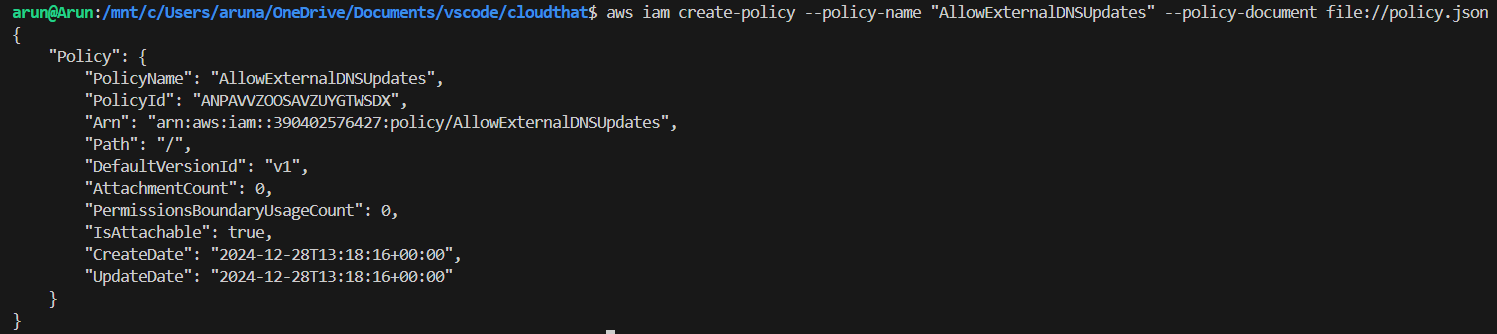
**External-DNS**

**Step 1:** create oidc connect

**Step 2:** aws iam create-policy --policy-name "AllowExternalDNSUpdates" --policy-document <file://policy.json>



**Step 3:**

export cluster\_name=my-cluster

export role\_name=AmazonExternal\_DNS\_Role

**# Create the IAM service account**

eksctl create iamserviceaccount \

--name external-dns-sa \

--namespace kube-system \

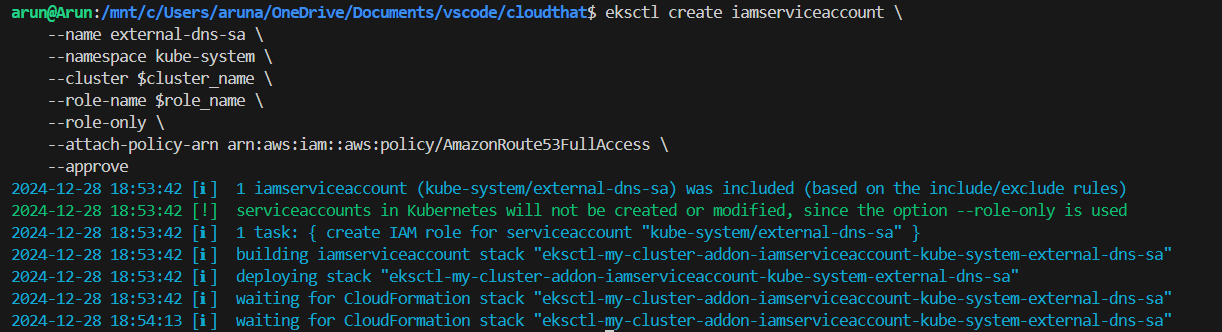
--cluster $cluster\_name \

--role-name $role\_name \

--role-only \

--attach-policy-arn arn:aws:iam::aws:policy/AmazonRoute53FullAccess \

--approve



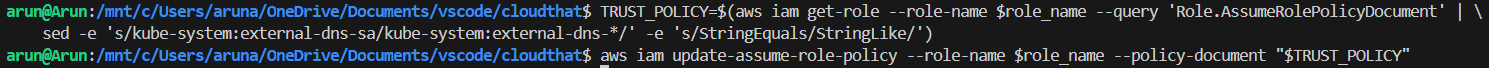
# Fetch and modify the trust policy

TRUST\_POLICY=$(aws iam get-role --role-name $role\_name --query 'Role.AssumeRolePolicyDocument' | \

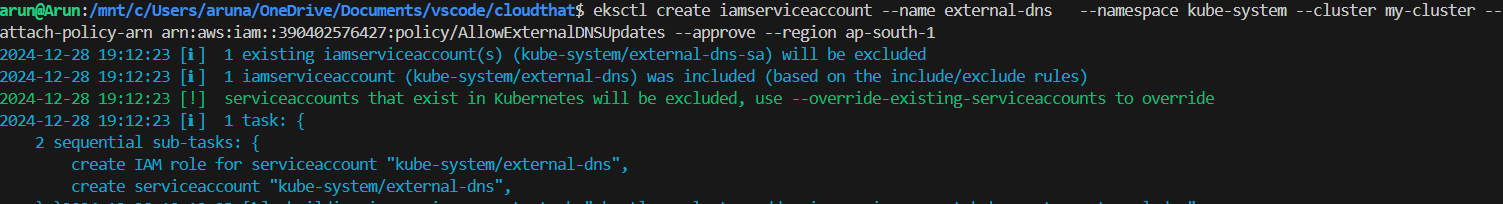
sed -e 's/kube-system:external-dns-sa/kube-system:external-dns-\*/' -e 's/StringEquals/StringLike/')

# Update the role with the modified trust policy

aws iam update-assume-role-policy --role-name $role\_name --policy-document "$TRUST\_POLICY"



**Step 4:**



#eksctl create iamserviceaccount --name <SERVICE\_ACCOUNT\_NAME> --namespace kube-system --cluster CLUSTER\_NAME --attach-policy-arn <IAM\_POLICY\_ARN> --approve --region < >

# kubectl api-versions | grep rbac.authorization.k8s.io

**Step 5:**

# kubectl create -f clusterrole.yaml

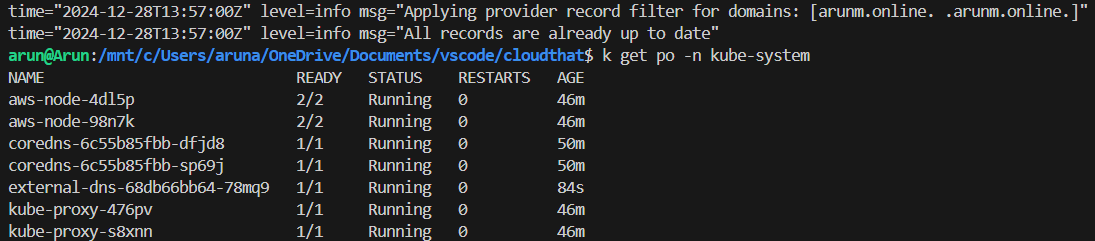


#kubectl create -f clusterrolebinding.yaml



# kubectl create -f external-dns.yaml (change txt-owner-id as zone id, domain-filter as domain and aws-zone-type as public

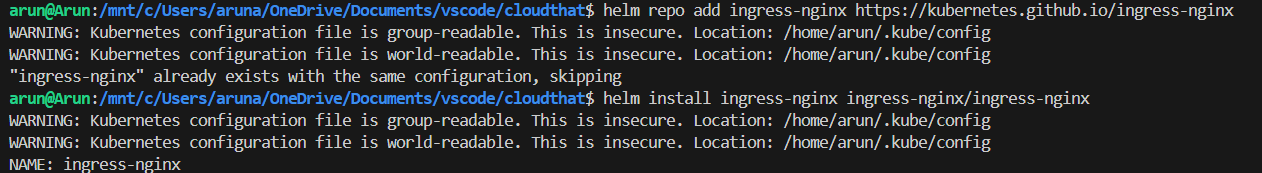
# kubectl logs -l app.kubernetes.io/name=external-dns -n kube-system



Kubectl apply -f deploy.yaml

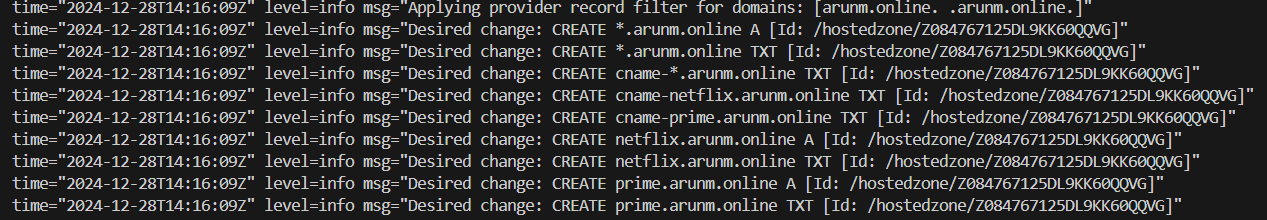
Kubectl apply -f deploy2.yaml

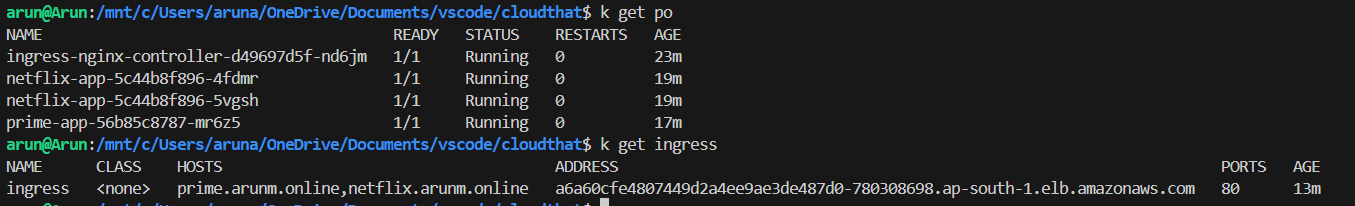
# Install ingress using helm

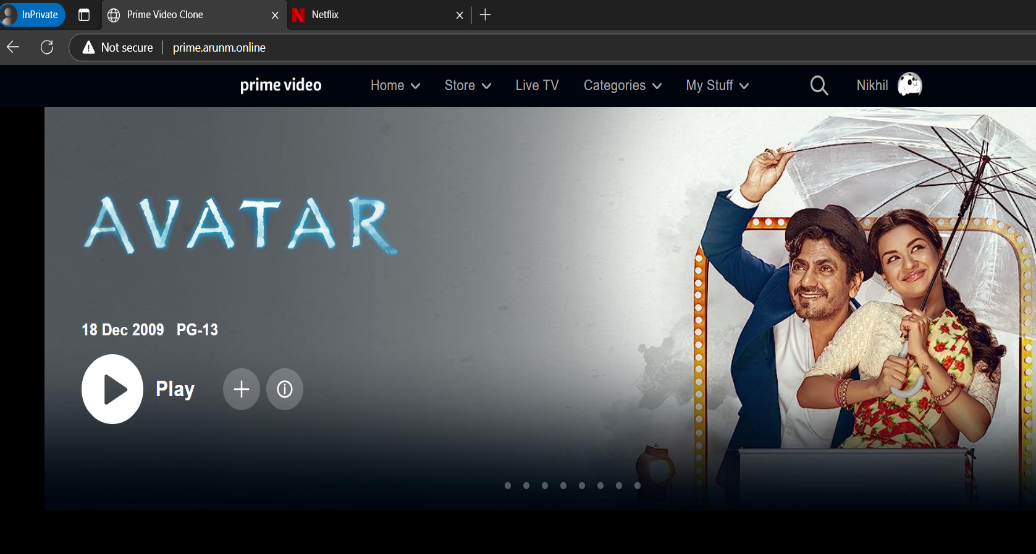


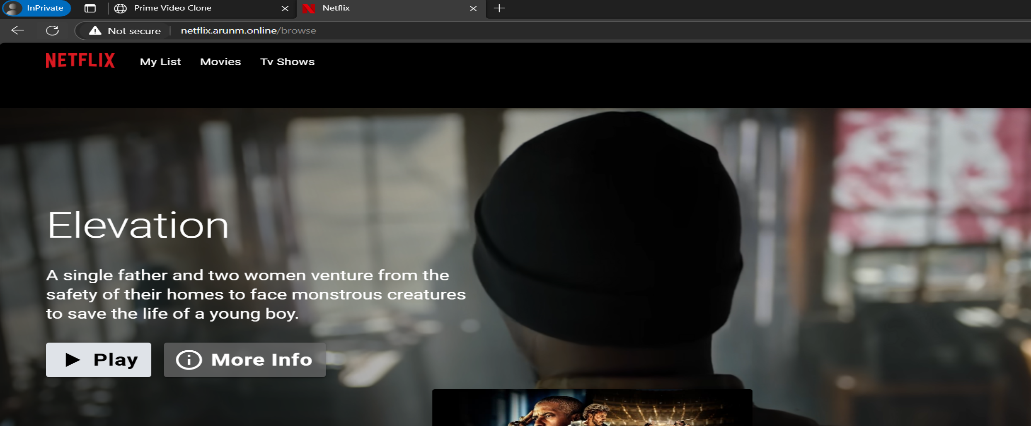
# Kubectl apply -f ingress.yaml

# kubectl logs external-dns-9f85d8d5b-sx5fg









CERT-MANAGER

Step 1: kubectl apply -f <https://github.com/cert-manager/cert-manager/releases/download/v1.15.3/cert-manager.yaml>

Step2: kubectl apply -f clusterissuer.yaml

Step 3: kubectl apply -f ingress.yaml