#######https://medium.com/@arun.gowda/securing-aws-elasticsearch-service-by-cognito-authentication-f4cd1ff7953c#######

--------Use AWS Elastic Search Service with Cognito Auth-------

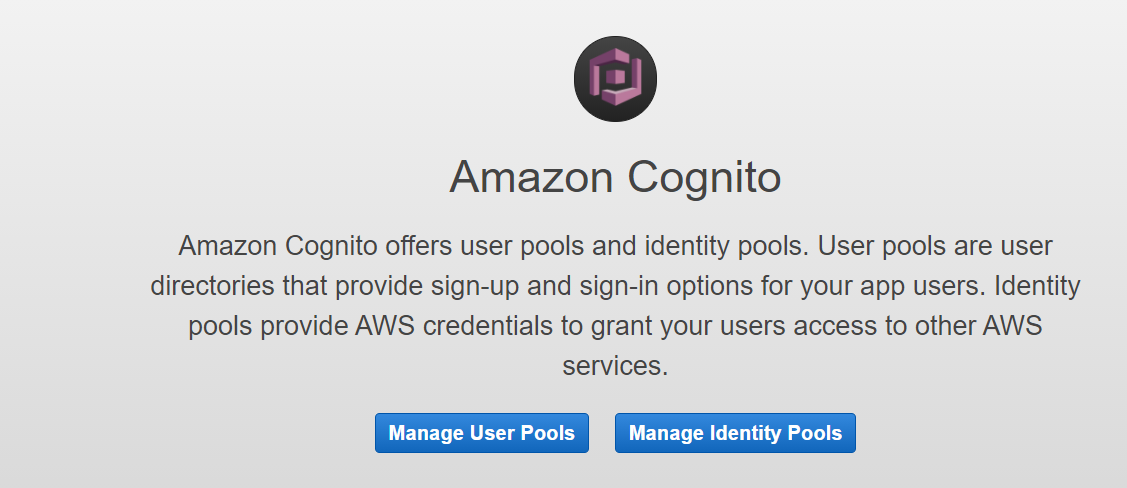
--------Setting up User Pool-------

#####Userpool is for managing users and groups. Inside User pool, we create users and add those users to Groups

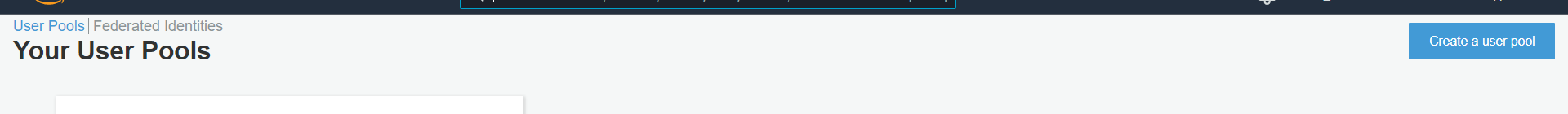
1. Open the AWS Management Console and sign in.

2. Go to the services section and type Cognito, you will get an option for Amazon Cognito, click on that and you will get a welcome dashboard for Amazon cognito.

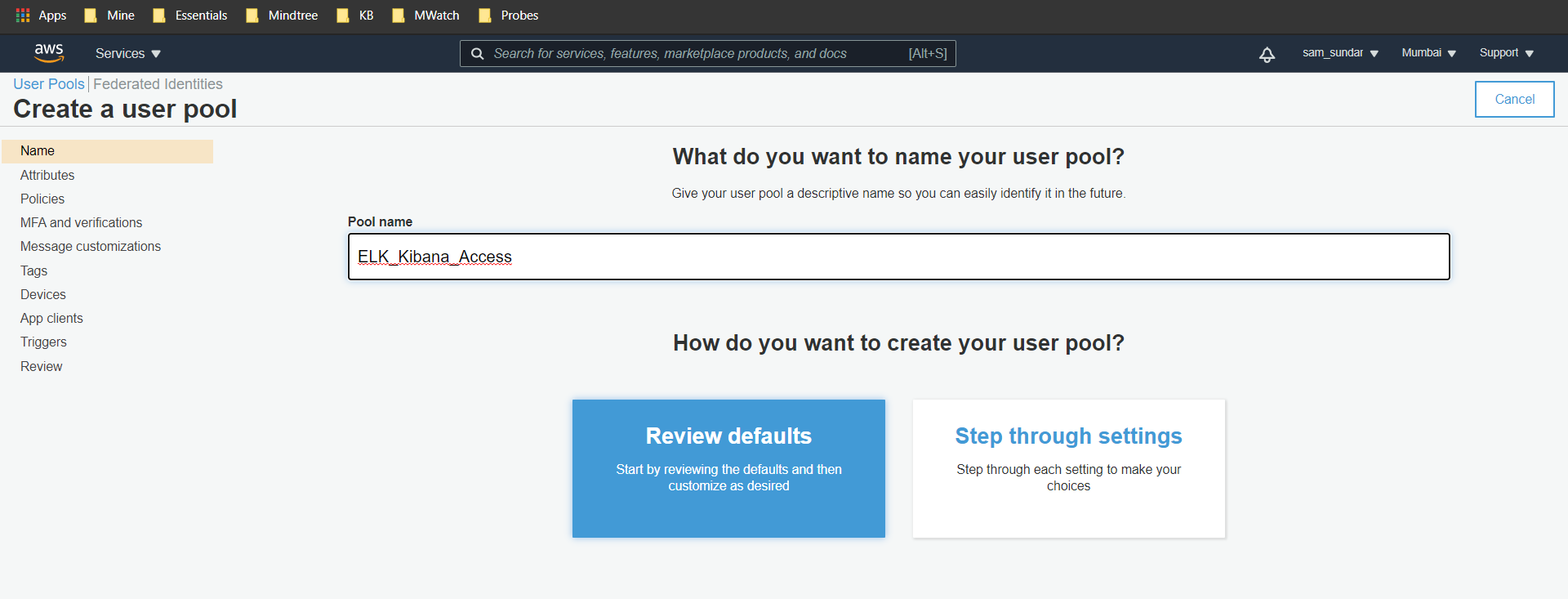
3. Click on Manage User Pools section.



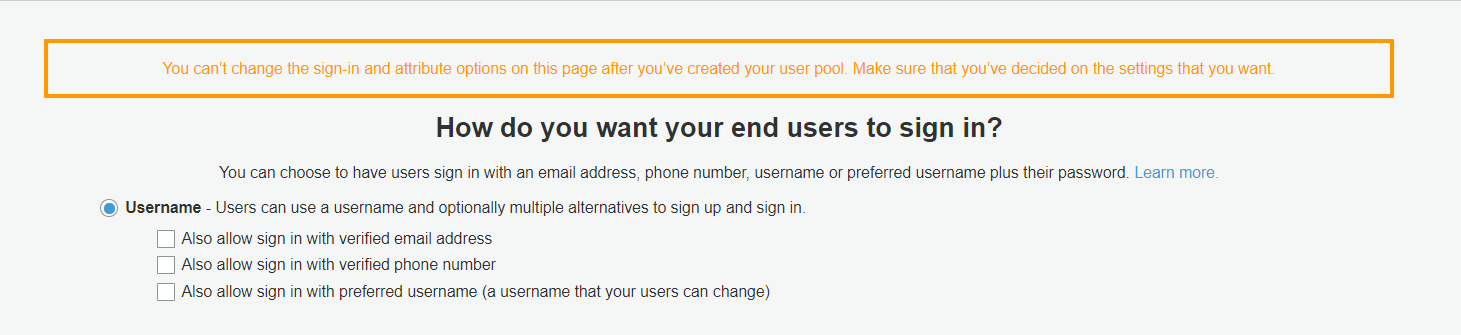
4. Click on Create a user pool on top left section.



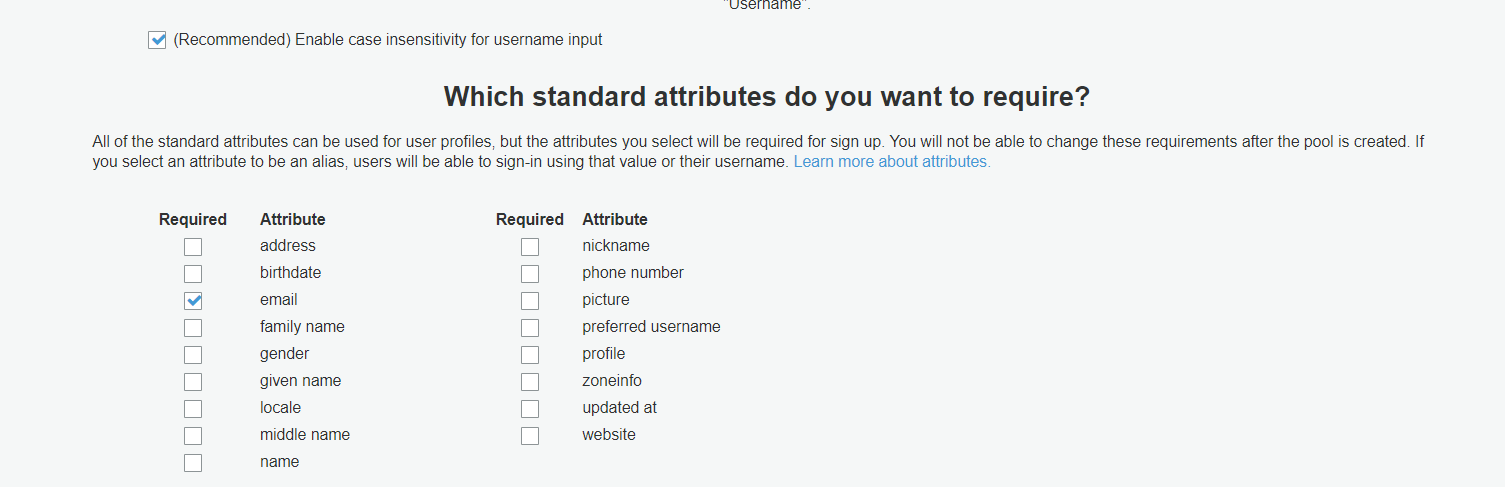
5. Give the user pool a name. In this example, I named my pool "ELK\_Kibana\_Access". You can step through the settings or choose the defaults. For now, choose Review defaults.



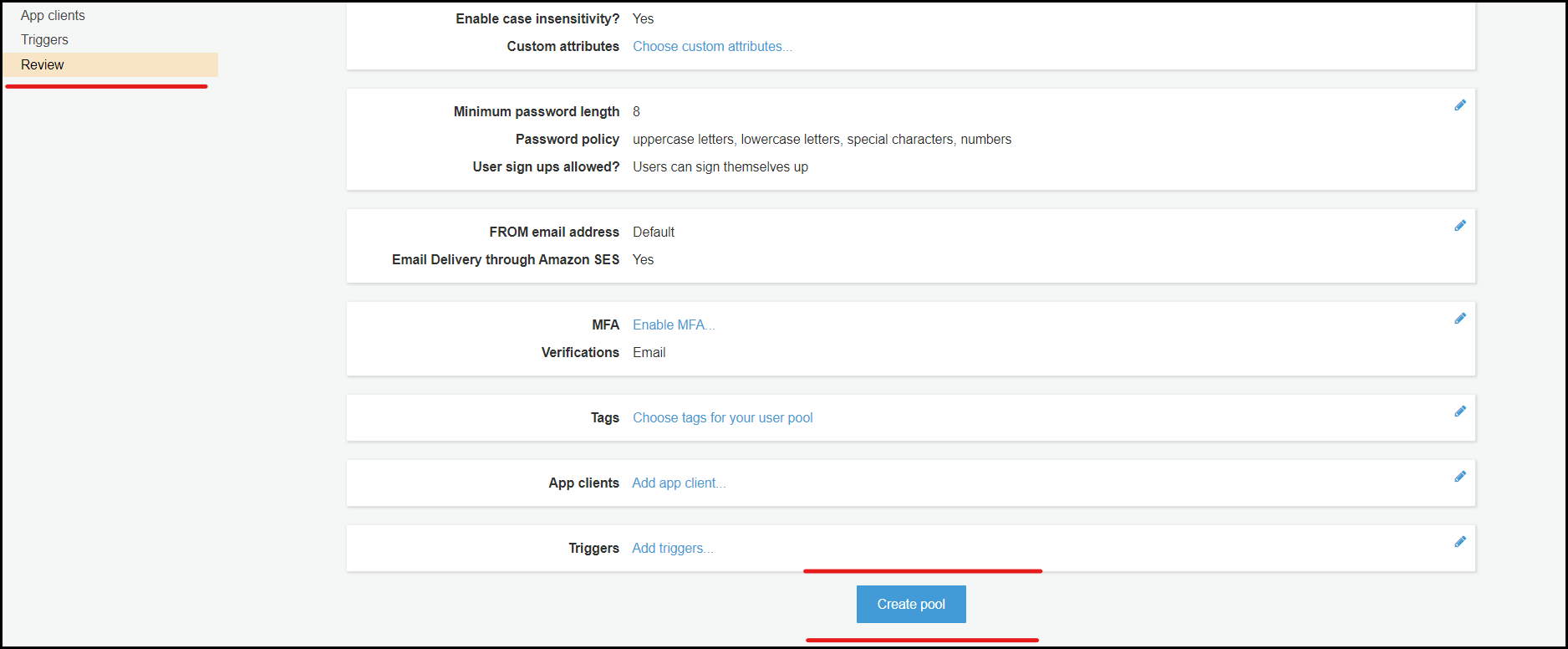
6. Click on attributes section which is on the top left section of the page.



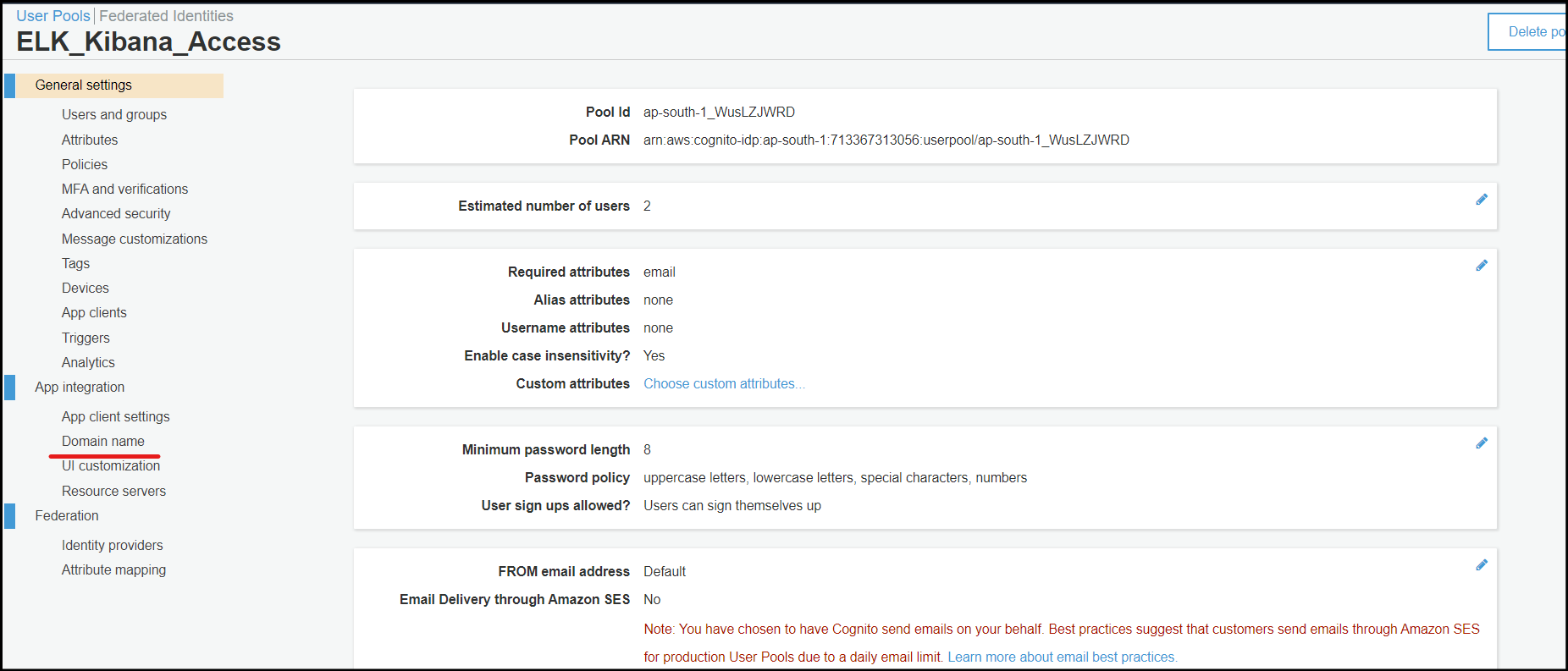
7. Verify that username option is checked and in standard attribute section email is checked.

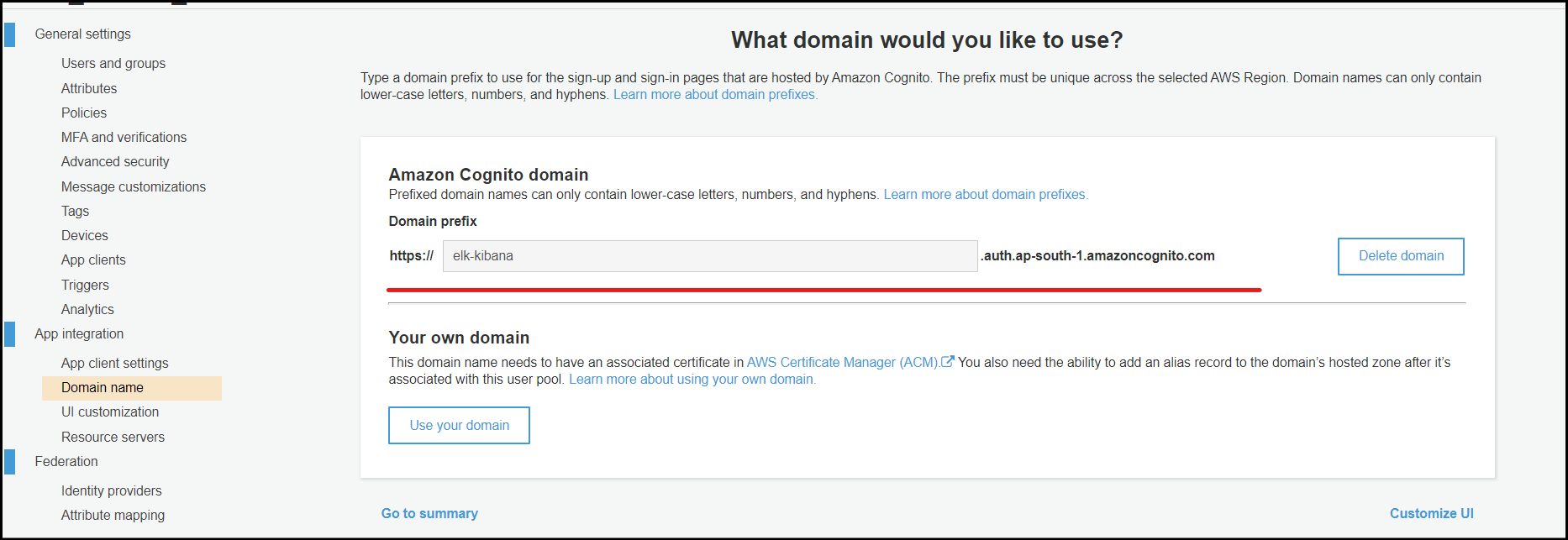


8. Once done click on the review section and click on create pool.

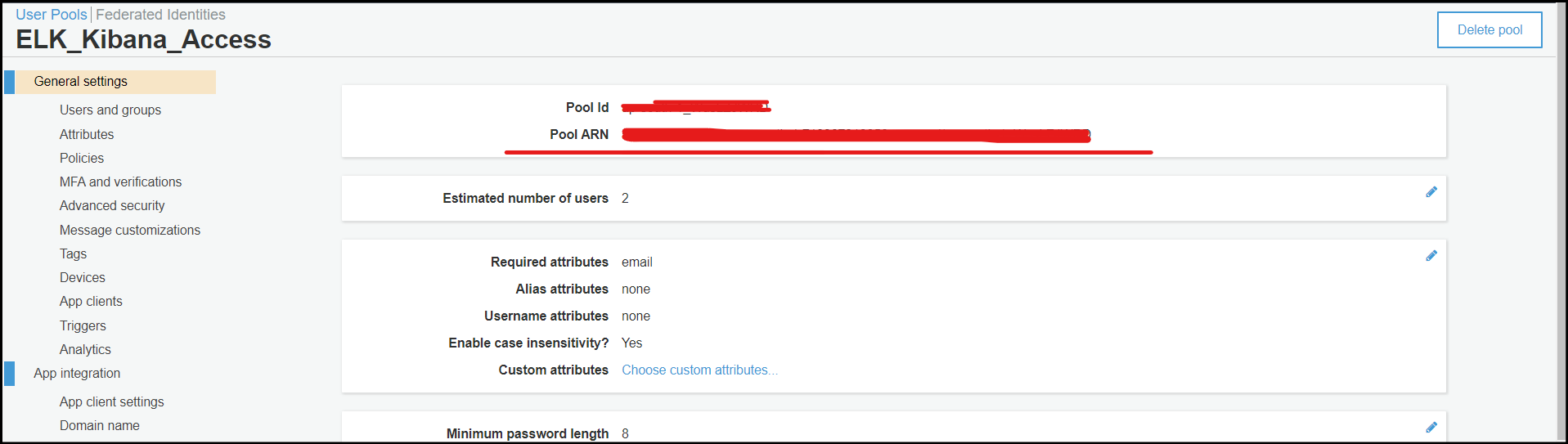


9. Click on domain name section on the left .Type a name in the text box. In this example, I used "elk-kibana". Be sure to choose save changes.

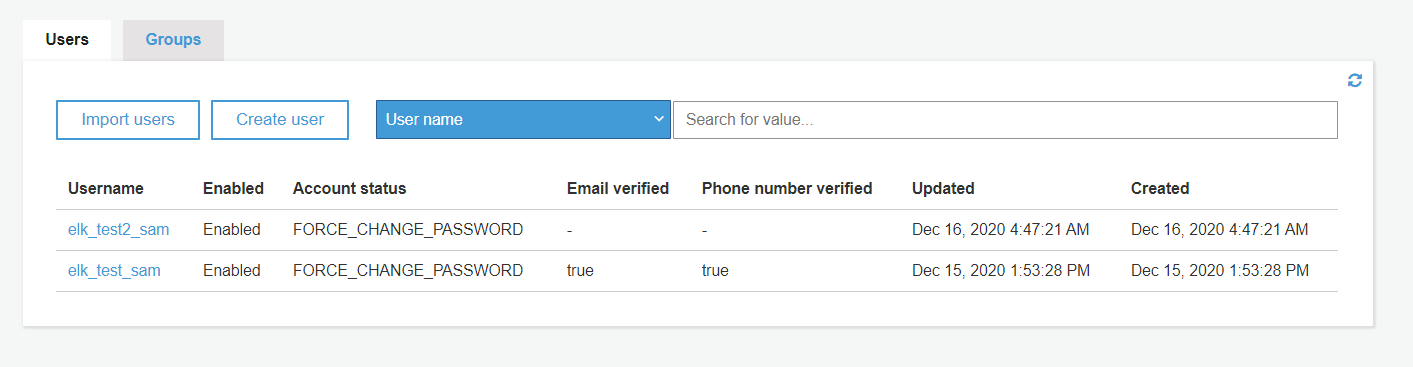




10. Make a note of Pool ID, we need those details again when we shall be creating the user identity pool.



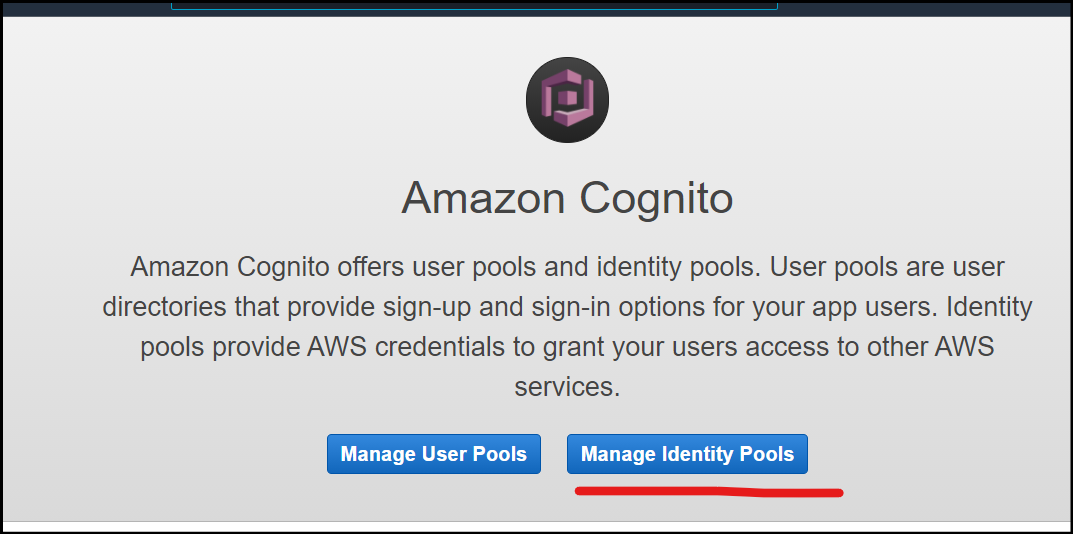
11. Create a user in userpool under "Users and groups" option and this is the user with which we will be able to login into Kibana endpoint



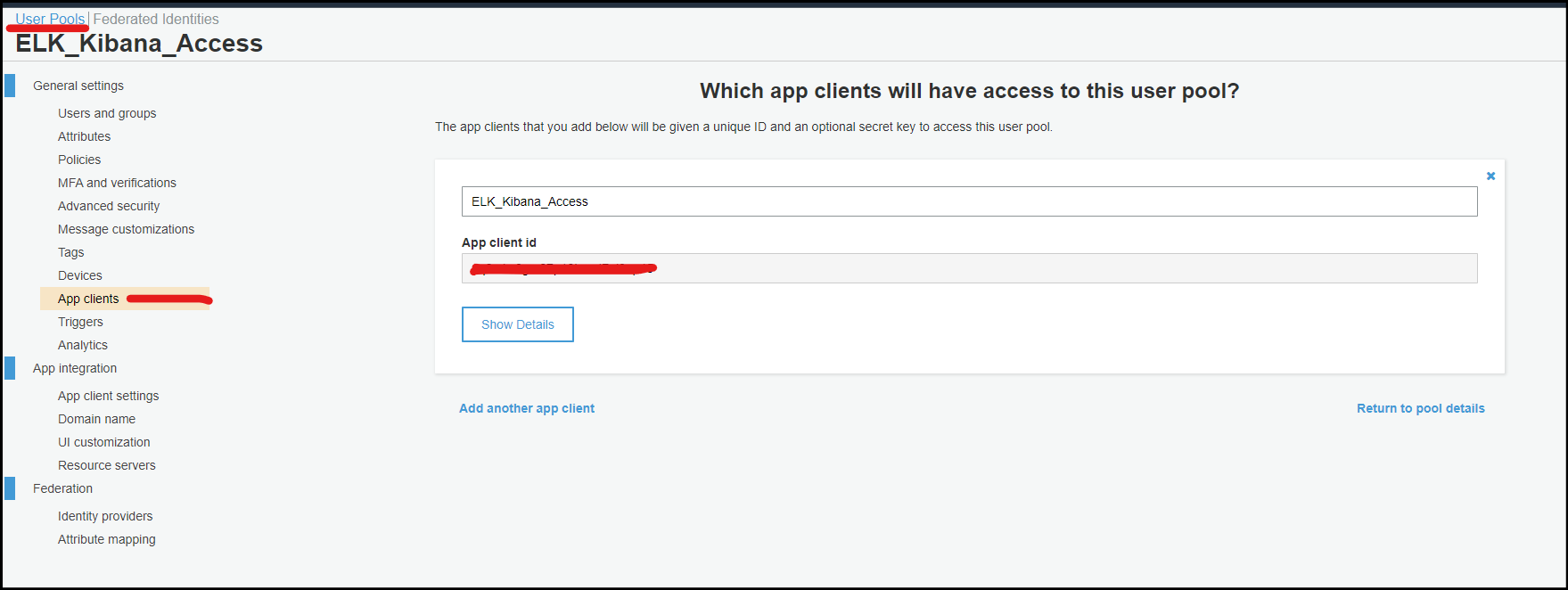
--------Setting up Identity Pool-------

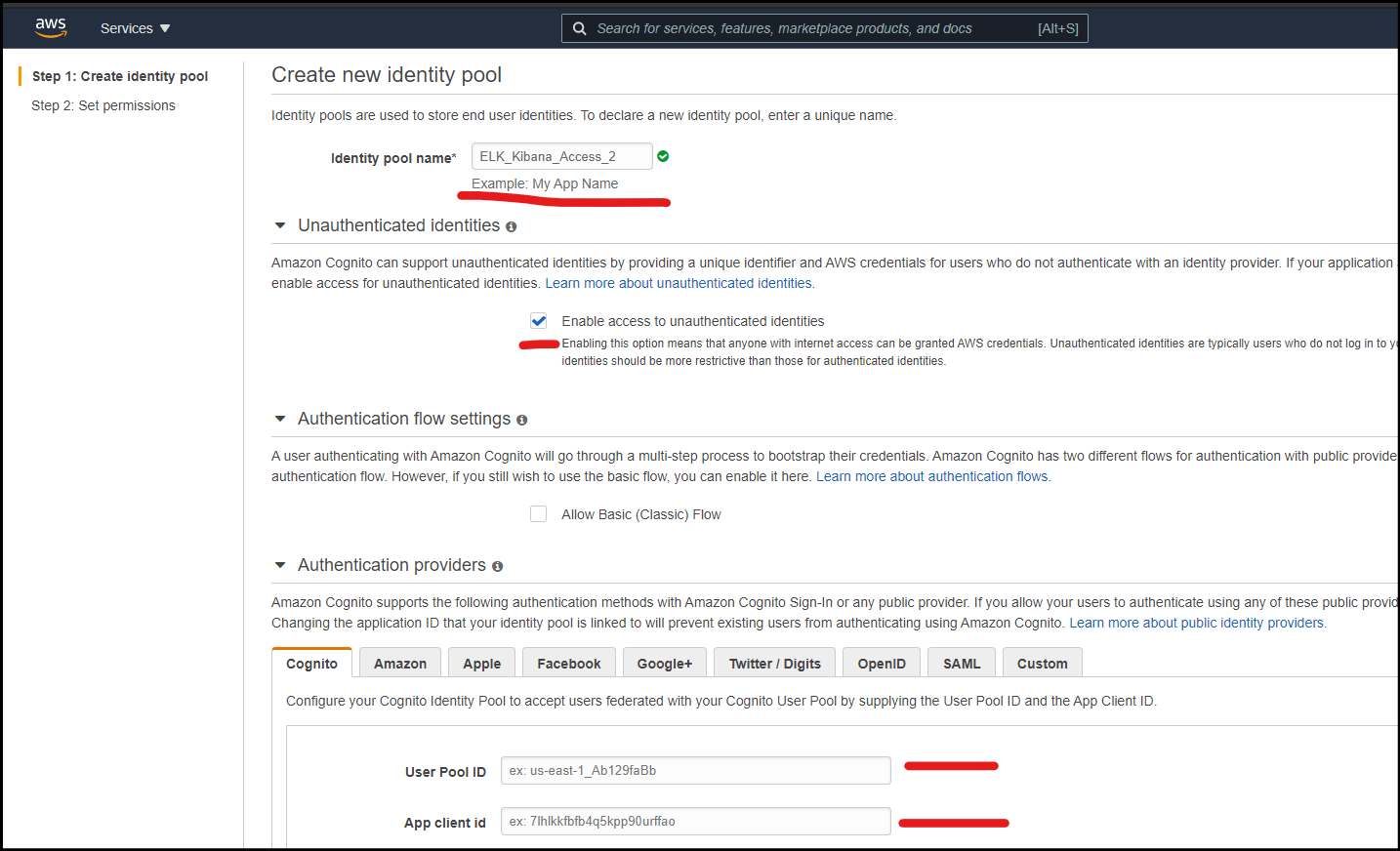
########Identity pool is to give level of access to our user pool

1. Give your identity pool a name. I chose "ELK\_Kibana\_Access". Then select the Enable access to unauthenticated identities check box.

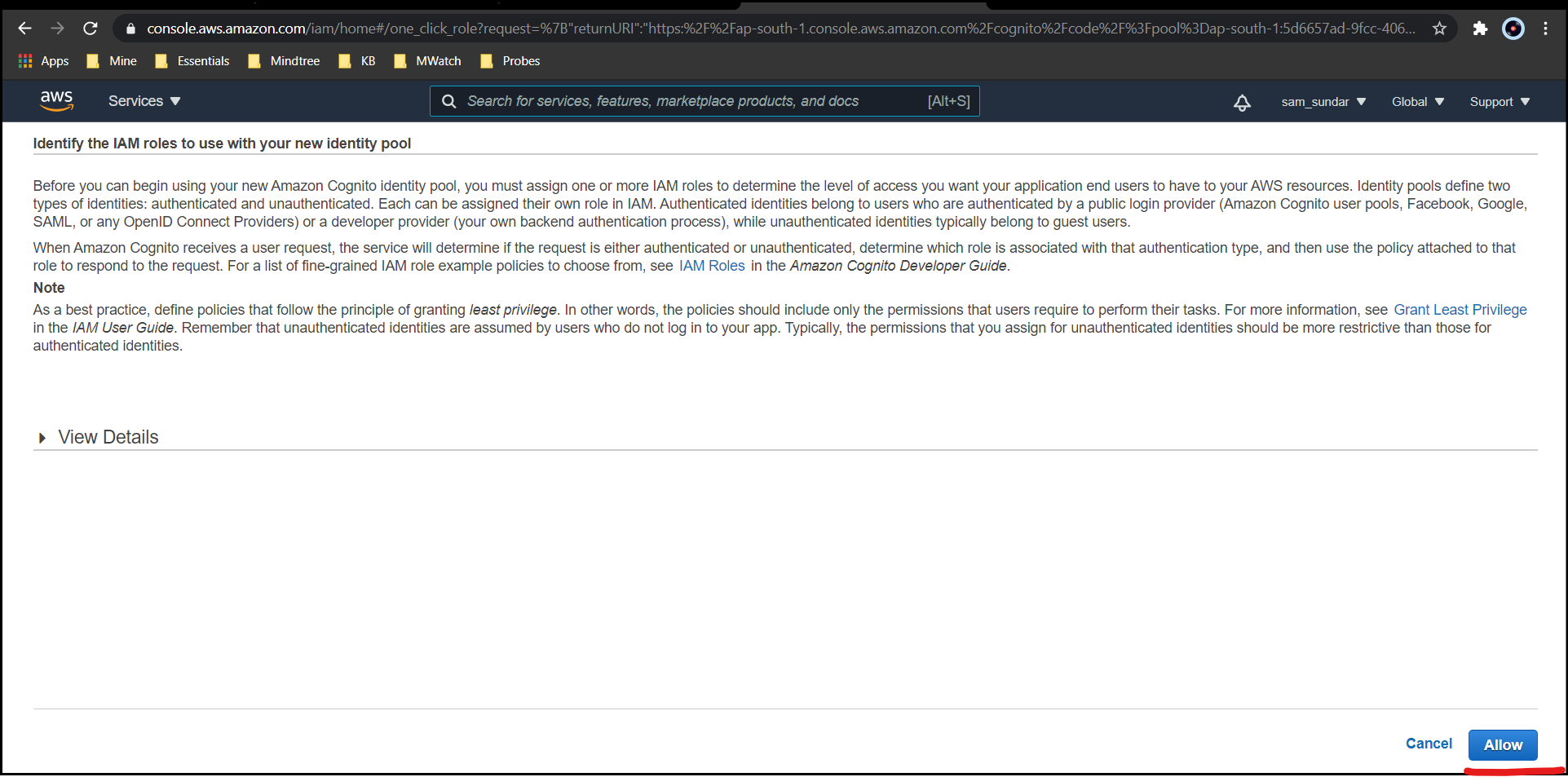


1. Now in below list of Auth providers, choose Cognito and paste the Userpool's User Pool ID and APP Client ID (Check in User Pool).



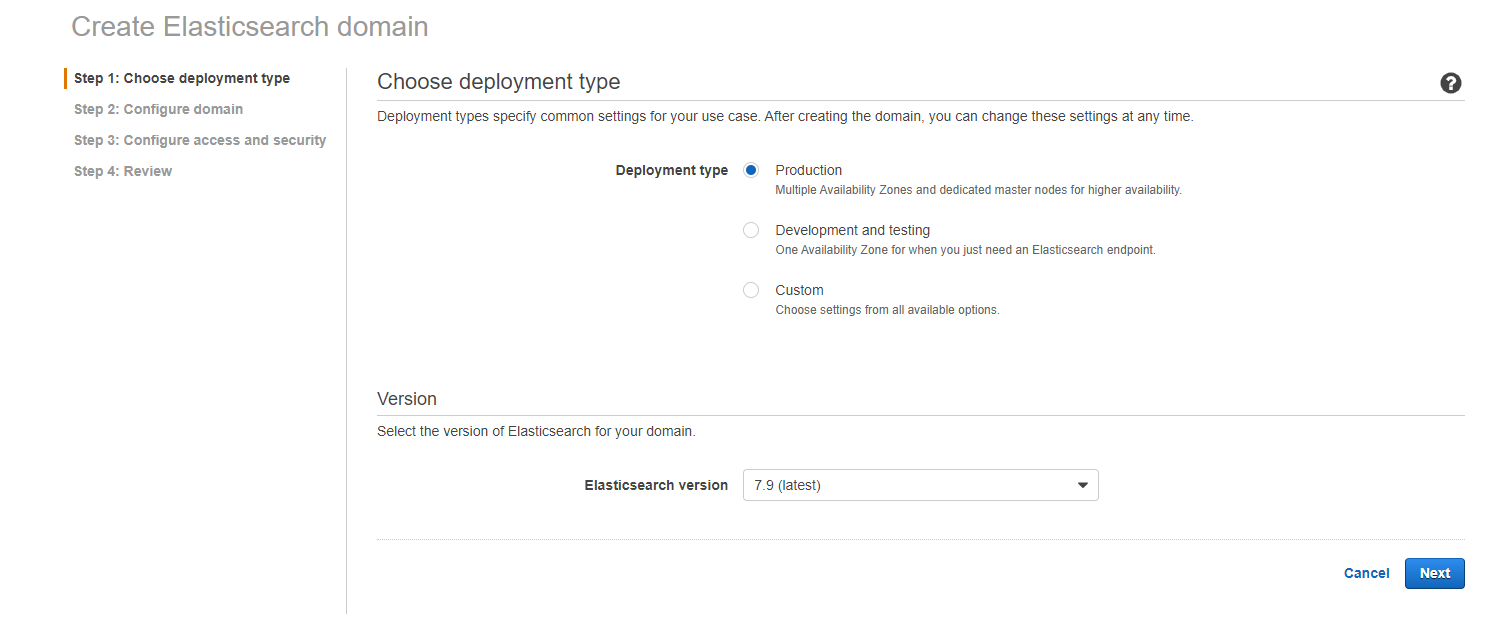


1. Post creating you will be redirected to IAM for creating a role. Just click OK at IAM page since all necessary roles are auto filled.

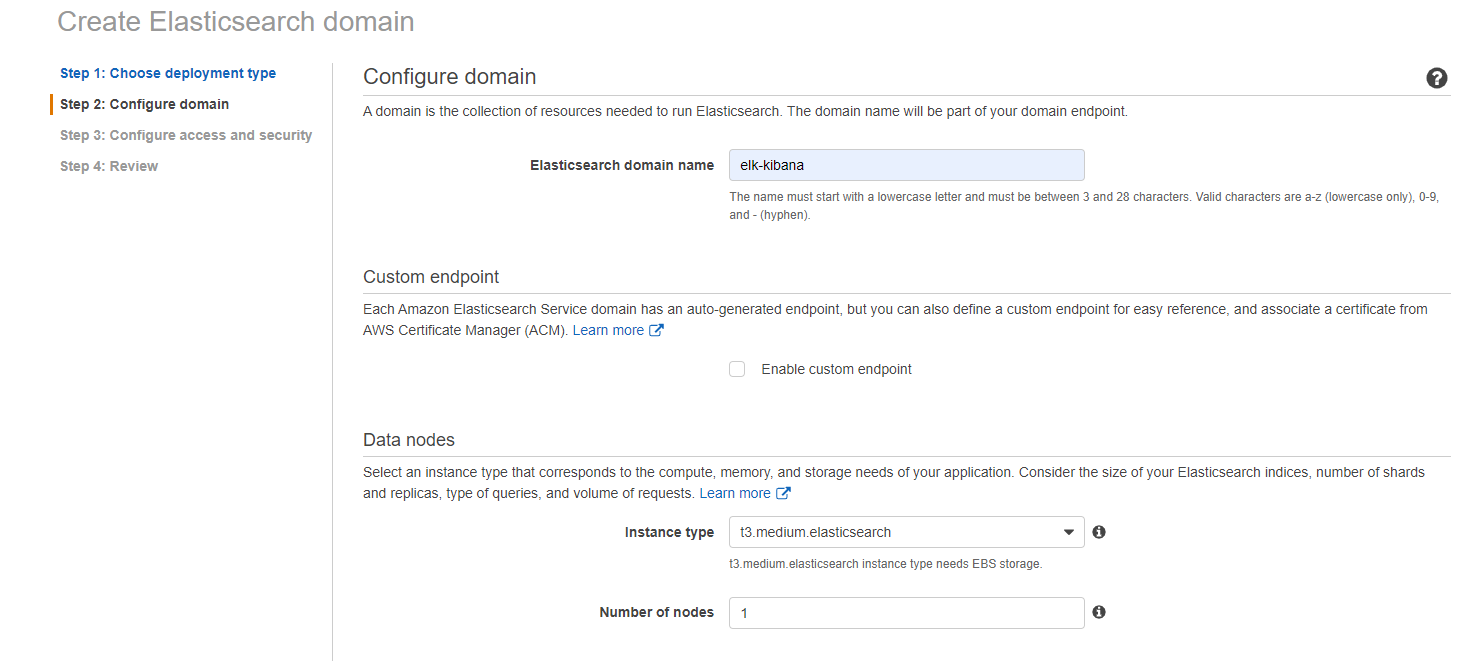


--------Setting up Elastic and Kibana-------

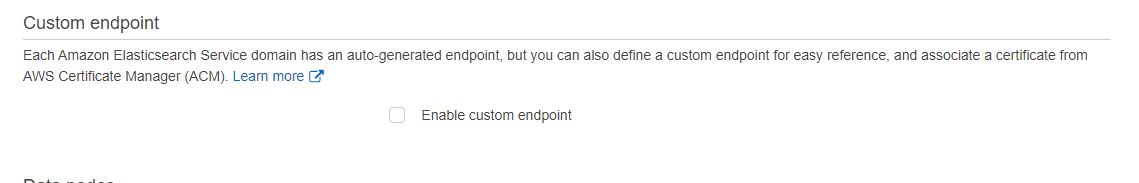
1. Open EES and select “Create a domain”, select type of deployment



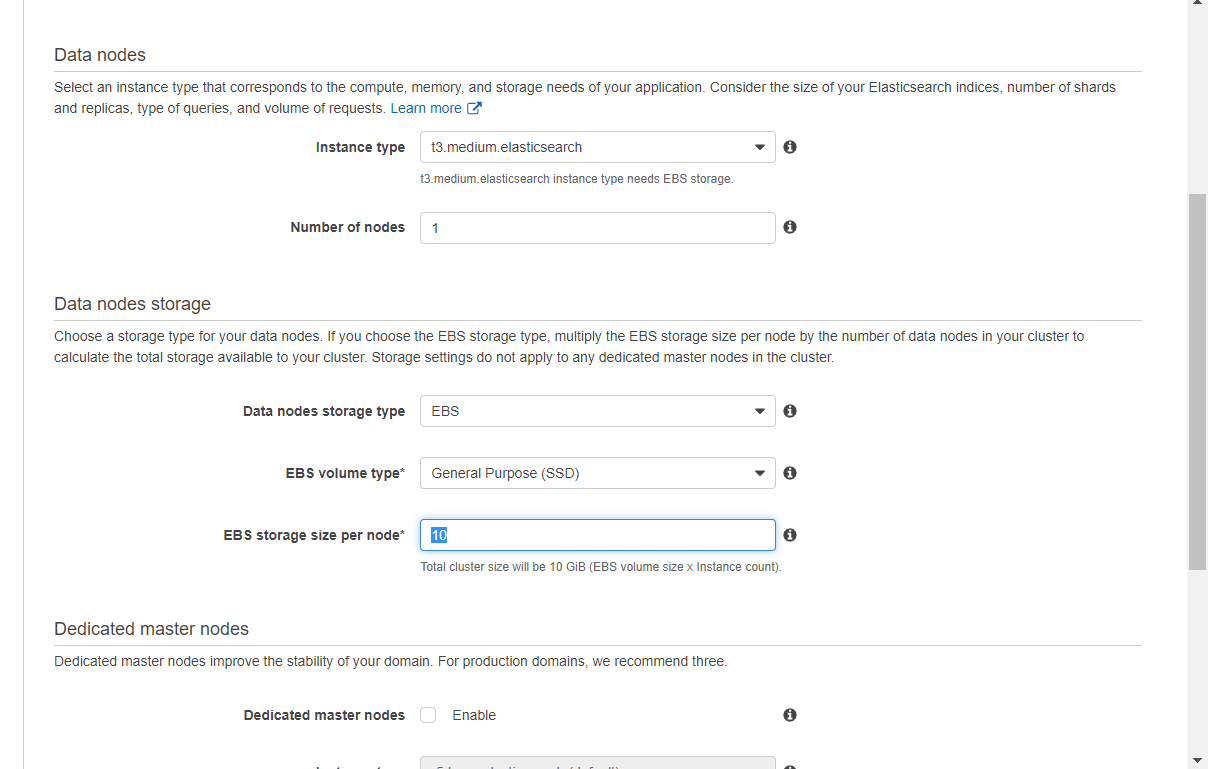
2. Enter ElasticSearch Domain Name

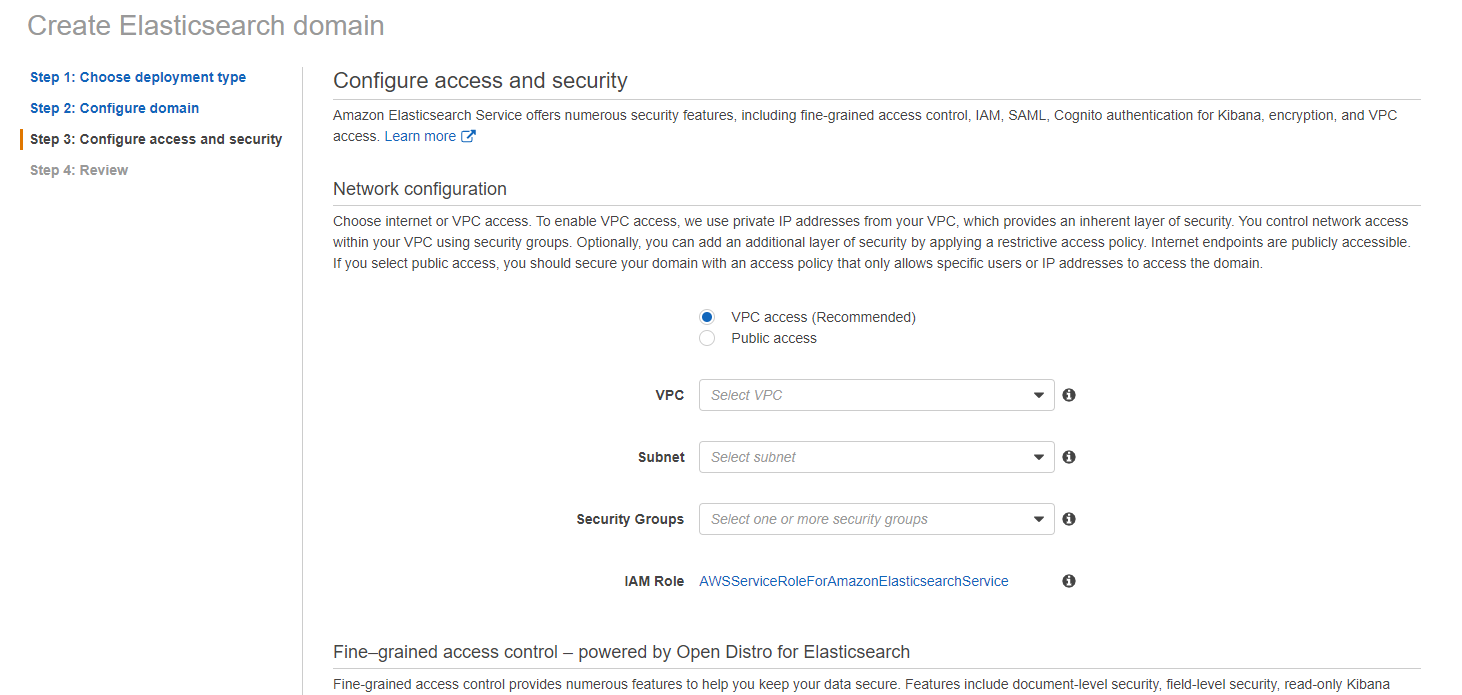


3. Select "Custom endpoint" if you want a custom URL endpoint with SSL Cert.

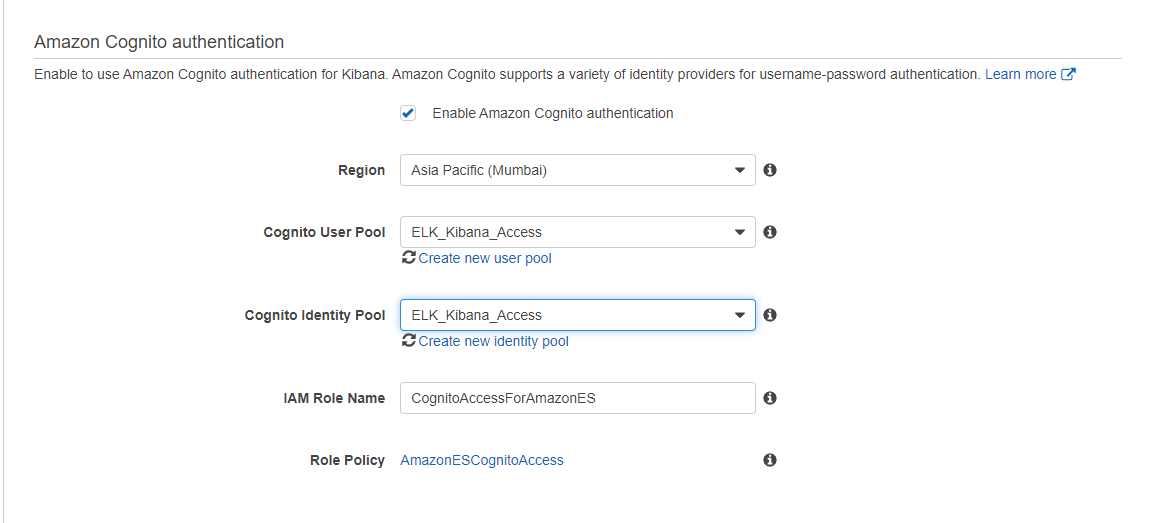


4. Select instance types and other common config. such as instance types, storage, Master Node, VPC



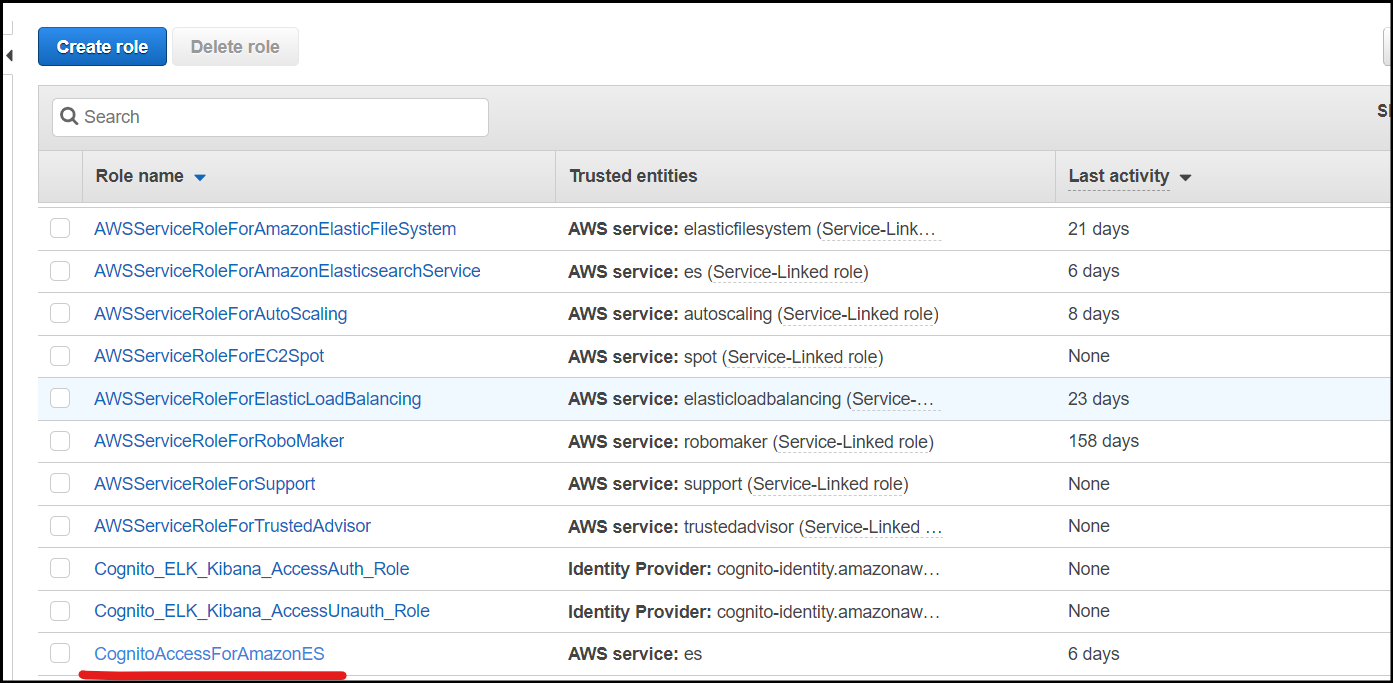


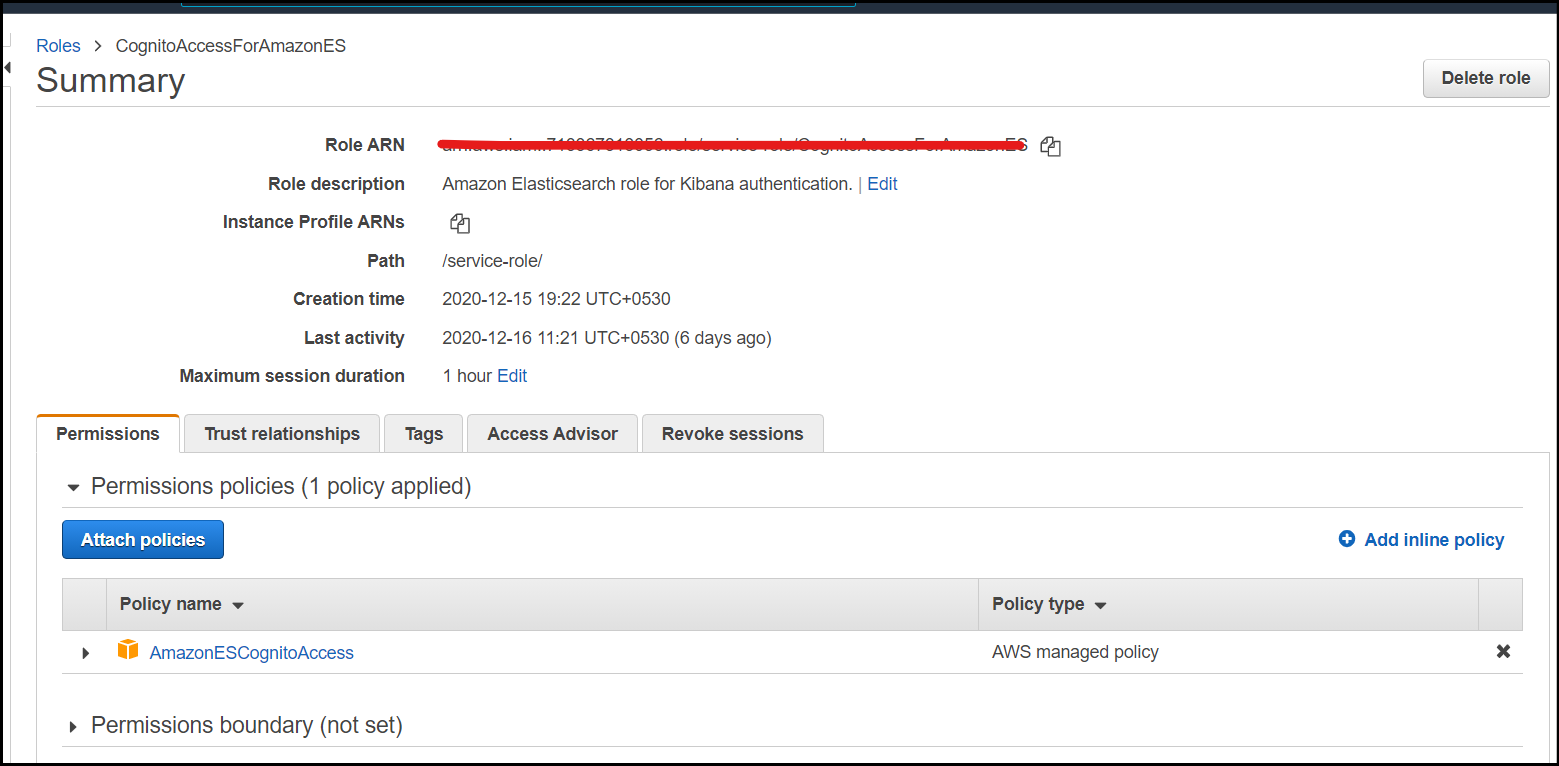
5. Select "Amazon Cognito authentication" and select the Cognito Userpool and Identity Pool.



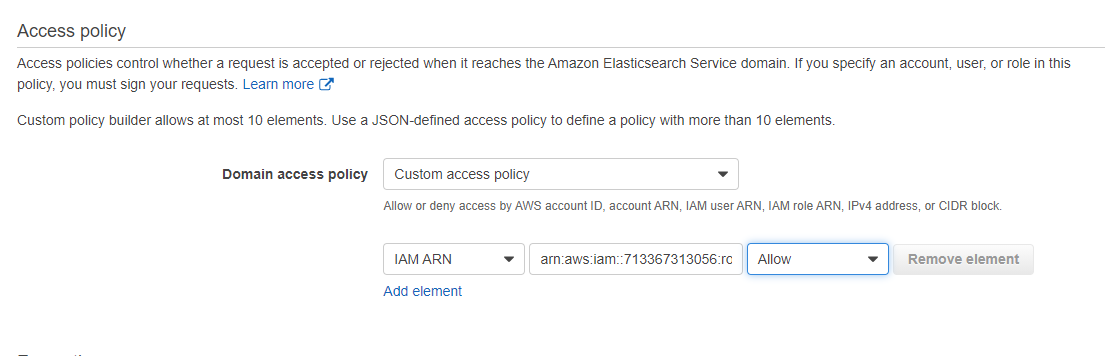
6. Under Access Policy select "Custom Access Policy" and choose IAM as element with IAM Role created for Cognito's arn being entered at Principal. (Open IAM and search for “[CognitoAccessForAmazonES](https://console.aws.amazon.com/iam/home?region=ap-south-1#/roles/CognitoAccessForAmazonES)” Role and copy it’s ARN and enter in principal section of custom access)

*IAM*

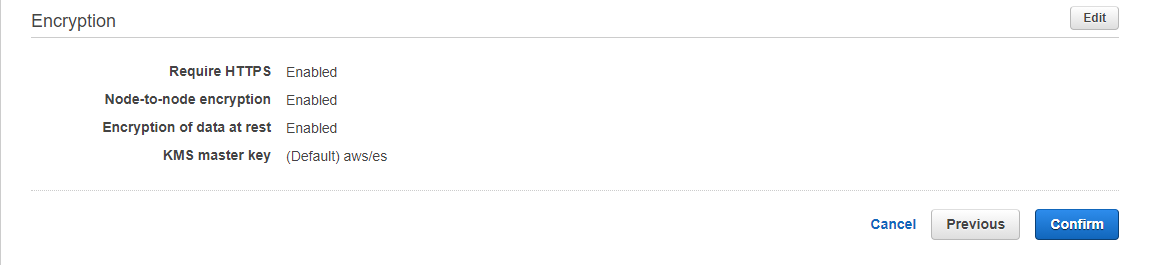




*AWS Elastic Search Service*



7. Once auth is chosen as Cognito and other data have been given click confirm to deploy the Elastic Search cluster on AWS.



8. Once the Elastic Search is ready, we will not be able to access it outside our VPC, hence access the Kibana endpoint "https://vpc-elk-kibana-afzwwcw5fnidvncijnelitzbzu.ap-south-1.es.amazonaws.com/\_plugin/kibana/" from an instance which is present in your same VPC.

9. At first login, password change will be asked post which we will be able to login into Kibana with Cognito Userpool