



UNIVERSIDADE
LUSÓFONA

Trabalho Final de Curso

Instalação do OpenCTI numa VM de Testes

Miguel Lourenço

Vasco Pereira

06/12/2024

www.ulusofona.pt

Índice

Índice.....	2
Lista de Figuras	3
Resumo.....	4
Instalação do Docker.....	5
Instalação do Repositório git.....	7
Configuração do OpenCTI.....	8
Iniciação do Docker com o OpenCTI	11
Abertura do OpenCTI	13
Bibliografia	14

Lista de Figuras

Figura 1	5
Figura 2	6
Figura 3	7
Figura 4	8
Figura 5	9
Figura 6	9
Figura 7	10
Figura 8	11
Figura 9	12
Figura 10	13
Figura 11	13

Resumo

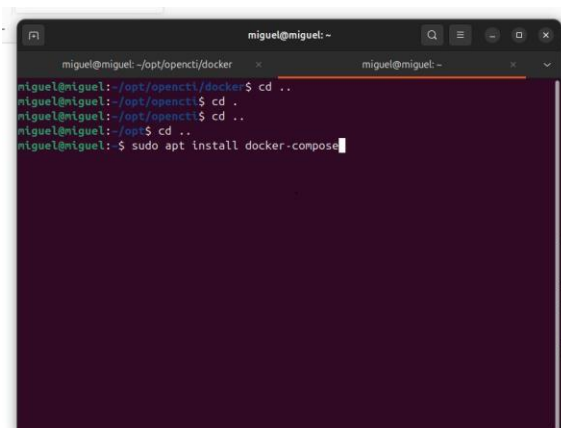
O objetivo desta tarefa é proceder à instalação do OpenCTI numa máquina virtual (VM), com o intuito de configurar uma plataforma de *threat intelligence* que permita a ingestão e análise de dados. O processo de instalação será realizado com base na documentação oficial do OpenCTI, disponível no guia [OpenCTI]. O resultado esperado é uma instalação funcional do OpenCTI, acessível através da porta configurada na VM e com todos os serviços necessários a operar corretamente.

Instalação do Docker

Começamos por instalar o Docker na nossa máquina: **sudo apt install docker-compose**.

Figura 1

Instalação do Docker-compose.

A terminal window with a dark purple background and white text. The window title is 'miguel@miguel: ~'. The terminal shows a series of commands and their outputs. The first command is 'cd ..' which changes the directory to '/opt/opencti/docker'. The second command is 'cd .' which changes the directory to '/opt/opencti'. The third command is 'cd ..' which changes the directory to '/opt'. The fourth command is 'cd ..' which changes the directory to the root. The final command is 'sudo apt install docker-compose' which is being typed at the prompt. The terminal output shows the directory changes and the command being executed.

```
miguel@miguel: ~/opt/opencti/docker$ cd ..
miguel@miguel: ~/opt/opencti$ cd .
miguel@miguel: ~/opt/opencti$ cd ..
miguel@miguel: ~/opt$ cd ..
miguel@miguel: ~$ sudo apt install docker-compose
```

Após a instalação bem-sucedida do Docker, vamos agora criar o caminho de pastas até ao local onde iremos clonar o repositório Git da OpenCTI, utilizando os comandos **sudo mkdir opt** e **sudo mkdir opencti**.

Figura 2

Criação das pastas para clonar o repositório do Git.

```
migueld@migueld:~$ cd ..
migueld@migueld:~$ cd ..
migueld@migueld:~$ cd ..
migueld@migueld:~$ cd ..
migueld@migueld:~$ cd /opt/openciti/
migueld@migueld:~$ ls -l
total 4
drwxr-xr-x 3 root root 4096 Nov 20 13:49 docker
migueld@migueld:~$ cd docker
migueld@migueld:~/docker$ sudo subl .env
[sudo] senha para migueld:
migueld@migueld:~/docker$ sudo mkdir openciti
mkdir: cannot create directory 'openciti': No such file or directory
```

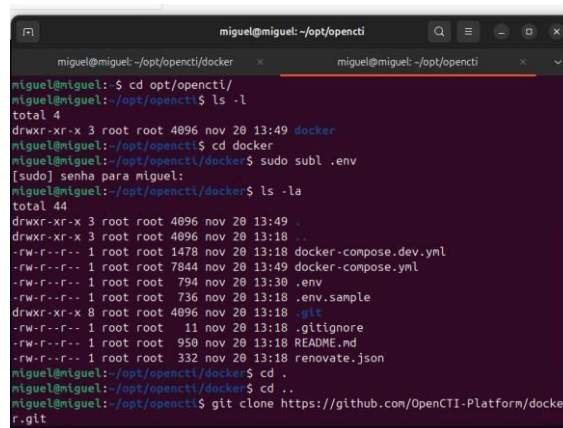
[illegible]

Instalação do Repositório git

Depois de criar o caminho, copiamos o repositório Git com o comando **git clone** <https://github.com/OpenCTI-Platform/docker.git> e, em seguida, acedemos à pasta com o comando **cd Docker**

Figura 3

Clonar o guit do openCTI.



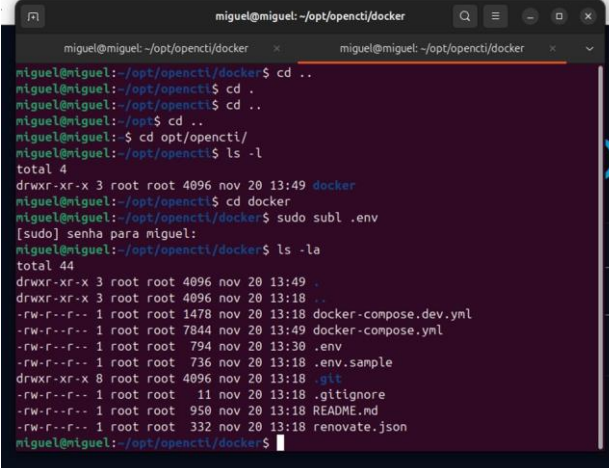
```
miguel@miguel: ~/opt/opencti
miguel@miguel:~/opt/opencti/docker$ ls -l
total 4
drwxr-xr-x 3 root root 4096 nov 20 13:49 docker
miguel@miguel:~/opt/opencti/docker$ sudo subl .env
[sudo] senha para miguel:
miguel@miguel:~/opt/opencti/docker$ ls -la
total 44
drwxr-xr-x 3 root root 4096 nov 20 13:49 .
drwxr-xr-x 3 root root 4096 nov 20 13:18 ..
-rw-r--r-- 1 root root 1478 nov 20 13:18 docker-compose.dev.yml
-rw-r--r-- 1 root root 7844 nov 20 13:49 docker-compose.yml
-rw-r--r-- 1 root root 794 nov 20 13:30 .env
-rw-r--r-- 1 root root 736 nov 20 13:18 .env.sample
drwxr-xr-x 8 root root 4096 nov 20 13:18 .git
-rw-r--r-- 1 root root 11 nov 20 13:18 .gitignore
-rw-r--r-- 1 root root 950 nov 20 13:18 README.md
-rw-r--r-- 1 root root 332 nov 20 13:18 renovate.json
miguel@miguel:~/opt/opencti/docker$ cd .
miguel@miguel:~/opt/opencti/docker$ cd ..
miguel@miguel:~/opt/opencti$ git clone https://github.com/OpenCTI-Platform/docker.git
```

Configuração do OpenCTI

Utilizando o comando `ls -la` para verificar todos os ficheiros presentes, observamos um `env.sample`, que contém um exemplo do ficheiro que teremos de configurar para que a instalação seja bem-sucedida.

Figura 4

Verificar se o `env.sample` esta presente.



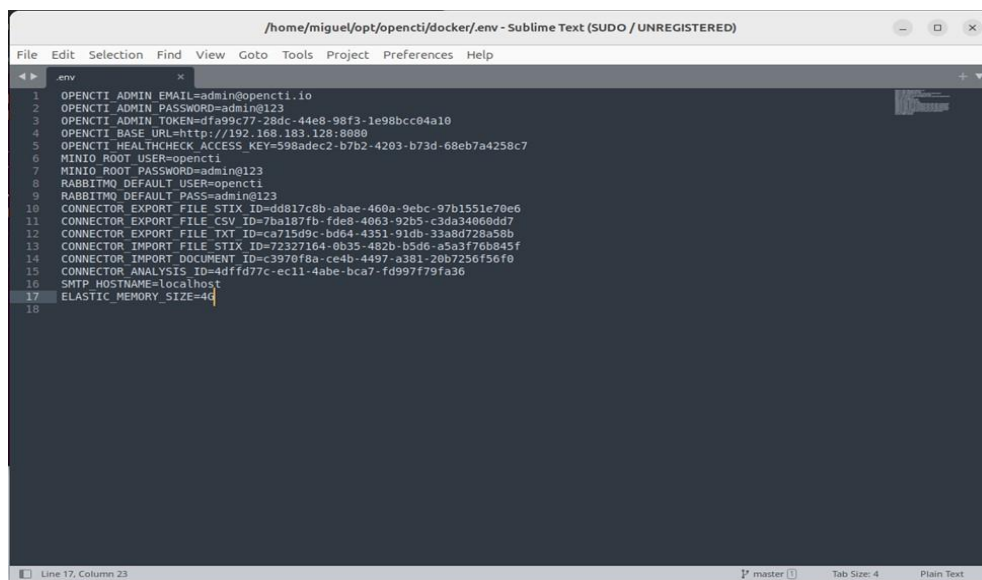
```
miguel@miguel: ~/opt/opencti/docker
miguel@miguel: ~/opt/opencti/docker
miguel@miguel: ~/opt/opencti/docker$ cd ..
miguel@miguel: ~/opt/opencti$ cd .
miguel@miguel: ~/opt/opencti$ cd ..
miguel@miguel: ~/opt$ cd ..
miguel@miguel: $ cd opt/opencti/
miguel@miguel: ~/opt/opencti$ ls -l
total 4
drwxr-xr-x 3 root root 4096 nov 20 13:49 docker
miguel@miguel: ~/opt/opencti$ cd docker
miguel@miguel: ~/opt/opencti/docker$ sudo subl .env
[sudo] senha para miguel:
miguel@miguel: ~/opt/opencti/docker$ ls -la
total 44
drwxr-xr-x 3 root root 4096 nov 20 13:49 .
drwxr-xr-x 3 root root 4096 nov 20 13:18 ..
-rw-r--r-- 1 root root 1478 nov 20 13:18 docker-compose.dev.yml
-rw-r--r-- 1 root root 7844 nov 20 13:49 docker-compose.yml
-rw-r--r-- 1 root root 794 nov 20 13:30 .env
-rw-r--r-- 1 root root 736 nov 20 13:18 .env.sample
drwxr-xr-x 8 root root 4096 nov 20 13:18 .git
-rw-r--r-- 1 root root 11 nov 20 13:18 .gitignore
-rw-r--r-- 1 root root 950 nov 20 13:18 README.md
-rw-r--r-- 1 root root 332 nov 20 13:18 renovate.json
miguel@miguel: ~/opt/opencti/docker$
```

Passamos, então, a fazer uma cópia do ficheiro, renomeando-o para `env`, que será o ficheiro que o sistema irá utilizar na configuração.

Iremos, então, configurar todas as linhas que contiverem “changeme”. No atributo TOKEN, devemos consultar [uuidv4] e copiar o token que aparece. Após isso, devemos atualizar a página (refresh) disponível nesse mesmo site e colar o novo token no campo HEALTHCHECK_ACCESS_KEY, substituindo os restantes parâmetros "changeme", de forma a ficar semelhante à **Erro! A origem da referência não foi encontrada..** Após concluir esta configuração, devemos guardar as alterações do ficheiro e fechá-lo.

Figura 7

Configurações do OpenCTI.



```
1 OPENCTI_ADMIN_EMAIL=admin@opencti.io
2 OPENCTI_ADMIN_PASSWORD=admin@123
3 OPENCTI_ADMIN_TOKEN=dfa99c77-28dc-44e8-98f3-1e98bcc04a10
4 OPENCTI_BASE_URL=http://192.168.183.128:8080
5 OPENCTI_HEALTHCHECK_ACCESS_KEY=598adec2-b7b2-4203-b73d-68eb7a4258c7
6 MINIO_ROOT_USER=opencti
7 MINIO_ROOT_PASSWORD=admin@123
8 RABBITMQ_DEFAULT_USER=opencti
9 RABBITMQ_DEFAULT_PASS=admin@123
10 CONNECTOR_EXPORT_FILE_STIX_ID=dd017c8b-abae-460a-9ebc-97b1551e70e6
11 CONNECTOR_EXPORT_FILE_CSV_ID=7ba187fb-fde8-4063-92b5-c3da34060dd7
12 CONNECTOR_EXPORT_FILE_TXT_ID=ca715d9c-bd64-4351-91db-33a8d728a58b
13 CONNECTOR_IMPORT_FILE_STIX_ID=72327164-0b35-482b-b5d6-a5a3f76b845f
14 CONNECTOR_IMPORT_DOCUMENT_ID=c3976f8a-ce4b-4497-a381-20b7256f56f0
15 CONNECTOR_ANALYSIS_ID=4dffd77c-ec11-4abe-bca7-fd997f79fa36
16 SMTP_HOSTNAME=localhost
17 ELASTIC_MEMORY_SIZE=4g
18
```

Iniciação do Docker com o OpenCTI

Após a configuração, iremos iniciar o serviço Docker utilizando o comando **sudo systemctl start docker.service** e, para verificar se está operacional, utilizamos o comando **sudo systemctl status docker.service**.

Figura 8

Verificar o funcionamento do Docker.

```
-rw-r--r-- 1 root root 950 nov 20 13:18 README.md
-rw-r--r-- 1 root root 332 nov 20 13:18 renovate.json
miguel@miguel:~/opt/opencti/docker$ sudo systemctl start docker.service
[sudo] senha para miguel:
miguel@miguel:~/opt/opencti/docker$ sudo systemctl status docker.service
● docker.service - Docker Application Container Engine
   Loaded: loaded (/usr/lib/systemd/system/docker.service; enabled; preset: e>
   Active: active (running) since Thu 2024-11-21 08:58:31 WET; 17min ago
   TriggeredBy: ● docker.socket
     Docs: https://docs.docker.com
    Main PID: 2067 (dockerd)
```

Para terminar a instalação, iremos, então, executar o comando **sudo docker-compose up -d**, que, da primeira vez, poderá demorar algum tempo. Após a conclusão, a instalação estará finalizada.

Figura 9

Utilização do Docker-compose up para iniciar o OpenCTI.

```
sudo: docker compose: comando não encontrado
miguel@miguel:~/opt/opencti/docker$ sudo docker-compose up -d
docker_rabbitmq_1 is up-to-date
docker_redis_1 is up-to-date
docker_minio_1 is up-to-date
docker_elasticsearch_1 is up-to-date
docker_opencti_1 is up-to-date
docker_connector-import-document_1 is up-to-date
docker_connector-export-file-stix_1 is up-to-date
docker_connector-export-file-txt_1 is up-to-date
docker_connector-analysis_1 is up-to-date
docker_worker_1 is up-to-date
docker_worker_2 is up-to-date
docker_worker_3 is up-to-date
docker_connector-export-file-csv_1 is up-to-date
docker_connector-import-file-stix_1 is up-to-date
```

Abertura do OpenCTI

Abrimos o motor de busca e acedemos a uma das seguintes páginas: <http://localhost:8080/> ou <http://ipdamaquina:8080/> . Introduzimos as credenciais que foram configuradas no ficheiro. env e, assim, estaremos dentro do OpenCTI, concluindo a instalação.

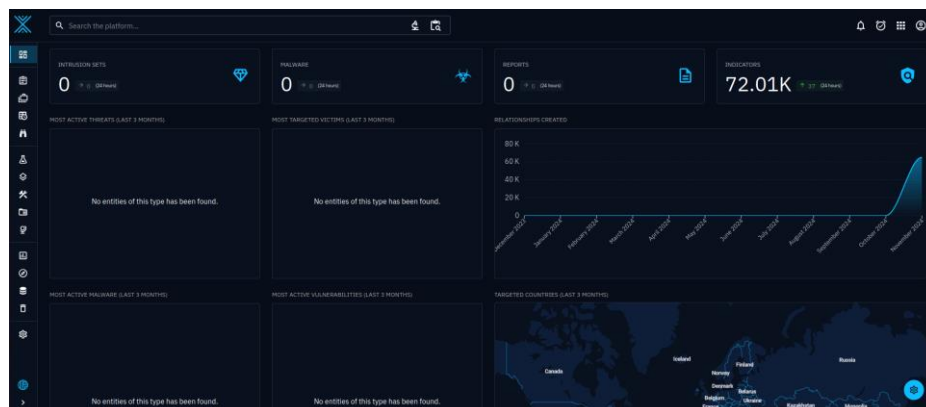
Figura 10

Página inicial do openCTI.



Figura 11

Página inicial do OpenCTi



Bibliografia

[OpenCTI] Filigran. (2024, June 28). *Installation - OpenCTI Documentation*. Opencti.io.
<https://docs.opencti.io/latest/deployment/installation/#using-docker>.

[uuidv4] *Online UUID Generator Tool*. (n.d.). Wwv.uuidgenerator.net.
<https://www.uuidgenerator.net/version4>.

[Sublime Text] Sublime Text. (n.d.). *Sublime Text - A sophisticated text editor for code, markup and prose*. Sublimetext.com. <https://www.sublimetext.com/>.