Logs

Installation des packages

À effectuer côté client et serveur :

```
apt install easy-rsa rsyslog rsyslog-gnutls
```

Certificats (easy-rsa)

ℹ️ Générer les clés dans /opt/easy-ras/pki

```
apt install easy-rsa
cp -r /usr/share/easy-rsa /opt/
cd /opt/easy-rsa
./easy-rsa init-pki
./easy-rsa build-ca nopass
./easy-rsa build-client-full client.domain.tld nopass
./easy-rsa build-server-full serveur.domain.tld nopass
tree .
```

ℹ️ Copie des clés vers le client :

`scp ca.pem user0@172.16.246.13 :/tmp`

`scp cert.pem user0@172.16.246.13 :/tmp`

`scp key.pem user0@172.16.246.13 :/tmp`

ATTENTION LES DROITS, LE PROPRIETAIRE ET LE GROUPE PEUT CHANGER LORS DE LA COPIE

Rsyslog (serveur)

ℹ️ /etc/rsyslog.d/server.conf

```
DefaultNetstreamDriver gtls

# certificate files
$DefaultNetstreamDriverCAFile /opt/easy-rsa/pki/ca.crt
$DefaultNetstreamDriverCertFile /opt/easy-rsa/pki/issued/log.tp.lan.crt
$DefaultNetstreamDriverKeyFile /opt/easy-rsa/pki/private/log.tp.lan.key

$ModLoad imtcp  # TCP listener
$InputTCPServerStreamDriverMode 1  # run driver in TLS-only mode
$InputTCPServerStreamDriverAuthMode x509/name
$InputTCPServerStreamDriverPermittedPeer srvapp.log.tp.lan
$InputTCPServerRun 514  # start up listener at port 514
$template RemoteLogs,"/srv/log/%FROMHOST%/%HOSTNAME%/%PROGRAMNAME%.log"
*.* ?RemoteLogs
```

Rsyslog (client)

ℹ️ /etc/rsyslog.d/client.conf

```
# certificate files
$DefaultNetStreamDriverCAFile /etc/rsyslog.d/ca.pem
$DefaultNetStreamDriverCertFile /etc/rsyslog.d/cert.pem
$DefaultNetStreamDriverKeyFile /etc/rsyslog.d/key.pem
```

```
# make gtls driver the default
$DefaultNetStreamDriver gtls
$ActionSendStreamDriverMode 1   # run driver in TLS-only mode
$ActionSendStreamDriverAuthMode x509/name

module(load="imfile" PollingInterval="2") #needs to be done just once
input(type="imfile"
      File="/var/log/nginx/access.log"
      Tag="tag1"
      Severity="info"
      Facility="local7")

*.*     @@log.tp.lan:514          # forward everything to remote server
```

Fail2ban

(Configuration) tp.conf

ℹ️ /etc/fail2ban/jail.d/tp.conf

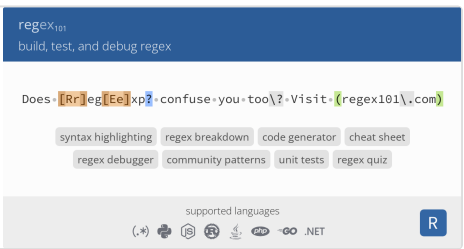
```
[sshd-login]
enabled = true
filter = sshd-login
action = iptables-allports[name=sshd-login]
  sshd-login[name="connection", dest="test456@champatux.fr", sender="tp@champatux.fr"]
findtime = 10000
maxretry = 1
bantime = 5
logpath = /var/log/auth.log
```

Filtre (sshd-login.conf)

regex101: build, test, and debug regex

Regular expression tester with syntax highlighting, explanation, cheat sheet for PHP/PCRE, Python, GO, JavaScript, Java, C#/.NET, Rust.

R https://regex101.com/



ℹ️ /etc/fail2ban/filter.d/sshd-login.conf

```
# fail2ban filter configuration for nginx
[Definition]
failregex = ^.* sshd\[\d+\]: (Accepted password|Accepted publickey) for .* from <HOST> port .*$
ignoreregex =
```

Action (sshd-login.conf)

ℹ️ /etc/fail2ban/action.d/sshd-login.conf

```
# Fail2Ban configuration file
#
# Author: Cyril Jaquier
#
#

[INCLUDES]

before = sendmail-common.conf
         mail-whois-common.conf

[Definition]

# bypass ban/unban for restored tickets
norestored = 1

# Option:  actionban
# Notes.:  command executed when banning an IP. Take care that the
#          command is executed with Fail2Ban user rights.
# Tags:    See jail.conf(5) man page
# Values:  CMD
#
actionban = printf %%b "Subject: [Fail2Ban] <name>: connection à <ip> depuis <f>
            Date: `LC_ALL=C date +"%%a, %%d %%h %%Y %%T %%z"`
            From: <sendername> <<sender>>
            To: <dest>\n
            coucou,\n
            une connection ssh viens d'avoir lieu sur <ip>
            \n
            Matches:\n
            <matches>\n\n
            cordialement,\n
            Fail2Ban" | <mailcmd>
```

```
[Init]

# Default name of the chain
#
name = default
```

Debug

```
fail2vab-regex /var/log/auth.log /etc/fail2ban/filter.d/sshd-login.conf --print-all-matched
```

ℹ️ /var/log/fail2ban.log

Postfix

Configuration (main.cf)

ℹ️ /etc/postfix/main.cf

```
#envoie des mails via champatux.fr
relayhost = mail.champatux.fr:465
smtp_sasl_password_maps = static:tp:34rV880SuCqXDA26969
smtp_sasl_security_options = noanonymous
smtp_tls_security_level = encrypt
smtp_tls_wrappermode = yes
```

Debug

ℹ️ /var/log/mail.log