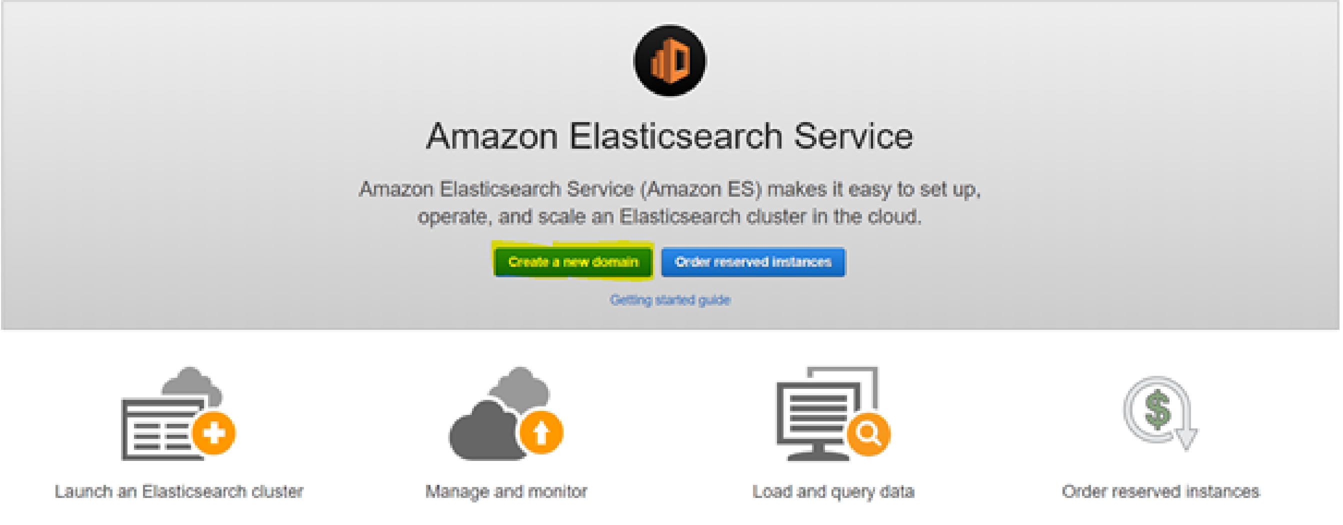
ELK installation on AWS

1. Login AWS console.

2. Search for “Elasticsearch Service”

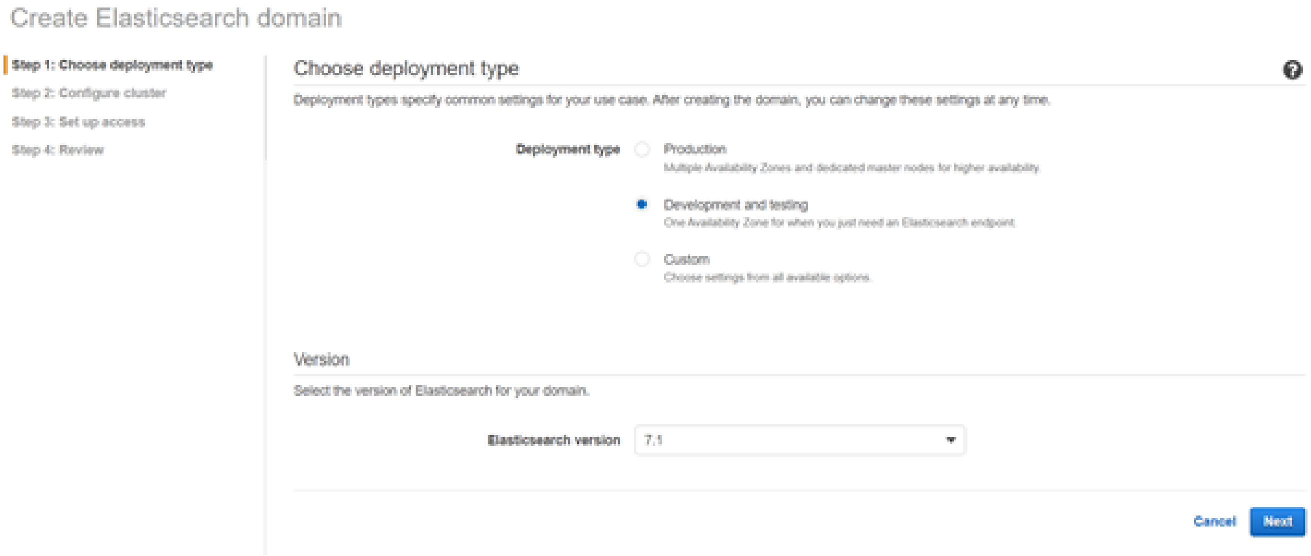
3. Click on “Create a new domain”



Amazon Elasticsearch Service

Amazon Elasticsearch Service (Amazon ES) makes it easy to set up, operate, and scale an Elasticsearch cluster in the cloud.

4. Select environment (Ex : Dev, PROD) type where you are going to setup ELK.



Create Elasticsearch domain

Choose deployment type

Deployment types specify common settings for your use case. After creating the domain, you can change these settings at any time.

Deployment type
○ Production
Multiple Availability Zones and dedicated master nodes for higher availability.
● Development and testing
One Availability Zone for when you just need an Elasticsearch endpoint.
○ Custom
Choose settings from all available options.

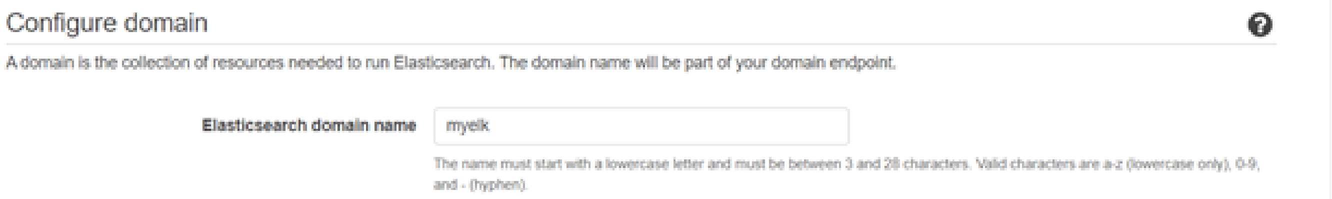
Version

Select the version of Elasticsearch for your domain.

Elasticsearch version: 7.1

5. Enter domain name, instance type, number of nodes, storage type, storage volume type, storage size per node, if you are using ELK for production aws recommend 3 production nodes, select encryption type(https, node to node encryption and Enable encryption of data at rest), select Snapshot configuration then click on next.

Domain name section:



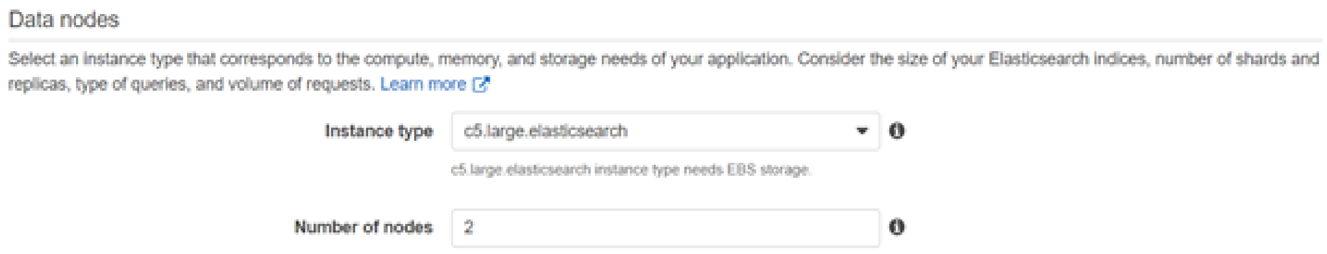
Configure domain

A domain is the collection of resources needed to run Elasticsearch. The domain name will be part of your domain endpoint.

Elasticsearch domain name: myelk

The name must start with a lowercase letter and must be between 3 and 28 characters. Valid characters are a-z (lowercase only), 0-9, and - (hyphen).

Data nodes section:



Data nodes

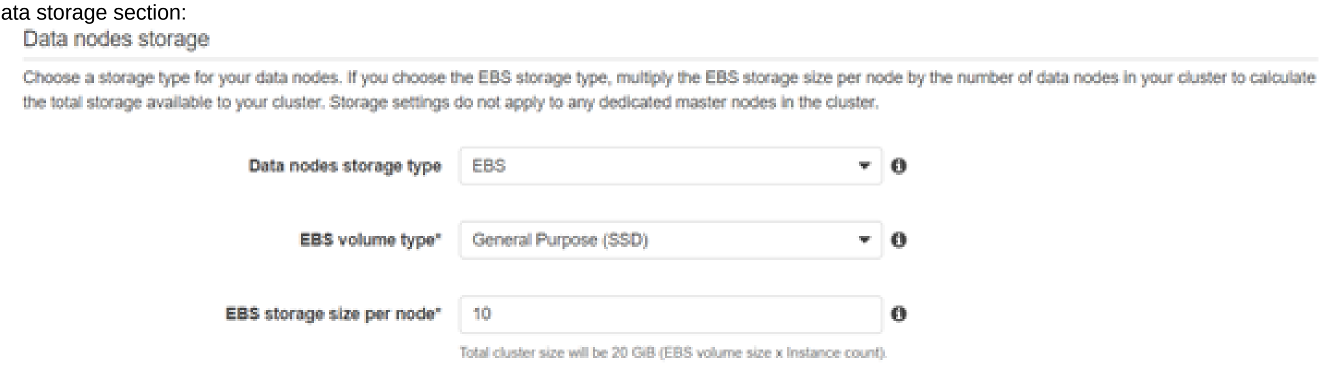
Select an instance type that corresponds to the compute, memory, and storage needs of your application. Consider the size of your Elasticsearch indices, number of shards and replicas, type of queries, and volume of requests. Learn more

Instance type: c5.large.elasticsearch

c5.large.elasticsearch instance type needs EBS storage.

Number of nodes: 2

Data storage section:



Data nodes storage

Choose a storage type for your data nodes. If you choose the EBS storage type, multiply the EBS storage size per node by the number of data nodes in your cluster to calculate the total storage available to your cluster. Storage settings do not apply to any dedicated master nodes in the cluster.

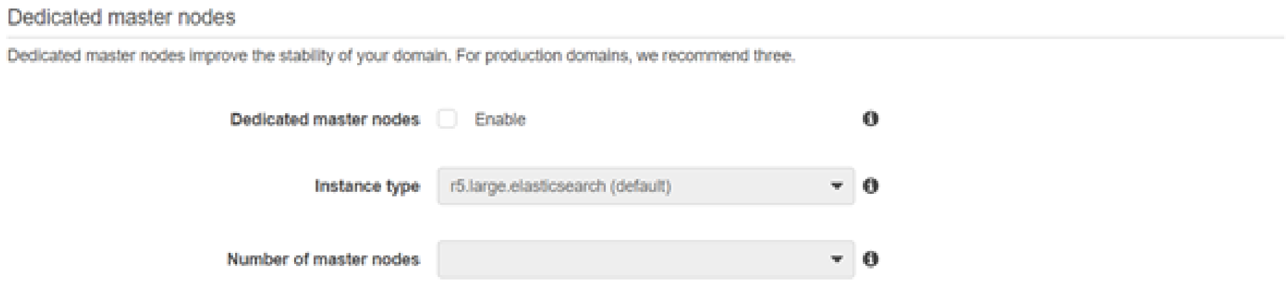
Data nodes storage type: EBS

EBS volume type*: General Purpose (SSD)

EBS storage size per node*: 10

Total cluster size will be 20 GiB (EBS volume size x Instance count).

Dedicated master node section:



Dedicated master nodes

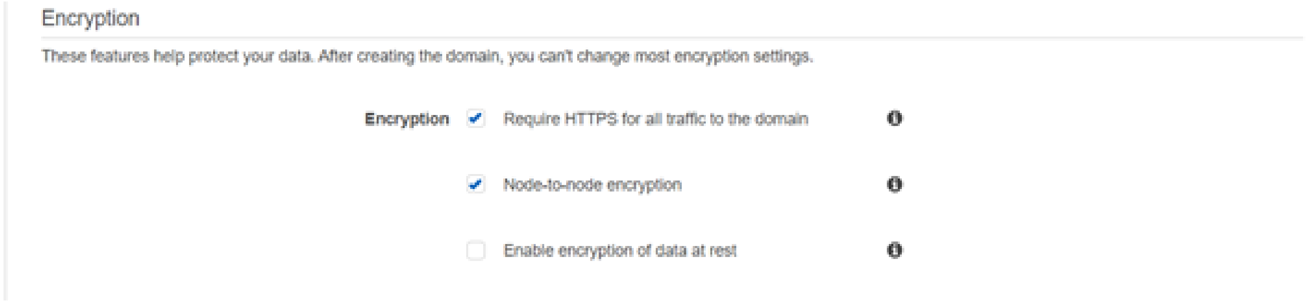
Dedicated master nodes improve the stability of your domain. For production domains, we recommend three.

Dedicated master nodes: ☐ Enable

Instance type: r5.large.elasticsearch (default)

Number of master nodes:

Encryption section:



Encryption

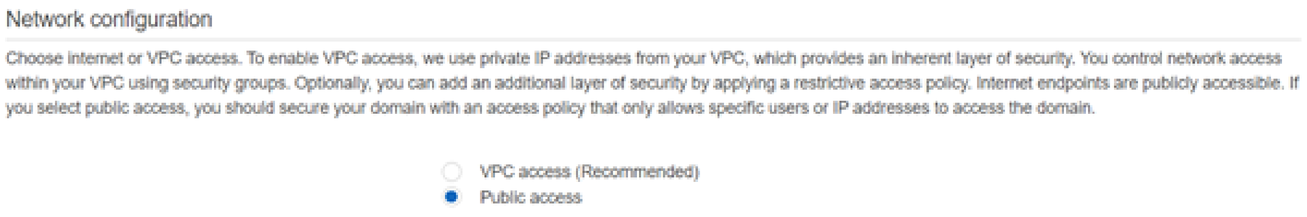
These features help protect your data. After creating the domain, you can't change most encryption settings.

Encryption: ☑ Require HTTPS for all traffic to the domain

☑ Node-to-node encryption

☐ Enable encryption of data at rest

6. Select EKL access option, 1 . VPC wide, 2. Public



Network configuration

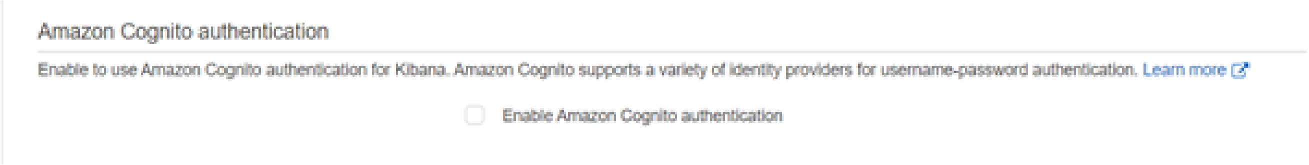
Choose internet or VPC access. To enable VPC access, we use private IP addresses from your VPC, which provides an inherent layer of security. You control network access within your VPC using security groups. Optionally, you can add an additional layer of security by applying a restrictive access policy. Internet endpoints are publicly accessible. If you select public access, you should secure your domain with an access policy that only allows specific users or IP addresses to access the domain.

○ VPC access (Recommended)

● Public access

7. Select/deselect “Amazon Cognito authentication”.

Using this we can allow Kibana URL access to specific location.

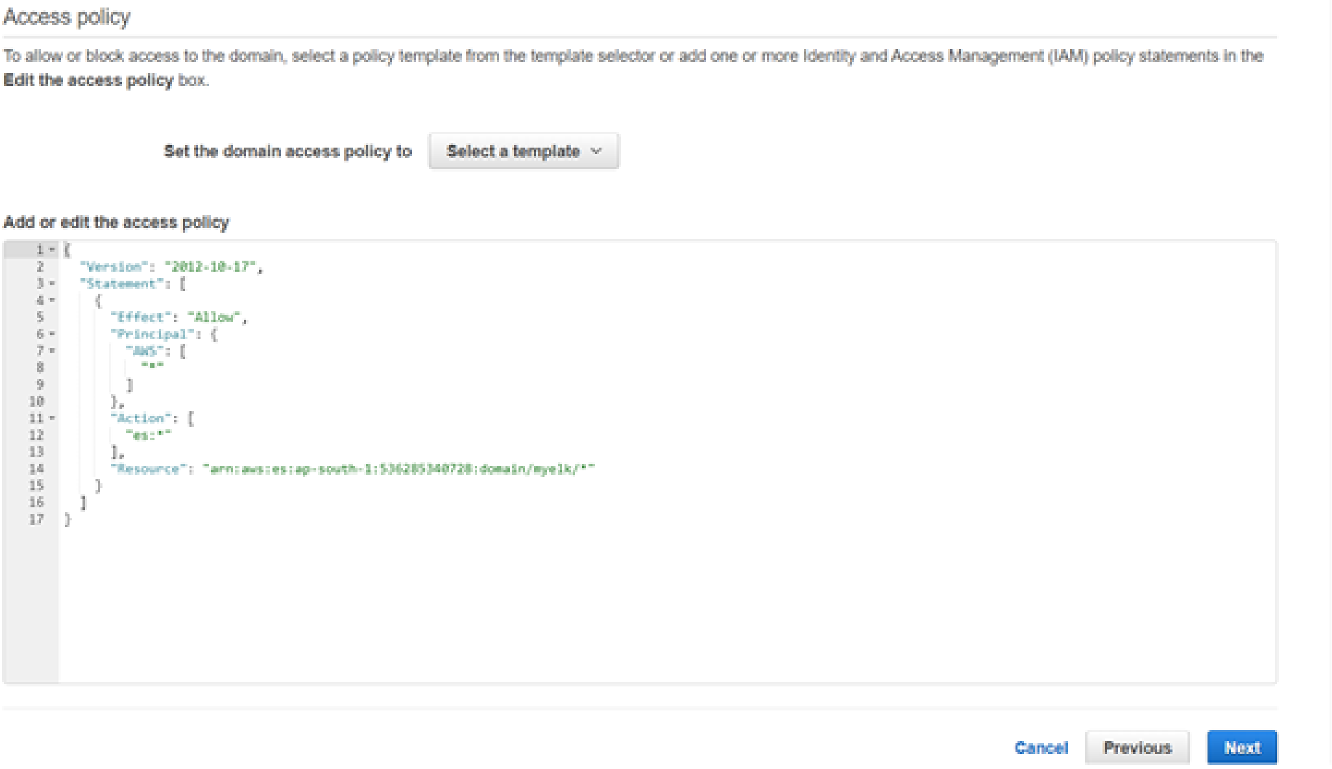


Amazon Cognito authentication

Enable to use Amazon Cognito authentication for Kibana. Amazon Cognito supports a variety of identity providers for username-password authentication. Learn more

□ Enable Amazon Cognito authentication

8. Select access policy, here I am selecting public access.



Access policy

To allow or block access to the domain, select a policy template from the template selector or add one or more Identity and Access Management (IAM) policy statements in the **Edit the access policy** box.

Set the domain access policy to Select a template

Add or edit the access policy

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "*"
        ]
      },
      "Action": [
        "es:*"
      ],
      "Resource": "arn:aws:es:ap-south-1:536285340728:domain/myelk/*"
    }
  ]
}
```

9. Click on next to configure ELK.

10. Once the configuration process complete, will get Kibana and endpoint URLs.