N-Partner

N-REPORTER

如何管理 MySQL 审核

V 1.1.4 (简体)

(01-01-02-007) 2014/12/04

前言

本文件描述如何使用 N-Reporter 接收 MySQL Audit syslog。先介绍如何开启 MySQL general log 功能，并将 general log 写入系统日志 syslog 中，然后利用 Linux 的 software Syslogd、Rsyslog、或 Syslog-ng 将 syslog 发送至 N-Reporter。为了避免 general log 写满硬盘空间，建议使用 Linux 的 software Logrotate 维护 general log。所以最后一节介绍如何使用 Logrotate 维护 general log。

N-Reporter 为 N-Partner 所有。为目前业界主要的 Syslog 分析仪。能够统计分析接收的 Syslog，产生各式各样的专业报表。

此文件为 Debian 6 环境安装 MySQL 5.5 版本的实际范例。

文件章节如下：

连络信息

N-Partner 公司连络方式：

TEL: +886-4-23752865

FAX: +886-4-23757458

有关技术问题请洽：

Email: support@npartnertech.com

有关业务相关问题请洽：

Email: sales@npartnertech.com

1 如何开启 MySQL 的 general log 功能

MySQL 设定步骤如下：

(1) 登入 MySQL 主机。请注意用户权限问题或者使用 root 登入。

(2) 编辑 MySQL 配置文件/etc/mysql/my.cnf

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

(3) 开启 general log 功能并设定 general log 输出的档案。

在[mysqld]下面新增红色两行字。

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

注：MySQL 提供 general log，其功能为写入 client 端的连线与断线记录。

(4) 重新启动 MySQL。

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

2 如何将 MySQL 的 general log 写入系统日志 syslog 中

(1) 登入 MySQL 主机。请注意用户权限问题或者使用 root 登入。

(2) 将 general log 送至系统日志 syslog。

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

注：facility 可设定范围为 local0~local7，本例选择 local1。

3 如何设定 Linux Syslogd、Rsyslog、或 Syslog-ng 转发 syslog

Linux 或类 Linux 系统请选择适合的 software 实现 syslog 转发。

(1) Syslogd 设定的步骤如下：

a. 登入 MySQL 主机。请注意用户权限问题或者使用 root 登入。

b. 编辑 Syslogd 配置文件。

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

c. 配置文件最后面新增下列一行。

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

注：facility 必须与 logger 时的 facility 一致。192.168.2.2 改成 N-Reporter IP。

d. 重新启动 Syslogd。

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

(2) Rsyslog 设定的步骤如下：

a. 登入 MySQL 主机。请注意用户权限问题或者使用 root 登入。

b. 编辑 Rsyslog 配置文件。

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

c. 配置文件最后面新增下列两行。

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

注：facility 必须与 logger 时的 facility 一致。192.168.2.2 改成 N-Reporter IP。

d. 重新启动 Rsyslog。

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

(3) Syslog-ng 设定的步骤如下：

a. 登入 MySQL 主机。请注意用户权限问题或者使用 root 登入。

b. 编辑 Syslog-ng 配置文件。

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

c. 配置文件最后面新增下列数行。

```
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); };
```

注 1：facility 必须与 logger 时的 facility 一致。192.168.2.2 改成 N-Reporter IP。

注 2：Syslog-ng 设定中有数个接收 message 的 sources、转发 message 的 destinations、与过滤规则 filters。若是 s_local、f_local1、d_network 与预设或已设定的 sources、filters、destinations 的名称冲突，请改成其他名称。

d. 重新启动 Syslog-ng。

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

Syslogd、Rsyslog 或 Syslog-ng 重启后，MySQL client 端使用者登入、注销 SQL Server，或是使用者登入失败，其讯息将送至 N-Reporter，并且可进一步抓取使用者 IP。如此，透过 N-Reporter 即可完整的追踪使用者和执行稽核的计划。

4 如何使用 Logrotate 维护 general log

(1) 登入 MySQL 主机。请注意用户权限问题或者使用 root 登入。

(2) 在/etc/logrotae.d 底下新增 mysql 配置文件。

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

(3) 编辑 mysql。

```
#general log 路径 {}
/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
#请依照个人需求设定 logrotate 参数。

        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
#请注意 mysqladmin 实际上的路径。
        if test -x /usr/local/mysql/bin/mysqladmin && \
#mysqladmin -u 管理者   -p 管理者密码，本例管理者为 root，密码 password。
           /usr/local/mysql/bin/mysqladmin -uroot -ppassword ping &>/dev/null
        then
#管理者 root 必须要有 Reload_priv 权限。
           /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
#重新启动 rsyslog。请依照实际情形启动 syslog、rsyslog or syslog-ng。
        /etc/init.d/rsyslog restart
        endscript
}
```

注 :flush logs 会将 MySQL 所有 logs 删除 ,包含 error log、general log、update log、binary log、slow query log ,而本例只有 rotate general log。如果需求保留其他 log ,请在 flush logs 前 ,rename 它们，或者同时利用 logrotate 维护它们。

(4) 编辑完毕，请测试下列指令，检查 gerenal log 是否正常 rotate，或是等待隔日检查是否正常 rotate，并且持续送出 syslog 到 N-Reporter。

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

采购与销售合作：sales@npartnertech.com
技术咨询：support@npartnertech.com