Guide Installation OpenCTI Ubuntu

Table des matières

Préambule

Ce guide détaille la configuration de la plateforme OpenCTI sur une station équipée d'une distribution Ubuntu 20.04.

Une connexion Internet est indispensable pour effectuer les téléchargements de briques logicielle *ad hoc*.

1 Composants logiciels de la Plateforme OpenCTI

Composant	Version
Plateforme OpenCTI	
OpenJDK	
NodeJS	
Python	
ElasticSearch	
MinIO	
Redis	
RabbitMQ	
RabbitMQ Management Pluggin	

2 Installation des briques logicielles

2.1 Installation OpenJDK-8

```
# sudo –s
# apt update
# apt install openjdk-8-jre
```

2.2 Installation NodeJS

- Suivre les instructions sur le site Github NodeJS https://github.com/nodesource/distributions/blob/master/README.md.

```
# sudo –s
# apt update
# apt install curl
# curl –sL https://deb.nodesource.com/setup_12.x | bash -
# apt install –y nodejs
```

2.3 Installation Python

```
# sudo –s
# apt update
# apt install python3
# apt install python3-pip
```

2.4 Installation ElasticSearch / LogStash / Kibana

```
# sudo –s
# apt update
# apt install apt-transport-https
# apt install wget
# wget –qO – https://artifacts.elastic.co/GPG-KEY-elasticsearch | apt-key add -
# echo « deb https://artifacts.elastic.co/packages/7.x/apt stable main » | tee –a /etc/apt/sources.list.d/elastic-7.x.list
# apt update
# apt install elasticsearch
# apt install logstash
#apt install kibana
```

2.5 Installation MinIO

```
# sudo –s
# mkdir /usr/share/minio
# cd /usr/share/minio
# wget https://dl.min.io/server/minio/release/linux-amd64/minio
# chmod +x minio
```

2.6 Installation Redis

```
# sudo –s
# apt update
# apt install redis-server
```

2.7 Installation RabbitMQ & Erlang-OTP

```
# sudo –s
# apt update
# curl –fsSL https://github.com/rabbitmq/signing-keys/releases/download/2.0/rabbitmq-signing-key.asc | apt-key add -
# echo « deb https://dl.bintray.com/rabbitmq-erlang/debian bionic erlang » >>
/etc/apt/sources.list.d/bintray.rabbitmq.list
# echo « deb https://dl.bintray.com/rabbitmq/debian bionic main » >>
/etc/apt/sources.list.d/bintray.rabbitmq.list
# apt update
# apt install rabbitmq-server –y –fix-missing
```

2.8 Installation Plateforme OpenCTI

```
# sudo –s
# cd /usr/share
# wget https://github.com/OpenCTI-Platform/opencti/releases/download/3.2.2/opencti-release-N.tar.gz
# tar xvfz opencti-release-N.tar.gz
# cd /opencti/src/python
# pip3 install –r requirements.txt
# cd ../../worker
# pip3 install –r requirements.txt
# chown –R root:root /usr/share/opencti
```

2.9 Installation Yarn

```
# sudo –s
# apt update
# curl –sS https://dl.yarnpkg.com/debian/pubkey.gpg | apt-key add -
# echo « deb https://dl.yarnpkg.com/debian/ stable main » | tee /etc/apt/sources.list.d/yarn.list
# apt update
# apt install yarnpkg
```

3 Configuration des briques logicielles

```
# sudo –s
# cd /var
# mkdir log
# mkdir data
# chmod 777 /var/log
# chmod 777 /var/data
```

3.1 Configuration ElasticSearch / LogStash / Kibana

- Exécuter les commandes infra.

```
# sudo –s
# mkdir –p /var/log/elasticsearch
# mkdir –p /var/log/logstash
# mpkdir –p /var/log/kibana
# mkdir –p /var/data/elasticsearch
# mkdir –p /var/data/logstash
# mkdir –p /var/data/kibana
# mkdir --p /var/lib/kibana
```

Fichiers à configurer
/etc/elasticsearch/elasticsearch.keystore
/etc/elasticsearch/elasticsearch.yml
/etc/elasticsearch/jvm.options
/etc/elasticsearch/log4j2.properties
/etc/elasticsearch/role_mapping.yml
/etc/elasticsearch/roles.yml
/etc/elasticsearch/users
/etc/elasticsearch/users_roles
/lib/systemd/system/elasticsearch.service
/etc/logstash/*
/lib/systemd/system/logstash.service
/etc/kibana/*
/lib/systemd/system/kibana.service

- Exécuter les commandes infra.

```
# sudo –s
# usermod –d /usr/share/elasticsearch –c « ElasticSearch Service User » -s /usr/sbin/nologin elasticsearch
# usermod –d /usr/share/logstash –c « LogStash Service User » -s /usr/sbin/nologin logstash
# usermod –d /usr/share/kibana –c « Kibana Service User » -s /usr/sbin/nologin kibana
# cd /etc
# chown –R root:elasticsearch elasticsearch/
# chown –R root:logstash logstash/
# chown –R root:kibana kibana/
# cd /usr/share
# chown –R root:elasticsearch elasticsearch/
# chown –R root:logstash logstash/
# chown –R root:kibana kibana/
# cd /var/log
# chown –R elasticsearch:elasticsearch elasticsearch/
# chown –R logstash:logstash logstash/
# chown –R kibana:kibana kibana/
# cd /var/data
# chown –R elasticsearch:elasticsearch elasticsearch/
# chown –R logstash:logstash logstash/
# chown –R kibana:kibana kibana/
# cd /lib/systemd/system
# systemctl daemon-reload
# systemctl enable elasticsearch.service
# systemctl start elasticsearch.service
# systemctl enable logstash.service
# systemctl start logstash.service
# systemctl enable kibana.service
# systemctl start kibana.service
```

3.2 Configuration MinIO

- Exécuter les commandes infra.

```
# sudo –s
# cd /usr/share/minio
# mkdir –p /var/log/minio
# ln –sfv /var/log/minio/ log
```

Fichiers à configurer
/lib/systemd/system/minio.service

- Exécuter les commandes infra.

```
# sudo –s
# useradd minio –U –s /usr/sbin/nologin –d /usr/share/minio –c « MinIO Service User »
# cd /usr/share
# chmod –R 755 minio
# cd /var/log
# chown –R minio:minio minio/
# cd /var/data
# chown –R minio:minio minio/
# cd /lib/systemd/system
# systemctl daemon-reload
# systemctl enable minio.service
# systemctl start minio.service
```

3.3 Configuration Redis

- Exécuter les commandes infra.

```
# sudo –s
# cd /usr/bin
# mkdir –p /var/log/redis
# mkdir –p /var/data/redis
```

Fichiers à configurer
/etc/redis/redis.conf
/lib/systemd/system/redis-server.service

- Exécuter les commandes infra.

```
# sudo –s
# usermod –d /usr/bin –c « Redis Service User » -s /usr/sbin/nologin redis
# cd /etc
# chown –R root:redis redis
# cd /var/log
# chown –R redis:redis redis/
# cd /var/data
# chown –R redis:redis redis/
# cd /lib/systemd/system
# systemctl daemon-reload
# systemctl enable redis-server.service
# systemctl start redis-server.service
```

3.4 Configuration RabbitMQ

- Exécuter les commandes infra.

```
# sudo –s
# mkdir –p /var/data/rabbitmq
# mkdir –p /var/log/rabbitmq
```

Fichiers à configurer
/etc/rabbitmq/rabbitmq.conf
/etc/rabbitmq/rabbitmq-env.conf
/etc/rabbitmq/enabled_plugins
/etc/rabbitmq/config/
/lib/systemd/system/rabbitmq-server.service

- Exécuter les commandes infra.

```
# sudo –s
# usermod –d /usr/lib/rabbitmq/bin –c « RabbitMQ Service User » -s /usr/sbin/nologin rabbitmq
# cd /etc
# chown –R root:rabbitmq rabbitmq
# cd /usr/lib/
# chown –R root:rabbitmq rabbitmq/
# chmod –R 770 rabbitmq/
# cd /var/log
# chown –R rabbitmq:rabbitmq rabbitmq/
# cd /var/data
# chown –R rabbitmq:rabbitmq rabbitmq/
# cd /lib/systemd/system
# systemctl daemon-reload
# systemctl enable rabbitmq-server.service
# systemctl start rabbitmq-server.service
```

3.5 Configuration Plateforme OpenCTI

- Exécuter les commandes infra.

```
# sudo –s
# cd /usr/share/opencti
# mkdir –p /var/data/opencti
# mkdir –p /var/log/opencti
# cd /usr/share/opencti
# ln –sfv /var/log/opencti/ log
```

Fichiers à configurer
/usr/share/opencti/01-Start-OpenCTI-Platform
/usr/share/opencti/02-Stop-OpenCTI-Platform
/usr/share/opencti/config/production.json
/usr/share/opencti/worker/config.yml
/usr/share/opencti/connectors/export-file-stix/src/config.yml
/usr/share/opencti/connectors/import-file-pdf-observables/src/config.yml
/usr/share/opencti/connectors/import-file-stix/src/config.yml
/usr/share/opencti/connectors/mitre-attack-enterprise/src/config.yml
/usr/share/opencti/connectors/mitre-attack-enterprise/src/mitre-attack-enterprise.py
/usr/share/opencti/connectors/mitre-attack-enterprise/src/requirements.txt
/usr/share/opencti/connectors/opencti/src/config.yml
/lib/systemd/system/opencti-platform.service

- Exécuter les commandes infra.

```
# sudo –s
# useradd opencti –U –s /usr/sbin/nologin –d /usr/share/opencti –c « OpenCTI Service User »
# useradd opencti staff
# cd /usr/share/
# chown –R root:opencti opencti/
# chmod 775 opencti/
# cd /usr/share/opencti
# chmod –R 640 worker/
# chmod 775 worker/
# cd /usr/share/opencti/connectors
# chmod –R 640 *
# chmod 755 *
# chmod 644 ./LICENSE ./CODE_OF_CONDUCT.md ./README.md
# chmod 755 */src
# cd /var/log
# chown –R opencti:opencti opencti/
# cd /lib/systemd/system
# systemctl daemon-reload
# systemctl enable opencti-platform.service
# systemctl start opencti-platform.service
```