ELK installation on EC2 instances

Install Elastic Stack Prerequisite - Java.

Connect with **EC2-instance** using **ssh**.

OpenJDK 8 is available in standard yum repository. Therefore, we are installing OpenJDK 8 using **yum** command.

[root@elasticsearch-01 ~]# yum install -y java-1.8.0-openjdk java-1.8.0-openjdk-devel

...

Installed:

java-1.8.0-openjdk.x86_64 1:1.8.0.212.b04-0.el7_6

java-1.8.0-openjdk-devel.x86_64 1:1.8.0.212.b04-0.el7_6

Dependency Installed:

atk.x86_64 0:2.28.1-1.el7

avahi-libs.x86_64 0:0.6.31-19.el7

cairo.x86_64 0:1.15.12-3.el7

cups-libs.x86_64 1:1.6.3-35.el7

fribidi.x86_64 0:1.0.2-1.el7

gdk-pixbuf2.x86_64 0:2.36.12-3.el7

graphite2.x86_64 0:1.3.10-1.el7_3

gtk-update-icon-cache.x86_64 0:3.22.30-3.el7

gtk2.x86_64 0:2.24.31-1.el7

harfbuzz.x86_64 0:1.7.5-2.el7

hicolor-icon-theme.noarch 0:0.12-7.el7

jasper-libs.x86_64 0:1.900.1-33.el7

java-1.8.0-openjdk-headless.x86_64 1:1.8.0.212.b04-0.el7_6

jbigkit-libs.x86_64 0:2.0-11.el7

libXcomposite.x86_64 0:0.4.4-4.1.el7

libXcursor.x86_64 0:1.1.15-1.el7

libXdamage.x86_64 0:1.1.4-4.1.el7

libXfixes.x86_64 0:5.0.3-1.el7

libXft.x86_64 0:2.3.2-2.el7

libXinerama.x86_64 0:1.1.3-2.1.el7

libXrandr.x86_64 0:1.5.1-2.el7

libXxf86vm.x86_64 0:1.1.4-1.el7

libglvnd.x86_64 1:1.0.1-0.8.git5baa1e5.el7

libglvnd-egl.x86_64 1:1.0.1-0.8.git5baa1e5.el7

libglvnd-glx.x86_64 1:1.0.1-0.8.git5baa1e5.el7

libthai.x86_64 0:0.1.14-9.el7

libtiff.x86_64 0:4.0.3-27.el7_3

libwayland-client.x86_64 0:1.15.0-1.el7

libwayland-server.x86_64 0:1.15.0-1.el7

libxshmfence.x86_64 0:1.2-1.el7

mesa-libEGL.x86_64 0:18.0.5-4.el7_6

mesa-libGL.x86_64 0:18.0.5-4.el7_6

mesa-libgbm.x86_64 0:18.0.5-4.el7_6

mesa-libglapi.x86_64 0:18.0.5-4.el7_6

pango.x86_64 0:1.42.4-2.el7_6

pcsc-lite-libs.x86_64 0:1.8.8-8.el7

pixman.x86_64 0:0.34.0-1.el7

Complete!

Installing Elasticsearch Yum Repository on CentOS 7:

The procedure to install **Elasticsearch Yum Repository** is available in Elasticsearch documentation. You can also install yum repoositories for previous versions of Elastic stack using the same procedure.

Download and install the **public signing key** as follows.

[root@elasticsearch-01 ~]# rpm --import https://artifacts.elastic.co/GPG-KEY-elasticsearch

Create a new yum configuration file to install Elasticsearch Yum Repository on CentOS 7.

```
[ROOT@ELASTICSEARCH-01 ~]# CAT > /ETC/YUM.REPOS.D/ELASTICSEARCH.REPO << EOF

[ELASTICSEARCH-7.X]

NAME=ELASTICSEARCH REPOSITORY FOR 7.X PACKAGES

BASEURL=HTTPS://ARTIFACTS.ELASTIC.CO/PACKAGES/7.X/YUM

GPGCHECK=1

GPGKEY=HTTPS://ARTIFACTS.ELASTIC.CO/GPG-KEY-ELASTICSEARCH

ENABLED=1

AUTOREFRESH=1

TYPE=RPM-MD

EOF
```

==========

Build cache for Elasticsearch Yum Repository.

[root@elasticsearch-01 ~]# **yum makecache fast**

Loaded plugins: fastestmirror

Loading mirror speeds from cached hostfile

- base: mirror.dhakacom.com
- extras: mirror.dhakacom.com
- updates: mirror.dhakacom.com

base | 3.6 kB 00:00

elasticsearch-7.x | 1.3 kB 00:00

extras | 3.4 kB 00:00

updates | 3.4 kB 00:00

elasticsearch-7.x/primary | 31 kB 00:01

elasticsearch-7.x 85/85

Metadata Cache Created

We have successfully installed Elasticsearch Yum Repository. We can now install Elastic stack components on our CentOS 7 server.

Installing Elasticsearch 7.2 on CentOS 7:

Install Elasticsearch 7.2 using **yum** command.

[root@elasticsearch-01 ~]# yum install -y elasticsearch

Loaded plugins: fastestmirror

Loading mirror speeds from cached hostfile

- base: mirror.dhakacom.com
- extras: mirror.dhakacom.com
- updates: mirror.dhakacom.com

Resolving Dependencies

- -> Running transaction check
- --> Package elasticsearch.x86_64 0:7.2.0-1 will be installed
- -> Finished Dependency Resolution

Dependencies Resolved

```
================================================================================
 Package            Arch        Version        Repository             Size
================================================================================
Installing:
 elasticsearch      x86_64      7.2.0-1        elasticsearch-7.x      321 M

Transaction Summary
================================================================================
Install  1 Package
```

Total download size: 321 M

Installed size: 511 M

Downloading packages:

elasticsearch-7.2.0-x86_64.rpm | 321 MB 15:01

Running transaction check

Running transaction test

Transaction test succeeded

Running transaction

Creating elasticsearch group... OK

Creating elasticsearch user... OK

Installing : elasticsearch-7.2.0-1.x86_64 1/1

NOT starting on installation, please execute the following statements to configure elasticsearch service to start automatically using systemd

```
 sudo systemctl daemon-reload
 sudo systemctl enable elasticsearch.service
```

You can start elasticsearch service by executing

```
 sudo systemctl start elasticsearch.service
```

Created elasticsearch keystore in /etc/elasticsearch

```
  Verifying  : elasticsearch-7.2.0-1.x86_64                      1/1

Installed:
  elasticsearch.x86_64 0:7.2.0-1

Complete!
```

This is optional:

Configure **JVM** (Java Virtual Machine) options for Elasticsearch as follows.

```
[root@elasticsearch-01 ~]# vi /etc/elasticsearch/jvm.options
```

Find and set following parameters.

- Xms256m
- Xmx512m

Enable and start Elasticsearch service.

```
[root@elasticsearch-01 ~]# systemctl daemon-reload
[root@elasticsearch-01 ~]# systemctl enable elasticsearch.service
Created symlink from /etc/systemd/system/multi-user.target.wants/elasticsearch.service to /usr/lib/systemd/system/elasticsearch.service.
[root@elasticsearch-01 ~]# systemctl start elasticsearch.service
```

Add Elasticsearch service port **9200/tcp** in SELinux Policy as follows.

```
[root@elasticsearch-01 ~]# semanage port -m -t http_port_t 9200 -p tcp
```

Test Elasticsearch configuration.

```
[root@elasticsearch-01 ~]# curl http://127.0.0.1:9200
{
  "name" : "elasticsearch-01.example.com",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "AkTQvcFiSwawa7mGqcH5hA",
  "version" : {
    "number" : "7.2.0",
    "build_flavor" : "default",
    "build_type" : "rpm",
    "build_hash" : "508c38a",
    "build_date" : "2019-06-20T15:54:18.811730Z",
    "build_snapshot" : false,
    "lucene_version" : "8.0.0",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
```

},

"tagline" : "You Know, for Search"

}

Elasticsearch has been installed .

For Redhat/Centos 6 server:

service elasticsearch start

chkconfig elasticsearch on

If there is any error during startup of Elasticsearch service then check **/var/log/elasticsearch/gc.log** for detailed information and troubleshooting.

To open elasticsreach globally, need to add below lines in configuration file and restart the service.

network.bind_host: 0.0.0.0
discovery.seed_hosts: []

==========

Installing Kibana 7.2 on CentOS 7:

Kibana 7.2 can be installed from Elasticsearch yum repository using **yum** command.

[root@elasticsearch-01 ~]# yum -y install kibana

Loaded plugins: fastestmirror

Loading mirror speeds from cached hostfile

- base: mirror.dhakacom.com
- extras: mirror.dhakacom.com
- updates: mirror.dhakacom.com

Resolving Dependencies

- -> Running transaction check
- --> Package kibana.x86_64 0:7.2.0-1 will be installed
- -> Finished Dependency Resolution

Dependencies Resolved

==========

Package Arch Version Repository Size

==========

Installing:

kibana x86_64 7.2.0-1 elasticsearch-7.x 209 M

Transaction Summary

==========

Install 1 Package

Total download size: 209 M

Installed size: 532 M

Downloading packages:

kibana-7.2.0-x86_64.rpm | 209 MB 09:40

Running transaction check

Running transaction test

Transaction test succeeded

Running transaction

  Installing : kibana-7.2.0-1.x86_64   1/1

  Verifying : kibana-7.2.0-1.x86_64   1/1

Installed:

  kibana.x86_64 0:7.2.0-1

Complete!

Configure Kibana settings as follows.

[root@elasticsearch-01 ~]# cat >> /etc/kibana/kibana.yml << EOF

server.port: 5601

server.host: "0.0.0.0"

server.name: "elasticsearch-01.example.com"

elasticsearch.hosts: ["http://localhost:9200"] *(Replace Elasticsearch URL/IP)*

EOF

Enable and start Kibana service.

[root@elasticsearch-01 ~]# systemctl enable --now kibana

Created symlink from /etc/systemd/system/multi-user.target.wants/kibana.service to /etc/systemd/system/kibana.service.

Allow Kibana service port in Linux firewall.

[root@elasticsearch-01 ~]# firewall-cmd --permanent --add-port=5601/tcp

success

[root@elasticsearch-01 ~]# firewall-cmd --reload

success

For Redhat/Centos 6:

service kibana start

chkconfig kibana on

Installing Filebeat:

Filebeat is an agent that sends logs to **Logstash**. Filebeat is also available in Elasticsearch yum repository.

Since, we are installing on the same server (**elasticsearch-01.example.com**), therefore, we have already installed Elasticsearch yum repository on this server. Otherwise, we have to install Elasticsearch yum repository before installing Filebeat on other CentOS 7 machines.

Install **Filebeat** using **yum** command.

[root@elasticsearch-01 ~]# yum install -y filebeat

Loaded plugins: fastestmirror

Loading mirror speeds from cached hostfile

- base: mirror.dhakacom.com
- extras: mirror.dhakacom.com
- updates: mirrors.psu.ac.th

base | 3.6 kB 00:00

elasticsearch-7.x | 1.3 kB 00:00

extras | 3.4 kB 00:00

updates | 3.4 kB 00:00

updates/7/x86_64/primary_db | 6.5 MB 00:20

Resolving Dependencies

- -> Running transaction check
- --> Package filebeat.x86_64 0:7.2.0-1 will be installed
- -> Finished Dependency Resolution

Dependencies Resolved

```
================================================================================
 Package        Arch        Version          Repository              Size
================================================================================
Installing:
 filebeat       x86_64      7.2.0-1          elasticsearch-7.x       21 M

Transaction Summary
================================================================================
Install  1 Package

Total download size: 21 M
Installed size: 77 M
Downloading packages:
filebeat-7.2.0-x86_64.rpm                          |  21 MB   00:57
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : filebeat-7.2.0-1.x86_64                           1/1
  Verifying  : filebeat-7.2.0-1.x86_64                           1/1

Installed:
  filebeat.x86_64 0:7.2.0-1

Complete!
```

Edit Filebeat configuration file.

```
[root@elasticsearch-01 ~]# vi /etc/filebeat/filebeat.yml
```

Locate and enabled **filebeat.input** section.

```
#========================== Filebeat inputs =============================
```

filebeat.inputs:

Each - is an input. Most options can be set at the input level, so
you can use different inputs for various configurations.
Below are the input specific configurations.

- type: log

  # Change to true to enable this input configuration.
  enabled: true

  # Paths that should be crawled and fetched. Glob based paths.
  paths:
    - /var/log/*.log
    #- c:\programdata\elasticsearch\logs*

Locate and comment all lines in **output.elasticsearch** section.

#------------------------- Elasticsearch output ------------------------------
#output.elasticsearch:
  # Array of hosts to connect to.
  #hosts: ["localhost:9200"]

  # Optional protocol and basic auth credentials.
  #protocol: "https"
  #username: "elastic"
  #password: "changeme"

Locate and uncomment **output.logstash** section as follows.

#------------------------------ Logstash output -------------------------------
output.logstash:
  # The Logstash hosts
  hosts: ["localhost:5044"]

  # Optional SSL. By default is off.
  # List of root certificates for HTTPS server verifications
  #ssl.certificate_authorities: ["/etc/pki/root/ca.pem"]

  # Certificate for SSL client authentication
  #ssl.certificate: "/etc/pki/client/cert.pem"

  # Client Certificate Key

#ssl.key: "/etc/pki/client/cert.key"

Enable and start Filebeat service.

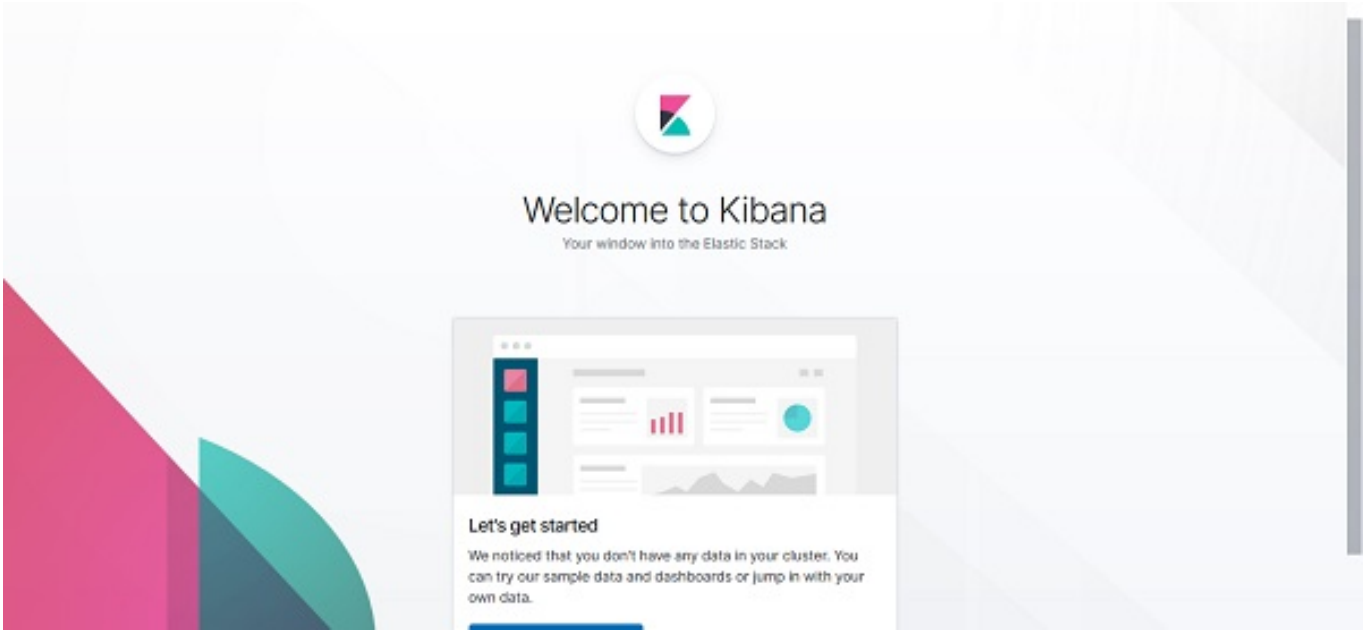
[root@elasticsearch-01 ~]# systemctl enable --now filebeat.service

Created symlink from /etc/systemd/system/multi-user.target.wants/filebeat.service to /usr/lib/systemd/system/filebeat.service.

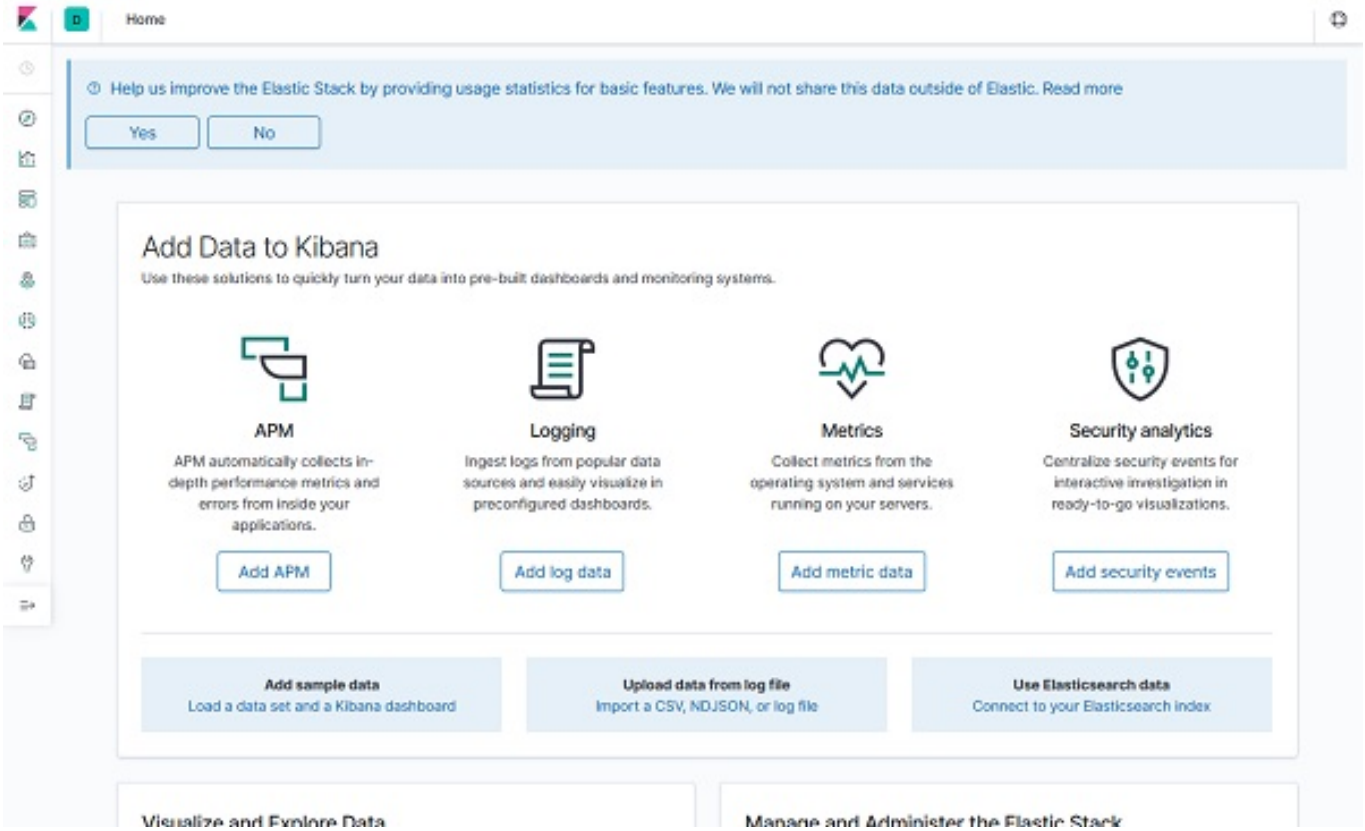
Filebeat installed and configured on the same server.

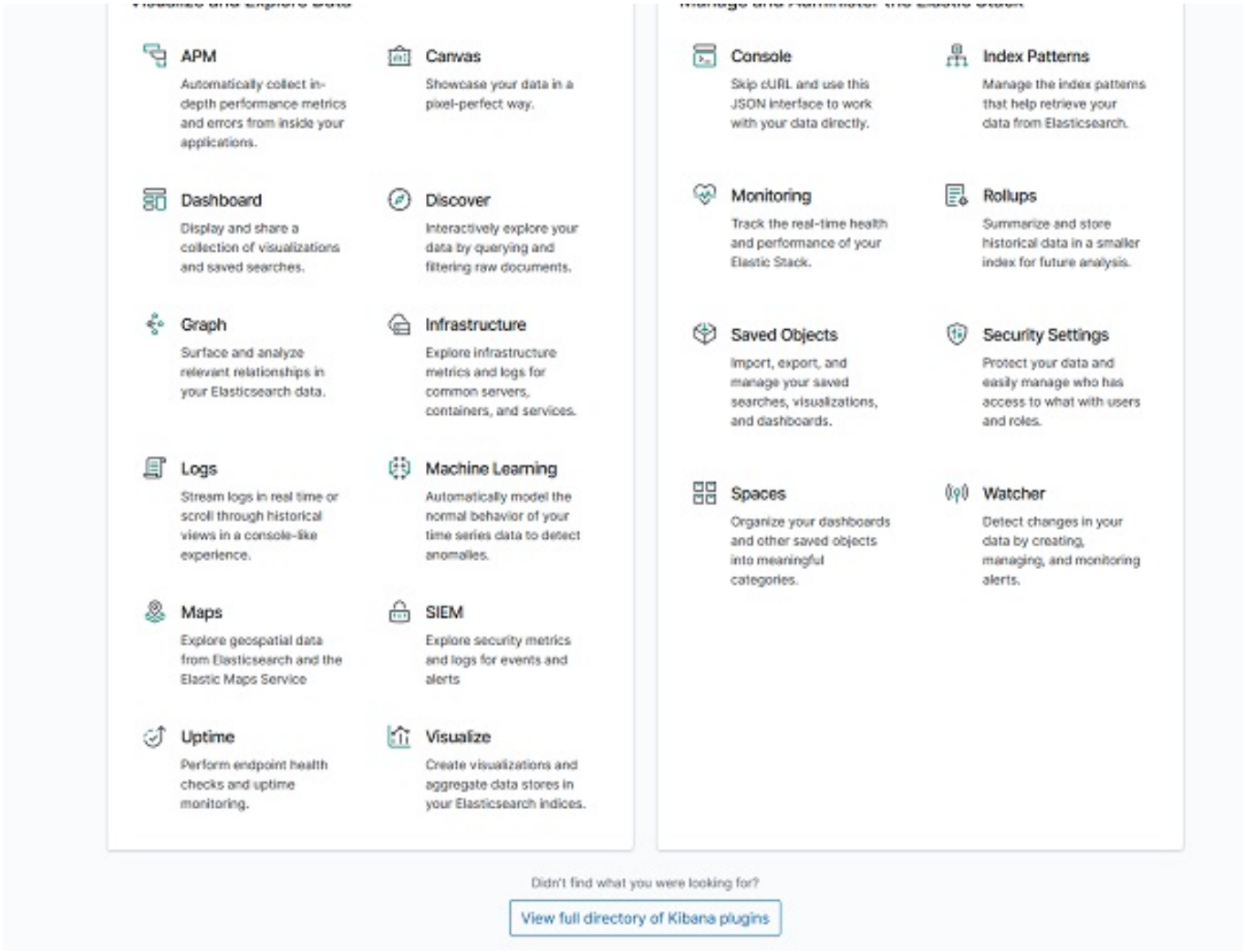
Testing Our Elastic Stack configurations:

Browse Kibana web interface **http://elasticsearch-01.example.com:5601** in a client's browser.

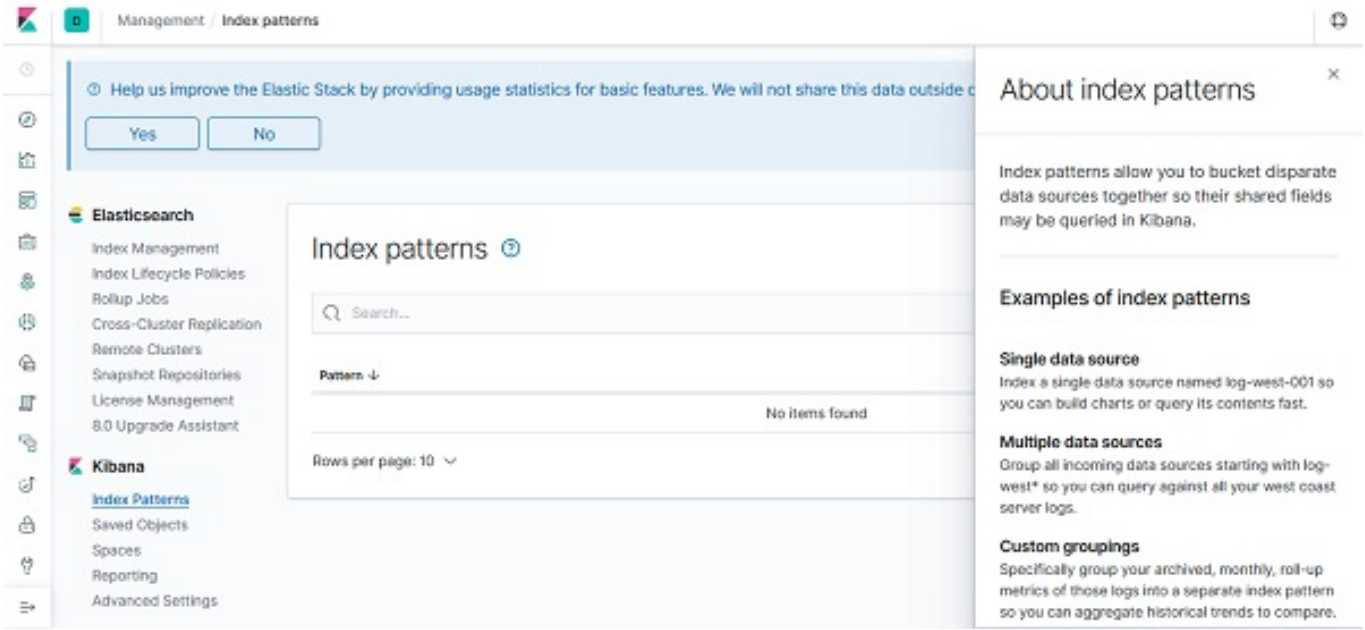


Click on Use own data.

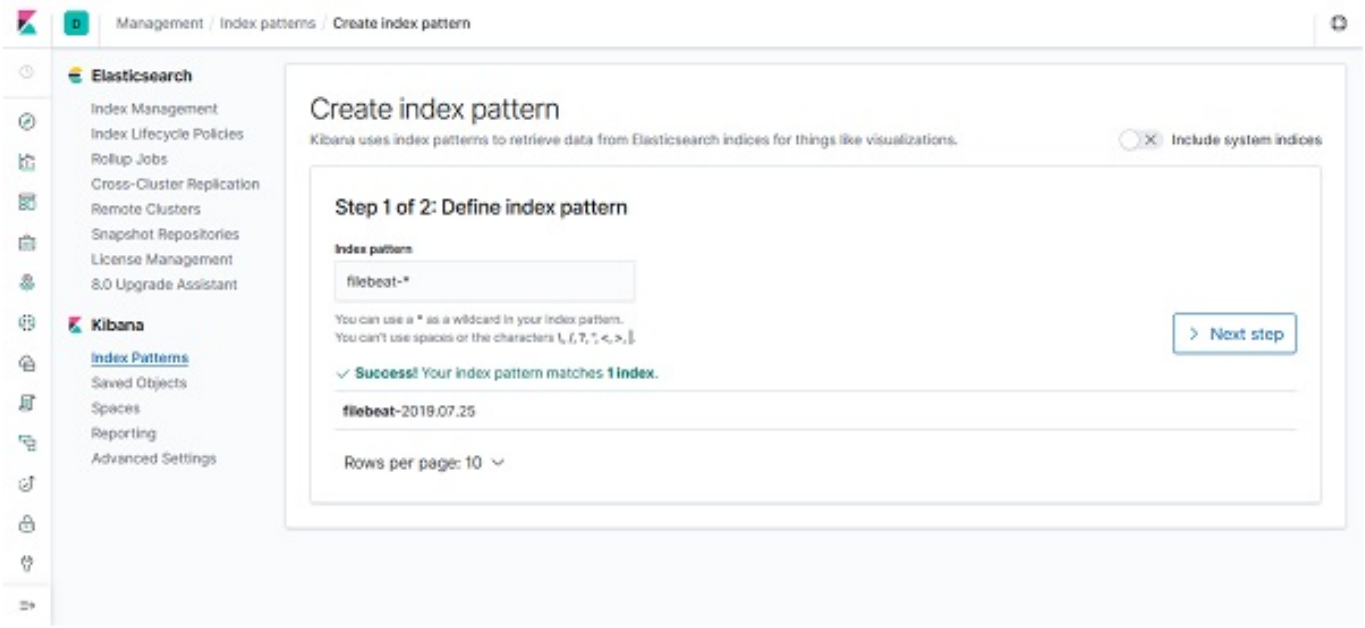




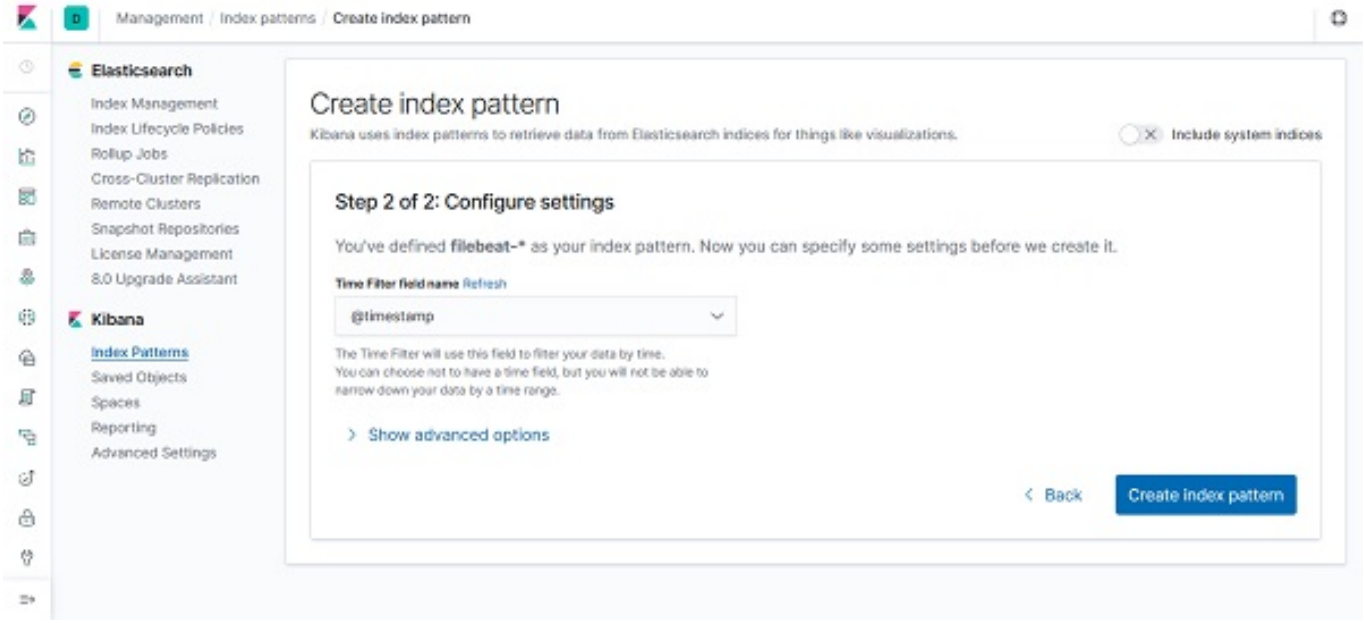
Click on Management icon under left side toolbar.



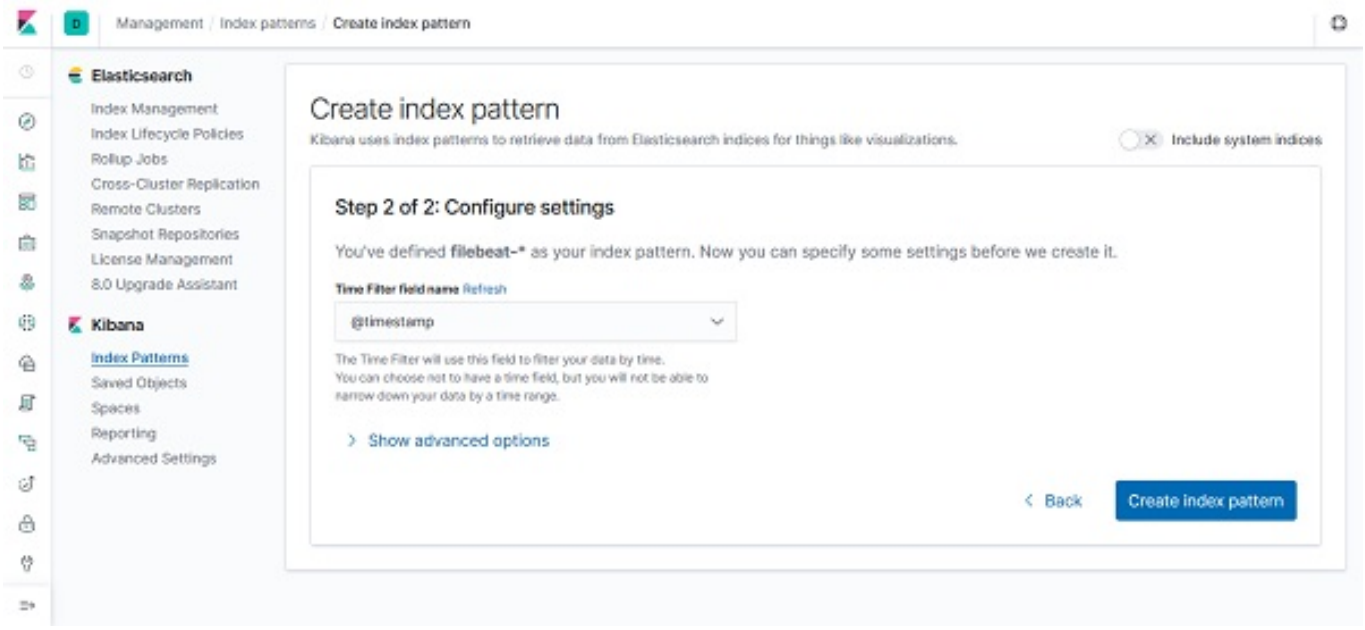
Click on Index Patterns under Kibana section.



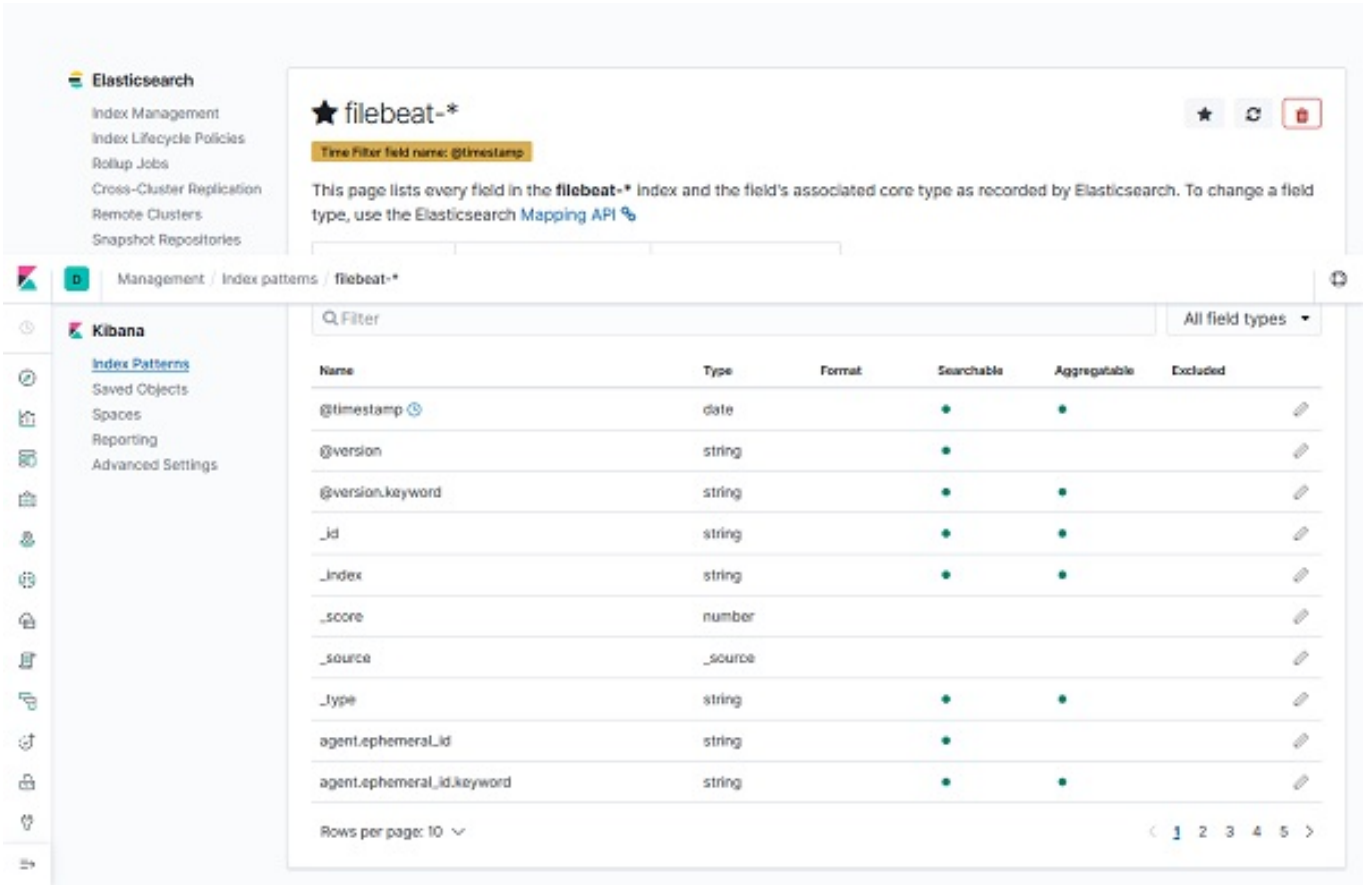
Click on Create Index Patterns.



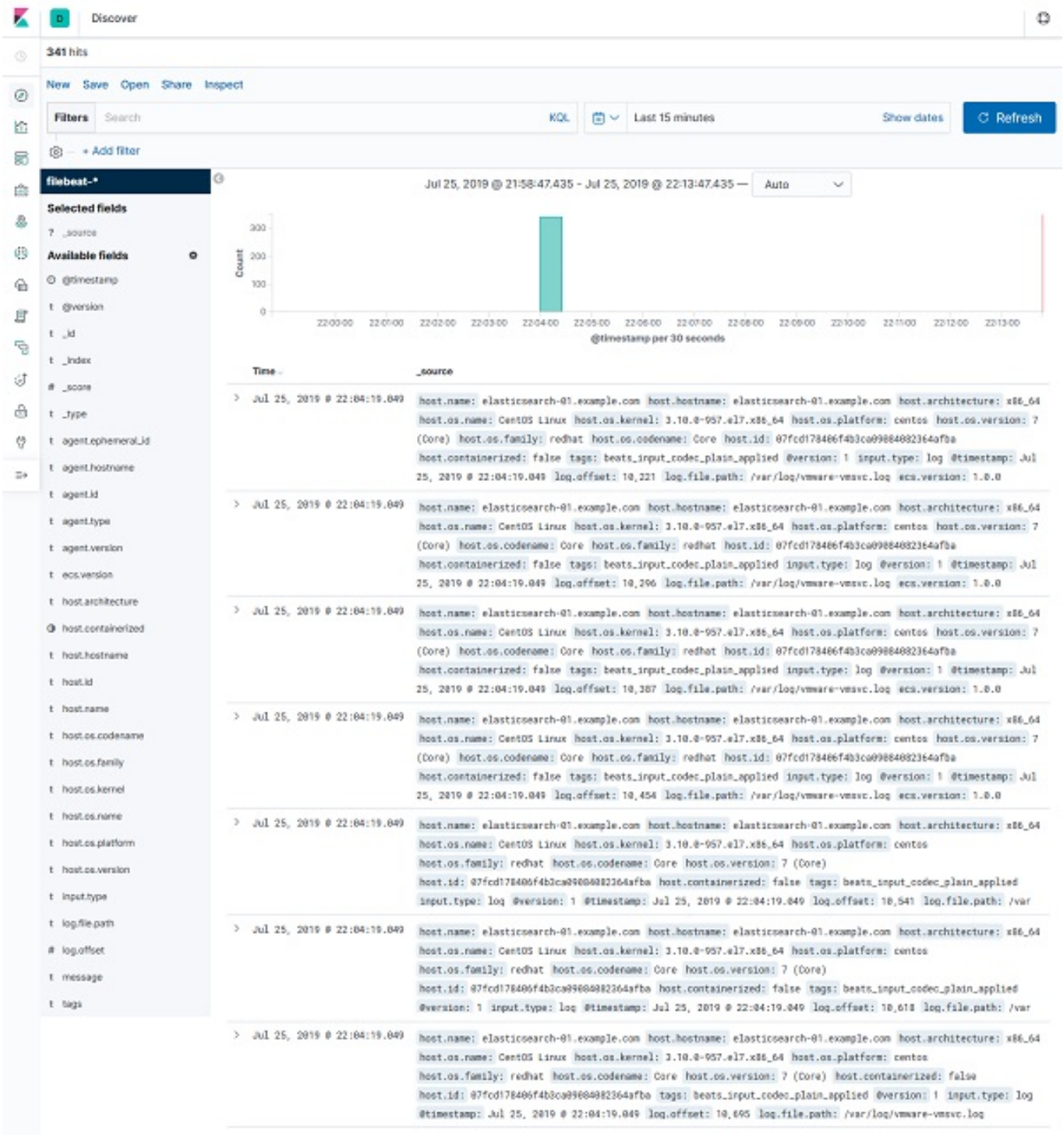
Click on > Next Step.



Click on Create Index.



Click on Discover icon under the left toolbar.



We have successfully installed Elastic Stack.