# Instalar Kibana

Los comandos de este manual deben ser ejecutados en un servidor **Linux Centos 7** con el usuario root o una cuenta de usuario que pertenezca al grupo root.

Cabe indicar que los comandos de este manual tienen como alcance la instalación de las versiones Open Source con una configuración de los servicios a nivel de desarrollo, no garantizando la optimización para un ambiente de producción.

## Requisitos previos:

Para poder instalar Kong debe tener instalado Docker en el servidor y tener acceso a internet.

En este caso instalaremos Docker Community Edition. Para ello se debe ejecutar los siguientes comandos:

sudo yum install -y yum-utils device-mapper-persistent-data lvm2

sudo yum-config-manager --add-repo https://download.docker.com/linux/centos/docker-ce.repo

#Se instala docker indicando explicitamente la version

sudo yum update -y && yum install -y containerd.io-1.2.13 docker-ce-19.03.11 docker-ce-cli-19.03.11

mkdir /etc/docker

cat > /etc/docker/daemon.json <<EOF

{

"exec-opts": ["native.cgroupdriver=systemd"],

"log-driver": "json-file",

"log-opts": {

"max-size": "100m"

},

"storage-driver": "overlay2",

"storage-opts": [

"overlay2.override\_kernel\_check=true"

]

}

EOF

mkdir -p /etc/systemd/system/docker.service.d

systemctl daemon-reload

systemctl restart docker

sudo systemctl enable docker

sudo systemctl start docker.service

sudo curl -L "https://github.com/docker/compose/releases/download/1.27.4/docker-compose-$(uname -s)-$(uname -m)" -o /usr/local/bin/docker-compose

sudo chmod +x /usr/local/bin/docker-compose

docker-compose --version

## Instalar Kibana

Ejecute los siguientes comandos de manera secuencial en el shell de Linux.

#Descargar la imagen:

docker pull docker.elastic.co/kibana/kibana:7.9.2

#Crear la ruta de carpetas y asignar los permisos

cd /usr/share

mkdir kibana

chmod g+rwx kibana

chgrp 0 kibana

cd kibana

mkdir config

chmod g+rwx config

chgrp 0 config

#crea el archivo de configuración personalizada

encryptionKeyKibana=$(openssl rand -base64 32)

encryptionKeySavedObjectsKibana=$(openssl rand -base64 32)

encryptionKeyReportingKibana=$(openssl rand -base64 32)

cat <<EOF | sudo tee /usr/share/kibana/config/kibana.yml

server.name: kibana

server.host: "0"

elasticsearch.hosts: [ "http://10.200.8.139:9200" ]

elasticsearch.username: "elasticsearch"

elasticsearch.password: "adminadmin"

xpack.security.encryptionKey: "${encryptionKeyKibana}"

xpack.reporting.kibanaServer.hostname: 0.0.0.0

xpack.encryptedSavedObjects.encryptionKey: "${encryptionKeySavedObjectsKibana}"

monitoring.cluster\_alerts.email\_notifications.email\_address: "sigsda11@minedu.gob.pe"

xpack.reporting.encryptionKey: "${encryptionKeyReportingKibana}"

EOF

#Ejecutar Kibana:

docker run -d -p 5601:5601 -v /usr/share/kibana/config/kibana.yml:/usr/share/kibana/config/kibana.yml --name kibana docker.elastic.co/kibana/kibana:7.9.2

En el script anterior debe reemplazar el host, puerto, usuario y clave (de elasticsearch) y un correo electrónico para notificaciones. Para ello modifique los atributos:

elasticsearch.hosts: [ "http://10.200.8.139:9200" ]

elasticsearch.username: "elasticsearch"

elasticsearch.password: "adminadmin

monitoring.cluster\_alerts.email\_notifications.email\_address: sigsda11@minedu.gob.pe