El objetivo de la práctica es monitorizar log's de forma centralizada, incluso filtrando por host's clientes, incluso al final de la misma incorporar log's a una Base de Datos → MariaDB, incluso tambien a una Base de Datos → postgreSQL.

Utilizamos como SERVIDOR → 'centos2'; como CLIENTE → 'centos1', según configuración -vagrant- adjunta:

↘↘ ==> Vagrantfile:

```
Vagrant.configure("2") do |config|
      config.vm.define "centos1" do |centos|
            centos.vm.box = "centos/7"
            centos.vm.hostname = "centos1.lpic.lan"
            centos.vm.network "private_network", ip: "192.168.1.10",
               virtualbox__intnet: "intnet"
      end
      config.vm.define "centos2" do |centos|
            centos.vm.box = "centos/7"
            centos.vm.hostname = "centos2.lpic.lan"
            centos.vm.network "private_network", ip: "192.168.1.20",
               virtualbox__intnet: "intnet"
      end
end
```

↘↘ => En los '2' respectivos: → '/etc/hosts':

```
192.168.1.10   centos1.lpic.lan      centos1
192.168.1.20   centos2.lpic.lan      centos2
```

↘↘ +++ Cliente -Rsyslog- → 'centos1' +++

```
[root@centos1 ~]# yum search rsyslog
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: ftp.cica.es
 * extras: ftp.cica.es
 * updates: mirror.airenetworks.es
================================================================
============== N/S matched: rsyslog
================================================================
pcp-pmda-rsyslog.x86_64 : Performance Co-Pilot (PCP) metrics for Rsyslog
```

rsyslog-doc.x86_64 : HTML Documentation for rsyslog
rsyslog-elasticsearch.x86_64 : ElasticSearch output module for rsyslog
rsyslog-gnutls.x86_64 : TLS protocol support for rsyslog
rsyslog-gssapi.x86_64 : GSSAPI authentication and encryption support for rsyslog
rsyslog-libdbi.x86_64 : Libdbi database support for rsyslog
rsyslog-mmnormalize.x86_64 : Log normalization support for rsyslog
rsyslog-mysql.x86_64 : MySQL support for rsyslog
rsyslog-pgsql.x86_64 : PostgresSQL support for rsyslog
rsyslog-relp.x86_64 : RELP protocol support for rsyslog
rsyslog-snmp.x86_64 : SNMP protocol support for rsyslog
rsyslog.x86_64 : Enhanced system logging and kernel message trapping daemon
rsyslog-crypto.x86_64 : Encryption support
rsyslog-mmaudit.x86_64 : Message modification module supporting Linux audit format
rsyslog-mmjsonparse.x86_64 : JSON enhanced logging support
rsyslog-mmsnmptrapd.x86_64 : Message modification module for snmptrapd generated messages
rsyslog-udpspoof.x86_64 : Provides the omudpspoof module

[root@centos1 ~]# systemctl status rsyslog.service

● rsyslog.service - System Logging Service
  Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled)
  Active: active (running) since Wed 2017-10-18 07:08:46 UTC; 1h 0min ago
    Docs: man:rsyslogd(8)
          http://www.rsyslog.com/doc/
Main PID: 548 (rsyslogd)
  CGroup: /system.slice/rsyslog.service
          └─548 /usr/sbin/rsyslogd -n

Oct 18 07:08:46 centos1.lpic.lan systemd[1]: Starting System Logging Service...
Oct 18 07:08:46 centos1.lpic.lan rsyslogd[548]: [origin software="rsyslogd" swVersion="8.24.0" x-pid="548" x-info="http://www.rsyslog.com"] start
Oct 18 07:08:46 centos1.lpic.lan systemd[1]: Started System Logging Service.

[root@centos1 ~]# systemctl status chronyd.service

● chronyd.service - NTP client/server
  Loaded: loaded (/usr/lib/systemd/system/chronyd.service; enabled; vendor preset: enabled)
  Active: active (running) since Wed 2017-10-18 07:08:46 UTC; 1h 2min ago

```
     Docs: man:chronyd(8)
           man:chrony.conf(5)
  Process: 569 ExecStartPost=/usr/libexec/chrony-helper update-daemon
(code=exited, status=0/SUCCESS)
  Process: 554 ExecStart=/usr/sbin/chronyd $OPTIONS (code=exited,
status=0/SUCCESS)
 Main PID: 568 (chronyd)
   CGroup: /system.slice/chronyd.service
           └─568 /usr/sbin/chronyd

Oct 18 07:08:46 centos1.lpic.lan systemd[1]: Starting NTP client/server...
Oct 18 07:08:46 centos1.lpic.lan chronyd[568]: chronyd version 3.1 starting
(+CMDMON +NTP +REFCLOCK +RTC +PRIVDROP +SCFILTER +SECHASH
+SIGND +ASYNCDNS +IPV6 +DEBUG)
Oct 18 07:08:46 centos1.lpic.lan chronyd[568]: Frequency 7.550 +/- 14.056 ppm read
from /var/lib/chrony/drift
Oct 18 07:08:46 centos1.lpic.lan systemd[1]: Started NTP client/server.
Oct 18 07:08:56 centos1.lpic.lan chronyd[568]: Selected source 193.145.15.15
```

[root@centos1 ~]# yum provides certtool

```
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: ftp.cica.es
 * extras: ftp.cica.es
 * updates: mirror.airenetworks.es
base/7/x86_64/filelists_db
| 6.7 MB  00:00:13
extras/7/x86_64/filelists_db
| 391 kB  00:00:00
updates/7/x86_64/filelists_db
| 1.5 MB  00:00:03
```

gnutls-utils-3.3.26-9.el7.x86_64 : Command line tools for TLS protocol

```
Repo        : base
Matched from:
Filename    : /usr/bin/certtool
```

[root@centos1 ~]# yum install gnutls-utils -y

↘ Creación de Certificados, … con 'certtool', ...:

```
[root@centos1 ~]# certtool --generate-privkey --outfile ca-key.pem
Generating a 2048 bit RSA private key...
[root@centos1 ~]# ll
total 24
-rw-------. 1 root root 5720 Sep 11 18:39 anaconda-ks.cfg
-rw-------. 1 root root 5826 Oct 18 08:25 ca-key.pem
-rw-------. 1 root root 5389 Sep 11 18:39 original-ks.cfg
[root@centos1 ~]# chmod 400 ca-key.pem
[root@centos1 ~]# ll
total 24
-rw-------. 1 root root 5720 Sep 11 18:39 anaconda-ks.cfg
-r--------. 1 root root 5826 Oct 18 08:25 ca-key.pem
-rw-------. 1 root root 5389 Sep 11 18:39 original-ks.cfg

[root@centos1 ~]# certtool --generate-self-signed --load-privkey ca-key.pem
--outfile ca.pem
Generating a self signed certificate...
Please enter the details of the certificate's distinguished name. Just press enter to
ignore a field.
Common name: centos1.lpic.lan
UID:
Organizational unit name:
Organization name:
Locality name:
State or province name:
Country name (2 chars):
Enter the subject's domain component (DC):
This field should not be used in new certificates.
E-mail:
Enter the certificate's serial number in decimal (default: 6478165668233946494): 1


Activation/Expiration time.
The certificate will expire in (days): 3650


Extensions.
Does the certificate belong to an authority? (y/N): y
Path length constraint (decimal, -1 for no constraint): -1
Is this a TLS web client certificate? (y/N):
```

```
Will the certificate be used for IPsec IKE operations? (y/N):
Is this a TLS web server certificate? (y/N):
Enter a dnsName of the subject of the certificate: centos1.lpic.lan
Enter a dnsName of the subject of the certificate:
Enter a URI of the subject of the certificate:
Enter the IP address of the subject of the certificate:
Enter the e-mail of the subject of the certificate:
Will the certificate be used to sign OCSP requests? (y/N):
Will the certificate be used to sign code? (y/N):
Will the certificate be used for time stamping? (y/N):
Will the certificate be used to sign other certificates? (y/N): y
Will the certificate be used to sign CRLs? (y/N):
Enter the URI of the CRL distribution point:
X.509 Certificate Information:
        Version: 3
        Serial Number (hex): 01
        Validity:
                Not Before: Wed Oct 18 08:31:34 UTC 2017
                Not After: Sat Oct 16 08:31:48 UTC 2027
        Subject: CN=centos1.lpic.lan
        Subject Public Key Algorithm: RSA
        Algorithm Security Level: Medium (2048 bits)
                Modulus (bits 2048):
                        00:ab:ab:79:dc:da:85:d6:fb:0d:a6:b4:fb:89:57:50
                        fa:13:9f:5d:fe:46:b9:12:f0:12:27:70:bc:48:0a:8c
                        21:7c:30:93:d3:2f:ad:c4:a3:0e:79:5d:9a:84:67:b6
                        65:40:2e:80:43:73:c8:3f:79:72:5f:e2:33:57:a1:1e
                        71:64:fe:d7:07:c2:72:42:58:af:bb:3e:cb:b0:d1:7d
                        1f:3b:19:0d:b8:38:86:c3:33:bb:ab:e5:4d:7c:9b:ee
                        82:54:f6:03:0f:b9:6b:c3:87:6c:eb:e8:db:dd:86:87
                        d4:36:ca:26:a5:95:af:0f:ad:9b:44:f6:30:7e:7c:e7
                        ad:87:b6:29:08:36:08:1c:b1:9f:76:ba:8d:7b:f2:ed
                        79:40:20:ad:6c:46:2b:22:15:5f:cc:79:17:e9:5b:d8
                        d2:84:f6:32:be:d5:21:d8:34:b9:1f:9f:9f:7b:f5:2b
                        fe:1a:47:d0:bf:9b:a6:1f:c3:e9:a6:8e:fe:5f:b5:34
                        ea:39:9c:4c:6c:4b:e9:c0:14:33:34:48:08:4c:c1:c9
                        36:a8:4b:42:f9:65:6a:83:df:09:79:af:d0:c1:03:68
                        d6:11:d2:b2:b4:ef:35:df:88:01:59:1d:dc:e1:57:41
                        a7:cc:07:a2:08:6d:3a:f4:9d:2e:aa:cd:8f:c3:80:6e
                        67
```

```
            Exponent (bits 24):
                01:00:01
        Extensions:
            Basic Constraints (critical):
                Certificate Authority (CA): TRUE
            Subject Alternative Name (not critical):
                DNSname: centos1.lpic.lan
            Key Usage (critical):
                Certificate signing.
            Subject Key Identifier (not critical):
                75c4d87f06e29977afb594425dce75529a53dde6
Other Information:
        Public Key ID:
            75c4d87f06e29977afb594425dce75529a53dde6
        Public key's random art:
            +--[ RSA 2048]----+
            |          +.  .=|
            |         ..+ o+B|
            |         ...==B+|
            |        . .+.ooE|
            |       S   .. +o|
            |           . oo|
            |            oo.|
            |            .. |
            |              |
            +-----------------+

Is the above information ok? (y/N): y


Signing certificate…
```

[root@centos1 ~]# ll

```
total 28
-rw-------. 1 root root 5720 Sep 11 18:39 anaconda-ks.cfg
-r--------. 1 root root 5826 Oct 18 08:25 ca-key.pem
-rw-r--r--. 1 root root 1123 Oct 18 08:33 ca.pem
-rw-------. 1 root root 5389 Sep 11 18:39 original-ks.cfg
```

[root@centos1 ~]# certtool --generate-privkey --outfile centos2-key.pem --bits 2048
** Note: Please use the --sec-param instead of --bits
Generating a 2048 bit RSA private key...
[root@centos1 ~]# ll
total 36
-rw-------. 1 root root 5720 Sep 11 18:39 anaconda-ks.cfg
-r--------. 1 root root 5826 Oct 18 08:25 ca-key.pem
-rw-r--r--. 1 root root 1123 Oct 18 08:33 ca.pem
-rw-------. 1 root root 5813 Oct 18 08:38 centos2-key.pem
-rw-------. 1 root root 5389 Sep 11 18:39 original-ks.cfg

[root@centos1 ~]# certtool --generate-request --load-privkey centos2-key.pem --outfile centos2-request.pem
Generating a PKCS #10 certificate request...
Common name: centos2.lpic.lan
Organizational unit name:
Organization name:
Locality name:
State or province name:
Country name (2 chars):
Enter the subject's domain component (DC):
UID:
Enter a dnsName of the subject of the certificate: centos2.lpic.lan
Enter a dnsName of the subject of the certificate:
Enter a URI of the subject of the certificate:
Enter the IP address of the subject of the certificate:
Enter the e-mail of the subject of the certificate:
Enter a challenge password:
Does the certificate belong to an authority? (y/N):
Will the certificate be used for signing (DHE and RSA-EXPORT ciphersuites)? (Y/n):
Will the certificate be used for encryption (RSA ciphersuites)? (Y/n):
Will the certificate be used to sign code? (y/N):
Will the certificate be used for time stamping? (y/N):
Will the certificate be used for IPsec IKE operations? (y/N):
Will the certificate be used to sign OCSP requests? (y/N):
Is this a TLS web client certificate? (y/N): y
Is this a TLS web server certificate? (y/N): y

```
[root@centos1 ~]# ll
total 40
-rw-------. 1 root root 5720 Sep 11 18:39 anaconda-ks.cfg
-r--------. 1 root root 5826 Oct 18 08:25 ca-key.pem
-rw-r--r--. 1 root root 1123 Oct 18 08:33 ca.pem
-rw-------. 1 root root 5813 Oct 18 08:38 centos2-key.pem
-rw-------. 1 root root 2516 Oct 18 08:42 centos2-request.pem
-rw-------. 1 root root 5389 Sep 11 18:39 original-ks.cfg

[root@centos1 ~]# certtool --generate-certificate --load-request centos2-request.pem --outfile centos2-cert.pem --load-ca-certificate ca.pem --load-ca-privkey ca-key.pem
Generating a signed certificate...
Enter the certificate's serial number in decimal (default: 6478171144245925868): 1


Activation/Expiration time.
The certificate will expire in (days): 365


Extensions.
Do you want to honour the extensions from the request? (y/N):
Does the certificate belong to an authority? (y/N):
Is this a TLS web client certificate? (y/N): y
Will the certificate be used for IPsec IKE operations? (y/N):
Is this a TLS web server certificate? (y/N): y
Enter a dnsName of the subject of the certificate: centos2.lpic.lan
Enter a dnsName of the subject of the certificate:
Enter a URI of the subject of the certificate:
Enter the IP address of the subject of the certificate:
Will the certificate be used for signing (DHE and RSA-EXPORT ciphersuites)? (Y/n):
Will the certificate be used for encryption (RSA ciphersuites)? (Y/n):
Will the certificate be used to sign OCSP requests? (y/N):
Will the certificate be used to sign code? (y/N):
Will the certificate be used for time stamping? (y/N):
X.509 Certificate Information:
        Version: 3
        Serial Number (hex): 01
        Validity:
```

```
        Not Before: Wed Oct 18 08:52:41 UTC 2017
        Not After: Thu Oct 18 08:52:50 UTC 2018
    Subject: CN=centos2.lpic.lan
    Subject Public Key Algorithm: RSA
    Algorithm Security Level: Medium (2048 bits)
        Modulus (bits 2048):
            00:a1:fe:52:7c:8c:16:f0:ec:22:0f:b2:6d:e5:8b:a2
            17:66:d0:f4:bd:83:ea:97:c3:fd:32:46:60:e0:cf:db
            c2:6d:69:d4:f8:3d:6f:36:c0:84:02:7f:49:2f:49:1a
            23:37:93:a5:a3:25:e0:f4:a8:31:29:4e:1c:0c:45:91
            a6:58:20:4d:77:83:ee:be:a1:a2:97:03:c5:b5:d8:01
            e5:32:f7:19:e8:47:67:81:79:a1:bc:84:16:42:7a:f5
            26:38:e3:01:08:11:c1:34:27:c9:3b:9b:78:e8:15:fd
            b7:83:03:f8:8e:6a:14:d2:6e:66:4e:7b:92:50:2e:ea
            be:cd:f5:e7:2a:e4:91:e3:df:79:41:ac:a7:57:80:a3
            14:16:93:45:87:fd:25:9d:5f:d9:f8:54:43:c5:29:f9
            11:cc:32:a8:a5:7c:4c:41:b2:6d:ca:73:1d:f3:7a:88
            42:7c:ce:aa:f8:e0:2d:01:24:48:1f:17:78:53:ea:4f
            4a:1e:d4:d7:46:a3:5c:16:cc:a2:b3:c1:57:cf:4f:a0
            3e:33:92:c1:f7:99:2e:7b:a2:6f:69:19:fb:d7:43:7f
            5e:14:c4:64:c4:54:db:5e:6b:9d:33:cc:df:0f:99:d7
            c2:f6:9f:51:44:38:c9:81:a9:4a:ac:ba:42:f5:33:e7
            eb
        Exponent (bits 24):
            01:00:01
    Extensions:
        Basic Constraints (critical):
            Certificate Authority (CA): FALSE
        Key Purpose (not critical):
            TLS WWW Client.
            TLS WWW Server.
        Subject Alternative Name (not critical):
            DNSname: centos2.lpic.lan
        Key Usage (critical):
            Digital signature.
            Key encipherment.
        Subject Key Identifier (not critical):
            dab62ded0631f8b025d1a1d8a841c6e310e3d7e3
        Authority Key Identifier (not critical):
            75c4d87f06e29977afb594425dce75529a53dde6
```

```
Other Information:
        Public Key ID:
                dab62ded0631f8b025d1a1d8a841c6e310e3d7e3
        Public key's random art:
                +--[ RSA 2048]----+
                |ooo    ...       |
                |o+o .+...        |
                | +.ooooo         |
                |  oo. = +        |
                |  .  E *So       |
                |     .oo         |
                |     . oo        |
                |      ..oo       |
                |       .+o       |
                +-----------------+

Is the above information ok? (y/N): y


Signing certificate...
```

[root@centos1 ~]# ll

```
total 44
-rw-------. 1 root root 5720 Sep 11 18:39 anaconda-ks.cfg
-r--------. 1 root root 5826 Oct 18 08:25 ca-key.pem
-rw-r--r--. 1 root root 1123 Oct 18 08:33 ca.pem
-rw-r--r--. 1 root root 1208 Oct 18 08:53 centos2-cert.pem
-rw-------. 1 root root 5813 Oct 18 08:38 centos2-key.pem
-rw-------. 1 root root 2516 Oct 18 08:42 centos2-request.pem
-rw-------. 1 root root 5389 Sep 11 18:39 original-ks.cfg
```

↘↘ +++ Servidor -Rsyslog- → 'centos2' +++

[root@centos2 ~]# mkdir /etc/rsyslog-keys
[root@centos2 ~]# cd /etc/rsyslog-keys/

↘ Copiar desde 'centos1':

[root@centos1 ~]# scp ca.pem centos2-cert.pem centos2-key.pem root@centos2:/etc/rsyslog-keys/

```
The authenticity of host 'centos2 (192.168.1.20)' can't be established.
ECDSA key fingerprint is
SHA256:1ENd1dhwY6/DPTloqFBALIzGAlNZhmEXJEQqzm4cbfM.
ECDSA key fingerprint is MD5:b2:8b:2e:40:cf:e2:c4:f1:a2:0d:f9:46:29:44:21:42.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'centos2,192.168.1.20' (ECDSA) to the list of known
hosts.
root@centos2's password:
ca.pem
100% 1123     1.4MB/s   00:00
centos2-cert.pem
100% 1208     1.7MB/s   00:00
centos2-key.pem
100% 5813     7.2MB/s   00:00
```

[root@centos2 rsyslog-keys]# ll

```
total 16
-rw-r--r--. 1 root root 1123 Oct 18 09:03 ca.pem
-rw-r--r--. 1 root root 1208 Oct 18 09:03 centos2-cert.pem
-rw-------. 1 root root 5813 Oct 18 09:03 centos2-key.pem
```

↘ Incorporar rutas en Server → 'centos2':

[root@centos2 rsyslog-keys]# vi /etc/rsyslog.d/server.conf

```
$DefaultNetstreamDriver gtls
$DefaultNetstreamDriverCAFile /etc/rsyslog-keys/ca.pem
$DefaultNetstreamDriverCertFile /etc/rsyslog-keys/centos2-cert.pem
$DefaultNetstreamDriverKeyFile /etc/rsyslog-keys/centos2-key.pem

#$ModLoad imtcp  ↘ Habilitamos este módulo posteriormente.

$InputTCPServerStreamDriverMode 1
$InputTCPServerStreamDriverAuthMode anon
$InputTCPServerRun 6514
```

[root@centos2 rsyslog-keys]# systemctl restart rsyslog.service
[root@centos2 rsyslog-keys]# systemctl status rsyslog.service

```
● rsyslog.service - System Logging Service
   Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; vendor preset:
enabled)
```

```
   Active: active (running) since Wed 2017-10-18 09:13:29 UTC; 3s ago
     Docs: man:rsyslogd(8)
           http://www.rsyslog.com/doc/
 Main PID: 23333 (rsyslogd)
   CGroup: /system.slice/rsyslog.service
           └─23333 /usr/sbin/rsyslogd -n

Oct 18 09:13:29 centos2.lpic.lan systemd[1]: Starting System Logging Service...
Oct 18 09:13:29 centos2.lpic.lan rsyslogd[23333]:  [origin software="rsyslogd"
swVersion="8.24.0" x-pid="23333" x-info="http://www.rsyslog.com"] start
Oct 18 09:13:29 centos2.lpic.lan rsyslogd[23333]: could not load module
'/usr/lib64/rsyslog/lmnsd_gtls.so', dlopen: /usr/lib64/rsyslog/lmnsd_gtls.so: cannot
ope...m/e/2066 ]
Oct 18 09:13:29 centos2.lpic.lan rsyslogd[23333]: tcpsrv could not create listener
(inputname: 'imtcp') [v8.24.0 try http://www.rsyslog.com/e/2066 ]
Oct 18 09:13:29 centos2.lpic.lan rsyslogd[23333]: activation of module imtcp failed
[v8.24.0 try http://www.rsyslog.com/e/2066 ]
Oct 18 09:13:29 centos2.lpic.lan systemd[1]: Started System Logging Service.
Hint: Some lines were ellipsized, use -l to show in full.
```

[root@centos2 rsyslog-keys]# yum provides */lmnsd_gtls.so

```
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: mirror.tedra.es
 * extras: mirror.tedra.es
 * updates: mirror.tedra.es
base/7/x86_64/filelists_db
| 6.7 MB  00:00:08
extras/7/x86_64/filelists_db
| 391 kB  00:00:00
updates/7/x86_64/filelists_db
| 1.5 MB  00:00:01
```

rsyslog-gnutls-8.24.0-12.el7.x86_64 : TLS protocol support for rsyslog

```
Repo        : base
Matched from:
Filename    : /usr/lib64/rsyslog/lmnsd_gtls.so
```

[root@centos2 rsyslog-keys]# yum install rsyslog-gnutls -y

[root@centos2 rsyslog-keys]# systemctl restart rsyslog.service
[root@centos2 rsyslog-keys]# systemctl status rsyslog.service
● rsyslog.service - System Logging Service
Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled)
Active: active (running) since Wed 2017-10-18 09:22:46 UTC; 4s ago
Docs: man:rsyslogd(8)
http://www.rsyslog.com/doc/
Main PID: 23446 (rsyslogd)
CGroup: /system.slice/rsyslog.service
└─23446 /usr/sbin/rsyslogd -n

Oct 18 09:22:46 centos2.lpic.lan systemd[1]: Starting System Logging Service...
Oct 18 09:22:46 centos2.lpic.lan rsyslogd[23446]: [origin software="rsyslogd" swVersion="8.24.0" x-pid="23446" x-info="http://www.rsyslog.com"] start
Oct 18 09:22:46 centos2.lpic.lan systemd[1]: Started System Logging Service.

[root@centos2 rsyslog-keys]# netstat -tulpen
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address Foreign Address State User Inode PID/Program name
tcp 0 0 0.0.0.0:111 0.0.0.0:* LISTEN 0 13603 1/systemd
tcp 0 0 0.0.0.0:6514 0.0.0.0:* LISTEN 0 48289 23446/rsyslogd
tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN 0 46817 23127/sshd
tcp 0 0 127.0.0.1:25 0.0.0.0:* LISTEN 0 17133 952/master
tcp6 0 0 :::111 :::* LISTEN 0 13602 1/systemd
tcp6 0 0 :::6514 :::* LISTEN 0 48290 23446/rsyslogd
tcp6 0 0 :::22 :::* LISTEN 0 46819 23127/sshd
tcp6 0 0 ::1:25 :::* LISTEN 0 17134 952/master
udp 0 0 127.0.0.1:323 0.0.0.0:* 0 14098 563/chronyd
udp 0 0 0.0.0.0:68 0.0.0.0:* 0 22098

```
2246/dhclient
udp        0      0 0.0.0.0:27259           0.0.0.0:*                           0          22009
2246/dhclient
udp6       0      0 ::1:323                 :::*                                0          14099
563/chronyd
udp6       0      0 :::6528                 :::*                                0          22010
2246/dhclient
```

[root@centos2 rsyslog-keys]# getent services 6514
syslog-tls 6514/tcp

↘↘ +++ Cliente -Rsyslog- → 'centos1' +++

↘ Generamos →'**client.conf**' → ↘↘ /etc/rsyslog.d/**client.conf**

[root@centos1 ~]# vi /etc/rsyslog.d/client.conf

```
$DefaultNetstreamDriverCAFile /etc/rsyslog-keys/ca.pem

$DefaultNetstreamDriver gtls
$ActionSendStreamDriverMode 1
$ActionSendStreamDriverAuthMode anon
*.* @@(o)centos2.lpic.lan:6514
```

[root@centos1 ~]# mkdir /etc/rsyslog-keys
[root@centos1 ~]# cp /root/ca.pem /etc/rsyslog-keys/

[root@centos1 ~]# systemctl restart rsyslog.service
[root@centos1 ~]# systemctl status rsyslog.service

```
● rsyslog.service - System Logging Service
   Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; vendor preset:
enabled)
   Active: active (running) since Wed 2017-10-18 22:42:48 UTC; 5s ago
     Docs: man:rsyslogd(8)
           http://www.rsyslog.com/doc/
 Main PID: 3046 (rsyslogd)
   CGroup: /system.slice/rsyslog.service
           └─3046 /usr/sbin/rsyslogd -n

Oct 18 22:42:48 centos1.lpic.lan systemd[1]: Starting System Logging Service...
```

Oct 18 22:42:48 centos1.lpic.lan rsyslogd[3046]: [origin software="rsyslogd" swVersion="8.24.0" x-pid="3046" x-info="http://www.rsyslog.com"] start
Oct 18 22:42:48 centos1.lpic.lan systemd[1]: Started System Logging Service.
Oct 18 22:42:48 centos1.lpic.lan rsyslogd[3046]: could not load module '/usr/lib64/rsyslog/lmnsd_gtls.so', dlopen: /usr/lib64/rsyslog/lmnsd_gtls.so: cannot open...m/e/2066]
Oct 18 22:42:48 centos1.lpic.lan rsyslogd[3046]: could not load module '/usr/lib64/rsyslog/lmnsd_gtls.so', dlopen: /usr/lib64/rsyslog/lmnsd_gtls.so: cannot open...m/e/2066]
Oct 18 22:42:48 centos1.lpic.lan rsyslogd[3046]: action 'action 0' suspended, next retry is Wed Oct 18 22:43:18 2017 [v8.24.0 try http://www.rsyslog.com/e/2007]
Hint: Some lines were ellipsized, use -l to show in full.

[root@centos1 ~]# yum provides */lmnsd_gtls.so
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: ftp.cica.es
 * extras: ftp.cica.es
 * updates: mirror.airenetworks.es
rsyslog-gnutls-8.24.0-12.el7.x86_64 : TLS protocol support for rsyslog
Repo : base
Matched from:
Filename : /usr/lib64/rsyslog/lmnsd_gtls.so

[root@centos1 ~]# yum install rsyslog-gnutls -y
…

[root@centos1 ~]# systemctl restart rsyslog.service
[root@centos1 ~]# systemctl status rsyslog.service
● rsyslog.service - System Logging Service
 Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled)
 Active: active (running) since Wed 2017-10-18 22:48:02 UTC; 16s ago
 Docs: man:rsyslogd(8)
 http://www.rsyslog.com/doc/
Main PID: 3067 (rsyslogd)
 CGroup: /system.slice/rsyslog.service
 └─3067 /usr/sbin/rsyslogd -n

Oct 18 22:48:02 centos1.lpic.lan systemd[1]: Starting System Logging Service...

Oct 18 22:48:02 centos1.lpic.lan rsyslogd[3067]: [origin software="rsyslogd" swVersion="8.24.0" x-pid="3067" x-info="http://www.rsyslog.com"] start
Oct 18 22:48:02 centos1.lpic.lan systemd[1]: Started System Logging Service.

↘↘ +++ PRUEBA -SIN FILTRAR- → 'logs' +++

Miauuuuuu, ….

[root@centos1 ~]# logger Hola mi amor, que gatita mas linda, …

[root@centos2 ~]# tail /var/log/messages
Oct 18 23:01:01 centos1 systemd: Starting Session 8 of user root.
Oct 18 23:01:01 centos2 systemd: Created slice User Slice of root.
Oct 18 23:01:01 centos2 systemd: Starting User Slice of root.
Oct 18 23:01:01 centos2 systemd: Started Session 8 of user root.
Oct 18 23:01:01 centos2 systemd: Starting Session 8 of user root.
Oct 18 23:01:01 centos1 systemd: Removed slice User Slice of root.
Oct 18 23:01:01 centos1 systemd: Stopping User Slice of root.
Oct 18 23:01:01 centos2 systemd: Removed slice User Slice of root.
Oct 18 23:01:01 centos2 systemd: Stopping User Slice of root.
Oct 18 23:11:12 centos1 vagrant: Hola mi amor, que gatita mas linda, ...

↘↘ +++ FILTRADO de -Rsyslog- → 'centos2' → SERVIDOR +++

↘ +++ Servidor -Rsyslog- → 'centos2' +++

[root@centos2 ~]# mkdir /var/log/rsyslog

[root@centos2 etc]# vi /etc/rsyslog.conf
↘ Habilitamos lo siguiente:

```
# Provides UDP syslog reception
$ModLoad imudp
$UDPServerRun 514

# Provides TCP syslog reception
$ModLoad imtcp
$InputTCPServerRun 514
```

[root@centos2 etc]# systemctl restart rsyslog.service
[root@centos2 etc]# systemctl status rsyslog.service
● rsyslog.service - System Logging Service
Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled)
Active: active (running) since Thu 2017-10-19 13:40:11 UTC; 2s ago
Docs: man:rsyslogd(8)
http://www.rsyslog.com/doc/
Main PID: 4520 (rsyslogd)
CGroup: /system.slice/rsyslog.service
└─4520 /usr/sbin/rsyslogd -n

Oct 19 13:40:11 centos2.lpic.lan systemd[1]: Starting System Logging Service...
Oct 19 13:40:11 centos2.lpic.lan rsyslogd[4520]: [origin software="rsyslogd" swVersion="8.24.0" x-pid="4520" x-info="http://www.rsyslog.com"] start
Oct 19 13:40:11 centos2.lpic.lan systemd[1]: Started System Logging Service.

[root@centos2 etc]# vi /etc/rsyslog.conf
↘ Añadimos lo siguiente:

RULES
REGLAS AÑADIDAS:

$template TmplAuth, "/var/log/rsyslog/%HOSTNAME%/%PROGRAMNAME%.log"
$template TmplMsg, "/var/log/rsyslog/%HOSTNAME%/%PROGRAMNAME%.log"
authpriv.* ?TmplAuth
***.info,mail.none,authpriv.none,cron.none ?TmplMsg**

[root@centos2 etc]# systemctl restart rsyslog.service
[root@centos2 etc]# systemctl status rsyslog.service
● rsyslog.service - System Logging Service
Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled)
Active: active (running) since Thu 2017-10-19 13:51:50 UTC; 2s ago
Docs: man:rsyslogd(8)
http://www.rsyslog.com/doc/
Main PID: 4615 (rsyslogd)

```
  CGroup: /system.slice/rsyslog.service
          └─4615 /usr/sbin/rsyslogd -n

Oct 19 13:51:50 centos2.lpic.lan systemd[1]: Starting System Logging Service...
Oct 19 13:51:50 centos2.lpic.lan rsyslogd[4615]:  [origin software="rsyslogd"
swVersion="8.24.0" x-pid="4615" x-info="http://www.rsyslog.com"] start
Oct 19 13:51:50 centos2.lpic.lan systemd[1]: Started System Logging Service.
```

↘↘ +++ PRUEBA -FILTRANDO- → 'logs' +++

MiauuuuuuMiauuuu, ….

[root@centos1 ~]# logger PRUEBA DE FILTRADO DE logs POR ANFITRION +++

[root@centos2 rsyslog]# pwd
/var/log/rsyslog
[root@centos2 rsyslog]# ls
centos1 centos2
[root@centos2 rsyslog]# ls centos1/
chronyd.log dbus.log kernel.log rsyslogd.log sshd.log systemd.log systemd-udevd.log yum.log
dbus-daemon.log groupmod.log polkitd.log sm-notify.log su.log systemd-logind.log **vagrant.log**

[root@centos2 rsyslog]# cat centos1/vagrant.log
...
Oct 23 14:46:30 centos1 vagrant: PRUEBA DE FILTRADO DE logs POR ANFITRION +++

↘ +++ Creamos -snapshot para utilización posterior +++

[labs@hp rsyslog]$ vagrant snapshot save Rsyslog-SIN_MySQL
==> centos1: Snapshotting the machine as 'Rsyslog-SIN_MySQL'...
==> centos1: Snapshot saved! You can restore the snapshot at any time by
==> centos1: using `vagrant snapshot restore`. You can delete it using
==> centos1: `vagrant snapshot delete`.
==> centos2: Snapshotting the machine as 'Rsyslog-SIN_MySQL'...
==> centos2: Snapshot saved! You can restore the snapshot at any time by
==> centos2: using `vagrant snapshot restore`. You can delete it using
==> centos2: `vagrant snapshot delete`.

===> BIBLIOGRAFIA:

http://www.rsyslog.com/doc/v8-stable/tutorials/tls_cert_ca.html
http://www.alcancelibre.org/staticpages/index.php/configuracion-rsyslog

===> LEGAL: