**5. NLB TLS Demo Deploy, Verify and Clean-Up**

--- Reference - <https://github.com/stacksimplify/aws-eks-kubernetes-masterclass/tree/master/19-ELB-Network-LoadBalancers-with-LBC/19-02-LBC-NLB-TLS>

**Introduction**

--- Understand about the 4 TLS Annotations for Network Load Balancers

--- aws-load-balancer-ssl-cert

--- aws-load-balancer-ssl-ports

--- aws-load-balancer-ssl-negotiation-policy

--- aws-load-balancer-ssl-negotiation-policy

**Review TLS Annotations**

--- **File Name: kube-manifests\02-LBC-NLB-LoadBalancer-Service.yml**

--- Security Policies: <https://docs.aws.amazon.com/elasticloadbalancing/latest/network/create-tls-listener.html#describe-ssl-policies>

apiVersion: v1

kind: Service

metadata:

  name: tls-lbc-network-lb

  annotations:

    # Traffic Routing

    service.beta.kubernetes.io/aws-load-balancer-name: tls-lbc-network-lb

    service.beta.kubernetes.io/aws-load-balancer-type: external

    service.beta.kubernetes.io/aws-load-balancer-nlb-target-type: instance

    #service.beta.kubernetes.io/aws-load-balancer-subnets: subnet-xxxx, mySubnet ## Subnets are auto-discovered if this annotation is not specified, see Subnet Discovery for further details.

    # Health Check Settings

    service.beta.kubernetes.io/aws-load-balancer-healthcheck-protocol: http

    service.beta.kubernetes.io/aws-load-balancer-healthcheck-port: traffic-port

    service.beta.kubernetes.io/aws-load-balancer-healthcheck-path: /index.html

    service.beta.kubernetes.io/aws-load-balancer-healthcheck-healthy-threshold: "3"

    service.beta.kubernetes.io/aws-load-balancer-healthcheck-unhealthy-threshold: "3"

    service.beta.kubernetes.io/aws-load-balancer-healthcheck-interval: "10" # The controller currently ignores the timeout configuration due to the limitations on the AWS NLB. The default timeout for TCP is 10s and HTTP is 6s.

    # Access Control

    service.beta.kubernetes.io/load-balancer-source-ranges: 0.0.0.0/0

    service.beta.kubernetes.io/aws-load-balancer-scheme: "internet-facing"

    # AWS Resource Tags

    service.beta.kubernetes.io/aws-load-balancer-additional-resource-tags: Environment=dev,Team=test

    # TLS

    service.beta.kubernetes.io/aws-load-balancer-ssl-cert: arn:aws:acm:us-east-1:180789647333:certificate/d86de939-8ffd-410f-adce-0ce1f5be6e0d # specifies the ARN of one or more certificates managed by the AWS Certificate Manager.

    service.beta.kubernetes.io/aws-load-balancer-ssl-ports: 443, # Specify this annotation if you need both TLS and non-TLS listeners on the same load balancer

    service.beta.kubernetes.io/aws-load-balancer-ssl-negotiation-policy: ELBSecurityPolicy-TLS13-1-2-2021-06 # specifies the Security Policy for NLB frontend connections, allowing you to control the protocol and ciphers.

    service.beta.kubernetes.io/aws-load-balancer-backend-protocol: tcp # specifies whether to use TLS or TCP for the backend traffic between the load balancer and the kubernetes pods.

spec:

  type: LoadBalancer

  selector:

    app: app3-nginx

  ports:

    - name: http

      port: 80        # Creates NLB Port 80 Listener

      targetPort: 80  # Creates NLB Port 80 Target Group-1

    - name: https

      port: 443       # Creates NLB Port 443 Listener

      targetPort: 80  # Creates NLB Port 80 Target Group-2

    - name: http81

      port: 81        # Creates NLB Port 81 Listener

      targetPort: 80  # Creates NLB Port 80 Target Group-3

    - name: http82

      port: 82        # Creates NLB Port 82 Listener

      targetPort: 80  # Creates NLB Port 80 Target Group-4

# Note-1: Listener to Target Group is a one to one Mapping

# Note-2: Every listener will have its own new Target Group created with that port mentioned in targetPort field

# Note-3: This might not be a effective way but unfortunately when you create via kubernetes service, thats the behavior

--- **01-Nginx-App3-Deployment.yml**

apiVersion: apps/v1

kind: Deployment

metadata:

  name: app3-nginx-deployment

  labels:

    app: app3-nginx

spec:

  replicas: 1

  selector:

    matchLabels:

      app: app3-nginx

  template:

    metadata:

      labels:

        app: app3-nginx

    spec:

      containers:

        - name: app2-nginx

          image: stacksimplify/kubenginx:1.0.0

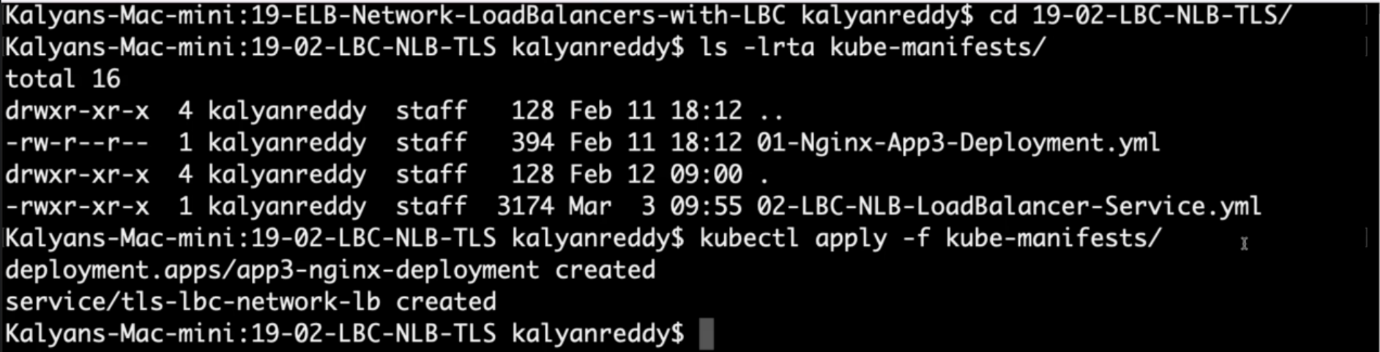
          ports:

            - containerPort: 80

**Deploy all kube-manifests**

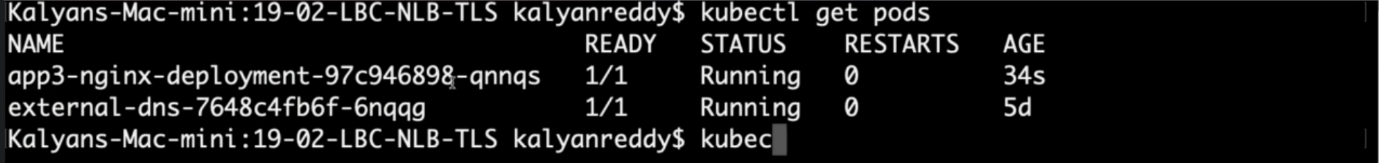
**# Deploy kube-manifests**

--- **kubectl apply -f kube-manifests/**



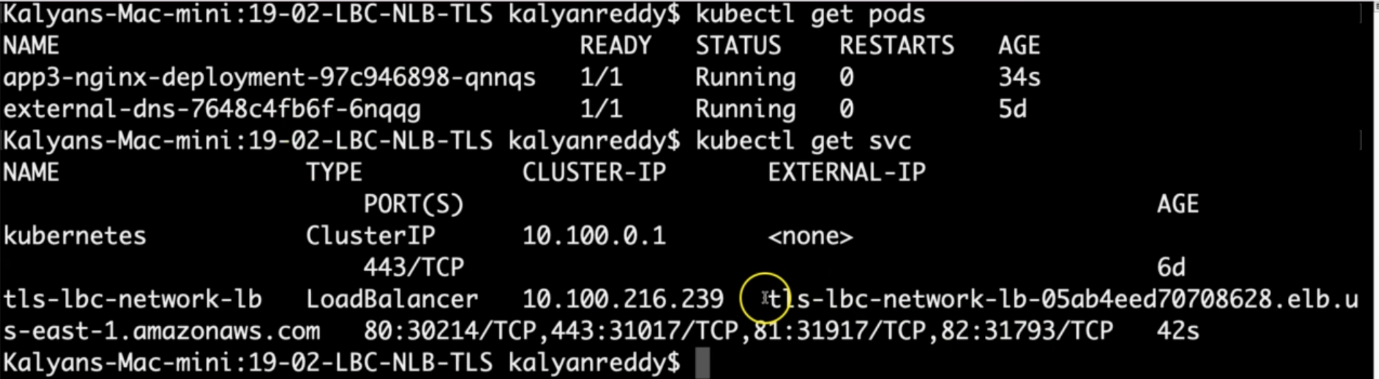
**# Verify Pods**

--- **kubectl get pods**



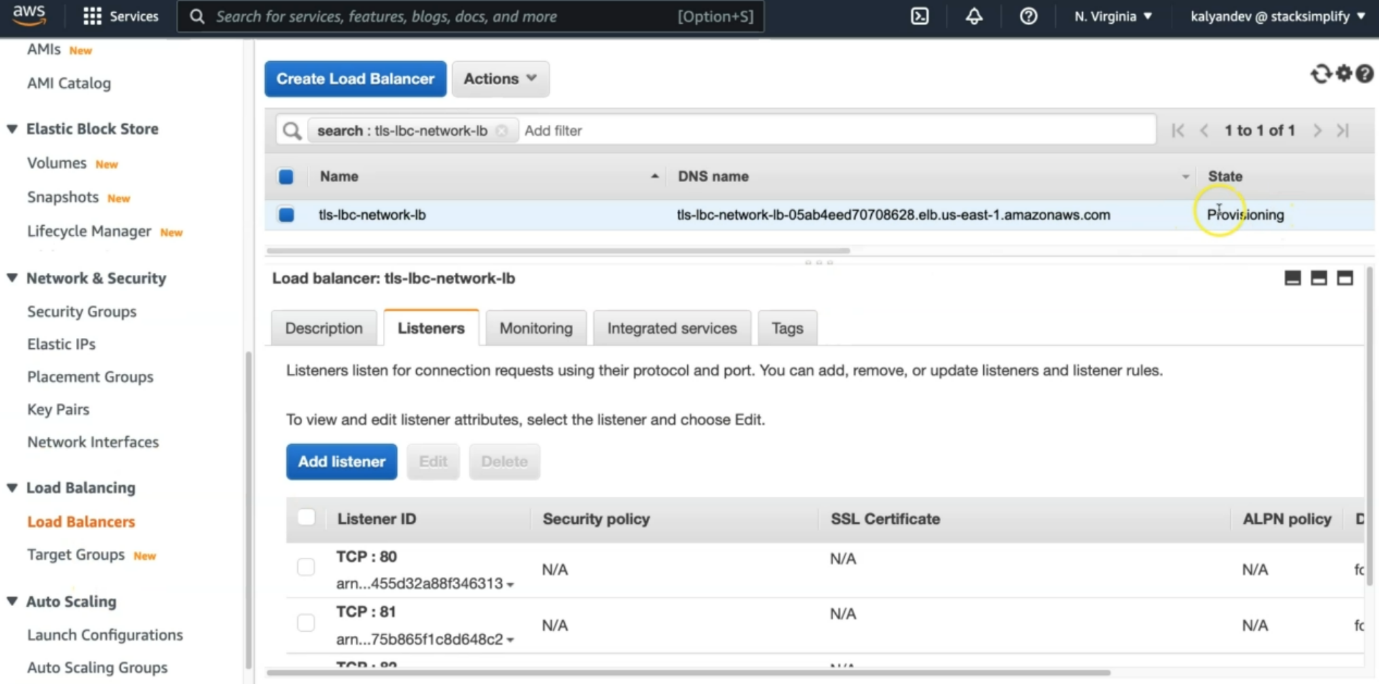
**# Verify Services**

--- **kubectl get svc**



Observation:

1. Verify the network lb DNS name



--- the name are matched.

**# Verify AWS Load Balancer Controller pod logs**

--- **kubectl -n kube-system get pods**

--- **kubectl -n kube-system logs -f <aws-load-balancer-controller-POD-NAME>**

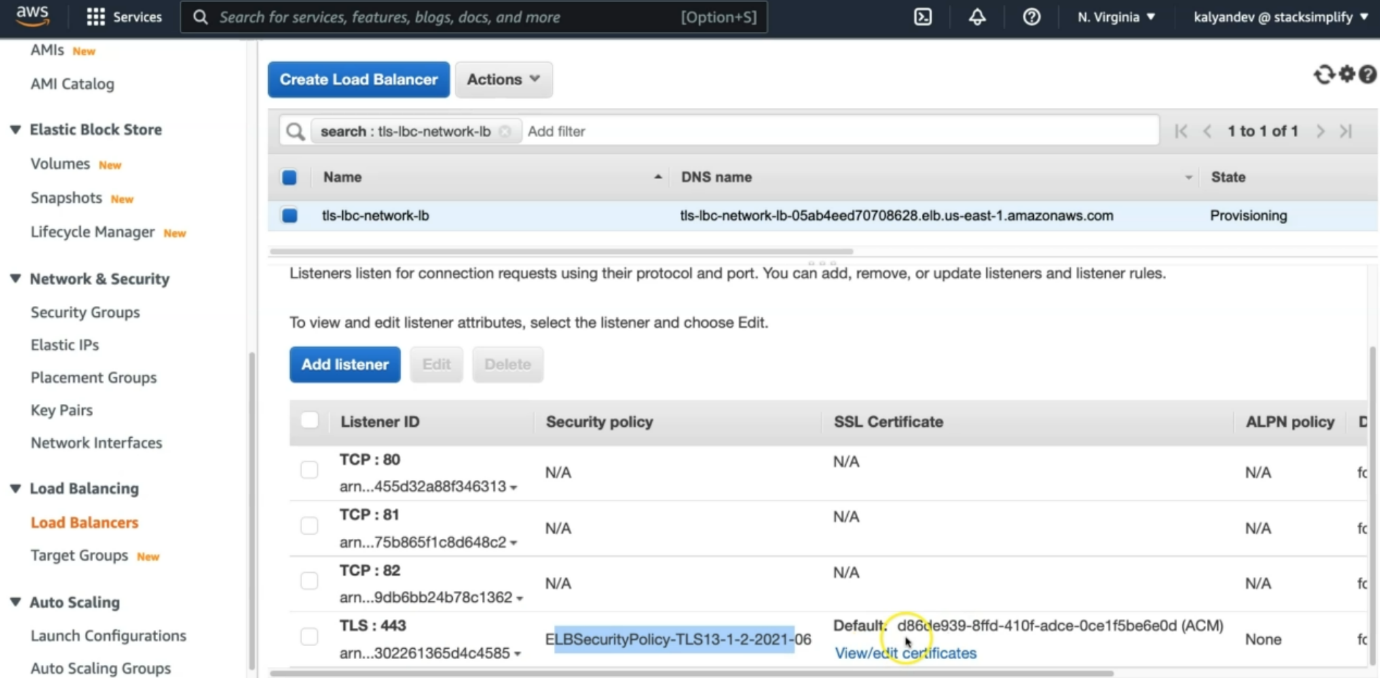
**# Verify using AWS Mgmt Console**

Go to Services -> EC2 -> Load Balancing -> Load Balancers

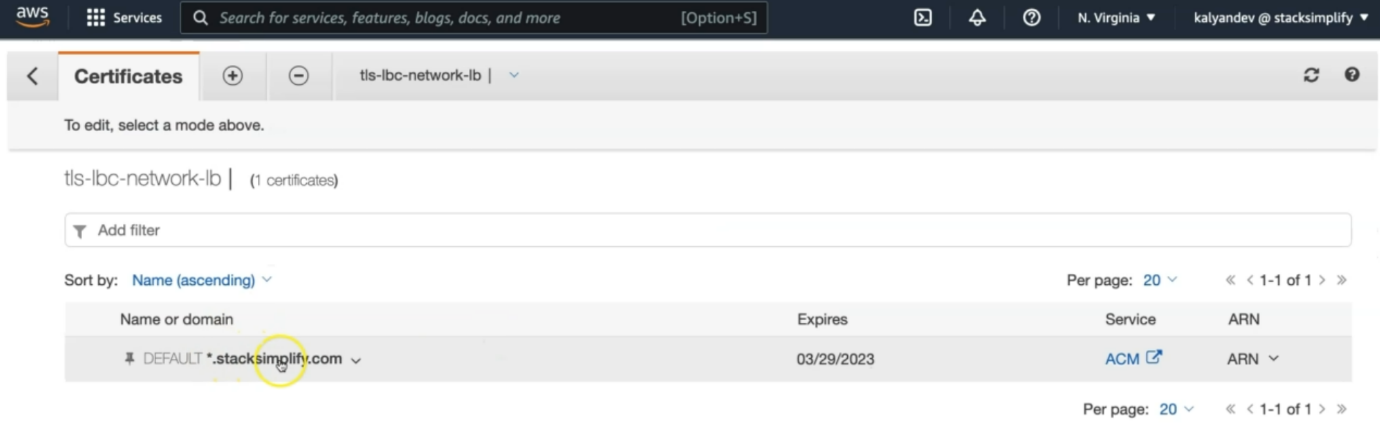
1. Verify Description Tab - DNS Name matching output of "kubectl get svc" External IP

2. Verify Listeners Tab

Observation: Should see two listeners Port 80 and 443



--- **note** – for 443, you can see that the security policy is attaches. Certificate also attached here.



Go to Services -> EC2 -> Load Balancing -> Target Groups

1. Verify Registered targets

2. Verify Health Check path

Observation: Should see two target groups. 1 Target group for 1 listener

**# Access Application**

**# Test HTTP URL**

--- **http://<NLB-DNS-NAME>**

--- **http://lbc-network-lb-tls-demo-a956479ba85953f8.elb.us-east-1.amazonaws.com**

**# Test HTTPS URL**

--- **https://<NLB-DNS-NAME>**

--- **https://lbc-network-lb-tls-demo-a956479ba85953f8.elb.us-east-1.amazonaws.com**

**Clean-Up**

**# Delete or Undeploy kube-manifests**

--- **kubectl delete -f kube-manifests/**

**# Verify if NLB deleted**

In AWS Mgmt Console,

Go to Services -> EC2 -> Load Balancing -> Load Balancers

**References**

--- **Network Load Balancer** - <https://docs.aws.amazon.com/eks/latest/userguide/network-load-balancing.html>

--- **NLB Service** - <https://kubernetes-sigs.github.io/aws-load-balancer-controller/v2.4/guide/service/nlb/>

--- **NLB Service Annotations** - <https://kubernetes-sigs.github.io/aws-load-balancer-controller/v2.4/guide/service/annotations/>