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
```

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

```
[root@centos2 ~]# yum install mariadb-server -y
[root@centos2 ~]# systemctl start mariadb
[root@centos2 ~]# systemctl status mariadb
● mariadb.service - MariaDB database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; vendor preset:
disabled)
   Active: active (running) since Mon 2017-10-23 15:34:03 UTC; 8s ago
  Process: 4343 ExecStartPost=/usr/libexec/mariadb-wait-ready $MAINPID
(code=exited, status=0/SUCCESS)
  Process: 4263 ExecStartPre=/usr/libexec/mariadb-prepare-db-dir %n (code=exited,
```

```
status=0/SUCCESS)
 Main PID: 4342 (mysqld_safe)
   CGroup: /system.slice/mariadb.service
           ├─4342 /bin/sh /usr/bin/mysqld_safe --basedir=/usr
           └─4504 /usr/libexec/mysqld --basedir=/usr --datadir=/var/lib/mysql --plugin-
dir=/usr/lib64/mysql/plugin --log-error=/var/log/mariadb/mariadb.log --pid-file=/va...

Oct 23 15:34:00 centos2.lpic.lan systemd[1]: Starting MariaDB database server...
Oct 23 15:34:00 centos2.lpic.lan mariadb-prepare-db-dir[4263]: Initializing MariaDB
database
Oct 23 15:34:01 centos2.lpic.lan mariadb-prepare-db-dir[4263]: 171023 15:34:01
[Note] /usr/libexec/mysqld (mysqld 5.5.56-MariaDB) starting as process 4326 ...
Oct 23 15:34:01 centos2.lpic.lan mariadb-prepare-db-dir[4263]: 171023 15:34:01
[Note] /usr/libexec/mysqld (mysqld 5.5.56-MariaDB) starting as process 4335 ...
Oct 23 15:34:01 centos2.lpic.lan mariadb-prepare-db-dir[4263]: PLEASE
REMEMBER TO SET A PASSWORD FOR THE MariaDB root USER !
Oct 23 15:34:01 centos2.lpic.lan mariadb-prepare-db-dir[4263]: To do so, start the
server, then issue the following commands:
Oct 23 15:34:01 centos2.lpic.lan mariadb-prepare-db-dir[4263]:
'/usr/bin/mysqladmin' -u root password 'new-password'
Oct 23 15:34:01 centos2.lpic.lan mysqld_safe[4342]: 171023 15:34:01 mysqld_safe
Logging to '/var/log/mariadb/mariadb.log'.
Oct 23 15:34:01 centos2.lpic.lan mysqld_safe[4342]: 171023 15:34:01 mysqld_safe
Starting mysqld daemon with databases from /var/lib/mysql
Oct 23 15:34:03 centos2.lpic.lan systemd[1]: Started MariaDB database server.
[root@centos2 ~]# systemctl enable mariadb
Created symlink from /etc/systemd/system/multi-user.target.wants/mariadb.service to
/usr/lib/systemd/system/mariadb.service.

[root@centos2 ~]# mysql_secure_installation
…

[root@centos2 ~]# mysqladmin -u root -p version
Enter password:
mysqladmin  Ver 9.0 Distrib 5.5.56-MariaDB, for Linux on x86_64
Copyright (c) 2000, 2017, Oracle, MariaDB Corporation Ab and others.

Server version          5.5.56-MariaDB
Protocol version    10
Connection          Localhost via UNIX socket
```

```
UNIX socket               /var/lib/mysql/mysql.sock
Uptime:                   5 min 8 sec

Threads: 1  Questions: 16  Slow queries: 0  Opens: 0  Flush tables: 2  Open tables: 26
Queries per second avg: 0.051
```

↘ Creamos Base de Datos:

```
[root@centos2 ~]# yum -y install rsyslog-mysql
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: mirror.tedra.es
 * extras: mirror.tedra.es
 * updates: mirror.tedra.es
Resolving Dependencies
--> Running transaction check
---> Package rsyslog-mysql.x86_64 0:8.24.0-12.el7 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
================================================================================
 Package                 Arch                    Version
Repository              Size
================================================================================
================================================================================
Installing:
 rsyslog-mysql           x86_64                  8.24.0-12.el7
base                    35 k

Transaction Summary
================================================================================
================================================================================
Install  1 Package

Total download size: 35 k
Installed size: 20 k
```

Downloading packages:
rsyslog-mysql-8.24.0-12.el7.x86_64.rpm
| 35 kB 00:00:00
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
Installing : rsyslog-mysql-8.24.0-12.el7.x86_64
1/1
Verifying : rsyslog-mysql-8.24.0-12.el7.x86_64
1/1

Installed:
rsyslog-mysql.x86_64 0:8.24.0-12.el7

Complete!

[root@centos2 ~]# ls /usr/share/doc/rsyslog-*/
AUTHORS ChangeLog COPYING COPYING.ASL20 COPYING.LESSER
mysql-createDB.sql

[root@centos2 ~]# ls /usr/share/doc/rsyslog-8.24.0/
AUTHORS ChangeLog COPYING COPYING.ASL20
COPYING.LESSER mysql-createDB.sql
[root@centos2 ~]# cat /usr/share/doc/rsyslog-8.24.0/mysql-createDB.sql

```
CREATE DATABASE Syslog;
USE Syslog;
CREATE TABLE SystemEvents
(
        ID int unsigned not null auto_increment primary key,
        CustomerID bigint,
        ReceivedAt datetime NULL,
        DeviceReportedTime datetime NULL,
        Facility smallint NULL,
        Priority smallint NULL,
        FromHost varchar(60) NULL,
        Message text,
        NTSeverity int NULL,
        Importance int NULL,
        EventSource varchar(60),
```

```
        EventUser varchar(60) NULL,
        EventCategory int NULL,
        EventID int NULL,
        EventBinaryData text NULL,
        MaxAvailable int NULL,
        CurrUsage int NULL,
        MinUsage int NULL,
        MaxUsage int NULL,
        InfoUnitID int NULL ,
        SysLogTag varchar(60),
        EventLogType varchar(60),
        GenericFileName VarChar(60),
        SystemID int NULL
);

CREATE TABLE SystemEventsProperties
(
        ID int unsigned not null auto_increment primary key,
        SystemEventID int NULL ,
        ParamName varchar(255) NULL ,
        ParamValue text NULL
);
```

[root@centos2 ~]# mysql -u root -p < /usr/share/doc/rsyslog-*/mysql-createDB.sql
Enter password:

[root@centos2 ~]# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 6
Server version: 5.5.56-MariaDB MariaDB Server

Copyright (c) 2000, 2017, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

```
MariaDB [(none)]> show databases;
+--------------------+
| Database           |
```

```
+--------------------+
| information_schema |
| Syslog             |
| mysql              |
| performance_schema |
| test               |
+--------------------+
5 rows in set (0.00 sec)
```

MariaDB [(none)]> use Syslog;

```
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [Syslog]> show tables;
+-----------------------+
| Tables_in_Syslog      |
+-----------------------+
| SystemEvents          |
| SystemEventsProperties |
+-----------------------+
2 rows in set (0.00 sec)
```

MariaDB [Syslog]> describe SystemEvents;

```
+-------------------+-----------------+------+-----+---------+----------------+
| Field             | Type            | Null | Key | Default | Extra          |
+-------------------+-----------------+------+-----+---------+----------------+
| ID                | int(10) unsigned | NO   | PRI | NULL    | auto_increment |
| CustomerID        | bigint(20)      | YES  |     | NULL    |                |
| ReceivedAt        | datetime        | YES  |     | NULL    |                |
| DeviceReportedTime | datetime        | YES  |     | NULL    |                |
| Facility          | smallint(6)     | YES  |     | NULL    |                |
| Priority          | smallint(6)     | YES  |     | NULL    |                |
| FromHost          | varchar(60)     | YES  |     | NULL    |                |
| Message           | text            | YES  |     | NULL    |                |
| NTSeverity        | int(11)         | YES  |     | NULL    |                |
| Importance        | int(11)         | YES  |     | NULL    |                |
| EventSource       | varchar(60)     | YES  |     | NULL    |                |
| EventUser         | varchar(60)     | YES  |     | NULL    |                |
| EventCategory     | int(11)         | YES  |     | NULL    |                |
```

```
| EventID          | int(11)         | YES |    | NULL    |               |
| EventBinaryData  | text            | YES |    | NULL    |               |
| MaxAvailable     | int(11)         | YES |    | NULL    |               |
| CurrUsage        | int(11)         | YES |    | NULL    |               |
| MinUsage         | int(11)         | YES |    | NULL    |               |
| MaxUsage         | int(11)         | YES |    | NULL    |               |
| InfoUnitID       | int(11)         | YES |    | NULL    |               |
| SysLogTag        | varchar(60)     | YES |    | NULL    |               |
| EventLogType     | varchar(60)     | YES |    | NULL    |               |
| GenericFileName  | varchar(60)     | YES |    | NULL    |               |
| SystemID         | int(11)         | YES |    | NULL    |               |
+------------------+-----------------+-----+-----+---------+---------------+
24 rows in set (0.00 sec)
```

MariaDB [Syslog]> describe SystemEventsProperties;

```
+--------------+-----------------+------+-----+---------+----------------+
| Field        | Type            | Null | Key | Default | Extra          |
+--------------+-----------------+------+-----+---------+----------------+
| ID           | int(10) unsigned | NO   | PRI | NULL    | auto_increment |
| SystemEventID | int(11)         | YES |    | NULL    |               |
| ParamName    | varchar(255)    | YES |    | NULL    |               |
| ParamValue   | text            | YES |    | NULL    |               |
+--------------+-----------------+------+-----+---------+----------------+
4 rows in set (0.00 sec)
```

MariaDB [Syslog]> exit

Bye

[root@centos2 ~]# mysql -u root -p

Enter password:

Welcome to the MariaDB monitor. Commands end with ; or \g.

Your MariaDB connection id is 7

Server version: 5.5.56-MariaDB MariaDB Server

Copyright (c) 2000, 2017, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> grant all on Syslog.* to Syslog@localhost identified by 'Mi-Contraseña';

Query OK, 0 rows affected (0.00 sec)

MariaDB [(none)]> exit;
Bye

↘ Editamos → '/etc/rsyslog.conf':
[root@centos2 ~]# cp /etc/rsyslog.conf /etc/rsyslog.conf.original

[root@centos2 ~]# vi /etc/rsyslog.conf
rsyslog configuration file

For more information see /usr/share/doc/rsyslog-*/rsyslog_conf.html
If you experience problems, see http://www.rsyslog.com/doc/troubleshoot.html

MODULES

The imjournal module bellow is now used as a message source instead of imuxsock.
$ModLoad imuxsock # provides support for local system logging (e.g. via logger command)
$ModLoad imjournal # provides access to the systemd journal
#$ModLoad imklog # reads kernel messages (the same are read from journald)
#$ModLoad immark # provides --MARK-- message capability

Provides UDP syslog reception
$ModLoad imudp
$UDPServerRun 514

Provides TCP syslog reception
$ModLoad imtcp
$InputTCPServerRun 514

AÑADIMOS:

 # Conexión a MySQL™/MariaDB™
$ModLoad ommysql
***.* :ommysql:127.0.0.1,Syslog,Syslog,contraseña-que-especificó-arriba**
$AllowedSender UDP, 127.0.0.1, 192.168.1.0/24, 10.0.2.0/24
$AllowedSender TCP, 127.0.0.1, 192.168.1.0/24, 10.0.2.0/24

…

[root@centos2 ~]# systemctl restart rsyslog.service
[root@centos2 ~]# 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 Tue 2017-10-24 03:25:24 UTC; 2s ago
    Docs: man:rsyslogd(8)
          http://www.rsyslog.com/doc/
 Main PID: 15992 (rsyslogd)
  CGroup: /system.slice/rsyslog.service
          └─15992 /usr/sbin/rsyslogd -n

Oct 24 03:25:24 centos2.lpic.lan systemd[1]: Starting System Logging Service...
Oct 24 03:25:24 centos2.lpic.lan rsyslogd[15992]: [origin software="rsyslogd" swVersion="8.24.0" x-pid="15992" x-info="http://www.rsyslog.com"] start
Oct 24 03:25:24 centos2.lpic.lan systemd[1]: Started System Logging Service.

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

[root@centos1 ~]# vi /etc/rsyslog.conf
RULES
AÑADIMOS REGLAS
***.* @centos2.lpic.lan**

[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 Tue 2017-10-24 03:59:29 UTC; 1s ago
    Docs: man:rsyslogd(8)
          http://www.rsyslog.com/doc/
 Main PID: 14865 (rsyslogd)
  CGroup: /system.slice/rsyslog.service
          └─14865 /usr/sbin/rsyslogd -n

Oct 24 03:59:29 centos1.lpic.lan systemd[1]: Starting System Logging Service...

Oct 24 03:59:29 centos1.lpic.lan rsyslogd[14865]: [origin software="rsyslogd" swVersion="8.24.0" x-pid="14865" x-info="http://www.rsyslog.com"] start
Oct 24 03:59:29 centos1.lpic.lan systemd[1]: Started System Logging Service.

[root@centos1 ~]# logger PRUEBA DE LOGS PARA MariaDB

↘ Comprobamos desde -MariaDB- → 'centos2':

[root@centos2 ~]# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 15
Server version: 5.5.56-MariaDB MariaDB Server

Copyright (c) 2000, 2017, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> show databases;
```
+--------------------+
| Database           |
+--------------------+
| information_schema |
| Syslog             |
| mysql              |
| performance_schema |
| test               |
+--------------------+
```
5 rows in set (0.00 sec)

MariaDB [(none)]> use Syslog;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [Syslog]> show tables;
```
+-----------------------+
| Tables_in_Syslog      |
+-----------------------+
| SystemEvents          |
```

| **SystemEventsProperties** |
+----------------------+
2 rows in set (0.00 sec)

MariaDB [Syslog]> select * from SystemEvents;

…
| 1134 | NULL | 2017-10-24 04:01:10 | 2017-10-24 04:01:10 | 1 | 5 | centos1 | PRUEBA DE LOGS PARA MariaDB | NULL | NULL | NULL | NULL | NULL | NULL | NULL | NULL | 1 | vagrant: | NULL | NULL | NULL |
| 1135 | NULL | 2017-10-24 04:01:10 | 2017-10-24 04:01:10 | 1 | 5 | centos1 | PRUEBA DE LOGS PARA MariaDB | NULL | NULL | NULL | NULL | NULL | NULL | NULL | NULL | 1 | vagrant: | NULL | NULL | NULL |
+------+------------+---------------------+---------------------+----------+----------+----------
+---

-----------+-----------+-----------+------------+----------+--------------+---------
+----------------+-------------+----------+----------+----------+-----------
+-----------------------------------+-------------+----------------+----------+
1135 rows in set (0.00 sec)

MariaDB [Syslog]> describe SystemEvents;

+-------------------+-----------------+------+-----+---------+----------------+
| Field | Type | Null | Key | Default | Extra |
+-------------------+-----------------+------+-----+---------+----------------+
ID	int(10) unsigned	NO	PRI	NULL	auto_increment
CustomerID	bigint(20)	YES		NULL	
ReceivedAt	datetime	YES		NULL	
DeviceReportedTime	datetime	YES		NULL	
Facility	smallint(6)	YES		NULL	
Priority	smallint(6)	YES		NULL	
FromHost	varchar(60)	YES		NULL	
Message	text	YES		NULL	
NTSeverity	int(11)	YES		NULL	
Importance	int(11)	YES		NULL	
EventSource	varchar(60)	YES		NULL	
EventUser	varchar(60)	YES		NULL	

```
| EventCategory      | int(11)         | YES  |     | NULL    |               |
| EventID            | int(11)         | YES  |     | NULL    |               |
| EventBinaryData    | text            | YES  |     | NULL    |               |
| MaxAvailable       | int(11)         | YES  |     | NULL    |               |
| CurrUsage          | int(11)         | YES  |     | NULL    |               |
| MinUsage           | int(11)         | YES  |     | NULL    |               |
| MaxUsage           | int(11)         | YES  |     | NULL    |               |
| InfoUnitID         | int(11)         | YES  |     | NULL    |               |
| SysLogTag          | varchar(60)     | YES  |     | NULL    |               |
| EventLogType       | varchar(60)     | YES  |     | NULL    |               |
| GenericFileName    | varchar(60)     | YES  |     | NULL    |               |
| SystemID           | int(11)         | YES  |     | NULL    |               |
+--------------------+-----------------+------+-----+---------+---------------+
24 rows in set (0.00 sec)
```

MariaDB [Syslog]> select Id, CustomerID,ReceivedAt,Message from SystemEvents;

```
...
| 1134 |      NULL | 2017-10-24 04:01:10 |  PRUEBA DE LOGS PARA MariaDB
|
| 1135 |      NULL | 2017-10-24 04:01:10 |  PRUEBA DE LOGS PARA MariaDB
|
+------+-----------+---------------------
+-------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------
-----------+
1135 rows in set (0.00 sec)
```

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

[labs@hp rsyslog]$ vagrant snapshot save Rsyslog_MariaDB
==> centos1: Snapshotting the machine as 'Rsyslog_MariaDB'...
==> 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_MariaDB'...
==> 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
https://www.digitalocean.com/community/tutorials/how-to-install-mariadb-on-centos-7

===> LEGAL: