Instructions & Tasks

You work as a system administrator and are in charge of a 3-node Elasticsearch cluster that has been used for ad-hoc, non-sensitive data analysis. However, your Business Intelligence office would like to start using this cluster to analyze some sensitive customer data, so they need you to secure the Elasticsearch cluster to meet the following data security requirements:

* Cluster network encryption
* Client network encryption
* User authentication

To do this, you will need to install X-Pack, which has been pre-downloaded to /home/elastic/x-pack.zip. After installation, you will need to create a certificate authority (CA) using X-Pack's certutil tool, and then use the CA to create node certificates for each Elasticsearch node. The CA and node certificates should be password-protected and stored in the /home/elastic/elasticsearch/config/certs directory.

To support full verification mode, the node certificates should be generated as follows:

| **Name** | **DNS** | **IP** | **Filename** | **Password** |
| --- | --- | --- | --- | --- |
| node1 | ip-10-0-1-101.ec2.internal | 10.0.1.101 | node1.p12 | elastic\_node1 |
| node2 | ip-10-0-1-102.ec2.internal | 10.0.1.102 | node2.p12 | elastic\_node2 |
| node3 | ip-10-0-1-103.ec2.internal | 10.0.1.103 | node3.p12 | elastic\_node3 |

**Don’t forget to add the password you used to protect the certificate package to the local Elasticsearch keystore on each node as both the truststore and keystore secure password.**

help

check\_box\_outline\_blank

**Install X-Pack on each Elasticsearch node.**

Log In

1. Using the Secure Shell (SSH), log in to node1 as cloud\_user via the public IP address.
2. Become the elastic user with:

sudo su - elastic

Install X-Pack

1. Change directory to the Elasticsearch installation path.

cd /home/elastic/elasticsearch

1. Install X-Pack with:

./bin/elasticsearch-plugin install file:///home/elastic/x-pack.zip

1. Grant additional permissions for X-Pack at the prompts by typing **Y** and pressing **Enter**.

Repeat

1. Repeat these steps for node2 and node3.

help

check\_box\_outline\_blank

**Use the X-Pack `certutil` tool to generate a certificate authority.**

Log In

1. Using the Secure Shell (SSH), log in to node1 as cloud\_user via the public IP address.
2. Become the elastic user with:

sudo su - elastic

Generate the Certificate Authority (CA)

1. Create a certs directory.

mkdir /home/elastic/elasticsearch/config/certs

1. Change directory to the certs directory.

cd /home/elastic/elasticsearch/config/certs

1. Create a CA certificate with:

/home/elastic/elasticsearch/bin/x-pack/certutil ca

1. Use the default output file.
2. Set the CA password to elastic\_ca.

Disseminate the CA to the Cluster

1. Remote copy the CA to node2.

scp /home/elastic/elasticsearch/config/certs/elastic-stack-ca.p12 cloud\_user@10.0.1.102:/tmp

1. Remote copy the CA to node3.

scp /home/elastic/elasticsearch/config/certs/elastic-stack-ca.p12 cloud\_user@10.0.1.103:/tmp

Install the CA on Nodes 2 and 3

1. Using the Secure Shell (SSH), log in to node2 as cloud\_user via the public IP address.
2. Become the root user with:

sudo su -

1. Change the ownership of the CA.

chown elastic:elastic /tmp/elastic-stack-ca.p12

1. Become the elastic user with:

su - elastic

1. Create a certs directory.

mkdir /home/elastic/elasticsearch/config/certs

1. Move the CA into the certs directory.

mv /tmp/elastic-stack-ca.p12 /home/elastic/elasticsearch/config/certs/.

1. Repeat these steps for node3.

help

check\_box\_outline\_blank

**Use the X-Pack `certutil` tool with the CA to generate a PKCS#12 keystore.**

Log In

1. Using the Secure Shell (SSH), log in to node1 as cloud\_user via the public IP address.
2. Become the elastic user with:

sudo su - elastic

Generate the Node Certificate

1. Change directory to the certs directory.

cd /home/elastic/elasticsearch/config/certs

1. Generate the node certificate with the CA and the CA's password (elastic\_ca).

/home/elastic/elasticsearch/bin/x-pack/certutil cert --ca elastic-stack-ca.p12 --name node\_name\_here --dns dns\_here --ip ip\_address\_here

1. Use the default output file name.
2. Set the node certificate password per the instructions.

Add the Password to Elasticsearch's Keystore

1. Add the transport keystore password.

/home/elastic/elasticsearch/bin/elasticsearch-keystore add xpack.security.transport.ssl.keystore.secure\_password

1. Add the transport truststore password.

/home/elastic/elasticsearch/bin/elasticsearch-keystore add xpack.security.transport.ssl.truststore.secure\_password

1. Add the HTTP keystore password.

/home/elastic/elasticsearch/bin/elasticsearch-keystore add xpack.security.http.ssl.keystore.secure\_password

1. Add the HTTP truststore password.

/home/elastic/elasticsearch/bin/elasticsearch-keystore add xpack.security.http.ssl.truststore.secure\_password

Repeat

1. Repeat these steps on node2 and node3.

help

check\_box\_outline\_blank

**Configure transport network encryption and start Elasticsearch.**

Log In

1. Using the Secure Shell (SSH), log in to node1 as cloud\_user via the public IP address.
2. Become the elastic user with:

sudo su - elastic

Configure Transport Network Encryption

1. Add the following to /home/elastic/elasticsearch/config/elasticsearch.yml:
2. #
3. # ---------------------------------- X-Pack ------------------------------------
4. #
5. xpack.security.enabled: true
6. xpack.security.transport.ssl.enabled: true
7. xpack.security.transport.ssl.verification\_mode: full
8. xpack.security.transport.ssl.keystore.path: certs/node1.p12

xpack.security.transport.ssl.truststore.path: certs/node1.p12

Start Elasticsearch

1. Change directory to the elasticsearch directory.

cd /home/elastic/elasticsearch/

1. Start Elasticsearch as a background daemon and record the PID to a file.

./bin/elasticsearch -d -p pid

Repeat

1. Repeat these steps on node2 and node3, but remember to change the name of the certificate to match the node you're on.

help

check\_box\_outline\_blank

**Use the X-Pack `setup-passwords` tool to set the password for each built-in user.**

Log In

1. Using the Secure Shell (SSH), log in to node1 as cloud\_user via the public IP address.
2. Become the elastic user with:

sudo su - elastic

1. Change directory to the elasticsearch directory.

cd /home/elastic/elasticsearch/

Set the Built-In User Passwords

1. Set the built-in user passwords using the setup-passwords utility.

./bin/x-pack/setup-passwords interactive

1. Use the following passwords:

User: elastic

Password: elastic

User: kibana

Password: kibana

User: logstash\_system

Password: logstash\_system

help

check\_box\_outline\_blank

**Configure HTTP network encryption and restart Elasticsearch.**

Log In

1. Using the Secure Shell (SSH), log in to node1 as cloud\_user via the public IP address.
2. Become the elastic user with:

sudo su - elastic

Configure HTTP Network Encryption

1. Add the following to /home/elastic/elasticsearch/config/elasticsearch.yml:
2. xpack.security.http.ssl.enabled: true
3. xpack.security.http.ssl.keystore.path: certs/node1.p12

xpack.security.http.ssl.truststore.path: certs/node1.p12

Restart Elasticsearch

1. Change directory to the elasticsearch directory.

cd /home/elastic/elasticsearch/

1. Stop Elasticsearch.

kill `cat pid`

1. Start Elasticsearch as a background daemon and record the PID to a file.

./bin/elasticsearch -d -p pid

Repeat

1. Repeat these steps on node2 and node3, but remember to change the name of the certificate to match the node you are on.