Instalación / Configuración ELK (Elasticsearch, Logstash, Kibabana)Stack

Angola Telecom

PROVISION

Escriba el Nº del Proyecto

Versión 0.1 | Nivel de Seguridad N2 - Restringido

Registro de Cambios

|  |  |  |  |
| --- | --- | --- | --- |
| **Versión** | **Fecha** | **Revisado** | **Resumen de los cambios producidos** |
| 1.0 | 23/02/2018 |  | Versión Inicial |

Versión de la Plantilla: 2.0

Índice

1 | Introducción 4

2 | Pasos previos 5

3 | Elasticsearch 6

3.1 Instalación Elasticsearch 6

3.2 Configuración 7

4 | Logstash 8

4.1 Instalación logstash 8

4.2 Configuración 10

5 | Kibana 11

5.1 Instalación kibana 11

5.2 Configuración 11

6 | Instalación con docker-compose 13

6.1 Instalar docker-compose 13

6.2 Instalar docker ELK Stack con docker-compose 13

# Introducción

En este documento se detallarán los pasos necesarios para la instalación y configuración del ELK Stack.

* Instalación y configuración de elasticsearch
* Instalación y configuración de logstash
* Instalación y configuración de kibana.

# Pasos previos

Crear un usuario **elkuser** para la ejecución

**sudo useradd -m elkuser**

Crear carpeta **elk** para contener los **logs** (/var/log/elk)

**cd /var/log**

**mkdir elk**

**chown –R /var/log/elk**

Las aplicaciones de elasticsearch y logstash requieren tener instalada la JDK de java en su versión 1.8.

* <http://www.oracle.com/technetwork/pt/java/javase/downloads/jdk8-downloads-2133151.html>

En este caso utilizamos la versión **jdk1.8.0\_111** y la situamos en la siguiente ruta: **/opt/provision/java/jdk1.8.0\_111/**

# Elasticsearch

## Instalación Elasticsearch

Descargar elasticsearch, en este caso utilizamos la versión: **6.2.2**

* <https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-6.2.2.zip>

**cd /opt/elk**

**wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-6.2.2.zip**

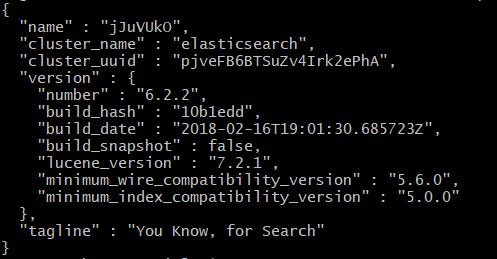
**unzip elasticsearch-6.2.2.zip**

Para arrancar elasticsearch:

**bin/elasticsearch**

Para probar que está funcionando:

**curl -XGET 'localhost:9200/?pretty'**



También se puede comprobar accediendo por el navegador:

* <http://localhost:9200/?pretty>

Guía de referencia de elascticsearch:

* <https://www.elastic.co/guide/en/elasticsearch/reference/current/index.html>

## Configuración

Para configurar elasticsearch como un servicio, se ha creado un fichero **elasticsearch.sh** que situaremos en la siguiente ruta**:**

* **[ruta\_base\_elasticsearch]/bin/init.d/** (opt/elk/elasticsearch-6.2.2/bin/init.d/elasticsearch.sh)

Dentro del fichero es necesario definir varias variables, a continuación, se muestra el valor que tendrán por defecto en él:

* ELASTICSEARCH\_HOME=**/opt/elk/elasticsearch-6.2.2**
* RUNAS=**elkuser**
* JAVA\_HOME=**"/opt/provision/java/jdk1.8.0\_111/"**
* PIDFILE=**/var/run/elasticsearch.pid**
* LOGFILE=**/var/log/elk/elasticsearch.log**

Es necesario dar permisos de ejecución sobre este fichero:

**chmod +x /opt/elk/elasticsearch-6.2.2/bin/init.d/elasticsearch.sh**

Crear un enlace simbólico al fichero en **/etc/init.d/elasticsearch:**

**ln -s /opt/elk/elasticsearch-6.2.2/bin/init.d/elasticsearch.sh /etc/init.d/elasticsearch**

Para arrancar, parar, reiniciar o comprobar el estado del servicio:

**service elasticsearch {start/stop/restart/status}**

# Logstash

## Instalación logstash

Descargar logstash, en este caso utilizamos la versión: **6.2.2**

* https://artifacts.elastic.co/downloads/logstash/logstash-6.2.2.tar.gz

**cd /opt/elk**

**wget https://artifacts.elastic.co/downloads/logstash/logstash-6.2.2.tar.gz**

**tar -xzf logstash-6.2.2.tar.gz**

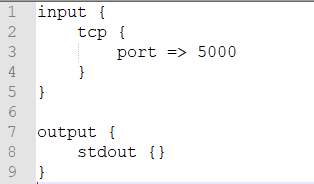
Para arrancar logstash

**bin/logstash**

Arrancar indicando un fichero de configuración.

**bin/logstash –f ./conf/logstash.conf**

Para probar que esta funcionado correctamente. Creamos fichero de configuración sencillo con lo siguiente: un input escuchando en el puerto 5000 y un output que escriba por consola.



Cuanto tengamos el logstash arrancado, nos conectamos desde otro terminal al puerto 5000.

**telnet 127.0.0.1 5000**

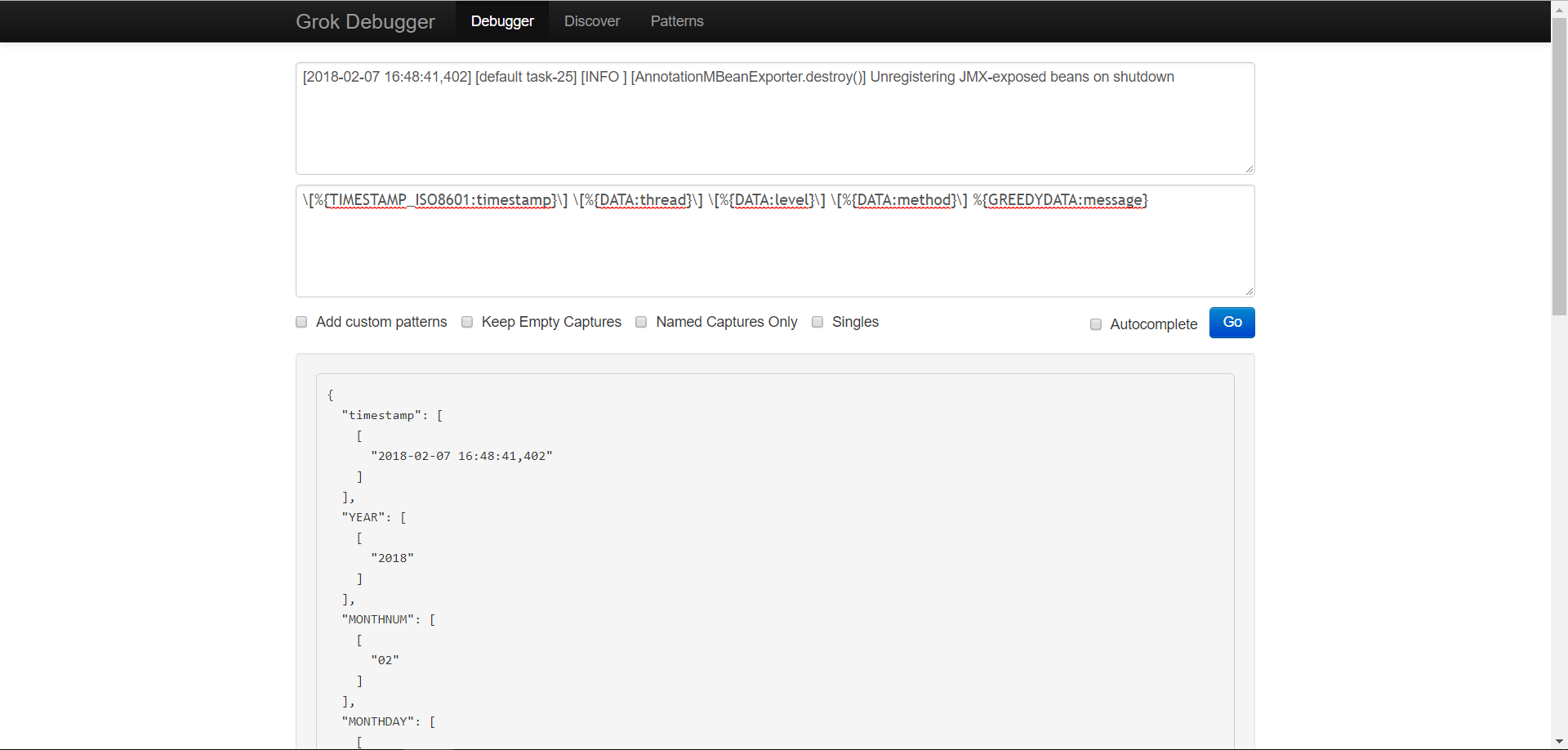
Ahora lo escribamos en este terminal debería capurarlo el logstash y mostrarlo por consola.

Guía de referencia de logstash:

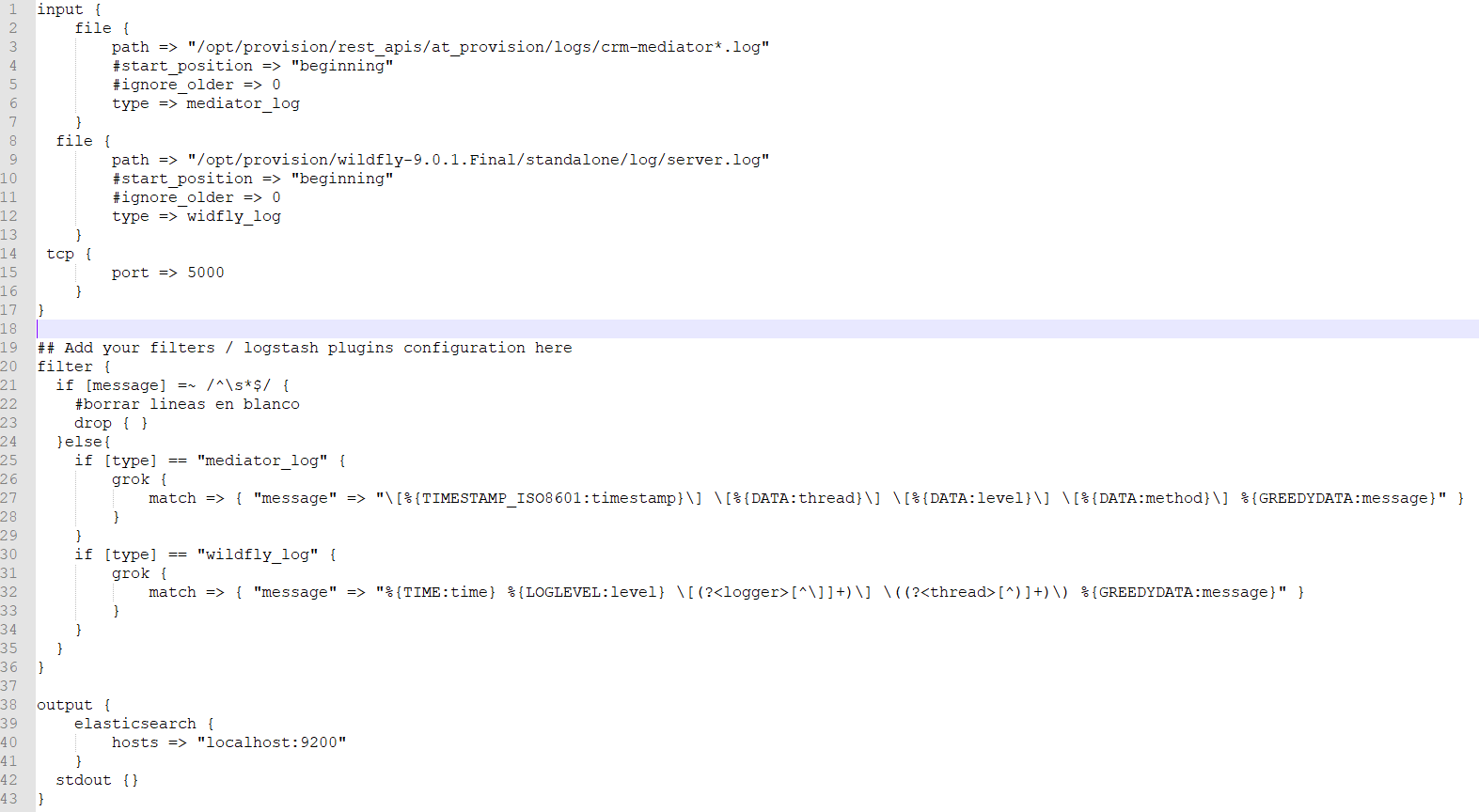
* <https://www.elastic.co/guide/en/logstash/current/index.html>

Utilidad web para la creación y comprobación de filtros grok

* <https://grokdebug.herokuapp.com/>



Ejemplo de fichero **logstash.conf** con dos inputs de fichero y dos filtros grok diferentes, para cada uno de los tipos de input definidos. El output en este caso va configurado a salida por consola y a elasticsearch.



Ejemplo de filtro grook para una línea de log sacada del log de crm-mediator:

* *[2018-02-07 16:48:41,402] [default task-25] [INFO ] [AnnotationMBeanExporter.destroy()] Unregistering JMX-exposed beans on shutdown*
* *pattern: \[%{TIMESTAMP\_ISO8601:timestamp}\] \[%{DATA:thread}\] \[%{DATA:level}\] \[%{DATA:method}\] %{GREEDYDATA:message}*

## Configuración

Para configurar logstash como un servicio, se ha creado un fichero **logstash.sh** que situaremos en la siguiente ruta**:**

* **[ruta\_base\_logstash]/bin/init.d/** (/opt/elk/logstash-6.2.2/bin/init.d/logstash.sh)

Dentro del fichero es necesario definir varias variables, a continuación, se muestra el valor que tendrán por defecto en él:

* LOGSTASH\_HOME=**/opt/elk/logstash-6.2.2**
* START=**"$LOGSTASH\_HOME/bin/logstash -f $LOGSTASH\_HOME/config/logstash.conf"**
* JAVA\_HOME=**"/opt/provision/java/jdk1.8.0\_111/"**
* JAVACMD=**"/opt/provision/java/jdk1.8.0\_111/bin/java"**
* PATH=**"/opt/provision/java/jdk1.8.0\_111/bin:$JAVA\_HOME:$PATH"**
* PIDFILE=**/var/run/logstash.pid**
* LOGFILE=**/var/log/elk/logstash.log**

Es necesario dar permisos de ejecución sobre este fichero:

**chmod +x /opt/elk/logstash-6.2.2/bin/init.d/logstash.sh**

Crear un enlace simbólico al fichero en **/etc/init.d/logstash**

**ln -s /opt/elk/logstash-6.2.2/bin/init.d/logstash.sh /etc/init.d/logstash**

Para arrancar, parar, reiniciar o comprobar el estado del servicio:

**service logstash {start/stop/restart/status}**

# Kibana

## Instalación kibana

Descargar kibana, en este caso utilizamos la versión: **6.2.2**

* <https://artifacts.elastic.co/downloads/kibana/kibana-6.2.2-linux-x86_64.tar.gz>

**Cd /opt/elk**

**wget https://artifacts.elastic.co/downloads/kibana/kibana-6.2.2-linux-x86\_64.tar.gz**

**tar -xzf kibana-6.2.2-linux-x86\_64.tar.gz**

Para arrancar kibana:

**bin/kibana**

Para probar que está funcionando accedemos a la siguiente url en el navegador

* http://localhost:5601

Guía de referencia de kibana:

* <https://www.elastic.co/guide/en/kibana/6.2/settings.html>

## Configuración

Para poder acceder desde fuera de la máquina, debemos editar el fichero **./conf/kibana.yml** y añadir la propiedad:

* server.host: "213.134.61.42"

Para configurar kibana como un servicio, se ha creado un fichero **kibana.sh** que situaremos en la siguiente ruta**:**

* **[ruta\_base\_kibana]/bin/init.d/** (opt/elk/kibana/bin/init.d/elasticsearch.sh)

Dentro del fichero es necesario definir varias variables, a continuación, se muestra el valor que tendrán por defecto en él:

* KIBANA\_HOME= **/opt/elk/kibana-6.2.2-linux-x86\_64**
* RUNAS=**root**
* PIDFILE=**/var/run/kibana.pid**
* LOGFILE=**/var/log/elk/kibana.log**

Es necesario dar permisos de ejecución sobre este fichero:

**chmod +x /opt/elk/kibana-6.2.2-linux-x86\_64/bin/init.d/kibana.sh**

Crear un enlace simbólico al fichero en **/etc/init.d/kibana:**

**ln -s /opt/elk/kibana-6.2.2-linux-x86\_64/bin/init.d/kibana.sh /etc/init.d/kibana**

Para arrancar, parar, reiniciar o comprobar el estado del servicio:

**service kibana {start/stop/restart/status}**

# Instalación con docker-compose

## Instalar docker-compose

Descargar la última versión de docker-compose:

**sudo curl -L https://github.com/docker/compose/releases/download/1.19.0/docker-compose-`uname -s`-`uname -m` -o /usr/local/bin/docker-compose**

Dar permisos de ejecución sobre el directorio **/usr/local/bin/docker-compose:**

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

Comprobar que se ha instalado correctamente:

**docker-compose --version**

Documentación acerca de docker-compose:

* <https://docs.docker.com/compose/overview/>
* <https://docs.docker.com/compose/reference/>

## Instalar docker ELK Stack con docker-compose

Página de referencia:

* <https://github.com/deviantony/docker-elk>

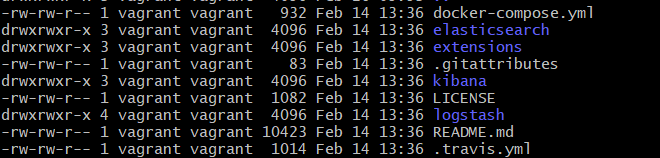
Descargar y descomprimir el zip con la última versión de elk-docker:

**wget https://github.com/deviantony/docker-elk/archive/master.zip**

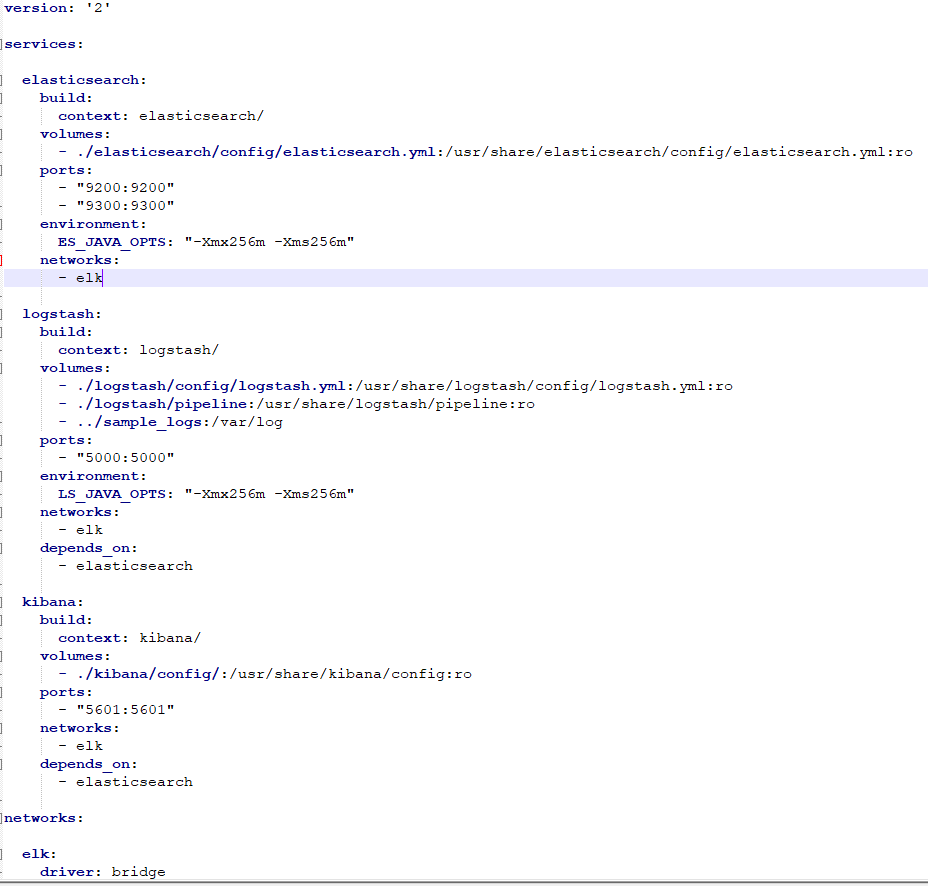
**unzip master.zip**

**cd docker-elk-master**

Una vez descomprimido, dentro de la carpeta docker-elk-master tendremos lo siguiente:



En el fichero **docker-compose.yml** esta la configuración de cada uno de los contenedores a arrancar (con el mapeo de puertos, volúmenes compartidos, entorno y dependencias)

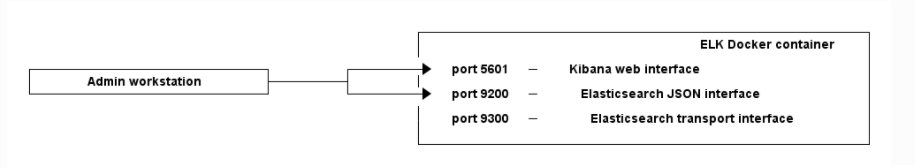


Cada una de las aplicaciones tiene una carpeta en donde se define la configuración particular de la misma:

* /elasticsearch
  + DockerFile
  + /config/elasticsearch.yml
* /logstash
  + DockerFile
  + /config/logstash.yml
  + /config/logstash.con
* /kibana
  + DockerFile
  + /config/kibana.yml

Por defecto las aplicaciones utilizan los siguientes puertos:

* 5000: Logstash TCP input.
* 9200: Elasticsearch HTTP
* 9300: Elasticsearch TCP transport
* 5601: Kibana



Arrancar los contenedores:

**docker-compose up**

Arrancar los contenedores en segundo plano:

**docker-compose up - d**

Parar los contenedores:

**docker-compose stop**