[사전준비]

•CentOS 7 64 bit with 4GB of RAM - elk-master

•CentOS 7 64 bit with 1 GB of RAM - client1

•Ubuntu 16 64 bit with 1GB of RAM - client2

* setenforce 0
* systemctl status firewalld.service

[자바설치]

* wget --no-cookies --no-check-certificate --header "Cookie: gpw\_e24=http:%2F%2Fwww.oracle.com%2F; oraclelicense=accept-securebackup-cookie" <http://download.oracle.com/otn-pub/java/jdk/8u77-b02/jdk-8u77-linux-x64.rpm>
* rpm -ivh jdk-8u77-linux-x64.rpm
* java –version

[Elasticsearch설치]

* rpm --import <https://artifacts.elastic.co/GPG-KEY-elasticsearch>
* wget <https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-5.1.1.rpm>
* rpm -ivh elasticsearch-5.1.1.rpm
* cd /etc/elasticsearch/
* vi elasticsearch.yml

bootstrap.memory\_lock: true

network.host: localhost  
http.port: 9200

* vi /usr/lib/systemd/system/elasticsearch.service

LimitMEMLOCK=infinity

* vi /etc/sysconfig/elasticsearch

MAX\_LOCKED\_MEMORY=unlimited

* sudo systemctl daemon-reload
* sudo systemctl enable elasticsearch
* sudo systemctl start elasticsearch
* curl -XGET 'localhost:9200/\_nodes?filter\_path=\*\*.mlockall&pretty'
* curl -XGET 'localhost:9200/?pretty'

|  |  |
| --- | --- |
| Elastic Search | RDB |
| Index | Database |
| Document\_Type | Table |
| Document | Row |
| Filed | Column |
| Mapping | Schema |

|  |  |
| --- | --- |
| Elastic Search | RDB |
| GET  curl –XGET localhost:9200/classes/class/1 | Select  Select \* from class where id =1 |
| PUT  curl –XPUT localhost:9200/classes/class/1 –d ‘{xxx}’ | Update  Update class set xxx where id=1 |
| POST  curl –XPOST localhost:9200/classes/class/1 –d ‘{xxx}’ | Insert  Insert into class values {xxx} |
| DELETE  curl –XDELETE localhost:9200/classes/class/1 | Delete  delete from class where id =1 |

* curl -XPUT http://localhost:9200/classes
* {"acknowledged":true,"shards\_acknowledged":true}
* curl -XPUT http://localhost:9200/classes
* {"acknowledged":true,"shards\_acknowledged":true}[root@q-nimi-os02 systemd]# curl -XGET http://localhost:9200/classes?pretty
* {
* "classes" : {
* "aliases" : { },
* "mappings" : { },
* "settings" : {
* "index" : {
* "creation\_date" : "1504420626707",
* "number\_of\_shards" : "5",
* "number\_of\_replicas" : "1",
* "uuid" : "qOAffW71TNKZzHEPkvbiLg",
* "version" : {
* "created" : "5010199"
* },
* "provided\_name" : "classes"
* }
* }
* }
* }
* curl -XDELETE http://localhost:9200/classes
* {"acknowledged":true}
* [root@q-nimi-os02 ~]# curl -XGET http://localhost:9200/classes?pretty
* {
* "error" : {
* "root\_cause" : [
* {
* "type" : "index\_not\_found\_exception",
* "reason" : "no such index",
* "resource.type" : "index\_or\_alias",
* "resource.id" : "classes",
* "index\_uuid" : "\_na\_",
* "index" : "classes"
* }
* ],
* "type" : "index\_not\_found\_exception",
* "reason" : "no such index",
* "resource.type" : "index\_or\_alias",
* "resource.id" : "classes",
* "index\_uuid" : "\_na\_",
* "index" : "classes"
* },
* "status" : 404
* }
* curl -XPOST http://localhost:9200/classes/class/1 -d '{"title":"compute","professor":"cho"}'
* {"\_index":"classes","\_type":"class","\_id":"1","\_version":1,"result":"created","\_shards":{"total":2,"successful":1,"failed":0},"created"
* [root@q-nimi-os02 ~]# curl -XGET http://localhost:9200/classes/class/1?pretty
* {
* "\_index" : "classes",
* "\_type" : "class",
* "\_id" : "1",
* "\_version" : 1,
* "found" : true,
* "\_source" : {
* "title" : "compute",
* "professor" : "cho"
* }
* }
* curl -XPOST http://localhost:9200/classes/class/1 -d @oneclass.json 🡪oneclass.json생성후
* {"\_index":"classes","\_type":"class","\_id":"1","\_version":2,"result":"updated","\_shards":{"total":2,"successful":1,"failed":0},"created":false}
* curl -XGET http://localhost:9200/classes/class/1?pretty
* {
* "\_index" : "classes",
* "\_type" : "class",
* "\_id" : "1",
* "\_version" : 2,
* "found" : true,
* "\_source" : {
* "title" : "Machine Learning",
* "Professor" : "Minsuk Heo",
* "major" : "Computer Science",
* "semester" : [
* "spring",
* "fall"
* ],
* "student\_count" : 100,
* "unit" : 3,
* "rating" : 5
* }
* }
* curl -XPOST http://localhost:9200/classes/class/1/\_update -d '{"doc":{"unit":1}}'
* {"\_index":"classes","\_type":"class","\_id":"1","\_version":5,"result":"updated","\_shards":{"total":2,"successful":1,"failed":0}}
* curl -XGET http://localhost:9200/classes/class/1?pretty
* {
* "\_index" : "classes",
* "\_type" : "class",
* "\_id" : "1",
* "\_version" : 5,
* "found" : true,
* "\_source" : {
* "title" : "compute",
* "professor" : "cho",
* "unit" : 1
* }
* }
* curl -XPOST http://localhost:9200/classes/class/1/\_update -d '{"doc":{"unit":2}}'
* curl -XGET http://localhost:9200/classes/class/1?pretty
* {
* "\_index" : "classes",
* "\_type" : "class",
* "\_id" : "1",
* "\_version" : 5,
* "found" : true,
* "\_source" : {
* "title" : "compute",
* "professor" : "cho",
* "unit" : 2
* }
* }
* [root@q-nimi-os02 ~]# curl -XPOST http://localhost:9200/classes/class/1/\_update?pretty -d '{"script":"ctx.\_source.unit += 5"}'
* {
* "\_index" : "classes",
* "\_type" : "class",
* "\_id" : "1",
* "\_version" : 8,
* "result" : "updated",
* "\_shards" : {
* "total" : 2,
* "successful" : 1,
* "failed" : 0
* }
* }
* [root@q-nimi-os02 ~]# curl -XGET http://localhost:9200/classes/class/1/?pretty
* {
* "\_index" : "classes",
* "\_type" : "class",
* "\_id" : "1",
* "\_version" : 8,
* "found" : true,
* "\_source" : {
* "title" : "compute",
* "professor" : "cho",
* "unit" : 8
* }
* }
* [root@q-nimi-os02 ~]# curl -XPOST http://localhost:9200/\_bulk?pretty --data-binary @classes.json
* {
* "took" : 137,
* "errors" : false,
* "items" : [
* {
* "index" : {
* "\_index" : "classes",
* "\_type" : "class",
* "\_id" : "1",
* "\_version" : 1,
* "result" : "created",
* "\_shards" : {
* "total" : 2,
* "successful" : 1,
* "failed" : 0
* },
* "created" : true,
* "status" : 201
* }
* },
* {
* [root@q-nimi-os02 ~]# curl -XPUT http://localhost:9200/classes/?pretty
* {
* "acknowledged" : true,
* "shards\_acknowledged" : true
* }
* [root@q-nimi-os02 ~]# curl -XGET http://localhost:9200/classes/?pretty
* {
* "classes" : {
* "aliases" : { },
* "mappings" : { },
* "settings" : {
* "index" : {
* "creation\_date" : "1504424550988",
* "number\_of\_shards" : "5",
* "number\_of\_replicas" : "1",
* "uuid" : "8MkgEq2FR7KofMvAsaWnDw",
* "version" : {
* "created" : "5010199"
* },
* "provided\_name" : "classes"
* }
* }
* }
* }
* [root@q-nimi-os02 ~]# curl -XPUT 'http://localhost:9200/classes/class/\_mapping' -d @mapping.json
* {"acknowledged":true}
* [root@q-nimi-os02 ~]# curl -XGET http://localhost:9200/classes/?pretty
* {
* "classes" : {
* "aliases" : { },
* "mappings" : {
* "class" : {
* "properties" : {
* "major" : {
* "type" : "text"
* },
* "professor" : {
* "type" : "text"
* },
* "rating" : {
* "type" : "integer"
* },
* "school\_location" : {
* "type" : "geo\_point"
* },
* "semester" : {
* "type" : "text"
* },
* "student\_count" : {
* "type" : "integer"
* },
* "submit\_date" : {
* "type" : "date",
* "format" : "yyyy-MM-dd"
* },
* "title" : {
* "type" : "text"
* },
* "unit" : {
* "type" : "integer"
* }
* }
* }
* },
* "settings" : {
* "index" : {
* "creation\_date" : "1504424550988",
* "number\_of\_shards" : "5",
* "number\_of\_replicas" : "1",
* "uuid" : "8MkgEq2FR7KofMvAsaWnDw",
* "version" : {
* "created" : "5010199"
* },
* "provided\_name" : "classes"
* }
* }
* }
* }
* curl -XPOST http://localhost:9200/\_bulk?pretty --data-binary @classes.json
* curl -XPOST 'http://localhost:9200/\_bulk' --data-binary @basketball.json
* {"took":348,"errors":false,"items":[{"index":{"\_index":"basketball","\_type":"record","\_id":"1","\_version":1,"resu lt":"created","\_shards":{"total":2,"successful":1,"failed":0},"created":true,"status":201}},{"index":{"\_index":"b asketball","\_type":"record","\_id":"2","\_version":1,"result":"created","\_shards":{"total":2,"successful":1,"failed ":0},"created":true,"status":201}}]}
* curl -XGET http://localhost:9200/basketball/record/\_search?pretty
* {
* "took" : 10,
* "timed\_out" : false,
* "\_shards" : {
* "total" : 5,
* "successful" : 5,
* "failed" : 0
* },
* "hits" : {
* "total" : 2,
* "max\_score" : 1.0,
* "hits" : [
* {
* "\_index" : "basketball",
* "\_type" : "record",
* "\_id" : "2",
* "\_score" : 1.0,
* "\_source" : {
* "team" : "Chicago Bulls",
* "name" : "Michael Jordan",
* "points" : 20,
* "rebounds" : 5,
* "assists" : 8,
* "submit\_date" : "1996-10-11"
* }
* },
* {
* "\_index" : "basketball",
* "\_type" : "record",
* "\_id" : "1",
* "\_score" : 1.0,
* "\_source" : {
* "team" : "Chicago Bulls",
* "name" : "Michael Jordan",
* "points" : 30,
* "rebounds" : 3,
* "assists" : 4,
* "submit\_date" : "1996-10-11"
* }
* }
* ]
* }
* }
* curl -XGET 'http://localhost:9200/basketball/record/\_search?q=points:30&pretty'
* {
* "took" : 7,
* "timed\_out" : false,
* "\_shards" : {
* "total" : 5,
* "successful" : 5,
* "failed" : 0
* },
* "hits" : {
* "total" : 1,
* "max\_score" : 1.0,
* "hits" : [
* {
* "\_index" : "basketball",
* "\_type" : "record",
* "\_id" : "1",
* "\_score" : 1.0,
* "\_source" : {
* "team" : "Chicago Bulls",
* "name" : "Michael Jordan",
* "points" : 30,
* "rebounds" : 3,
* "assists" : 4,
* "submit\_date" : "1996-10-11"
* }
* }
* ]
* }
* }
* curl -XGET http://localhost:9200/\_search?pretty --data-binary @avg\_points\_aggs.json
* {
* "took" : 22,
* "timed\_out" : false,
* "\_shards" : {
* "total" : 11,
* "successful" : 11,
* "failed" : 0
* },
* "hits" : {
* "total" : 27,
* "max\_score" : 0.0,
* "hits" : [ ]
* },
* "aggregations" : {
* "avg\_score" : {
* "value" : 25.0
* }
* }
* }
* curl -XGET http://localhost:9200/\_search?pretty --data-binary @min\_points\_aggs.json
* {
* "took" : 15,
* "timed\_out" : false,
* "\_shards" : {
* "total" : 11,
* "successful" : 11,
* "failed" : 0
* },
* "hits" : {
* "total" : 27,
* "max\_score" : 0.0,
* "hits" : [ ]
* },
* "aggregations" : {
* "min\_score" : {
* "value" : 20.0
* }
* }
* }
* curl -XGET http://localhost:9200/\_search?pretty --data-binary @max\_points\_aggs.json
* {
* "took" : 6,
* "timed\_out" : false,
* "\_shards" : {
* "total" : 11,
* "successful" : 11,
* "failed" : 0
* },
* "hits" : {
* "total" : 27,
* "max\_score" : 0.0,
* "hits" : [ ]
* },
* "aggregations" : {
* "max\_score" : {
* "value" : 30.0
* }
* }
* }
* curl -XGET http://localhost:9200/\_search?pretty --data-binary @sum\_points\_aggs.json
* {
* "took" : 4,
* "timed\_out" : false,
* "\_shards" : {
* "total" : 11,
* "successful" : 11,
* "failed" : 0
* },
* "hits" : {
* "total" : 27,
* "max\_score" : 0.0,
* "hits" : [ ]
* },
* "aggregations" : {
* "sum\_score" : {
* "value" : 50.0
* }
* }
* }
* curl -XGET http://localhost:9200/\_search?pretty --data-binary @stats\_points\_aggs.json
* {
* "took" : 3,
* "timed\_out" : false,
* "\_shards" : {
* "total" : 11,
* "successful" : 11,
* "failed" : 0
* },
* "hits" : {
* "total" : 27,
* "max\_score" : 0.0,
* "hits" : [ ]
* },
* "aggregations" : {
* "stats\_score" : {
* "count" : 2,
* "min" : 20.0,
* "max" : 30.0,
* "avg" : 25.0,
* "sum" : 50.0
* }
* }
* curl -XPOST 'localhost:9200/basketball/record\_mapping' -d @basketball\_mapping.json

{"\_index":"basketball","\_type":"record\_mapping","\_id":"AV5G6CEA216dEIH7i9R\_","\_version":1,"result":"created","\_shards":{"total":2,"successful":1,"failed":0},"created":true}

* curl -XPOST 'localhost:9200/\_bulk' --data-binary @twoteam\_basketball.json
* {"took":67,"errors":false,"items":[{"index":{"\_index":"basketball","\_type":"record","\_id":"1","\_version":1,"result":"created","\_shards":{"total":2,"successful":1,"failed":0},"created":true,"status":201}},{"index":{"\_index":"basketball","\_type":"record","\_id":"2","\_version":1,"result":"created","\_shards":{"total":2,"successful":1,"failed":0},"created":true,"status":201}},{"index":{"\_index":"basketball","\_type":"record","\_id":"3","\_version":1,"result":"created","\_shards":{"total":2,"successful":1,"failed":0},"created":true,"status":201}},{"index":{"\_index":"basketball","\_type":"record","\_id":"4","\_version":1,"result":"created","\_shards":{"total":2,"successful":1,"failed":0},"created":true,"status":201}}]}
* curl -XGET localhost:9200/\_search?pretty --data-binary @terms\_aggs.json 🡪팀별 grouping
* curl -XGET localhost:9200/\_search?pretty --data-binary @stats\_by\_team.json 🡪팀에서 스코어별로 다시 grouping

[elasticsearch x-pack설치]

[root@q-nimi-os02 filebeat]# cd /usr/share/elasticsearch/bin/

[root@q-nimi-os02 elasticsearch]# bin/elasticsearch-plugin install x-pack

-> Downloading x-pack from elastic

[=================================================] 100%

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

@ WARNING: plugin requires additional permissions @

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

\* java.lang.RuntimePermission accessClassInPackage.com.sun.activation.registries

\* java.lang.RuntimePermission getClassLoader

\* java.lang.RuntimePermission setContextClassLoader

\* java.lang.RuntimePermission setFactory

\* java.security.SecurityPermission createPolicy.JavaPolicy

\* java.security.SecurityPermission getPolicy

\* java.security.SecurityPermission putProviderProperty.BC

\* java.security.SecurityPermission setPolicy

\* java.util.PropertyPermission \* read,write

\* java.util.PropertyPermission sun.nio.ch.bugLevel write

\* javax.net.ssl.SSLPermission setHostnameVerifier

See http://docs.oracle.com/javase/8/docs/technotes/guides/security/permissions.html

for descriptions of what these permissions allow and the associated risks.

Continue with installation? [y/N]y

-> Installed x-pack

[kibana x-pack설치]

[root@q-nimi-os02 share]# cd kibana/

[root@q-nimi-os02 kibana]# bin/kibana-plugin install x-pack

Attempting to transfer from x-pack

Attempting to transfer from https://artifacts.elastic.co/downloads/kibana-plugins/x-pack/x-pack-5.1.1.zip

Transferring 107852891 bytes....................

Transfer complete

Retrieving metadata from plugin archive

Extracting plugin archive

Extraction complete

Optimizing and caching browser bundles...

Plugin installation complete

* kibana x-pack 설치후 사용자 `elastic`과 비밀번호 `changeme’로 로그인

[logstash x-pack설치]

[root@q-nimi-os02 share]# cd logstash/

[root@q-nimi-os02 logstash]# bin/logstash-plugin install x-pack

Validating x-pack

x-pack is not a Logstash plugin

ERROR: Installation aborted, verification failed for x-pack