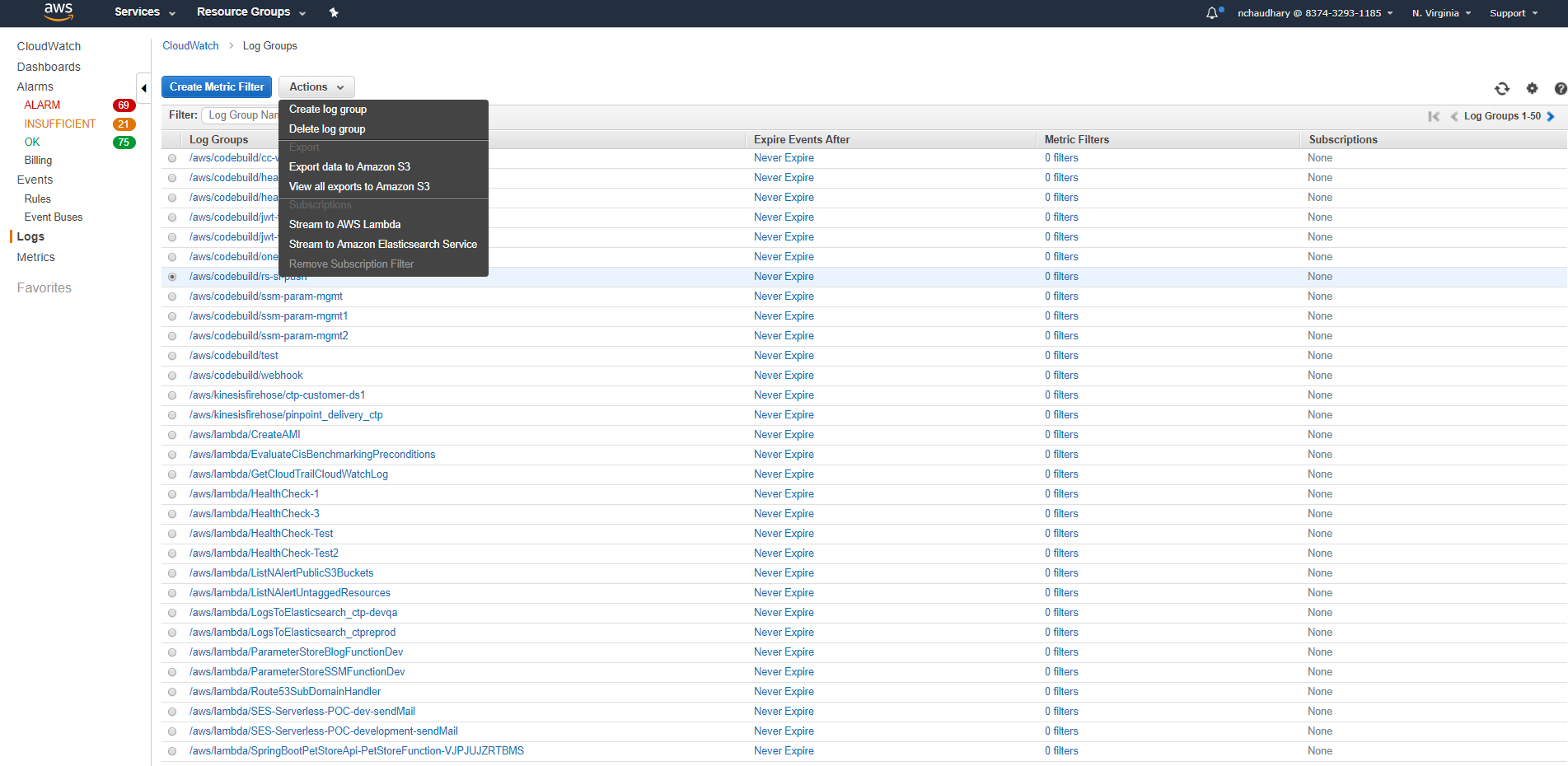
Configure and Enable Log Streams onto CTP Kibana

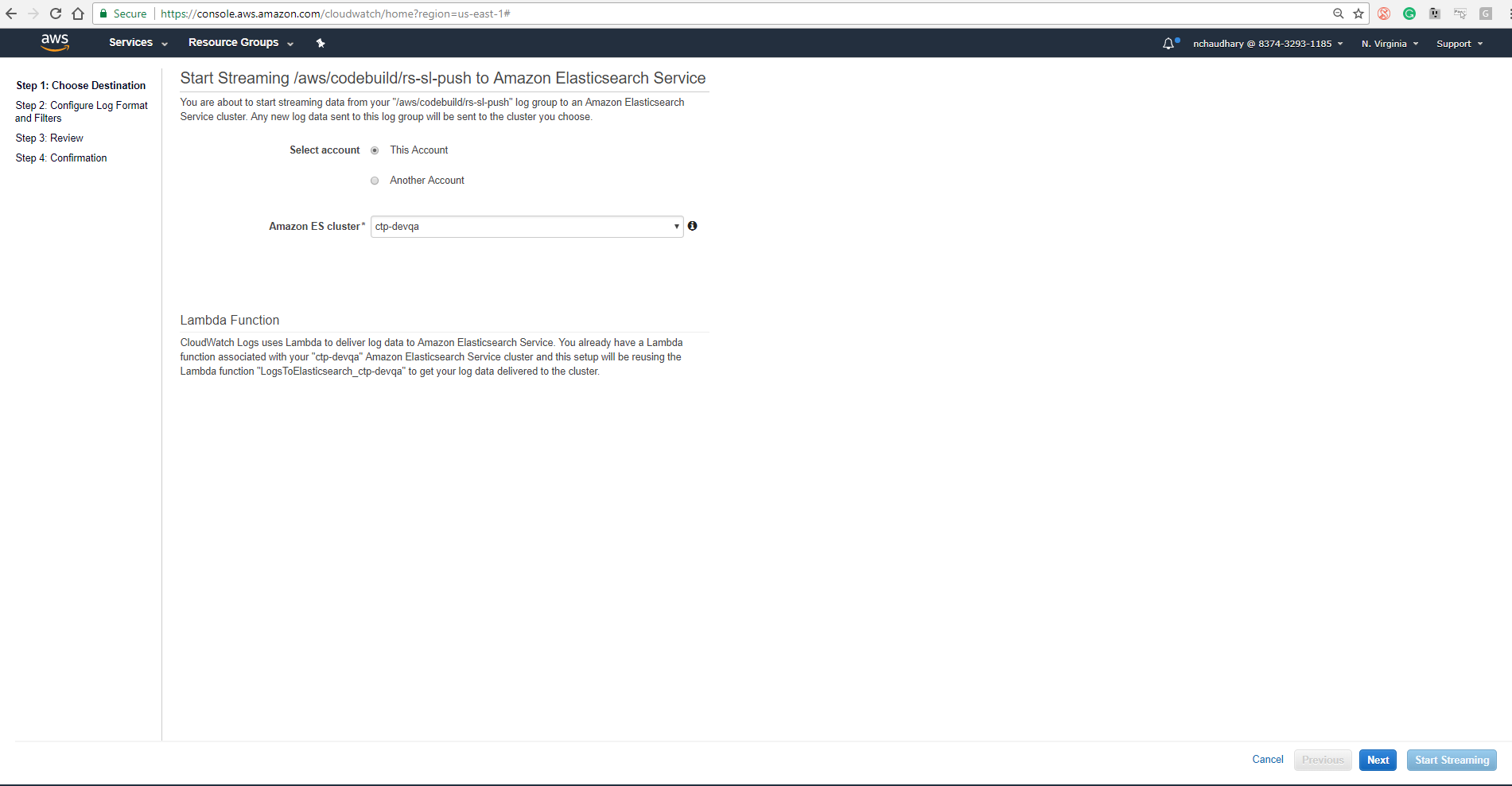
All logs get created in cloudwatch by ECS task configuration during the setup of a new service. These logs are then directly fetched into the cloudwatch.

These logs are organized in log groups in cloudwatch, each group contains different services for each of the application team. These log groups can be streamed into Elastic Search Kibana by following these steps:

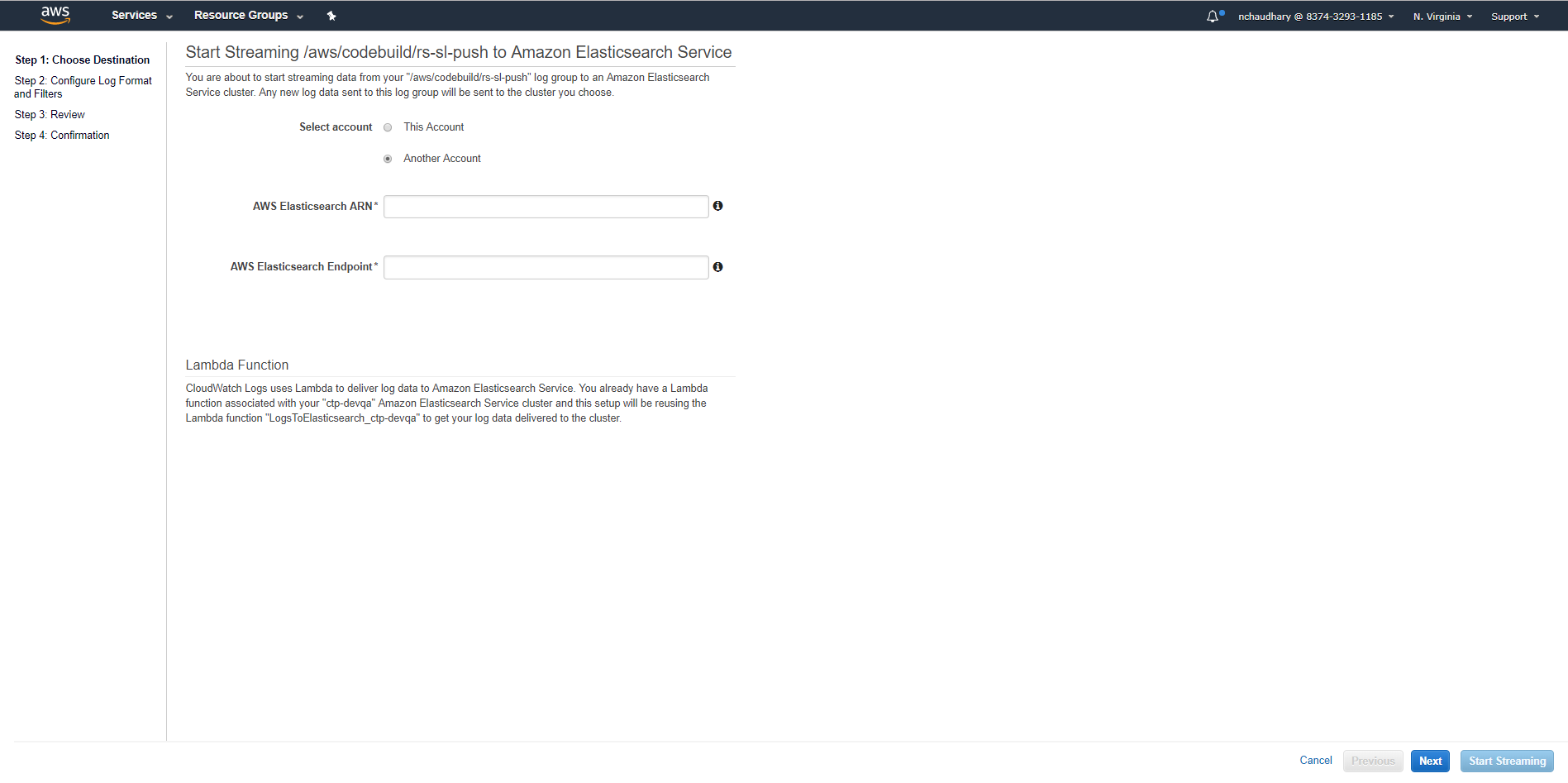
1. Click on any log group and under actions select “Stream to Elasticsearch Service”



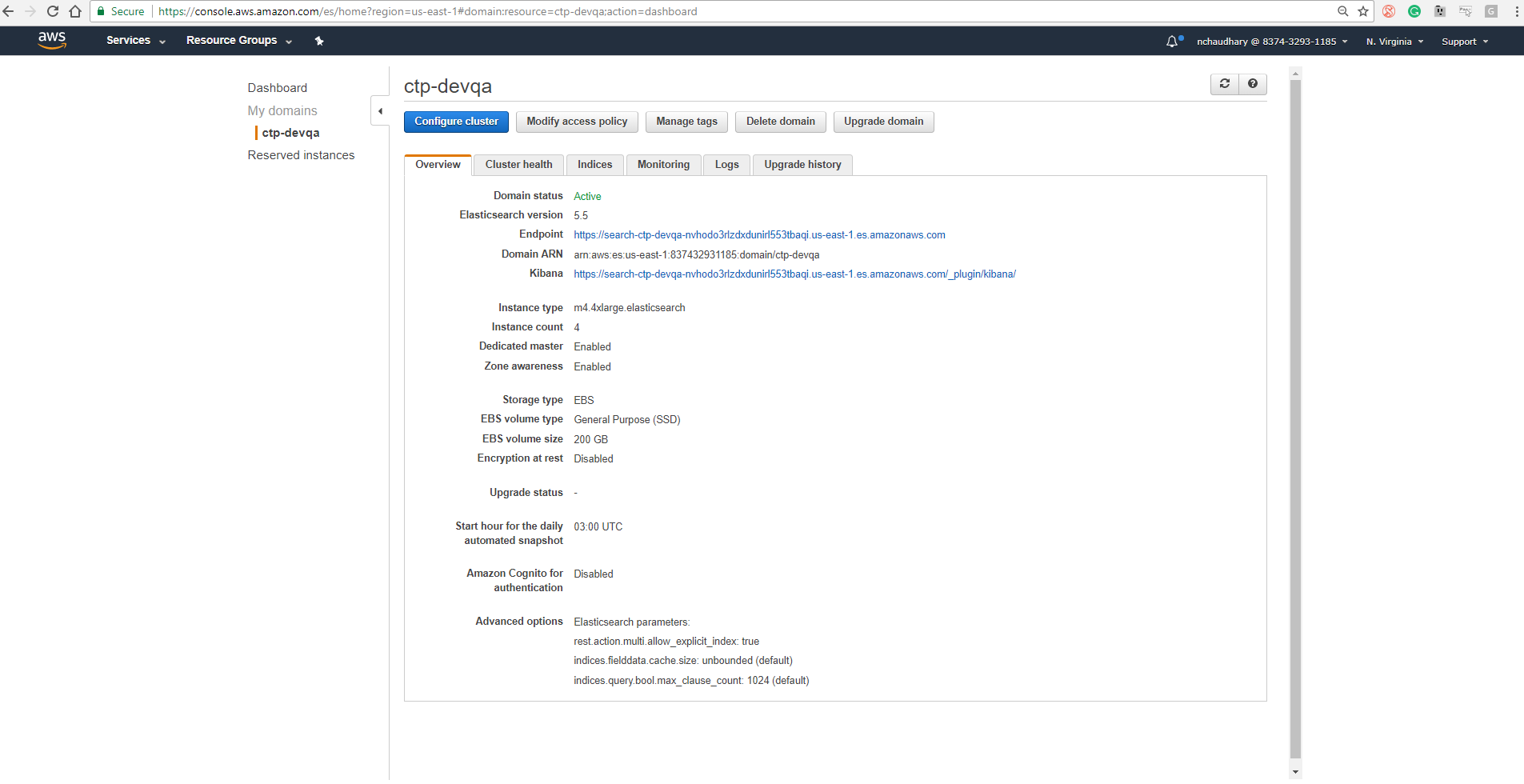
1. Elastic search treats different regions as different accounts. If the service is in same region, select ‘This Account’, if it is another region, select “Another Account”



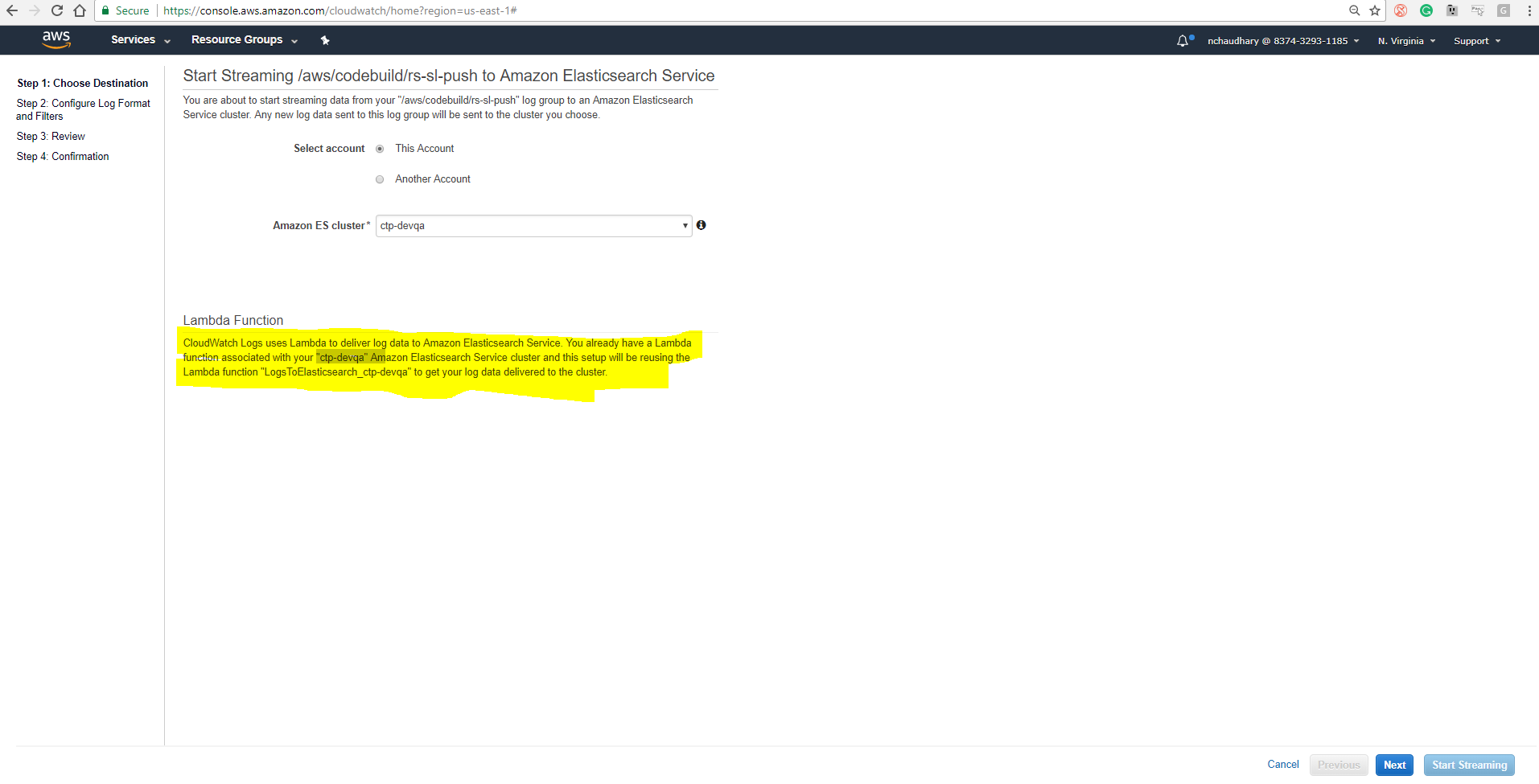
1. This step applies only if you are using a different region.



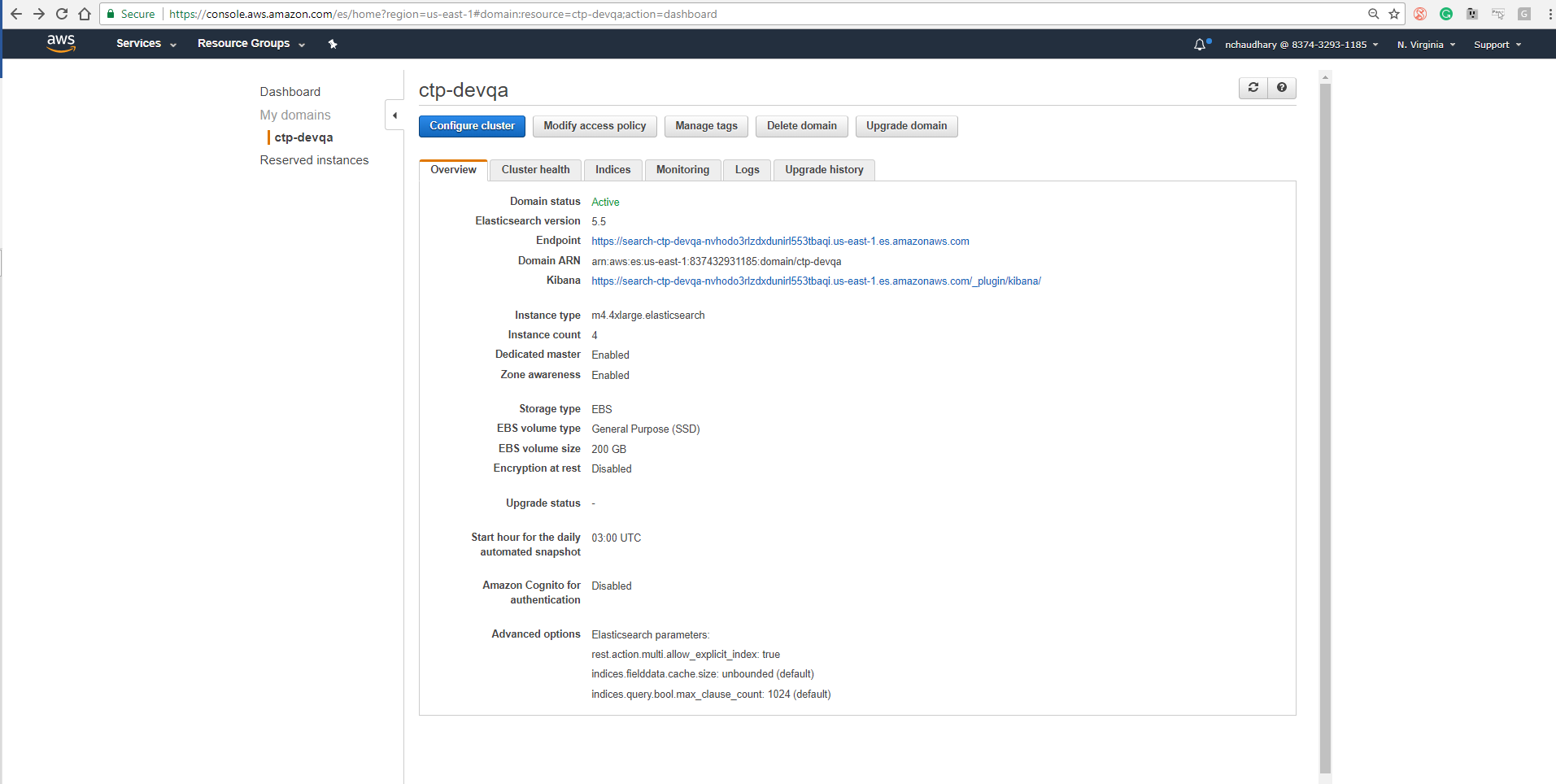
1. Provide the ARN for the cluster from “Elastic Search” service in AWS. For the Endpoint remove the https from the url.



1. Access policy for the Elastic Search is specified once whenever the cluster is created. You do not need to specify or add anything as the process automatically picks up the already created policy.



1. Any modifications to the policy can be made under ‘Modify Access Policy”



1. Select the Log format as JSON for output.
2. DONE