Brette Morgane BTS SIO 2 **2024/2025**

Guide d'installation de Rsyslog dans un environnement Linux

Table des matières

I- Qu'est-ce que Rsyslog ?

1. Définition de Rsyslog

Rsyslog signifie « The rocket-fast system for log processing », ou en français « le système ultra-rapide de traitement des journaux ». De ce fait, Rsyslog est un logiciel open-source (logiciel libre) de journalisation avancée pour les systèmes UNIX ou Linux, tels que Debian, Ubuntu, sous lesquels il s'exécute en tant que service[1]. Ce démon[2] de journalisation fonctionne en arrière-plan, en temps réel afin de collecter, filtrer, stocker, centraliser, et transmettre les messages des journaux d'évènements générés par les applications, ainsi que le système. L'objectif est de repérer de manière plus efficace, et rapide les défaillances.
Rsyslog apparaît au début des années 2000 grâce à Rainer Gerhards[3], et est issu de Syslog qui est également un système de journalisation pour les systèmes Unix, et Linux. Rsyslog se veut une version améliorée de Syslog, qui est un vieux protocole des années 80.

[1] Cela signifie que le programme s'exécute en processus de fond, démarrant automatiquement lors du démarrage du système, et s'exécute en continu sans intervention directe de le l'utilisation.
[2] Démon, ou (daemon en anglais) est un programme qui fonctionne en arrière-plan.
[3] Ingénieur de logiciels, réseaux allemand.

2. Objectifs et utilité de Rsyslog

Dans notre système, Rsyslog va être utilisé pour :

-centraliser les logs[4]. En effet, lorsque Rsyslog est installé, et configuré sur un serveur central (serveur de centralisation de logs) , il peut collecter les logs de plusieurs machines clientes ;

-faciliter le diagnostic, et le dépannage. Rsyslog permet de faciliter l'analyse des évènements du système, en la rendant davantage rapide ;

-améliorer la sécurité. De plus, Rsyslog grâce à la surveillance des activités, peut détecter des intrusions qui sembleraient suspectes ;

-une évolution de Rsyslog, par rapport à Syslog est la gestion efficace du stockage des logs. En autre, Rsyslog peut être configuré pour enregistrer les logs dans des fichiers locaux de la machine, ou les envoyer vers des databases[5], d'autres fichiers, ou encore des outils d'analyse (comme Graylog) afin de diagnostiquer les logs et ;

-une autre évolution, est l'automatisation de la gestion des logs, en appliquant des règles de filtrage (niveau de gravité), compression des anciens fichiers de logs pour libérer de l'espace disque tout en conservant l'intégrité des informations, ou encore la rotation en gérant la taille, ainsi que la durée de vie des logs, jusqu'à les supprimer.

[4] Diminutif de « logging », pouvant être traduit par journal en français.
[5] Bases de données.

3. Avantages de Rsyslog

Les avantages de Rsyslog reposent sur plusieurs aspects :

-il est capable de traiter, et d'expédier un grand volume de logs rapidement, il a donc une performance élevée de traitement, et de gestion des logs ;

-il est capable de supporter différents formats, et on peut l'intégrer avec d'autres outils tels que Logstash[6], ce qui rend Rsyslog extensible ;

-Rsyslog est flexible, puisqu'il permet de filtrer les logs selon des critères précis, tels que le niveau de gravité, le type d'évènement, et bien d'autres ;

-Il est capable de supporter les databases pour stocker les logs comme dans MySQL ;

-L'autre avantage de Rsyslog est qu'il compatible avec les anciens formats de Syslog et ;

-Une nécessité également à l'heure actuelle, est qu'il prend en charge le protocole cryptographique TLS[7] permettant de chiffrer les logs, lors de leur envoi à distance.

[6] Outil servant à collecter, traiter, transformer, et acheminer de données de logs.
[7] Transport Layer Security, en français Sécurité de la couche de transport.

4. Fonctionnalités principales de Rsyslog.

Rsyslog est doté de multiples fonctionnalités principales :

-il est capable d'envoyer les logs vers des outils externes, tels que Graylog[8].

-il peut stocker les logs sous différents formats comme texte, bases de données, et bien d'autres.

-il a une rotation automatique des logs afin d'éviter que leur stockage entraine une surcharge.

-il supporte les protocoles TCP[9] et UDP[10], lorsque Rsyslog envoie, et réceptionne des logs.

-Rsyslog permet de filtrer de manière efficace les logs.

-Rsyslog gère évidemment les logs selon leur niveau de priorité (log d'erreur, d'information, critique, et bien d'autres).

[8] Outil de gestion, et d'analyse de logs.
[9] Transmission Control Protocol, ou Protocole de contrôle de Transmission, est un protocole réseau permettant de transporter de manière fiable les données.
[10] User Data Protocol, ou protocole de datagramme utilisateur est un protocole de communication moins fiable, mais plus rapide de transport des données.

II- Installation de Rsyslog

1. Vérifier si Rsyslog est déjà présent sur le système

Ouvrir le terminal dans l'interface graphique

Passer en « root » en rentrant la commande « **su root** »

```
@debian:~$ su root
```

Commande « **dpkg -l | grep rsyslog** »
Cette commande permet de lister tous les paquets installés sur le système | filtrer les résultats et afficher unique ceux contenant le mot « rsyslog »

```
root@debian:/home/elk# dpkg -l | grep rsyslog
ii  rsyslog                      8.2302.0-1                  amd64        reliable system and kernel logging daemon
```

→Ici, on constate que les paquets :
*Package Rsyslog installé et configuré (ii)
*Avec la version du paquet (8.2302.0-1)
*Architecture du système (amd64) : architecture de Rsyslog en 64 bits
*Description du paquet (daemon de journalisation système et noyau)

→ Si après commande rien ne s'affiche, c'est que Rsyslog n'est pas installé.

```
root@debian:/home/a# dpkg -l | grep rsyslog
root@debian:/home/a# apt upgrade && apt update
```

2. Installation de Rsyslog sous Debian

Il faut mettre à jour, et à niveau les paquets disponibles avec la commande
« **apt update && apt upgrade** »

```
root@debian:/home/elk# apt update && apt upgrade
```

→ « *Après cette opération, 0 o d'espace disque supplémentaires seront utilisées. Souhaitez-vous continuer ? [O/N]* »
Choisir «O » afin de confirmer, et de terminer la commande en cours d'exécution.

```
root@debian:/home/elk# apt update && apt upgrade
Atteint :1 http://security.debian.org/debian-security bookworm-security InRelease
Atteint :2 http://deb.debian.org/debian bookworm InRelease
Réception de :3 http://deb.debian.org/debian bookworm-updates InRelease [55,4 kB]
Atteint :4 https://artifacts.elastic.co/packages/7.x/apt stable InRelease
55,4 ko réceptionnés en 0s (114 ko/s)
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
5 paquets peuvent être mis à jour. Exécutez « apt list --upgradable » pour les voir.
W: https://artifacts.elastic.co/packages/7.x/apt/dists/stable/InRelease: Key is stored in legacy trusted
.gpg keyring (/etc/apt/trusted.gpg), see the DEPRECATION section in apt-key(8) for details.
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Calcul de la mise à jour... Fait
Les paquets suivants seront mis à jour :
  libopenh264-7 xserver-common xserver-xephyr xserver-xorg-core xserver-xorg-legacy
5 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 0 o/12,2 Mo dans les archives.
Après cette opération, 0 o d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] o
```

Installer Rsyslog avec la commande « **apt install rsyslog** »

```
root@debian:/home/elk# apt install  rsyslog
```

→ « *Après cette opération, 2 280 ko d'espace disque supplémentaires seront utilisées. Souhaitez-vous continuer ? [O/N]* »
choisir «O » afin de confirmer, et de poursuivre l'installation de Rsyslog.

```
root@debian:/home/elk# apt install  rsyslog
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  libestr0 libfastjson4 liblognorm5
Paquets suggérés :
  rsyslog-mysql | rsyslog-pgsql rsyslog-mongodb rsyslog-doc rsyslog-openssl
  | rsyslog-gnutls rsyslog-gssapi rsyslog-relp
Les NOUVEAUX paquets suivants seront installés :
  libestr0 libfastjson4 liblognorm5 rsyslog
0 mis à jour, 4 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 829 ko dans les archives.
Après cette opération, 2 280 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] o
```

Maintenant on veut vérifier que le service Rsyslog fonctionne

→ On utilise la commande « **systemctl start rsyslog** » permettre de démarrer rsyslog

→ On utilise la commande « **systemctl enable rsyslog** » permettre d'activer le service Rsyslog, pour qu'il démarre automatiquement à chaque démarrage du système.

```
root@debian:/home/elk# systemctl start rsyslog
root@debian:/home/elk# systemctl enable rsyslog
```

Vérifier que Rsyslog fonctionne correctement

→ On utilise la commande « **systemctl status rsyslog** »

```
root@debian:/home/a# systemctl status rsyslog
● rsyslog.service - System Logging Service
     Loaded: loaded (/lib/systemd/system/rsyslog.service; enabled; preset: enabled)
     Active: active (running) since Fri 2025-05-02 10:42:42 CEST; 38min ago
TriggeredBy: ● syslog.socket
       Docs: man:rsyslogd(8)
             man:rsyslog.conf(5)
             https://www.rsyslog.com/doc/
   Main PID: 3528 (rsyslogd)
      Tasks: 4 (limit: 4590)
     Memory: 1.7M
        CPU: 10ms
     CGroup: /system.slice/rsyslog.service
             └─3528 /usr/sbin/rsyslogd -n -iNONE

mai 02 10:42:42 debian systemd[1]: Starting rsyslog.service - System Logging Service...
mai 02 10:42:42 debian rsyslogd[3528]: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3) from systemd.  [v8.2302.0]
mai 02 10:42:42 debian rsyslogd[3528]: [origin software="rsyslogd" swVersion="8.2302.0" x-pid="3528" x-info="https://www.rsyslog.com"] start
mai 02 10:42:42 debian systemd[1]: Started rsyslog.service - System Logging Service.
```

<u>Voici ce que présente la capture</u>

```
Loaded: loaded (/lib/systemd/system/rsyslog.service; enabled; preset: enabled)
```

*__Loaded__ : le fichier du service est bien chargé depuis le répertoire système.

*__Enabled__ : le service est configuré pour se lancer automatiquement au démarrage.

*__Preset: enabled__ : cela suit la configuration par défaut de Debian.

```
Active: active (running) since Fri 2025-05-02 10:42:42 CEST; 38min ago
```

*__Active (running)__ : le service fonctionne normalement.

*Il est démarré depuis 38 minutes (à la date indiquée).

```
TriggeredBy: ● syslog.socket
```

Cela indique que rsyslog peut aussi être déclenché via un socket système.

```
Main PID: 3528 (rsyslogd)
   Tasks: 4 (limit: 4590)
  Memory: 1.7M
     CPU: 10ms
  CGroup: /system.slice/rsyslog.service
          └─3528 /usr/sbin/rsyslogd -n -iNONE
```

*__Memory : 1.7__ : exemple mémoire utilisé par le service

```
mai 02 10:42:42 debian systemd[1]: Starting rsyslog.service - System Logging Service...
mai 02 10:42:42 debian rsyslogd[3528]: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3) from systemd.  [v8.2302.0]
mai 02 10:42:42 debian rsyslogd[3528]: [origin software="rsyslogd" swVersion="8.2302.0" x-pid="3528" x-info="https://www.rsyslog.com"] start
mai 02 10:42:42 debian systemd[1]: Started rsyslog.service - System Logging Service.
```

Journal de logs au démarrage

*ex : *mai 02 10:42:42 debian systemd[1]: Starting rsyslog.service - System Logging Service...*

Ici, le systemd commence à lancer le service rsyslog.

3. Vérification des logs

Par défaut, Rsyslog stocke les logs dans « **/var/log** ». Parmi les fichiers les plus importants, on trouve dans :

→ « **var/log/syslog** » les logs systèmes et applicatifs

→La commande « **tail -f /var/log/syslog** » afficher les dernières lignes du fichier.

```
root@debian:/home/a# tail -f /var/log/syslog
2025-05-02T10:42:42.720649+02:00 debian kernel: [    9.483724] vmwgfx 0000:00:0f.0: [drm] Using CursorMob mobid 3, max dimension 2048
2025-05-02T10:42:42.720654+02:00 debian kernel: [    9.488326] vmwgfx 0000:00:0f.0: [drm] Using CursorMob mobid 4, max dimension 2048
2025-05-02T10:42:42.720654+02:00 debian kernel: [   15.895630] rfkill: input handler enabled
2025-05-02T10:42:42.720654+02:00 debian kernel: [   17.200826] rfkill: input handler disabled
2025-05-02T10:42:42.720654+02:00 debian kernel: [   18.651907] input: VMware DnD UInput pointer as /devices/virtual/input/input7
2025-05-02T10:42:48.594915+02:00 debian PackageKit: get-updates transaction /47_ddcacaeb from uid 1000 finished with success after 236ms
2025-05-02T10:44:02.056067+02:00 debian anacron[646]: Job `cron.daily' started
2025-05-02T10:44:02.060252+02:00 debian anacron[3559]: Updated timestamp for job `cron.daily' to 2025-05-02
2025-05-02T10:44:04.028706+02:00 debian anacron[646]: Job `cron.daily' terminated
2025-05-02T10:45:34.188550+02:00 debian systemd[1]: Reloading.
```

→ « **/var/log/auth.log** » les logs d'authentification en temps réel.

```
root@debian:/home/elk# tail -f /var/log/auth.log
2025-03-01T18:30:01.116825+01:00 debian CRON[34435]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
2025-03-01T18:30:01.118394+01:00 debian CRON[34435]: pam_unix(cron:session): session closed for user root
```

***2025-03-01T18:30:01.118625+01:00** : date et heure de l'évènement.

***debian** : nom de la machine.

***session opened for user root (uid=0) by (uid=0)** : session cron[11] ouverte par l'utilisateur root.

***session closed for user root** : session CRON fermé derrière.

[11] CRON est un planificateur de tâches sous Linux permettant d'exécuter de façon automatique commandes/scripts à des intervalles de temps (secondes/ heures/ …) définis.

→ « **/var/log/kern.log** » contenant les logs du noyau Linux, c'est-à-dire tous les messages générés par le noyau (kernel).

```
root@debian:/home/a# cat /var/log/kern.log
2025-05-02T10:42:42.718389+02:00 debian kernel: [    0.000000] Linux version 6.1.0-34-amd64 (debian-kernel@lists.debian.org) (gcc-12 (Debian 12.2.0-14+deb12u1) 12.2.0, GNU ld (GNU Binutils for Debian) 2.40) #1 S
MP PREEMPT_DYNAMIC Debian 6.1.135-1 (2025-04-25)
2025-05-02T10:42:42.718917+02:00 debian kernel: [    0.000000] Command line: BOOT_IMAGE=/boot/vmlinuz-6.1.0-34-amd64 root=UUID=d0fd9259-efc3-4d9d-b2db-8d2c86bbdb05 ro quiet
2025-05-02T10:42:42.718919+02:00 debian kernel: [    0.000000] BIOS-provided physical RAM map:
2025-05-02T10:42:42.718920+02:00 debian kernel: [    0.000000] BIOS-e820: [mem 0x0000000000000000-0x000000000009e7ff] usable
2025-05-02T10:42:42.718920+02:00 debian kernel: [    0.000000] BIOS-e820: [mem 0x000000000009e800-0x000000000009ffff] reserved
2025-05-02T10:42:42.718921+02:00 debian kernel: [    0.000000] BIOS-e820: [mem 0x00000000000dc000-0x00000000000fffff] reserved
```

4. Tester Rsyslog

Pour tester Rsyslog, on doit envoyer un message de test.
Pour cela, nous allons utiliser la commande « **logger « Test de Rsyslog – Messagdetest** ». La commande « **logger** » permet d'envoyer un message dans les journaux système.

```
root@debian:/home/elk# logger "test de rsyslog - coucou ca marche ou pas"
```

Maintenant, il faut vérifier que le message test apparaisse dans « **/var/log/syslog** »
Nous utilisons la commande « **tail -n 1 /var/log/syslog** »

```
2025-03-01T19:06:24.158715+01:00 debian root: test de rsyslog - coucou ca marche ou pas
```

Rsyslog fonctionne, car le message apparaît bien.