Documentation technique - Mise en place de Graylog

Objectif

L'objectif de cette documentation est la mise en place de Graylog, un logiciel permettant de centraliser, d'indexer et de faciliter la lecture des logs. Il est capable de traiter les logs de plusieurs sources différentes, tout en créant des alertes.

Dans le cadre du projet Health North, cela va nous permettre d'identifier et de résoudre plus efficacement les incidents sur des services tels que le reverse proxy, les serveurs Web ou encore l'Active Directory.

Préparation de la machine virtuelle

Pour commencer, il faut d'abord installer Graylog. Pour cela, nous avons besoin de créer une machine virtuelle sous Ubuntu, avec un serveur équipé au minimum de 8 Go de RAM. Cette machine doit être positionnée dans le VLAN 170 avec une adresse IP fixe qui est : 10.170.0.11.

Préparation et installation de Graylog

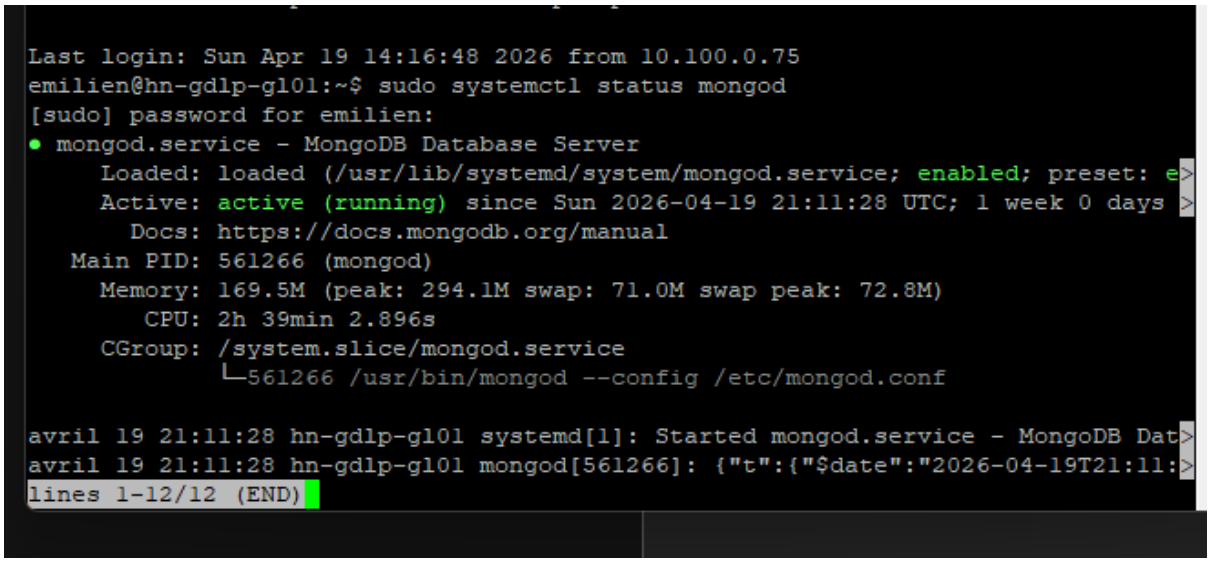
Dans un premier temps, nous devons installer OpenJDK 17, qui est requis pour le bon fonctionnement de Graylog.

Afin que Graylog fonctionne correctement, plusieurs composants sont nécessaires. Tout d'abord MongoDB, qu'il faut ajouter à la machine virtuelle, installer puis démarrer grâce aux commandes suivantes :

```
sudo apt install -y gnupg curl


curl -fsSL https://www.mongodb.org/static/pgp/server-8.0.asc | \
sudo gpg -o /usr/share/keyrings/mongodb-server-8.0.gpg --dearmor


echo "deb [ arch=amd64, arm64 signed-by=/usr/share/keyrings/mongodb-server-8.0.gpg ] https://repo.mongodb.org/apt/ubuntu noble/mongodb-org/8.0 multiverse" | \
sudo tee /etc/apt/sources.list.d/mongodb-org-8.0.list


sudo apt update
sudo apt install -y mongodb-org
sudo systemctl daemon-reload
sudo systemctl enable mongod
```

sudo systemctl start mongod

sudo systemctl status mongod



Dans un second temps, nous avons besoin d'installer OpenSearch qui est utilisé par Graylog afin d'indexer les logs reçus. Pour cela, nous devons ajouter le dépôt OpenSearch à Ubuntu, puis lancer l'installation. Pour finir, nous devons configurer OpenSearch à l'aide des commandes suivantes :

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

sudo apt update

sudo OPENSEARCH_INITIAL_ADMIN_PASSWORD='HNOpenSearch2026!' apt install -y opensearch

Une fois l'installation réalisée, nous pouvons donc configurer OpenSearch. Pour cela, il faut ouvrir le fichier de configuration suivant :

sudo nano /etc/opensearch/opensearch.yml

À l'intérieur de ce fichier, nous pouvons copier ceci :

cluster.name: graylog
node.name: HN-GDLP-GL01
path.data: /var/lib/opensearch
path.logs: /var/log/opensearch
network.host: 127.0.0.1
http.port: 9200
discovery.type: single-node
action.auto_create_index: false
plugins.security.disabled: true

Ensuite, nous pouvons configurer la mémoire vive utilisée par Java, dans notre cas 1 Go.
Pour cela il faut accéder au fichier de configuration de Java :

sudo nano /etc/opensearch/jvm.options

Une fois ouvert, nous pouvons ajouter les lignes suivantes :

-Xms1g
-Xmx1g

Pour configurer les paramètres système, nous devons utiliser ces commandes :

sudo sysctl -w vm.max_map_count=262144
echo "vm.max_map_count=262144" | sudo tee -a /etc/sysctl.conf

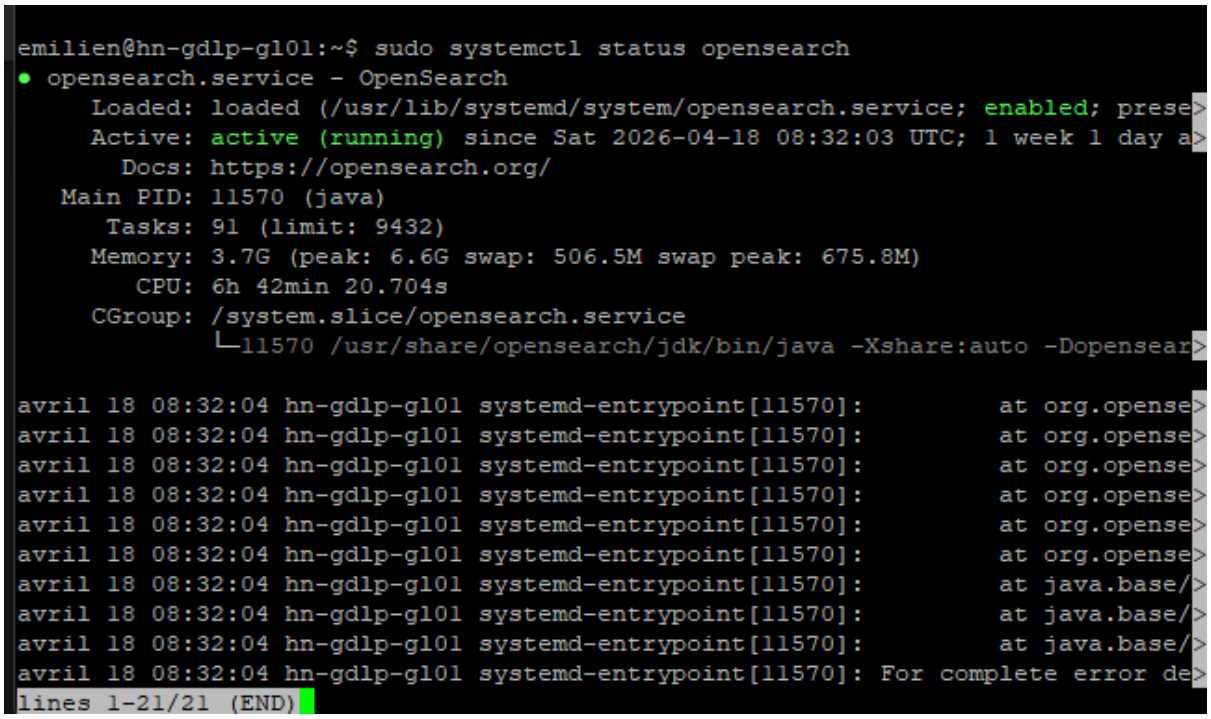
Dès que les paramètres sont modifiés, nous pouvons redémarrer OpenSearch afin d'appliquer la configuration.

sudo systemctl daemon-reload

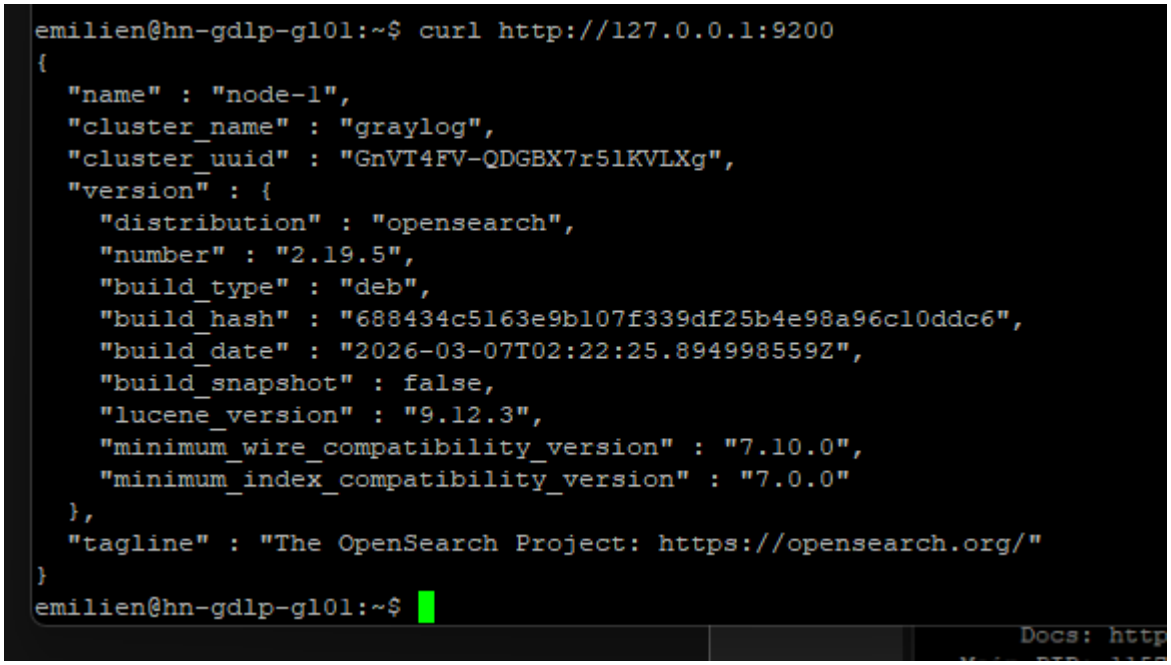
sudo systemctl enable opensearch

sudo systemctl start opensearch

sudo systemctl status opensearch



Nous pouvons ensuite tester le bon fonctionnement d'OpenSearch à l'aide de la commande suivante : http://127.0.0.1:9200



Ensuite, nous pouvons installer Graylog. Pour cela, nous devons ajouter le dépôt Graylog, puis lancer l'installation en suivant les commandes comme ceci :

wget https://packages.graylog2.org/repo/packages/graylog-7.0-repository_latest.deb

sudo dpkg -i graylog-7.0-repository_latest.deb

sudo apt update

sudo apt install -y graylog-server

Une fois l'installation terminée, nous pouvons accéder au fichier de configuration du serveur afin d'y ajouter les paramètres de sécurité. Nous devons définir un mot de passe fort, puis générer le hash avec ces commandes :

sudo nano /etc/graylog/server/server.conf

Dans ce fichier, nous devons renseigner :

password_secret = Le mots de passe ici

Puis générer le hash :

echo -n "mots de passe ici " | sha256sum

Puis remplir dans le fichier de configuration :

root_password_sha2 = HASH_SHA256_ICI

Puis nous pouvons ensuite configurer l'accès à Graylog ainsi que les différents services que nous avons installés plus tôt :

http_bind_address = 0.0.0.0:9000

http_external_uri = http://10.170.0.11:9000/

elasticsearch_hosts = http://127.0.0.1:9200

mongodb_uri = mongodb://localhost:27017/graylog

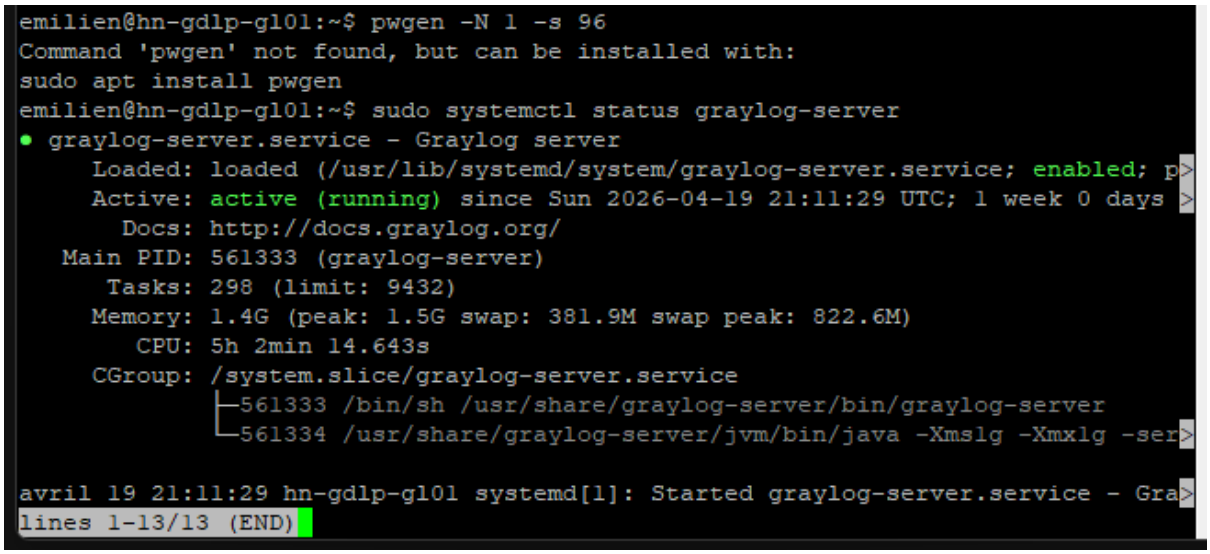
Puis nous pouvons démarrer le service Graylog à l'aide des commandes suivantes :

sudo systemctl daemon-reload

sudo systemctl enable graylog-server

sudo systemctl start graylog-server

sudo systemctl status graylog-server



Configuration de Graylog

Nous pouvons nous connecter à l'interface web via l'adresse suivante :

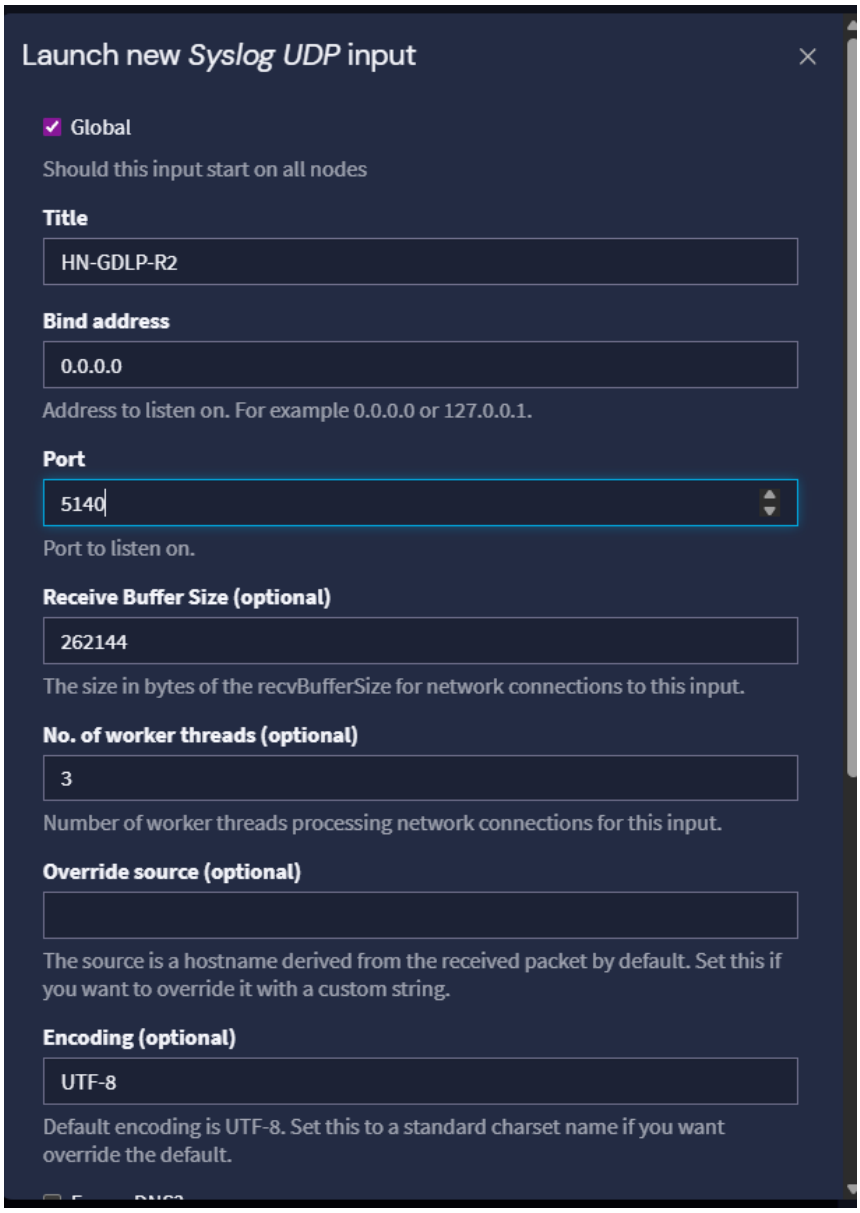
http://10.170.0.11:9000

L'identifiant est **admin**, et le mot de passe est celui défini précédemment.

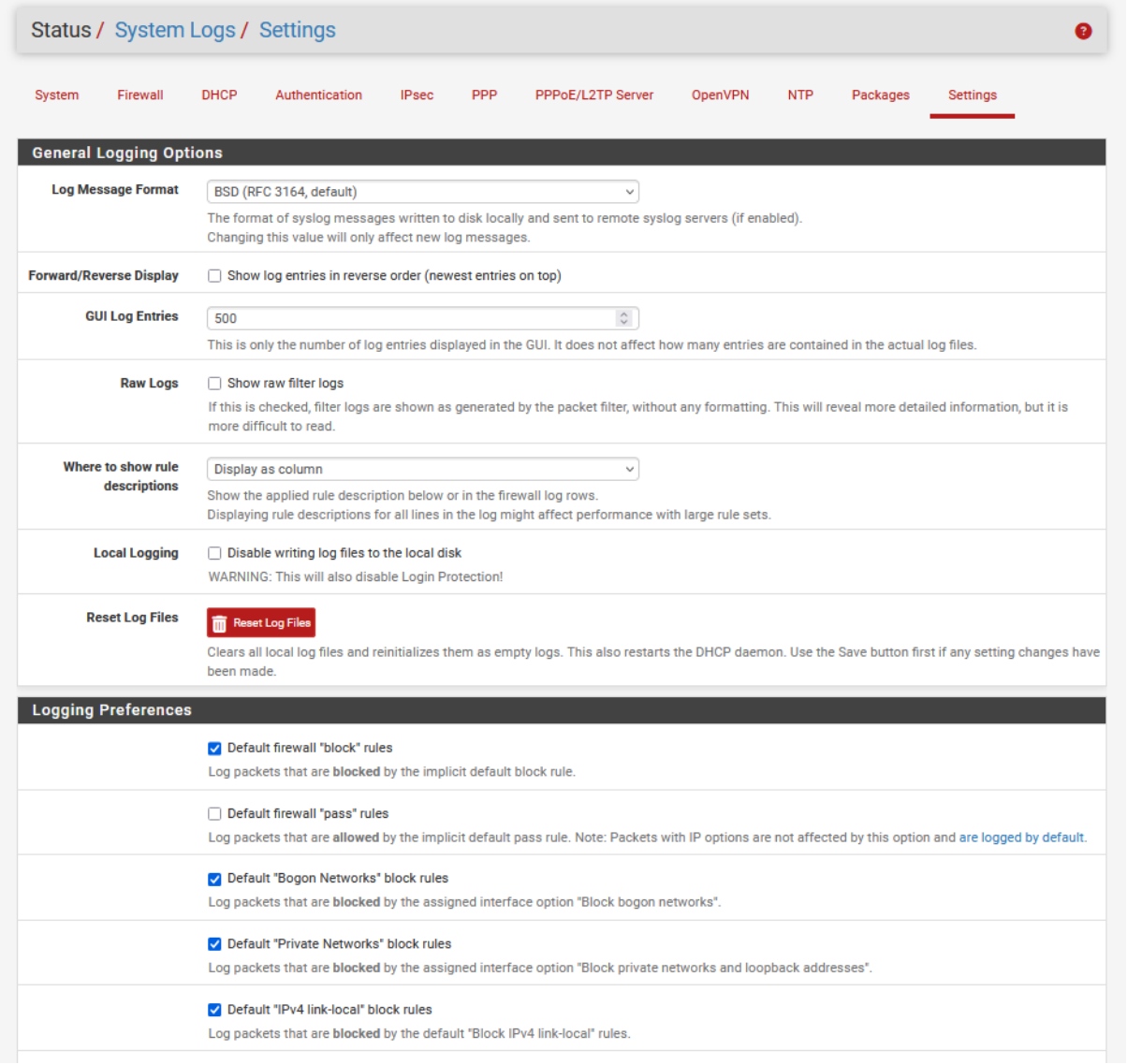
Ensuite, nous allons pouvoir créer un *input*. Dans Graylog, un input correspond à la porte d'entrée des logs, c'est par ce biais où ils vont entrer dans Graylog avant d'être indexés.

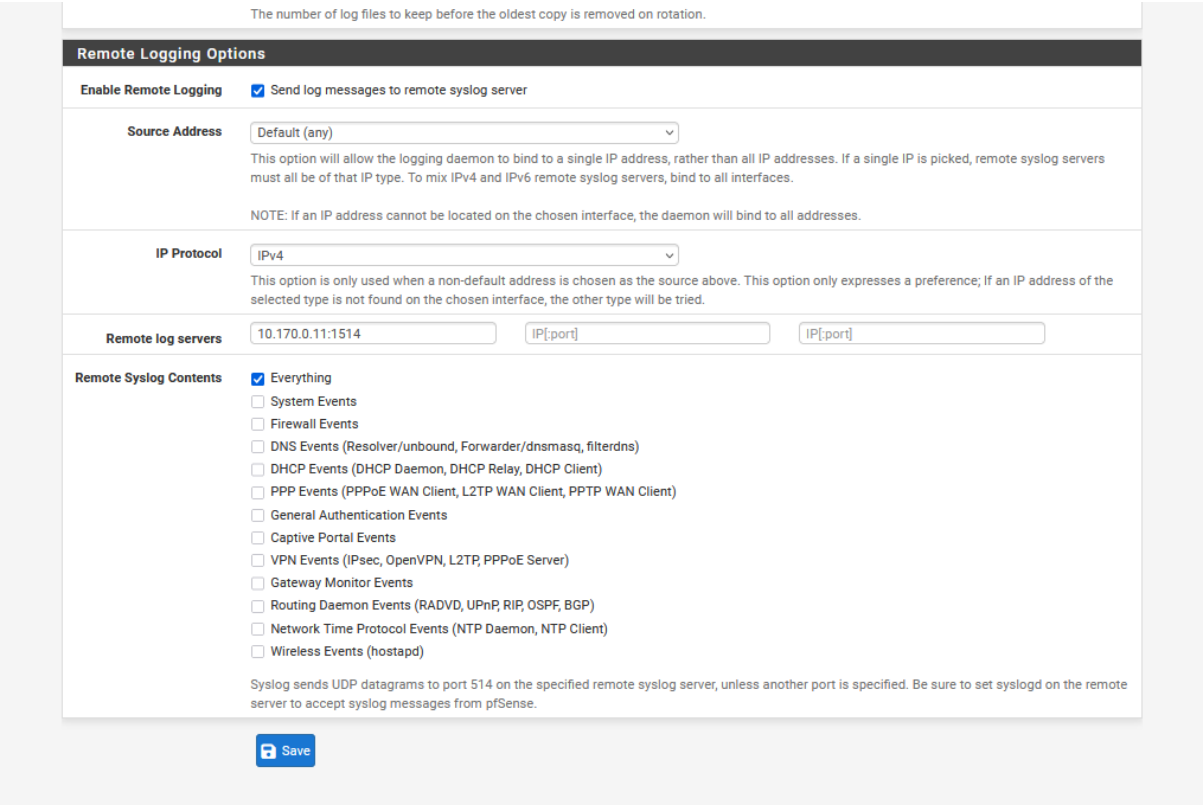
Dans la section «Imputs», nous allons pouvoir sélectionner Syslog UDP afin de recevoir les logs provenant de pfSense.

Nous pouvons ensuite attribuer un nom à cet input, ainsi que définir le port utilisé.



Ensuite, nous allons pouvoir configurer l'envoi des logs depuis pfSense. Pour cela, nous devons nous connecter à l'interface de configuration de pfSense, puis aller dans « System Logs » et « Settings », et configurer le remote logging en cochant l'option permettant d'envoyer l'intégralité des logs.


Status / System Logs / Settings
System
Firewall
DHCP
Authentication
IPsec
PPP
PPPoE/L2TP Server
OpenVPN
NTP
Packages
Settings
General Logging Options
Log Message Format
BSD (RFC 3164, default)
The format of syslog messages written to disk locally and sent to remote syslog servers (if enabled).
Changing this value will only affect new log messages.
Forward/Reverse Display
Show log entries in reverse order (newest entries on top)
GUI Log Entries
500
This is only the number of log entries displayed in the GUI. It does not affect how many entries are contained in the actual log files.
Raw Logs
Show raw filter logs
If this is checked, filter logs are shown as generated by the packet filter, without any formatting. This will reveal more detailed information, but it is more difficult to read.
Where to show rule descriptions
Display as column
Show the applied rule description below or in the firewall log rows.
Displaying rule descriptions for all lines in the log might affect performance with large rule sets.
Local Logging
Disable writing log files to the local disk
WARNING: This will also disable Login Protection!
Reset Log Files
Reset Log Files
Clears all local log files and reinitializes them as empty logs. This also restarts the DHCP daemon. Use the Save button first if any setting changes have been made.
Logging Preferences
Default firewall "block" rules
Log packets that are blocked by the implicit default block rule.
Default firewall "pass" rules
Log packets that are allowed by the implicit default pass rule. Note: Packets with IP options are not affected by this option and are logged by default.
Default "Bogon Networks" block rules
Log packets that are blocked by the assigned interface option "Block bogon networks".
Default "Private Networks" block rules
Log packets that are blocked by the assigned interface option "Block private networks and loopback addresses".
Default "IPv4 link-local" block rules
Log packets that are blocked by the default "Block IPv4 link-local" rules.



Pour un serveur Linux, il est également nécessaire d'ajouter un input dans Graylog, puis d'installer rsyslog et de configurer l'envoi des logs comme ceci :

sudo apt update

sudo apt install -y rsyslog

sudo nano /etc/rsyslog.d/90-graylog.conf

. @10.170.0.11: le port que l'on a choisi

Puis, nous pouvons redémarrer rsyslog :

sudo systemctl restart rsyslog

sudo systemctl enable rsyslog

Pour un serveur Windows, nous pouvons utiliser NXLog, qui permet de centraliser les logs de la machine et de les envoyer vers Graylog.

Après installation, nous pouvons modifier le fichier de configuration et y entrer :

define ROOT C:\Program Files\nxlog

```
define CERTDIR %ROOT%\cert

define CONFDIR %ROOT%\conf

define LOGDIR %ROOT%\data


Moduledir %ROOT%\modules

CacheDir %ROOT%\data

Pidfile %ROOT%\data\nxlog.pid

SpoolDir %ROOT%\data

LogFile %ROOT%\data\nxlog.log


<Input eventlog>

    Module im_msvistalog

</Input>


<Output graylog>

    Module om_udp

    Host 10.170.0.11

    Port 1514

    Exec to_syslog_bsd();

</Output>


<Route route1>

    Path eventlog => graylog

</Route>
```

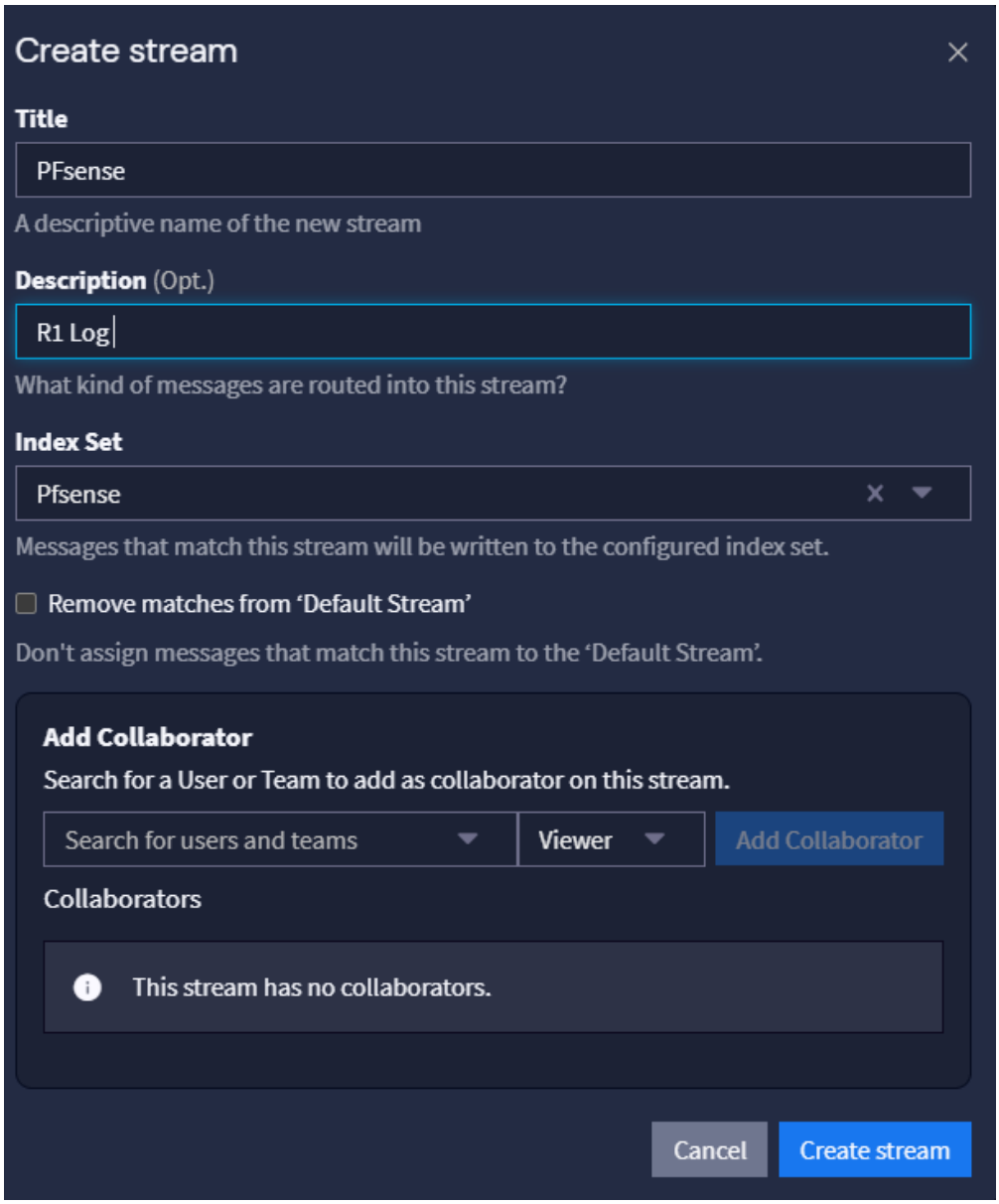
Une fois les trois différents inputs créés, nous pouvons créer des streams dans Graylog afin d'organiser et de filtrer les logs selon leur provenance ou leur type.

Création des Stream

Les streams permettent de séparer les logs selon leur source.

Pour cela, nous devons nous rendre dans « Streams », et cliquer sur « Create Stream ».

Ensuite, il suffit de donner un nom à notre stream, et sélectionner l'index pfSense.

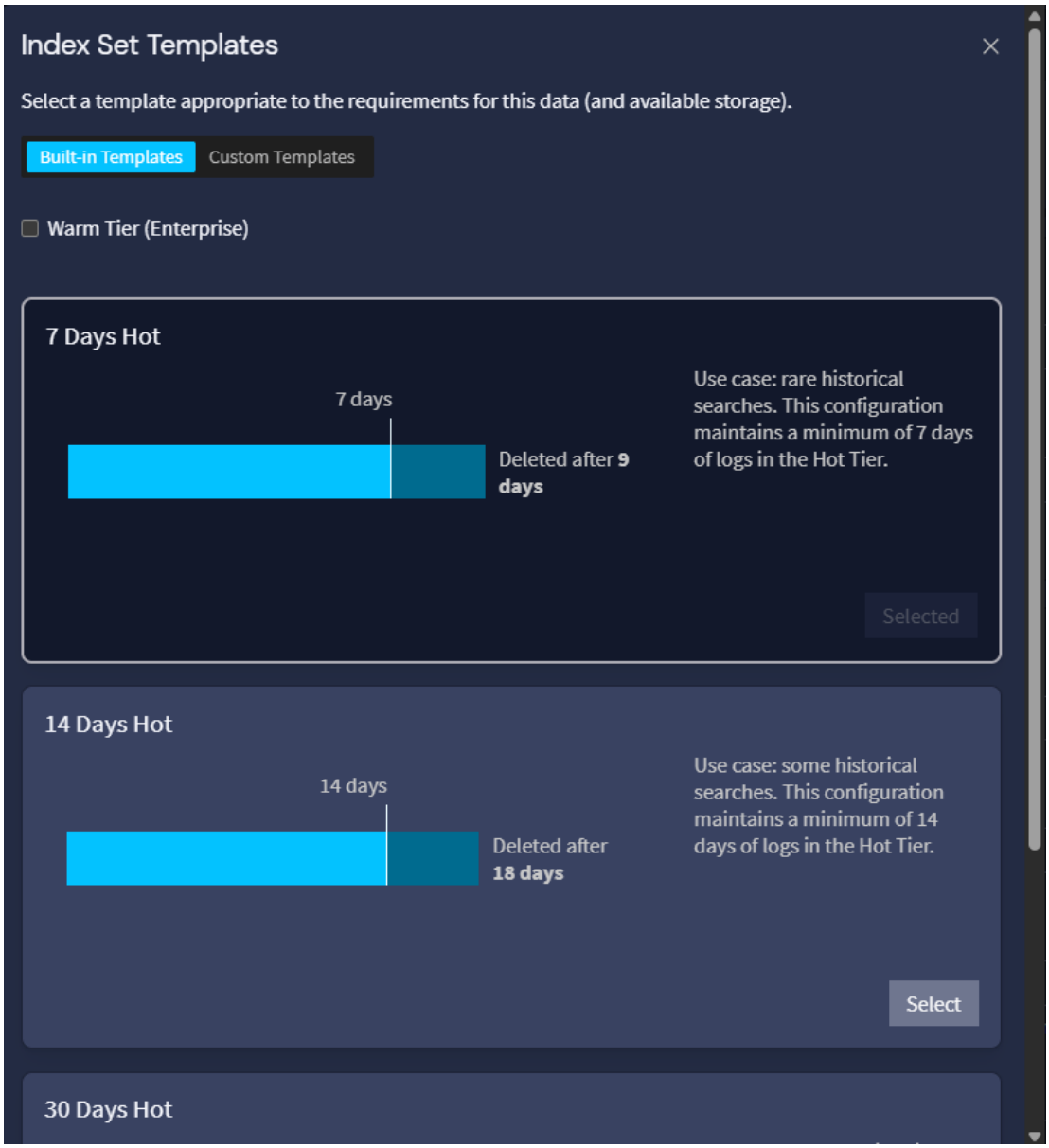


Création des index

Les index vont permettre de gérer la durée de stockage des logs.

Pour cela, nous devons nous rendre dans « System », puis « Indices », et créer des index en cliquant sur « Create Index ».

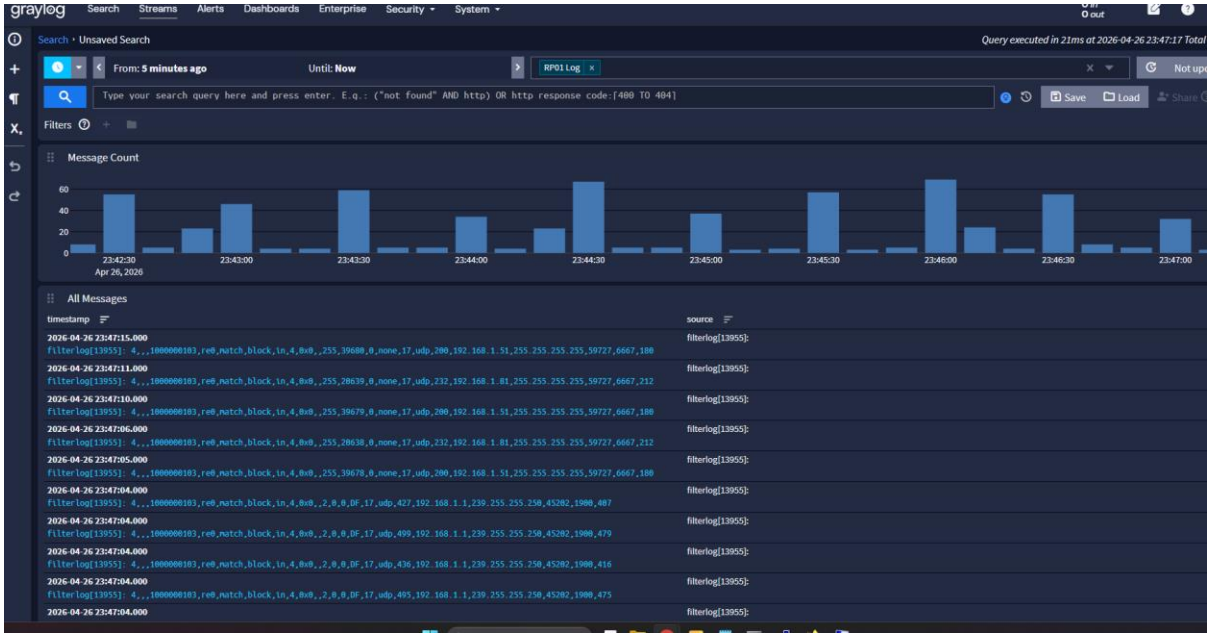
Ici, nous allons pouvoir choisir la durée minimum et maximale de conservation des logs.



Ensuite, nous choisir un nom à notre index et définir si l'on souhaite modifier la durée de rétention des logs.

Utilisation de Graylog

Une fois nos stream correctement configurés, nous pouvons nous rendre dans l'onglet «Streams», puis cliquer sur le stream dans lequel on souhaite consulter les logs afin de visualiser les logs de la machine.



Un des axes d'amélioration possible est la création d'alertes afin d'être prévenu en cas de logs spécifiques.

Également, il serait pertinent d'ajouter l'ensemble de nos serveurs afin d'obtenir un regroupement complet des logs, ainsi que de pouvoir augmenter la capacité de stockage du serveur pour améliorer la rétention des logs.