Shield

SSH ไปที่ Elasticsearch 1
ip: 52.74.104.59
port: 9200
key: TMN-Log-Monitoring-key-pair

You have Java™ 7 or above installed.
You have downloaded elasticsearch 1.5.0+ and extracted it

การติดตั้ง Shield

1. cd ไปที่ลง elasticsearch ไว้
2. ติดตั้ง license plugin โดยใช้คำสั่ง
   bin/plugin -i elasticsearch/license/latest
3. ติดตั้ง shield plugin โดยใช้คำสั่ง
   bin/plugin -i elasticsearch/shield/latest
4. Start Elasticsearch โดยใช้คำสั่ง (กรณีไม่ได้เป็น service)
   bin/elasticsearch
   ถ้าเป็น service ใช้คำสั่ง
   service elasticsearch restart

ดูเพิ่มเติมที่
https://www.elastic.co/guide/en/shield/current/installing-shield.html

---

Add User

1. cd ไปที่ **usr/share/elasticsearch/**
   ถ้าจะ Enable Message authentication ใช้คำสั่ง

bin/shield/syskeygen

2. จากนั้นใช้คำสั่ง **./bin/shield/esusers useradd** เพื่อเพิ่ม user

ตัวอย่าง เช่น

./bin/shield/esusers useradd admin -p adminqwe -r admin

#หลัง useradd คือชื่อ user ในที่นี้คือ admin

หลัง -p คือ password ในที่นี้คือ adminqwe ถ้าไม่ใส่ shield จะขึ้นมาให้ใส่เอง

(the tool will prompt you to enter and confirm a password in interactive mode.)

หลัง-r Role ที่กำหนดให้ ในที่นี้คือ admin

**สามารถดู role ที่ shield กำหนดให้แล้ว ได้ที่

etc/elasticsearch/shield/roles.yml

3. ใช้คำสั่ง **bin/shield/esusers list** เพื่อดู role ของ user ทั้งหมด

ตัวอย่าง เช่น rdeniro : admin

alpacino : power_user

jacknich : marvel,logstash

ถ้าใช้ bin/shield/esusers list <ชื่อuser> จะแสดงแค่ role ของ user นั้น

ตัวอย่าง เช่น esusers list jacknich จะแสดง

jacknich : marvel,logstash

Edit User

1. ถ้าจะเปลี่ยน Password ใช้คำสั่ง

bin/shield/esusers passwd <username> -p <password>

หลัง passwd จะเป็นชื่อ user
หลัง -p จะเป็น password ใหม่ที่ต้องการ ถ้าไม่ใส่ -p shield จะขึ้นมาให้ใส่เอง
(the tool will prompt you to enter and confirm a password in interactive mode.)

2. ถ้าจะ assign role ให้ user ใช้คำสั่ง

bin/shield/esusers roles <username> -a <commma-separate list of roles>
-r <commma-separate list of roles>

ตัวอย่าง เช่น

bin/shield/esusers roles jacknich -r logstash,marvel -a user

หลัง roles คือ ชื่อ user

หลัง -r คือ role ที่เราจะลบออกจาก user นี้

หลัง -a คือ role ที่เราเพิ่มเข้าไป

ถ้าใช้ esusers list jacknich จะเป็น

jacknich : user

Delete User

bin/shield/esusers userdel <username>

ตัวอย่าง เช่น bin/shield/esusers userdel jacknich

ใช้คำสั่ง **bin/shield/esusers list**

user jacknich จะหายไป

ดูเพิ่มเติมที่

https://www.elastic.co/guide/en/shield/current/_managing_users_in_an_esusers_realm.html

---

Defining Role

เปิดไฟล์ roles.yml ในเครื่อง elasticsearch ตัวอย่าง

```
# All cluster rights
# All operations on all indices
admin:
  cluster: all
  indices:
    '*': all

# Monitoring cluster privileges
# All operations on all indices
power_user:
  cluster: monitor
  indices:
    '*': all
```

```
# Only read operations on indices
user:
  indices:
    '*': read

# Only read operations on indices named events_*
events_user:
  indices:
    'events_*': read
```

ดูเพิ่มเติมที่

https://www.elastic.co/guide/en/shield/current/defining-roles.html

และ

https://www.elastic.co/guide/en/shield/current/mapping-roles.html

***ใน indices '*' คือทุก indices

คำสั่ง ในการกำหนด role

privilege

Cluster

all	All cluster administration operations, like snapshotting, node shutdown/restart, settings update or rerouting
monitor	All cluster read-ony operations, like cluster health & state, hot threads, node info, node & cluster stats, snapshot/restore status, pending cluster tasks
manage_shield	All Shield related operations (currently only exposing an API for clearing the realm caches)

Indices

all	Any action on an index
manage	All monitor privileges plus index administration (aliases, analyze, cache clear, close, delete, exists, flush, mapping, open, optimize, refresh, settings, search shards, templates, validate, warmers) monitor": All actions, that are required for monitoring and read-only (recovery, segments info, index stats & status)
data_access	A shortcut of all of the below privileges

crud	A shortcut of read and write privileges
read	Read only access to actions (count, explain, get, exists, mget, get indexed scripts, more like this, multi percolate/search/termvector), percolate, scroll, clear_scroll, search, suggest, tv)
search	All of suggest and executing an arbitrary search request (including multi-search API)
get	Allow to execute a GET request for a single document or multiple documents via the multi-get API
suggest	Allow to execute the _suggest API
index	Privilege to index and update documents
create_index	Privilege to create an index. A create index request may contain aliases to be added to the index once created. In that case the request requires manage_aliasesprivilege as well, on both the index and the aliases names.

manage_aliases	Privilege to add and remove aliases, as well as retrieve aliases information. Note that in order to add an alias to an existing index, the manage_aliases privilege is required on the existing index as well as on the alias name
delete	Privilege to delete documents (includes delete by query)
write	Privilege to index, update, delete, delete by query and bulk operations on documents, in addition to delete and put indexed scripts

Cluster Action privileges

- cluster:admin/nodes/restart
- cluster:admin/nodes/shutdown
- cluster:admin/repository/delete
- cluster:admin/repository/get
- cluster:admin/repository/put
- cluster:admin/repository/verify
- cluster:admin/reroute
- cluster:admin/settings/update
- cluster:admin/snapshot/create
- cluster:admin/snapshot/delete
- cluster:admin/snapshot/get
- cluster:admin/snapshot/restore
- cluster:admin/snapshot/status
- cluster:admin/plugin/license/get
- cluster:admin/plugin/license/delete
- cluster:admin/plugin/license/put

- cluster:admin/indices/scroll/clear_all
- cluster:admin/analyze
- cluster:admin/shield/realm/cache/clear
- cluster:monitor/health
- cluster:monitor/nodes/hot_threads
- cluster:monitor/nodes/info
- cluster:monitor/nodes/stats
- cluster:monitor/state
- cluster:monitor/stats
- cluster:monitor/task
- indices:admin/template/delete
- indices:admin/template/get
- indices:admin/template/put

Indices Action privileges

- indices:admin/aliases
- indices:admin/aliases/exists
- indices:admin/aliases/get
- indices:admin/analyze
- indices:admin/cache/clear
- indices:admin/close
- indices:admin/create
- indices:admin/delete
- indices:admin/exists
- indices:admin/flush
- indices:admin/get
- indices:admin/mapping/delete
- indices:admin/mapping/put
- indices:admin/mappings/fields/get
- indices:admin/mappings/get

- indices:admin/open
- indices:admin/optimize
- indices:admin/refresh
- indices:admin/settings/update
- indices:admin/shards/search_shards
- indices:admin/types/exists
- indices:admin/validate/query
- indices:admin/warmers/delete
- indices:admin/warmers/get
- indices:admin/warmers/put
- indices:monitor/recovery
- indices:monitor/segments
- indices:monitor/settings/get
- indices:monitor/stats
- indices:monitor/status
- indices:data/read/count
- indices:data/read/exists
- indices:data/read/explain
- indices:data/read/get
- indices:data/read/mget
- indices:data/read/mlt
- indices:data/read/mpercolate
- indices:data/read/msearch
- indices:data/read/mtv
- indices:data/read/percolate
- indices:data/read/script/get
- indices:data/read/scroll
- indices:data/read/scroll/clear
- indices:data/read/search
- indices:data/read/suggest

- indices:data/read/tv
- indices:data/write/bulk
- indices:data/write/delete
- indices:data/write/delete/by_query
- indices:data/write/index
- indices:data/write/script/delete
- indices:data/write/script/put
- indices:data/write/update

ดูเพิ่มเติมที่

https://www.elastic.co/guide/en/shield/current/reference.html

---

REFERENCE :

https://www.elastic.co/guide/en/shield/current/index.html