



Installation et configuration de NXLog pour envoyer des journaux Windows vers Graylog

Équipe de rédaction et d'approbation		
NGANSOP NJANOU ULRICH SOSTAIRE	Junior Network Administrator EVOLV IZSOFTWARES GROUP Itd	Date: 20 janvier 2025
GILDAS FOTSO TABAFO	Junior Network Administrator EVOLV IZSOFTWARES GROUP Itd	Date: 20 janvier 2025
Beryl Ngonga	Professionally Framed EVOLV IZSOFTWARES GROUP Itd	Date de fin : _
Sommaire des révisions		
Historique de Révision	Description générale	Date approuvée
0.0.1	Document, version 1	

[Envoyer les logs Windows vers Graylog avec NXLog](#)

I. Présentation

Ce guide explique comment installer et configurer NXLog sur un serveur Windows pour envoyer les journaux Windows vers un serveur Graylog. Cela permet de centraliser et d'indexer les journaux de l'Observateur d'événements de plusieurs machines Windows dans Graylog.

Vous aurez besoin d'un serveur Graylog et d'une machine Windows Server (ou Windows).

Windows ne peut pas envoyer ses journaux vers un serveur Graylog (ou équivalent) par défaut, car ses fonctionnalités de transfert de journaux sont limitées. Pour résoudre ce problème, nous utiliserons l'agent NXLog communautaire. Il permettra de collecter les journaux sur la machine Windows et de les acheminer vers le serveur Graylog.

II. Configuration d'un Input NXLog pour Graylog

Pour commencer, créez un nouvel input dans la configuration de Graylog, car c'est ainsi que les données seront réceptionnées. Depuis l'interface web de Graylog, accédez au menu "Système", puis sélectionnez "Inputs". Choisissez ensuite "GELF UDP" dans la liste et cliquez sur "Lancer un nouvel input".

The screenshot shows the Graylog web interface with the URL graylog:9000. The top navigation bar includes links for Search, Streams, Alerts, Dashboards, Enterprise, Security, System / Inputs (which is currently selected), and a user icon. The main content area is titled 'Inputs' with a sub-instruction: 'Graylog nodes accept data via inputs. Launch or terminate as many inputs as you want here.' Below this, there's a table with one row. The row contains a 'Name' column with 'GELF UDP', a 'Type' column with 'GELF UDP', and two buttons: 'Launch new input' and 'Find more inputs'. At the bottom of the page, a note states: 'Remarque : GELF (Graylog Extended Log Format) est le format de log utilisé par Graylog ; les données sont transmises via le protocole UDP.'

Une fenêtre s'affiche pour configurer ce nouvel Input. Un Input peut gérer plusieurs machines Windows. Nommez-le, par exemple, "Graylog NXlogs Windows", et définissez l'adresse de liaison ("Bind address") sur "0.0.0.0" pour permettre l'accès depuis toutes les interfaces de l'hôte Graylog (ajustez cette valeur si nécessaire). La connexion se fera sur le port 12201.

Editing Input Graylog NXlogs Windows

Global
Should this input start on all nodes

Node
cb824c8b / Graylog-Server

On which node should this input start

Title
Graylog NXlogs Windows

Bind address
0.0.0.0

Address to listen on. For example 0.0.0.0 or 127.0.0.1.

Port
12201

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)
4

ⓘ Validez. Vous obtiendrez alors un résultat similaire à l'exemple suivant.

Local inputs 2 configured

Graylog NXlogs Windows GELF UDP (678f5f87cdb8cda80fd48e7) RUNNING
On node ★ cb824c8b / Graylog-Server

Show received messages Manage extractors Stop input More actions ▾

```
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
```

Throughput / Metrics
1 minute average rate: 1 msg/s
Network IO: ▼ 0B ▲ 0B (total: ▼ 8.7MB ▲ 0B)
Empty messages discarded: 0

La configuration de Graylog est finalisée. La suite du processus se déroulera sur l'hôte Windows.

III. Installation et configuration de NXLog sous Windows ↗

A. Installer NXLog sur Windows Server ↗

Commencez par vous connecter à votre serveur Windows Server (ici, un serveur 2019 nommé "DC-local", ou le nom de votre serveur). Téléchargez ensuite l'agent NXLog Community Edition. Cette version gratuite offre de nombreuses fonctionnalités, bien qu'elles soient moins complètes que celles de la version Entreprise.

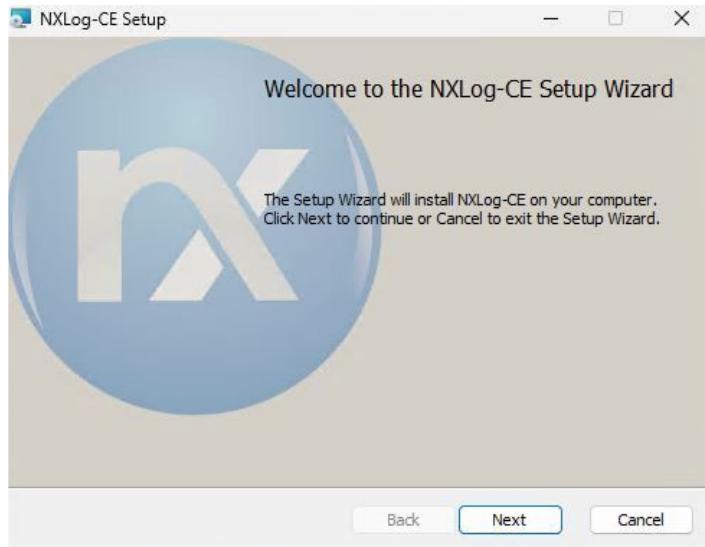
Téléchargez-le ici :

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

Sélectionnez ensuite "Windows", cochez la case "Windows x86-64" et lancez le téléchargement.

The screenshot shows the NXLog Community Edition download page. At the top, there's a navigation bar with links for Products, Solutions, Plans, Partners, Resources, Support, and About Us. Below the navigation is a search bar and two buttons: 'Let's talk' and 'Start free'. The main content area is titled 'Available Downloads'. It shows a dropdown menu set to 'NXLog Community Edition' and a 'Platform' section with icons for various operating systems. A checkbox labeled 'Select All' is present. Under the 'Windows' heading, a file named 'nxlog-ce-3.2.2329.msi' is listed with a checked checkbox. Below the file list is a note about opening a new popup window for multiple downloads. At the bottom right of the download area, there's a 'Download' button with a file count of '1 files selected (remove)'.

Installez nxlog sur votre machine Windows à l'aide du package « nxlog-ce-3.2.2329.msi ». Suivez les instructions de l'assistant d'installation. La configuration se fera ensuite automatiquement. Ce package MSI permet un déploiement facile et l'automatisation de l'installation sur plusieurs machines.



B. Configurer NXLog pour Graylog ↗

Une fois NXLog installé, vous pouvez modifier son fichier de configuration situé ici :

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 :

```
1 # Récupérer les journaux de l'observateur d'événements
2
3 <Input in>
4
5     Module      im_msvistalog
6
7 </Input>
8
9 # Déclarer le serveur Graylog (selon input)
10
11 <Extension gelf>
```

```

12
13     Module      xm_gelf
14
15 </Extension>
16
17 <Output graylog_udp>
18
19     Module      om_udp
20
21     Host       192.168.2.99
22
23     Port       12201
24
25     OutputType   GELF_UDP
26
27 </Output>
28
29 # Routage des flux in vers out
30
31 <Route 1>
32
33     Path       in => graylog_udp
34
35 </Route>

```

Pour faciliter la compréhension, voici quelques explications :

- **im_msvistalog** : Ce module d'entrée (Input) collecte les journaux de l'Observateur d'événements Windows. Compatible avec Windows Server 2008, Windows Vista et les versions ultérieures (y compris Windows 11 et Windows Server 2025), il remplace le module **im_mseventlog** pour les systèmes antérieurs à Windows Server 2008.
- **om_udp** : Ce module de sortie (Output graylog_udp) transmet les données à votre serveur Graylog. Modifiez l'adresse IP (ici : 192.168.10.220) et le port si nécessaire. L'utilisation de "GELF_UDP" assure la cohérence avec le module d'entrée Graylog.
- **Route 1**: Cette règle de routage NXLog achemine les données d'entrée ("in", les journaux Windows) vers la sortie "graylog_udp", c'est-à-dire votre serveur Graylog.

Après avoir enregistré vos modifications, redémarrez le service NXLog depuis une console PowerShell administrateur (ou via les Services) avec la commande :

```
Restart-Service nxlog
```

- i** Je vous recommande de consulter le fichier journal de NXLog pour résoudre d'éventuels problèmes de configuration. Par exemple, si vous ne recevez aucun log sur Graylog, ce fichier vous sera utile.

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

C. Amélioration des règles de collecte de NXLog ↗

Par son paramétrage d'origine, **NXLog** transmet tous les événements de tous les journaux Windows vers notre puits de logs **Graylog**. Mais vous avez la possibilité de personnaliser cette configuration pour cibler précisément ce qui est envoyé. Par exemple, vous pouvez choisir de transmettre uniquement les événements d'un journal particulier ou ceux qui répondent à certains critères spécifiques.

Pour vous guider dans cette personnalisation, la documentation officielle est disponible ici :

[Guide de configuration de NXLog - Filtrage.](#)

Voici un exemple pratique : nous modifions la section **Input** dans la configuration de NXLog pour que seuls les événements du journal **Sécurité** soient transmis à Graylog..

```

1 <Input in>
2
3     Module      im_msvistalog
4
5     <QueryXML>
6
7         <QueryList>
8
9             <Query Id='1'>
10
11                 <Select Path='Security'/*></Select>
12
13             </Query>
14
15         </QueryList>
16

```

```

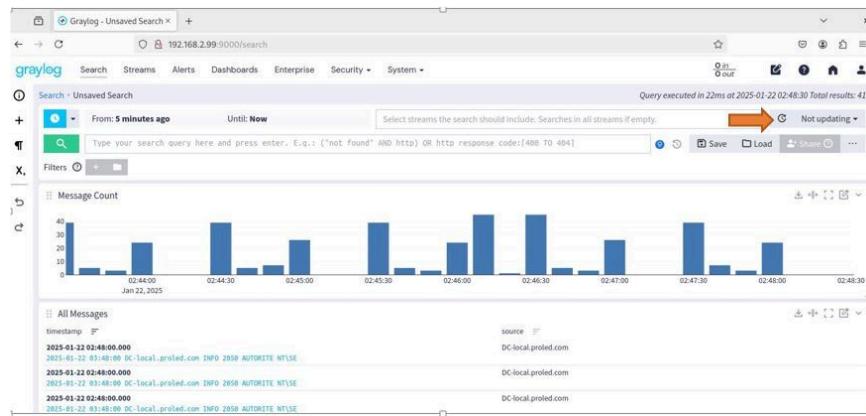
17     </QueryXML>
18
19  </Input>

```

IV. Recevoir les journaux Windows dans Graylog

Après avoir configuré Graylog et l'agent NXLog sur votre machine Windows, vos journaux devraient maintenant être envoyés vers Graylog. Pour vérifier cela, cliquez simplement sur "Search" dans le menu Graylog.

Vous devriez voir les premiers journaux arriver, ce qui peut entraîner un pic d'activité. Il est recommandé de cliquer sur le bouton indiqué sur l'image ci-dessous pour rafraîchir automatiquement la liste toutes les 5 secondes (par défaut).



En cliquant sur un log dans la liste, vous visualiserez son contenu, de la même manière que si vous consultiez le journal via l'Observateur d'événements Windows.



Graylog stocke et indexe les journaux, sa puissance étant sa fonction de recherche. Créez un filtre dans le champ de recherche (à droite de la loupe).

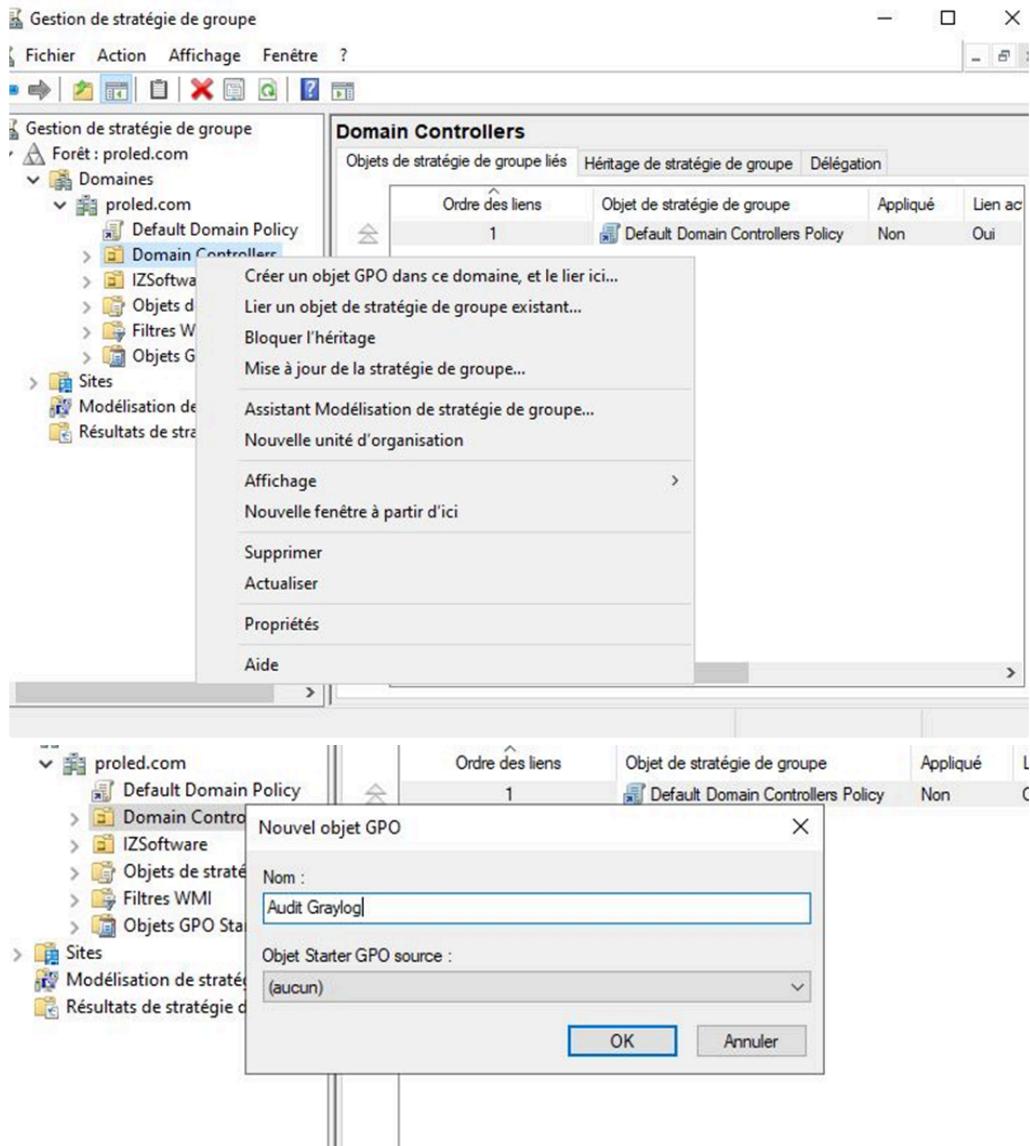
Par exemple, pour afficher uniquement les événements avec l'ID **4776** ou **4771**, identifiez ainsi les tentatives de connexion infructueuses sur un ou plusieurs serveurs. Pour générer ces événements, vous devrez **ajuster la stratégie d'audit de Windows**.

- Configuration de la stratégie d'audit Windows

Cette procédure décrit la configuration de la stratégie d'audit Windows, l'exécution de tests et l'analyse des résultats dans Graylog.

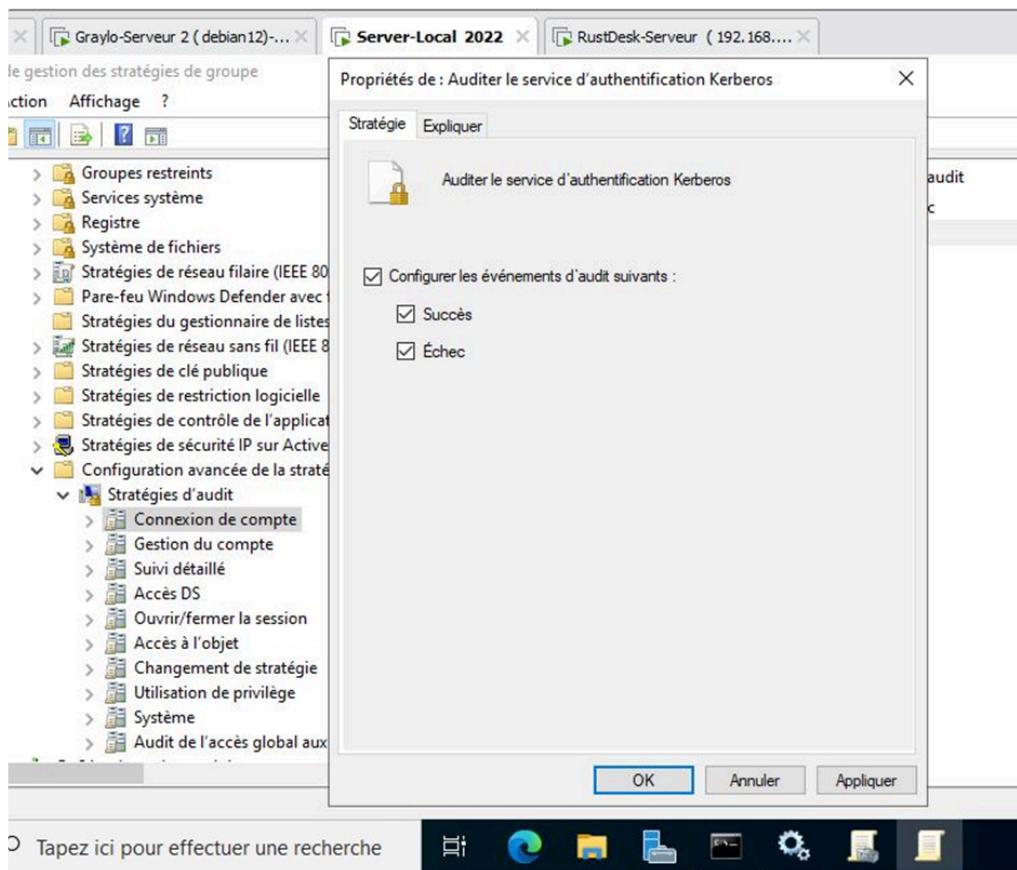
1. Création d'un objet GPO:

Commencez par créer un objet GPO (stratégie de groupe) pour configurer la politique d'audit.



2. Modification de la GPO:

Modifiez la GPO en suivant ce chemin : Stratégie/Paramètres Windows/Paramètres de sécurité/Configuration avancée de la stratégie d'audit. Accédez à "Stratégie d'audit", cliquez sur "Connexion de compte" et activez les quatre paramètres, en configurant les événements d'audit (Succès/Échec) pour chacun.



3. Mise à jour de la stratégie:

Mettez à jour la stratégie sur le serveur avec la commande :

```
gpupdate /force
C:\Users\Administrateur>gpupdate /force
Mise à jour de la stratégie...
La mise à jour de la stratégie d'ordinateur s'est terminée sans erreur.
La mise à jour de la stratégie utilisateur s'est terminée sans erreur.

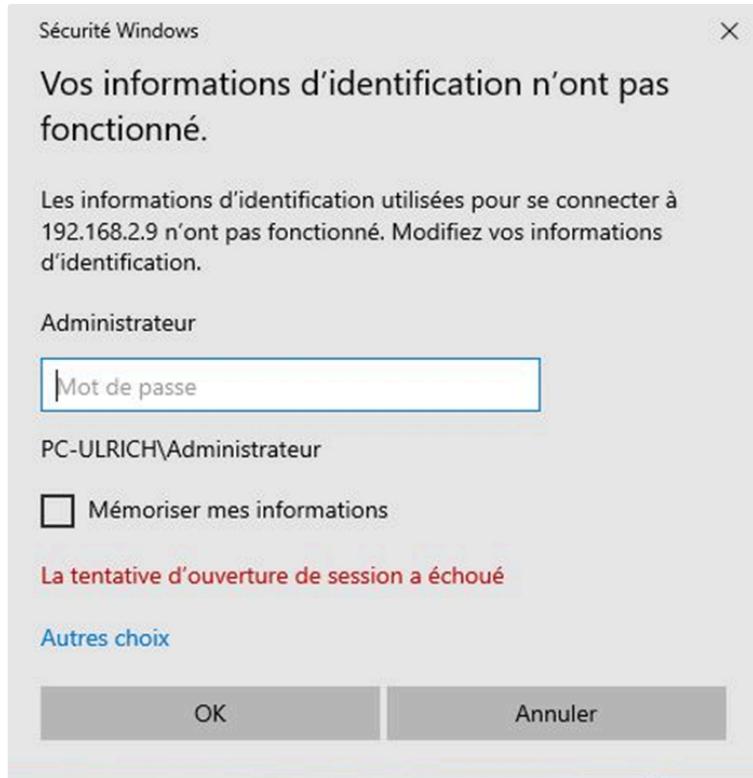
C:\Users\Administrateur>
```

i Article de référence pour plus de détails sur la stratégie d'audit de Windows :

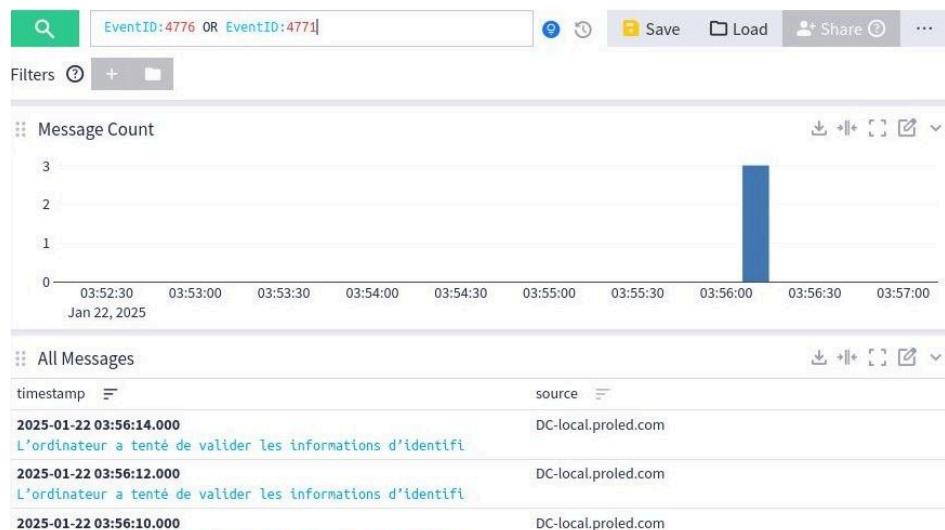
<https://www.it-connect.fr/securite-active-directory-detecter-attaques-par-brute-force/>

Tests et analyse des résultats dans Graylog:

Après la mise en place de la nouvelle stratégie d'audit, effectuez des tests en tentant des connexions infructueuses depuis des machines distantes (bureaux à distance). Ceci générera des erreurs dans l'explorateur Windows, erreurs que vous devriez retrouver dans Graylog.



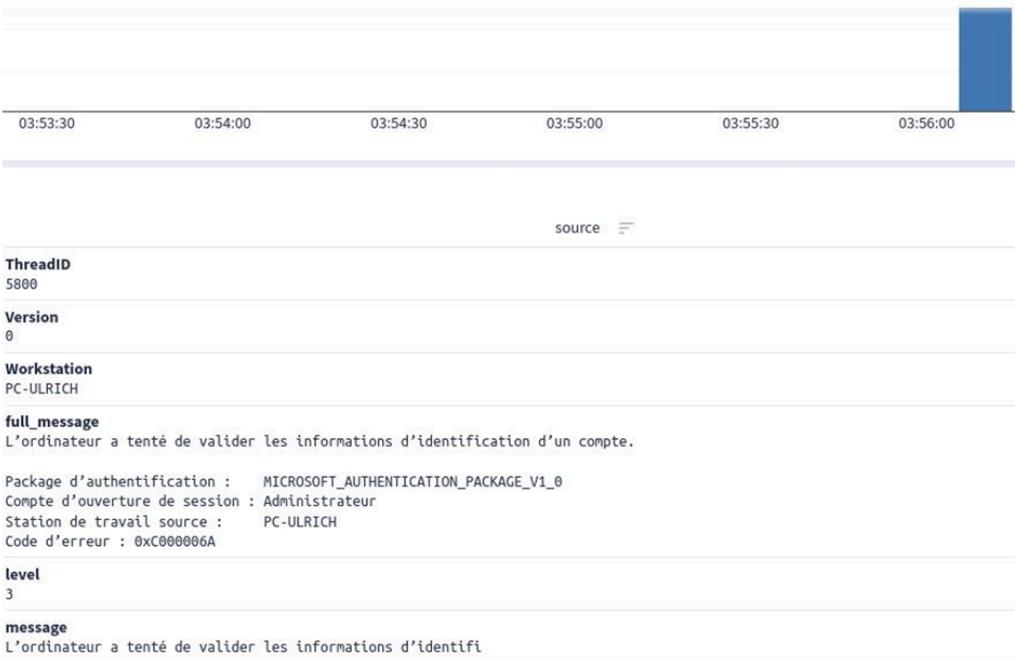
Exemple de requête Graylog pour identifier ces erreurs : (EventID:4776 OR EventID:4771)



Enregistrez vos requêtes pour une utilisation ultérieure. Pour analyser les journaux d'une machine spécifique, ajoutez AND source:nom_de_la_machine à votre requête.

Remarque: Échappez les caractères spéciaux suivants avec un anti-slash : & | : \ \ / + - ! () { } \[\] ^ " ~ * ?

En cliquant sur un message, vous obtiendrez plus de détails sur la cause et la source de l'erreur.



Documentation sur la syntaxe des requêtes Graylog :

https://go2docs.graylog.org/current/making_sense_of_your_log_data/writing_search_queries.html

V. Déployer NXLog sur Windows avec une GPO

Cette section explique comment déployer NXLog sur Windows à l'aide d'une GPO (stratégie de groupe). Cette méthode permet d'automatiser l'installation et la configuration de NXLog sur plusieurs machines Windows dans un réseau. L'utilisation d'une GPO garantit une gestion centralisée et un déploiement uniforme du logiciel.

A completer

VI. Conclusion

Ce document fournit une explication approfondie concernant l'installation et la configuration de NXLog sur un système d'exploitation Windows, spécifiquement pour le but d'envoyer des journaux vers Graylog. Graylog est un outil puissant pour la gestion et l'analyse des journaux, et NXLog joue un rôle crucial dans le processus de collecte de ces données. En plus de cela, le document aborde également la manière d'adapter cette configuration pour qu'elle soit compatible avec un environnement Active Directory. Cela est particulièrement pertinent pour les organisations qui souhaitent déployer NXLog de manière efficace sur plusieurs serveurs ainsi que sur des postes de travail au sein de leur infrastructure. Cette approche permet non seulement d'optimiser la gestion des journaux, mais aussi de garantir une intégration fluide et sécurisée au sein des systèmes existants.

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)