



27/11/2017

# Rsyslog et Script Backup Base de données Mysql

Version 1.0 : Version Initiale

Fabien MAUHOURLAT  
[NOM DE LA SOCIETE]

## Rsyslog et Script de backup de Base de données Mysql

### Contexte :

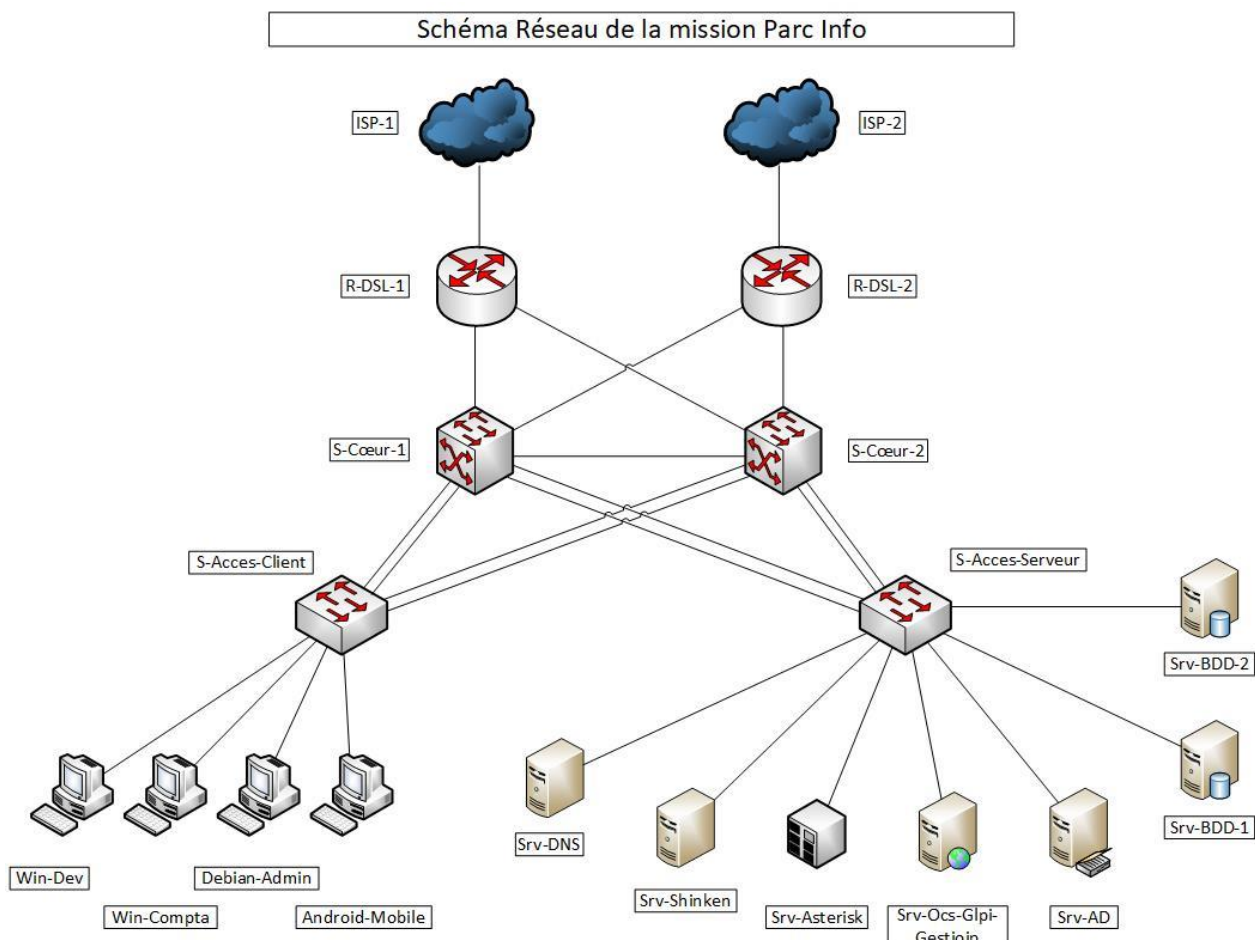
Pour permettre une haute disponibilité de l'infrastructure il est nécessaire de procéder à des sauvegardes des bases de données ainsi qu'à la centralisation des logs pour réaliser des traitements.

La sauvegarde des logs des serveurs linux utilise le logiciel rsyslog qui est déjà présent dans toutes les distributions par défaut.

Les équipements d'interconnexion sont également compatible syslog.

Pour effectuer la sauvegarde des bases de données de façon complète tous les jours sur une rotation par défaut de 1 semaine, la solution du scripting bash a été utilisée.

### Voici l'architecture mise en place :



# Sommaire

- I. Présentation et choix des solutions
- II. Prérequis
- III. Configuration préalable du serveur
- IV. Configuration du serveur Rsyslog
- V. Configuration des clients Rsyslog
  - a. Centraliser les logs de Mysql
  - b. Centraliser les logs du DNS
  - c. Centraliser les logs d'Asterisk
  - d. Centraliser les logs d'Apache
  - e. Capture de trame de l'envoi de logs
- VI. Configuration de Rsyslog sur les équipement csico
- VII. Mise en place de la rotation des logs avec logrotate
- VIII. Script de sauvegarde de bases de données Mysql
- IX. Script de restauration de bases de données Mysql
- X. Annexes

## I. Présentation et choix des solutions

Sous Linux quand on parle de gestion de logs, les facilites sont des catégories dans lesquelles les logs vont se "ranger" afin de mieux les archiver et les trier. Parmi ces facilites, on retrouve par exemple :

- **auth** : Utilisé pour des évènements concernant la sécurité ou l'authentification à travers des applications d'accès (type SSH)
- **authpriv** : Utilisé pour les messages relatifs au contrôle d'accès
- **daemon** : Utilisé par les différents processus systèmes et d'application
- **kern** : Utilisé pour les messages concernant le kernel
- **mail** : Utilisé pour les évènements des [services](#) mail
- **user** : Facilitie par défaut quand aucune n'est spécifiée
- **local7** : Utilisé pour les messages du boot
- **\*** : Désigne toutes les facilites, par soucis de simplicité c'est ce que nous avons spécifié lors de notre première règle de redirection des logs un peu plus haut
- **none** : Désigne aucune facilites

En plus de ces facilites, nous retrouvons pour chaque facilites un niveau de gravité (appelé Priorité) qui va du plus grave à la simple information :

- **Emerg** : Urgence, système inutilisable
- **Alert** : Alerte. Intervention immédiate nécessaire
- **Crit** : Erreur système critique
- **Err** : Erreur de fonctionnement
- **Warning** : Avertissement
- **Notice** : Évènement normaux devant être signalé
- **Info** : Pour information
- **Debug** : Message de debogage

## II. Configuration du serveur Rsyslog

### Configurer le serveur pour qu'il écoute sur le port 514 en UDP :

```
#####
#### MODULES ####
#####

module(load="imuxsock") # provides support for local system logging
module(load="imklog")   # provides kernel logging support
#module(load="immark")  # provides --MARK-- message capability

# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514")

# provides TCP syslog reception
#module(load="imtcp")
#input(type="imtcp" port="514")
```

### Après redémarrage du service rsyslog verifier qu'il écoute bien sur le port 514 :

- Netstat -ntpl | grep rsyslog

```
fabien@Rsyslog-srv:/var/log/Rsyslog-client$ sudo netstat -petulan | grep rsyslog
udp        0      0 0.0.0.0:514          0.0.0.0:*           0             73997       1541/rsyslogd
udp6       0      0 :::514              :::*                 0             73998       1541/rsyslogd
fabien@Rsyslog-srv:/var/log/Rsyslog-client$
```

### Configuration du serveur pour permettre d'avoir les logs des clients dans des dossiers par non d'hôte :

- \$template incoming-logs,"/var/log/%HOSTNAME%/syslog.log"

### Tous les logs provenant de la facilities local 3 sont redirigés vers le template :

- local3.\* ?incoming-logs
- & ~ (Permet pour la facilities local3 de ne pas utiliser les règles en dessous)

```
#####
#### RULES ####
#####

$template incoming-logs,"/var/log/%HOSTNAME%/syslog.log"
local3.* ?incoming-logs
& ~
```

On se retrouvera alors avec un dossier **"/var/log/clients/"** contenant un dossier par IP/nom client et contenant respectivement un fichier **"syslog.log"** avec les logs de chaque client respectif, ce qui simplifie la recherche d'information dans les logs d'un client précis.

**Dans l'exemple deux dossier ont été créer :**

- Rsyslog-client et rsyslog-srv qui sont les non d'hôte des clients

```
fabien@Rsyslog-srv:/var/log$ cd /var/log/
fabien@Rsyslog-srv:/var/log$ ls -al
total 5292
drwxr-xr-x  9 root      root    4096 nov.   4 21:59 .
drwxr-xr-x 13 root      root    4096 oct.  22 19:00 ..
-rw-r--r--  1 root      root  25404 nov.   4 13:25 alternatives.log
drwxr-xr-x  2 root      root    4096 nov.   4 13:28 apt
drwxr-xr-x  5 root      root    4096 nov.   4 13:57 asterisk
-rw-r----- 1 root      adm    63361 nov.   5 08:05 auth.log
-rw-----  1 root      utmp         0 oct.  22 17:28 btmp
-rw-r----- 1 root      adm   132138 nov.   5 07:52 daemon.log
drwxr-xr-x  2 root      root    4096 nov.   4 19:44 debian-template
-rw-r----- 1 root      adm   387622 nov.   4 21:57 debug
-rw-r--r--  1 root      root  345641 nov.   4 13:28 dpkg.log
drwxr-s---  2 Debian-exim adm     4096 oct.  22 19:52 exim4
-rw-r--r--  1 root      root   32032 oct.  22 19:48 faillog
drwxr-xr-x  3 root      root    4096 oct.  22 17:36 installer
-rw-r----- 1 root      adm   1186230 nov.   5 07:29 kern.log
-rw-rw-r--  1 root      utmp  292292 nov.   5 07:30 lastlog
-rw-r----- 1 root      adm   1313512 nov.   5 07:36 messages
drwxr-xr-x  2 root      root    4096 nov.   4 21:59 Rsyslog-client
drwxr-xr-x  2 root      root    4096 nov.   4 21:57 Rsyslog-srv
-rw-r----- 1 root      adm  1839748 nov.   5 07:58 syslog
-rw-r----- 1 root      adm     580 nov.   4 21:57 user.log
-rw-r--r--  1 root      root    3145 oct.  22 19:58 vmware-vmtoolsd.log
-rw-rw-r--  1 root      utmp   20352 nov.   5 07:30 wtmp
fabien@Rsyslog-srv:/var/log$
```

### III. Configuration des clients Rsyslog

#### **Il existe plusieurs façons d'identifier les logs pour les envoyer au serveur :**

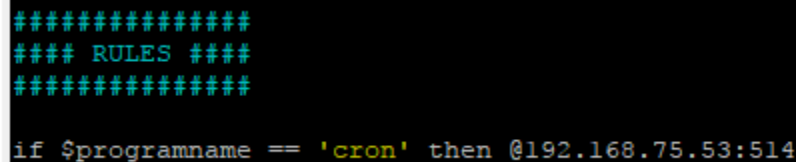
- Identification par programme avec des variables comme \$programme
- Identification des logs avec les facilities et les priorités
- Et traitement des logs par fichier

#### **1. Identification des logs avec les facilities et les priorités :**

```
cron.* @ IP_reomte_syslog_server:514
*. * @@IP_reomte_syslog_server:514
```

#### **2. Identification par programme avec des variables comme \$programme**

```
if $programname == 'cron' then @192.168.75.53:514
```



```
#####
#### RULES ####
#####

if $programname == 'cron' then @192.168.75.53:514
```

#### **3. Traitement des logs par fichier**

L'avantage du traitement par fichier est que l'on peut envoyer les logs d'une application en changeant la facilities ce qui permet une meilleur gestion de la centralisation :

```
$ModLoad imfile
```

```
$InputFileName /var/log/shinken/arbiterd.log
```

```
$InputFileTag shinken-info
```

```
$InputFileStateFile stat-shinken-info
```

```
$InputFileSeverity info
```

```
$InputFileFacility local3
```

```
$InputRunFileMonitor
```

```
local3.* @192.168.75.53:514
```

## a. Centraliser les logs de Mysql

Les fichiers de logs de mysql se trouve dans /var/log/mysql :

L'identification par fichier à été choisie et les logs du fichier erreur de mysql sont envoyer au serveur rsyslog avec la facilities local3:

```
# Custum
#

$ModLoad imfile
$InputFileName /var/log/mysql/error.log
$InputFileTag mysql-error
$InputFileStateFile stat-mysql-error
$InputFileSeverity info
$InputFileFacility local3
$InputRunFileMonitor
local3.* @192.168.10.240:514
```

Sur le serveur de log un dossier est crée avec le nom de la machine cliente et un fichier syslog est créer dans lequel tous les logs du client seront stockés :

➤ Tail -f /var/log/hostname/syslog.log

```
fabien@Srv-Shinken:/var/log$ cd Srv-BDD-1
fabien@Srv-Shinken:/var/log/Srv-BDD-1$ ls
syslog.log
fabien@Srv-Shinken:/var/log/Srv-BDD-1$ tail -f syslog.log
tail: impossible d'ouvrir 'syslog.log' en lecture: Permission non accordée
tail: aucun fichier restant
fabien@Srv-Shinken:/var/log/Srv-BDD-1$ sudo tail -f syslog.log
Nov  5 10:32:10 Srv-BDD-1 mysql-error Version: '10.1.26-MariaDB-0+deb9u1' socket:
Nov  5 10:32:10 Srv-BDD-1 mysql-error 2017-11-03 21:04:44 139728590698240 [Warning]
Nov  5 10:32:10 Srv-BDD-1 mysql-error 2017-11-04 7:42:13 140111472984640 [Note] Inn
In order to use backoff, increase buffer pool at least up to 20MB.
Nov  5 10:32:10 Srv-BDD-1 mysql-error 2017-11-04 7:42:13 140111472984640 [Note] Inn
Nov  5 10:32:10 Srv-BDD-1 mysql-error 2017-11-04 7:42:13 140111472984640 [Note] Inn
Nov  5 10:32:10 Srv-BDD-1 mysql-error 2017-11-04 7:42:13 140111472984640 [Note] Inn
Nov  5 10:32:10 Srv-BDD-1 mysql-error 2017-11-04 7:42:14 140110855104256 [Note] Inn
Nov  5 10:32:10 Srv-BDD-1 mysql-error 2017-11-05 10:28:32 140022949540416 [Note] Inn
Nov  5 10:32:10 Srv-BDD-1 mysql-error 2017-11-05 10:28:33 140022949540416 [ERROR] my
Nov  5 10:32:10 Srv-BDD-1 mysql-error 2017-11-05 10:29:39 140022948280064 [Warning]
```



## b. Centraliser les logs du DNS

BIND9 dispose d'une large variété de configurations possibles pour le logging. Il existe deux options principales, l'option Channel configure où vont les logs, et l'option Category détermine ce qui doit être loggé.

Dans un premier temps, nous devons configurer un channel pour spécifier dans quel fichier les messages seront enregistrés.

**Nous configurons ensuite une catégorie pour envoyer un certain type de logs du serveur BIND dans le fichier de logs spécifiques :**

- La categorie queries : Logs all query transactions.
- La categorie security : Approval and denial of requests.
- La categorie general : Anything that is not classified as any other item in this list defaults to this category.
- La categorie config : Configuration file parsing and processing.

```
logging {  
  
    channel "requetes" {  
        file "/var/log/bind/queries.log" size 10m;  
        print-time yes;  
        print-category yes;  
    };  
  
    category queries { "requetes"; };  
  
    channel "securite" {  
        file "/var/log/bind/securite.log" size 5m;  
        print-category yes;  
        print-severity yes;  
        print-time yes;  
    };  
  
    category security { "securite"; };  
  
    channel "global" {  
        file "/var/log/bind/global.log" size 5m;  
        print-category yes;  
        print-severity yes;  
        print-time yes;  
    };  
  
    category general { "global"; };  
  
    channel "configuration" {  
        file "/var/log/bind/config.log" size 5m;  
        print-category yes;  
        print-severity yes;  
        print-time yes;  
    };  
  
    category config { "configuration"; };  
};
```

Ensuite il faut inclure le fichier de configuration des logs dans la configuration de bind :

➤ Sudo vim /etc/bind/named.conf

```
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian.gz for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local

include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";
include "/etc/bind/log.conf";
```

Ensuite il faut redémarrer le service bind.

Cependant le service ne peut pas démarrer car les fichiers de log ne sont pas créés et ou les droit n'ont pas été attribué à l'utilisateur bind :

```
fabien@Srv-DNS:/etc/bind$ sudo systemctl restart bind9
fabien@Srv-DNS:/etc/bind$ sudo systemctl status bind9
● bind9.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/bind9.service; enabled; vendor preset: enabled)
   Active: failed (Result: exit-code) since Sun 2017-11-05 09:51:58 +11; 5s ago
     Docs: man:named(8)
  Process: 1092 ExecStop=/usr/sbin/rndc stop (code=exited, status=1/FAILURE)
  Process: 1085 ExecStart=/usr/sbin/named -f $OPTIONS (code=exited, status=1/FAILURE)
 Main PID: 1085 (code=exited, status=1/FAILURE)

nov. 05 09:51:58 Srv-DNS named[1085]: automatic empty zone: 95.100.IN-ADDR.ARPA
nov. 05 09:51:58 Srv-DNS named[1085]: automatic empty zone: 96.100.IN-ADDR.ARPA
nov. 05 09:51:58 Srv-DNS named[1085]: automatic empty zone: 97.100.IN-ADDR.ARPA
nov. 05 09:51:58 Srv-DNS named[1085]: automatic empty zone: 98.100.IN-ADDR.ARPA
nov. 05 09:51:58 Srv-DNS named[1085]: isc_stdio_open '/var/log/bind/queries.log' failed: file not found
nov. 05 09:51:58 Srv-DNS systemd[1]: bind9.service: Main process exited, code=exited, status=1/FAILURE
nov. 05 09:51:58 Srv-DNS rndc[1092]: rndc: connect failed: 127.0.0.1#953: connection refused
nov. 05 09:51:58 Srv-DNS systemd[1]: bind9.service: Control process exited, code=exited status=1
nov. 05 09:51:58 Srv-DNS systemd[1]: bind9.service: Unit entered failed state.
nov. 05 09:51:58 Srv-DNS systemd[1]: bind9.service: Failed with result 'exit-code'.
```

Il suffit pour cela de se rendre dans /var/log/bind puis de créer les fichiers de logs :

- Sudo mkdir bind
- Touch config.log && Touch global.log && Touch queries.log && Touch securite.log

```
fabien@Srv-DNS:/etc/bind$ cd /var/log/
fabien@Srv-DNS:/var/log$ ls
alternatives.log  auth.log  daemon.log  dpkg.log  faillog  kern.log  messages  syslog  vmware-vmtoolsd.log
apt  btmap  debug  exim4  installer  lastlog  ocsinventory-agent  user.log  wtmp
fabien@Srv-DNS:/var/log$ sudo mkdir bind
fabien@Srv-DNS:/var/log$ cd bind/
fabien@Srv-DNS:/var/log/bind$ sudo touch queries.log
fabien@Srv-DNS:/var/log/bind$ sudo touch securite.log
fabien@Srv-DNS:/var/log/bind$ sudo touch global.log
fabien@Srv-DNS:/var/log/bind$ sudo touch config.log
fabien@Srv-DNS:/var/log/bind$ ls -al
total 8
drwxr-xr-x 2 root root 4096 nov. 5 09:53 .
drwxr-xr-x 6 root root 4096 nov. 5 09:52 ..
-rw-r--r-- 1 root root 0 nov. 5 09:53 config.log
-rw-r--r-- 1 root root 0 nov. 5 09:53 global.log
-rw-r--r-- 1 root root 0 nov. 5 09:53 queries.log
-rw-r--r-- 1 root root 0 nov. 5 09:53 securite.log
fabien@Srv-DNS:/var/log/bind$
```

Ensuite il faut changer les droits des fichiers de logs :

Sudo chown bind :bind \*.log

```
fabien@Srv-DNS:/var/log/bind$ ls -al
total 8
drwxr-xr-x 2 root root 4096 nov. 5 09:53 .
drwxr-xr-x 6 root root 4096 nov. 5 09:52 ..
-rw-r--r-- 1 root root 0 nov. 5 09:53 config.log
-rw-r--r-- 1 root root 0 nov. 5 09:53 global.log
-rw-r--r-- 1 root root 0 nov. 5 09:53 queries.log
-rw-r--r-- 1 root root 0 nov. 5 09:53 securite.log
fabien@Srv-DNS:/var/log/bind$ sudo chown bind:bind *.log
fabien@Srv-DNS:/var/log/bind$ ls -al
total 8
drwxr-xr-x 2 root root 4096 nov. 5 09:53 .
drwxr-xr-x 6 root root 4096 nov. 5 09:52 ..
-rw-r--r-- 1 bind bind 0 nov. 5 09:53 config.log
-rw-r--r-- 1 bind bind 0 nov. 5 09:53 global.log
-rw-r--r-- 1 bind bind 0 nov. 5 09:53 queries.log
-rw-r--r-- 1 bind bind 0 nov. 5 09:53 securite.log
fabien@Srv-DNS:/var/log/bind$
```

Ensuite il faut configurer rsyslog pour chaque fichier de logs et les rediriger avec la facilities local3 vers le serveur rsyslog :

/var/log/bind/config.log

/var/log/bind/global.log

/var/log/bind/queries.log

/var/log/bind/securite.log

```
# Custum
#
$ModLoad imfile
$InputFileName /var/log/bind/config.log
$InputFileTag dns-config
$InputFileStateFile stat-dns-info
$InputFileSeverity info
$InputFileFacility local3
$InputRunFileMonitor
local3.* @192.168.10.240:514

$InputFileName /var/log/bind/global.log
$InputFileTag dns-global
$InputFileStateFile stat-dns-info
$InputFileSeverity info
$InputFileFacility local3
$InputRunFileMonitor
local3.* @192.168.10.240:514

$InputFileName /var/log/bind/queries.log
$InputFileTag dns-queries
$InputFileStateFile stat-dns-info
$InputFileSeverity info
$InputFileFacility local3
$InputRunFileMonitor
local3.* @192.168.10.240:514

$InputFileName /var/log/bind/securite.log
$InputFileTag dns-securite
$InputFileStateFile stat-dns-info
$InputFileSeverity info
$InputFileFacility local3
$InputRunFileMonitor
local3.* @192.168.10.240:514
```

Dans le fichier syslog du serveur on peut voir la tag des different type de logs du client DNS :

- Dans l'exemple ce sont les requêtes DNS

```
fabien@Srv-Shinken:/var/log$ cd Srv-DNS/
fabien@Srv-Shinken:/var/log/Srv-DNS$ ls
syslog.log
fabien@Srv-Shinken:/var/log/Srv-DNS$ sudo tail -f syslog.log
Nov  5 10:23:01 Srv-DNS dns-queries 05-Nov-2017 10:11:29.034 queries: client 192.168.10.230#49183
Nov  5 10:23:01 Srv-DNS dns-queries 05-Nov-2017 10:11:34.039 queries: client 192.168.10.230#49183
Nov  5 10:23:01 Srv-DNS dns-queries 05-Nov-2017 10:11:34.039 queries: client 192.168.10.230#49183
Nov  5 10:23:01 Srv-DNS dns-queries 05-Nov-2017 10:11:39.035 queries: client 192.168.10.230#48348
+ (192.168.10.230)
Nov  5 10:23:01 Srv-DNS dns-queries 05-Nov-2017 10:11:39.035 queries: client 192.168.10.230#48348
AA + (192.168.10.230)
Nov  5 10:23:01 Srv-DNS dns-queries 05-Nov-2017 10:10:04.028 queries: client 192.168.10.230#34590
Nov  5 10:23:01 Srv-DNS dns-queries 05-Nov-2017 10:11:39.035 queries: client 192.168.10.230#48348
+ (192.168.10.230)
Nov  5 10:23:01 Srv-DNS dns-queries 05-Nov-2017 10:14:34.064 queries: client 192.168.10.230#48950
Nov  5 10:23:01 Srv-DNS dns-queries 05-Nov-2017 10:12:54.049 queries: client 192.168.10.230#42007
Nov  5 10:23:01 Srv-DNS dns-queries 05-Nov-2017 10:13:29.050 queries: client 192.168.10.230#47401
^C
```

### c. Centraliser les logs d'Asterisk

Les fichiers de logs d'asterisk sont les suivant :

- /var/log/asterisk/cdr-csv/Master.csv (logs de SIP)
- /var/log/asterisk/messages

```
# Custum
#
$ModLoad imfile
$InputFileName /var/log/asterisk/cdr-csv/Master.csv
$InputFileTag asterisk-sip
$InputStateFile stat-asterisk-info
$InputFileSeverity info
$InputFileFacility local3
$InputRunFileMonitor
local3.* @192.168.10.240:514

$InputFileName /var/log/asterisk/messages
$InputFileTag asterisk-info
$InputStateFile stat-asterisk-info
$InputFileSeverity info
$InputFileFacility local3
$InputRunFileMonitor
local3.* @192.168.10.240:514
```

On peut voir les logs du serveur asterisk dans le fichier syslog de l'hôte :

```
fabien@Srv-Shinken:/var/log/Srv-DNS$ cd ../Srv-Asterisk/
fabien@Srv-Shinken:/var/log/Srv-Asterisk$ ls
syslog.log
fabien@Srv-Shinken:/var/log/Srv-Asterisk$ sudo tail -f syslog.log
Nov  5 09:40:50 Srv-Asterisk asterisk-info [Nov  5 09:40:49] WARNING[1226]
Nov  5 09:40:50 Srv-Asterisk asterisk-info [Nov  5 09:40:49] WARNING[1226]
Nov  5 09:40:50 Srv-Asterisk asterisk-info [Nov  5 09:40:49] WARNING[1226]
Nov  5 09:40:50 Srv-Asterisk asterisk-info [Nov  5 09:40:49] WARNING[1226]
Nov  5 09:40:50 Srv-Asterisk asterisk-info [Nov  5 09:40:49] WARNING[1226]
Nov  5 09:40:50 Srv-Asterisk asterisk-info [Nov  5 09:40:49] NOTICE[1226]
Nov  5 09:40:50 Srv-Asterisk asterisk-info [Nov  5 09:40:49] NOTICE[1226]
Nov  5 09:40:50 Srv-Asterisk asterisk-info [Nov  5 09:40:50] NOTICE[1226]
Nov  5 09:40:50 Srv-Asterisk asterisk-info [Nov  5 09:40:50] NOTICE[1226]
Nov  5 09:40:50 Srv-Asterisk asterisk-info [Nov  5 09:40:50] ERROR[1226] c
^C
fabien@Srv-Shinken:/var/log/Srv-Asterisk$
```

## d. Centraliser les logs d'Apache

Les fichiers de logs d'asterisk sont les suivant :

- /var/log/apache2/access.log
- /var/log/apache2/error.log

```
# Custum
#

$ModLoad imfile
$InputFileName /var/log/apache2/error.log
$InputFileTag apache-error
$InputFileStateFile stat-apache-error
$InputFileSeverity info
$InputFileFacility local3
$InputRunFileMonitor
local3.* @192.168.10.240:514

$ModLoad imfile
$InputFileName /var/log/apache2/access.log
$InputFileTag apache-access
$InputFileStateFile stat-apache-access
$InputFileSeverity info
$InputFileFacility local3
$InputRunFileMonitor
local3.* @192.168.10.240:514
```

On peut voir les logs du serveur apache dans le fichier syslog de l'hôte :

- Dans l'exemple ce sont les requêtes d'accès au page web

```
fabien@Srv-Shinken:/var/log$ cd Srv-Ocs-Glpi-Gestioip/
fabien@Srv-Shinken:/var/log/Srv-Ocs-Glpi-Gestioip$ ls
syslog.log
fabien@Srv-Shinken:/var/log/Srv-Ocs-Glpi-Gestioip$ sudo tail -f syslog.log
Nov  5 10:40:51 Srv-Ocs-Glpi-Gestioip apache-access 192.168.10.1 - - [04/Nov/2017:08:11:30 +1100] "G
 200 542 "https://192.168.10.1/glpi/lib/jquery/css/smoothness/jquery-ui-1.10.4.custom.min.css?v=9.2"
Nov  5 10:40:51 Srv-Ocs-Glpi-Gestioip apache-access 192.168.10.1 - - [04/Nov/2017:08:11:38 +1100] "G
t/computer.php" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"
Nov  5 10:40:51 Srv-Ocs-Glpi-Gestioip apache-access 192.168.10.1 - - [04/Nov/2017:08:24:10 +1100] "G
947 "https://192.168.10.1/ocsreports/" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Fire
Nov  5 10:40:51 Srv-Ocs-Glpi-Gestioip apache-access 192.168.10.1 - - [04/Nov/2017:08:24:10 +1100] "G
ports/" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"
Nov  5 10:40:51 Srv-Ocs-Glpi-Gestioip apache-access 192.168.10.1 - - [04/Nov/2017:08:25:06 +1100] "G
nt/user.php" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"
Nov  5 10:40:51 Srv-Ocs-Glpi-Gestioip apache-access 192.168.10.1 - - [04/Nov/2017:08:25:28 +1100] "G
tps://192.168.10.1/ocsreports/css/dataTables-custom.css" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0)
Nov  5 10:40:51 Srv-Ocs-Glpi-Gestioip apache-access 192.168.10.240 - - [04/Nov/2017:11:58:50 +1100]
Nov  5 10:40:51 Srv-Ocs-Glpi-Gestioip apache-access 192.168.10.240 - - [04/Nov/2017:12:24:29 +1100]
Nov  5 10:40:51 Srv-Ocs-Glpi-Gestioip apache-access 192.168.10.240 - - [04/Nov/2017:12:08:49 +1100]
Nov  5 10:40:51 Srv-Ocs-Glpi-Gestioip apache-access 192.168.10.240 - - [05/Nov/2017:10:32:40 +1100]
^C
```



## e. Capture de trame de l'envoi de logs

The screenshot displays a Wireshark capture of network traffic. The top pane shows a list of captured packets, all of which are Syslog messages. The middle pane shows the details of the selected packet (No. 171), which is a Syslog message from 192.168.75.51 to 192.168.75.53. The details pane shows the structure of the Syslog message, including the header, message, and trailer. The bottom pane shows the raw data of the packet in hexadecimal and ASCII.

Packet 171: Syslog message from 192.168.75.51 to 192.168.75.53. The message content is: "Facility: LOCAL3 - reserved for local use (19) ... ..lib = level: INFO - informational (8) Message: Nov 4 22:17:12 Rsyslog-client shinken-info [1509794232] INFO: [Shinken] OK, all schedulers configurations are dispatched :)"

## IV. Configuration de Rsyslog sur les équipement csico

logging trap notifications

logging facility local3

logging source-interface Vlan30

logging host 192.168.10.240

```
S_Coeur_1>en
S_Coeur_1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S_Coeur_1(config)#loggi
S_Coeur_1(config)#logging 192.168.10.240
S_Coeur_1(config)#log
*Nov  4 23:43:59.095: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.10.2
40 port 514 started - CLI initiated
S_Coeur_1(config)#logging trap notifications
S_Coeur_1(config)#logging source-interface vlan 30
S_Coeur_1(config)#archive
S_Coeur_1(config-archive)#log config
S_Coeur_1(config-archive-log-cfg)#logging size 1000
S_Coeur_1(config-archive-log-cfg)#hidekeys
S_Coeur_1(config-archive-log-cfg)#notify syslog
S_Coeur_1(config-archive-log-cfg)#exit
S_Coeur_1(config-archive)#exit
S_Coeur_1(config)#
```

```
logging trap notifications
logging facility local3
logging source-interface Vlan30
logging host 192.168.10.240
```

```
*Nov  5 00:05:39.467: %SYS-5-CONFIG_I: Configured from console by consoleCompressed configuration from 6580 bytes to 3022 bytes[OK]
S_Coeur_1#
*Nov  5 00:05:43.429: %SSH-5-SSH2_USERAUTH: User 'admin' authentication for SSH2 Session from 192.168.10.235 (tty = 0) using crypto cipher 'aes256-ctr', hmac 'hmac-shal' Failed
*Nov  5 00:05:43.429: %SSH-5-SSH2_CLOSE: SSH2 Session from 192.168.10.235 (tty = 0) for user 'admin' using crypto cipher 'aes256-ctr', hmac 'hmac-shal' closed
*Nov  5 00:05:43.481: %GRUB-5-CONFIG_WRITING: GRUB configuration is being updated on disk. Please wait...
*Nov  5 00:05:44.189: %GRUB-5-CONFIG_WRITTEN: GRUB configuration was written to disk successfully.
S_Coeur_1#
*Nov  5 00:05:51.756: %SSH-5-SSH2_SESSION: SSH2 Session request from 192.168.10.235 (tty = 0) using crypto cipher 'aes256-ctr', hmac 'hmac-shal' Succeeded
S_Coeur_1#
*Nov  5 00:05:55.904: %SSH-5-SSH2_USERAUTH: User 'admin' authentication for SSH2 Session from 192.168.10.235 (tty = 0) using crypto cipher 'aes256-ctr', hmac 'hmac-shal' Succeeded
S_Coeur_1#
```



```
fabien@Srv-Shinken:/var/log$ cd 192.168.30.254/
fabien@Srv-Shinken:/var/log/192.168.30.254$ ls
syslog.log
fabien@Srv-Shinken:/var/log/192.168.30.254$ tail -f syslog.log
tail: impossible d'ouvrir 'syslog.log' en lecture: Permission non accordée
tail: aucun fichier restant
fabien@Srv-Shinken:/var/log/192.168.30.254$ sudo tail -f syslog.log
Nov  5 10:55:15 192.168.30.254 69: *Nov  4 23:55:20.377: %SYS-5-CONFIG_I: Configured from console by console
Nov  5 10:57:42 192.168.30.254 70: *Nov  4 23:57:44.697: %SYS-5-CONFIG_I: Configured from console by console
Nov  5 11:00:10 192.168.30.254 71: *Nov  5 00:00:10.664: %SSH-5-ENABLED: SSH 1.9
9 has been enabled
Nov  5 11:01:13 192.168.30.254 72: *Nov  5 00:01:13.001: %SYS-5-CONFIG_I: Config
ured from console by console
Nov  5 11:01:17 192.168.30.254 73: *Nov  5 00:01:16.865: %GRUB-5-CONFIG_WRITING:
GRUB configuration is being updated on disk. Please wait...
Nov  5 11:01:17 192.168.30.254 74: *Nov  5 00:01:17.588: %GRUB-5-CONFIG_WRITTEN:
GRUB configuration was written to disk successfully.
Nov  5 11:02:02 192.168.30.254 75: *Nov  5 00:02:01.090: %SSH-5-SSH2_SESSION: SSH2 Session request from 192.168.10.235 (tty = 0)
ceded
Nov  5 11:02:32 192.168.30.254 76: *Nov  5 00:02:31.113: %SSH-5-SSH2_USERAUTH: User 'admin' authentication for SSH2 Session from
tr', hmac 'hmac-sha1' Failed
Nov  5 11:02:32 192.168.30.254 77: *Nov  5 00:02:31.114: %SSH-5-SSH2_CLOSE: SSH2 Session from 192.168.10.235 (tty = 0) for user '
al' closed
```

## V. Mise en place de la rotation des logs avec logrotate

### Logrotate

```
/var/log/dpkg.log {  
    monthly  
    rotate 12  
    compress  
    delaycompress  
    missingok  
    notifempty  
    create 640 root adm  
postrotate  
systemctl reload rsyslog > /dev/null  
endscript  
}
```

pour dpkg, Logrotate surveille le fichier /var/log/dpkg.log et génère une rotation une fois par mois - c'est l' "intervalle de rotation".

'rotate 12' signifie qu'à chaque intervalle, on conserve 12 mois de journalisation.

Les fichiers de logs peuvent être compressés au format gzip en spécifiant 'compress' et, 'delaycompress' retarde le processus de compression jusqu'à la prochaine rotation. 'delaycompress' ne fonctionnera que si l'option 'compress' est clairement spécifiée.

'missingok' permet au processus de ne pas s'arrêter à chaque erreur et de poursuivre avec le fichier de log suivant.

'notifempty' empêche la rotation de s'effectuer si le fichier de log est vide.

'create <mode> <owner> <group>' crée un fichier vide avec les propriétés spécifiées, après la rotation des logs.

```
# system-specific logs may be configured here
#
#
/var/log/Srv-DNS/syslog.log
/var/log/Srv-BDD-1/syslog.log
/var/log/Srv-BDD-2/syslog.log
/var/log/Srv-Ocs-Glpi-Gestioip/syslog.log
/var/log/Srv-Asterisk/syslog.log
/var/log/192.168.30.254/syslog.log
{
    daily
    rotate 12
    compress
    delaycompress
    missingok
    notifempty
    create 640 root adm
    postrotate
    systemctl reload rsyslog > /dev/null
    endscript
}
```

```
/var/log/bind/*.log {
weekly
missingok
rotate 10
compress
delaycompress
create 775 root bind
postrotate
/etc/init.d/bind9 reload > /dev/null
endscript
}
```

## VI. Script de sauvegarde de bases de données Mysql

```

MariaDB [(none)]> CREATE USER "backup"@'%';
Query OK, 0 rows affected (0.00 sec)

MariaDB [(none)]> GRANT ALL ON *.* TO "backup"@'%' identified by 'toor';
Query OK, 0 rows affected (0.00 sec)

MariaDB [(none)]> select user from mysql.user;
+-----+
| user |
+-----+
| backup |
| gestioip |
| glpi |
| ocs |
| slave |
| shinken |
| root |
+-----+
7 rows in set (0.00 sec)

MariaDB [(none)]>

```

```

[client]
user = backup
password = toor
host = 192.168.10.10
port = 3306
~

```

```

DB_config_file="./config_mysql.cnf"
MYSQL_Backup_folder="/var/log/mysql-backup"
Database=("ocsweb" "glpi" "gestioip")
Rotation=7
ssh_host=192.168.10.10
ssh_port=47000
ssh_public_key=/home/fabien/.ssh/id_rsa
ssh_user=fabien
ssh_path_tmp=/tmp
~

```

```

fabien@Srv-Ocs-Glpi-Gestioip:~/Script-Fabien/Mysql-Backup$ ./mysql-backup.sh

*****
***** Script qui Sauvegarde la base de données OCS GLPI et Gestioip *****
*****

***** Check de la configuration *****

* Le check de configuration n a pas trouve d erreurs!

***** La configuration est la suivante : *****

Le fichier de configuration du script : ./config_mysql_backup.conf
Le serveur Backup : Srv-Ocs-Glpi-Gestioip
Le chemin du dossier de backup : /var/log/mysql-backup
Le fichier de configuration mysql : ./config_mysql.cnf
* user = backup
* host = 192.168.10.10
* port = 3306

***** Sauvegarde des bases de données *****

Creation du dossier /var/log/mysql-backup/backup-17-11-09 : [OK]

Protection des tables en ecriture activer : [OK]

***** Recap Export *****
Export de la base ocsweb : [OK]
Taille de la base : 1,1M

***** Recap Export *****
Export de la base glpi : [OK]
Taille de la base : 956K

***** Recap Export *****
Export de la base gestioip : [OK]
Taille de la base : 56K

Protection des tables en ecriture desactiver : [OK]

Base de donnes sauvegarder [OK]

***** Rotation des Logs *****

Rotation des logs [OK]

***** Script termine avec succes ! *****

fabien@Srv-Ocs-Glpi-Gestioip:~/Script-Fabien/Mysql-Backup$

```

```

La sauvegarde des base de donnes a commencer le jeudi 9 novembre 2017, 19:44:28 (UTC+1100)
La sauvegarde des base de donnes a commencer le jeudi 9 novembre 2017, 19:44:49 (UTC+1100)
La sauvegarde des base de donnes a commencer le jeudi 9 novembre 2017, 19:50:29 (UTC+1100)
La sauvegarde des bases ----- ocsweb glpi gestioip ---- s est terminee avec succes !
mysql-backup.log (END)

```

```
fabien@Srv-Ocs-Glpi-Gestioip:~/Script-Fabien/Mysql-Backup$ ls -alR /var/log/mysql-backup/
/var/log/mysql-backup/:
total 12
drwxr-xr-x  3 fabien fabien 4096 nov.  9 19:50 .
drwxr-xr-x 10 root   root   4096 nov.  9 19:45 ..
drwxr-xr-x  2 fabien fabien 4096 nov.  9 19:50 backup-17-11-09

/var/log/mysql-backup/backup-17-11-09:
total 2072
drwxr-xr-x  2 fabien fabien    4096 nov.  9 19:50 .
drwxr-xr-x  3 fabien fabien    4096 nov.  9 19:50 ..
-rw-r--r--  1 fabien fabien  53427 nov.  9 19:50 gestioip.sql
-rw-r--r--  1 fabien fabien 974929 nov.  9 19:50 glpi.sql
-rw-r--r--  1 fabien fabien 1074661 nov.  9 19:50 ocsweb.sql
fabien@Srv-Ocs-Glpi-Gestioip:~/Script-Fabien/Mysql-Backup$
```

```
0 18 * * 1-5 /usr/share/gestioip/bin/ip_update_gestioip_dns.pl >/dev/null 2>&1
0 */1 * * 1-5 /usr/share/gestioip/Script-Gestioip/gestioip_users_check_fin_func.sh >/dev/null 2>&1
0 18 * * * /home/fabien/Script-Fabien/Mysql-Backup/mysql-backup.sh >/dev/null 2>&1
```

## Annexes

<https://www.it-connect.fr/centralisez-vos-logs-avec-rsyslog/>

<https://www.howtoforge.com/tutorial/rsyslog-centralized-log-server-in-debian-9/>

[https://www.ssi.gouv.fr/uploads/2016/07/nt\\_commutateurs.pdf](https://www.ssi.gouv.fr/uploads/2016/07/nt_commutateurs.pdf)

<https://doc.ubuntu-fr.org/logrotate>

<https://support.rackspace.com/how-to/understanding-logrotate-utility/>

<http://www.robertain.com/post/2011/12/12/activer-les-logs-dans-bind/>

<http://www.zytrax.com/books/dns/ch7/logging.html>