

3.TLS로 노드 연결하기

Elasticsearch TLS 설정 가이드

1. TLS 및 HTTPS 필요성

1. 현재 Elasticsearch 인스턴스는 기본적으로 9200 포트를 통해 누구나 접근 가능 → 보안 설정 필요.
2. **TLS**는 안전한 통신을 위한 프로토콜이며, HTTPS는 TLS를 기반으로 한 HTTP 암호화.
 - HTTPS를 사용하지 않으면 데이터 탈취 가능성이 높음.
3. TLS는 공개키와 대칭키 방식을 조합해 통신을 암호화.

2. Elasticsearch 보안 및 TLS 활성화

설정 파일 수정 (`config/elasticsearch.yml`)

1. 보안을 활성화:

```
yaml
xpack.security.enabled: true
```

2. TLS 설정 추가:

```
yaml
xpack.security.transport.ssl.enabled: true
xpack.security.transport.ssl.keystore.path: certs/elastic.p12
xpack.security.transport.ssl.truststore.path: certs/elastic.p12
```

3. 인증서 생성

1. Root CA 생성 (대칭키 생성)

```
bash
./bin/elasticsearch-certutil ca
```

- 생성된 파일: `elastic-stack-ca.p12`
- 비밀번호는 자유롭게 설정.

2. 노드 인증서 생성

```
bash
./bin/elasticsearch-certutil cert \
  --ca elastic-stack-ca.p12 \
  --dns <각 노드의 별명 ex) es-1,es-2,...>es-1,es-2,es-3 \
  --ip <각 노드의 private-ip> \
  --out config/certs/elastic.p12
```

- 노드 인증서 `elastic.p12` 생성.
- 비밀번호를 설정 (예: `qlalfqjsgh`).

4. 인증서 및 설정 파일 배포

Cyberduck 을 이용해서 각 노드에 원격으로 배포할 수 있음

1. 인증서(`elastic.p12`)를 각 노드에 배포:
 - `scp` 또는 Cyberduck을 사용해 인증서 로컬에 받고 업로드. 이때 연결을

- 각 노드에서 다음과 같이 설정:

```
bash
mkdir -p config/certs
mv <path_to_elastic.p12> config/certs/
```

2. Cyberduck 으로 각 노드에 config/certs/ 에 ca.12 파일 업로드해도동일함
3. `elasticsearch.yml` 파일에 동일한 설정 적용.

5. Keystore 설정

1. Keystore 생성

```
bash
./bin/elasticsearch-keystore create
```

2. Keystore에 비밀번호 추가

```
bash
./bin/elasticsearch-keystore add xpack.security.transport.ssl.keystore.secure_password
```

```
./bin/elasticsearch-keystore add xpack.security.transport.ssl.truststore.secure_password
```

- 비밀번호 노출을 방지하고, Keystore에 저장.

3. Keystore 확인

```
bash
./bin/elasticsearch-keystore list
```

- Keystore에 저장된 키 목록 확인.

6. Elasticsearch 재시작 및 테스트

1. 각 노드에서 Elasticsearch 실행:

```
bash
./bin/elasticsearch
```

2. 정상적으로 실행되었는지 확인:

```
# 클러스터에 포함된 모든 노드의 상태와 메트릭을 확인
curl -XGET "http://<노드_IP>:9200/_cat/nodes"
```

마스터 노드는 세 노드중 따로 설정하지 않더라도 자동으로 하나가 선택됨

7. 패스워드 설정

1. 사용자 계정 비밀번호 설정:

```
bash
./bin/elasticsearch-setup-passwords interactive
```

- **elastic** 계정 등 기본 계정의 비밀번호를 설정. → 동일한 **비밀번호** 입력 !

```
ubuntu@ip-172-31-44-111:~/elasticsearch-7.10.2$ ./bin/elas
Initiating the setup of passwords for reserved users elast
You will be prompted to enter passwords as the process pro
Please confirm that you would like to continue [y/N]y
```

```

Enter password for [elastic]:
Reenter password for [elastic]:
Enter password for [apm_system]:
Reenter password for [apm_system]:
Enter password for [kibana_system]:
Reenter password for [kibana_system]:
Enter password for [logstash_system]:
Reenter password for [logstash_system]:
Enter password for [beats_system]:
Reenter password for [beats_system]:
Enter password for [remote_monitoring_user]:
Reenter password for [remote_monitoring_user]:
Changed password for user [apm_system]
Changed password for user [kibana_system]
Changed password for user [kibana]
Changed password for user [logstash_system]
Changed password for user [beats_system]
Changed password for user [remote_monitoring_user]
Changed password for user [elastic]

```

2. Elasticsearch API 호출 시 인증 필요:

```

bash
# 해당 Elasticsearch 클러스터의 기본 상태와 정보를 요약해서 확인
curl -XGET "http://<노드_IP>:9200" -u elastic
인증 정보를 요청받으면 사용자명과 비밀번호 입력.

```

- 비밀번호 입력 후 결과를 확인.

```

Enter host password for user 'elastic':
{
  "name" : "node-1",
  "cluster_name" : "elastic-cluster",
  "cluster_uuid" : "Ti0zl7YySgikPHSAzuTl3w",
  "version" : {
    "number" : "7.10.2",

```

```

    "build_flavor" : "default",
    "build_type" : "tar",
    "build_hash" : "747e1cc71def077253878a59143c1f785afa92",
    "build_date" : "2021-01-13T00:42:12.435326Z",
    "build_snapshot" : false,
    "lucene_version" : "8.7.0",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}

```

```

# 모든 elastic 노드의 상태를 조회
curl -XGET "http://<노드_IP>:9200/_cat/nodes -elastic

```

```

Enter host password for user 'elastic':
172.31.44.111 30 51 -1 0.00 0.02 0.00 cdhilmrstw * node-1
172.31.44.216 42 71 -1 0.00 0.02 0.00 cdhilmrstw - node-3
172.31.43.128 31 53 -1 0.00 0.01 0.00 cdhilmrstw - node-2

```

8. 문제 해결

1. `keystore password was incorrect` 오류
 - Keystore 비밀번호가 일치하지 않는 경우 발생.
 - Keystore에 저장된 비밀번호를 확인하고, 필요시 재설정.
 - `bin/elasticsearch-keystore` 명령어로 수정 가능.
2. `missing authentication credentials` 오류
 - API 호출 시 인증 정보가 누락된 경우.
 - `u <사용자명>` 옵션을 사용하여 비밀번호와 함께 요청.

정리

1. `./bin/elasticsearch-certutil` 명령으로 인증서를 생성.
2. 인증서를 각 노드에 배포하고 설정 파일(`elasticsearch.yml`)을 수정.

3. Keystore를 생성하고 비밀번호를 등록.
4. Elasticsearch를 재시작한 뒤, API 호출 시 인증 정보를 제공.