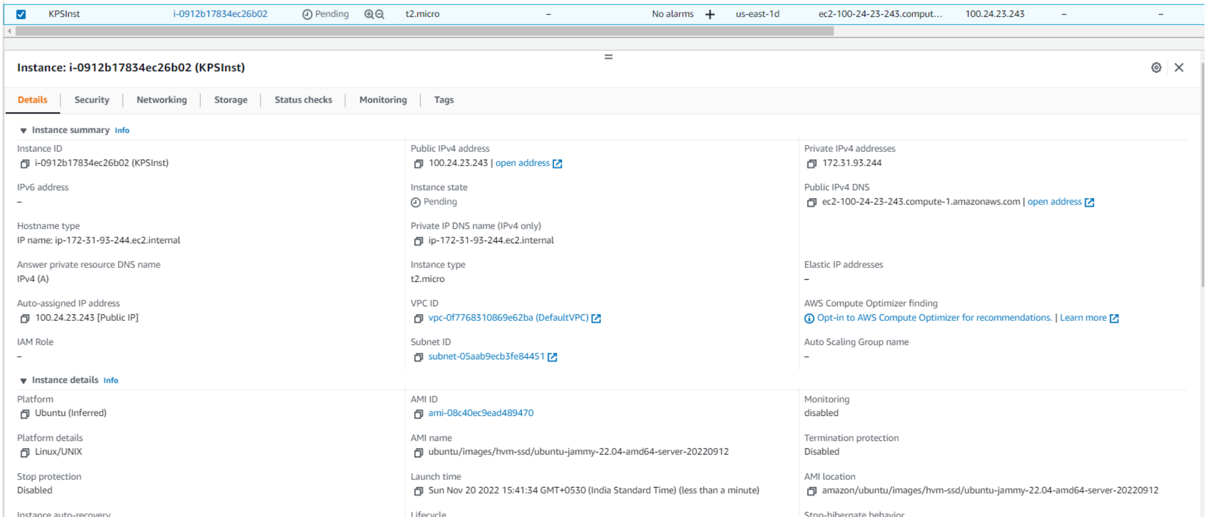
Setup K8s clusters with KOPS

This project explains the setup of Kubernetes clusters with KOPS. Created a Linux VM with KOPS, Kubectls, ssh Keys and awscli to execute commands. A domain was created in Godaddy for Kubernetes DNS records and subdomain was created in Route53 for hosted zone. S3 bucket is created to store the state of Kops, so we can perform KOPS command from anywhere. An IAM user was created to perform AWScli commands,

1. Create an EC2 instance for KOPS, and make sure it allow ssh from Myip



☑	KPSInst	i-0912b17834ec26b02	Pending	t2.micro	–	No alarms	us-east-1d	ec2-100-24-23-243.comput...	100.24.23.243	–

Instance: i-0912b17834ec26b02 (KPSInst)

▼ Instance summary Info

Instance ID
i-0912b17834ec26b02 (KPSInst)

IPv6 address
–

Hostname type
IP name: ip-172-31-93-244.ec2.internal

Answer private resource DNS name
IPv4 (A)

Auto-assigned IP address
100.24.23.243 [Public IP]

IAM Role
–

Public IPv4 address
100.24.23.243 | open address

Instance state
Pending

Private IP DNS name (IPv4 only)
ip-172-31-93-244.ec2.internal

Instance type
t2.micro

VPC ID
vpc-0f7768310869e62ba (DefaultVPC)

Subnet ID
subnet-05aab9ecb3fe84451

Private IPv4 addresses
172.31.93.244

Public IPv4 DNS
ec2-100-24-23-243.compute-1.amazonaws.com | open address

Elastic IP addresses
–

AWS Compute Optimizer finding
Opt-in to AWS Compute Optimizer for recommendations. | Learn more

Auto Scaling Group name
–

▼ Instance details Info

Platform
Ubuntu (Inferred)

Platform details
Linux/UNIX

Stop protection
Disabled

Instance auto-recovery

AMI ID
ami-08c40ec9ead489470

AMI name
ubuntu/images/hvm-ssd/ubuntu-jammy-22.04-amd64-server-20220912

Launch time
Sun Nov 20 2022 15:41:34 GMT+0530 (India Standard Time) (less than a minute)

Lifecycle

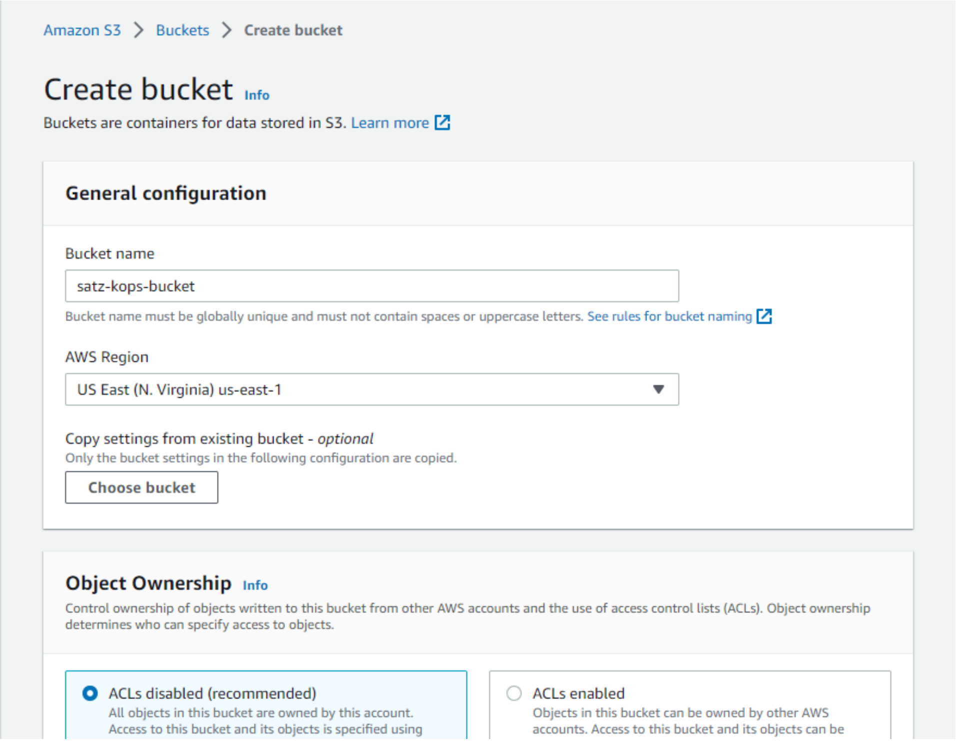
Monitoring
disabled

Termination protection
Disabled

AMI location
amazon/ubuntu/images/hvm-ssd/ubuntu-jammy-22.04-amd64-server-20220912

Stop-hibernate behavior

2. Create an S3 bucket.



Create bucket Info

Buckets are containers for data stored in S3. Learn more

General configuration

Bucket name

satz-kops-bucket

Bucket name must be globally unique and must not contain spaces or uppercase letters. See rules for bucket naming

AWS Region

US East (N. Virginia) us-east-1

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

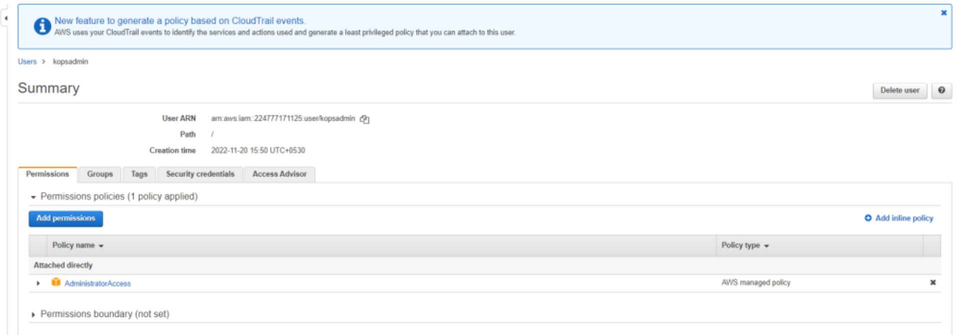
Object Ownership Info

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

● ACLs disabled (recommended)
All objects in this bucket are owned by this account.
Access to this bucket and its objects is specified using

○ ACLs enabled
Objects in this bucket can be owned by other AWS
accounts. Access to this bucket and its objects can be

3. Created the IAM user with Full Admin access,



New feature to generate a policy based on CloudTrail events.
AWS uses your CloudTrail events to identify the services and actions used and generate a least privileged policy that you can attach to this user.

Summary

User ARN arn:aws:iam::224777171125:user/kopsadmin

Path /

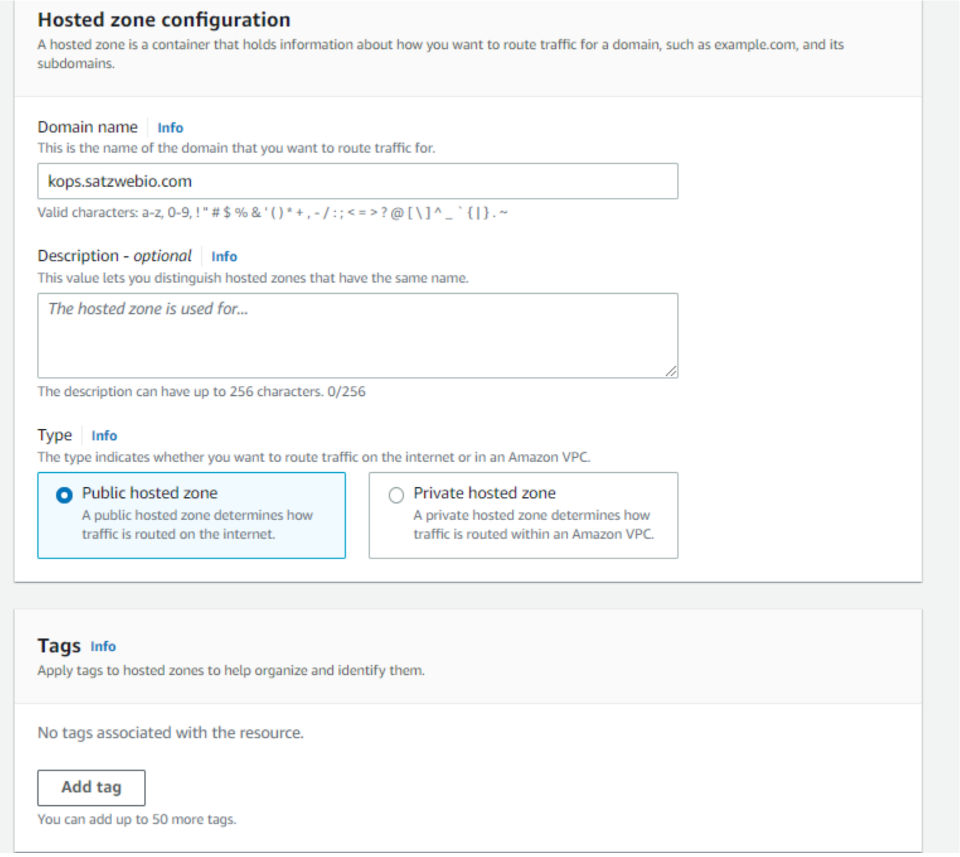
Creation time 2022-11-20 15:50 UTC+0530

Permissions policies (1 policy applied)

Policy name	Policy type
Attached directly	
AdministratorAccess	AWS managed policy

Permissions boundary (not set)

4. Create a hosted zone,



Hosted zone configuration

A hosted zone is a container that holds information about how you want to route traffic for a domain, such as example.com, and its subdomains.

Domain name | Info

This is the name of the domain that you want to route traffic for.

kops.satzwebio.com

Valid characters: a-z, 0-9, ! " # $ % & ' ( ) * + , - / : ; < = > ? @ [\ ] ^ _ ` { | } . ~

Description - *optional* | Info

This value lets you distinguish hosted zones that have the same name.

The hosted zone is used for...

The description can have up to 256 characters. 0/256

Type | Info

The type indicates whether you want to route traffic on the internet or in an Amazon VPC.

● Public hosted zone
A public hosted zone determines how traffic is routed on the internet.

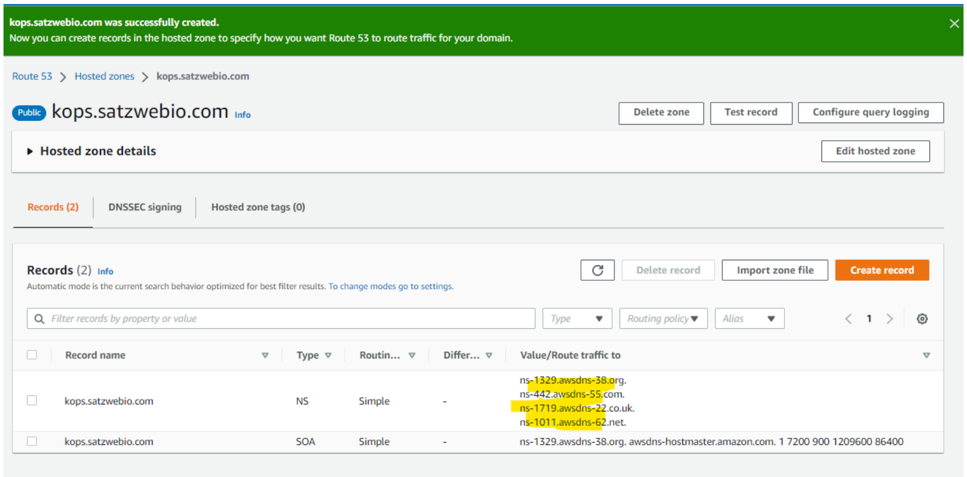
○ Private hosted zone
A private hosted zone determines how traffic is routed within an Amazon VPC.

Tags Info

Apply tags to hosted zones to help organize and identify them.

No tags associated with the resource.

You can add up to 50 more tags.



kops.satzwebio.com was successfully created.
Now you can create records in the hosted zone to specify how you want Route 53 to route traffic for your domain.

Route 53 > Hosted zones > kops.satzwebio.com

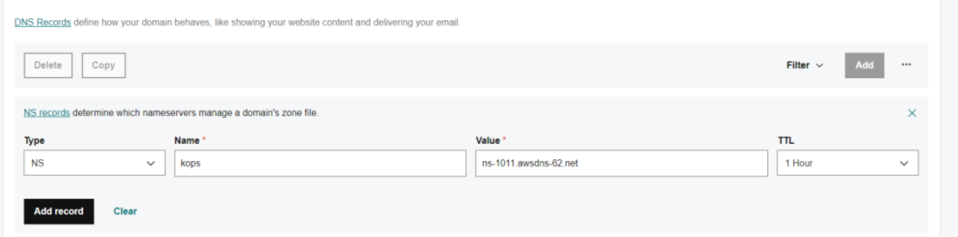
Public kops.satzwebio.com Info

Records (2) Info

Automatic mode is the current search behavior optimized for best filter results. To change modes go to settings.

□	Record name	Type	Routin...	Differ...	Value/Route traffic to
□	kops.satzwebio.com	NS	Simple	-	ns-1329.awsdns-38.org. ns-442.awsdns-55.com. ns-1719.awsdns-22.co.uk. ns-1011.awsdns-62.net.
□	kops.satzwebio.com	SOA	Simple	-	ns-1329.awsdns-38.org. awsdns-hostmaster.amazon.com. 1 7200 900 1209600 86400

5. Update NS record with domain register

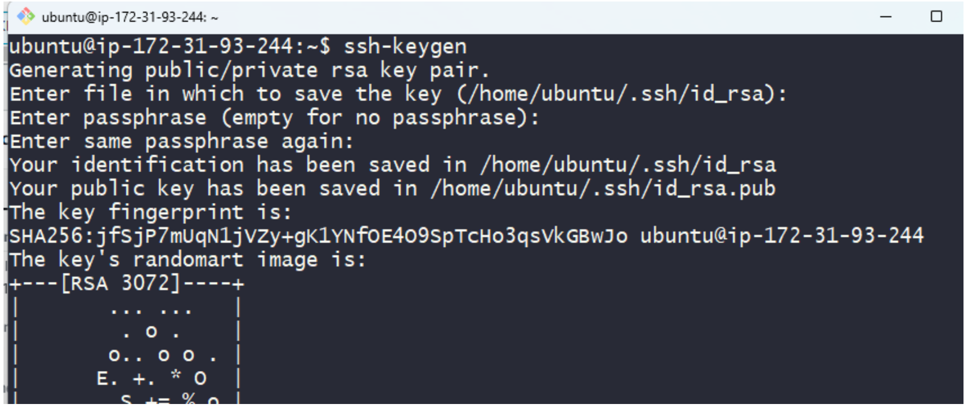


DNS Records define how your domain behaves, like showing your website content and delivering your email.

NS records determine which nameservers manage a domain's zone file.

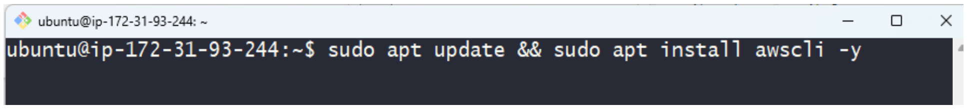
Type	Name *	Value *	TTL
NS	kops	ns-1011.awsdns-62.net	1 Hour

6. Login to the EC2 instance, and generate ssh key



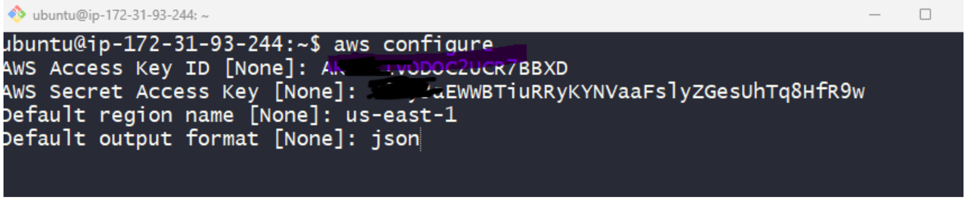
```
ubuntu@ip-172-31-93-244: ~
ubuntu@ip-172-31-93-244:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/ubuntu/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/ubuntu/.ssh/id_rsa
Your public key has been saved in /home/ubuntu/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:jfSjP7mUqN1jVZy+gK1YNfOE4O9SpTcHo3qsVkGBwJo ubuntu@ip-172-31-93-244
The key's randomart image is:
+---[RSA 3072]----+
|       ... ...   |
|        . o .    |
|       o.. o o . |
|      E. +. * O  |
|        S += % o |
```

7. sudo apt update && sudo apt install awscli -y



```
ubuntu@ip-172-31-93-244: ~
ubuntu@ip-172-31-93-244:~$ sudo apt update && sudo apt install awscli -y
```

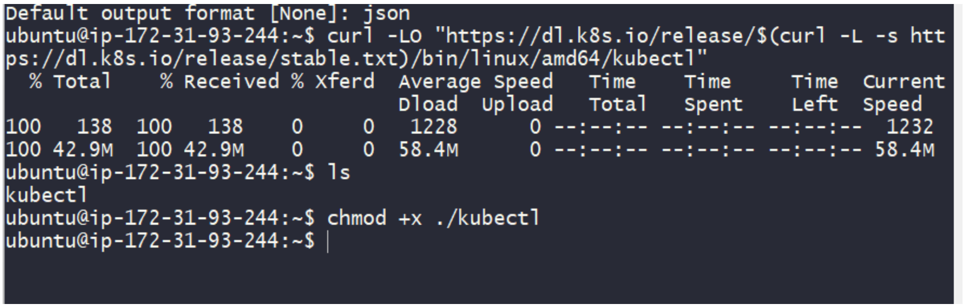
8. Do AWS configure with access key and secret key,



```
ubuntu@ip-172-31-93-244: ~
ubuntu@ip-172-31-93-244:~$ aws configure
AWS Access Key ID [None]: AK[redacted]BBXD
AWS Secret Access Key [None]: [redacted]EWWBTiuRRyKYNVaaFslyZGesUhTq8HfR9w
Default region name [None]: us-east-1
Default output format [None]: json
```

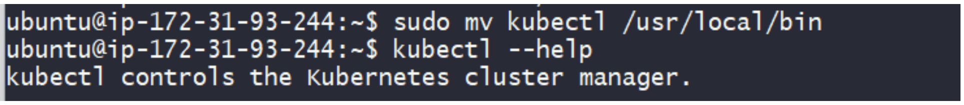
9. Install and setup kubectl, and provide exec permission

Refer: https://kubernetes.io/docs/tasks/tools/install-kubectl-linux/



```
Default output format [None]: json
ubuntu@ip-172-31-93-244:~$ curl -LO "https://dl.k8s.io/release/$(curl -L -s htt
ps://dl.k8s.io/release/stable.txt)/bin/linux/amd64/kubectl"
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   138  100   138    0     0   1228      0 --:--:-- --:--:-- --:--:--  1232
100 42.9M  100 42.9M    0     0  58.4M      0 --:--:-- --:--:-- --:--:-- 58.4M
ubuntu@ip-172-31-93-244:~$ ls
kubectl
ubuntu@ip-172-31-93-244:~$ chmod +x ./kubectl
ubuntu@ip-172-31-93-244:~$ 
```

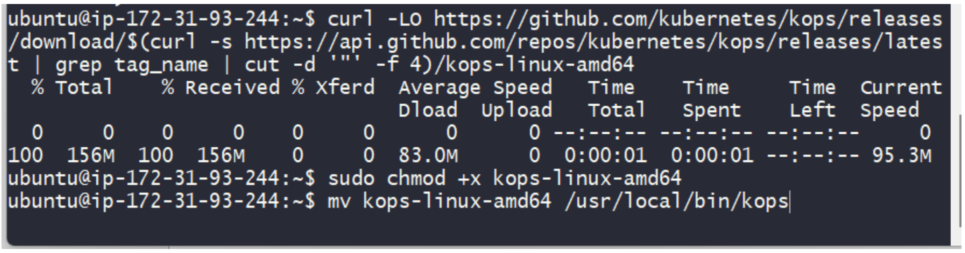
Move to usr/loca/bin to access the tool globally,



```
ubuntu@ip-172-31-93-244:~$ sudo mv kubectl /usr/local/bin
ubuntu@ip-172-31-93-244:~$ kubectl --help
kubectl controls the Kubernetes cluster manager.
```

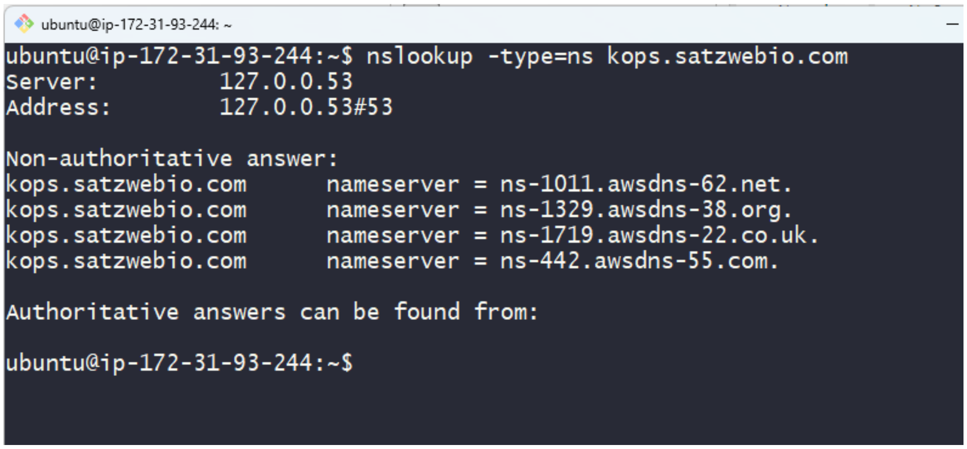
10. Installing Kubernetes with kOps

Refer https://kubernetes.io/docs/setup/production-environment/tools/kops/



```
ubuntu@ip-172-31-93-244:~$ curl -LO https://github.com/kubernetes/kops/releases
/download/$(curl -s https://api.github.com/repos/kubernetes/kops/releases/lates
t | grep tag_name | cut -d '"' -f 4)/kops-linux-amd64
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0
100  156M  100  156M    0     0  83.0M      0  0:00:01  0:00:01 --:--:-- 95.3M
ubuntu@ip-172-31-93-244:~$ sudo chmod +x kops-linux-amd64
ubuntu@ip-172-31-93-244:~$ mv kops-linux-amd64 /usr/local/bin/kops
```

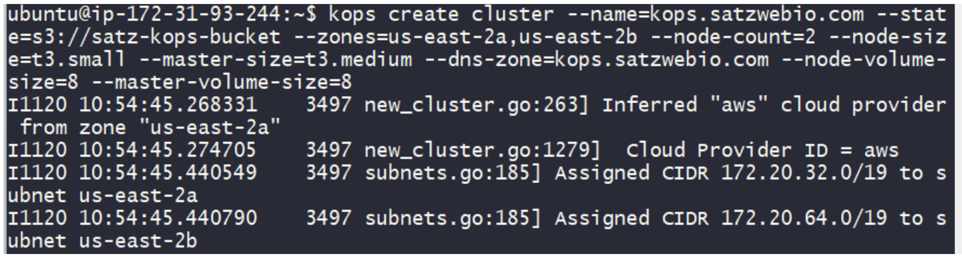
11. Nslookup validation,



```
ubuntu@ip-172-31-93-244:~$ nslookup -type=ns kops.satzwebio.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
kops.satzwebio.com      nameserver = ns-1011.awsdns-62.net.
kops.satzwebio.com      nameserver = ns-1329.awsdns-38.org.
kops.satzwebio.com      nameserver = ns-1719.awsdns-22.co.uk.
kops.satzwebio.com      nameserver = ns-442.awsdns-55.com.

Authoritative answers can be found from:

ubuntu@ip-172-31-93-244:~$
```

12. Execute Kops create cluster command,

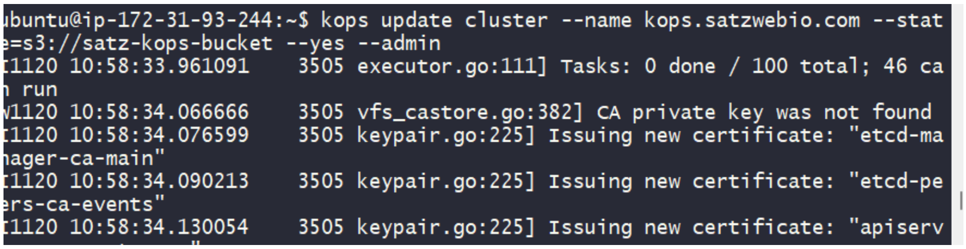
kops create cluster --name=kops.satzwebio.com --state=s3://satz-kops-bucket --zones=us-east-2a,us-east-2b --node-count=2 --node-size=t3.small --master-size=t3.medium --dns-zone=kops.satzwebio.com --node-volume-size=8 --master-volume-size=8



```
ubuntu@ip-172-31-93-244:~$ kops create cluster --name=kops.satzwebio.com --stat
e=s3://satz-kops-bucket --zones=us-east-2a,us-east-2b --node-count=2 --node-siz
e=t3.small --master-size=t3.medium --dns-zone=kops.satzwebio.com --node-volume-
size=8 --master-volume-size=8
I1120 10:54:45.268331    3497 new_cluster.go:263] Inferred "aws" cloud provider
 from zone "us-east-2a"
I1120 10:54:45.274705    3497 new_cluster.go:1279]  Cloud Provider ID = aws
I1120 10:54:45.440549    3497 subnets.go:185] Assigned CIDR 172.20.32.0/19 to s
ubnet us-east-2a
I1120 10:54:45.440790    3497 subnets.go:185] Assigned CIDR 172.20.64.0/19 to s
ubnet us-east-2b
```

13. Following above, perform update cluster

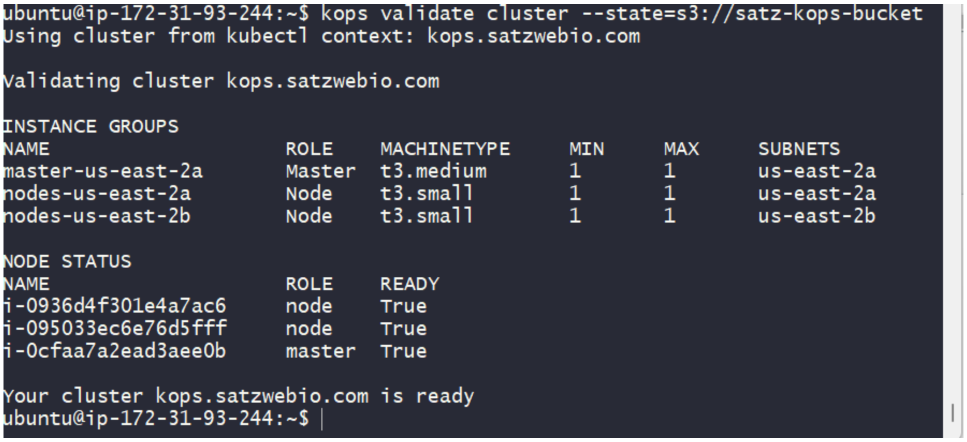
kops update cluster --name kops.satzwebio.com --state=s3://satz-kops-bucket --yes –admin



```
ubuntu@ip-172-31-93-244:~$ kops update cluster --name kops.satzwebio.com --stat
e=s3://satz-kops-bucket --yes --admin
I1120 10:58:33.961091    3505 executor.go:111] Tasks: 0 done / 100 total; 46 ca
n run
W1120 10:58:34.066666    3505 vfs_castore.go:382] CA private key was not found
I1120 10:58:34.076599    3505 keypair.go:225] Issuing new certificate: "etcd-ma
nager-ca-main"
I1120 10:58:34.090213    3505 keypair.go:225] Issuing new certificate: "etcd-pe
ers-ca-events"
I1120 10:58:34.130054    3505 keypair.go:225] Issuing new certificate: "apiserv
```

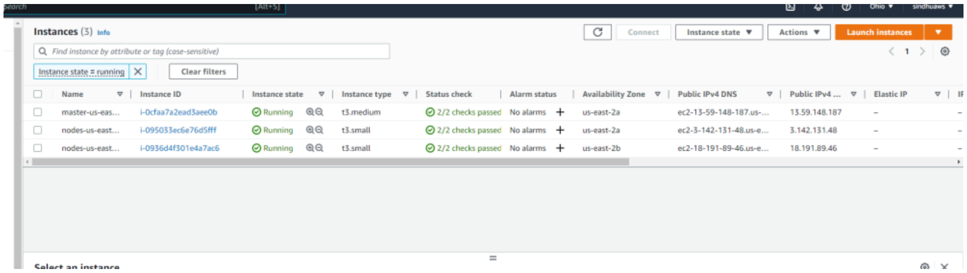
14. After 15 mins, validate your cluster with below commands,

kops validate cluster --state=s3://satz-kops-bucket



```
ubuntu@ip-172-31-93-244:~$ kops validate cluster --state=s3://satz-kops-bucket
Using cluster from kubectl context: kops.satzwebio.com

Validating cluster kops.satzwebio.com

INSTANCE GROUPS
NAME                    ROLE    MACHINETYPE     MIN     MAX     SUBNETS
master-us-east-2a       Master  t3.medium       1       1       us-east-2a
nodes-us-east-2a        Node    t3.small        1       1       us-east-2a
nodes-us-east-2b        Node    t3.small        1       1       us-east-2b

NODE STATUS
NAME                    ROLE    READY
i-0936d4f301e4a7ac6     node    True
i-095033ec6e76d5fff     node    True
i-0cfaa7a2ead3aee0b     master  True

Your cluster kops.satzwebio.com is ready
ubuntu@ip-172-31-93-244:~$ |
```

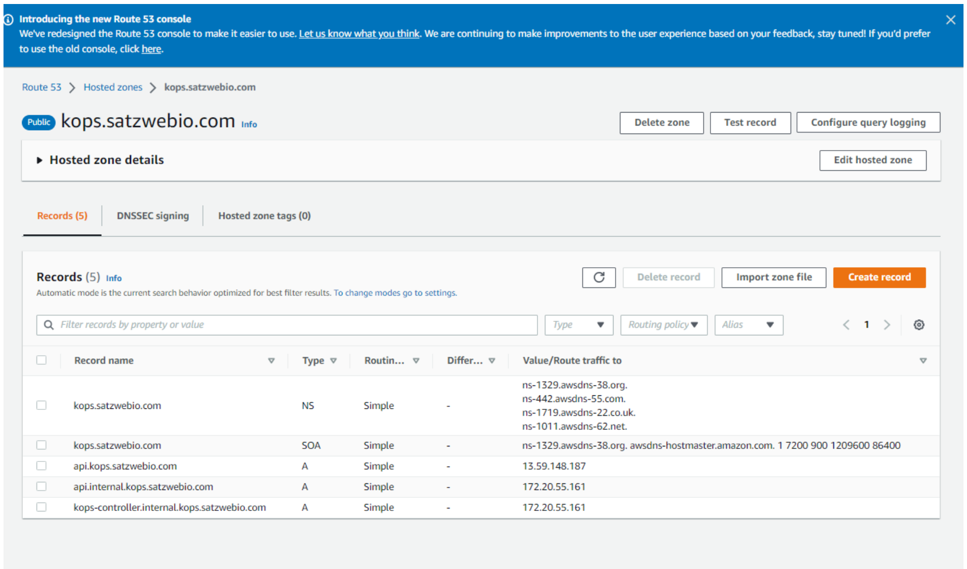
15. Show below the resources created in AWS.



Instances (3) Info

Instance state = running

☐	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
☐	master-us-eas...	i-0cfaa7a2ead3aee0b	✓ Running	t3.medium	✓ 2/2 checks passed	No alarms +	us-east-2a	ec2-13-59-148-187.us-...	13.59.148.187	–
☐	nodes-us-east...	i-095033ec6e76d5fff	✓ Running	t3.small	✓ 2/2 checks passed	No alarms +	us-east-2a	ec2-3-142-131-48.us-e...	3.142.131.48	–
☐	nodes-us-east...	i-0936d4f301e4a7ac6	✓ Running	t3.small	✓ 2/2 checks passed	No alarms +	us-east-2b	ec2-18-191-89-46.us-e...	18.191.89.46	–



Introducing the new Route 53 console

We've redesigned the Route 53 console to make it easier to use. Let us know what you think. We are continuing to make improvements to the user experience based on your feedback, stay tuned! If you'd prefer to use the old console, click here.

Route 53 > Hosted zones > kops.satzwebio.com

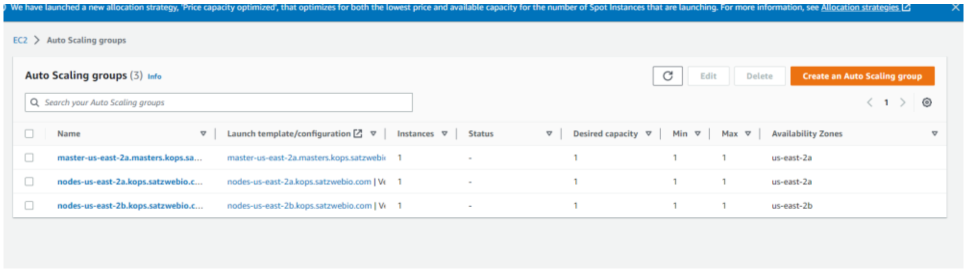
Public kops.satzwebio.com Info

▸ Hosted zone details

Records (5) Info

Automatic mode is the current search behavior optimized for best filter results. To change modes go to settings.

☐	Record name	Type	Routin...	Differ...	Value/Route traffic to
☐	kops.satzwebio.com	NS	Simple	-	ns-1329.awsdns-38.org. ns-442.awsdns-55.com. ns-1719.awsdns-22.co.uk. ns-1011.awsdns-62.net.
☐	kops.satzwebio.com	SOA	Simple	-	ns-1329.awsdns-38.org. awsdns-hostmaster.amazon.com. 1 7200 900 1209600 86400
☐	api.kops.satzwebio.com	A	Simple	-	13.59.148.187
☐	api.internal.kops.satzwebio.com	A	Simple	-	172.20.55.161
☐	kops-controller.internal.kops.satzwebio.com	A	Simple	-	172.20.55.161

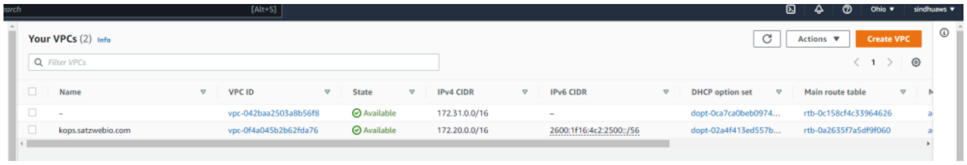


We have launched a new allocation strategy, 'Price capacity optimized', that optimizes for both the lowest price and available capacity for the number of Spot Instances that are launching. For more information, see Allocation strategies

EC2 > Auto Scaling groups

Auto Scaling groups (3) Info

Name	Launch template/configuration	Instances	Status	Desired capacity	Min	Max	Availability Zones
master-us-east-2a.masters.kops.sa...	master-us-east-2a.masters.kops.satzwebi	1	-	1	1	1	us-east-2a
nodes-us-east-2a.kops.satzwebio.c...	nodes-us-east-2a.kops.satzwebio.com | Ve	1	-	1	1	1	us-east-2a
nodes-us-east-2b.kops.satzwebio.c...	nodes-us-east-2b.kops.satzwebio.com | Ve	1	-	1	1	1	us-east-2b

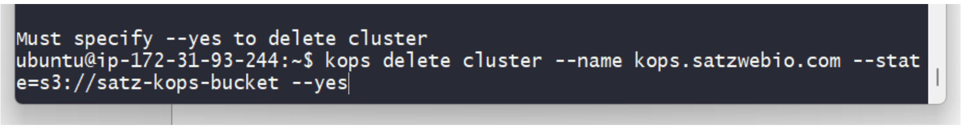


Your VPCs (2) Info

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP option set	Main route table
–	vpc-042baa2503a8b56f8	Available	172.31.0.0/16	–	dopt-0ca7ca0beb0974...	rtb-0c158cf4c33964626
kops.satzwebio.com	vpc-0f4a045b2b62fda76	Available	172.20.0.0/16	2600:1f16:4c2:2500::/56	dopt-02a4f413ed557b...	rtb-0a2635f7a5df9f060

16. To delete the cluster

kops delete cluster --name kops.satzwebio.com --state=s3://satz-kops-bucket --yes



```
Must specify --yes to delete cluster
ubuntu@ip-172-31-93-244:~$ kops delete cluster --name kops.satzwebio.com --stat
e=s3://satz-kops-bucket --yes
```