



## Installation et configuration de Rsyslog pour envoyer les logs Linux vers Graylog

Équipe de rédaction et d'approbation		
<b>NGANSOP NJANOU ULRICH SOSTAIRE</b>	Junior Network Administrator <b>EVOLV IZSOFTWARES GROUP Ltd</b>	Date: 20 janvier 2025
<b>GILDAS FOTSO TABAFO</b>	Junior Network Administrator <b>EVOLV IZSOFTWARES GROUP Ltd</b>	Date: 20 janvier 2025
<b>Beryl Ngonga</b>	Professional Framer <b>EVOLV IZSOFTWARES GROUP Ltd</b>	Date de fin : _
Sommaire des révisions		
Historique de Révision	Description générale	Date approuvée
0.0.2	Document, version 2	

Linux : envoyer les logs vers Graylog avec rsyslog

### I. Introduction

Ce guide détaille le processus de configuration d'une machine Linux pour l'envoi de ses journaux système à un serveur Graylog, en utilisant Rsyslog. Il est essentiel d'avoir un serveur Graylog déjà installé.

- Vous trouverez des instructions d'installation de Graylog pour Debian et AlmaLinux dans nos documentations précédentes .
- Remarque : cette configuration est compatible avec plusieurs distributions Linux, notamment Debian, Ubuntu, Rocky Linux et AlmaLinux.

### II. Configurer Graylog pour la réception des logs Linux

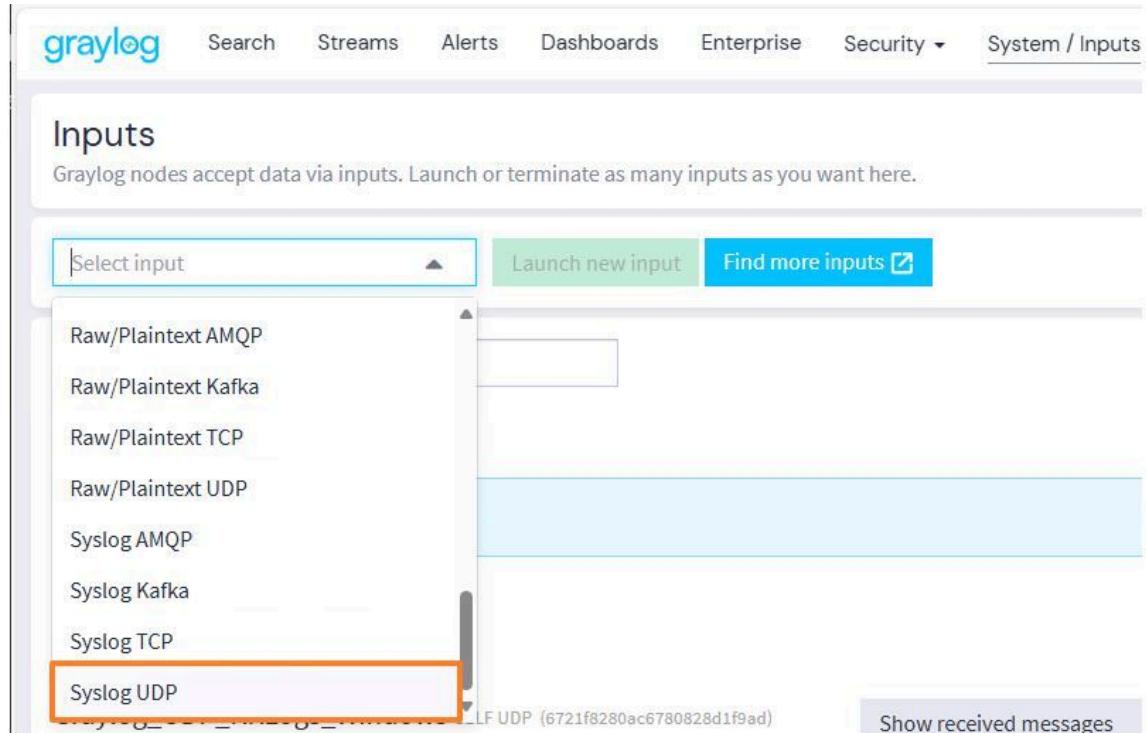
Commençons par configurer Graylog en trois étapes :

- Création d'un Input :** Configurez un point d'entrée permettant aux machines Linux d'envoyer les journaux Syslog via UDP.
- Création d'un Index :** Créez un nouvel index pour stocker et indexer tous les journaux Linux.
- Création d'un Stream :** Configurez un stream pour router les journaux reçus par Graylog vers le nouvel index Linux.

#### A. Créer un Input pour Syslog

Pour commencer, connectez-vous à l'interface Graylog. Dans le menu, cliquez sur "**System**", puis sur "**Inputs**". Sélectionnez "**Syslog UDP**" dans le menu déroulant et cliquez sur "**Launch new input**".

 Il est également possible de créer une entrée Syslog en TCP, mais cela nécessite l'utilisation d'un certificat TLS (ce point n'est pas traité dans cette documentation).



The screenshot shows the Graylog interface with the 'System / Inputs' tab selected. Under the 'Inputs' section, a dropdown menu lists several input types. The 'Syslog UDP' option is highlighted with an orange box. To the right of the dropdown, there is a status message showing a log entry: 'LF UDP (6721f8280ac6780828d1f9ad)'. At the bottom right, there is a button labeled 'Show received messages'.

Un assistant s'affichera à l'écran. Nommez-le, par exemple "*Graylog Rsyslog Linux*", puis choisissez un port. **Le port 514** est utilisé par défaut, mais vous pouvez le modifier.

## Editing Input Graylog Rsyslog Linux

✖

### Global

Should this input start on all nodes

### Node

cb824c8b / Graylog-Server



On which node should this input start

### Title

Graylog Rsyslog Linux

### Bind address

0.0.0.0

Address to listen on. For example 0.0.0.0 or 127.0.0.1.

### Port

514



Port to listen on.

### Receive Buffer Size (optional)

262144



The size in bytes of the recvBufferSize for network connections to this input.

### No. of worker threads (optional)

2



Vous pouvez également sélectionner l'option « **Store full message** » pour enregistrer le message de log entier dans Graylog. Cliquez ensuite sur « Lancer l'entrée ».

### Override source (optional)

The source is a hostname derived from the received packet by default. Set this if you want to override it with a custom string.

### Encoding (optional)

UTF-8

Default encoding is UTF-8. Set this to a standard charset name if you want to override the default.

Force rDNS?

Force rDNS resolution of hostname? Use if hostname cannot be parsed. (Be careful if you are sending DNS logs into this input because it can cause a feedback loop.)

Allow overriding date?

Allow to override with current date if date could not be parsed?

Store full message?

Store the full original syslog message as full\_message?

Expand structured data?

Expand structured data elements by prefixing attributes with their SD-ID?

### Time Zone (optional)

Not configured

Default time zone used when no timezone detected

Cancel

Launch Input

Le nouvel Input est actif et reçoit désormais les logs Syslog sur le port UDP 12514. La configuration de l'application n'est cependant pas terminée.

Graylog Rsyslog Linux Syslog UDP (6790208f7cd8c0aa0fdb6d1) [RELOAD]  
On node ★ cb824c8b / Graylog-Server

Show received messages Manage extractors

```
allow_override_date: true
bind_address: 0.0.0.0
charset_name: UTF-8
expand_structured_data: false
force_rdns: false
number_worker_threads: 2
override_source: <empty>
port: 514
recv_buffer_size: 262144
store_full_message: true
timezone: NotSet
```

Throughput / Metrics  
1 minute average rate: 0 msg/s  
Network IO: ▾ 0B ▲ 0B (total: ▾ 13.9KB) ▾  
Empty messages discarded: 0

**i** Remarque : un seul fichier d'entrée peut servir à stocker les journaux de plusieurs machines Linux.

Pour stocker les journaux de vos machines Linux, il est nécessaire de créer un nouvel index dans Graylog. Un index Graylog sert de structure de stockage pour les messages journaux reçus et utilise OpenSearch pour un stockage efficace, facilitant des recherches rapides.

Pour procéder, accédez à la section "**System**" puis "**Indices**" dans le menu Graylog, et cliquez sur "**Create index set**" sur la page suivante.

The screenshot shows the Graylog interface with the 'Indices & Index Sets' tab selected. At the top right, there is a green button labeled 'Create index set'. A red arrow points to this button. Below it, there is a status message: 'OpenSearch cluster graylog is green. Shards: 7 active, 0 initializing, 0 relocating, 0 unassigned, What does this mean?'. The top navigation bar includes 'Search', 'Streams', 'Alerts', 'Dashboards', 'Enterprise', 'Security', and 'System / Indices'.

Nommez cet index, par exemple "Index Linux", ajoutez-y une description et un préfixe avant de le valider. Cet index servira à stocker tous les journaux Linux. Il est également possible de créer des index dédiés pour archiver uniquement certains types de logs (logs SSH, logs du service web, etc.)..

The screenshot shows the 'Create Index Set' configuration page. In the 'Configuration Information' section, the 'Title' is set to 'Linux Index' and the 'Description' is 'Index pour les journaux Linux'. In the 'Details' section, the 'Index prefix' is 'linux\_index' and the 'Analyzer' is 'standard'. A red arrow points to the 'Index prefix' input field.

Nous devons maintenant créer un nouveau stream pour acheminer les messages vers cet index.

### C. Création d'un Stream

Pour créer un nouveau stream dans Graylog, accédez au menu principal et cliquez sur "Streams". Cliquez ensuite sur le bouton "Create stream" situé à droite. Dans la fenêtre suivante, nommez votre stream (par exemple, "Linux Stream") et sélectionnez l'index "Linux Index" dans le champ "Index Set". Confirmez votre choix.

- i** Remarque : les messages associés à ce stream seront également inclus dans le "Default Stream", sauf si vous activez l'option "Remove matches from 'Default Stream'".

The screenshot shows two windows side-by-side. On the left is the 'Create stream' dialog box. It has a title 'Create stream'. Under 'Title', the input field contains 'Linux Stream'. Below it is a 'Description (Opt.)' input field which is empty. Under 'Index Set', the input field contains 'Linux Index'. Below this is a note: 'Messages that match this stream will be written to the configured index set.' There is a checkbox labeled 'Remove matches from 'Default Stream'' which is unchecked. A note below it says 'Don't assign messages that match this stream to the 'Default Stream''. At the bottom are 'Cancel' and 'Create stream' buttons, with 'Create stream' being green. On the right is the 'Streams' list interface. It has a header row with columns 'Outputs', 'Throughput', 'Status', and 'Actions'. There are three entries, all showing '0 msg/s' in the throughput column and 'Running' in the status column. Each entry has a 'Data Routing' button, a 'Share' button, and a 'More' dropdown menu. The 'Actions' column also contains a 'More' dropdown menu. At the top of the list area are buttons for 'Show', '20 Rows', and 'Columns'.

Ensuite, dans les paramètres de votre stream Steam, ajoutez une nouvelle règle de routage des messages en cliquant sur le bouton « **Add a stream rule** ». Si vous ne trouvez pas cette option, accédez au menu « **Streams** », sélectionnez votre stream, puis cliquez sur « **More** » suivi de « **Manage rules** ».

Choisissez le type "**match input**" et **sélectionnez l'Input Rsyslog en UDP créée précédemment**. Validez avec le bouton "**Create Rule**". Ainsi, tous les messages à destination de notre nouvel Input seront envoyés dans l'Index pour Linux.

The screenshot shows the 'New Stream Rule' dialog box over a background of the 'Rules of Stream "Linux Stream"' configuration page. The dialog has a 'Type' section with 'match input' selected, an 'Input' section with 'Graylog Rsyslog Linux (Syslog UDP)' selected, and an 'Inverted' checkbox which is unchecked. A note on the right says 'The server will try to convert to strings or numbers based on the matcher type as well as it can.' Below the input section is a 'Description (Opt.)' input field which is empty. At the bottom are 'Cancel' and 'Create Rule' buttons, with 'Create Rule' being green. The background page shows a 'Recent Message' tab and a 'Select an Input' dropdown. The '2. Manage stream rules' section contains two radio buttons: one for 'A message must match all of the following rules' and another for 'A message must match at least one of the following rules'. A note at the bottom says 'Please load a message in Step 1 above to check if it would match here.' At the very bottom is a 'I'm done!' button.

Votre nouveau **Stream** devrait maintenant apparaître dans la liste et être en état "**Running**". À ce stade, la bande passante des messages indique "**0 msg/s**", car aucun journal n'est encore envoyé vers l'**Input Rsyslog UDP**. Pour consulter les journaux associés à un Stream, il vous suffit de cliquer sur son nom.

Streams								<a href="#">Streams documentation</a>
You can route incoming messages into streams by applying rules against them. Messages matching the rules of a stream are routed into it. A message can also be routed into multiple streams.								<a href="#">Create stream</a>
<input type="text" value="Search for streams"/> Filters <a href="#">+ +</a>								Show 20 Rows <a href="#">Columns</a>
<input type="checkbox"/>	Title	Index Set	Archiving	Rules	Pipelines	Outputs	Throughput	Status
<input type="checkbox"/>	All events	Graylog Events				0 msg/s	<span>Running</span>	<a href="#">Data Routing</a> <a href="#">Share</a> <a href="#">More</a>
<input type="checkbox"/>	All system events	Graylog System Events				0 msg/s	<span>Running</span>	<a href="#">Data Routing</a> <a href="#">Share</a> <a href="#">More</a>
<input type="checkbox"/>	Default Stream <small>Default</small>	Default index set				0 msg/s	<span>Running</span>	<a href="#">Data Routing</a> <a href="#">Share</a> <a href="#">More</a>
<input type="checkbox"/>	Linux Stream	Linux Index	<a href="#">X</a>	<a href="#">1</a>	<a href="#">0</a>	<a href="#">0</a>	0 msg/s	<span>Running</span> <a href="#">Edit</a>

La configuration Graylog est terminée. Passons à l'étape suivante : la configuration de la machine Linux.

### III. Installation et configuration de Rsyslog sous Linux

Connectez-vous à votre machine Linux, localement ou à distance, avec un compte utilisateur disposant des priviléges d'élévation (via `sudo`). Sinon, utilisez le compte root.

#### A. Installation du paquet Rsyslog

Commencez par mettre à jour le cache des paquets et installez le paquet "**rsyslog**" :

```
sudo apt-get update
```

```
sudo apt-get install rsyslog
```

 version équivalente de la commande pour AlmaLinux , CentOS et les autres distributions basées sur **DNF** :

```
sudo dnf update
```

```
sudo dnf install rsyslog
```

Vérifiez ensuite le statut du service. Il est généralement déjà en cours d'exécution :

```
1 sudo systemctl status rsyslog
```

Le fichier de configuration principal de Rsyslog est situé en `/etc/rsyslog.conf`. Le répertoire `/etc/rsyslog.d/` contient des fichiers de configuration supplémentaires. Le fichier principal inclut une directive importante tous les fichiers ".conf" de ce répertoire, assurant ainsi une configuration modulaire. Cette approche évite les modifications directes du fichier principal et simplifie la gestion des configurations.

Pour gérer l'ordre de chargement des fichiers dans `/etc/rsyslog.d/` (qui se fait par ordre alphabétique), il est recommandé d'utiliser une numérotation préfixe. Ceci permet de prioriser les configurations. Dans ce cas précis, un seul fichier complémentaire étant utilisé, cette précaution est superflue.

Ce répertoire accueillera un nouveau fichier nommé "**10-graylog.conf**".

```
sudo nano /etc/rsyslog.d/10-graylog.conf
```

Ajoutez la ligne suivante à ce fichier :

```
1 *.* @192.168.2.99:514;RSYSLOG_SyslogProtocol23Format
```

Cette ligne de configuration Rsyslog envoie tous les logs système d'une machine Linux vers Graylog :

- `*.*` : Spécifie l'envoi de tous les messages Syslog (toutes les facilités et niveaux de严重性).
- `@` : Indique le transport UDP. Utilisez `@@` pour le transport TCP.
- `192.168.2.99:514` : Adresse IP et port du serveur Graylog (port d'écoute de l'Input Graylog).
- `RSYSLOG_SyslogProtocol23Format` : Définit le format des messages envoyés à Graylog.

Une fois ces modifications enregistrées, redémarrez le service Rsyslog pour appliquer les changements..

```
sudo systemctl restart rsyslog.service
```

Une fois cette action effectuée, les premiers messages devraient arriver sur votre serveur Graylog !

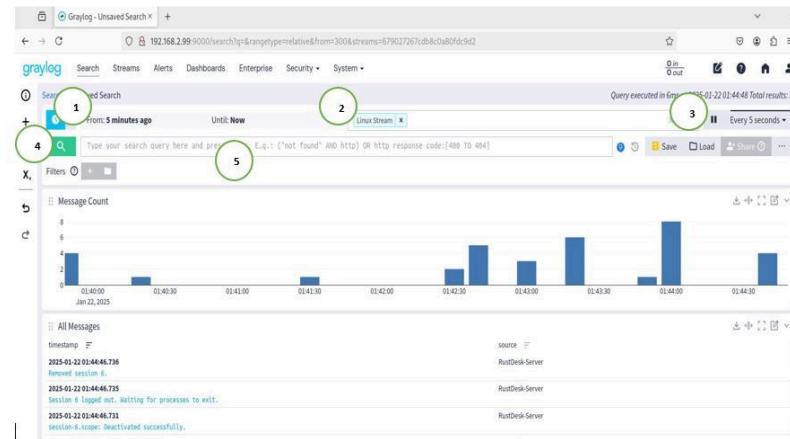
## IV. Visualiser les journaux Linux dans Graylog

Depuis Graylog, affichez les messages de votre stream en cliquant sur "Streams" puis en sélectionnant votre stream. Vous pouvez aussi utiliser la fonction "Search" : sélectionnez votre stream et lancez une recherche.

L'interface Graylog présente les éléments clés suivants :

- Sélection de la période:** Affichez les messages des 5 dernières minutes par défaut. Modifiez cette période selon vos besoins.
- Sélection du ou des streams:** Choisissez le(s) stream(s) à afficher.
- Actualisation automatique:** Activez l'actualisation automatique des messages (par exemple, toutes les 5 secondes) pour une mise à jour dynamique. Sinon, l'affichage est statique et nécessite une actualisation manuelle.
- Lancement de la recherche:** Cliquez sur la loupe pour lancer une recherche après avoir modifié la période, le stream ou le filtre.
- Barre de filtres:** Utilisez la barre de saisie pour affiner vos recherches. Par exemple, "**source:RustDesk-Server**" affiche uniquement les journaux de votre machine linux ( Notre serveur RustDesk )nouvellement configuré avec Rsyslog.

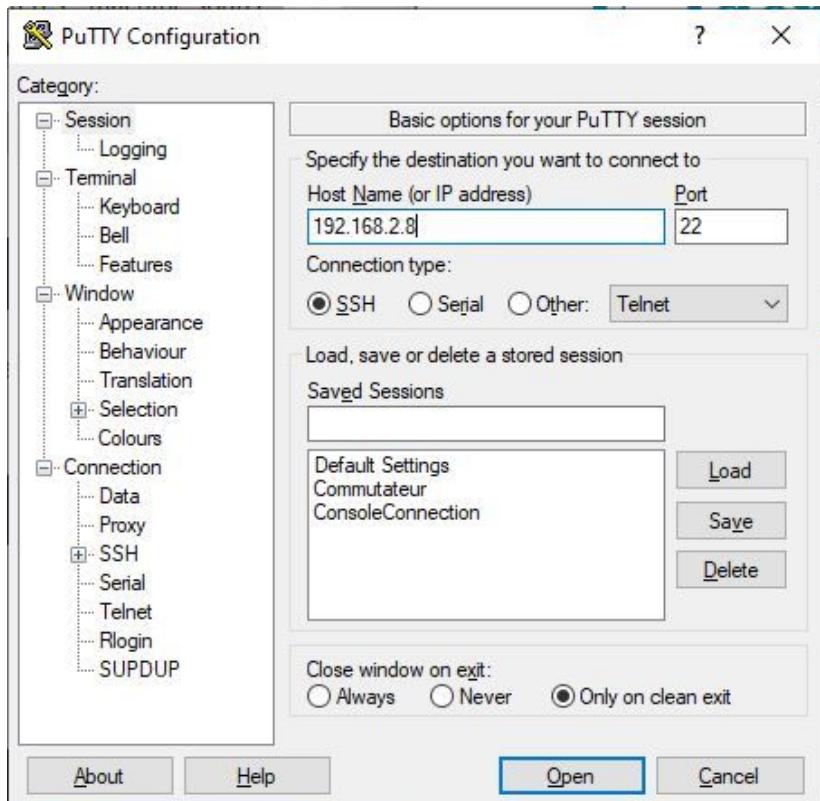
Confirmation : les journaux sont correctement envoyés par la machine Linux (Notre serveur RustDesk).



## V. Identification d'une défaillance de connexion SSH

Graylog est puissant car il indexe les journaux système, permettant des recherches multicritères : machine source, horodatage, contenu du message, etc. Par exemple, on peut facilement identifier les échecs de connexion SSH.

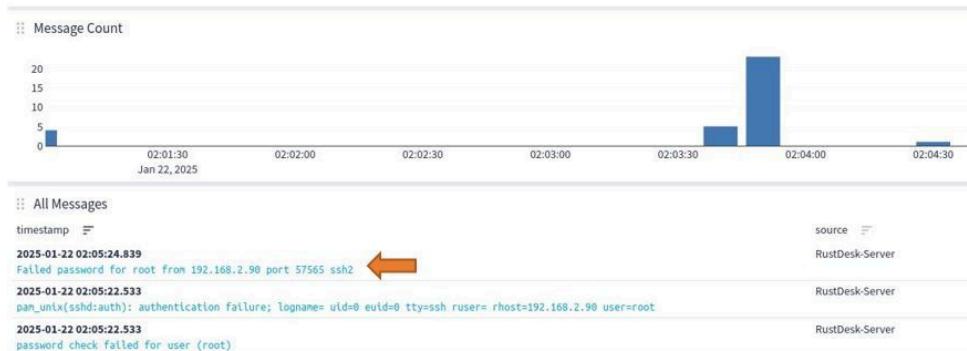
Depuis une machine distante (via PuTTY, par exemple), essayez de vous connecter à votre serveur Linux (RustDesk-Server) sur lequel vous venez de configurer Rsyslog. Par exemple :



Puis indiquez volontairement un nom d'utilisateur et un mot de passe incorrect, afin de générer des erreurs de connexion. Dans le fichier "/var/log/auth.log", ceci va générer des messages de logs similaires à celui-ci :

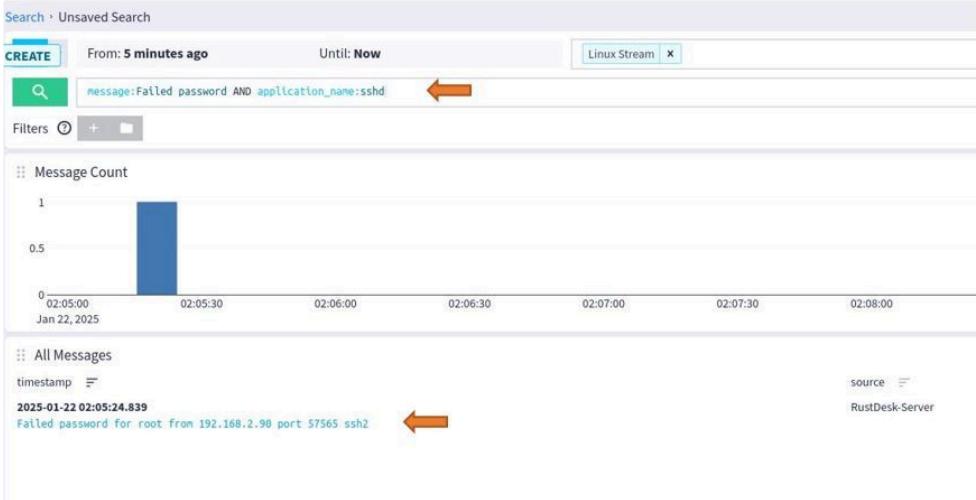
- Failed password for invalid user root from 192.168.2.8 port 57565 ssh2

Vous devriez retrouver ces messages sur Graylog.



- Sur Graylog, utilisez le filtre de recherche suivant pour afficher uniquement les messages correspondants :

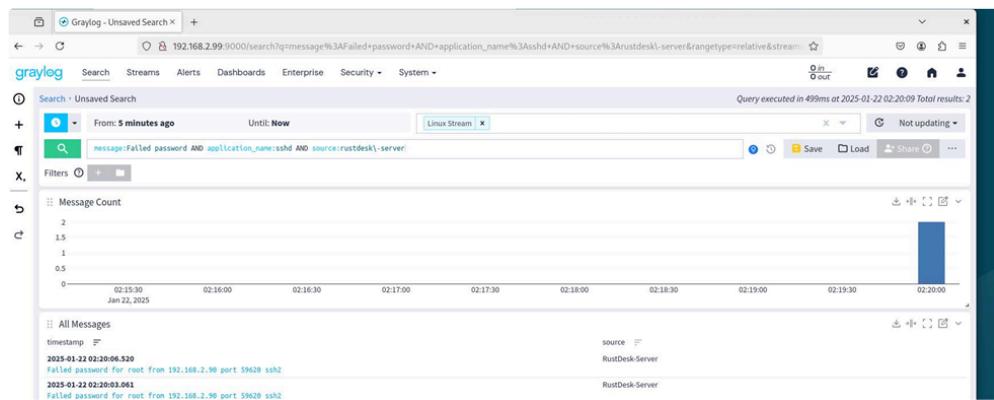
```
message:Failed password AND application_name:sshd
```



**💡 Si vous avez plusieurs serveurs et que vous souhaitez analyser les logs d'un serveur spécifique, précisez son nom en supplément :**

```
message:Failed password AND application_name:sshd AND source: Nom_de_Votre_Machine
```

Voici un aperçu des résultats obtenus sur une machine ayant subi plusieurs erreurs de connexion à différents moments de la soirée :



Les tentatives de connexion infructueuses sont effectuées à partir de la machine avec l'adresse IP "**192.168.2.99**". Si vous souhaitez en savoir plus sur l'activité de cet hôte, vous pouvez **effectuer une recherche sur cette adresse IP**. Graylog vous sortira tous les logs où cette adresse IP est référencée, sur tous les hôtes (pour lesquels l'envoi de logs est configuré).

Dans ce cas, le filtre à utiliser pourra être :

**💡 message:"192.168.2.99"**

## VI. Conclusion ↗

Ce tutoriel a pour objectif de vous guider pas à pas dans le processus de configuration d'une machine fonctionnant sous Linux. Cette configuration est essentielle pour permettre l'envoi efficace de ses journaux vers un serveur Graylog. Grâce à cette démarche, vous pourrez bénéficier d'une centralisation de vos logs Linux, ce qui est crucial pour une gestion et une surveillance optimales de votre système.

En outre, pour une gestion encore plus optimisée de vos journaux, il est fortement recommandé de créer des tableaux de bord personnalisés. Ces tableaux de bord vous permettront de visualiser rapidement l'état de vos logs et d'identifier les tendances ou les problèmes potentiels. De plus, n'oubliez pas de mettre en place des alertes. Ces alertes vous notifieront

instantanément en cas d'anomalie, vous permettant ainsi de réagir rapidement et d'assurer la sécurité et la performance de votre système.

 La configuration de ces options de Graylog sera documentée prochainement.

En cas de problème, veuillez contacter les auteurs de ce document ou consulter la documentation et les forums Graylog.

**Editorial Team:**

- **Ulrich Sostaire Ngansop Njanou** (Junior Network Administrator)
- **Gildas Fotso Tabafo** (Junior Network Administrator)