journalctl-remote

/via: https://www.digitalocean.com/community/tutorials/how-to-centralize-logs-with-journald-on-ubuntu-20-04-es
/via: https://serverfault.com/questions/758244/how-to-configure-systemd-journal-remote

basico

```
sudo apt update -y && sudo apt upgrade -y
sudo apt install systemd-journal-remote
```

servidor

- instalar servicios:

```
sudo systemctl enable --now systemd-journal-remote.socket
sudo systemctl enable systemd-journal-remote.service

# si ufw
sudo ufw allow in 19532/tcp
sudo ufw allow in 80/tcp    # solo si vamos a usar Let's Encrypt
```

con certificados TLS

- conseguir certificados Let's Encrypt

- /etc/systemd/journal-remote.conf

```
[Remote]
Seal=false # true, firma los datos de registro en el diario.
SplitMode=host # false, todos los registros en un único archivo
ServerKeyFile=/etc/letsencrypt/live/server.your_domain/privkey.pem
ServerCertificateFile=/etc/letsencrypt/live/server.your_domain/fullchain.pem
TrustedCertificateFile=/etc/letsencrypt/live/server.your_domain/letsencrypt-combined-certs.pem
```

- ```
  sudo chmod 0755 /etc/letsencrypt/{live,archive}
  sudo chmod 0640 /etc/letsencrypt/live/server.your_domain/privkey.pem
  sudo chgrp systemd-journal-remote
  /etc/letsencrypt/live/server.your_domain/privkey.pem
  ```

sin certificados

- ubicación fichero puerto escucha: **/etc/systemd/system/sockets.target.wants/systemd-journal-remote.socket**
  ```

- protocolo:

```
sudo cp /lib/systemd/system/systemd-journal-remote.service
/etc/systemd/system/
```

- cambiar `--listen-https=-3` por `--listen-http=-3`

  /etc/systemd/system/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
PrivateDevices=yes
PrivateNetwork=yes
WatchdogSec=3min

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

  - `output` permitiría cambiar la ubicación de los archivos remotos

continuación server

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

sudo systemctl daemon-reload
sudo systemctl start systemd-journal-remote.service
```

cliente

- `sudo adduser --system --home /run/systemd --no-create-home --disabled-login --group systemd-journal-upload`

con certificados TLS

- conseguir certificados Let's Encrypt
- `sudo chmod 0755 /etc/letsencrypt/{live,archive}`
  `sudo chmod 0640 /etc/letsencrypt/live/client.your_domain/privkey.pem`

```
sudo chgrp systemd-journal-upload
/etc/letsencrypt/live/client.your_domain/privkey.pem
```

- /etc/systemd/journal-upload.conf

```
[Upload]
URL=https://server.your_domain:19532
ServerKeyFile=/etc/letsencrypt/live/client.your_domain/privkey.pem
ServerCertificateFile=/etc/letsencrypt/live/client.your_domain/fullchain.
pem
TrustedCertificateFile=/etc/letsencrypt/live/client.your_domain/letsencry
pt-combined-certs.pem
```

sin certificados

- /etc/systemd/journal-upload.conf

```
[Upload]
URL=http://server.your_domain:19532
#ServerKeyFile=/etc/letsencrypt/live/client.your_domain/privkey.pem
#ServerCertificateFile=/etc/letsencrypt/live/client.your_domain/fullchain
.pem
#TrustedCertificateFile=/etc/letsencrypt/live/client.your_domain/letsencr
ypt-combined-certs.pem
```

continuación cliente

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

verificación

- on server:

```
sudo ls -la /var/log/journal/remote/
sudo journalctl --file=/var/log/journal/remote/client.your_domain.journal
```

- on client:

```
sudo logger -p syslog.debug "### TEST MESSAGE from client.your_domain ###"
```