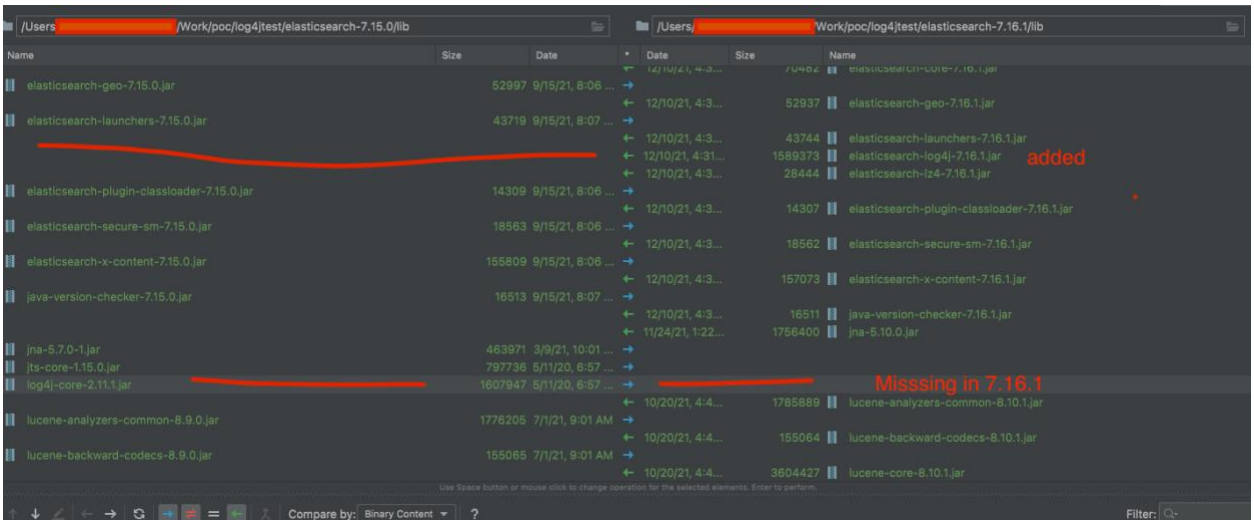
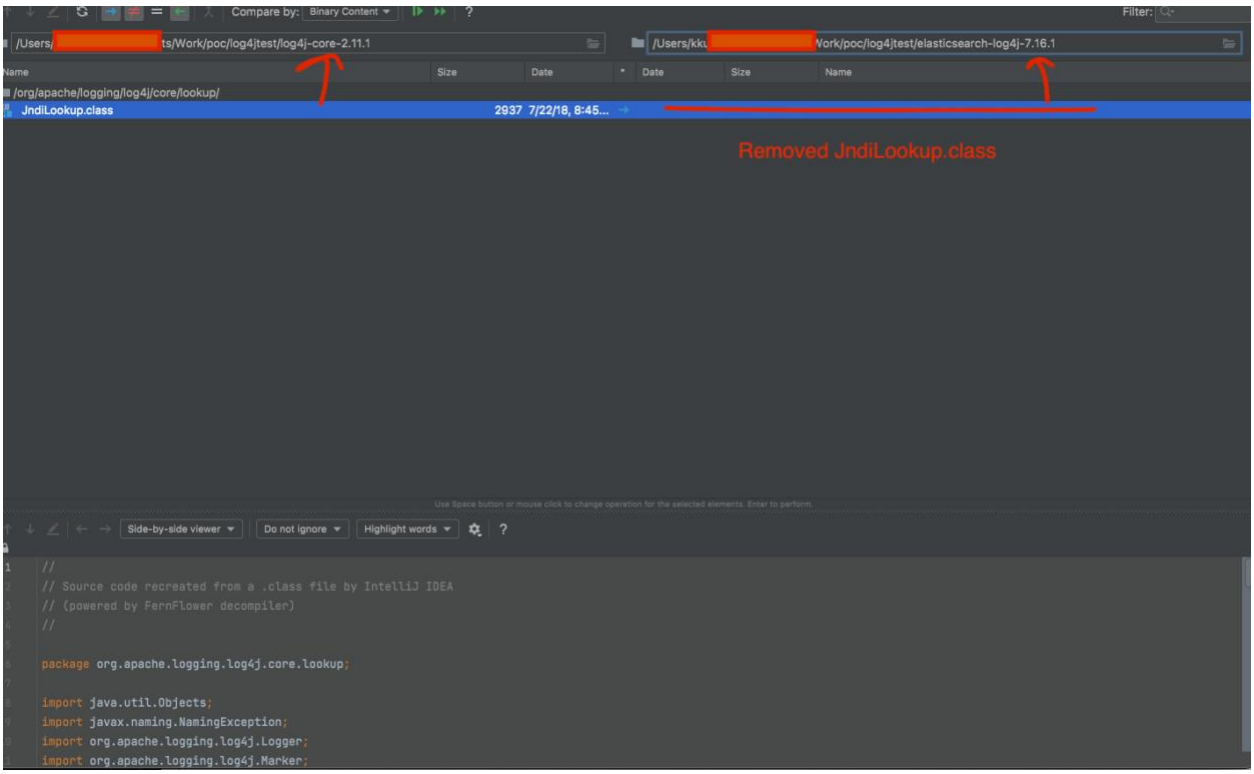
Resolve log4j JNDI lookup in Elastic Search 7.11.0:

What ES release elasticsearch-7.16.1 did to solve the log4j JNDI lookup problem:

1: Removed the original log4j-core-2.11.1.jar
2: Added elasticsearch- log4j-7.16.1.jar → which is actually log4j-core-2.11.1.jar MINUS JndiLookup.class (as shown in second screenshot)





We tested this and it is working so far:

ES Version:


```
"version" : {
    "number" : "7.11.0",
    "build_flavor" : "default",
    "build_type" : "rpm",
    "build_hash" : "8ced7813d6f16d2ef30792e2fcde3e755795ee04",
    "build_date" : "2021-02-08T22:44:01.320463Z",
    "build_snapshot" : false,
    "lucene_version" : "8.7.0",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  }
```


Solution:

1: Stop the es node

2: Replace

2.1: elasticsearch/lib/ log4j-api-2.11.1.jar
2.2: elasticsearch/lib/log4j-core-2.11.1.jar

with

2.3: elasticsearch/lib/log4j-api-2.16.0.jar
2.4: elasticsearch/lib/log4j-core-2.16.0.jar

3: set file permissions

chmod o+r elasticsearch/lib/log4j-*

Restart the Elasticsearch.

This seems a better solution than upgrading to ES 7.16.1, as this is going to address the second log4j vulnerability CVE-2021-45046 in addition to the original CVE-2021-44228 aka Log4Shell