

Use below URL for the installatoion of elasticsearch and kibana

https://www.elastic.co/guide/en/elastic-stack/8.15/installing-stack-demo-self.html

Elastic search Users:

Changed password for user apm\_system

PASSWORD apm\_system = wbaEAa6wLRo77bkMxJeK

Changed password for user kibana\_system

PASSWORD kibana\_system = wk1sCtCb5Zy4TzllzrsS

Changed password for user kibana

PASSWORD kibana = wk1sCtCb5Zy4TzllzrsS

Changed password for user logstash\_system

PASSWORD logstash\_system = fQLZErBPkn7CYHsodO2G

Changed password for user beats\_system

PASSWORD beats\_system = hH2op4pedwF1o4ENRkvP

Changed password for user remote\_monitoring\_user

PASSWORD remote\_monitoring\_user = I6ew5HvwBLQX0SouHbY7

Changed password for user elastic

PASSWORD elastic = W6vCNRzEvZugpmpZSFmR

Below is the shell through which logs are sent to elastic search.

[root@PAYTECHDBBAKSRV conf.d]# cat test.sh

#!/bin/bash

# Elasticsearch configuration

ELASTICSEARCH\_URL="http://127.0.0.1:9200"

INDEX\_NAME="test-$(date +%Y-%m-%d)"

USER="elastic"

PASSWORD="W6vCNRzEvZugpmpZSFmR"

# Path to your log files

LOG\_FILE\_PATH="/tmp/test/log/\*.log"

# Read each log file

for log\_file in $LOG\_FILE\_PATH; do

while IFS= read -r line; do

# Prepare JSON payload

json\_payload=$(jq -n --arg message "$line" '{message: $message, timestamp: now | todate}')

# Send data to Elasticsearch

curl -u "$USER:$PASSWORD" -X POST "$ELASTICSEARCH\_URL/$INDEX\_NAME/\_doc/" -H 'Content-Type: application/json' -d "$json\_payload"

done < "$log\_file"

done

---------------------------------------------------------------------------------------------------------

Elastic search conf file

[root@PAYTECHDBBAKSRV conf.d]# cat /etc/elasticsearch/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 consult the documentation for further information on configuration options:

# https://www.elastic.co/guide/en/elasticsearch/reference/index.html

#

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

#

# Use a descriptive name for your cluster:

#

cluster.name: my-application

#

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

#

# Use a descriptive name for the node:

#

node.name: node-1

#

# Add custom attributes to the node:

#

node.attr.rack: r1

#

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

#

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

#

path.data: /mnt/elasticsearch/data

#

# Path to log files:

#

path.logs: /mnt/elasticsearch/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 -----------------------------------

#

# By default Elasticsearch is only accessible on localhost. Set a different

# address here to expose this node on the network:

#

network.host: 127.0.0.1

#

# By default Elasticsearch listens for HTTP traffic on the first free port it

# finds starting at 9200. Set a specific HTTP port here:

#

http.port: 9200

#

# For more information, consult the network module documentation.

#

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

#

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

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

#

#discovery.seed\_hosts: ["host1", "host2"]

#

# Bootstrap the cluster using an initial set of master-eligible nodes:

#

#cluster.initial\_master\_nodes: ["node-1", "node-2"]

#

# For more information, consult the discovery and cluster formation module documentation.

#

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

#

xpack.security.enabled: true

#

# Allow wildcard deletion of indices:

#

#action.destructive\_requires\_name: false

You have mail in /var/spool/mail/root

[root@PAYTECHDBBAKSRV conf.d]#

--------------------------------------------------------------------------------------------------------------

[root@PAYTECHDBBAKSRV conf.d]# cat /etc/kibana/kibana.yml

# For more configuration options see the configuration guide for Kibana in

# https://www.elastic.co/guide/index.html

# =================== System: Kibana Server ===================

# 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: "10.188.40.14"

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

# Use the `server.rewriteBasePath` setting to tell Kibana if it should remove the basePath

# from requests it receives, and to prevent a deprecation warning at startup.

# This setting cannot end in a slash.

#server.basePath: ""

# Specifies whether Kibana should rewrite requests that are prefixed with

# `server.basePath` or require that they are rewritten by your reverse proxy.

# Defaults to `false`.

#server.rewriteBasePath: false

# Specifies the public URL at which Kibana is available for end users. If

# `server.basePath` is configured this URL should end with the same basePath.

#server.publicBaseUrl: ""

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

#server.maxPayload: 1048576

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

#server.name: "your-hostname"

# =================== System: Kibana Server (Optional) ===================

# Enables SSL and paths to the PEM-format SSL certificate and SSL key files, respectively.

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

#server.ssl.enabled: false

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

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

# =================== System: Elasticsearch ===================

# The URLs of the Elasticsearch instances to use for all your queries.

elasticsearch.hosts: ["http://localhost:9200"]

# 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: "kibana"

elasticsearch.password: "wk1sCtCb5Zy4TzllzrsS"

# Kibana can also authenticate to Elasticsearch via "service account tokens".

# Service account tokens are Bearer style tokens that replace the traditional username/password based configuration.

# Use this token instead of a username/password.

# elasticsearch.serviceAccountToken: "my\_token"

# 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

# The maximum number of sockets that can be used for communications with elasticsearch.

# Defaults to `Infinity`.

#elasticsearch.maxSockets: 1024

# Specifies whether Kibana should use compression for communications with elasticsearch

# Defaults to `false`.

#elasticsearch.compression: false

# 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: 30000

# =================== System: Elasticsearch (Optional) ===================

# These files are used to verify the identity of Kibana to Elasticsearch and are required when

# xpack.security.http.ssl.client\_authentication in Elasticsearch is set to required.

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

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

# Enables you to specify a path to the PEM file for the certificate

# authority for your Elasticsearch instance.

#elasticsearch.ssl.certificateAuthorities: [ "/path/to/your/CA.pem" ]

# To disregard the validity of SSL certificates, change this setting's value to 'none'.

#elasticsearch.ssl.verificationMode: full

# =================== System: Logging ===================

# Set the value of this setting to off to suppress all logging output, or to debug to log everything. Defaults to 'info'

#logging.root.level: debug

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

logging:

appenders:

file:

type: file

fileName: /var/log/kibana/kibana.log

layout:

type: json

root:

appenders:

- default

- file

# policy:

# type: size-limit

# size: 256mb

# strategy:

# type: numeric

# max: 10

# layout:

# type: json

# Logs queries sent to Elasticsearch.

#logging.loggers:

# - name: elasticsearch.query

# level: debug

# Logs http responses.

#logging.loggers:

# - name: http.server.response

# level: debug

# Logs system usage information.

#logging.loggers:

# - name: metrics.ops

# level: debug

# Enables debug logging on the browser (dev console)

#logging.browser.root:

# level: debug

# =================== System: Other ===================

# The path where Kibana stores persistent data not saved in Elasticsearch. Defaults to data

#path.data: data

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

pid.file: /run/kibana/kibana.pid

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

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

#ops.interval: 5000

# Specifies locale to be used for all localizable strings, dates and number formats.

# Supported languages are the following: English (default) "en", Chinese "zh-CN", Japanese "ja-JP", French "fr-FR".

#i18n.locale: "en"

# =================== Frequently used (Optional)===================

# =================== Saved Objects: Migrations ===================

# Saved object migrations run at startup. If you run into migration-related issues, you might need to adjust these settings.

# The number of documents migrated at a time.

# If Kibana can't start up or upgrade due to an Elasticsearch `circuit\_breaking\_exception`,

# use a smaller batchSize value to reduce the memory pressure. Defaults to 1000 objects per batch.

#migrations.batchSize: 1000

# The maximum payload size for indexing batches of upgraded saved objects.

# To avoid migrations failing due to a 413 Request Entity Too Large response from Elasticsearch.

# This value should be lower than or equal to your Elasticsearch cluster’s `http.max\_content\_length`

# configuration option. Default: 100mb

#migrations.maxBatchSizeBytes: 100mb

# The number of times to retry temporary migration failures. Increase the setting

# if migrations fail frequently with a message such as `Unable to complete the [...] step after

# 15 attempts, terminating`. Defaults to 15

#migrations.retryAttempts: 15

# =================== Search Autocomplete ===================

# Time in milliseconds to wait for autocomplete suggestions from Elasticsearch.

# This value must be a whole number greater than zero. Defaults to 1000ms

#unifiedSearch.autocomplete.valueSuggestions.timeout: 1000

# Maximum number of documents loaded by each shard to generate autocomplete suggestions.

# This value must be a whole number greater than zero. Defaults to 100\_000

#unifiedSearch.autocomplete.valueSuggestions.terminateAfter: 100000

xpack.encryptedSavedObjects.encryptionKey: b5ebd3d6ab3008218ce5648291eebbf5

xpack.reporting.encryptionKey: c4ac2da8c3a43f9dedcbdb99c284a45c

xpack.security.encryptionKey: 41d29e2dbeea3025e4a7c1914388e251



