Elastic Search setting 5.0

write by : shkim

Date : 2017-04-25

**SERVER setting**

1. **NTP(Network Time Protocol) install**

# 시간을 정확하게 유지시키기 위한 통신망 규약

yum –y install ntp

/etc/init.d/ntpd restart

chkconfig ntpd on

ntpq -p

1. **SELINUX 해제 (Security-Enhanced Linux)**

# .Linux의 보안 강화번으로서 리눅스 커널에 의무 접근 제어를 구현함

sed -i 's/SELINUX=enforcing/SELINUX=disabled/g' /etc/selinux/config

1. **iptables 방화벽 설정 조절**

# 현재는 테스트여서 off로 진행하나 client와 연결되므로 후에 적용해서 돌려봐야 할 듯

# ES shield plugin을 붙이면 접근성이 제한 가능하나 후에 서버 자체에 대한 접근 제어를 위# 해 주차해야 한다.

/etc/init.d/iptables stop

chkconfig iptables off

# centOS7 일경우는 firewalld

systemctl stop firewalld

systemctl disable firewalld

1. **User Add**

useradd irteam

passwd irteam

1. **sudoers add**

echo ‘irteam All=(All) NOPASSWD: ALL’ >> /etc/sudoers

1. **open files config**

# 65536로 적용해도 적다는 메시지가 나온다. 어느 부분에서 문제되는지 확인해 봐야함

# 5.0은 65536 이상을 명시해주지 않으면 실행이 안된다.

vi /etc/security/limits.conf

#맨 밑에 추가

irteam hard nofile 65536

irteam soft nofile 65536

1. **Thread config**

#default 1024 but elastic default 2048

vi /etc/security/limits.conf

irteam soft nproc 2048

irteam hard nproc 2048

1. **sysctl vm.max set**

# 5.0 에서 베이직으로 세팅되어져야 된다 부가 정보는 찾아보고 입력

sysctl -w vm.max\_map\_count=262144

echo 262144 > /proc/sys/vm/max\_map\_count

vi /etc/sysctl.conf

#vm\_memory\_config

vm.max\_map\_count = 262144

1. **system configuration**

EL7 use system

vi /etc/system/system/elasticsearch.service.d/elasticsearch.conf

LimitMEMLOCK=infinity

EL6 use limits.conf

vi /etc/security/limits.conf

irteam hard memlock unlimited

irteam soft memlock unlimited

1. **Setting elasticsearch & kibana**

* **ELASTICSEARCH.yml**

# ======================== Elasticsearch Configuration =========================

#

# NOTE: Elasticsearch comes with reasonable defaults for most settings.

# Before you set out to tweak and tune the configuration, make sure you

# understand what are you trying to accomplish and the consequences.

#

# The primary way of configuring a node is via this file. This template lists

# the most important settings you may want to configure for a production cluster.

#

# Please see the documentation for further information on configuration options:

# <http://www.elastic.co/guide/en/elasticsearch/reference/current/setup-configuration.html>

#

# ---------------------------------- Cluster -----------------------------------

#

# Use a descriptive name for your cluster:

#

cluster.name: jin\_cluster

#

# ------------------------------------ Node ------------------------------------

#

# Use a descriptive name for the node:

#

# 이부분은 node의 세팅이다. master / client / data / ingest로 나눈다.

# master node는 전체 클러스터의 상태에 대한 정보 관리

# client node는 외부에서의 요청을 받아들이는 node ( load balancer)

# data node 는 단순 저장업무 & 간단한 쓰레드처리

# ingest는 아직 확실히 정리가 안되었습니다.

# master & data & ingest를 전부 false로 해두어야 client 노드로 인식

# client노드는 http설정을 enabled로 해준다.

# 나머지 노드를 사용하려면 각각의 노드만 true http는 false로 설정

node.name: node-5

node.master: false

node.data: false

node.ingest: false

http.enabled: true

#

# Add custom attributes to the node:

#

#node.attr.rack: r1

#

# ----------------------------------- Paths ------------------------------------

#

# Path to directory where to store the data (separate multiple locations by comma):

#

# 사용하려면 디렉토리 미리 생성

path.data: /opt/elastic/search/data

#

# Path to log files:

#

path.logs: /opt/elastic/search/logs

#

# ----------------------------------- Memory -----------------------------------

#

# Lock the memory on startup:

#

bootstrap.memory\_lock: true

#

# Make sure that the heap size is set to about half the memory available

# on the system and that the owner of the process is allowed to use this

# limit.

#

# Elasticsearch performs poorly when the system is swapping the memory.

#

# ---------------------------------- Network -----------------------------------

#

# Set the bind address to a specific IP (IPv4 or IPv6):

#

network.host: 192.168.0.158

transport.tcp.port: 9300

#

# Set a custom port for HTTP:

#

http.port: 9200

#

# For more information, see the documentation at:

# <http://www.elastic.co/guide/en/elasticsearch/reference/current/modules-network.html>

#

# --------------------------------- Discovery ----------------------------------

#

# Pass an initial list of hosts to perform discovery when new node is started:

# The default list of hosts is ["127.0.0.1", "[::1]"]

#

discovery.zen.ping.unicast.hosts: ["192.168.0.154:9300", "192.168.0.155:9300", "192.168.0.156:9300", "192.168.0.157:9300", "192.168.0.158:9300"]

#

# Prevent the "split brain" by configuring the majority of nodes (total number of nodes / 2 + 1):

#

# 이 부분 중요 위에 공식 적용. 싱글 노드로 전부 구성할 땐 무조건 0 설정 해 주어야함.

discovery.zen.minimum\_master\_nodes: 1

#

# For more information, see the documentation at:

# <http://www.elastic.co/guide/en/elasticsearch/reference/current/modules-discovery.html>

#

# ---------------------------------- Gateway -----------------------------------

#

# Block initial recovery after a full cluster restart until N nodes are started:

#

#gateway.recover\_after\_nodes: 3

#

# For more information, see the documentation at:

# <http://www.elastic.co/guide/en/elasticsearch/reference/current/modules-gateway.html>

#

# ---------------------------------- Various -----------------------------------

#

# Disable starting multiple nodes on a single system:

#

#node.max\_local\_storage\_nodes: 1

#

# Require explicit names when deleting indices:

#

#action.destructive\_requires\_name: true

* **kibana.yml**

# Kibana is served by a back end server. This setting specifies the port to use.

server.port: 5601

# Specifies the address to which the Kibana server will bind. IP addresses and host names are both valid values.

# The default is 'localhost', which usually means remote machines will not be able to connect.

# To allow connections from remote users, set this parameter to a non-loopback address.

server.host: "192.168.0.158"

# Enables you to specify a path to mount Kibana at if you are running behind a proxy. This only affects

# the URLs generated by Kibana, your proxy is expected to remove the basePath value before forwarding requests

# to Kibana. This setting cannot end in a slash.

#server.basePath: ""

# The maximum payload size in bytes for incoming server requests.

#server.maxPayloadBytes: 1048576

# The Kibana server's name. This is used for display purposes.

#server.name: "your-hostname"

# The URL of the Elasticsearch instance to use for all your queries.

elasticsearch.url: "http://192.168.0.158:9200"

# When this setting’s value is true Kibana uses the hostname specified in the server.host

# setting. When the value of this setting is false, Kibana uses the hostname of the host

# that connects to this Kibana instance.

#elasticsearch.preserveHost: true

# Kibana uses an index in Elasticsearch to store saved searches, visualizations and

# dashboards. Kibana creates a new index if the index doesn’t already exist.

#kibana.index: ".kibana"

# The default application to load.

#kibana.defaultAppId: "discover"

# If your Elasticsearch is protected with basic authentication, these settings provide

# the username and password that the Kibana server uses to perform maintenance on the Kibana

# index at startup. Your Kibana users still need to authenticate with Elasticsearch, which

# is proxied through the Kibana server.

#elasticsearch.username: "user"

#elasticsearch.password: "pass"

# Paths to the PEM-format SSL certificate and SSL key files, respectively. These

# files enable SSL for outgoing requests from the Kibana server to the browser.

#server.ssl.cert: /path/to/your/server.crt

#server.ssl.key: /path/to/your/server.key

# Optional settings that provide the paths to the PEM-format SSL certificate and key files.

# These files validate that your Elasticsearch backend uses the same key files.

#elasticsearch.ssl.cert: /path/to/your/client.crt

#elasticsearch.ssl.key: /path/to/your/client.key

# Optional setting that enables you to specify a path to the PEM file for the certificate

# authority for your Elasticsearch instance.

#elasticsearch.ssl.ca: /path/to/your/CA.pem

# To disregard the validity of SSL certificates, change this setting’s value to false.

#elasticsearch.ssl.verify: true

# Time in milliseconds to wait for Elasticsearch to respond to pings. Defaults to the value of

# the elasticsearch.requestTimeout setting.

#elasticsearch.pingTimeout: 1500

# Time in milliseconds to wait for responses from the back end or Elasticsearch. This value

# must be a positive integer.

#elasticsearch.requestTimeout: 30000

# List of Kibana client-side headers to send to Elasticsearch. To send \*no\* client-side

# headers, set this value to [] (an empty list).

#elasticsearch.requestHeadersWhitelist: [ authorization ]

# Header names and values that are sent to Elasticsearch. Any custom headers cannot be overwritten

# by client-side headers, regardless of the elasticsearch.requestHeadersWhitelist configuration.

#elasticsearch.customHeaders: {}

# Time in milliseconds for Elasticsearch to wait for responses from shards. Set to 0 to disable.

#elasticsearch.shardTimeout: 0

# Time in milliseconds to wait for Elasticsearch at Kibana startup before retrying.

#elasticsearch.startupTimeout: 5000

# Specifies the path where Kibana creates the process ID file.

pid.file: /opt/elastic/kibana/kibana.pid

# Enables you specify a file where Kibana stores log output.

#logging.dest: stdout

# Set the value of this setting to true to suppress all logging output.

#logging.silent: false

# Set the value of this setting to true to suppress all logging output other than error messages.

#logging.quiet: false

# Set the value of this setting to true to log all events, including system usage information

# and all requests.

#logging.verbose: false

# Set the interval in milliseconds to sample system and process performance

# metrics. Minimum is 100ms. Defaults to 5000.

#ops.interval: 5000