N-Partner

N-REPORTER

如何管理 MySQL 稽核

V 005 (繁體)

2017/09/15

前言

本文件描述如何使用 N-Reporter 接收 MySQL Audit syslog。先介紹如何開啟 MySQL general log 功能，並將 general log 寫入系統日誌 syslog 中，然後利用 Linux 的 software Syslogd、Rsyslog、或 Syslog-ng 將 syslog 發送至 N-Reporter。為了避免 general log 寫滿硬碟空間，建議使用 Linux 的 software Logrotate 維護 general log。所以最後一節介紹如何使用 Logrotate 維護 general log。

N-Reporter 為 N-Partner 所有。為目前業界主要的 Syslog 分析儀。能夠統計分析接收的 Syslog，產生各式各樣的專業報表。

此文件為 Debian 6 環境安裝 MySQL 5.5 版本的實際範例。

文件章節如下：

1 如何開啟 MySQL 的 general log 功能

MySQL 設定步驟如下：

(1) 登入 MySQL 主機。請注意使用者權限問題或者使用 root 登入。

(2) 編輯 MySQL 設定檔/etc/mysql/my.cnf

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

(3) 開啟 general log 功能並設定 general log 輸出的檔案。

在[mysqld]下面新增紅色兩行字。

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

註：MySQL 提供 general log，其功能為寫入 client 端的連線與斷線記錄。

(4) 重新啟動 MySQL。

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

2 如何將 MySQL 的 general log 寫入系統日誌 syslog 中

(1) 登入 MySQL 主機。請注意使用者權限問題或者使用 root 登入。

(2) 將 general log 送至系統日誌 syslog。

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

註：facility 可設定範圍為 local0~local7，本例選擇 local1。

3 如何設定 Linux Syslogd、Rsyslog、或 Syslog-ng 轉發 syslog

Linux 或類 Linux 系統請選擇適合的 software 實現 syslog 轉發。

(1) Syslogd 設定的步驟如下：

a. 登入 MySQL 主機。請注意使用者權限問題或者使用 root 登入。

b. 編輯 Syslogd 設定檔。

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

c. 設定檔最後面新增下列一行。

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

註：facility 必須與 logger 時的 facility 一致。192.168.2.2 改成 N-Reporter IP。

d. 重新啟動 Syslogd。

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

(2) Rsyslog 設定的步驟如下：

a. 登入 MySQL 主機。請注意使用者權限問題或者使用 root 登入。

b. 編輯 Rsyslog 設定檔。

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

c. 設定檔最後面新增下列兩行。

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

註：facility 必須與 logger 時的 facility 一致。192.168.2.2 改成 N-Reporter IP。

d. 重新啟動 Rsyslog。

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

(3) Syslog-ng 設定的步驟如下：

a. 登入 MySQL 主機。請注意使用者權限問題或者使用 root 登入。

b. 編輯 Syslog-ng 設定檔。

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

c. 設定檔最後面新增下列數行。

```
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); };
```

註 1：facility 必須與 logger 時的 facility 一致。192.168.2.2 改成 N-Reporter IP。

註 2：Syslog-ng 設定中有數個接收 message 的 sources、轉發 message 的 destinations、與過濾規則 filters。若是 s_local、f_local1、d_network 與預設或已設定的 sources、filters、destinations 的名稱衝突，請改成其他名稱。

d. 重新啟動 Syslog-ng。

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

Syslogd、Rsyslog 或 Syslog-ng 重啟後，MySQL client 端使用者登入、登出 SQL Server，或是使用者登入失敗，其訊息將送至 N-Reporter，並且可進一步抓取使用者 IP。如此，透過 N-Reporter 即可完整的追踪使用者和執行稽核的計畫。

4 如何使用 Logrotate 維護 general log

(1) 登入 MySQL 主機。請注意使用者權限問題或者使用 root 登入。

(2) 在/etc/logrotae.d 底下新增 mysql 設定檔。

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

(3) 編輯 mysql。

```
#general log 路徑 {}
/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
#請依照個人需求設定 logrotate 參數。

        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
#請注意 mysqladmin 實際上的路徑。
        if test -x /usr/local/mysql/bin/mysqladmin && \
#mysqladmin -u 管理者   -p 管理者密碼，本例管理者為 root，密碼 password。
           /usr/local/mysql/bin/mysqladmin -uroot -ppassword ping &>/dev/null
        then
#管理者 root 必須要有 Reload_priv 權限。
           /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
#重新啟動 rsyslog。請依照實際情形啟動 syslog、rsyslog or syslog-ng。
        /etc/init.d/rsyslog restart
        endscript
}
```

註：flush logs 會將 MySQL 所有 logs 刪除，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，請在 flush logs 前，rename 它們，或者同時利用 logrotate 維護它們。

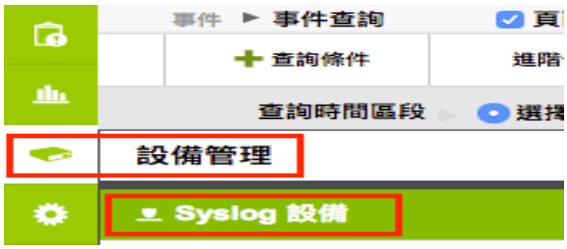
(4) 編輯完畢，請測試下列指令，檢查 gerenal log 是否正常 rotate，或是等待隔日檢查是否正常 rotate，並且持續送出 syslog 到 N-Reporter。

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

5 將設備加入系統及 Syslog 資料格式及 Facility 的設定

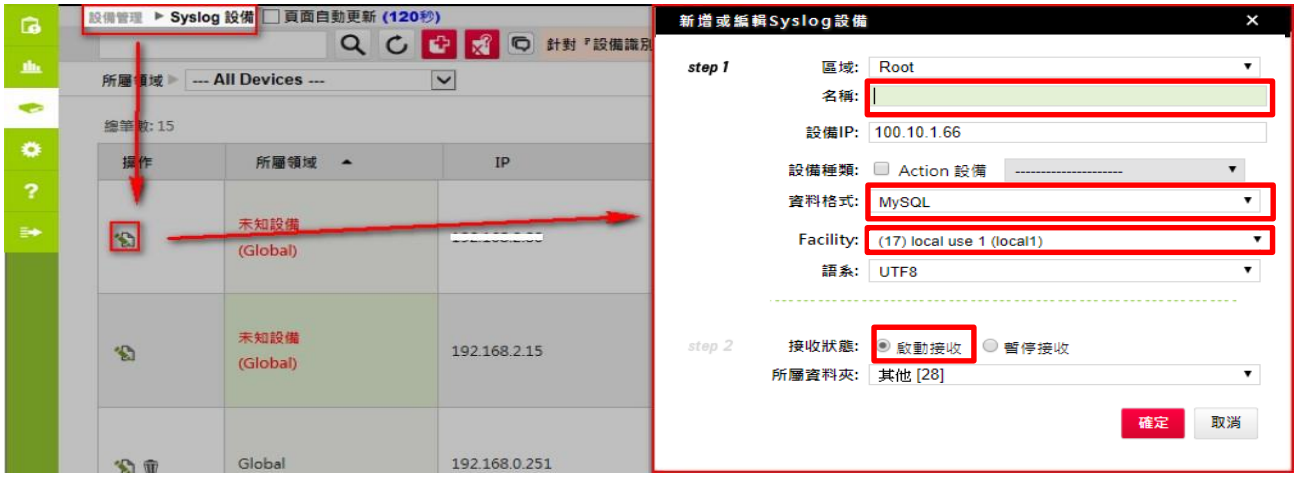
(1) 登入 N-Reporter / N-Cloud 系統

(2) 滑鼠點選[設備管理 / Syslog 設備]



(3) 滑鼠點選 [未知設備的編輯圖示]，在 IP 欄位中應該能看見此台的設備的 IP。請輸入一個方便記憶的設備名稱，接著在[資料格式]下拉選單中依設備的類型選擇[**MySQL**]，在[Facility] 下拉選單中選**[(17)]**，勾選[**啟動接收**]，按下[**確定**] ，即完成設備的系統新增程序

註：依上述章節 2 的設定值內容，本例選擇 Facility[(17) local use 1 (local1)]



連絡資訊

N-Partner 公司連絡方式：

TEL: +886-4-23752865

FAX: +886-4-23757458

有關技術問題請洽：

Email: support@npartnertech.com

Skype：support@npartnertech.com

有關業務相關問題請洽：

Email: sales@npartnertech.com

N-Partner