

Plan d'Action : Réparer rsyslog

Maintenant que nous sommes certains que les paquets frappent à la porte, nous allons forcer rsyslog à leur ouvrir. Nous allons appliquer l'**Étape 2** de mon message précédent, la méthode "brutale" mais infaillible.

1. **Arrêtez tcpdump** avec Ctrl+C.
2. **Créez (ou videz) le fichier de configuration GNS3 :**

Bash

```
sudo nano /etc/rsyslog.d/40-gns3.conf
```

3. **Assurez-vous que son seul et unique contenu est cette ligne :**

Plain Text

```
*.* /var/log/gns3/catch-all.log
```

Cette règle est prioritaire et très générale. Elle devrait tout capturer.

4. **Vérifiez que le dossier existe** (nous l'avons déjà fait, mais une double vérification ne coûte rien) :

Bash

```
sudo mkdir -p /var/log/gns3
sudo chown syslog:adm /var/log/gns3
```

5. **Redémarrez rsyslog pour appliquer la nouvelle configuration :**

Bash

```
sudo systemctl restart rsyslog
```

etape 2 : Utiliser une règle spécifique et finale

1. **Éditez ce nouveau fichier :**

Bash

```
sudo nano /etc/rsyslog.d/20-gns3.conf
```

2. **Supprimez tout son contenu** et remplacez-le par ceci :

Plain Text

```
# Configuration pour capturer les logs du réseau GNS3
# La syntaxe ":fromhost-ip, !isequal, '127.0.0.1'" filtre les messages
# qui viennent d'une IP autre que la machine locale.
:fromhost-ip, !isequal, "127.0.0.1" /var/log/gns3/network-devices.log

# La ligne suivante dit à rsyslog d'arrêter de traiter ces messages.
```

```
# Ils n'iront donc pas polluer les autres fichiers de log (comme  
/var/log/syslog).  
& stop
```

- **Explication :** C'est une syntaxe plus ancienne mais très robuste.
 - `:fromhost-ip, !isequal, "127.0.0.1"` est un filtre qui signifie "Si l'IP de l'expéditeur (`fromhost-ip`) n'est pas égale (`!isequal`) à `127.0.0.1` (la machine locale)..."
 - `... /var/log/gns3/network-devices.log` "...alors écris la ligne dans ce fichier."
 - `& stop :` "...et arrête de traiter cette ligne."

```
sudo systemctl restart rsyslog
```