ELK: Elasticserch (instalación y configuración)

1.2_instalacion_y_configuracion.pdf

- matriz OS/JVMs: https://www.elastic.co/support/matrix/show_os
- oracle JVM 1.8.0_131 o superior
- recomendable 64 bits
- la misma versión en todos los nodos

instalación

- Java:

```
sudo add-apt-repository ppa:webupd8team/java # obsoleto?
sudo apt update
sudo apt install oracle-java8-installer
```

/etc/environment

```
...
JAVA_HOME="/usr/lib/jvm/java-8-oracle"
```

- `source /etc/environment`
- Elasticsearch:

```
wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key
add -
sudo apt isntall apt-transport-https
echo "deb https://artifacts.elastic.co/packages/5.x/apt stable main" | sudo
tee -a /etc/apt/sources.list.d/elastic-5.x.list
sudo apt update && sudo apt install elasticsearch
```

```
update-rc.d elasticsearch defaults 95 10
service elasticsearch status
```

systemd

```
sudo systemctl daemon-reload
sudo systemctl enable elasticsearch.service
sudo systemctl start elasticsearch.service
```

</code>

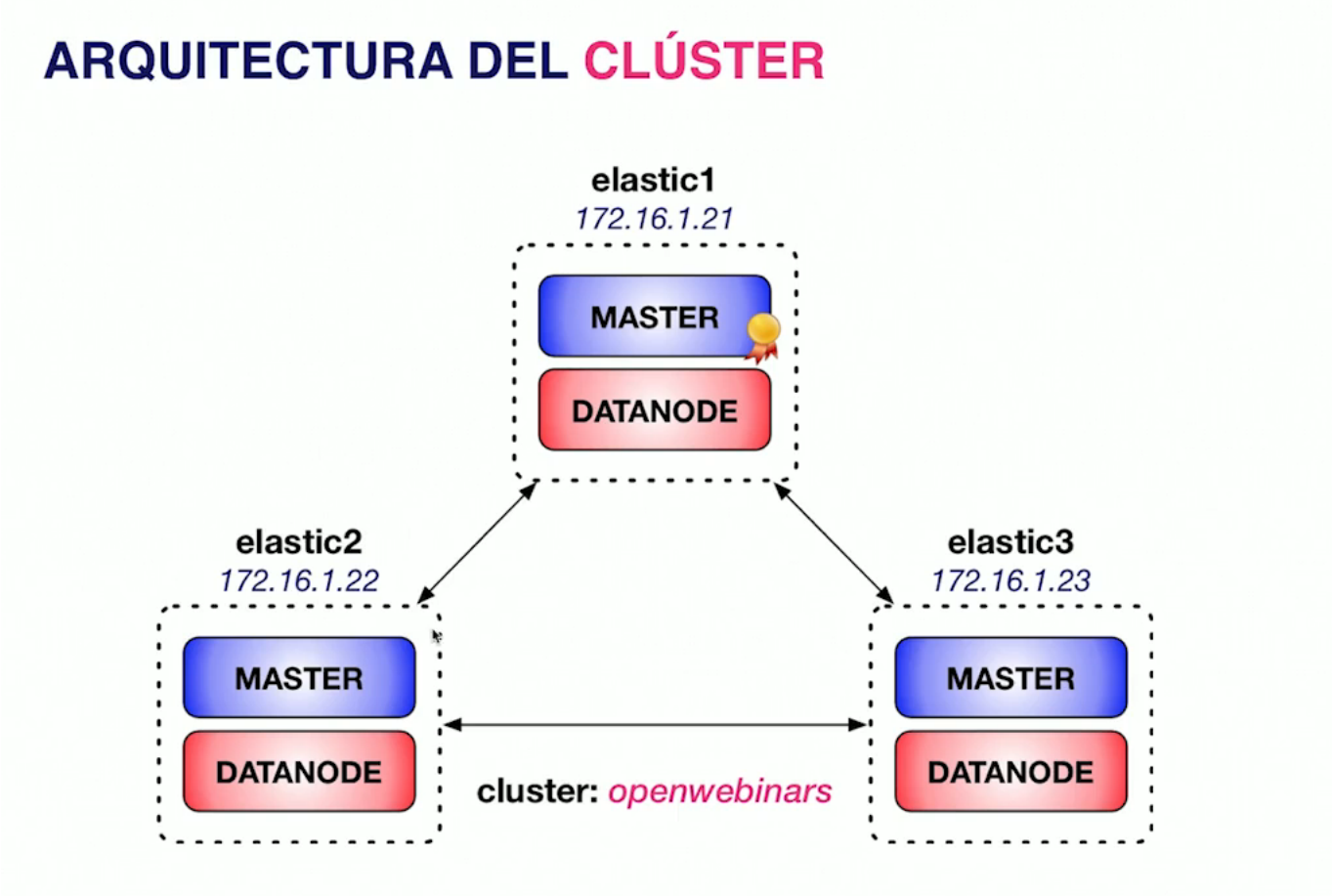
- rutas:
  - HOME: **/usr/share/elasticsearch**
  - BIN: **/usr/share/elasticsearch/bin**
  - CONF: **/etc/elasticsearch**
  - ENV: **/etc/default/elasticsearch**
  - DATA: **/var/lib/elasticsearch**

    - LOGS: **/var/log/elasticsearch**
    - PLUGINS: **/usr/share/elasticsearch/plugins**

```
curl -XGET http://localhost:9200
```

configuración

- JVM Options (reserva memoria):
    - elasticsearch.yml: `bootstrap.memory_lock=true`
    - jvm.options: `-Xms2g, -Xmx2G` (aproximadamente la mitad de la memoria)
    - /etc/default/elasticsearch: `MAX_LOCKED_MEMORY=unlimited` ← cogerá la máxima indicada en el parámetro anterior
    - /usr/lib/systemd/system/elasticsearch.service: `LimitMEMLOCK=infinity`
        - `sudo systemctl daemon-reload`
    - deshabilitar SWAP (en /etc/fstab)
- Paths (/etc/elasticsearch/elasticsearch.yml)
    - `path.data=/var/lib/elasticsearch`
        - podría haber múltiples rutas, se usarán todas.
        - Los datos de un shard se almacena en la misma ruta
    - `path.logs=/var/log/elasticsearch`
    - `cluster.name=elasticsearch`
    - `node.name=<7 primeros caracteres del UUID (generado aleatoriamente)>`
        - también se podría usar el nombre de la máquina (${HOSTNAME})
    - `network.host=127.0.0.1`
        - para cluster, añadir IP «pública»
        - varias direcciones: `[«IP»,«IP»]` → `[«127.0.0.1»,«192.168.100.10»]`
    - `discovery.zen.ping.unicast.hosts`: lista de nodos.
        - Por defecto usará desde el puerto 9300 a 9305 intentando conectar con otros nodos (auto-clustering) → `[«IP_nodo1»,«IP_nodo2»,«IP_nodo3»]`
    - `discovery.zen.minimum_master_nodes`
        - no configurado correctamente, puede provocar un split brain (separación del cluster)
        - (master_elegible_nodes/2)+1
    - `curl -XGET http://localhost:9200/_cluster/health?pretty`



tips

- VMs con 2 interfaces (para trabajar, otra interna)
- asignar las mismas IPs a las mismas máquinas