Lesson-End Project

Implementing Jenkins Logging using ELK Stack

Project agenda: To create Jenkins logging integration with ELK Stack for centralized log collection and analysis

Description: You have been given a task to onboard the Jenkins application for implementing CI/CD pipelines. Once pipelines are created you need to ensure Jenkins is working fine as expected. So, you will integrate Jenkins logging on ELK stack so that developers don't need root access to monitor Jenkins logs.

Tools required: Jenkins, ELK Stack

Prerequisites: None

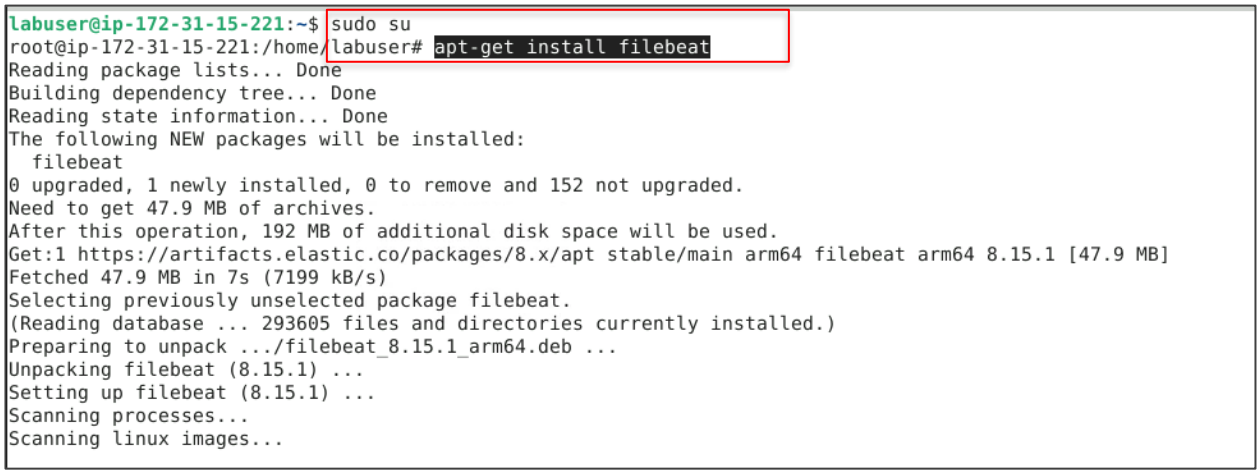
Expected deliverables: A fully integrated Jenkins logging system with the ELK Stack for centralized log collection and analysis. This system should enable efficient visualization and monitoring of Jenkins logs through Kibana, without requiring root access for developers to monitor the logs

Steps to be followed:

1. Configure file beat to collect Jenkins logs
2. Configure the Kibana visualization tool to check Jenkins logs

Step 1: Configure file beat to collect Jenkins logs

1.1 Run the following command on the terminal to download and install Filebeat:
sudo su
apt-get install filebeat



1.2 Execute the below command to modify Filebeat, so that it can send logs to Logstash
nano /etc/filebeat/filebeat.yml

1.3 Add the below code into the file:

filebeat.inputs:
- type: filestream
paths:
- "/var/log/jenkins/jenkins*.log"
enabled: true

 # ======================== Elasticsearch template setting ========================

setup.template.settings:
index.number_of_shards: 1
#index.codec: best_compression
#_source.enabled: false

output.elasticsearch:
hosts: ["localhost:9200"]

```
filebeat.inputs:
- type: filestream
  paths:
    - "/var/log/jenkins/jenkins*.log"
  enabled: true

# ======================== Elasticsearch template setting ========================

setup.template.settings:
  index.number_of_shards: 1
  #index.codec: best_compression
  #_source.enabled: false

output.elasticsearch:
  hosts: ["localhost:9200"]
```

1.4 Run the below command to open Service configuration using the vi command and uncomment the below code line as shown in the screenshot:
vi /lib/systemd/system/jenkins.service

```
No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
root@ip-172-31-15-221:/home/labuser# nano /etc/filebeat/filebeat.yml
root@ip-172-31-15-221:/home/labuser# vi /lib/systemd/system/jenkins.service
```

```
# Directory where Jenkins stores its configuration and workspaces
Environment="JENKINS_HOME=/var/lib/jenkins"
WorkingDirectory=/var/lib/jenkins

# Location of the Jenkins WAR
#Environment="JENKINS_WAR=/usr/share/java/jenkins.war"

# Location of the exploded WAR
Environment="JENKINS_WEBROOT=%C/jenkins/war"

# Location of the Jenkins log. By default, systemd-journald(8) is used.
Environment="JENKINS_LOG=%L/jenkins/jenkins.log"

# The Java home directory. When left empty, JENKINS_JAVA_CMD and PATH are consulted.
#Environment="JAVA_HOME=/usr/lib/jvm/java-17-openjdk-amd64"
```

Note: press esc and enter **:wq** to save and exit the file.

1.5 Once the configuration is saved run the below command to restart the Jenkins:

systemctl daemon-reload

service jenkins restart

```
No VM guests are running outdated hypervisor (qemu) binaries on this host.
root@ip-172-31-15-221:/home/labuser# nano /etc/filebeat/filebeat.yml
root@ip-172-31-15-221:/home/labuser# vi /lib/systemd/system/jenkins.service
root@ip-172-31-15-221:/home/labuser# systemctl daemon-reload
root@ip-172-31-15-221:/home/labuser# service jenkins restart
```

1.6 Run the below commands to restart the configuration file:

sudo systemctl start filebeat

sudo systemctl enable filebeat

sudo systemctl status filebeat

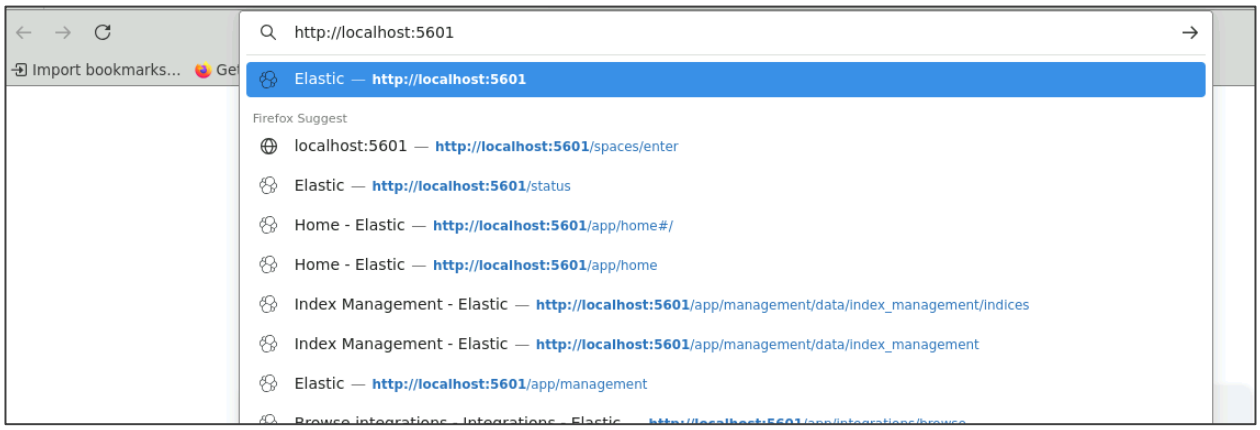
```
root@ip-172-31-15-221:/home/labuser# sudo systemctl start filebeat
root@ip-172-31-15-221:/home/labuser# sudo systemctl enable filebeat
Synchronizing state of filebeat.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable filebeat
Created symlink /etc/systemd/system/multi-user.target.wants/filebeat.service → /lib/systemd/system/filebeat.service.
root@ip-172-31-15-221:/home/labuser# sudo systemctl status filebeat
● filebeat.service - Filebeat sends log files to Logstash or directly to Elasticsearch.
     Loaded: loaded (/lib/systemd/system/filebeat.service; enabled; vendor preset: enabled)
     Active: active (running) since Wed 2024-09-25 09:49:23 UTC; 27s ago
       Docs: https://www.elastic.co/beats/filebeat
   Main PID: 10105 (filebeat)
      Tasks: 8 (limit: 9361)
     Memory: 64.1M
        CPU: 726ms
     CGroup: /system.slice/filebeat.service
             └─10105 /usr/share/filebeat/bin/filebeat --environment systemd -c /etc/filebeat/filebeat.yml --path.home /usr/share/filebeat --path.con>

Sep 25 09:49:23 ip-172-31-15-221 systemd[1]: Started Filebeat sends log files to Logstash or directly to Elasticsearch..
```

1.7 Execute the below command to verify that Elasticsearch is receiving the filebeat data log:
curl -XGET http://localhost:9200/_cat/indices?v | grep filebeat

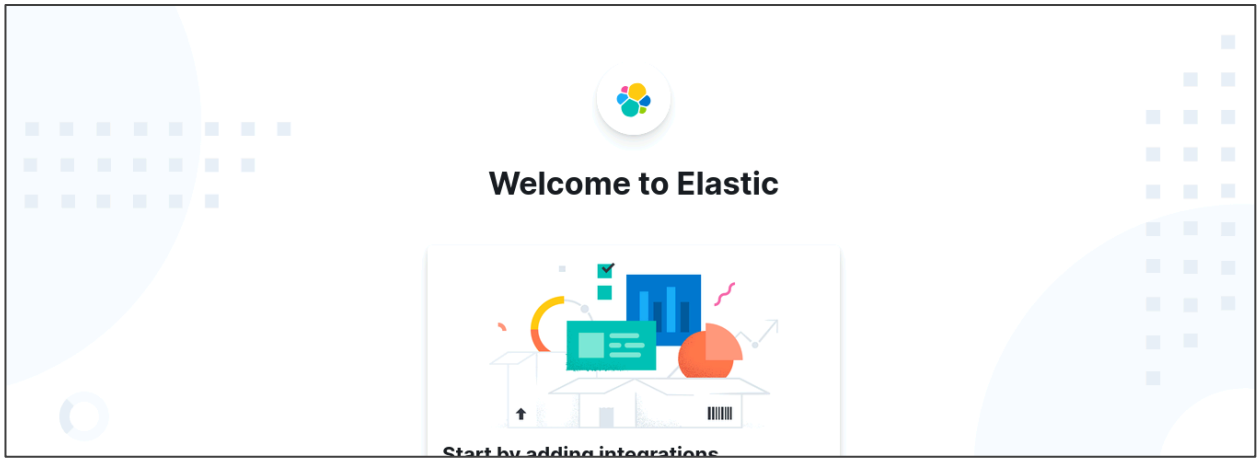
```
root@ip-172-31-15-221:/home/labuser# curl -XGET http://localhost:9200/_cat/indices?v | grep filebeat
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  3500    0  3500    0     0  32134      0 --:--:-- --:--:-- --:--:-- 32407
yellow open   .ds-filebeat-8.15.1-2024.09.25-000001                        sMIh2u9mQa6IaAFsAj5xbg   1   1
      26.8kb       26.8kb
root@ip-172-31-15-221:/home/labuser#
```

Step 2: Configure Kibana visualization tool to check Jenkins logs

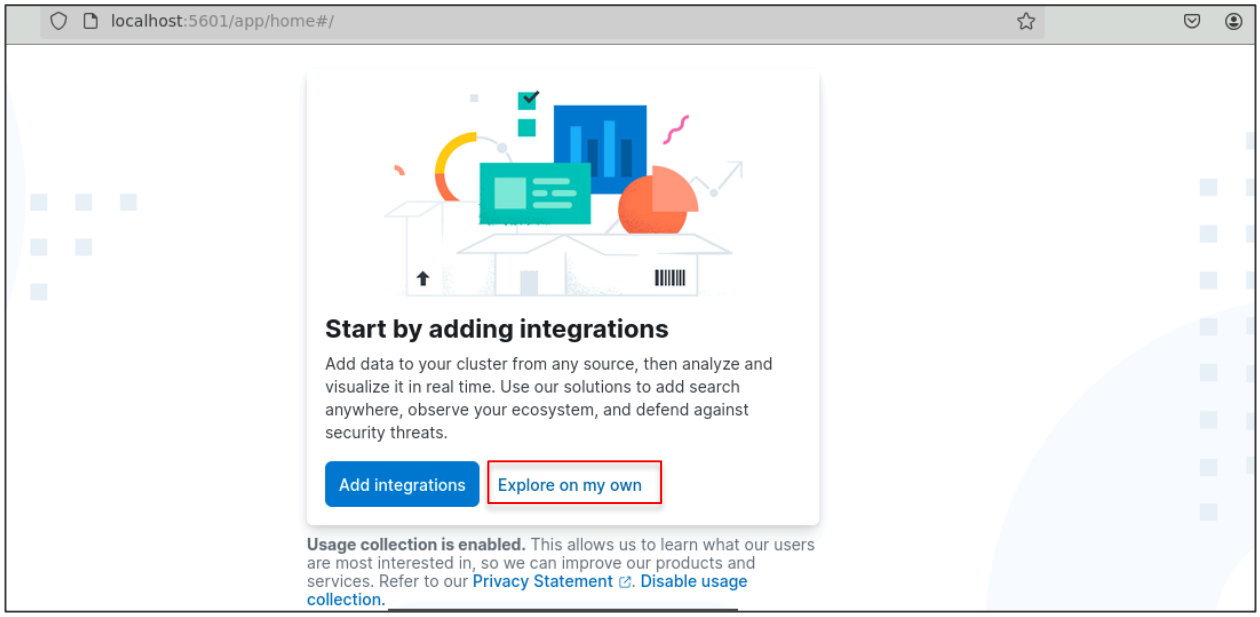
2.1 Enter the below URL to access the Kibana web interface to visualized logs collected by filebeat
http://localhost:5601



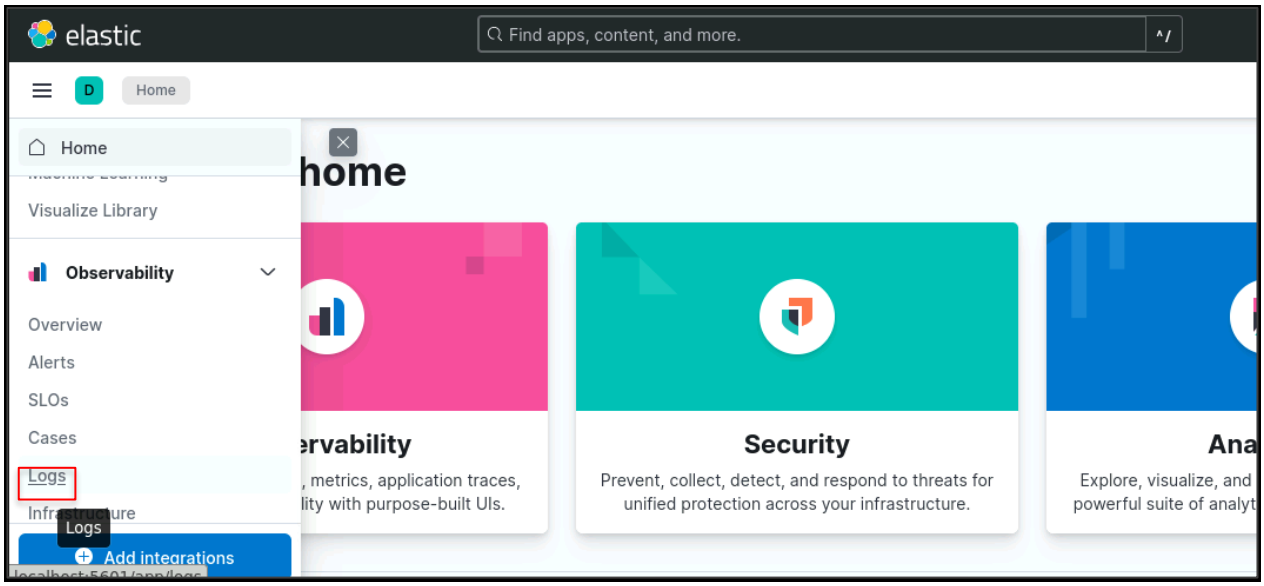
You can see the below screen:

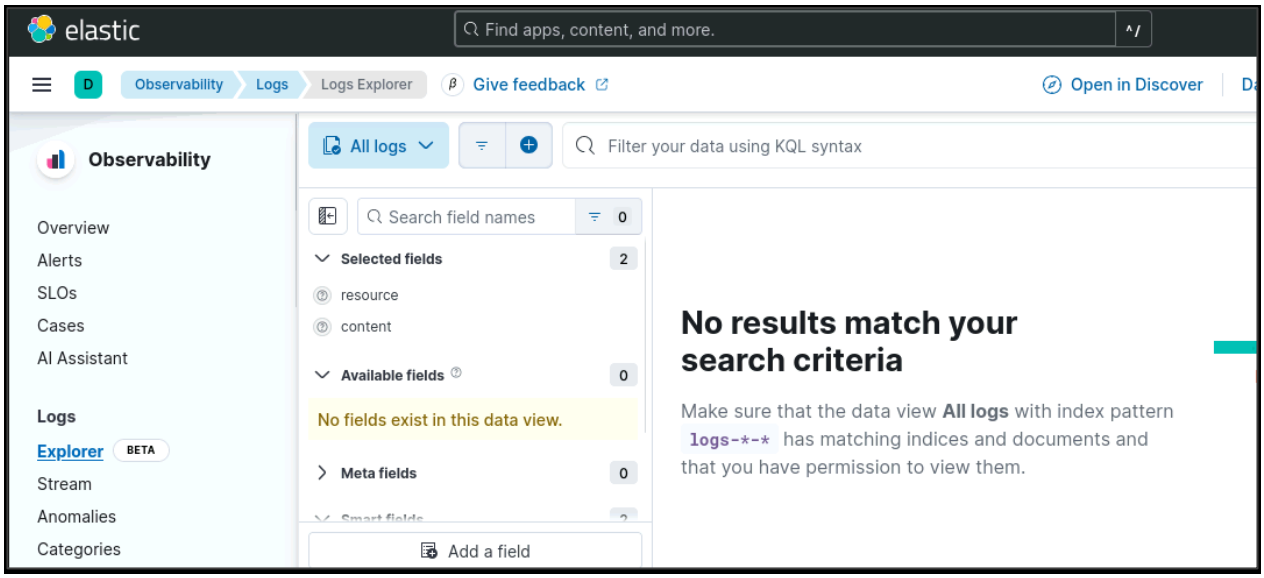


2.2 Click on **Explore on my own**

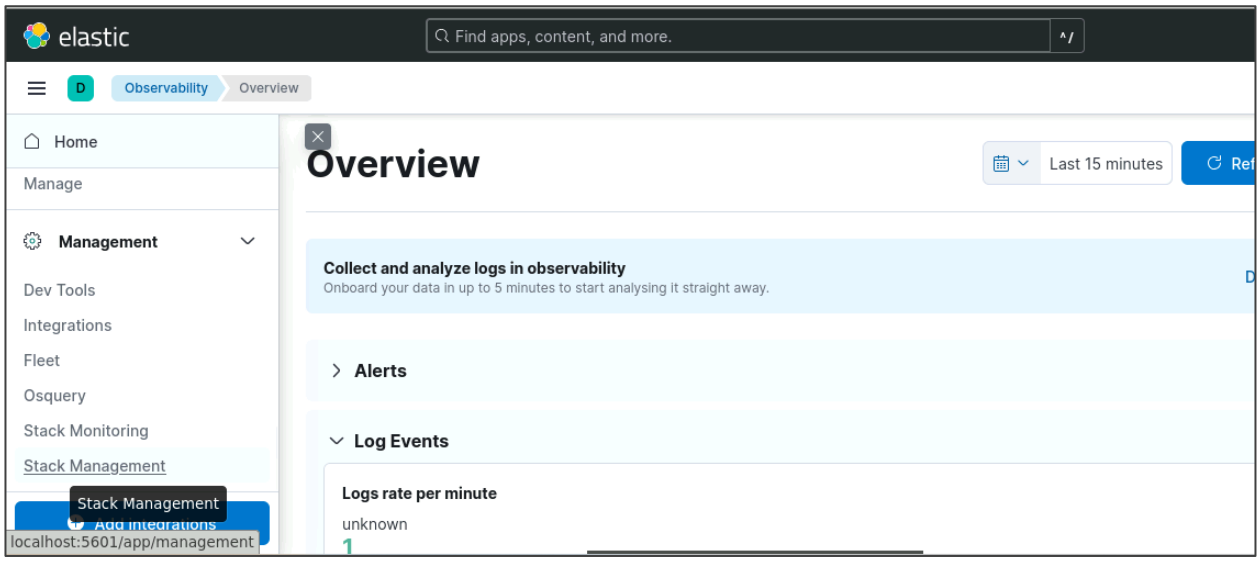


2.3 Click on Home, click **Logs** to check the system logs in Kibana

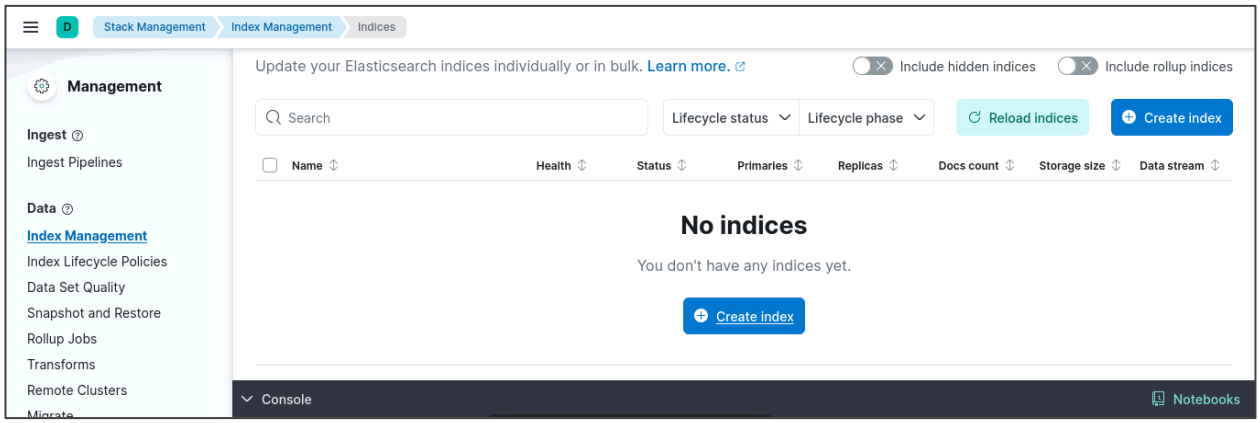

elastic
Find apps, content, and more.
Home
Home
Visualize Library
Observability
Overview
Alerts
SLOs
Cases
Logs
Logs
Add integrations
home
Security
Prevent, collect, detect, and respond to threats for unified protection across your infrastructure.


elastic
Find apps, content, and more.
Observability
Logs
Logs Explorer
Give feedback
Open in Discover
Observability
Overview
Alerts
SLOs
Cases
AI Assistant
Logs
Explorer
BETA
Stream
Anomalies
Categories
All logs
Filter your data using KQL syntax
Search field names
Selected fields
resource
content
Available fields
No fields exist in this data view.
Meta fields
Add a field
No results match your search criteria
Make sure that the data view All logs with index pattern logs-*-* has matching indices and documents and that you have permission to view them.

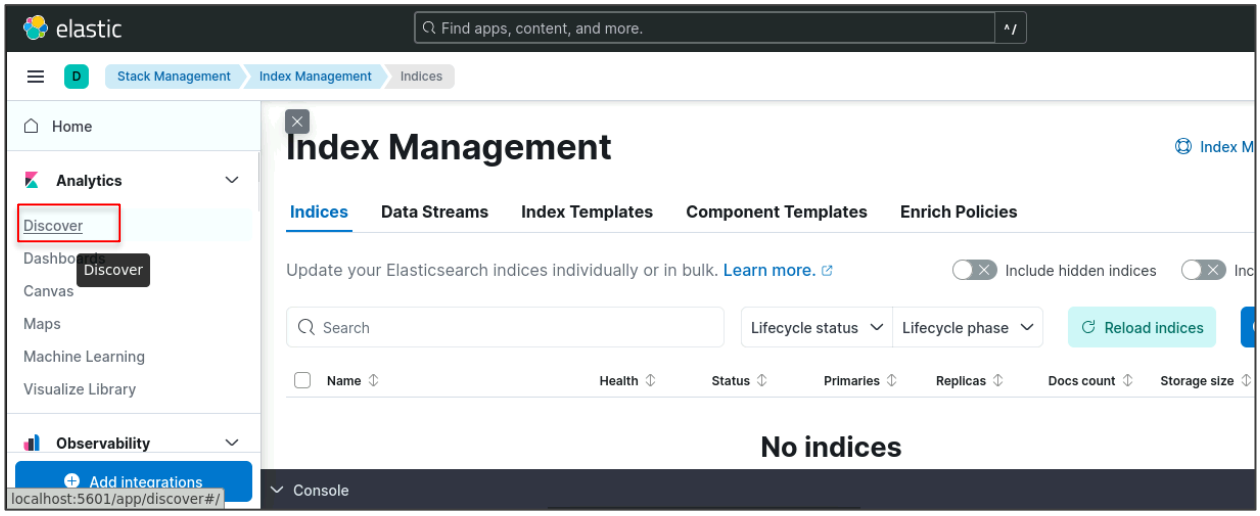
2.4 Now navigate back to **Home** and click on **Stack Management**



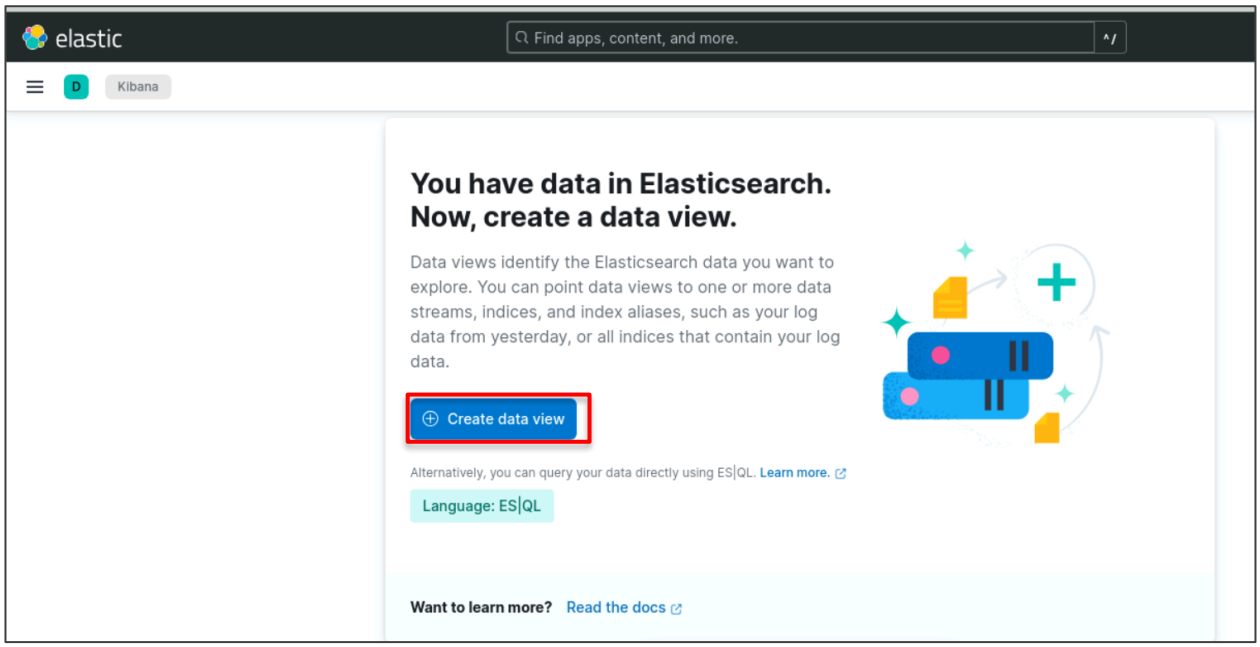
2.5 Click on **Index Management**

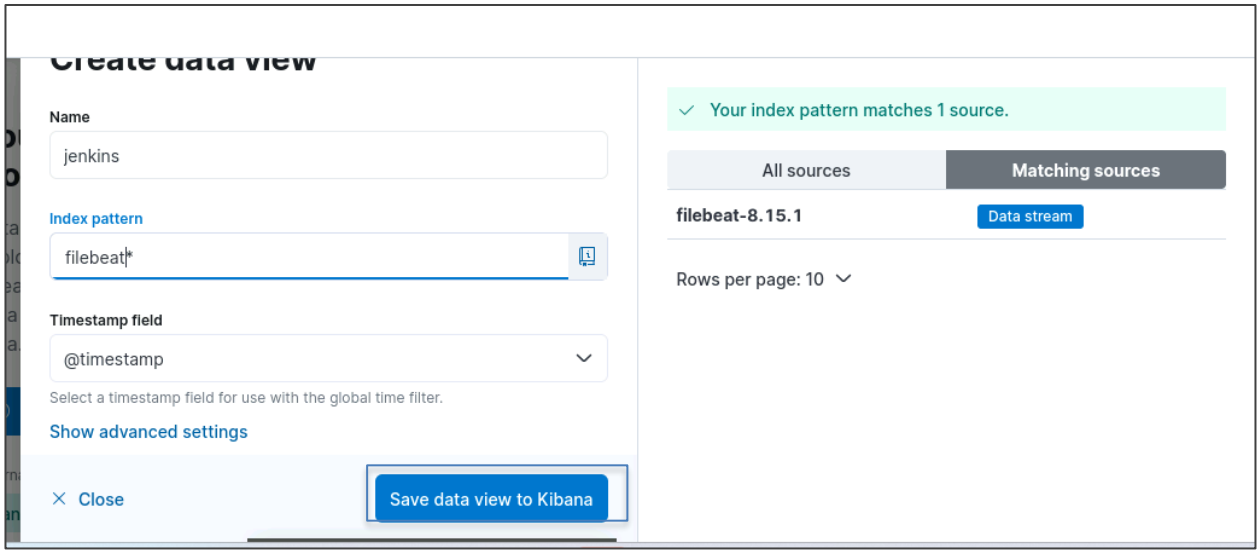


2.6 Uder **Analytics** click on **Discover**

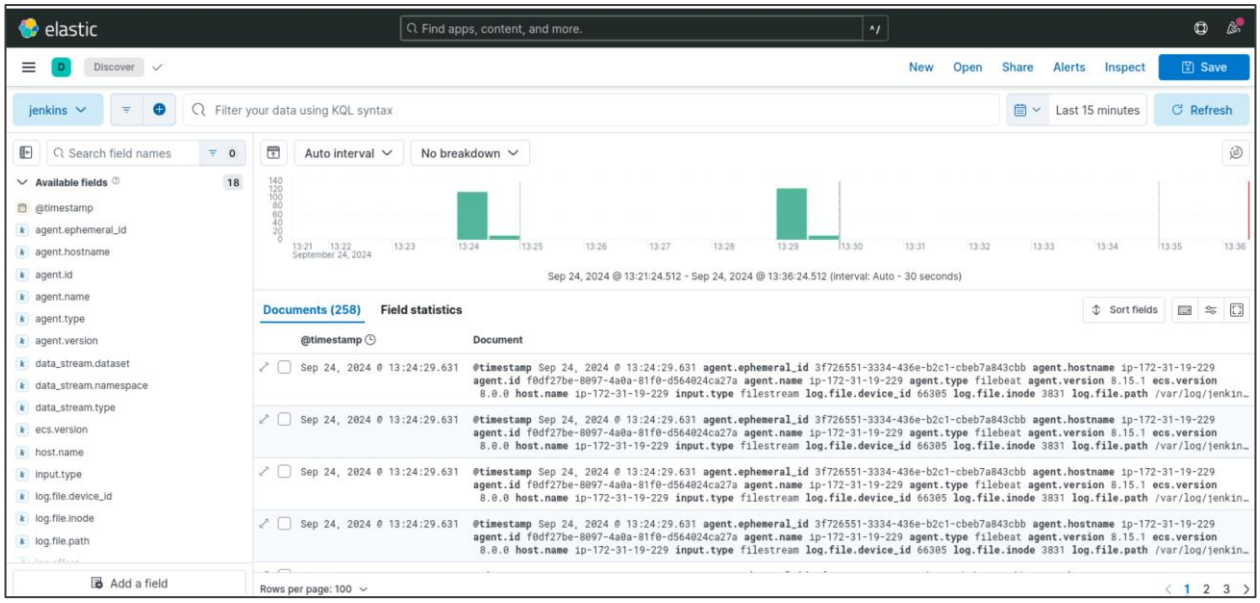


2.7 Click on **Create data view** then fill the details as shown in the screenshot and click on **Save data view to Kibana**

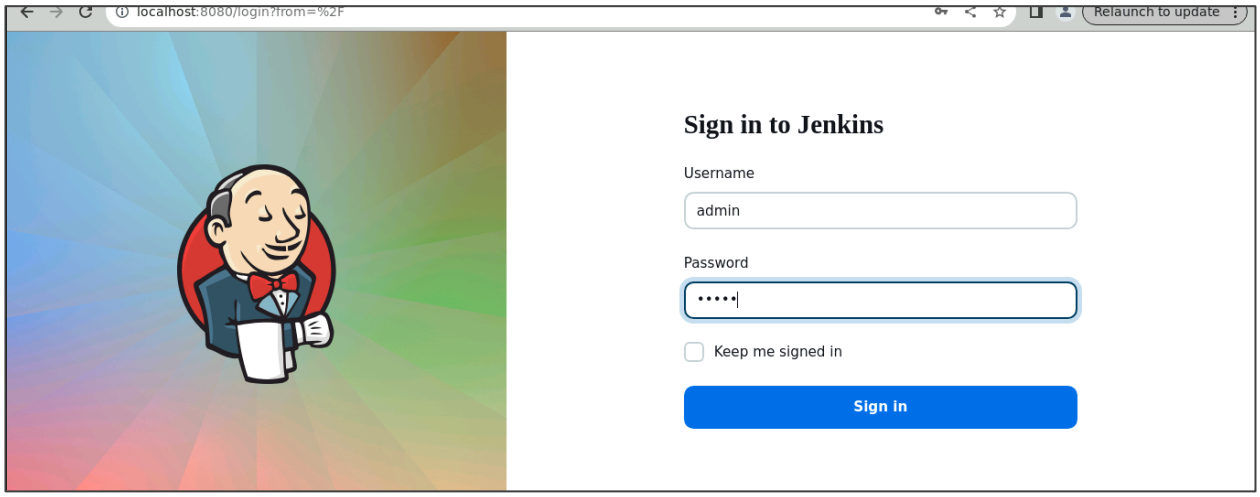




You can visualize the logs as shown below:

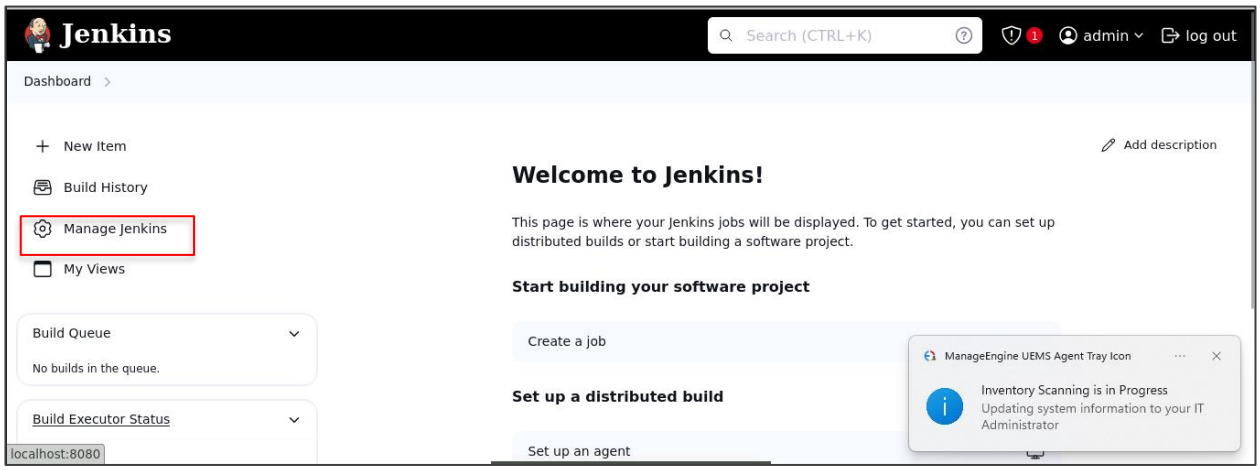


2.8 Navigate to Jenkins using the below **URL**:
localhost:8080

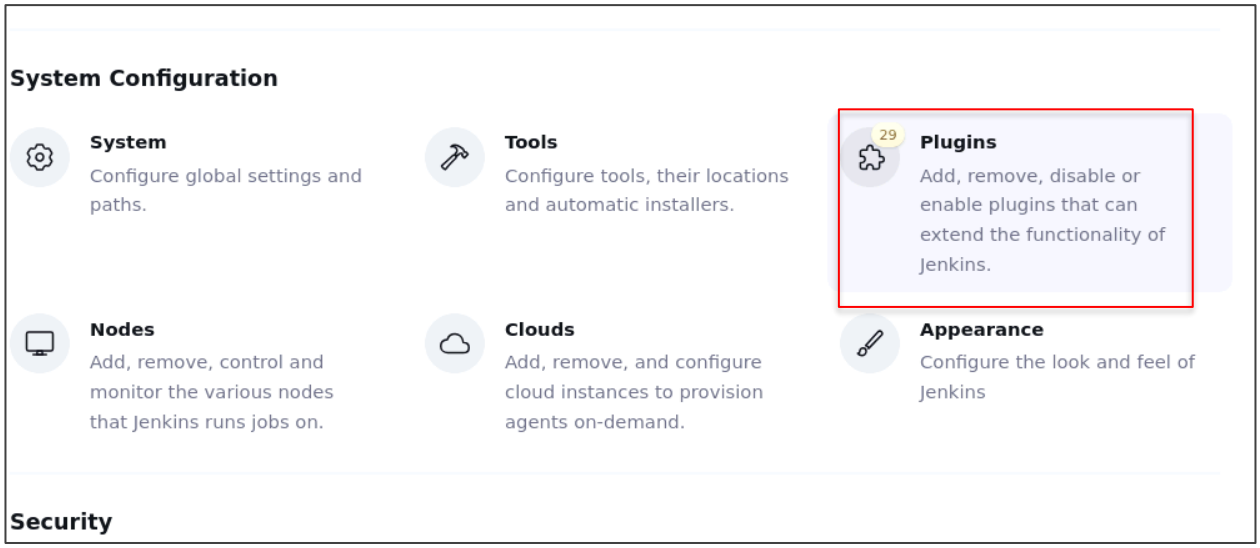


Note: Username: admin and Password: Root123$

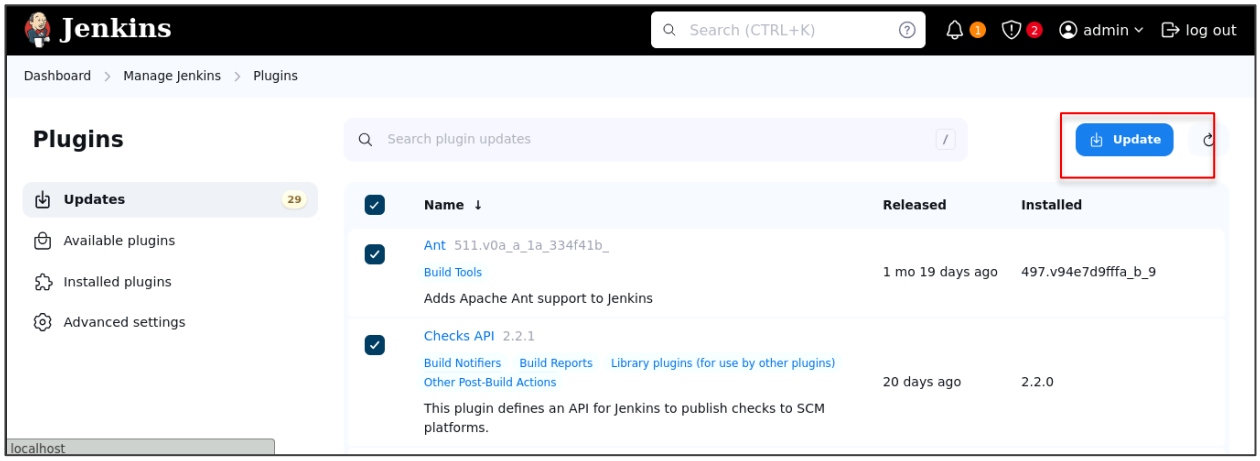
2.9 Click on **Manage Jenkins**



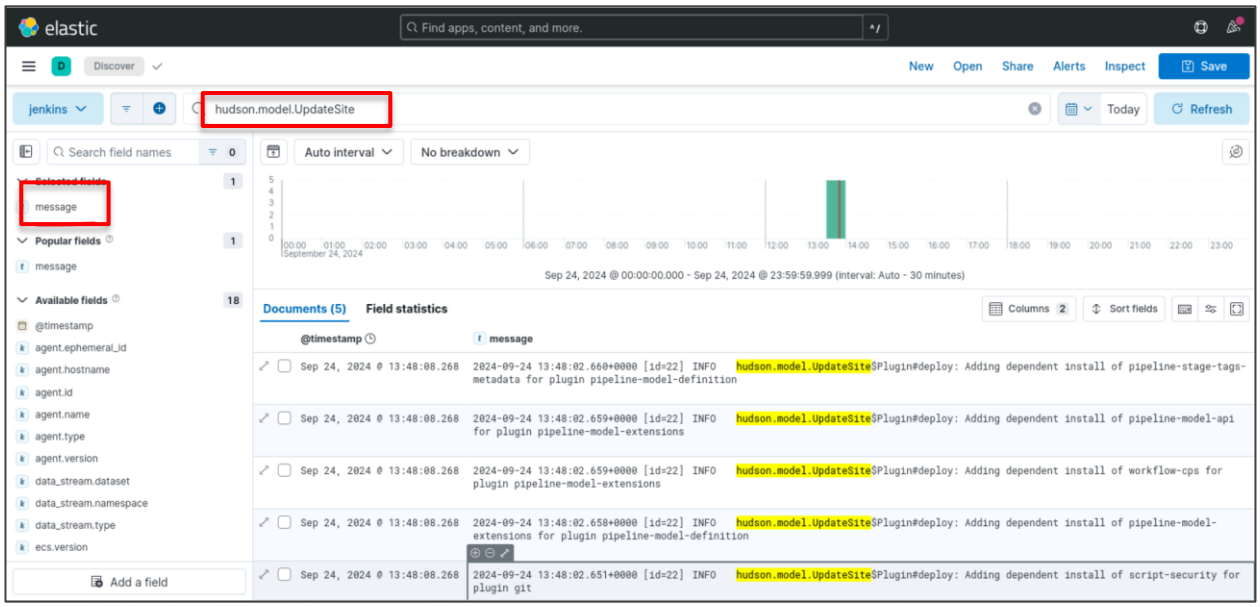
2.10 Click on the **Plugins**



2.11 Select all the plugins and click on **Update**



2.12 Navigate back to Kibana and search for the below keyword to see recent log entries regarding plugin upgrade activity on Jenkins. Also, select the **message** field to get only log entries in Kibana without any metadata.
Keyword: hudson.model.UpdateSite



By following these steps, you have successfully created Jenkins logging integration with ELK Stack for centralized log collection and analysis.