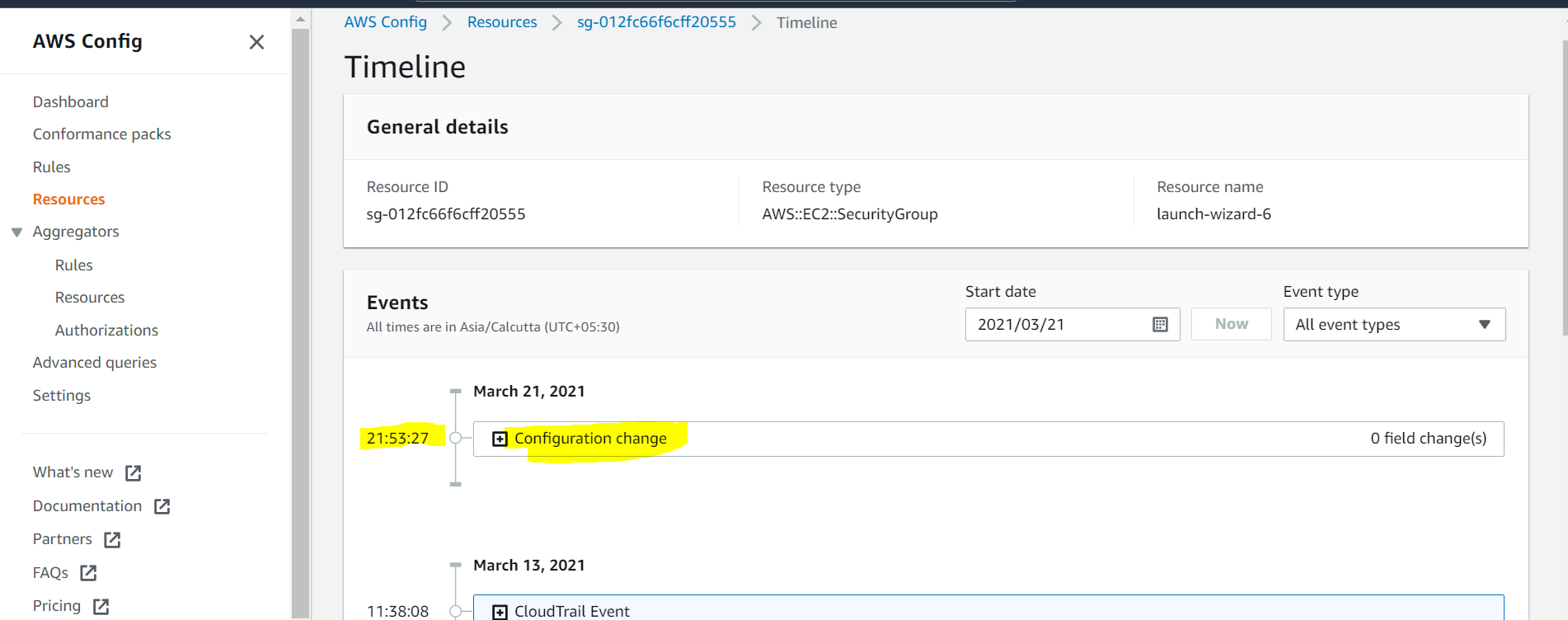


Change the port 22 inbound source to my ip



Click on resource time line to track the changes.





This will work on in use resources:

