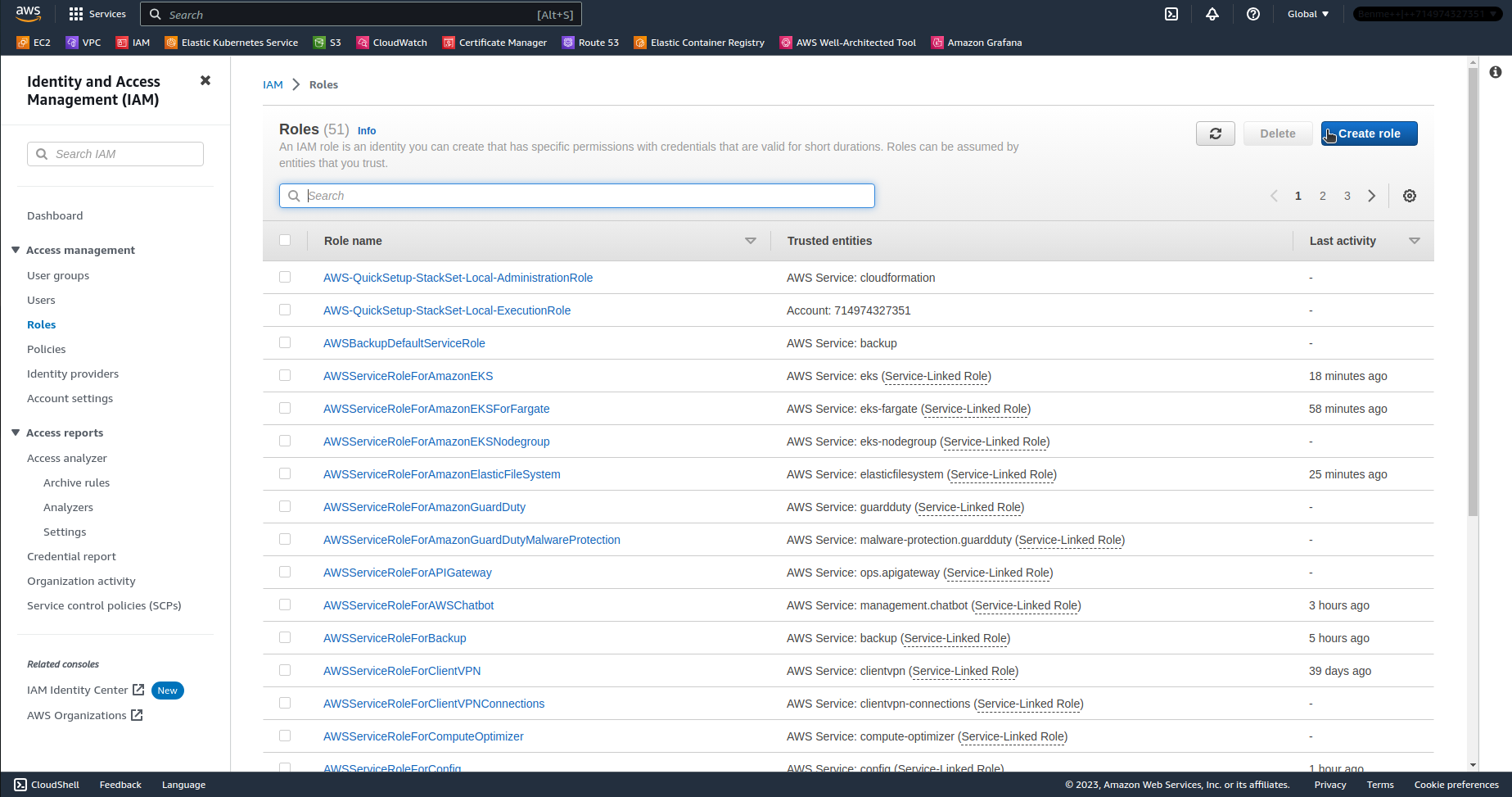
**How to create IAM role for EKS service account**

1. Open AWS Console and navigate to IAM service and head to “[Roles](https://us-east-1.console.aws.amazon.com/iamv2/home?region=eu-central-1" \l "/roles)”.

2. Next Click on “Create role” button in upper right.



3. Select “Custom trust policy” and use policy as follows:

{

"Version": "2012-10-17",

"Statement": [

{

"Effect": "Allow",

"Principal": {

"Federated": "*arn:aws:iam::111122223333:oidc-provider/oidc.eks.region-code.amazonaws.com/id/EXAMPLED539D4633E53DE1B71EXAMPLE*"

},

"Action": "sts:AssumeRoleWithWebIdentity",

"Condition": {

"StringLike": {

"oidc.eks.*region-code*.amazonaws.com/id/*EXAMPLED539D4633E53DE1B71EXAMPLE*:sub": "system:serviceaccount:\*",

"oidc.eks.*region-code*.amazonaws.com/id/*EXAMPLED539D4633E53DE1B71EXAMPLE*:aud": "sts.amazonaws.com"

}

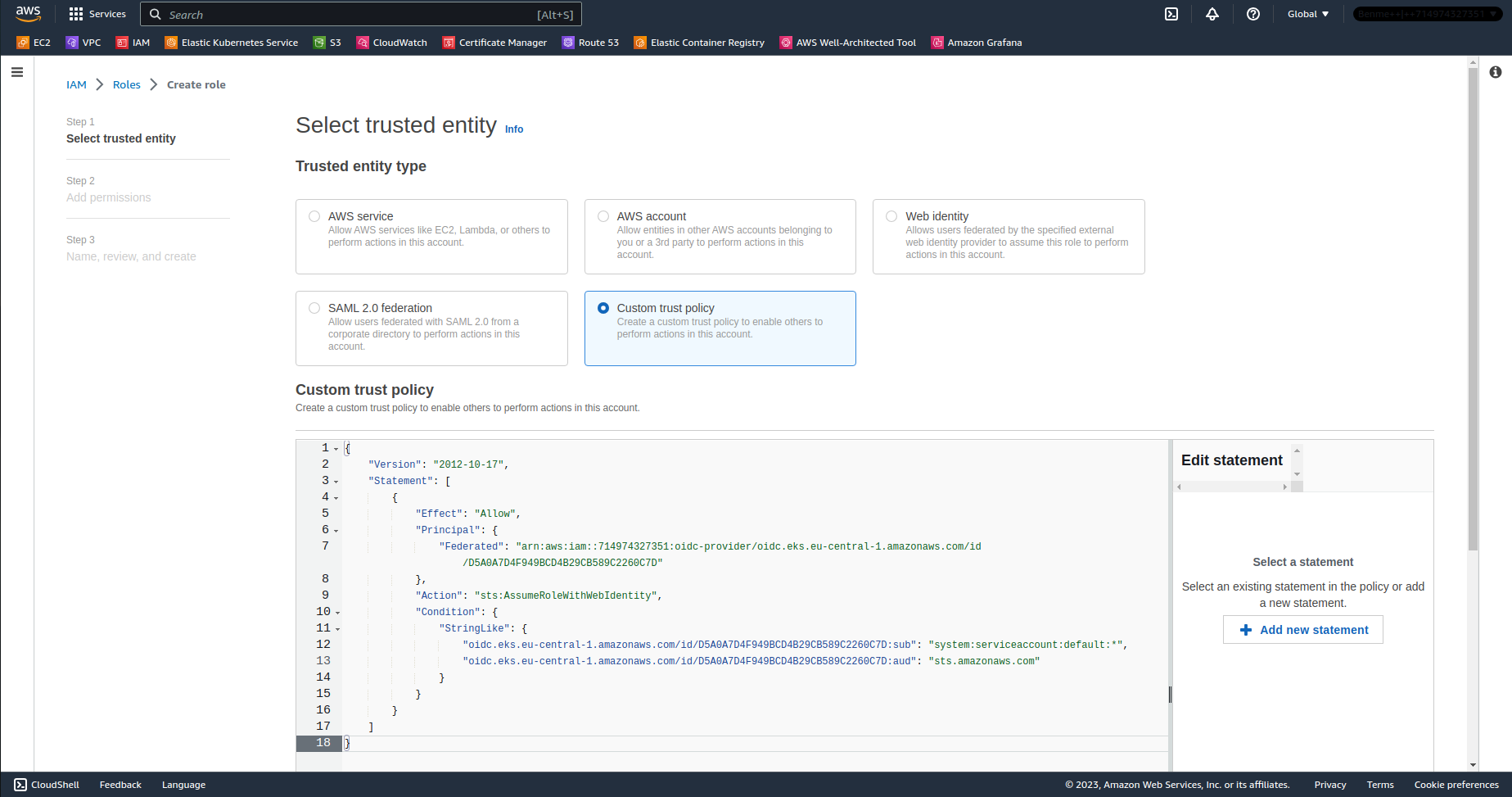
}

}

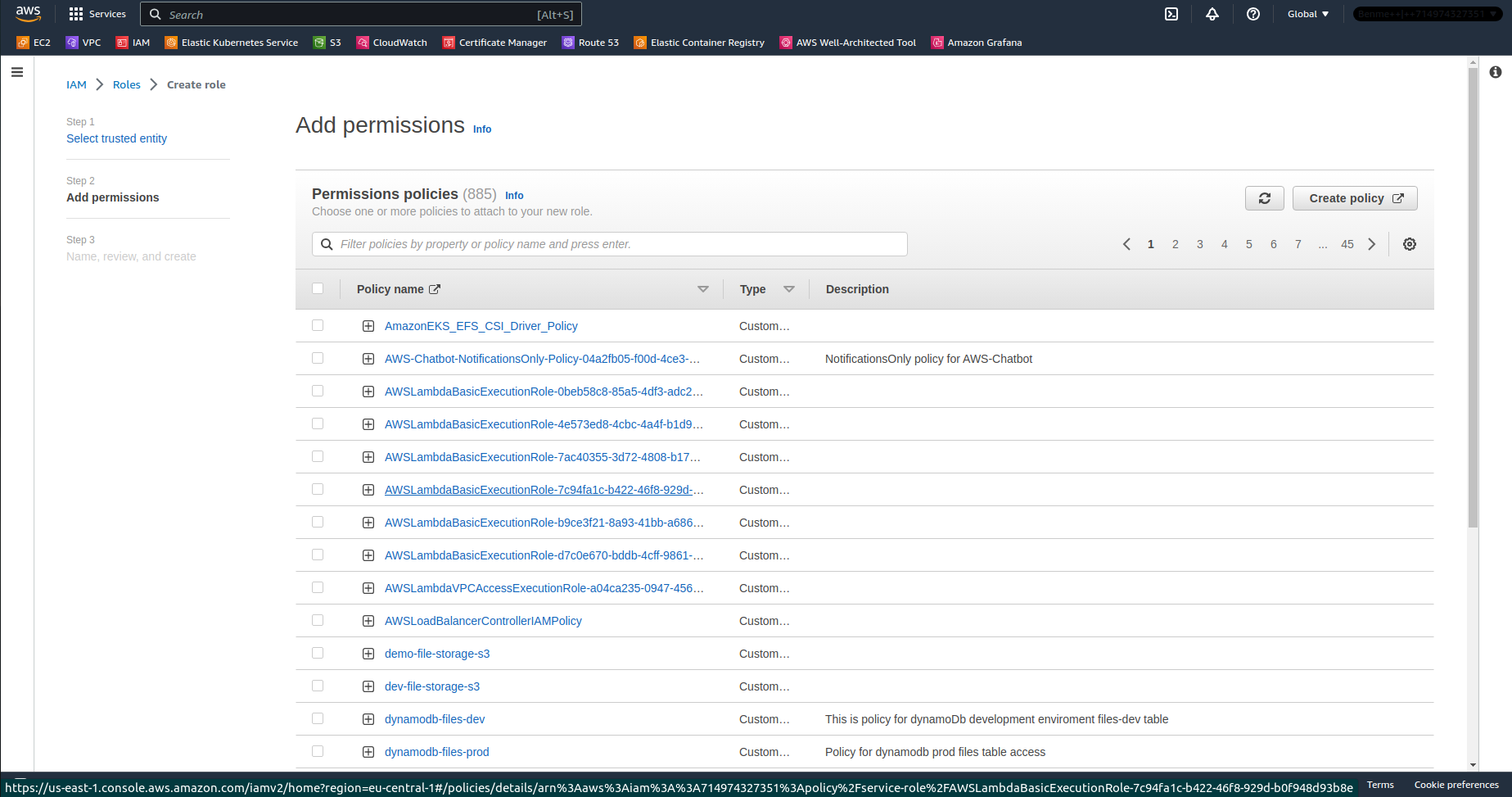
]

}

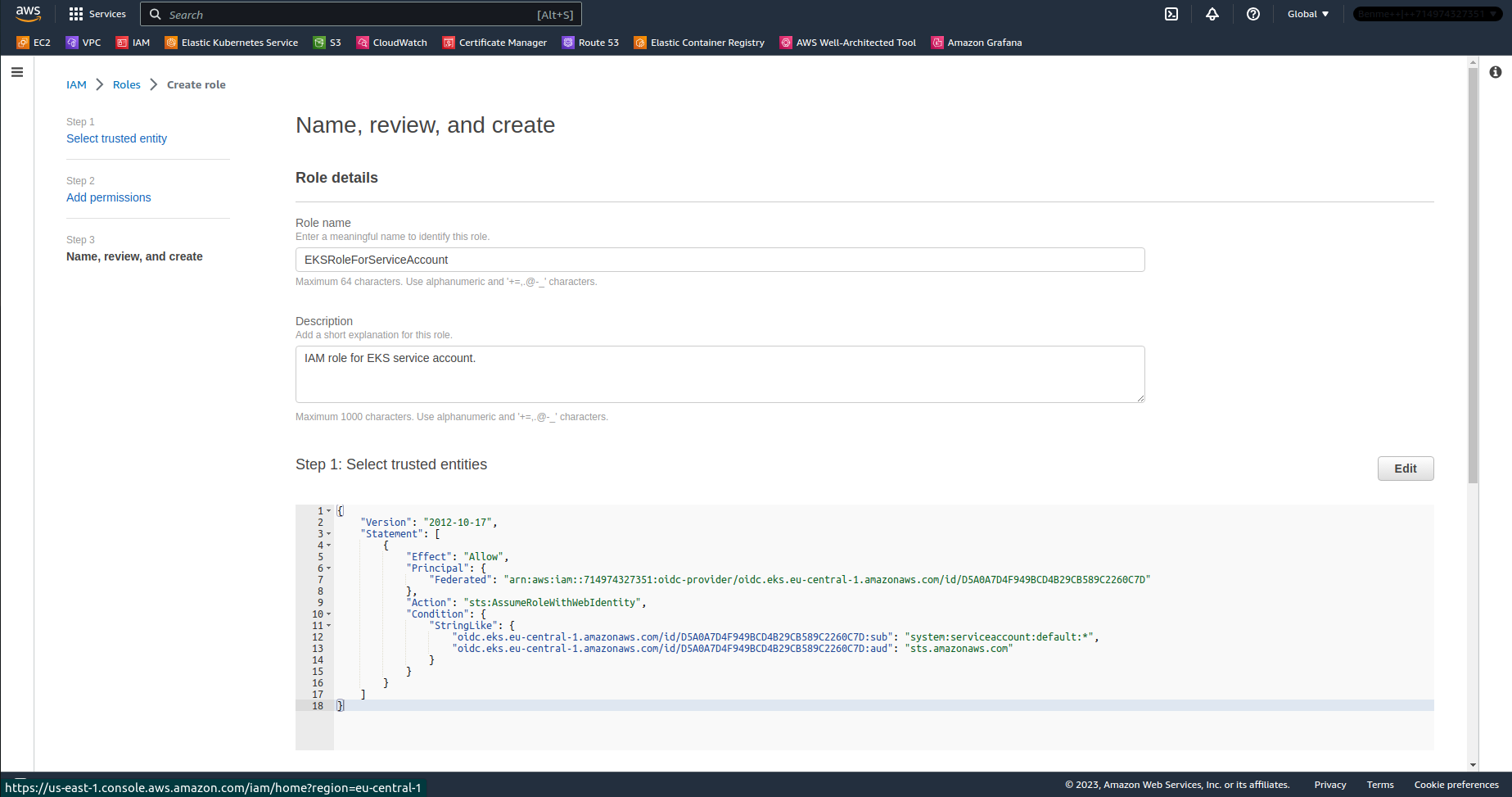
You can get OIDC provider arn and name from IAM Service > [Identity providers](https://us-east-1.console.aws.amazon.com/iamv2/home?region=eu-central-1" \l "/identity_providers). Remember to change region-code. Values to change are marked blue.



4. Click on “Next” in the right bottom and add permissions to the IAM Role.



5. Give the Role a name, optionally description and click on “Create role” in the bottom right.



6. Now create Service Account in Kubernetes which will assume the role. Here’s the example manifest:

apiVersion: v1

kind: ServiceAccount

metadata:

name: example-service-account

namespace: default

annotations:

eks.amazonaws.com/role-arn: arn:aws:iam::714974327351:role/EKSRoleForServiceAccount