Graylog - Configuration

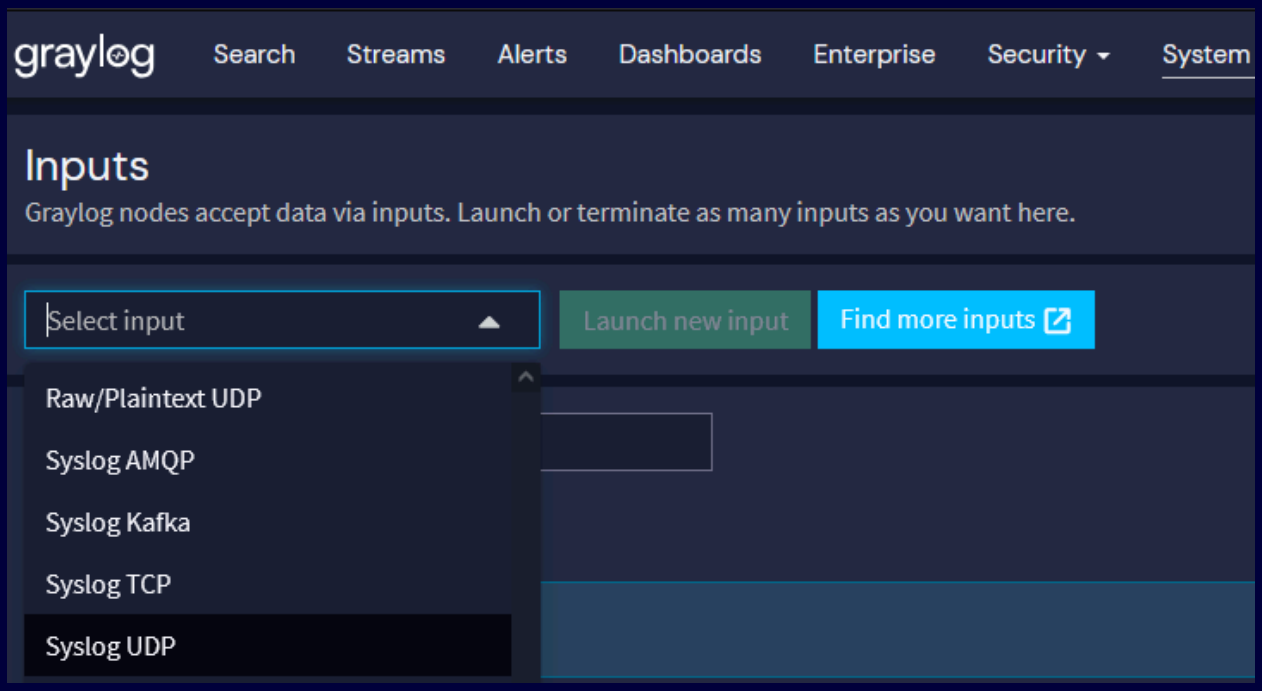
FRELAUT
Raphaël
BTSSIO

Sommaire :

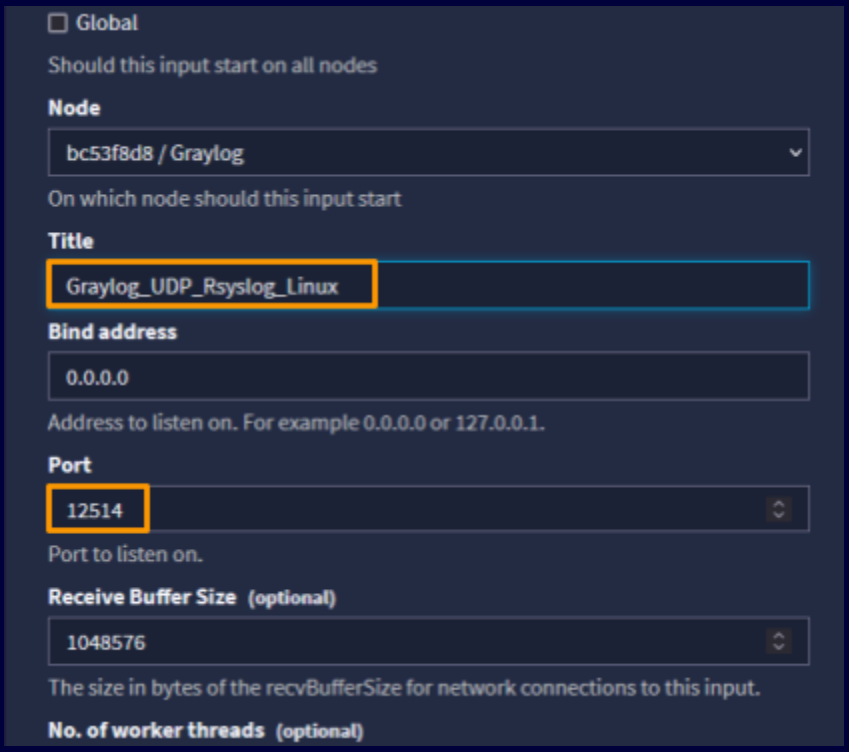
1. Installation sur un poste Linux

A. Creation d'un input Syslog

Connectez-vous à l'interface de Graylog, cliquez sur "**System**" dans le menu puis sur "**Inputs**". Dans la liste déroulante, sélectionnez "**Syslog UDP**" puis cliquez sur le bouton intitulé "**Launch new input**". Il est également possible de créer un Input Syslog en TCP, mais cela implique d'utiliser un certificat TLS : c'est un plus pour la sécurité, mais ce point ne sera pas abordé dans cet article.

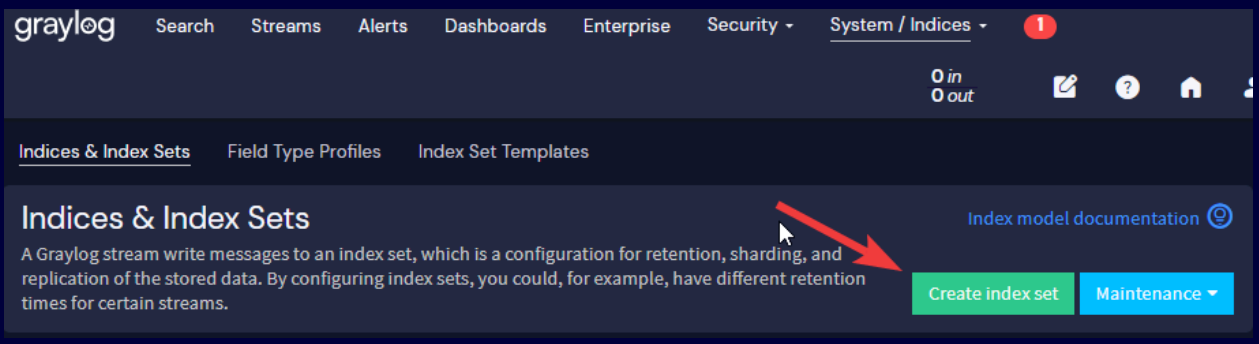


Un assistant va s'afficher à l'écran. Commencez par donner un nom à cet Input, par exemple "**Graylog_UDP_Rsyslog_Linux**" et choisissez un port. Par défaut, le port est "**514**" mais vous pouvez le personnaliser. Ici, le port "**12514**" est retenu.



Node: La base de données ou seront stockés les logs
Bind address : sur quelle adresse l'input va écouter. Ici on met 0.0.0.0 pour écouter sur toutes les interfaces.
Port: Sur quelle port écouter.

B. Création du nouvel index :



Nommez cet index, par exemple "Linux Index", ajoutez une description et un préfixe, avant de valider. Ici, nous allons stocker tous les journaux Linux dans cet index. Il est également possible de créer des index spécifiques pour stocker uniquement certains logs (uniquement les logs SSH, du service Web, etc...).
Configuration exemple ci-dessous :

Indices & Index Sets | Field Type Profiles | Index Set Templates

Configure Index Set

Index model documentation

Modify the current configuration for this index set, allowing you to customize the retention, sharding, and replication of messages coming from one or more streams.

Configuration Information

Title

Linux set

Descriptive name of the index set.

Description

Index pour les journau Linux

Add a description of this index set.

Details

Index Shards

1

Number of search cluster Shards used per index in this Index Set. Increasing the Index Shards improves the search cluster write speed of data stored to this Index Set by distributing the active write Index over multiple search nodes. Increasing the Index Shards can degrade search performance and increases the memory footprint of the Index. This value should not be set higher than the number of search nodes.

Index Replica

0

Number of search cluster Replica Shards used per Index in this Index Set. Adding Replica Shards improves search performance during parallel reads of the index, such as occurs on dashboards, and is a component of HA and backup strategy. Each Replica Shard set multiplies the storage requirement and memory footprint of the index. This value should not be set higher than the number of search nodes, and typically not higher than 1.

Maximum Number of Segments

1

Advanced Option. Maximum number of segments per Search Cluster Index after optimization (force merge). Setting higher values decreases the compression ratio of Index Optimization.

☐ Disable Index Optimization after Rotation

Advanced Option. Index Optimization is a compression process that occurs after an active Index has been rotated and reduces the size of an Index on disk. It manifests as a CPU intensive maintenance task performed by the search cluster after Index rotation. Compressing Indexes improves search performance and decreases the storage footprint of Index Sets.

Field Type Refresh Interval

5 seconds

Advanced Option. How often the Field Type Information for the active write Index will be updated. Setting this value higher can marginally reduce search cluster overhead and improve performance, but will result in new data messages longer to be searchable in Graylog.

Rotation & Retention

Data Tiering | Legacy (Deprecated)

Max. days in storage

40

After how many days your data should be deleted.

Min. days in storage

30

How many days at minumum your data should be stored.

Field Type Profile

With index set field type profiles you can bundle up custom field types into profiles. You can assign any profile to this index set. To see and use profile setting for index set, you have to rotate indices.

Index field type mapping profile

Select index field type profile

Update index set | Cancel

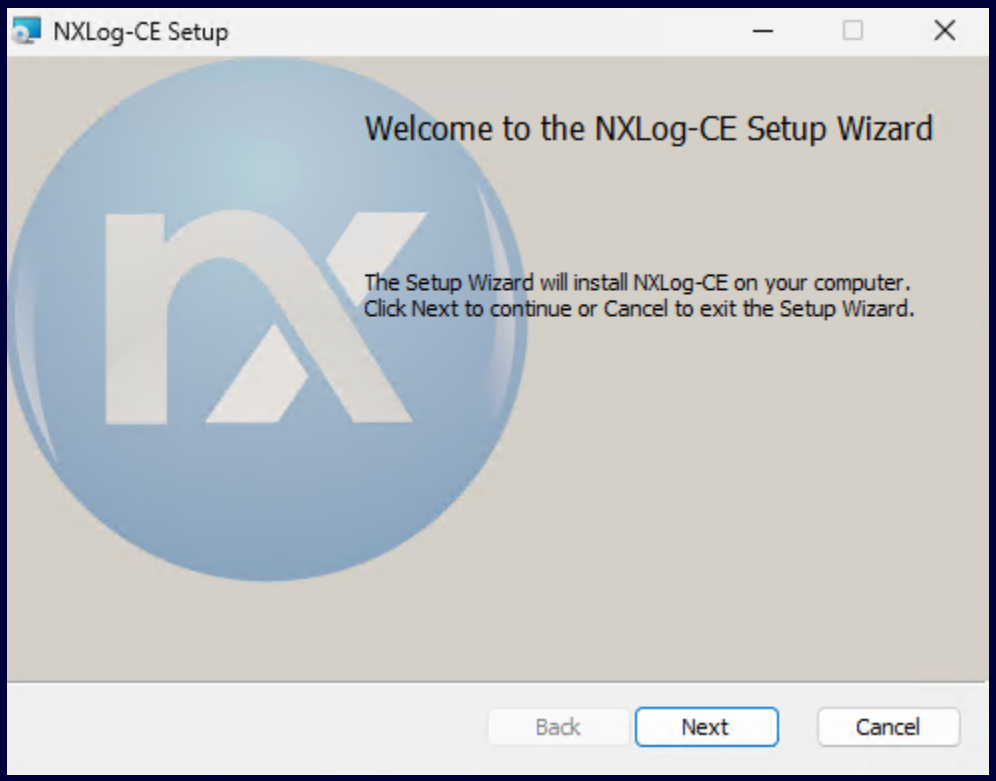
2. Installation pour un poste Windows :

A. Installation NXLOG :

Il faudra tout d'abord installer NXlog via ce lien:

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

Et selectionner la version msi : nxlog-ce-3.2.2329.msi
Lancer le .msi puis suivre les étapes jusqu'à la fin de l'installation :



Le fichier de configuration d'NXLog se trouve a l'emplacement :
C:\Program Files\nxlog\conf\nxlog.conf

En complément de la configuration déjà présente dans le fichier "nxlog.conf", vous devez ajouter ces lignes à la fin

```
# 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          193.253.40.180
    Port      12222
    OutputType    GELF_UDP
</Output>

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

Sauvegardez les changements et redémarrez le service NXLog à partir d'une console PowerShell ouverte en tant qu'administrateur (ou via la console Services).

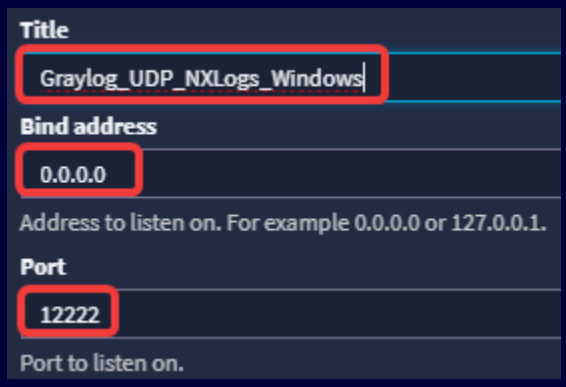
```
Restart-Service nxlog
```

Si vous ne recevez pas de logs sur Graylog, le fichier de logs d'NXLog peut s'avérer utile.

```
C:\Program Files\nxlog\data\nxlog.log
```

B. Création d’un input pour windows

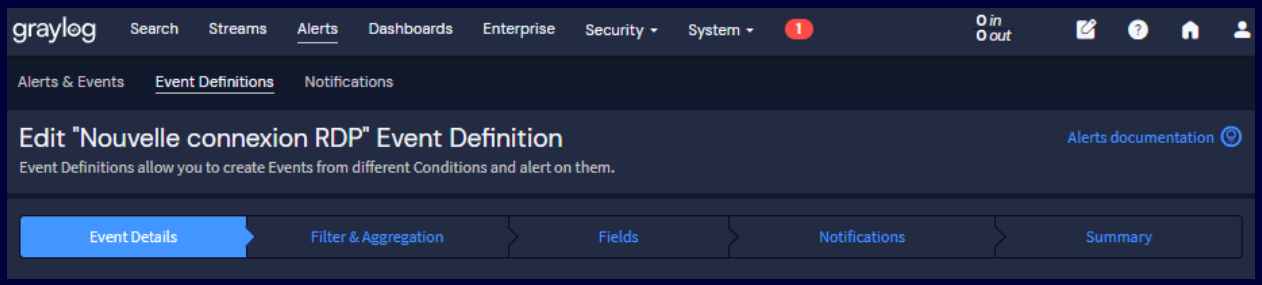
À partir de l'interface web de Graylog, cliquez sur le menu "Système" puis sur "Inputs". Ensuite, sélectionnez "GELF UDP" dans la liste, puis cliquez sur "Launch new input". Puis remplir les cases avec les bonnes informations :



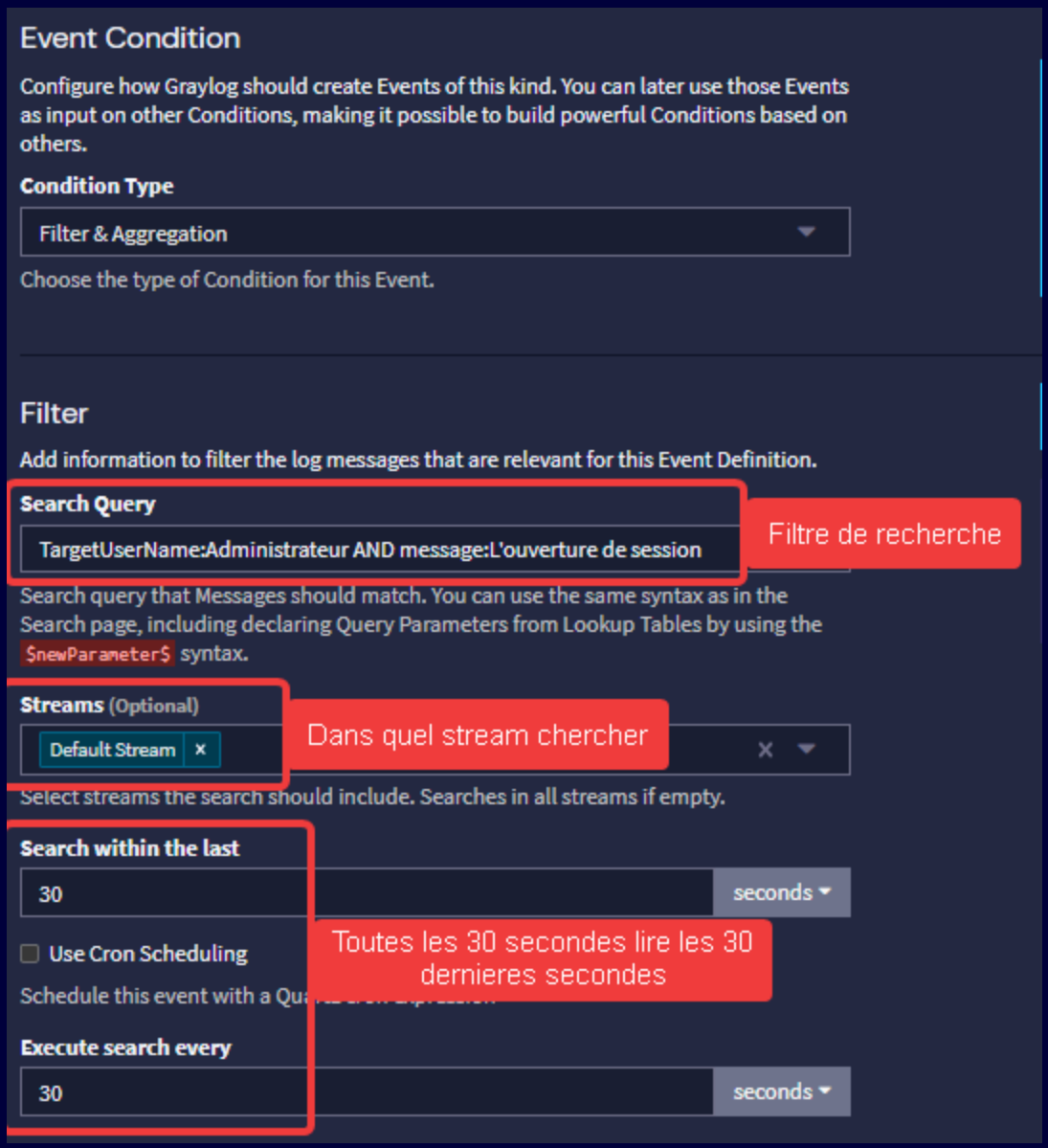
3. Configuration des alertes

1. Alerte lors d’une nouvelle connexion RDP vers WS2022

Le système d’alerte sous Graylog est sous forme d'Évent qui entraîne une notification. Il font donc tout d’abord faire un évent.

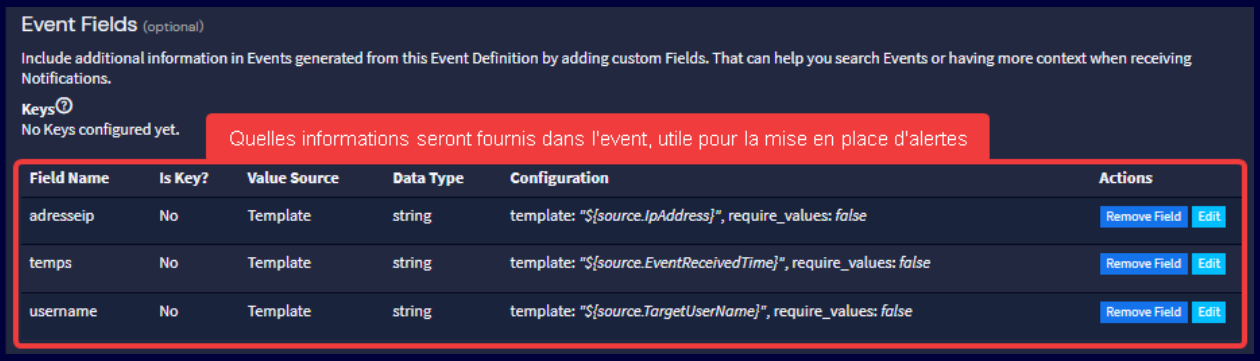


Dans l’onglet Event Detail, lui donner un nom puis une description, dans l’onglet Filter & Aggregation :

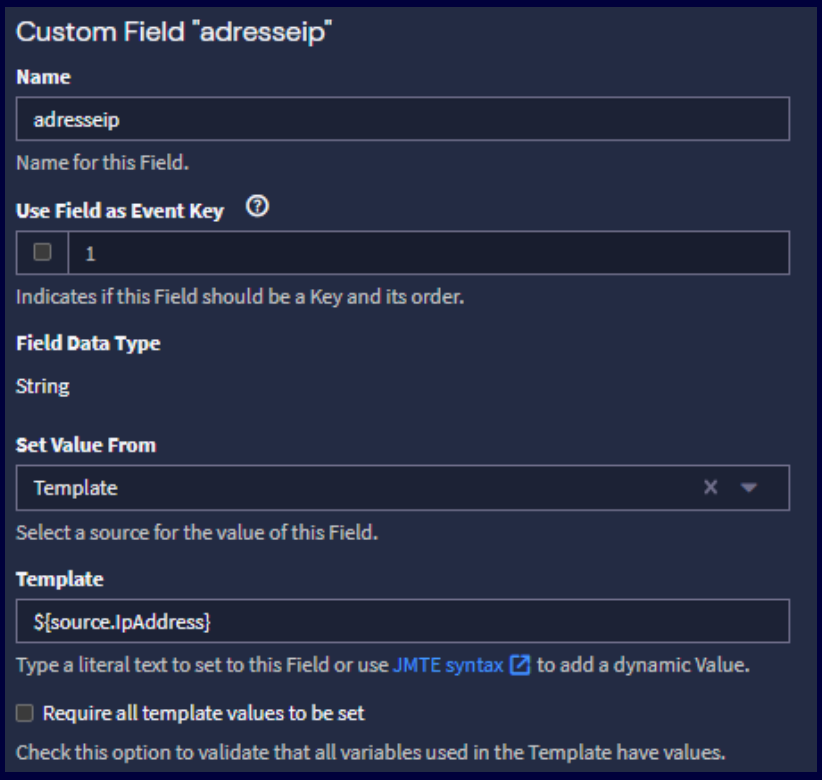


Ici le filtre n'alerte qu'en cas de logs respectant le filtre. C'est a dire : L'utilisateur est *Administrateur* et le message contient "*L'ouverture de session*". Basiquement, une notification sera envoyée à chaque fois que l'utilisateur Administrateur se connecte.

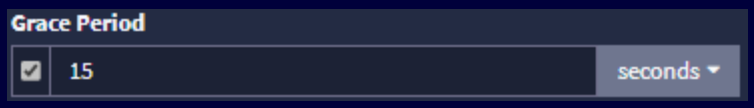
Dans l'onglet suivant, les events fields sont les info remonté avec l'event(extractors). Ici nous recuperons les informations ipAdress, EventReceivedTime et TargetUserName visible dans la colonne Configuration. Ces informations seront stocké sous le nom lié dans la colonne Field Name



Exemple :



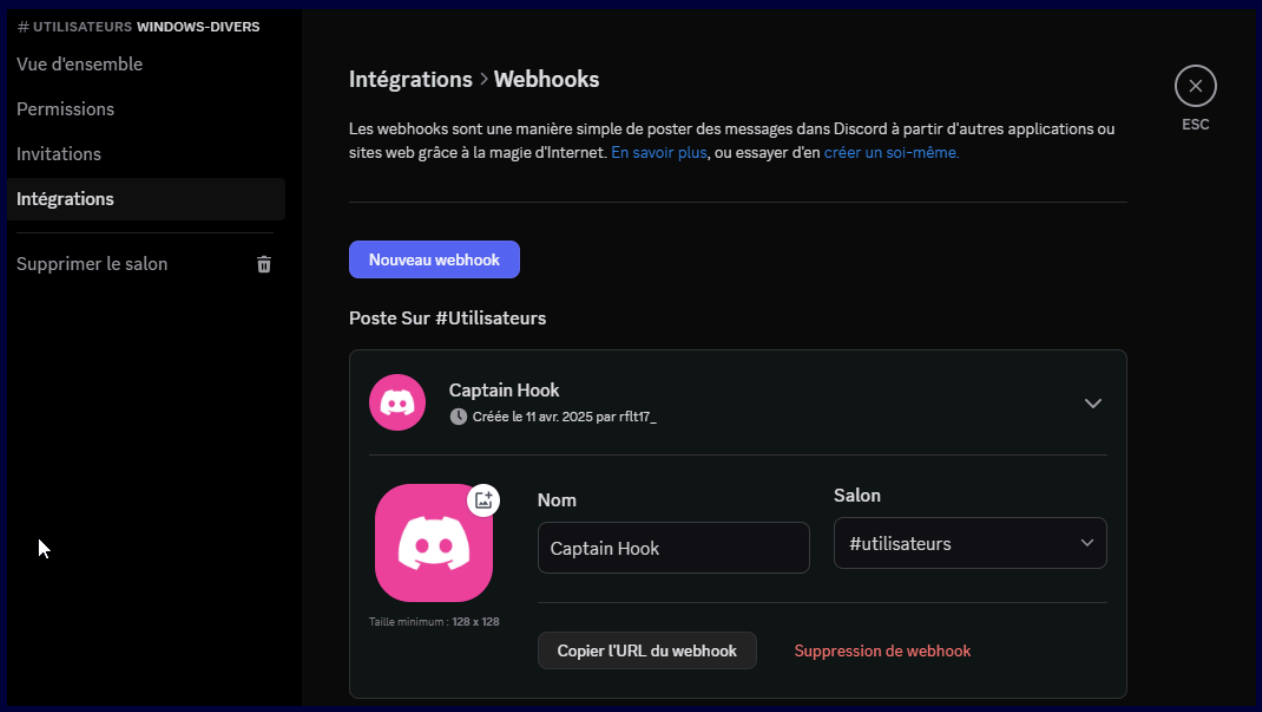
Ensuite dans l'onglet notification, nous y mettrons la notification lorsque nous l'aurons créée. Pour l'instant, mettre une période de grâce de 15 secondes afin d'éviter le SPAM et les doublons.



2. Mise en place de la notification

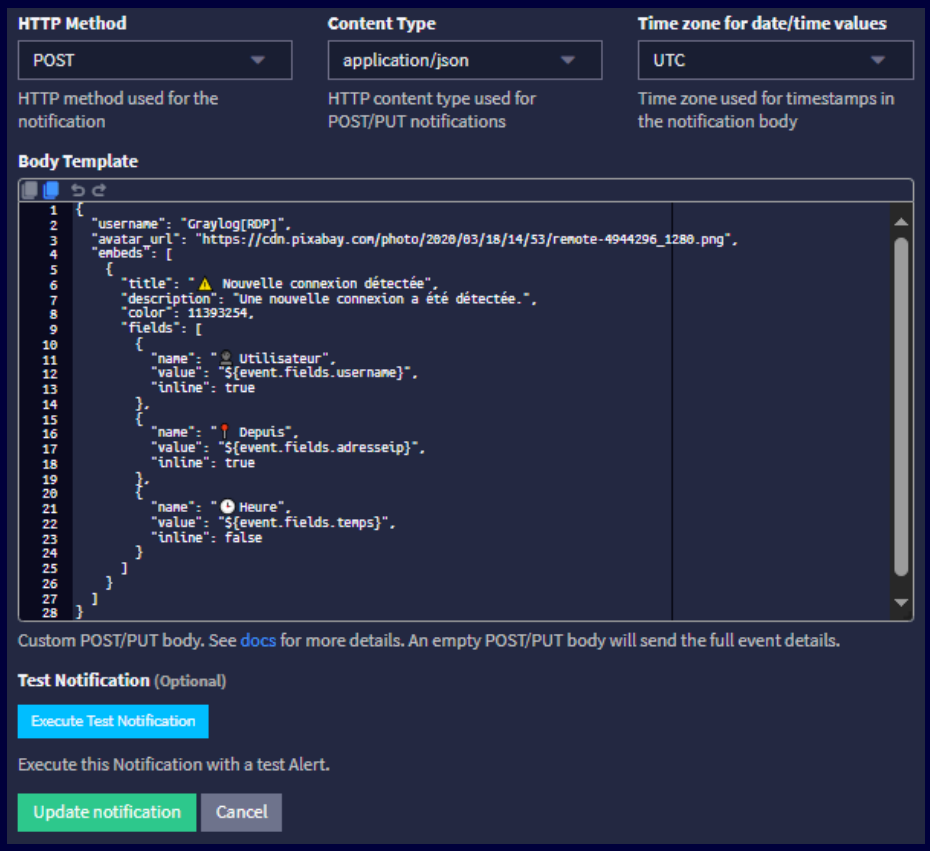
Ici, à des fins de simplicité, nous mettons en place des notifications vers **DISCORD.** Et partons du principe que le serveur DISCORD est déjà créé. L'utilisation d'un robot discord peut être envisagé mais le webhook est plus simple.

Dans les paramètres du channel ou la notification sera envoyé, créer et récupérer le webhook.

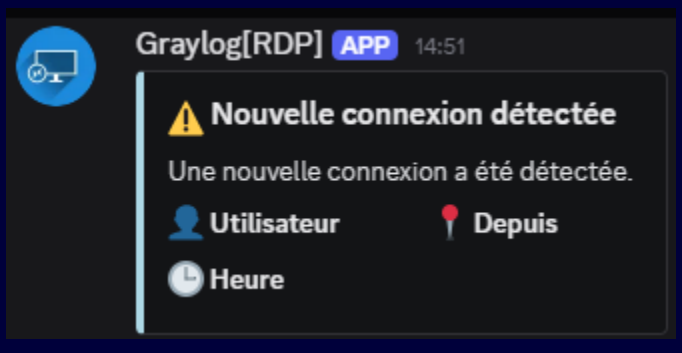


Sur l'interface web graylog, se rendre dans Alerts > Notification > Créer une nouvelle notification.

Laisser les paramètres par défaut et changer les suivants :



Dans le Body Template, se trouve le contenu de la notification. Nous avons précédemment mis en place les fields dans l'Event, c'est ici que nous les entrons sous la forme ${event.fields.***nomdufield***}.
Une notification de test peut etre envoyé :



Pas d'informations ici, il s'agit d'un test.

Si tout fonctionne comme prévu, a chaque connexion de l'utilisateur administrateur, Une notification est déclenchée.

Aides Complémentaires :

Comment envoyer les logs Linux vers Graylog avec rsyslog ?
Comment envoyer les logs Windows vers Graylog avec NXLog ?
NXLog - Achieve complete security observability with powerful insights from your log data.