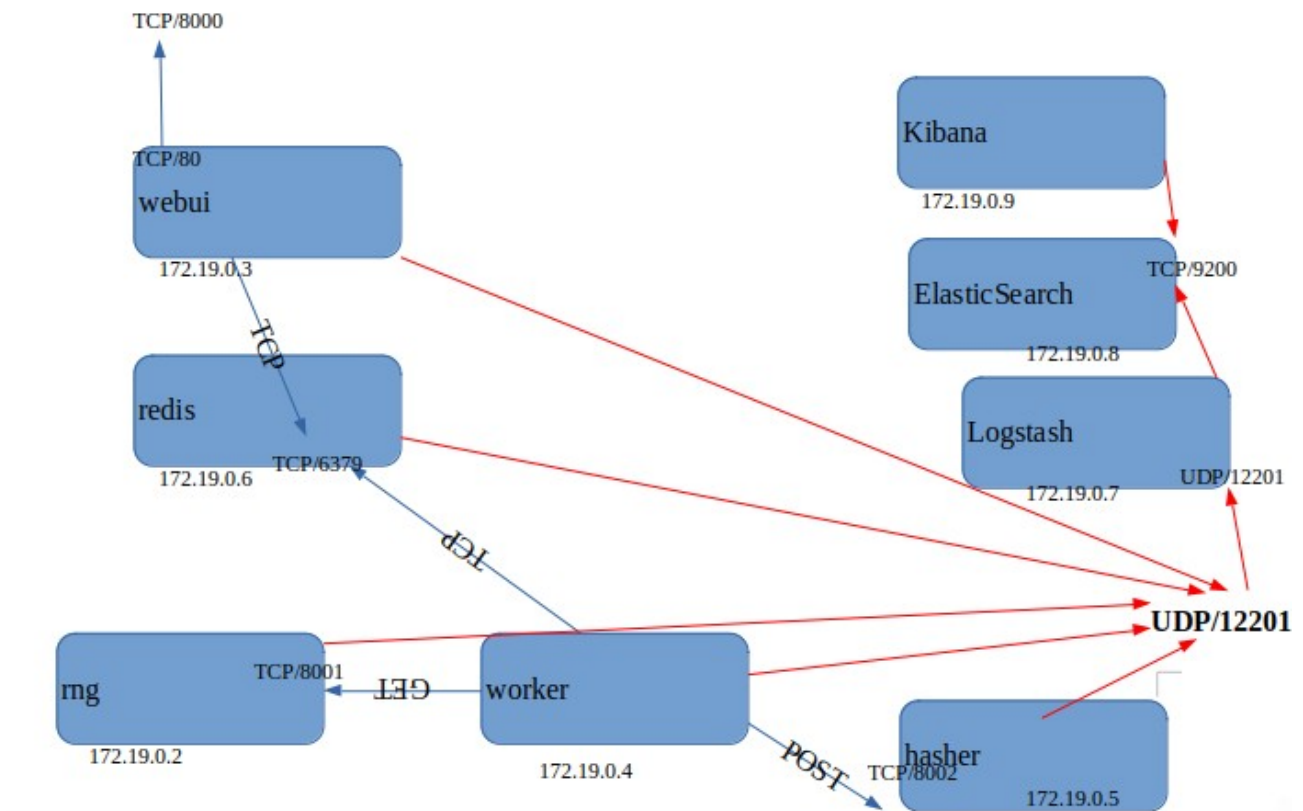


## Lab11 – ELK

[https://github.com/brahimhamdi/dockercoins\\_logs](https://github.com/brahimhamdi/dockercoins_logs)



```
brahim@Training:/tmp$ git clone https://github.com/brahimhamdi/dockercoins_logs
Clonage dans 'dockercoins_logs'...
remote: Enumerating objects: 24, done.
remote: Counting objects: 100% (24/24), done.
remote: Compressing objects: 100% (22/22), done.
remote: Total 24 (delta 2), reused 24 (delta 2), pack-reused 0
Réception d'objets: 100% (24/24), 108.64 Kio | 639.00 Kio/s, fait.
Résolution des deltas: 100% (2/2), fait.
brahim@Training:/tmp$ cd dockercoins_logs/
brahim@Training:/tmp/dockercoins_logs$
```

```
brahim@Training:/tmp/dockercoins_logs$ tree
.
├── docker-compose.yml
├── hasher
│   ├── Dockerfile
│   └── hasher.rb
├── rng
│   ├── Dockerfile
│   └── rng.py
├── webui
│   ├── Dockerfile
│   └── files
│       ├── d3.min.js
│       ├── index.html
│       ├── jquery-1.11.3.min.js
│       ├── jquery.js
│       ├── rickshaw.min.css
│       └── rickshaw.min.js
└── webui.js

5 directories, 15 files
brahim@Training:/tmp/dockercoins_logs$ vim docker-compose.yml
```

```
brahim@Training:/tmp/dockercoins_logs$ docker-compose up -d
Creating network "dockercoins_logs_default" with the default driver
Creating dockercoins_logs_hasher_1          ... done
Creating dockercoins_logs_webui_1           ... done
Creating dockercoins_logs_kibana_1          ... done
Creating dockercoins_logs_elasticsearch_1   ... done
Creating dockercoins_logs_rng_1             ... done
Creating dockercoins_logs_worker_1         ... done
Creating dockercoins_logs_redis_1           ... done
Creating dockercoins_logs_logstash_1       ... done
brahim@Training:/tmp/dockercoins_logs$ docker-compose ps
```

```
brahim@Training:/tmp/dockercoins_logs$ docker-compose ps
```

Name	Command	State	Ports
dockercoins_logs_elasticsearch_1	/usr/local/bin/docker-entr ...	Exit 78	
dockercoins_logs_hasher_1	ruby hasher.rb	Up (unhealthy)	80/tcp, 0.0.0.0:8002->8002/tcp,:::8002->8002/tcp
dockercoins_logs_kibana_1	/usr/local/bin/kibana-docker	Up	0.0.0.0:5601->5601/tcp,:::5601->5601/tcp
dockercoins_logs_logstash_1	/usr/local/bin/docker-entr ...	Up	0.0.0.0:12201->12201/udp,:::12201->12201/udp, 0.0.0.0:5044->5044/tcp,:::5044->5044/tcp, 9600/tcp
dockercoins_logs_redis_1	docker-entrypoint.sh redis ...	Up	6379/tcp
dockercoins_logs_rng_1	python rng.py	Up	80/tcp, 0.0.0.0:8001->8001/tcp,:::8001->8001/tcp
dockercoins_logs_webui_1	node webui.js	Up	0.0.0.0:8000->80/tcp,:::8000->80/tcp
dockercoins_logs_worker_1	python worker.py	Up	

```
brahim@Training:/tmp/dockercoins_logs$ docker-compose logs elasticsearch | grep ERROR -A3
elasticsearch_1 | ERROR: [1] bootstrap checks failed
elasticsearch_1 | [1]: max virtual memory areas vm.max_map_count [65530] is too low, increase to at least [262144]
elasticsearch_1 | [2023-06-21T09:07:33,482][INFO ][o.e.n.Node ] [Q-M50-b] stopping ...
elasticsearch_1 | [2023-06-21T09:07:33,520][INFO ][o.e.n.Node ] [Q-M50-b] stopped
brahim@Training:/tmp/dockercoins_logs$
```

```
brahim@Training:/tmp/dockercoins_logs$ sudo sysctl -w vm.max_map_count=262144
vm.max_map_count = 262144
```

```
brahim@Training:/tmp/dockercoins_logs$ docker-compose ps elasticsearch
```

Name	Command	State	Ports
dockercoins_logs_elasticsearch_1	/usr/local/bin/docker-entr ...	Exit 78	

```
brahim@Training:/tmp/dockercoins_logs$
brahim@Training:/tmp/dockercoins_logs$ docker-compose start elasticsearch
Starting elasticsearch ... done
brahim@Training:/tmp/dockercoins_logs$ docker-compose ps elasticsearch
```

Name	Command	State	Ports
dockercoins_logs_elasticsearch_1	/usr/local/bin/docker-entr ...	Up	0.0.0.0:9200->9200/tcp,:::9200->9200/tcp, 9300/tcp

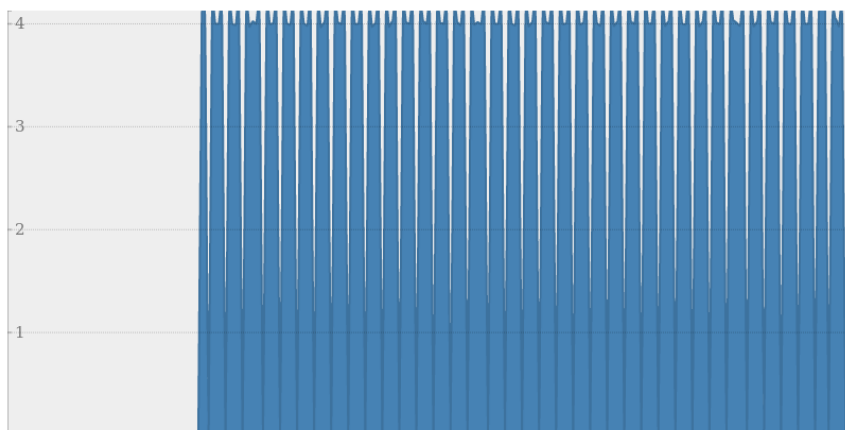
```
brahim@Training:/tmp/dockercoins_logs$
brahim@Training:/tmp/dockercoins_logs$ docker-compose ps elasticsearch
```

Name	Command	State	Ports
dockercoins_logs_elasticsearch_1	/usr/local/bin/docker-entr ...	Up	0.0.0.0:9200->9200/tcp,:::9200->9200/tcp, 9300/tcp

```
brahim@Training:/tmp/dockercoins_logs$
```

← → ↺ 🏠 localhost:8000/index.html

## DockerCoin Miner WebUI



Current mining speed: ~4.0 hashes/second ([Tweet this!](#))

← → ↻ 🏠 localhost:5601/app/kibana#/management/kibana/indices/54f39030-1015-11ee-8c67-7d233b38915b?\_g= ⭐

**kibana**

- Discover
- Visualize
- Dashboard
- Timelion
- Canvas
- Maps
- Machine Learning
- Infrastructure
- Logs
- APM
- Uptime

🔔 Help us improve the Elastic Stack by providing usage statistics for basic features. We will not share this data outside of Elastic. [Read more](#)

**Elasticsearch** Create index pat...

- Index Management
- Index Lifecycle Policies
- Rollup Jobs
- Cross Cluster Replication
- Remote Clusters
- License Management
- 7.0 Upgrade Assistant

**Kibana**

- [Index Patterns](#)
- Saved Objects
- Spaces
- Reporting
- Advanced Settings

★ **logstash-\*** ★ ↺ 🗑

**Time Filter field name: @timestamp**

This page lists every field in the **logstash-\*** index and the field's associated core type as recorded by Elasticsearch. To change a field type, use the Elasticsearch [Mapping API](#) 📄

Fields (32) | Scripted fields (0) | Source filters (0)

🔍 Filter All field types ▾

Name	Type	Format	Search...	Aggreg...	Excluded
@timestamp 🕒	date		●	●	✎
@version	string		●	●	✎

```

brahim@Training: /sauvegarde/formations/forma... x      brahim@Training: /tmp/dockercoins_logs x
brahim@Training: /tmp/dockercoins_logs$
brahim@Training: /tmp/dockercoins_logs$
brahim@Training: /tmp/dockercoins_logs$ docker-compose scale worker=100
WARNING: The scale command is deprecated. Use the up command with the --scale flag instead.
Creating dockercoins_logs_worker_2 ...
Creating dockercoins_logs_worker_3 ...

```

← → ↻ 🏠 localhost:5601/app/kibana#/discover?\_g=()&\_a=(columns:(!\_source),index:'54f39030-1015-11ee-8c67-7d233b38915b') ⭐

**kibana**

- Discover
- Visualize
- Dashboard
- Timelion
- Canvas
- Maps
- Machine Learning
- Infrastructure
- Logs
- APM
- Uptime
- Dev Tools

🔔 Help us improve the Elastic Stack by providing usage statistics for basic features. We will not share this data outside of Elastic. [Read more](#)

**14,046 hits** New Save Open Share Inspect 🔁 Auto-refresh ⏪ Last 15 minutes ⏩

🔍 Search... (e.g. status:200 AND extension:PHP) Options 🔄 Refresh

**logstash-\*** +

**Selected fields**

- ? \_source

**Available fields** ⚙

- @timestamp
- @version
- \_id
- \_index
- \_score
- #\_score
- \_type
- command

June 21st 2023, 11:14:21.678 - June 21st 2023, 11:29:21.678 — Auto ▾

**Time** 📄 **\_source**

▶ June 21st 2023, 11:29:14.294

```

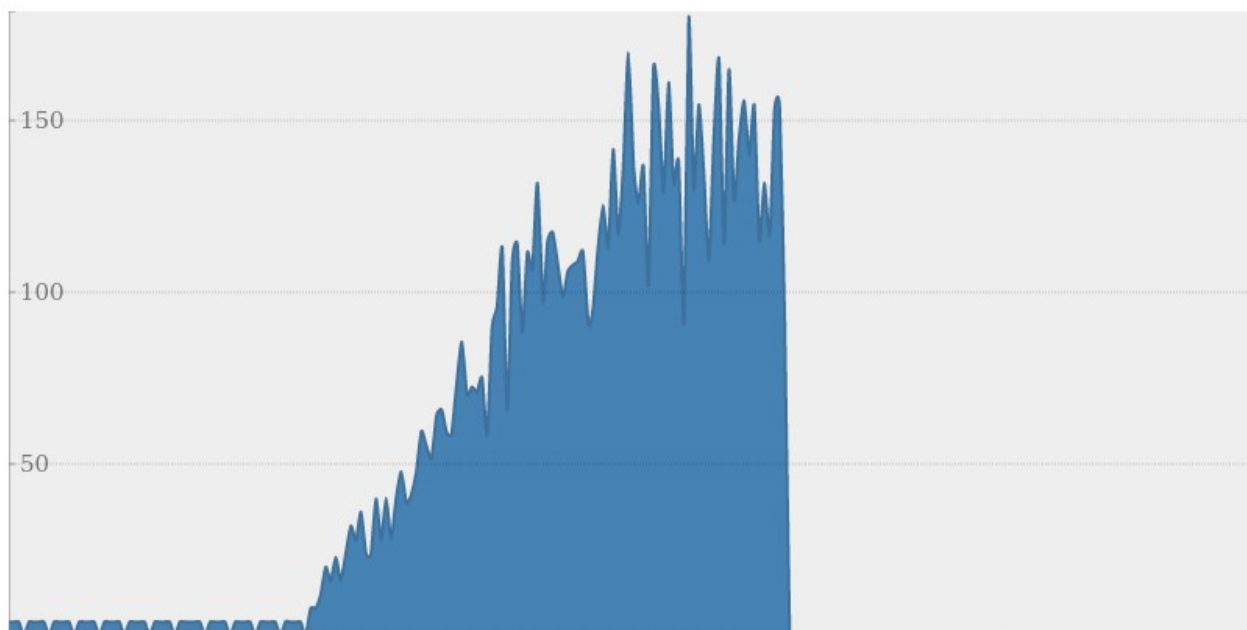
version: 1.1 host: Training command: ruby hasher.rb source_host: 172.18.0.1
message: 172.18.0.52 - - [21/Jun/2023:09:29:14 +0000] "POST / HTTP/1.1" 200 64 0.1018
container_id: e77413bc2fc757a1698ef8936cd8cf8293940e83b9a2660d65eeb57a628375

```

```
brahim@Training:/tmp/dockercoins_logs$ docker-compose ps hasher
-----
Name                  Command                  State      Ports
-----
dockercoins_logs_hasher_1  ruby hasher.rb          Exit 1
brahim@Training:/tmp/dockercoins_logs$
```

← → ↻ 🏠 localhost:8000/index.html

## DockerCoin Miner WebUI



**Current mining speed: ~0.0 hashes/second** ([Tweet this!](#))