

Graylog - Configuration



Lycée Elie Vinet

Barbezieux Saint-Hilaire (16)

FRELAUT
Raphaël
BTSSIO

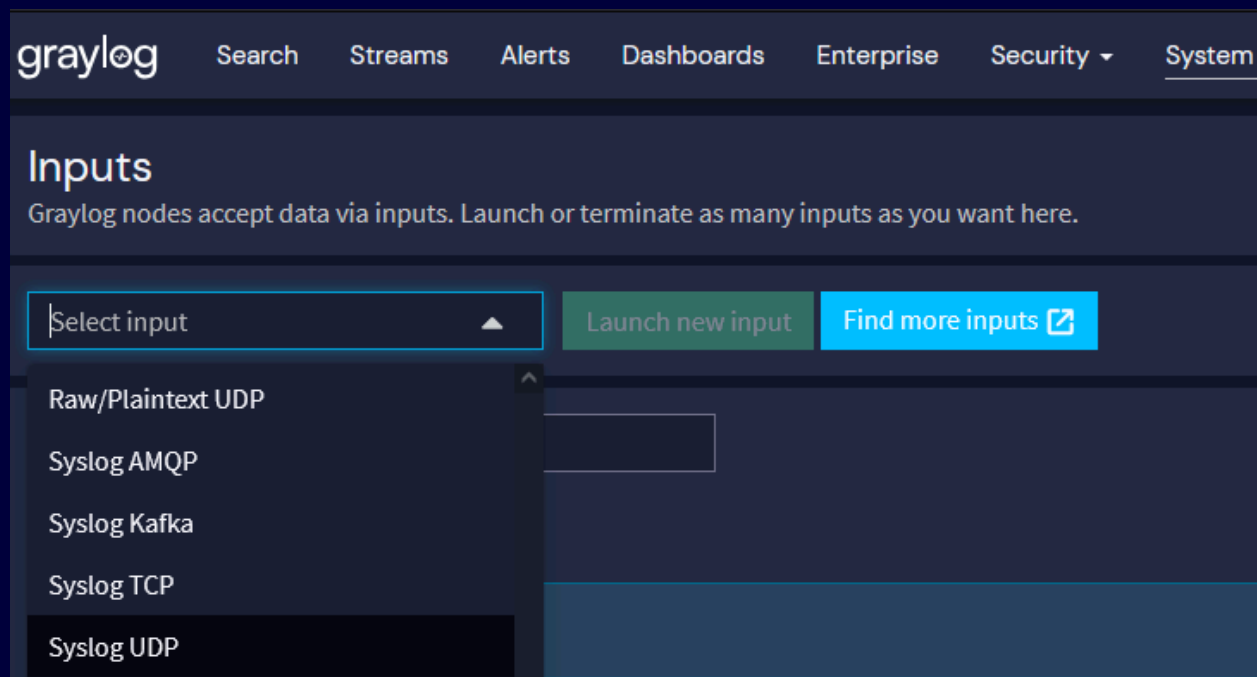
Sommaire :

1. Installation sur un poste Linux	3
A. Creation d'un input Syslog	3
B. Création du nouvel index :	4
2. Installation pour un poste Windows :	6
A. Installation NXLOG :	6
B. Création d'un input pour windows	8
3. Configuration des alertes	8
1. Alerte lors d'une nouvelle connexion RDP vers WS2022	8
2. Mise en place de la notification	11
Aides Complémentaires :	13

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.

☐ Global
Should this input start on all nodes

Node
bc53f8d8 / Graylog

On which node should this input start

Title
Graylog_UDP_Rsyslog_Linux

Bind address
0.0.0.0
Address to listen on. For example 0.0.0.0 or 127.0.0.1.

Port
12514
Port to listen on.

Receive Buffer Size (optional)
1048576
The size in bytes of the recvBufferSize for network connections to this input.

No. of worker threads (optional)

Node: La base de données où 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 :

The screenshot shows the Graylog web interface. The top navigation bar includes 'graylog', 'Search', 'Streams', 'Alerts', 'Dashboards', 'Enterprise', 'Security', and 'System / Indices'. Below this, there's a sub-navigation bar with 'Indices & Index Sets', 'Field Type Profiles', and 'Index Set Templates'. The main content area is titled 'Indices & Index Sets' and contains a description: 'A Graylog stream write messages to an index set, which is a configuration for retention, sharding, and replication of the stored data. By configuring index sets, you could, for example, have different retention times for certain streams.' At the bottom right of this section, there are two buttons: 'Create index set' (green) and 'Maintenance' (blue). A red arrow points to the 'Create index set' button.

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 :

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 journaux 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 minimum 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 :

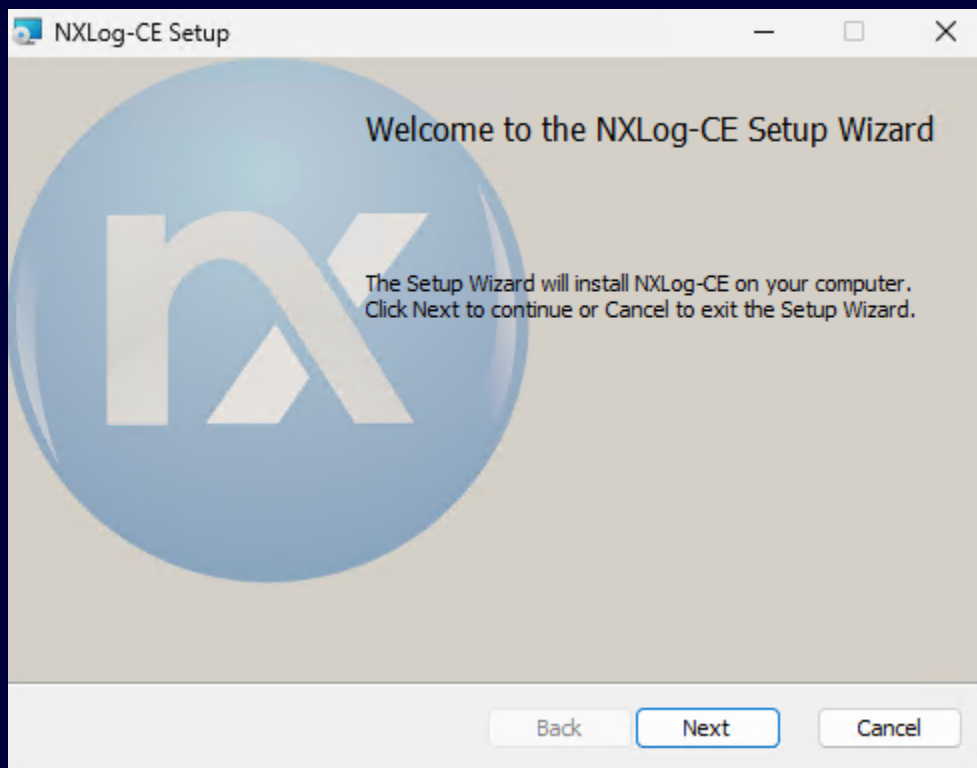
A. Installation NXLOG :

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

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

Et sélectionner 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 à 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 :

Title
Graylog_UDP_NXLogs_Windows

Bind address
0.0.0.0
Address to listen on. For example 0.0.0.0 or 127.0.0.1.

Port
12222
Port to listen on.

3. Configuration des alertes

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

Le système d'alerte sous Graylog est sous forme d'Événement qui entraîne une notification. Il faut donc tout d'abord faire un événement.

graylog Search Streams Alerts Dashboards Enterprise Security System 1 0 in 0 out

Alerts & Events Event Definitions Notifications

Edit "Nouvelle connexion RDP" Event Definition Alerts documentation

Event Definitions allow you to create Events from different Conditions and alert on them.

Event Details Filter & Aggregation Fields Notifications Summary

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

Event Condition

Configure how Graylog should create Events of this kind. You can later use those Events as input on other Conditions, making it possible to build powerful Conditions based on others.

Condition Type

Filter & Aggregation

Choose the type of Condition for this Event.

Filter

Add information to filter the log messages that are relevant for this Event Definition.

Search Query

TargetUserName:Administrateur AND message:L'ouverture de session

Search query that Messages should match. You can use the same syntax as in the Search page, including declaring Query Parameters from Lookup Tables by using the `$newParameter$` syntax.

Streams (Optional)

Default Stream

Dans quel stream chercher

Select streams the search should include. Searches in all streams if empty.

Search within the last

30

seconds

☐ Use Cron Scheduling

Toutes les 30 secondes lire les 30 dernières secondes

Execute search every

30

seconds

Ici le filtre n'alerte qu'en cas de logs respectant le filtre. C'est à 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 ipAddress, EventReceivedTime et TargetUserName visible dans la colonne Configuration. Ces informations seront stocké sous le nom lié dans la colonne Field Name

Event Fields (optional)
Include additional information in Events generated from this Event Definition by adding custom Fields. That can help you search Events or having more context when receiving Notifications.
Keys ⓘ
No Keys configured yet.

Quelles informations seront fournis dans l'event, utile pour la mise en place d'alertes

Field Name	Is Key?	Value Source	Data Type	Configuration	Actions
adresseip	No	Template	string	template: "\${source.IpAddress}", require_values: false	Remove Field Edit
temps	No	Template	string	template: "\${source.EventReceivedTime}", require_values: false	Remove Field Edit
username	No	Template	string	template: "\${source.TargetUserName}", require_values: false	Remove Field Edit

Exemple :

Custom Field "adresseip"

Name

Name for this Field.

Use Field as Event Key ⓘ
☐ 1
Indicates if this Field should be a Key and its order.

Field Data Type
String

Set Value From
 × ▼
Select a source for the value of this Field.

Template

Type a literal text to set to this Field or use [JMTE syntax](#) ⓘ to add a dynamic Value.
☐ **Require all template values to be set**
Check this option to validate that all variables used in the Template have values.

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.

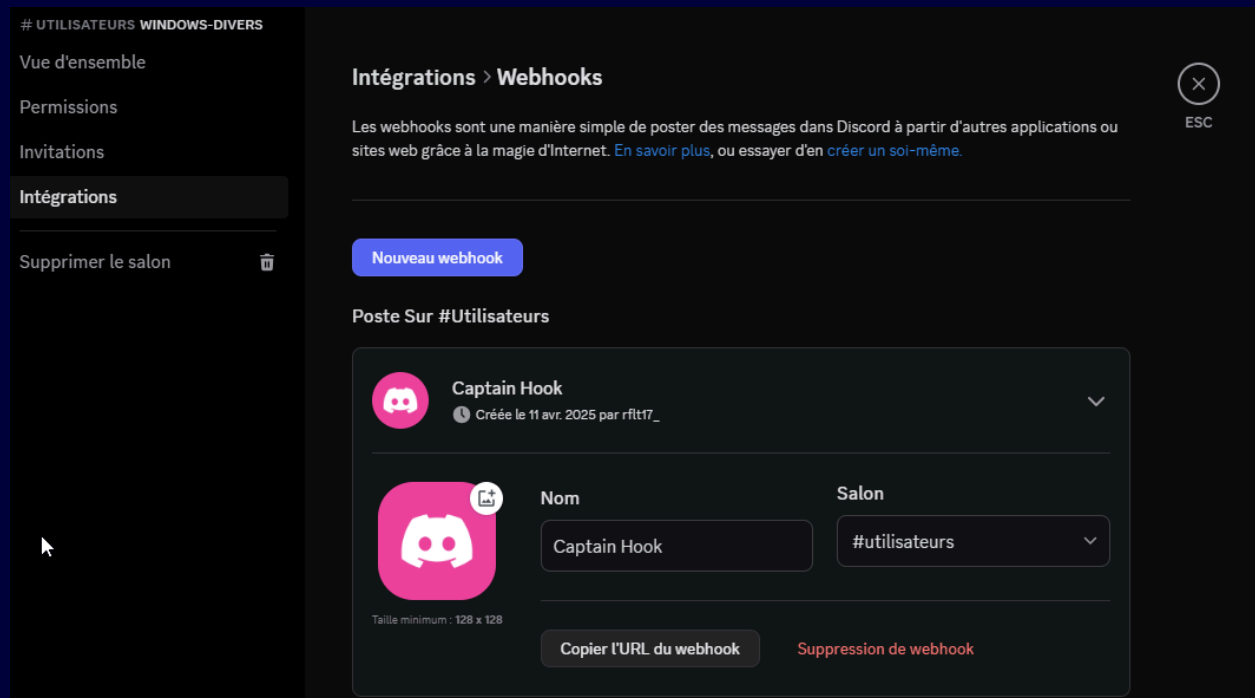
Grace Period

☒ 15 seconds ▼

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.

Title
[RDP] Notification Discord Nommer la notification
Title to identify this Notification.

Description (Optional)
Notification Discord
Longer description for this Notification.

Notification Type
Custom HTTP Notification Sélectionner CUSTOM HTTP
Choose the type of Notification to create.

URL
https://discord.com/api/webhooks/1356984754288857239/Z9WT-3XrbwiNzZgelPxbthr3-d_DuMzJpuF_DJ6eXvzXb
The URL to POST to when an Event occurs
☐ Skip TLS verification Copier le lien du WEBHOOK

Laisser les paramètres par défaut et changer les suivants :

HTTP Method

POST

Content Type

application/json

Time zone for date/time values

UTC

HTTP method used for the notification

HTTP content type used for POST/PUT notifications

Time zone used for timestamps in the notification body

Body Template

```

1 {
2   "username": "Graylog[RDP]",
3   "avatar_url": "https://cdn.pixabay.com/photo/2020/03/18/14/53/remote-4944296_1280.png",
4   "embeds": [
5     {
6       "title": "⚠ Nouvelle connexion détectée",
7       "description": "Une nouvelle connexion a été détectée.",
8       "color": 11393254,
9       "fields": [
10        {
11          "name": "👤 Utilisateur",
12          "value": "${event.fields.username}",
13          "inline": true
14        },
15        {
16          "name": "📍 Depuis",
17          "value": "${event.fields.adresseip}",
18          "inline": true
19        },
20        {
21          "name": "🕒 Heure",
22          "value": "${event.fields.temps}",
23          "inline": false
24        }
25      ]
26    }
27  ]
28 }
```

Custom POST/PUT body. See [docs](#) for more details. An empty POST/PUT body will send the full event details.

Test Notification (Optional)

Execute Test Notification

Execute this Notification with a test Alert.

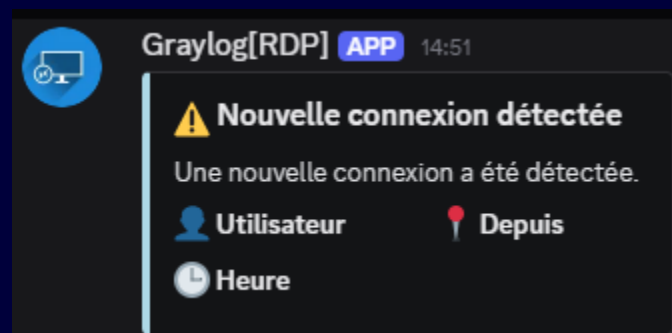
Update notification Cancel

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 être envoyée :

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



Si tout fonctionne comme prévu, à 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.](#)