Manual de Instalación y Uso de ELK en Docker sobre Rocky Linux

# 1. Requisitos previos

- Máquina virtual con Rocky Linux instalado  
- Acceso a internet  
- Usuario con permisos de administrador (root o sudo)  
- Memoria mínima recomendada: 4GB RAM  
- Espacio en disco: al menos 20GB libres

# 2. Instalación de Docker y Docker Compose

Ejecutar los siguientes comandos para instalar Docker:  
sudo dnf install -y yum-utils  
sudo dnf config-manager --add-repo https://download.docker.com/linux/centos/docker-ce.repo  
sudo dnf install -y docker-ce docker-ce-cli containerd.io  
sudo systemctl enable docker --now  
  
Verificar que Docker funciona:  
docker --version  
  
Instalar Docker Compose:  
sudo curl -L "https://github.com/docker/compose/releases/download/v2.20.2/docker-compose-$(uname -s)-$(uname -m)" -o /usr/local/bin/docker-compose  
sudo chmod +x /usr/local/bin/docker-compose  
docker-compose --version

# 3. Configuración de ELK con docker-compose.yml

Crear un directorio de trabajo:  
mkdir elk-docker && cd elk-docker  
  
Crear el archivo docker-compose.yml con el siguiente contenido:

version: '3.8'  
services:  
 elasticsearch:  
 image: docker.elastic.co/elasticsearch/elasticsearch:8.14.0  
 container\_name: elasticsearch  
 environment:  
 - discovery.type=single-node

- ES\_JAVA\_OPTS=-Xms1g –Xmx1g

- xpack.security.enabled=false

unlimits:

memolock:

soft: -1

hard: -1

volumes:

- es\_data:/usr/share/elasticsearch/data  
 ports:  
 - "9200:9200"  
  
 logstash:  
 image: docker.elastic.co/logstash/logstash:8.14.0  
 container\_name: logstash

environment:  
 - LS\_JAVA\_OPTS=-Xms1g –Xmx1g

volumes:  
 - ./logstash.conf:/usr/share/logstash/pipeline/logstash.conf  
 ports:  
 - "514:514/udp" # syslog UDP

- "514:514/tcp" # syslog TCP

- "162:162/udp" # SNMP traps

- "5044:5044" # Beats (Filebeat, Winlogbeat, etc.)  
   
 depends\_on:  
 - elasticsearch  
  
 kibana:  
 image: docker.elastic.co/kibana/kibana:8.14.0  
 container\_name: kibana  
 environment:  
 - ELASTICSEARCH\_HOSTS=http://elasticsearch:9200

ports:  
 - "5601:5601"  
 depends\_on:  
 - elasticsearch

volumes:

es\_data:

driver: local

# 4. Solución de problemas de certificados (x509)

Si aparece el error TLS x509 al descargar imágenes, ejecutar:  
sudo mkdir -p /etc/docker  
echo '{ "insecure-registries":["docker.elastic.co"] }' | sudo tee /etc/docker/daemon.json  
sudo systemctl restart docker

# 5. Levantar los servicios

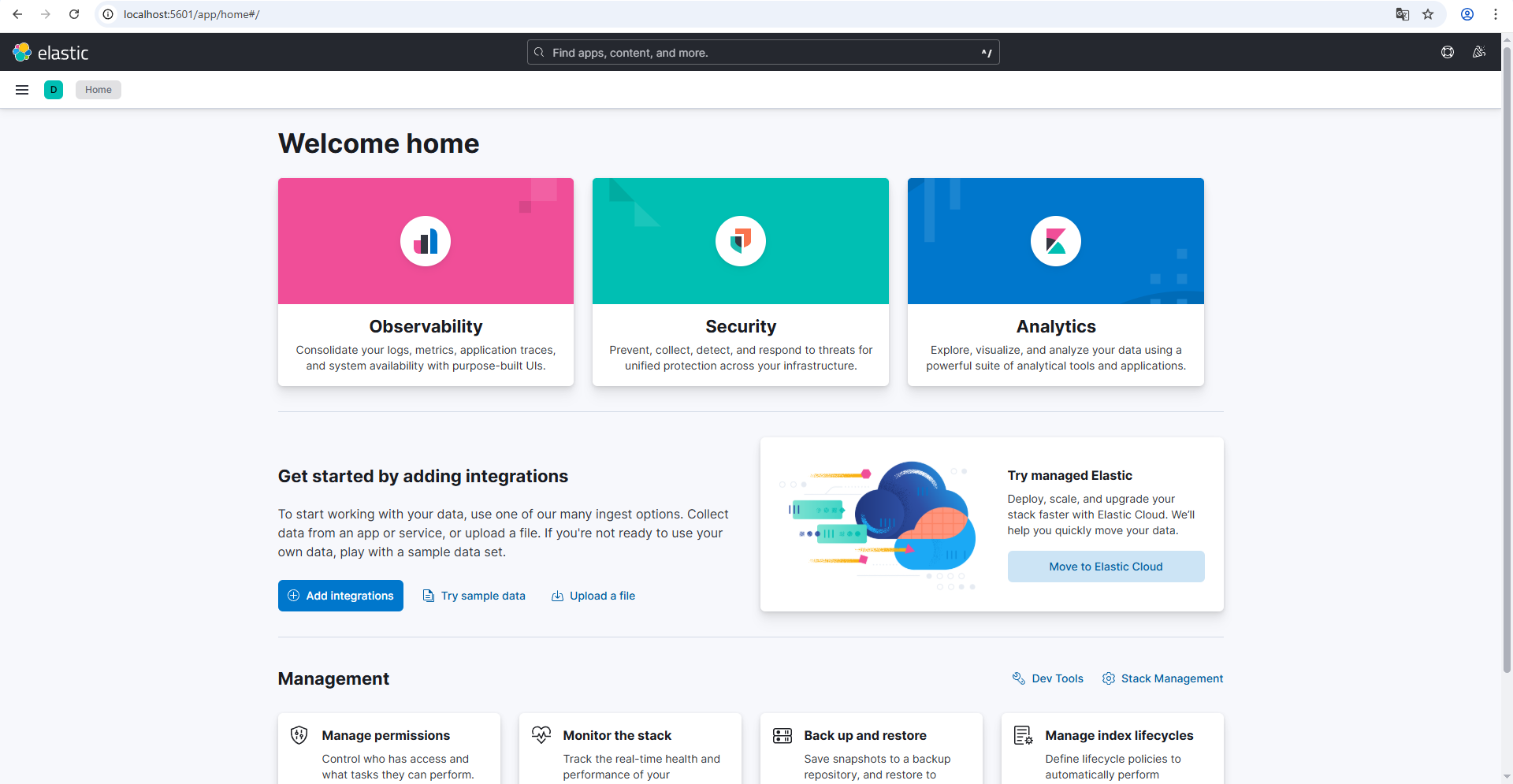
Ejecutar:  
docker compose up -d  
  
Verificar que los contenedores están corriendo:  
docker ps

# 6. Verificar Elasticsearch

Ejecutar en la terminal:  
curl **http://localhost:9200**  
  
Debe mostrar información del nodo con versión y cluster\_name.

# 7. Acceder a Kibana

Desde un navegador web, acceder a:  
http://localhost:5601



# 8. Comandos Docker

- docker ps → Lista los contenedores activos  
- docker compose up -d → Inicia los servicios en segundo plano  
- docker compose down → Apaga los servicios  
- docker logs <logstash> → Ver logs de un contenedor

