[SOC] Graylog

Introduction

Graylog est un SIEM qui permet de centraliser vos logs et de faire des queries pour faire des analyses de threat hunting notamment.

Sources

- https://www.it-connect.fr/tuto-graylog-sur-debian-centraliser-et-analyser-logs/
- https://www.it-connect.fr/envoyer-les-logs-windows-vers-graylog-avec-nxlog/

Installation

Serveur (Debian 12)

Tout d'abord, configurez correctement la timezone ou le serveur de temps :

```
timedatectl set-timezone Europe/Paris
```

Installez quelques outils de base dont nous auront besoin pour la suite :

```
apt update && apt install -y install curl lsb-release ca-certificates gnupg2 pwgen
```

MongoDB

```
curl -fsSL https://www.mongodb.org/static/pgp/server-6.0.asc | sudo gpg -o /usr/share/keyrings/mongodb-server-6.0.gpg --dearmor && echo "deb [ signed-by=/usr/share/keyrings/mongodb-server-6.0.gpg] http://repo.mongodb.org/apt/debian bullseye/mongodb-org/6.0 main" | sudo tee /etc/apt/sources.list.d/mongodb-org-6.0.list && apt update && apt-get install -y mongodb-org
```

> Vous allez obtenir une erreur par rapport à **libssl** à ce stade et c'est normal, passez à la suite.

Rendez-vous sur le site suivant pour trouver la version la plus récente de libssl et copiez le lien :

- http://archive.ubuntu.com/ubuntu/pool/main/o/openssl/

> Faite CTRL+F et cherchez "**libssl1.1_1.1.1f-1ubuntu**2." puis sélectionnez la version deb amd64.

Une fois l'URL récupérée, vous devriez faire quelque chose comme ça :

```
wget http://archive.ubuntu.com/ubuntu/pool/main/o/openssl/libssl1.1_1.1.1f-1ubuntu2.23_amd64.deb && dpkg -i libssl1.1_1.1.1f-1ubuntu2.23_amd64.deb
```

Puis réinstallez le paquet **mongodb-org** :

```
apt install -y mongodb-org
```

Et lancez le service :

```
sudo systemctl daemon-reload && sudo systemctl enable --now mongod.service
```

> Si l'installation de MongoDB s'est mal passée c'est que vous n'avez pas téléchargé le bon paquet sur le site d'Ubuntu.

> Si l'installation de MongoDB s'est bien passée mais que le service ne démarre pas, assurez-vous de passer le CPU en mode host s'il s'agit d'une VM.

Opensearch

```
curl -o- https://artifacts.opensearch.org/publickeys/opensearch.pgp | sudo gpg --dearmor --batch --yes -o /usr/share/keyrings/opensearch-keyring && echo "deb [signed-by=/usr/share/keyrings/opensearch-keyring] https://artifacts.opensearch.org/releases/bundle/opensearch/2.x/apt stable main" | sudo tee /etc/apt/sources.list.d/opensearch-2.x.list && apt update
```

```
env OPENSEARCH_INITIAL_ADMIN_PASSWORD=<PASSWORD> apt-get install opensearch
```

> Choisissez un mot de passe d'au moins 8 caractères avec minuscule, majuscule, chiffre et caractère spécial sinon l'installation d'opensearch échouera.

Maintenant ouvrez le fichier de configuration **/etc/opensearch/opensearch.yml** et ajustez la configuration avec les éléments suivants :

```
cluster.name: graylog
node.name: ${HOSTNAME}
path.data: /var/lib/opensearch
path.logs: /var/log/opensearch
discovery.type: single-node
network.host: 127.0.0.1
action.auto_create_index: false
plugins.security.disabled: true
```

Java

Éditez le fichier de configuration **/etc/opensearch/jvm.options** pour définir la ram utilisée par Java (minimum 4G) :

```
-Xms4g
-Xmx4g
```

Vérifiez que le max_map_count est définit à **262144** :

```
cat /proc/sys/vm/max_map_count
```

Si ce n'est pas le cas (uniquement) :

```
sysctl -w vm.max_map_count=262144
```

Une fois que java est configuré, lancez et activez le service opensearch :

```
systemctl daemon-reload && systemctl enable --now opensearch
```

Graylog

```
wget https://packages.graylog2.org/repo/packages/graylog-6.1-repository_latest.deb && dpkg -i graylog-6.1-repository_latest.deb && apt update && apt install -y graylog-server
```

Avant de lancez Graylog il faut configurer le **password_secret** que vous pouvez générer avec la commande suivante :

```
pwgen -N 1 -s 96
```

Renseignez le à l'endroit adéquat dans le fichier **/etc/graylog/server/server.conf** .

Ensuite il faut configurer le mot de passe admin de Graylog. Pour cela on doit calculer son hash :

```
echo -n "<PASSWORD>" | shasum -a 256
```

Et renseignez le dans le fichier **/etc/graylog/server/server.conf** au niveau du champ **root_password_sha2** .

Toujours dans le fichier de configuration, définissez les paramètres suivants :

```
http_bind_address = 0.0.0.0:9000
elasticsearch_hosts = http://127.0.0.1:9200
```

Et enfin, activez et démarrez Graylog :

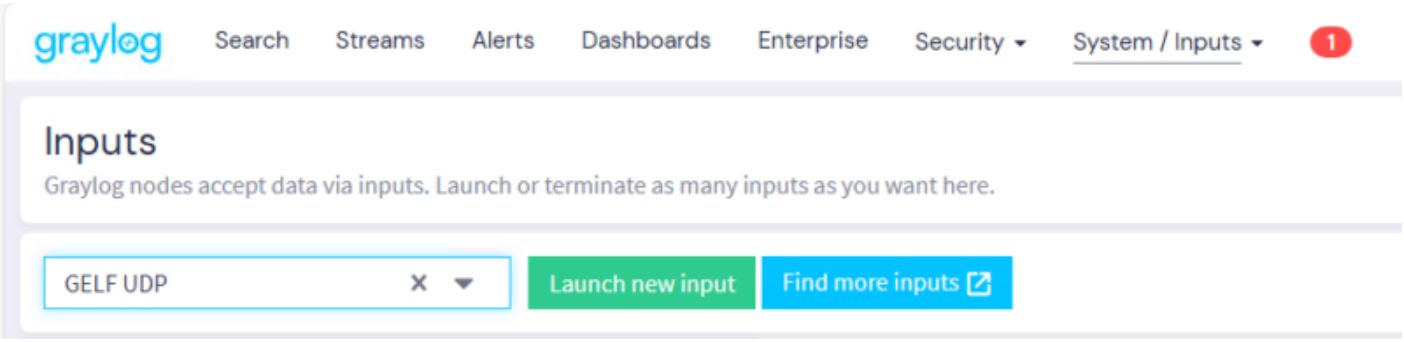
```
systemctl enable --now graylog-server
```

> Graylog est désormais accessible via **http://<IP>:9000** .

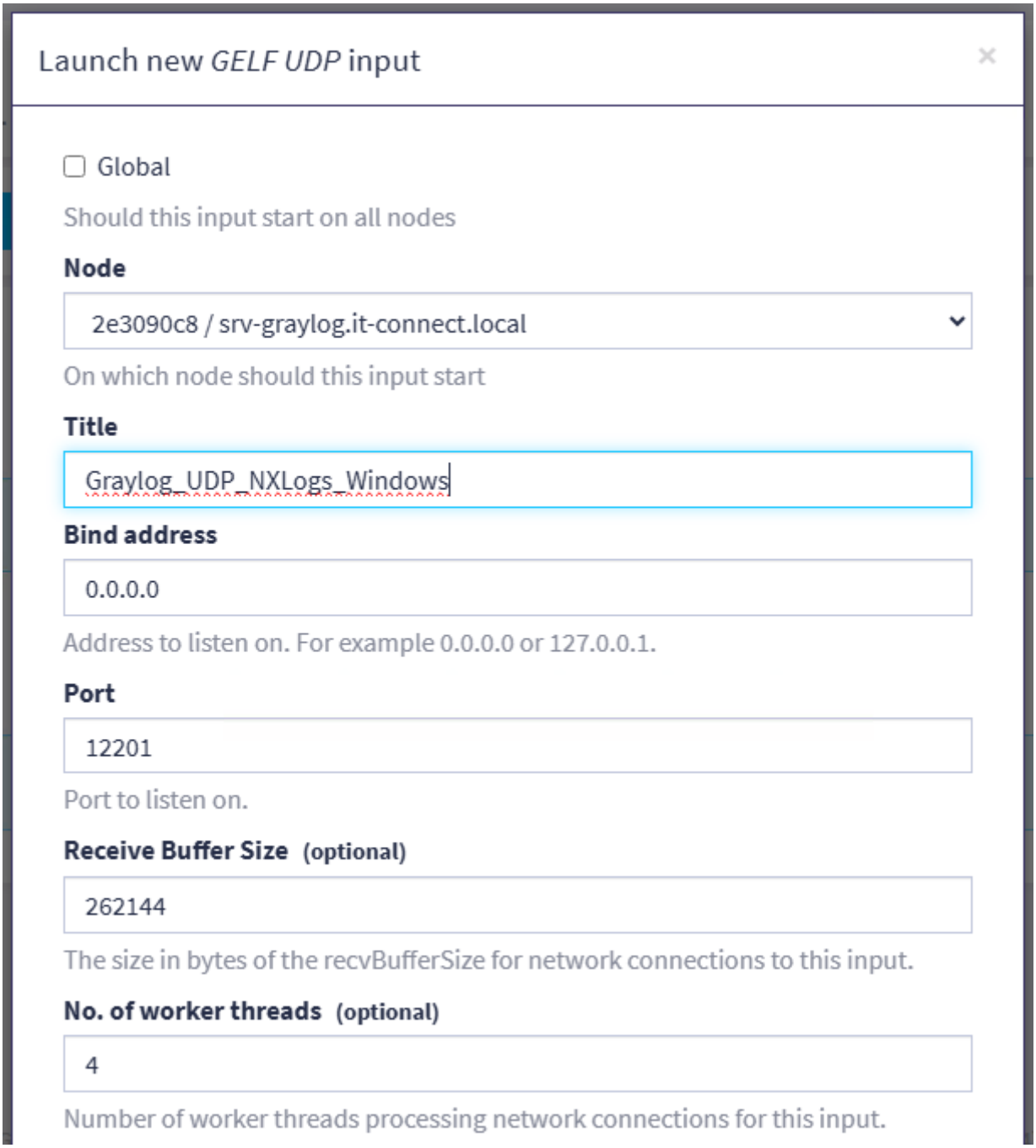
Agent Windows

Tout d'abord il faut configurer Graylog pour recevoir les logs.

Pour cela rendez-vous dans **System > Inputs** et sélectionnez **GELF UDP** comme ci et cliquez sur **Launch new input** :



Configurez de la sorte (sauf pour le titre, mettez ce que vous souhaitez) :



Vous devriez voir quelque chose comme ça :

Local inputs 1 configured

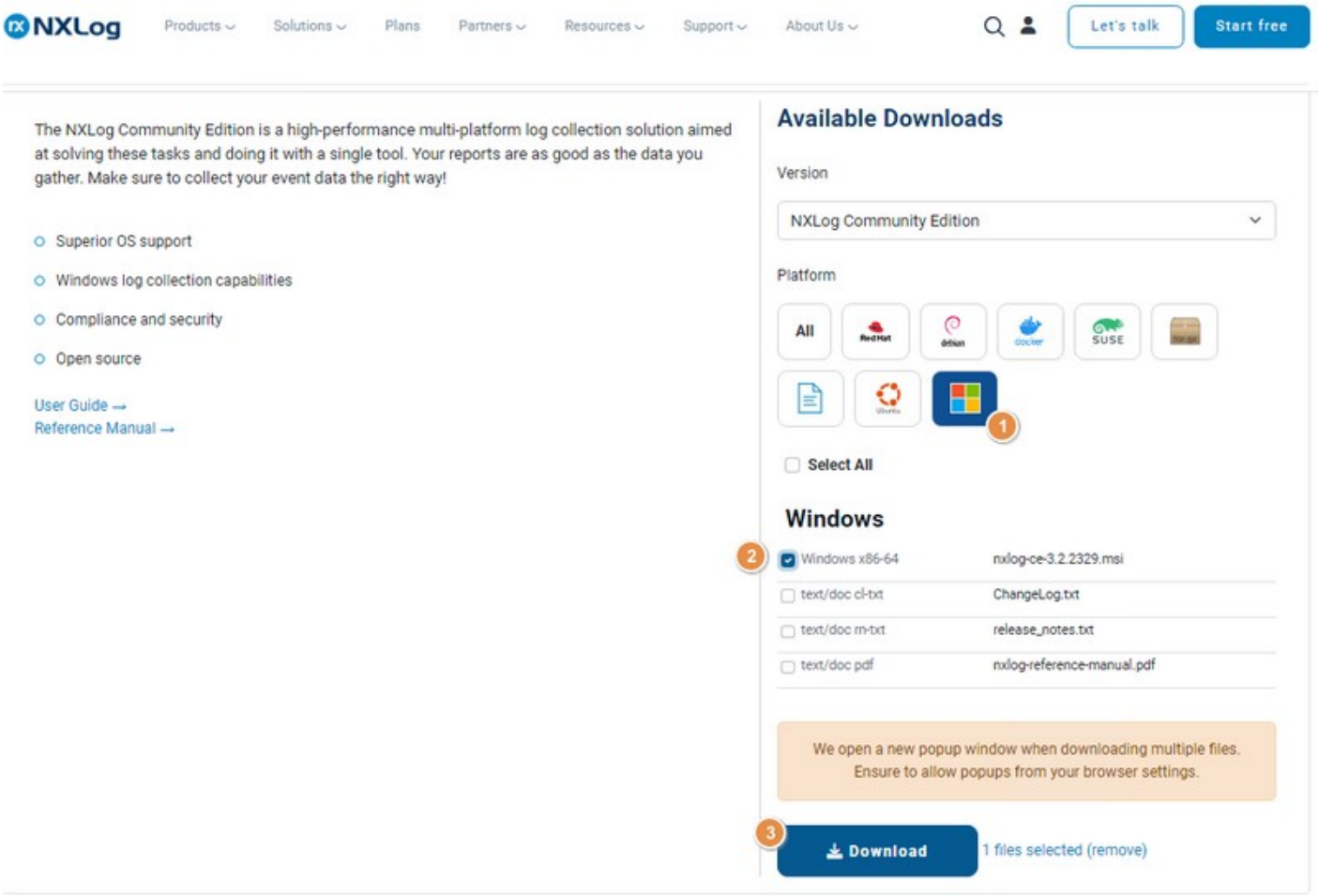
Graylog_UDP_NXLogs_Windows GELF UDP (6721f8280ac6780828d1f9ad) RUNNING

On node ⭐ 2e3090c8 / srv-graylog.it-connect.local

```
bind_address: 0.0.0.0
charset_name: UTF-8
decompress_size_limit: 8388608
number_worker_threads: 4
override_source: <empty>
port: 12201
recv_buffer_size: 262144
```

Maintenant téléchargez l'agent **NXLog** sur la machine qui va envoyer les logs :

- https://nxlog.co/downloads/nxlog-ce#nxlog-community-edition



Saisissez la configuration suivante dans le fichier **C:\Program Files\nxlog\conf\nxlog.conf** :

```
# Récupérer les journaux de l'observateur d'événements
<Input in>
```

```
    Module      im_msvistalog
</Input>

# Déclarer le serveur Graylog (selon input)
<Extension gelf>
    Module      xm_gelf
</Extension>

<Output graylog_udp>
    Module      om_udp
    Host        192.168.10.220
    Port        12201
    OutputType  GELF_UDP
</Output>

# Routage des flux in vers out
 <Route 1>
     Path       in => graylog_udp
 </Route>
```

> Celle-ci enverra tous les logs de la machine sur Graylog, ce qui n'est pas forcément nécessaire, on pourrait envoyer seulement les logs **Security** et appliquer la configuration suivante :

```
# Récupérer les journaux Security de l'observateur d'événements
<Input in>
    Module      im_msvistalog
    <QueryXML>
        <QueryList>
            <Query Id='1'>
                <Select Path='Security'>*</Select>
            </Query>
        </QueryList>
    </QueryXML>
</Input>

# Déclarer le serveur Graylog (selon input)
<Extension gelf>
    Module      xm_gelf
```

```
</Extension>

<Output graylog_udp>
    Module        om_udp
    Host          192.168.10.220
    Port          12201
    OutputType    GELF_UDP
</Output>

# Routage des flux in vers out
 <Route 1>
     Path        in => graylog_udp
 </Route>
```

Désormais relancez le service NXlog pour appliquer la configuration :

```
Restart-Service nxlog
```

> Le fichier de log de NXlog est le fichier **C:\Program Files\nxlog\data\nxlog.log** si vous devez debugger.

Revision #3
Created 5 June 2025 12:09:01 by Elieroc
Updated 5 June 2025 12:52:55 by Elieroc