N-Partner

N-REPORTER

How to manage MySQL Audit syslog

v1.1.4

(01-01-01-007) 2014/12/04

Preface

This manual describes how to use N-Reporter to receive MySQL Audit syslog. We first introduce how to enable MySQL general log function and write general log into syslog. Then use Linux software Syslogd, Rsyslog, or Syslog-ng to send syslog to N-Reporter. To avoid general log using too much space of HDD, we advise you use Linux Logrotate to maintain general log. Therefore, the last chapter we introduce how to maintain general log by using Logrotate。

N-Reporter is a product of N-Partner, it is the main Syslog analyzer in the industry. It can analyze, received Syslog, and produce many kinds of professional reports.
In this manual we use Debian 6 with MySQL 5.5 as the environment.

Contents

1 How to enable MySQL general log function

MySQL setup steps：

(1) Login MySQL with root or the user has a proper permission.

(2) Edit MySQL profile /etc/mysql/my.cnf

```
vi /etc/mysql/my.cnf
```

(3) Enable general log function and set up the output path of general log. Under [mysqld], add the following two red lines。

```
[mysqld]
general_log
general_log_file = /usr/local/mysql/data/general.log
```

Note: MySQL can provide general log. And it can write client's record about connect and disconnection into general log.

(4) Restart MySQL。

```
/etc/init.d/mysql.server restart
```

2 How to write MySQL general log into syslog

(1) Login MySQL with root or the user has a proper permission.

(2) Send general log to syslog。

```
tail -f /usr/local/mysql/data/general.log | /usr/bin/logger -p local1.info -t mysql &
```

Note: facility can be set up between local0~local7, here we use local1.

3 How to Set up Linux Syslogd, Rsyslog, or Syslog-ng to forward to syslog

Note: Please choose the suitable software for Linux or some other kind of Linux to forward syslog.

(1) Syslogd setup steps：

a. Login MySQL with root or the user has a proper permission.

b. Edit Syslogd profile.

```
vi /etc/syslog.conf
```

c. Add the following line in the end of profile.

```
local1.info @192.168.2.2:514
```

Note: The facility must be the same as logger. You might need to change N-Reporter IP to a real one IP.

d. Restart Syslogd。

```
/etc/init.d/syslog restart
/etc/init.d/syslog reload
```

(2) Rsyslog setup steps：

a. Login MySQL with root or the user has a proper permission.

b. Edit Rsyslog profile.

```
vi /etc/rsyslog.conf
```

c. Add the following two lines in the end of profile.

```
$EscapeControlCharactersOnReceive off
local1.info @192.168.2.2:514
```

Note: The facility must be the same as logger. You might need to change N-Reporter IP to a real one IP.

d. Restart Rsyslog。

```
/etc/init.d/rsyslog restart
```

(3) Syslog-ng setup steps：

a. Login MySQL with root or the user has a proper permission.

b. Edit Syslog-ng profile.

```
vi /etc/syslog-ng/syslog-ng.conf
```

c. Add the following lines in the end of profile.

```
source s_local { unix-dgram("/dev/log"); internal(); file("/proc/kmsg" rogram_override("kernel")); };
filter f_local1 { facility(local1); };
destination d_network { udp("192.168.2.2" port(514) ); };
log { source(s_local); filter(f_local1); destination(d_network); };
```

Note1: The facility must be the same as logger. You might need to change N-Reporter IP to a real one IP.

Note2: In the setting of Syslog-ng, there are some sources receive message, and destinations forward message, and rule filters. If the name of s_local, f_local1, and d_network conflict with the default or existing name of sources, filters, or destinations, please change to another name.

d. Restart Syslog-ng。

```
/etc/init.d/syslog-ng restart
```

When restarting Syslogd、Rsyslog or Syslog-ng, MySQL clients login and logout SQL server, or user login fail, all these action log will be send to N-Reporter and it can get the user IP information. we can track and execute audit planning completely through N-Reporter.

4 How to maintain general log by using Logrotate

(1) Login MySQL with root or the user has a proper permission.

(2) Add mysql profile under /etc/logrotae.d.

```
vi /etc/logrotate.d/mysql
```

(3) Edit mysql。

```
#general log path{}
/usr/local/mysql/data/general.log {
#if empty,don't rotate.
        notifempty
#when log grows bigger than 10M, rotate it.
        size 10M
#rotate every day.
        daily
#count times of rotated log.
        rotate 3
        missingok
        compress
# The setting of logrotate can be changed by your own needs.

        prerotate
        kill -9 $(ps aux|grep '/usr/bin/logger -p local1.info -t mysql'|grep -v 'grep'|awk '{print $2}')
        kill -9 $(ps aux|grep 'tail -f /usr/local/mysql/data/general.log'|grep -v 'grep'|awk '{print $2}')
        sleep 2
        endscript

        postrotate
#just if mysqld is really running
# Be aware the true path of mysqladmin。
        if test -x /usr/local/mysql/bin/mysqladmin && \
# mysqladmin –u user    –p user password, here we use user: root, password: password.
            /usr/local/mysql/bin/mysqladmin -uroot -ppassword ping &>/dev/null
        then
# (The) Manager root must have Reload_priv permission.
            /usr/local/mysql/bin/mysqladmin -uroot -ppassword flush-logs
        fi
        tail -f /usr/local/mysql/data/general.log | /usr/bin/logger -p local1.info -t mysql &
        sleep 5
# Restart rsyslog. Restart syslog, rsyslog, or syslog-ng according to the situation.
        /etc/init.d/rsyslog restart
        endscript
}
```

Note: flush logs will delete all the MySQL logs, including error log, general log, update log, binary log, and slow query log. And in this case there is only rotate general log. If you need to keep other logs, you can rename them before flush logs, or maintain them with logrotate at the same time.

(4) After finish editing, please test the command below. Check if the general log rotate normally, or wait for the next day. And keep sending syslog to N-Reporter。

```
logrotate -f /etc/logrotate.conf
```

Technical Support：

Email: support@npartnertech.com

Skype：support@npartnertech.com

Sales Information：

Email: sales@npartnertech.com

N-Partner