

Journald et systemd

Le développement de **systemd** a permis le développement de **journald** et **journalctl** permettant une exploitation plus efficace des logs.

journal-remote permet d'exporter les logs **journald** et de les intégrer sur une machine distante.

journal-remote : le récepteur ou serveur de collecte

On doit spécifier 3 paramètres situés dans 2 fichiers de configuration :

- le port TCP d'écoute
- le protocole utilisé : **http** ou **https**
- le répertoire de destination des logs en entrée

On doit installer le paquet **systemd-journal-remote** et activer l'écoute sur le port :

```
sudo apt-get install systemd-journal-remote
sudo systemctl enable systemd-journal-remote.socket
```

Journal-remote peut fonctionner en mode **passif** ou **actif**, le mode **passif** nous intéressera seul ici.

Le fichier de configuration **/etc/systemd/system/sockets.target.wants/systemd-journal-remote.socket** décrit le port d'écoute avec la rubrique **ListenStream**.

```
[Unit]
Description=Journal Remote Sink Socket
```

```
[Socket]
ListenStream=19532
```

```
[Install]
WantedBy=sockets.target
```

Protocole(http/https) et emplacement du journal/log

Pour changer le protocole utilisé (http/https) pour le transfert, et la destination, copier **/lib/systemd/system/systemd-journal-remote.service** dans le répertoire **/etc/systemd/system/**,

puis éditer le fichier **/etc/systemd/system/systemd-journal-remote.service**

[systemd-journal-remote.service](#)

```
[Unit]
Description=Journal Remote Sink Service
Documentation=man:systemd-journal-remote(8) man:journal-remote.conf(5)
Requires=systemd-journal-remote.socket
```

```
[Service]
ExecStart=/etc/systemd/systemd-journal-remote \
    --listen-http=-3 \
    --output=/var/log/journal/remote/
User=systemd-journal-remote
Group=systemd-journal-remote
PrivateTmp=yes
```

Mission I3 - Centralisation des logs

Journald et systemd

```
PrivateDevices=yes  
PrivateNetwork=yes  
WatchdogSec=3min
```

```
[Install]  
Also=systemd-journal-remote.socket
```

La clause **–listen-http=-3** indique que le journal utilise **http**. On peut le changer pour **https** avec **–listen-https=-3**.

La clause **–output=/var/log/journal/remote/** indique le répertoire de stockage du journal. Il doit être créé s'il n'existe pas et doit être possédé par l'utilisateur **systemd-journal-remote**.

```
sudo mkdir /var/log/journal/remote  
sudo chown systemd-journal-remote /var/log/journal/remote
```

Relancer **journal-remote.socket** après la configuration avec :

```
sudo systemctl daemon-reload
```

journal-remote : l'émetteur

L'application à installer est également **systemd-journal-remote**

```
sudo apt install -y systemd-journal-remote
```

La configuration ne concerne qu'un seul fichier : **/etc/systemd/journal-upload.conf**, dans lequel on doit indiquer l' de destination (écoute sur le port 19532). Il est possible d'utiliser une liaison sécurisée par TLS en gérant les certificats.

Fichier **/etc/systemd/journal-upload.conf**

```
[Upload]  
URL=http://10.0.0.1:19532  
# ServerKeyFile=/etc/ssl/private/journal-upload.pem  
# ServerCertificateFile=/etc/ssl/certs/journal-upload.pem  
# TrustedCertificateFile=/etc/ssl/ca/trusted.pem
```

Pour lancer automatiquement **systemd-journal-upload.service** au démarrage :

```
sudo systemctl enable systemd-journal-upload.service
```

On peut alors relancer le service **systemd-journal-upload.service** pour prendre en charge le changement de configuration :

```
sudo systemctl restart systemd-journal-upload.service
```

Exploitation et examen des logs

journalctl permet d'examiner et d'effectuer des recherches sur les logs

Mission I3 - Centralisation des logs

Journald et systemd

journalctl affiche par défaut les logs de la machine locale.

Pour afficher les logs issus de machines distantes, on doit spécifier le répertoire de stockage des logs distants

```
journalctl -D /var/log/journal/remote
```

On peut également spécifier un fichier avec `journalctl -file=fichier`

```
journalctl -D /var/log/journal/remote # affiche tous les logs hébergés dans le
répertoire /var/log/journal/remote
Jan 06 21:17:01 journald-snd-1 CRON[833]: pam_unix(cron:session): session opened
for user root(uid=0) by (uid=0)
-- Boot fed69de4b7ca4d1fb0146227197b67b4 --
Jan 06 21:17:01 journald-snd-2 CRON[833]: (root) CMD (  cd / && run-parts --
report /etc/cron.hourly)
-- Boot 6e692b3ce23b4e47992a2856c4536262 --
Jan 06 21:17:01 journald-snd-1 CRON[834]: (root) CMD (  cd / && run-parts --
report /etc/cron.hourly)
-- Boot fed69de4b7ca4d1fb0146227197b67b4 --
Jan 06 21:17:01 journald-snd-2 CRON[832]: pam_unix(cron:session): session closed
for user root
-- Boot 6e692b3ce23b4e47992a2856c4536262 --
Jan 06 21:17:01 journald-snd-1 CRON[833]: pam_unix(cron:session): session closed
for user root
...
```

```
vagrant@journald-rcv:~$ ls -lh /var/log/journal/remote
total 17M
-rw-r----- 1 systemd-journal-remote systemd-journal-remote 8.0M Jan  6 21:17
remote-192.168.56.11.journal
-rw-r----- 1 systemd-journal-remote systemd-journal-remote 8.0M Jan  6 21:17
remote-192.168.56.12.journal
```

La commande **journalctl** offre de très nombreuses options décrites dans la **manpage**.