Infosys - DGARM

Search Cluster Setup Document

Last Updated:- 7th Feb, 2026

By

Prashant Kashyap

Document Control

Document No.	Doc_1
Document Version	1
Prepared By	Prashant Kashyap
Release Date	7th Feb 2026

Table of Contents

Infosys - DGARM 1

Document Control 2

Installation of Elasticsearch 4

Kibana Installation 9

Installation of Elasticsearch

1. **Enable subscription-manager register**

```
subscription-manager register --username actual_user --password  actual_pass
```

- Note :- After installation please subscription-manager unregister
  Command :- `subscription-manager unregister`

2 . **Install java on node (server), check the java version and Installation it**

```
yum  install java*
java -version
```

3. **make Elasticsearch as user**

```
useradd elasticsearch
groupadd elasticsearch
```

4. **create data directory as per elasticsearch node functionality**

```
mkdir /data                          // for normal node master and data
mkdir /ml-data                       // for ml node
```

5. **create ELASTIC Directory for installation work**

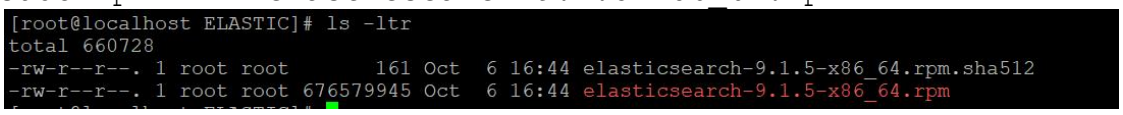
```
mkdir ELASTIC
cd ELASTIC
```

Download Elasticsearch rpm package

```
wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-9.1.5-x86_64.rpm
```

Install Elasticsearch

```
sudo rpm -ivh elasticsearch-9.1.5-x86_64.rpm
```



6. **take backup of original elasticsearch.yml file before make any changes**

```
cp /etc/elasticsearch/elasticsearch.yml /etc/elasticsearch/elasticsearch_yml.backup
```

7. **Change ownership of elk directories and owner**

```
chown -R root:elasticsearch /etc/elasticsearch
chown -R root:elasticsearch /data
chown -R root:elasticsearch /var/log/elasticsearch
```

8. Put necessary node certificates in elasticsearch certs folder

```
[root@localhost elasticsearch]# ls -ltr
total 56
-rw-rw----. 1 root          elasticsearch   197 Oct  3 03:41 roles.yml
-rw-rw----. 1 root          elasticsearch   473 Oct  3 03:41 role_mapping.yml
-rw-rw----. 1 root          elasticsearch 20073 Oct  3 03:41 log4j2.properties
-rw-rw----. 1 root          elasticsearch  3445 Oct  3 03:41 jvm.options
-rw-rw----. 1 root          elasticsearch  1042 Oct  3 03:41 elasticsearch-plugins.example.yml
drwxr-s---. 2 root          elasticsearch     6 Oct  3 03:43 jvm.options.d
-rw-rw----. 1 root          elasticsearch   536 Jan  6 17:21 elasticsearch.keystore
-rw-r-----. 1 root          elasticsearch  4054 Jan  6 17:22 elasticsearch_yml.backup
drwxr-x---. 2 elasticsearch elasticsearch  4096 Jan 13 17:07 certs
-rw-rw----. 1 root          elasticsearch  5627 Jan 13 17:31 elasticsearch.yml
-rw-rw----. 1 root          elasticsearch     0 Jan 13 19:39 users
-rw-rw----. 1 root          elasticsearch     0 Jan 13 19:39 users_roles
[root@localhost elasticsearch]#
```

```
cd /etc/elasticsearch/certs
```

```
[root@[redacted] ~]# cd /etc/elasticsearch/certs/
[root@[redacted] certs]# ls -l
total 56
-rw-r--r--. 1 elasticsearch elasticsearch  4175 Oct 23 16:31 ca.crt
-rw-r--r--. 1 elasticsearch elasticsearch   229 Oct 23 17:13 [redacted].cnf
-rw-r--r--. 1 elasticsearch elasticsearch  2155 Oct 23 17:13 [redacted].crt
-rw-r--r--. 1 elasticsearch elasticsearch  6330 Oct 23 17:13 [redacted].fullchain.crt
-rw-------. 1 elasticsearch elasticsearch  3272 Oct 23 17:13 [redacted].key
-rw-rw----. 1 elasticsearch elasticsearch  1935 Oct 22 13:19 http_ca.crt
-rw-rw----. 1 elasticsearch elasticsearch 10093 Oct 22 13:19 http.p12
-rw-r--r--. 1 elasticsearch elasticsearch  2175 Oct 23 13:56 intermediateCA.crt
-rw-rw----. 1 elasticsearch elasticsearch  5038 Oct 22 13:19 transport.p12
[root@[redacted] certs]#
```

Note :- .cnf, .dgarm.gov.in.crt, fullchain.crt and key will different as per node

9. Enter host entry in hosts file

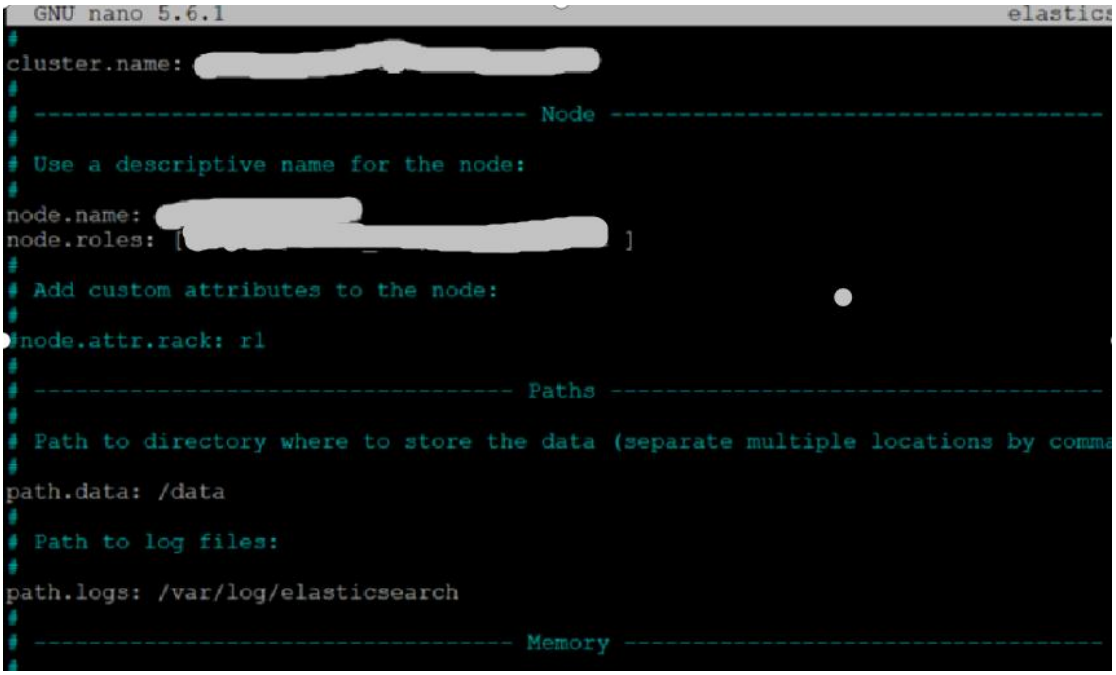
Note : host entry wil be different for DR and Prod as per cluster design or setup

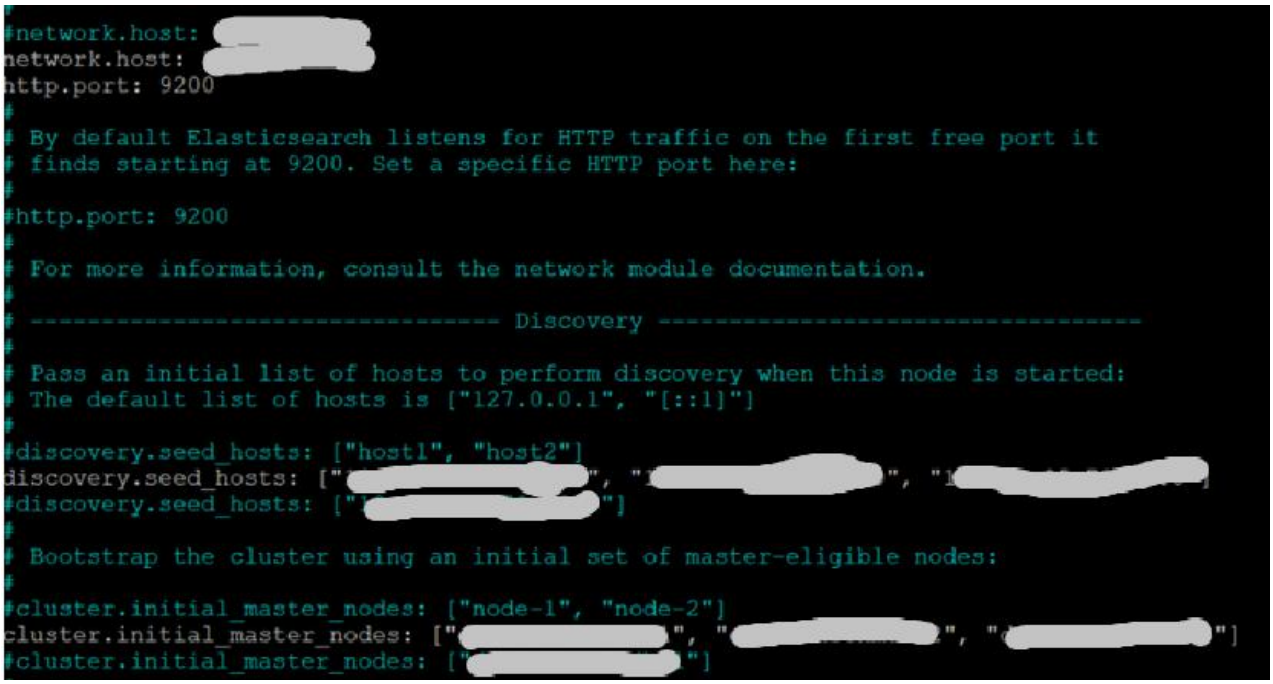
```
nano /etc/hosts
```

All ELK Cluster node entry

10. go to elasticserch folder and make changes in yml file

```
nano elasticsearch.yml
```


GNU nano 5.6.1
cluster.name:
Node
Use a descriptive name for the node:
node.name:
node.roles: [
Add custom attributes to the node:
node.attr.rack: r1
Paths
Path to directory where to store the data (separate multiple locations by comma
path.data: /data
Path to log files:
path.logs: /var/log/elasticsearch
Memory


#network.host:
network.host:
http.port: 9200
By default Elasticsearch listens for HTTP traffic on the first free port it
finds starting at 9200. Set a specific HTTP port here:
#http.port: 9200
For more information, consult the network module documentation.
Discovery
Pass an initial list of hosts to perform discovery when this node is started:
The default list of hosts is ["127.0.0.1", "[::1]"]
#discovery.seed_hosts: ["host1", "host2"]
discovery.seed_hosts:
#discovery.seed_hosts:
Bootstrap the cluster using an initial set of master-eligible nodes:
#cluster.initial_master_nodes: ["node-1", "node-2"]
cluster.initial_master_nodes:
#cluster.initial_master_nodes:

```
xpack.security.enrollment.enabled: true

# Enable encryption for HTTP API client connections, such as Kibana, Logstash, and Agents
#xpack.security.http.ssl:
#  enabled: true
#  keystore.path: certs/http.p12

# Enable encryption and mutual authentication between cluster nodes
#xpack.security.transport.ssl:
#  enabled: true
#  verification_mode: certificate
#  keystore.path: certs/transport.p12
#  truststore.path: certs/transport.p12
#xpack.security.transport.ssl.enabled: false
xpack.security.enabled: true
xpack.security.transport.ssl.enabled: true
xpack.security.transport.ssl.verification_mode: certificate
xpack.security.transport.ssl.certificate: /etc/elasticsearch/certs/[redacted].fullchain.crt
xpack.security.transport.ssl.key: /etc/elasticsearch/certs/[redacted].key
xpack.security.transport.ssl.certificate_authorities: ["/etc/elasticsearch/certs/ca.crt"]
  #xpack.security.transport.ssl.keystore.path: /etc/elasticsearch/certs/transport.p12
  #xpack.security.transport.ssl.truststore.path: /etc/elasticsearch/certs/transport.p12


xpack.security.http.ssl.enabled: true
xpack.security.http.ssl.certificate: /etc/elasticsearch/certs/[redacted].fullchain.crt
xpack.security.http.ssl.key: /etc/elasticsearch/certs/[redacted].key
xpack.security.http.ssl.certificate_authorities: ["/etc/elasticsearch/certs/ca.crt"]
  #xpack.security.http.ssl.keystore.path: /etc/elasticsearch/certs/transport.p12
  #xpack.security.http.ssl.truststore.path: /etc/elasticsearch/certs/transport.p12

# Create a new cluster with the current node only
# Additional nodes can still join the cluster later
#cluster.initial_master_nodes: ["dcplelkshmdh01"]

# Allow HTTP API connections from anywhere
# Connections are encrypted and require user authentication
http.host: 0.0.0.0
```

```
# Allow HTTP API connections from anywhere
# Connections are encrypted and require user authenticati
http.host: 0.0.0.0

# Allow other nodes to join the cluster from anywhere
# Connections are encrypted and mutually authenticated
#transport.host: 0.0.0.0
#bootstrap.memory_lock: true

action.destructive_requires_name: true
```

11. start 9200 and 9300 port

```
systemctl start firewalld
firewall-cmd --permanent --add-port=9200/tcp
firewall-cmd --permanent --add-port=9300/tcp
systemctl reload firewalld
```

12. start the elasticsearch service

```
sudo systemctl daemon-reload
sudo systemctl enable elasticsearch
sudo systemctl start  elasticsearch
sudo systemctl restart  elasticsearch
sudo systemctl status elasticsearch
```

```
sudo systemctl stop elasticsearch
```

13. Commands for check the error of Elasticsearch

```
sudo journalctl -u elasticsearch.service
sudo journalctl -u elasticsearch.service -f
```

14. Elasticsearch Instance

```
ps aux | grep elasticsearch
sudo netstat -plnt | grep 9200
```

15. command to change password for Elasticsearch user i custom form

```
/usr/share/bin/elasticsearch-reset-password -u elastic -i    // set custom password
```

Note:- The same steps are followed for all other Elasticsearch nodes.

Overview for Search Cluster nodes:- 3 master/hot nodes, 1 ml node and 2 Kibana nodes.

Kibana Installation

1. **Enable subscription-manager register**

   subscription-manager register --username ABC --password abc@123

   Note :- After installation please subscription-manager unregister

   Command :- subscription-manager unregister

2. **Install java on node (server), check the java version and Install it**

   yum install java*

   java -version

3. **Make Kibana as user and group**

   useradd elasticsearch

   groupadd elasticsearch

4. **Create Kibana Directory for installation work**

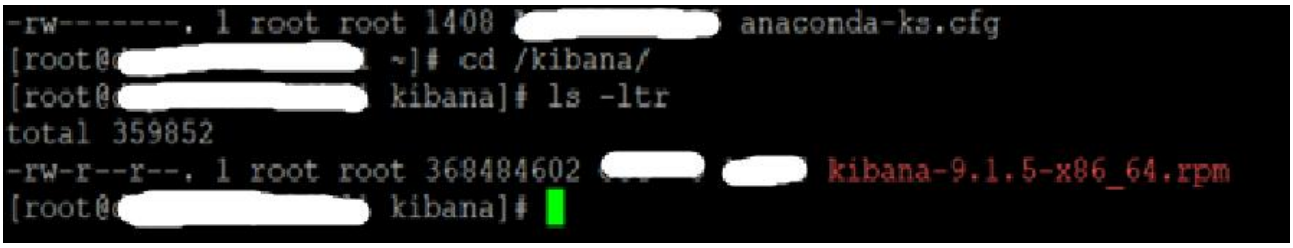
   mkdir /kibana

   cd /kibana/

   wget https://artifacts.elastic.co/downloads/kibana/kibana-9.1.5-x86_64.rpm

   yum install net-tools

   rpm -ivh kibana-9.1.5-x86_64.rpm

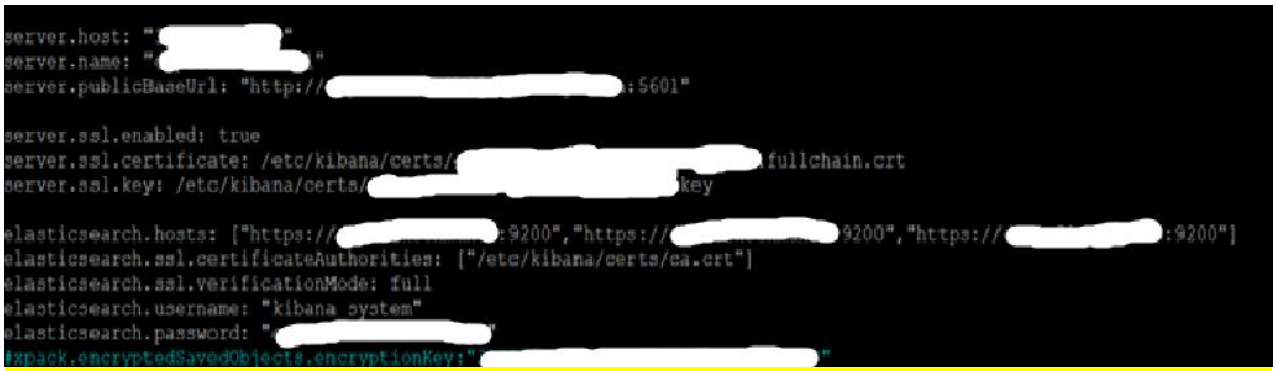


5. **put all certificates in certs directory**

cd /etc/kibana/certs/

6. make changes in kibana.yml file

```
# Enables you to specify a file where Kibana stores log output.
logging:
  appenders:
    file:
      type: file
      fileName: /var/log/kibana/kibana.log
      layout:
        type: json
  root:
    appenders:
      - default
      - file
#  policy:
```



Note : As per node, cluster and server host name will be different

7. open port and reload

```
firewall-cmd --permanent --add-port=5601/tcp
systemctl reload firewalld
netstat -an | grep 5601
```

8. Give permission to kibana respect folders

```
chown -R kibana:kibana /etc/kibana/certs
chown  -R kibana:kibana /opt/kibana
chown  -R kibana:kibana /var/log/kibana
```

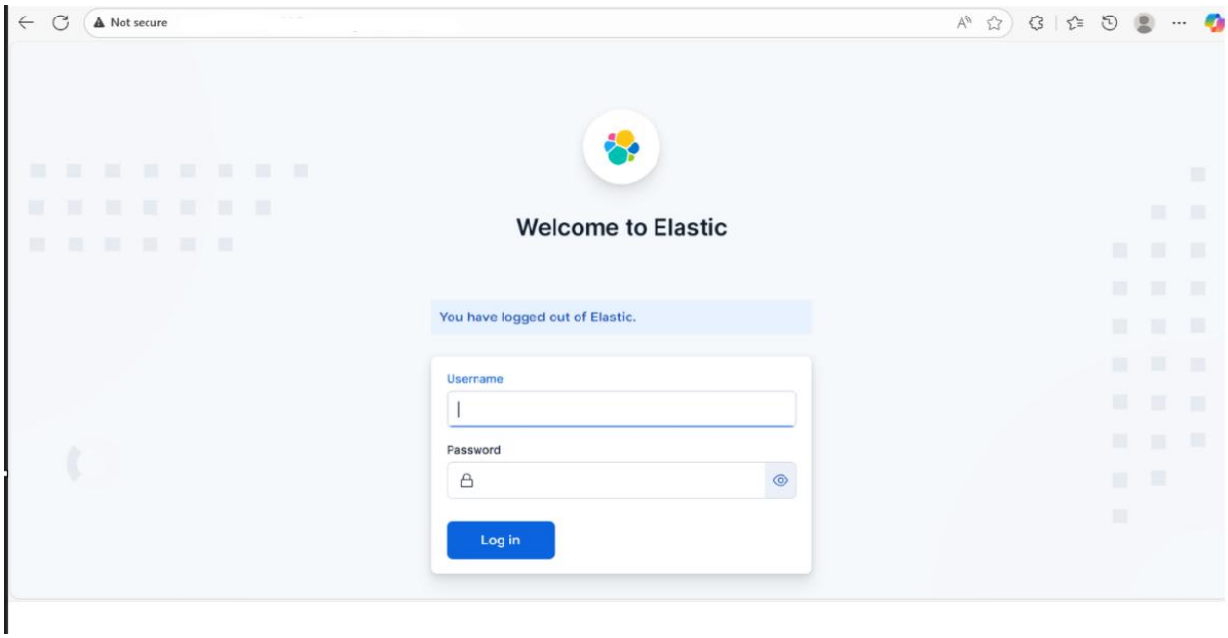
9. restart kibana service

```
sudo systemctl daemon-reload
sudo systemctl enable kibana
sudo systemctl start kibana
sudo systemctl restart kibana
sudo systemctl status kibana
```

10. Command to reset kibana_system user password from elasticsearch master node.

```
Cd /usr/share/elasticsearch
Sudo  ./bin/elasticsearch-reset-password -u kibana_system
```

11. Now go to search engine and access kiban dashboard or url



https://kibanalocalhost:5601

Enter elastic and its password

Username :- elastic

Password :- custom or auto generated.

Note: The same process will be followed for the other Kibana node.