

## TUTORIEL PRATIQUE

BTS SIO SISR – 2ème année

# CENTRALISATION DES LOGS AVEC RSYSLOG SUR DEBIAN 13

*Serveur centralisé, clients Linux, équipements réseau et interface web LogAnalyzer*

### POINTS CLÉS DU TUTORIEL

- ✓ Installation et configuration du serveur Rsyslog sur Debian 13
- ✓ Réception des logs via UDP et TCP (ports 514)
- ✓ Envoi de logs depuis un client Linux (Debian)
- ✓ Envoi de logs depuis un équipement réseau Cisco et depuis pfSense
- ✓ Tri et classement des logs par machine dans des fichiers dédiés
- ✓ Interface web de consultation des logs avec LogAnalyzer

Utilisation commerciale interdite – 03/2026 © <https://tutos-info.fr>

**Prérequis :** Ce tutoriel nécessite une machine Debian 13 (Trixie) installée et opérationnelle avec un accès réseau. Un accès SSH est recommandé pour plus de confort. Reportez-vous au tutoriel « Installer et configurer Debian 13 » sur [tutos-info.fr](https://tutos-info.fr).

*Tutoriel généré par IA*

## 1 – PRÉSENTATION DE RSYSLOG ET DE LA CENTRALISATION DES LOGS

**Rsyslog** est un démon de journalisation système, présent par défaut sur Debian. Il gère la collecte, le filtrage et l'acheminement des messages système (logs) générés par le noyau, les services et les applications.

Dans une infrastructure réseau, il est essentiel de **centraliser les logs** sur un serveur unique pour :

- **Simplifier l'audit et la surveillance** des équipements et serveurs
- **Détecter rapidement les incidents** (tentatives d'intrusion, pannes, erreurs critiques)
- **Conserver une trace** des événements pour les obligations légales et la conformité
- **Corréler les événements** entre plusieurs machines pour une analyse globale

### Architecture mise en place

Voici l'architecture que nous allons déployer dans ce tutoriel :

| Émetteurs de logs                                             |                     | Serveur Rsyslog                                                            | Consultation                                                                 |
|---------------------------------------------------------------|---------------------|----------------------------------------------------------------------------|------------------------------------------------------------------------------|
| Client Linux (Debian)<br>Équipement Cisco<br>Pare-feu pfSense | UDP/TCP<br>port 514 | Debian 13 – Rsyslog<br>Logs stockés dans<br><code>/var/log/clients/</code> | HTTP<br>port 80<br><br>Interface web<br><b>LogAnalyzer</b><br>(Apache + PHP) |

### Les niveaux de sévérité Syslog

Le protocole Syslog définit **8 niveaux de sévérité** (de 0 à 7). Il est indispensable de les connaître pour filtrer et analyser efficacement les logs :

| Niveau | Nom            | Description                                      |
|--------|----------------|--------------------------------------------------|
| 0      | <b>emerg</b>   | Urgence – système inutilisable                   |
| 1      | <b>alert</b>   | Alerte – action immédiate requise                |
| 2      | <b>crit</b>    | Critique – conditions critiques                  |
| 3      | <b>err</b>     | Erreur – conditions d'erreur                     |
| 4      | <b>warning</b> | Avertissement – conditions d'avertissement       |
| 5      | <b>notice</b>  | Notice – conditions normales mais significatives |
| 6      | <b>info</b>    | Information – messages informatifs               |
| 7      | <b>debug</b>   | Débogage – messages de débogage (très verbeux)   |

## 2 – INSTALLATION ET CONFIGURATION DU SERVEUR RSYSLOG

Rsyslog est installé par défaut sur Debian 13. Nous allons le configurer pour qu'il écoute les connexions entrantes des clients et équipements réseau.

### 2.1 – Vérification et mise à jour

- Connectez-vous en SSH à votre machine Debian 13 (serveur Rsyslog, ex. : 10.10.10.60) :

```
ssh debian@10.10.10.60 -p 2213
```

- Mettez à jour les paquets et vérifiez que Rsyslog est installé :

```
sudo apt update && sudo apt upgrade -y  
rsyslogd -v # affiche la version installée
```

- Si Rsyslog n'est pas présent, installez-le :

```
sudo apt install -y rsyslog
```

### 2.2 – Activation de la réception des logs (UDP et TCP)

Par défaut, Rsyslog ne reçoit pas les logs distants. Il faut activer l'écoute sur le port **514** en UDP et en TCP en modifiant le fichier de configuration principal :

- Ouvrez le fichier de configuration principal :

```
sudo nano /etc/rsyslog.conf
```

- Recherchez le bloc suivant et **décommentez les lignes** en supprimant le caractère **#** devant chacune d'elles. Activez à la fois UDP et TCP :

```
# — Réception UDP (port 514) —  
module(load="imudp")  
input(type="imudp" port="514")  
  
# — Réception TCP (port 514) —  
module(load="imtcp")  
input(type="imtcp" port="514")
```

**Info :** UDP est privilégié pour les équipements réseau (Cisco, switches) car plus léger. TCP est recommandé pour les serveurs Linux car il garantit la livraison des messages.

### 2.3 – Classement des logs par machine cliente

Nous allons créer une règle Rsyslog pour stocker les logs de chaque client dans un fichier dédié, classé par nom d'hôte. Créez un fichier de configuration dédié :

- Créez le fichier de règles personnalisées :

```
sudo nano /etc/rsyslog.d/10-clients-distants.conf
```

- Saisissez le contenu suivant :

```
# — Stockage des logs distants par machine —  
$template LogsDistants, "/var/log/clients/%HOSTNAME%/%PROGRAMNAME%.log"  
  
# Tous les logs reçus de sources distantes sont redirigés  
if $fromhost-ip != '127.0.0.1' then ?LogsDistants  
& stop
```

**Note :** La directive & stop empêche les logs distants d'être aussi écrits dans les fichiers locaux (/var/log/syslog, etc.), évitant ainsi les doublons.

- Créez le répertoire de stockage des logs clients et définissez les bonnes permissions :

```
sudo mkdir -p /var/log/clients  
sudo chmod 755 /var/log/clients
```

- Vérifiez la syntaxe de la configuration Rsyslog avant de relancer le service :

```
sudo rsyslogd -N1 # vérifie la configuration sans redémarrer
```

- Redémarrez le service Rsyslog et vérifiez son statut :

```
sudo systemctl restart rsyslog  
sudo systemctl status rsyslog
```

- Vérifiez que les ports 514 UDP et TCP sont bien en écoute :

```
ss -ulnp | grep 514 # vérifie l'écoute UDP  
ss -tlnp | grep 514 # vérifie l'écoute TCP
```

**Attention :** Si vous utilisez un pare-feu sur le serveur (nftables, UFW), autorisez le port 514 en UDP et TCP : `sudo ufw allow 514/udp && sudo ufw allow 514/tcp`

### 3 – CONFIGURATION D'UN CLIENT LINUX (DEBIAN)

Sur chaque machine Linux à superviser, Rsyslog doit être configuré pour **transmettre ses logs au serveur centralisé** tout en conservant une copie locale.

- Connectez-vous en SSH sur la machine cliente (ex. : `10.10.10.61`) et vérifiez que Rsyslog est installé :

```
sudo apt update && sudo apt install -y rsyslog
```

- Créez un fichier de configuration dédié à la transmission des logs vers le serveur :

```
sudo nano /etc/rsyslog.d/50-serveur-central.conf
```

- Saisissez la configuration suivante (remplacez l'IP par celle de votre serveur Rsyslog) :

```
# — Envoi de TOUS les logs vers le serveur Rsyslog central —  
# @@ = TCP (recommandé pour Linux) | @ = UDP  
*,* @@10.10.10.60:514
```

**Info :** L'utilisation de @@ indique TCP (fiable). Si vous préférez UDP, utilisez @ (un seul arabase). Pour Linux, TCP est toujours recommandé.

- Redémarrez Rsyslog sur le client :

```
sudo systemctl restart rsyslog
```

- Générez un message de test pour vérifier que la transmission fonctionne :

```
logger -t TEST "Message de test depuis client Linux"
```

- Sur le **serveur Rsyslog**, vérifiez que le log est bien arrivé :

```
ls /var/log/clients/ # doit afficher un dossier au nom de la machine cliente  
cat /var/log/clients/nom-machine-cliente/TEST.log
```

**Note :** Le nom du dossier correspond au hostname de la machine cliente. Vérifiez que le hostname est correctement défini avec la commande hostnamectl.

## 4 – ENVOI DES LOGS DEPUIS LES ÉQUIPEMENTS RÉSEAU

### 4.1 – Depuis un commutateur ou routeur Cisco

Les équipements Cisco (IOS, IOS-XE) supportent nativement le protocole Syslog. La configuration s'effectue en mode **EXEC privilégié** (**enable**) ou en mode **configuration globale**.

- Connectez-vous à l'équipement Cisco via console ou SSH et passez en mode configuration :

```
enable  
configure terminal
```

- Configurez l'adresse du serveur Syslog (remplacez par l'IP de votre serveur Rsyslog) :

```
logging host 10.10.10.60
```

- Définissez le niveau de sévérité minimum des logs à envoyer (nous recommandons **informational** = niveau 6) :

```
logging trap informational
```

- Activez l'horodatage précis des logs (indispensable pour la corrélation) :

```
service timestamps log datetime msec localtime show-timezone
```

- Activez la journalisation et définissez la taille du buffer local :

```
logging buffered 16384  
logging on
```

- Sauvegardez la configuration :

```
end  
write memory
```

- Vérifiez la configuration Syslog sur l'équipement Cisco :

```
show logging
```

**Info :** Les équipements Cisco envoient leurs logs en UDP par défaut sur le port 514. Assurez-vous que le chemin réseau entre l'équipement et le serveur Rsyslog est ouvert sur ce port.

## 4.2 – Depuis un pare-feu pfSense

pfSense intègre une interface graphique pour configurer l'envoi des logs vers un serveur Syslog distant. Aucune ligne de commande n'est nécessaire.

- Connectez-vous à l'interface web de pfSense et naviguez vers **Status** → **System Logs** → **Settings**.
- Dans la section « **Remote Logging** », activez l'option « **Send log messages to remote syslog server** ».
- Renseignez l'adresse IP de votre serveur Rsyslog dans le champ « **Remote log servers** » sous la forme **10.10.10.60:514**.
- Cochez les catégories de logs à envoyer. Pour une supervision complète, cochez au minimum :
  - **Firewall Events** – règles bloquées/acceptées
  - **DHCP Service** – attributions d'adresses IP
  - **Authentication** – connexions à l'interface pfSense
  - **VPN** – événements OpenVPN / IPsec (si utilisé)
- Cliquez sur « **Save** » pour enregistrer et activer la configuration.
- Vérifiez la réception des logs pfSense sur le serveur Rsyslog :

```
ls /var/log/clients/ # un dossier pfSense doit apparaître
tail -f /var/log/clients/pfSense/filterlog.log # suivi en temps réel des logs
firewall
```

**Note :** pfSense envoie ses logs en UDP. Le nom du dossier créé sur le serveur correspond au hostname configuré dans pfSense (System → General Setup → Hostname).

## 5 – INTERFACE WEB DE CONSULTATION AVEC LOGANALYZER

**LogAnalyzer** est une interface web légère, développée par Adiscon (les créateurs de Rsyslog), permettant de consulter et de rechercher dans les logs Syslog directement depuis un navigateur. Elle fonctionne avec Apache et PHP.

## 5.1 – Installation des dépendances (Apache + PHP)

- Installez Apache2 et les modules PHP nécessaires :

```
sudo apt install -y apache2 php php-mysql php-gd php-mbstring libapache2-mod-php
```

- Activez et démarrez Apache :

```
sudo systemctl enable --now apache2
sudo systemctl status apache2
```

## 5.2 – Téléchargement et installation de LogAnalyzer

- Téléchargez la dernière version de LogAnalyzer (vérifiez la version disponible sur <https://loganalyzer.adiscon.com>) :

```
cd /tmp
wget https://download.adiscon.com/loganalyzer/loganalyzer-4.1.13.tar.gz
```

- Extrayez l'archive et déplacez les fichiers dans le répertoire web d'Apache :

```
tar xzf loganalyzer-4.1.13.tar.gz
sudo cp -r loganalyzer-4.1.13/src /var/www/html/loganalyzer
```

- Créez le fichier de configuration vide et définissez les permissions :

```
sudo touch /var/www/html/loganalyzer/config.php
sudo chmod 666 /var/www/html/loganalyzer/config.php
sudo chown -R www-data:www-data /var/www/html/loganalyzer
```

## 5.3 – Configuration de LogAnalyzer via l'assistant web

- Ouvrez votre navigateur et accédez à l'assistant de configuration (remplacez l'IP par celle du serveur) :

```
http://10.10.10.60/loganalyzer/install.php
```

- Suivez les étapes de l'assistant :

| Étape | Page                  | Action                                                                                                      |
|-------|-----------------------|-------------------------------------------------------------------------------------------------------------|
| 1     | <b>Vérification</b>   | Vérifiez que toutes les dépendances PHP sont au vert puis cliquez « Next »                                  |
| 2     | <b>Configuration</b>  | Laissez les valeurs par défaut. Activez « Enable User Database » si vous souhaitez une authentification     |
| 3     | <b>Source de logs</b> | Choisissez « Syslog Files » comme type de source. Indiquez le chemin :<br><code>/var/log/clients/*/*</code> |
| 4     | <b>Fin</b>            | Cliquez « Finish ». L'installation est terminée                                                             |

- Supprimez le fichier d'installation pour des raisons de sécurité :

```
sudo rm /var/www/html/loganalyzer/install.php
```

- Accédez à l'interface principale de LogAnalyzer :

<http://10.10.10.60/loganalyzer/>

L'interface affiche en temps réel les logs reçus par le serveur Rsyslog. Il est possible de **filtrer par machine**, **par niveau de sévérité**, **par programme** ou d'effectuer une **recherche par mot-clé**.

**Info :** LogAnalyzer lit directement les fichiers de logs sur le disque. Aucune base de données n'est requise dans cette configuration. Pour des volumes importants, une configuration avec MariaDB est possible.

## 6 – ROTATION ET ARCHIVAGE AUTOMATIQUE DES LOGS

La centralisation de logs génère rapidement de **grands volumes de données**. Il est indispensable de configurer la rotation automatique des fichiers pour éviter de saturer le disque du serveur.

- Créez un fichier de configuration Logrotate dédié aux logs clients :

`sudo nano /etc/logrotate.d/rsyslog-clients`

- Saisissez la configuration suivante :

```
/var/log/clients/*/*.log {
    daily
    rotate 30
    compress
    delaycompress
    missingok
    notifempty
    sharedscripts
    postrotate
        /usr/lib/rsyslog/rsyslog-rotate
    endscript
}
```

Cette configuration applique les règles suivantes :

| Directive                  | Effet                                                                            |
|----------------------------|----------------------------------------------------------------------------------|
| <code>daily</code>         | Rotation quotidienne des fichiers                                                |
| <code>rotate 30</code>     | Conservation des 30 dernières archives (30 jours)                                |
| <code>compress</code>      | Compression des archives au format gzip                                          |
| <code>delaycompress</code> | Le fichier le plus récent n'est pas compressé immédiatement                      |
| <code>missingok</code>     | Pas d'erreur si un fichier de log est absent                                     |
| <code>notifempty</code>    | Pas de rotation si le fichier est vide                                           |
| <code>postrotate</code>    | Redémarre Rsyslog après la rotation pour prendre en compte les nouveaux fichiers |

- Testez la configuration Logrotate sans effectuer de rotation réelle :  
`sudo logrotate --debug /etc/logrotate.d/rsyslog-clients`

**Info :** Par défaut, Logrotate s'exécute automatiquement chaque nuit via une tâche cron. Aucune configuration supplémentaire n'est nécessaire.

## CONCLUSION

La mise en place d'un serveur **Rsyslog centralisé** sur Debian 13 constitue un élément fondamental d'une infrastructure réseau sécurisée. En collectant les logs de l'ensemble des machines et équipements réseau (Linux, Cisco, pfSense) en un point unique, l'administrateur dispose d'une **visibilité globale** sur l'état du système d'information.

L'interface web **LogAnalyzer** permet de consulter et de rechercher rapidement parmi les événements enregistrés, sans nécessiter de base de données. Combiné à la rotation automatique des logs avec **Logrotate**, cet ensemble forme une solution de journalisation complète, légère et adaptée au niveau BTS SIO SISR.

Documentation officielle Rsyslog : <https://www.rsyslog.com/doc/>

Documentation LogAnalyzer : <https://loganalyzer.adiscon.com/doc/>