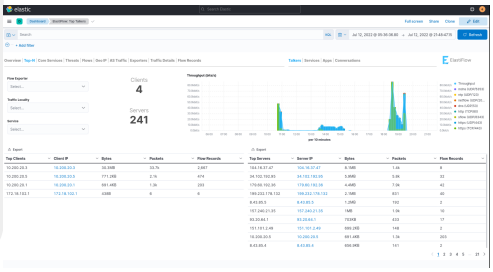
Table des matières

Le guide ELASTIFLOW



Debian Install

Elastic Stack Install

Paramètres requis

/etc/sysctl.d/70-elasticsearch.conf

```
echo "vm.max_map_count=262144" | sudo tee /etc/sysctl.d/70-
elasticsearch.conf > /dev/null
```

Tunning Réseaux

/etc/sysctl.d/60-net.conf

```
echo -e
"net.core.netdev_max_backlog=4096\nnet.core.rmem_default=262144\nnet.core.rm
em_max=67108864\nnet.ipv4.udp_rmem_min=131072\nnet.ipv4.udp_mem=2097152
4194304 8388608" | sudo tee /etc/sysctl.d/60-net.conf > /dev/null
```

Modif Sans reboot (Option)

```
  sudo sysctl -w vm.max_map_count=262144 && \
  sudo sysctl -w net.core.netdev_max_backlog=4096 && \
  sudo sysctl -w net.core.rmem_default=262144 && \
  sudo sysctl -w net.core.rmem_max=67108864 && \
  sudo sysctl -w net.ipv4.udp_rmem_min=131072 && \
  sudo sysctl -w net.ipv4.udp_mem='2097152 4194304 8388608'
```

Règles de FireWall

```
sudo systemctl stop ufw.service && sudo systemctl disable ufw.service
```

Ports Utilisés

```
Elasticsearch   TCP/9200
Kibana  TCP/5601
Unified Flow Collector  UDP 9995 or other port(s) configured by
EF_FLOW_SERVER_UDP_PORT
```

Install Package

```
sudo apt install -y apt-transport-https
sudo apt install -y unzip
```

Ajouter clé du repo

```
  wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-
key add -
```

Ajouter sources du Repo

```
 echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo
tee /etc/apt/sources.list.d/elastic-7.x.list > /dev/null
```

Install

```
  sudo apt update && sudo apt install -y elasticsearch
```

JVM Param

Créer le fichier `heap.options` to /etc/elasticsearch/jvm.options.d et déclarer les valeurs -Xms et -Xmx en fonction de l'allocation de mémoire de votre système (4g pour le test)

```
echo -e "-Xms4g\n-Xmx4g" | sudo tee
/etc/elasticsearch/jvm.options.d/heap.options > /dev/null
```

Des limites système accrues doivent être spécifiées dans un fichier d'attributs systemd pour le service elasticsearch:

```
sudo mkdir /etc/systemd/system/elasticsearch.service.d && \
  echo -e
"[Service]\nLimitNOFILE=131072\nLimitNPROC=8192\nLimitMEMLOCK=infinity\nLimi
```

```
tFSIZE=infinity\nLimitAS=infinity" | \
  sudo tee /etc/systemd/system/elasticsearch.service.d/elasticsearch.conf >
/dev/null
```

Générer des Certificats

```
sudo /usr/share/elasticsearch/bin/elasticsearch-certutil ca --pem
```

Faire enter au prompt (par defaut)

Le fichier résultant sera placé dans **/usr/share/elasticsearch**. Pour décompresser et déplacer la clé CA et le certificat vers /etc/elasticsearch/certs, exécutez les commandes suivantes:

```
 sudo mkdir /etc/elasticsearch/certs && \
sudo unzip /usr/share/elasticsearch/elastic-stack-ca.zip -d
/etc/elasticsearch/certs
```

Pour générer des certificats pour le nœud Elasticsearch, créez un fichier nommé **/usr/share/elasticsearch/instances.yml** semblable au suivant. Remplacez les valeurs par celles qui conviennent à votre environnement:

```
instances:
  - name: "myhost"
    ip:
      - "Mon-IP"
    dns:
      - "myhost.mydomain.com"   (la partie DNS n'est pas dans le test)
```

Genérer Certificats et Clé pour l'instance

```
 sudo /usr/share/elasticsearch/bin/elasticsearch-certutil cert --silent --in
instances.yml --out certs.zip --pem --ca-cert
/etc/elasticsearch/certs/ca/ca.crt --ca-key
/etc/elasticsearch/certs/ca/ca.key
```

Décompresser le tout dans le bon repertoire: (**elasticsearch/certs**)

```
 sudo unzip /usr/share/elasticsearch/certs.zip -d /etc/elasticsearch/certs
```

Data Store

Par exemple, pour stocker des données sur /mnt/data0,
exécutez

```
sudo mkdir /mnt/data0/elasticsearch && sudo chown -R
elasticsearch:elasticsearch /mnt/data0/elasticsearch
```

La modification de l'option path.data dans elasticsearch.yml en spécifiant ce chemin.

CONF elasticsearch.yml

/etc/elasticsearch/elasticsearch.yml

Defaut

```
cluster.name: elastiflow

path.data: /var/lib/elasticsearch
path.logs: /var/log/elasticsearch

bootstrap.memory_lock: true

network.host: 0.0.0.0
http.port: 9200

discovery.type: 'single-node'

indices.query.bool.max_clause_count: 8192
search.max_buckets: 250000

action.destructive_requires_name: 'true'

xpack.security.http.ssl.enabled: 'true'
xpack.security.http.ssl.verification_mode: 'none'
xpack.security.http.ssl.certificate_authorities:
/etc/elasticsearch/certs/ca/ca.crt
xpack.security.http.ssl.key: /etc/elasticsearch/certs/debian-
elastiflow/debian-elastiflow.key
xpack.security.http.ssl.certificate: /etc/elasticsearch/certs/debian-
elastiflow/debian-elastiflow.crt

xpack.monitoring.enabled: 'true'
xpack.monitoring.collection.enabled: 'true'
xpack.monitoring.collection.interval: 30s

xpack.security.enabled: 'true'
xpack.security.audit.enabled: 'false'
```

(Note pour la partie SSL (key et certificat) il sera nécessaire de les copier à la mains si il n'y sont pas)

Activer et demarrer ElastiSearch

```
sudo systemctl daemon-reload && \
  sudo systemctl enable elasticsearch && \
  sudo systemctl start elasticsearch
```

Check Status

```
sudo systemctl status elasticsearch
```

Set Password pour tous les compte de services

```
 sudo /usr/share/elasticsearch/bin/elasticsearch-setup-passwords interactive
```

```
"Initiating the setup of passwords for reserved users
elastic,apm_system,kibana,kibana_system,logstash_system,beats_system,remote_
monitoring_user.
You will be prompted to enter passwords as the process progresses.
Please confirm that you would like to continue [y/N]"
```

```
User account:
Changed password for user [apm_system]
Changed password for user [kibana_system]
Changed password for user [kibana]
Changed password for user [logstash_system]
Changed password for user [beats_system]
Changed password for user [remote_monitoring_user]
Changed password for user [elastic]
```

Vérifier l'état d' ElasticSearch:

```
curl -XGET -k "https://elastic:MyPasswd@127.0.0.1:9200"
```

Doit renvoyer:

```
{
  "name" : "myhost",
  "cluster_name" : "elastiflow",
  "cluster_uuid" : "S5Y3Z2USSq2sR2TyOkLe3A",
  "version" : {
    "number" : "7.17.0",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "66b55ebfa59c92c15db3f69a335d500018b3331e",
    "build_date" : "2021-08-26T09:01:05.390870785Z",
```

```
    "build_snapshot" : false,
    "lucene_version" : "8.9.0",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
```

La tout est OK !

Install Kibana

```
 sudo apt update && sudo apt install -y kibana
```

Kibana utilise les memes cert qu'ElasticSearch (les copier)

```
<code bash>sudo cp -r /etc/elasticsearch/certs /etc/kibana</code>
```

Config Kibana.yml

```
(**/etc/kibana/kibana.yml**) \\
```

```
telemetry.enabled: false
telemetry.optIn: false
newsfeed.enabled: false

server.host: '0.0.0.0'
server.port: 5601
server.maxPayload: 8388608
server.publicBaseUrl: 'https://10.200.20.5:5601'

server.ssl.enabled: true
server.ssl.certificateAuthorities: /etc/kibana/certs/ca/ca.crt
server.ssl.key: /etc/kibana/certs/debian-elastiflow/debian-elastiflow.key
server.ssl.certificate: /etc/kibana/certs/debian-elastiflow/debian-
elastiflow.crt

elasticsearch.hosts: ['https://10.200.20.5:9200']
elasticsearch.username: 'kibana_system'
elasticsearch.password: 'MyPasswd'
elasticsearch.ssl.certificateAuthorities: /etc/kibana/certs/ca/ca.crt
elasticsearch.ssl.key: /etc/kibana/certs/debian-elastiflow/debian-
elastiflow.key
elasticsearch.ssl.certificate: /etc/kibana/certs/debian-elastiflow/debian-
elastiflow.crt
elasticsearch.ssl.verificationMode: 'certificate'
```

```
elasticsearch.requestTimeout: 132000
elasticsearch.shardTimeout: 120000

kibana.autocompleteTimeout: 2000
kibana.autocompleteTerminateAfter: 500000

monitoring.enabled: true
monitoring.kibana.collection.enabled: true
monitoring.kibana.collection.interval: 30000

monitoring.ui.enabled: true
monitoring.ui.min_interval_seconds: 20

xpack.maps.showMapVisualizationTypes: true

xpack.security.enabled: true
xpack.security.audit.enabled: false

xpack.encryptedSavedObjects.encryptionKey:
'ElastiFlow_0123456789_0123456789_0123456789'
```

Demarrer et Activer Kibana

```
sudo systemctl daemon-reload && \
   sudo systemctl enable kibana && \
   sudo systemctl start kibana
```

Check Status

```
 sudo systemctl status kibana
```

WEB ui : https://IP_OF_KIBANA_HOST:5601

Install ElastiFlow Unified Flow Collector

Download Package

```
wget https://elastiflow-packages.s3.amazonaws.com/flow-collector/flow-
collector_5.5.2_linux_amd64.deb
```

Flowcoll Install

APT methode

```
<code bash>sudo apt install ./flow-collector_5.5.2_linux_amd64.deb</code>
```

DPKG methode

```
sudo dpkg -i flow-collector_5.5.2_linux_amd64.deb
```

Contrôler que libpcap-dev est présent

```
sudo dpkg-query -l | grep libpcap-dev
```

Installer là si non présente!

Path : /etc/elastiflow
Conf du collecteur:

```
/etc/systemd/system/flowcoll.service.d/flowcoll.conf
```

Démarrer le collecteur

```
sudo systemctl daemon-reload && sudo systemctl start flowcoll.service
```

Contrôle du service

```
sudo systemctl status flowcoll.service
```

Commande de management

```
sudo systemctl stop flowcoll.service (start/stop/status)
```

Démarrage Auto au boot

```
sudo systemctl enable flowcoll.service
```

FICHIER DE CONF:

```
/etc/systemd/system/flowcoll.service.d/flowcoll.conf
```

copie des certificats

```
sudo mkdir /etc/elastiflow/ca && \
```

```
    sudo cp /etc/elasticsearch/certs/ca/ca.crt /etc/elastiflow/ca
```

CONFIGURATION

```
#product documentation at https://docs.elastiflow.com

[Service]
Environment="EF_FLOW_ACCOUNT_ID=62c82xxxxxxxxxxxxxxxx"
Environment="EF_FLOW_LICENSE_KEY=eyJhbGciOixxxxxxxxxxxxxxxxxxxxx"
Environment="EF_FLOW_LICENSED_UNITS=1"

Environment="EF_FLOW_LOGGER_LEVEL=info"
Environment="EF_FLOW_LOGGER_ENCODING=console"
Environment="EF_FLOW_LOGGER_FILE_LOG_ENABLE=true"
Environment="EF_FLOW_LOGGER_FILE_LOG_FILENAME=/var/log/elastiflow/flowcoll/f
lowcoll.log"
#Environment="EF_FLOW_LOGGER_FILE_LOG_MAX_SIZE=100"
#Environment="EF_FLOW_LOGGER_FILE_LOG_MAX_AGE="
#Environment="EF_FLOW_LOGGER_FILE_LOG_MAX_BACKUPS=4"
#Environment="EF_FLOW_LOGGER_FILE_LOG_COMPRESS=false"

Environment="EF_FLOW_SERVER_UDP_IP=0.0.0.0"
Environment="EF_FLOW_SERVER_UDP_PORT=2055,6343,9995"
Environment="EF_FLOW_SERVER_UDP_PACKET_STREAM_MAX_SIZE=4096"
Environment="EF_FLOW_SERVER_UDP_READ_BUFFER_MAX_SIZE=33554432"

Environment="EF_FLOW_DECODER_POOL_SIZE=1"
Environment="EF_FLOW_DECODER_SETTINGS_PATH=/etc/elastiflow"

#Environment="EF_FLOW_DECODER_IPFIX_ENABLE=true"
Environment="EF_FLOW_DECODER_NETFLOW1_ENABLE=true"
Environment="EF_FLOW_DECODER_NETFLOW5_ENABLE=true"
Environment="EF_FLOW_DECODER_NETFLOW6_ENABLE=true"
Environment="EF_FLOW_DECODER_NETFLOW7_ENABLE=true"
Environment="EF_FLOW_DECODER_NETFLOW9_ENABLE=true"
Environment="EF_FLOW_DECODER_SFLOW5_ENABLE=true"
Environment="EF_FLOW_DECODER_SFLOW_FLOWS_ENABLE=true"
#Environment="EF_FLOW_DECODER_SFLOW_FLOWS_KEEP_SAMPLES=false"
Environment="EF_FLOW_DECODER_SFLOW_COUNTERS_ENABLE=true"

Environment="EF_FLOW_DECODER_TRANSLATE_KEEP_IDS=all"

Environment="EF_FLOW_DECODER_ENRICH_IPADDR_METADATA_ENABLE=false"
#Environment="EF_FLOW_DECODER_ENRICH_IPADDR_METADATA_USERDEF_PATH=metadata/i
paddrs.yml"
#Environment="EF_FLOW_DECODER_ENRICH_IPADDR_METADATA_REFRESH_RATE=15"

Environment="EF_FLOW_DECODER_ENRICH_DNS_ENABLE=false"
Environment="EF_FLOW_DECODER_ENRICH_DNS_NAMESERVER_IP="
Environment="EF_FLOW_DECODER_ENRICH_DNS_NAMESERVER_TIMEOUT=3000"
```

```
#Environment="EF_FLOW_DECODER_ENRICH_DNS_RESOLVE_PRIVATE=true"
#Environment="EF_FLOW_DECODER_ENRICH_DNS_RESOLVE_PUBLIC=true"
#Environment="EF_FLOW_DECODER_ENRICH_DNS_USERDEF_PATH=hostname/user_defined.yml"
#Environment="EF_FLOW_DECODER_ENRICH_DNS_USERDEF_REFRESH_RATE=15"
#Environment="EF_FLOW_DECODER_ENRICH_DNS_INCLEXCL_PATH=hostname/incl_excl.yml"
#Environment="EF_FLOW_DECODER_ENRICH_DNS_INCLEXCL_REFRESH_RATE=15"

Environment="EF_FLOW_DECODER_ENRICH_MAXMIND_ASN_ENABLE=true"
Environment="EF_FLOW_DECODER_ENRICH_MAXMIND_ASN_PATH=maxmind/GeoLite2-ASN.mmdb"

Environment="EF_FLOW_DECODER_ENRICH_MAXMIND_GEOIP_ENABLE=true"
Environment="EF_FLOW_DECODER_ENRICH_MAXMIND_GEOIP_PATH=maxmind/GeoLite2-City.mmdb"
Environment="EF_FLOW_DECODER_ENRICH_MAXMIND_GEOIP_VALUES=city,country,country_code,location,timezone"
Environment="EF_FLOW_DECODER_ENRICH_MAXMIND_GEOIP_LANG=en"
Environment="EF_FLOW_DECODER_ENRICH_MAXMIND_GEOIP_INCLEXCL_PATH=maxmind/incl_excl.yml"
Environment="EF_FLOW_DECODER_ENRICH_MAXMIND_GEOIP_INCLEXCL_REFRESH_RATE=15"

Environment="EF_FLOW_DECODER_ENRICH_RISKIQ_ASN_ENABLE=false"
#Environment="EF_FLOW_DECODER_ENRICH_RISKIQ_ASN_ENDPOINT=https://api.passivetotal.org/v2/netflow/as/download"
#Environment="EF_FLOW_DECODER_ENRICH_RISKIQ_ASN_REFRESH_INTERVAL=1440"
Environment="EF_FLOW_DECODER_ENRICH_RISKIQ_THREAT_ENABLE=false"
#Environment="EF_FLOW_DECODER_ENRICH_RISKIQ_THREAT_ENDPOINT=https://api.passivetotal.org/v2/netflow/blocklist/download"
#Environment="EF_FLOW_DECODER_ENRICH_RISKIQ_THREAT_REFRESH_INTERVAL=1440"
#Environment="EF_FLOW_DECODER_ENRICH_RISKIQ_THREAT_INCLEXCL_PATH=riskiq/incl_excl.yml"
#Environment="EF_FLOW_DECODER_ENRICH_RISKIQ_THREAT_INCLEXCL_REFRESH_RATE=15"
#Environment="EF_FLOW_DECODER_ENRICH_RISKIQ_API_USER="
#Environment="EF_FLOW_DECODER_ENRICH_RISKIQ_API_KEY="
#Environment="EF_FLOW_DECODER_ENRICH_RISKIQ_API_TIMEOUT=180"

Environment="EF_FLOW_DECODER_ENRICH_ASN_PREF=lookup"

Environment="EF_FLOW_DECODER_ENRICH_NETIF_METADATA_ENABLE=false"
#Environment="EF_FLOW_DECODER_ENRICH_NETIF_METADATA_USERDEF_PATH=metadata/ipaddrs.yml"
#Environment="EF_FLOW_DECODER_ENRICH_NETIF_METADATA_REFRESH_RATE=15"

Environment="EF_FLOW_DECODER_ENRICH_NETIF_FLOW_OPTIONS_ENABLE=true"

Environment="EF_FLOW_DECODER_ENRICH_NETIF_SNMP_ENABLE=false"
#Environment="EF_FLOW_DECODER_ENRICH_NETIF_SNMP_PORT=161"
#Environment="EF_FLOW_DECODER_ENRICH_NETIF_SNMP_VERSION=2"
Environment="EF_FLOW_DECODER_ENRICH_NETIF_SNMP_COMMUNITIES=public"
```

```
#Environment="EF_FLOW_DECODER_ENRICH_NETIF_SNMP_TIMEOUT=2"
#Environment="EF_FLOW_DECODER_ENRICH_NETIF_SNMP_RETRIES=1"

Environment="EF_FLOW_DECODER_ENRICH_APP_CACHE_SIZE=8388608"

Environment="EF_FLOW_DECODER_ENRICH_APP_USERDEF_ENABLE=true"
Environment="EF_FLOW_DECODER_ENRICH_APP_USERDEF_PRIVATE=true"
Environment="EF_FLOW_DECODER_ENRICH_APP_USERDEF_PUBLIC=false"
Environment="EF_FLOW_DECODER_ENRICH_APP_USERDEF_PATH=settings/apps_user_defi
ned.yml"

#Environment="EF_FLOW_DECODER_ENRICH_TOTALS_IF_NO_DELTAS=false"

#Environment="EF_FLOW_DECODER_ENRICH_SAMPLERATE_CACHE_SIZE=32768"
#Environment="EF_FLOW_DECODER_ENRICH_SAMPLERATE_USERDEF_ENABLE=false"
#Environment="EF_FLOW_DECODER_ENRICH_SAMPLERATE_USERDEF_PATH=settings/sample
_rate.yml"

#Environment="EF_FLOW_DECODER_ENRICH_COMMUNITYID_ENABLE=true"
#Environment="EF_FLOW_DECODER_ENRICH_COMMUNITYID_SEED=0"
#Environment="EF_FLOW_DECODER_ENRICH_CONVERSATIONID_ENABLE=true"
#Environment="EF_FLOW_DECODER_ENRICH_CONVERSATIONID_SEED=0"

Environment="EF_FLOW_DECODER_ENRICH_JOIN_ASN=true"
Environment="EF_FLOW_DECODER_ENRICH_JOIN_GEOIP=true"
Environment="EF_FLOW_DECODER_ENRICH_JOIN_SEC=true"
Environment="EF_FLOW_DECODER_ENRICH_JOIN_NETATTR=true"
Environment="EF_FLOW_DECODER_ENRICH_JOIN_SUBNETATTR=true"

Environment="EF_FLOW_DECODER_DURATION_PRECISION=ms"
Environment="EF_FLOW_DECODER_TIMESTAMP_PRECISION=ms"
Environment="EF_FLOW_DECODER_PERCENT_NORM=100"
Environment="EF_FLOW_DECODER_ENRICH_EXPAND_CLISRV=true"
#Environment="EF_FLOW_DECODER_ENRICH_KEEP_CPU_TICKS=false"

#Environment="EF_FLOW_DECODER_ENRICH_DROP_FIELDS="

Environment="EF_FLOW_RECORD_STREAM_MAX_SIZE=8192"

# stdout
#Environment="EF_FLOW_OUTPUT_STDOUT_ENABLE=false"
#Environment="EF_FLOW_OUTPUT_STDOUT_FORMAT=json_pretty"

# monitor
#Environment="EF_FLOW_OUTPUT_MONITOR_ENABLE=true"
#Environment="EF_FLOW_OUTPUT_MONITOR_INTERVAL=300"

# Elasticsearch
Environment="EF_FLOW_OUTPUT_ELASTICSEARCH_ENABLE=true"
Environment="EF_FLOW_OUTPUT_ELASTICSEARCH_ECS_ENABLE=true"
Environment="EF_FLOW_OUTPUT_ELASTICSEARCH_BATCH_DEADLINE=2000"
```

```
Environment="EF_FLOW_OUTPUT_ELASTICSEARCH_BATCH_MAX_BYTES=8388608"
Environment="EF_FLOW_OUTPUT_ELASTICSEARCH_TIMESTAMP_SOURCE=collect"
Environment="EF_FLOW_OUTPUT_ELASTICSEARCH_INDEX_PERIOD=daily"
#Environment="EF_FLOW_OUTPUT_ELASTICSEARCH_INDEX_SUFFIX="
#Environment="EF_FLOW_OUTPUT_ELASTICSEARCH_DROP_FIELDS="

Environment="EF_FLOW_OUTPUT_ELASTICSEARCH_INDEX_TEMPLATE_ENABLE=true"
#Environment="EF_FLOW_OUTPUT_ELASTICSEARCH_INDEX_TEMPLATE_OVERWRITE=true"
Environment="EF_FLOW_OUTPUT_ELASTICSEARCH_INDEX_TEMPLATE_SHARDS=1"
Environment="EF_FLOW_OUTPUT_ELASTICSEARCH_INDEX_TEMPLATE_REPLICAS=0"
Environment="EF_FLOW_OUTPUT_ELASTICSEARCH_INDEX_TEMPLATE_REFRESH_INTERVAL=10
s"
Environment="EF_FLOW_OUTPUT_ELASTICSEARCH_INDEX_TEMPLATE_CODEC=best_compress
ion"
Environment="EF_FLOW_OUTPUT_ELASTICSEARCH_INDEX_TEMPLATE_ILM_LIFECYCLE=elast
iflow"
#Environment="EF_FLOW_OUTPUT_ELASTICSEARCH_INDEX_TEMPLATE_PIPELINE_DEFAULT=_
none"
#Environment="EF_FLOW_OUTPUT_ELASTICSEARCH_INDEX_TEMPLATE_PIPELINE_FINAL=_no
ne"

# A comma separated list of Elasticsearch nodes to use. DO NOT include
"http://" or "https://"
Environment="EF_FLOW_OUTPUT_ELASTICSEARCH_ADDRESSES=127.0.0.1:9200"
Environment="EF_FLOW_OUTPUT_ELASTICSEARCH_USERNAME=elastic"
Environment="EF_FLOW_OUTPUT_ELASTICSEARCH_PASSWORD=MyPasswd"
#Environment="EF_FLOW_OUTPUT_ELASTICSEARCH_CLOUD_ID="
#Environment="EF_FLOW_OUTPUT_ELASTICSEARCH_API_KEY="
#Environment="EF_FLOW_OUTPUT_ELASTICSEARCH_CLIENT_CA_CERT_FILEPATH="
#Environment="EF_FLOW_OUTPUT_ELASTICSEARCH_CLIENT_CERT_FILEPATH="
#Environment="EF_FLOW_OUTPUT_ELASTICSEARCH_CLIENT_KEY_FILEPATH="

Environment="EF_FLOW_OUTPUT_ELASTICSEARCH_TLS_ENABLE=true"
Environment="EF_FLOW_OUTPUT_ELASTICSEARCH_TLS_SKIP_VERIFICATION=true"
Environment="EF_FLOW_OUTPUT_ELASTICSEARCH_TLS_CA_CERT_FILEPATH=/etc/elastifl
ow/ca/ca.crt"

Environment="EF_FLOW_OUTPUT_ELASTICSEARCH_RETRY_ENABLE=true"
Environment="EF_FLOW_OUTPUT_ELASTICSEARCH_RETRY_ON_TIMEOUT_ENABLE=true"
Environment="EF_FLOW_OUTPUT_ELASTICSEARCH_MAX_RETRIES=3"
Environment="EF_FLOW_OUTPUT_ELASTICSEARCH_RETRY_BACKOFF=1000"

# OpenSearch
Environment="EF_FLOW_OUTPUT_OPENSEARCH_ENABLE=false"
Environment="EF_FLOW_OUTPUT_OPENSEARCH_ECS_ENABLE=false"
#Environment="EF_FLOW_OUTPUT_OPENSEARCH_BATCH_DEADLINE=2000"
#Environment="EF_FLOW_OUTPUT_OPENSEARCH_BATCH_MAX_BYTES=8388608"
#Environment="EF_FLOW_OUTPUT_OPENSEARCH_TIMESTAMP_SOURCE=end"
#Environment="EF_FLOW_OUTPUT_OPENSEARCH_INDEX_PERIOD=daily"
#Environment="EF_FLOW_OUTPUT_OPENSEARCH_INDEX_SUFFIX="
#Environment="EF_FLOW_OUTPUT_OPENSEARCH_DROP_FIELDS="
```

```
#Environment="EF_FLOW_OUTPUT_OPENSEARCH_INDEX_TEMPLATE_ENABLE=true"
#Environment="EF_FLOW_OUTPUT_OPENSEARCH_INDEX_TEMPLATE_OVERWRITE=true"
Environment="EF_FLOW_OUTPUT_OPENSEARCH_INDEX_TEMPLATE_SHARDS=1"
Environment="EF_FLOW_OUTPUT_OPENSEARCH_INDEX_TEMPLATE_REPLICAS=0"
#Environment="EF_FLOW_OUTPUT_OPENSEARCH_INDEX_TEMPLATE_REFRESH_INTERVAL=10s"
#Environment="EF_FLOW_OUTPUT_OPENSEARCH_INDEX_TEMPLATE_CODEC=best_compressio
n"
#Environment="EF_FLOW_OUTPUT_OPENSEARCH_INDEX_TEMPLATE_ISM_POLICY="
#Environment="EF_FLOW_OUTPUT_OPENSEARCH_INDEX_TEMPLATE_PIPELINE_DEFAULT=_non
e"
#Environment="EF_FLOW_OUTPUT_OPENSEARCH_INDEX_TEMPLATE_PIPELINE_FINAL=_none"

# A comma separated list of OpenSearch nodes to use. DO NOT include
"http://" or "https://"
Environment="EF_FLOW_OUTPUT_OPENSEARCH_ADDRESSES=127.0.0.1:9200"
Environment="EF_FLOW_OUTPUT_OPENSEARCH_USERNAME=admin"
Environment="EF_FLOW_OUTPUT_OPENSEARCH_PASSWORD=admin"
#Environment="EF_FLOW_OUTPUT_OPENSEARCH_CLIENT_CA_CERT_FILEPATH="
#Environment="EF_FLOW_OUTPUT_OPENSEARCH_CLIENT_CERT_FILEPATH="
#Environment="EF_FLOW_OUTPUT_OPENSEARCH_CLIENT_KEY_FILEPATH="

Environment="EF_FLOW_OUTPUT_OPENSEARCH_TLS_ENABLE=false"
Environment="EF_FLOW_OUTPUT_OPENSEARCH_TLS_SKIP_VERIFICATION=false"
Environment="EF_FLOW_OUTPUT_OPENSEARCH_TLS_CA_CERT_FILEPATH="

#Environment="EF_FLOW_OUTPUT_OPENSEARCH_RETRY_ENABLE=true"
#Environment="EF_FLOW_OUTPUT_OPENSEARCH_RETRY_ON_TIMEOUT_ENABLE=true"
#Environment="EF_FLOW_OUTPUT_OPENSEARCH_MAX_RETRIES=3"
#Environment="EF_FLOW_OUTPUT_OPENSEARCH_RETRY_BACKOFF=1000"

# Splunk
Environment="EF_FLOW_OUTPUT_SPLUNK_HEC_ENABLE=false"
#Environment="EF_FLOW_OUTPUT_SPLUNK_HEC_CIM_ENABLE=false"
Environment="EF_FLOW_OUTPUT_SPLUNK_HEC_ADDRESSES=127.0.0.1:8088"
Environment="EF_FLOW_OUTPUT_SPLUNK_HEC_TOKEN="
#Environment="EF_FLOW_OUTPUT_SPLUNK_HEC_BATCH_MAX_BYTES=8388608"
#Environment="EF_FLOW_OUTPUT_SPLUNK_HEC_BATCH_DEADLINE=2000"
#Environment="EF_FLOW_OUTPUT_SPLUNK_HEC_TLS_ENABLE=true"
#Environment="EF_FLOW_OUTPUT_SPLUNK_HEC_TLS_SKIP_VERIFICATION=false"
#Environment="EF_FLOW_OUTPUT_SPLUNK_HEC_TLS_CA_CERT_FILEPATH="
#Environment="EF_FLOW_OUTPUT_SPLUNK_HEC_DROP_FIELDS="

# Logz.io
Environment="EF_FLOW_OUTPUT_LOGZIO_ENABLE=false"
Environment="EF_FLOW_OUTPUT_LOGZIO_ADDRESSES=listener.logz.io:8070"
Environment="EF_FLOW_OUTPUT_LOGZIO_TOKEN="
#Environment="EF_FLOW_OUTPUT_LOGZIO_TIMESTAMP_SOURCE=end"
#Environment="EF_FLOW_OUTPUT_LOGZIO_BATCH_DEADLINE=2000"
#Environment="EF_FLOW_OUTPUT_LOGZIO_BATCH_MAX_BYTES=8388608"
#Environment="EF_FLOW_OUTPUT_LOGZIO_ECS_ENABLE=false"
```

```
#Environment="EF_FLOW_OUTPUT_LOGZIO_TIMEOUT=30000"
#Environment="EF_FLOW_OUTPUT_LOGZIO_TLS_ENABLE=false"
#Environment="EF_FLOW_OUTPUT_LOGZIO_DROP_FIELDS="

# Kafka
Environment="EF_FLOW_OUTPUT_KAFKA_ENABLE=false"
Environment="EF_FLOW_OUTPUT_KAFKA_BROKERS="
#Environment="EF_FLOW_OUTPUT_KAFKA_VERSION=1.0.0"
#Environment="EF_FLOW_OUTPUT_KAFKA_TOPIC=elastiflow-flow-codex"
#Environment="EF_FLOW_OUTPUT_KAFKA_PARTITION_KEY=flow.export.ip.addr"
#Environment="EF_FLOW_OUTPUT_KAFKA_CLIENT_ID=elastiflow-flowcoll"
#Environment="EF_FLOW_OUTPUT_KAFKA_RACK_ID="
#Environment="EF_FLOW_OUTPUT_KAFKA_TIMEOUT=30"
#Environment="EF_FLOW_OUTPUT_KAFKA_DROP_FIELDS="

Environment="EF_FLOW_OUTPUT_KAFKA_SASL_ENABLE=false"
#Environment="EF_FLOW_OUTPUT_KAFKA_SASL_USERNAME="
#Environment="EF_FLOW_OUTPUT_KAFKA_SASL_PASSWORD="

#Environment="EF_FLOW_OUTPUT_KAFKA_TLS_ENABLE=false"
#Environment="EF_FLOW_OUTPUT_KAFKA_TLS_CA_CERT_FILEPATH="
#Environment="EF_FLOW_OUTPUT_KAFKA_TLS_CERT_FILEPATH="
#Environment="EF_FLOW_OUTPUT_KAFKA_TLS_KEY_FILEPATH="
#Environment="EF_FLOW_OUTPUT_KAFKA_TLS_SKIP_VERIFICATION=false"

#Environment="EF_FLOW_OUTPUT_KAFKA_PRODUCER_MAX_MESSAGE_BYTES=1000000"
#Environment="EF_FLOW_OUTPUT_KAFKA_PRODUCER_REQUIRED_ACKS=1"
#Environment="EF_FLOW_OUTPUT_KAFKA_PRODUCER_TIMEOUT=10"
#Environment="EF_FLOW_OUTPUT_KAFKA_PRODUCER_COMPRESSION=0"
#Environment="EF_FLOW_OUTPUT_KAFKA_PRODUCER_COMPRESSION_LEVEL=-1000"
#Environment="EF_FLOW_OUTPUT_KAFKA_PRODUCER_FLUSH_BYTES=1000000"
#Environment="EF_FLOW_OUTPUT_KAFKA_PRODUCER_FLUSH_MESSAGES=1024"
#Environment="EF_FLOW_OUTPUT_KAFKA_PRODUCER_FLUSH_FREQUENCY=500"
#Environment="EF_FLOW_OUTPUT_KAFKA_PRODUCER_FLUSH_MAX_MESSAGES=0"
#Environment="EF_FLOW_OUTPUT_KAFKA_PRODUCER_RETRY_MAX=3"
#Environment="EF_FLOW_OUTPUT_KAFKA_PRODUCER_RETRY_BACKOFF=100"

# Cribl
Environment="EF_FLOW_OUTPUT_CRIBL_ENABLE=false"
Environment="EF_FLOW_OUTPUT_CRIBL_ADDRESSES=127.0.0.1:10080"
Environment="EF_FLOW_OUTPUT_CRIBL_TOKEN="
#Environment="EF_FLOW_OUTPUT_CRIBL_BATCH_DEADLINE=2000"
#Environment="EF_FLOW_OUTPUT_CRIBL_BATCH_MAX_BYTES=8388608"
#Environment="EF_FLOW_OUTPUT_CRIBL_TLS_ENABLE=false"
#Environment="EF_FLOW_OUTPUT_CRIBL_TLS_SKIP_VERIFICATION=false"
#Environment="EF_FLOW_OUTPUT_CRIBL_TLS_CA_CERT_FILEPATH="
#Environment="EF_FLOW_OUTPUT_CRIBL_DROP_FIELDS="

# RiskIQ
Environment="EF_FLOW_OUTPUT_RISKIQ_ENABLE=false"
#Environment="EF_FLOW_OUTPUT_RISKIQ_HOST="
```

```
#Environment="EF_FLOW_OUTPUT_RISKIQ_PORT="
#Environment="EF_FLOW_OUTPUT_RISKIQ_CUSTOMER_UUID="
#Environment="EF_FLOW_OUTPUT_RISKIQ_CUSTOMER_ENCRYPTION_KEY=" </nowiki>
```

Activer et Demarrer Unified Flow Collector:

```
sudo systemctl daemon-reload && \
    sudo systemctl enable flowcoll && \
    sudo systemctl start flowcoll
```

Check status:

```
sudo systemctl status flowcoll
```

Apres chaque modif de conf

```
sudo systemctl daemon-reload && sudo systemctl start flowcoll.service
```

IMPORTER LES OBJET KIBANA

```
7.14.x - 8.1.x    ECS    dark    kibana-7.14.x-ecs-dark.ndjson
7.14.x - 8.1.x    ECS    light    kibana-7.14.x-ecs-light.ndjson
```

https://raw.githubusercontent.com/elastiflow/elastiflow_for_elasticsearch/master/kibana/kibana-7.14.x-ecs-dark.ndjson
https://raw.githubusercontent.com/elastiflow/elastiflow_for_elasticsearch/master/kibana/kibana-7.14.x-ecs-light.ndjson

How to:
https://docs.elastiflow.com/docs/elastic_kibana

Pour la partie Geo IP

Ouvrir un compte sur maxmind.com.
Après l'enregistrement télécharger les mmdb City country et ASN

Puis les intégrer dans la conf

Dans /etc/elastiflow/

```
      - ca   (Certificats)
    - hostname (pour definir les host manuellement)
    - maxmind   (fichier mmdb pour GeoIp)
    - metadata (pour definir la GeoIp manuellement)
    - riskiq (concerne la partie surface d'attaque)
    - settings (sert à l apartie app N° port )
```