**3. Review and Update External DNS k8s manifest**

--- **Reference** - <https://github.com/stacksimplify/aws-eks-kubernetes-masterclass/tree/master/08-NEW-ELB-Application-LoadBalancers/08-06-Deploy-ExternalDNS-on-EKS>

**Update External DNS Kubernetes manifest**

--- Original Template you can find in <https://github.com/kubernetes-sigs/external-dns/blob/master/docs/tutorials/aws.md>

--- File Location: kube-manifests/01-Deploy-ExternalDNS.yml

apiVersion: v1

kind: ServiceAccount

metadata:

  name: external-dns

  # If you're using Amazon EKS with IAM Roles for Service Accounts, specify the following annotation.

  # Otherwise, you may safely omit it.

  annotations:

    # Substitute your account ID and IAM service role name below. #Change-1: Replace with your IAM ARN Role for extern-dns

    eks.amazonaws.com/role-arn: arn:aws:iam::180789647333:role/eksctl-eksdemo1-addon-iamserviceaccount-defa-Role1-1KZREOLB5TGO5

---

apiVersion: rbac.authorization.k8s.io/v1

kind: ClusterRole

metadata:

  name: external-dns

rules:

- apiGroups: [""]

  resources: ["services","endpoints","pods"]

  verbs: ["get","watch","list"]

- apiGroups: ["extensions","networking.k8s.io"]

  resources: ["ingresses"]

  verbs: ["get","watch","list"]

- apiGroups: [""]

  resources: ["nodes"]

  verbs: ["list","watch"]

---

apiVersion: rbac.authorization.k8s.io/v1

kind: ClusterRoleBinding

metadata:

  name: external-dns-viewer

roleRef:

  apiGroup: rbac.authorization.k8s.io

  kind: ClusterRole

  name: external-dns

subjects:

- kind: ServiceAccount

  name: external-dns

  namespace: default

---

apiVersion: apps/v1

kind: Deployment

metadata:

  name: external-dns

spec:

  strategy:

    type: Recreate

  selector:

    matchLabels:

      app: external-dns

  template:

    metadata:

      labels:

        app: external-dns

      # If you're using kiam or kube2iam, specify the following annotation.

      # Otherwise, you may safely omit it.  #Change-2: Commented line 55 and 56

      #annotations:

        #iam.amazonaws.com/role: arn:aws:iam::ACCOUNT-ID:role/IAM-SERVICE-ROLE-NAME

    spec:

      serviceAccountName: external-dns

      containers:

      - name: external-dns

        image: k8s.gcr.io/external-dns/external-dns:v0.10.2 # the latest pod version is taking here. In future the pod version may changes.

        args:

        - --source=service

        - --source=ingress

        # Change-3: Commented line 65 and 67 - --domain-filter=external-dns-test.my-org.com # will make ExternalDNS see only the hosted zones matching provided domain, omit to process all available hosted zones

        - --provider=aws

       # Change-3: Commented line 65 and 67  - --policy=upsert-only # would prevent ExternalDNS from deleting any records, omit to enable full synchronization

        - --aws-zone-type=public # only look at public hosted zones (valid values are public, private or no value for both)

        - --registry=txt

        - --txt-owner-id=my-hostedzone-identifier

      securityContext:

        fsGroup: 65534 # For ExternalDNS to be able to read Kubernetes and AWS token files

**Change-1: Line number 9: IAM Role update**

Copy the role-arn you have made a note at the end of step-03 and replace at line no 9.

    eks.amazonaws.com/role-arn: arn:aws:iam::180789647333:role/eksctl-eksdemo1-addon-iamserviceaccount-defa-Role1-JTO29BVZMA2N

**Change-2: Line 55, 56: Commented them**

We used eksctl to create IAM role and attached the AllowExternalDNSUpdates policy

We didnt use KIAM or Kube2IAM so we don't need these two lines, so commented

      #annotations:

        #iam.amazonaws.com/role: arn:aws:iam::ACCOUNT-ID:role/IAM-SERVICE-ROLE-NAME

**Change-3: Line 65, 67: Commented them**

        # - --domain-filter=external-dns-test.my-org.com # will make ExternalDNS see only the hosted zones matching provided domain, omit to process all available hosted zones

       # - --policy=upsert-only # would prevent ExternalDNS from deleting any records, omit to enable full synchronization # you want ingress service to create external DNS and you don’t want ingress to delete the external DNS then uncomment this parameter.

--- **note** - if you have multiple domains then this line should be commented out because if not then it will applicable to all domains. If you have multiple domains and if did not mentioned your domain specifically then it will update and delete create…etc inside of all hosted zones.

**Change-4: Line 61: Get latest Docker Image name**

--- Get latest external dns image name - https://github.com/kubernetes-sigs/external-dns/releases/tag/v0.10.2

    spec:

      serviceAccountName: external-dns

      containers:

      - name: external-dns

        image: k8s.gcr.io/external-dns/external-dns:v0.10.2