LabSheet 06:

การติดตั้งโปรแกรม Syslog-ng บนเซิร์ฟเวอร์ที่มีระบบปฏิบัติการ Linux

Date: 8 August 2008

Program name: syslog-ng

Description: Send system log files and Apache web log files to Centralized Log Server (logger.ku.ac.th)

Step:

1. Download : http://ftp.ku.ac.th/pub/syslog-ng/linux/CentOS/CentOS5/i386/eventlog-0.2.5-1.el5.i386.rpm
   http://ftp.ku.ac.th/pub/syslog-ng/linux/CentOS/CentOS5/i386/eventlog-devel-0.2.5-1.el5.i386.rpm
   http://ftp.ku.ac.th/pub/syslog-ng/linux/CentOS/CentOS5/i386/syslog-ng-2.0.4-1.el5.i386.rpm

```
# cd  /tmp
# wget  http://ftp.ku.ac.th/pub/syslog-ng/linux/CentOS/CentOS5/i386/eventlog-0.2.5-1.el5.i386.rpm
# wget  http://ftp.ku.ac.th/pub/syslog-ng/linux/CentOS/CentOS5/i386/eventlog-devel-0.2.5-1.el5.i386.rpm
# wget  http://ftp.ku.ac.th/pub/syslog-ng/linux/CentOS/CentOS5/i386/syslog-ng-2.0.4-1.el5.i386.rpm
```

2. ติดตั้งโปรแกรม

```
# rpm –ivh  eventlog-0.2.5-1.el5.i386.rpm   eventlog-devel-0.2.5-1.el5.i386.rpm  syslog-ng-2.0.4-1.el5.i386.rpm
```

3. กำหนดและแก้ไขค่าคอนฟิก /etc/syslog-ng.conf หรือ /etc/syslog-ng/syslog-ng.conf

```
#  nano –w /etc/syslog-ng.conf
```

ค่าคอนฟิก ดังตัวอย่าง

```
# syslog-ng configuration file.
#
# This should behave pretty much like the original syslog on RedHat. But
# it could be configured a lot smarter.
#
# See syslog-ng(8) and syslog-ng.conf(5) for more information.
#


# General settings
options {
```

```
        sync (0);
        time_reopen (10);
        log_fifo_size (1000);
        long_hostnames (off);
        use_dns (yes);
        use_fqdn (yes);
        create_dirs (no);
        keep_hostname (yes);
};

# Log Source
source s_sys {
        unix-stream ("/dev/log");
        pipe ("/proc/kmsg");
        internal();
};

# Log to specified file on localhost
destination d_mesg { file("/var/log/messages"); };
destination d_auth { file("/var/log/secure"); };
destination d_mail { file("/var/log/maillog" sync(10)); };
destination d_boot { file("/var/log/boot.log"); };
destination d_cron { file("/var/log/cron"); };
destination d_kern { file("/var/log/kern"); };
destination d_emergency { usertty("*"); };
destination d_vsftpd { file("/var/log/vsftpd.log"); };

# Log over Stunnel to Centralized log server
destination remote {tcp("127.0.0.1" port(514));};

# filters
filter f_kernel     { facility(kern); };
filter f_default    { level(info..emerg) and
                      not (facility(mail)
```

```
                or facility(authpriv)
                or facility(cron)); };
filter f_auth       { facility(authpriv); };
filter f_mail       { facility(mail); };
filter f_emergency  { level(emerg); };
filter f_boot       { facility(local7); };
filter f_cron       { facility(cron); };
filter f_vsftpd     { program(vsftpd) or program(ftp); };

# Store log on localhost
log { source(s_sys); filter(f_kernel); destination(d_kern); };
log { source(s_sys); filter(f_default); destination(d_mesg); };
log { source(s_sys); filter(f_auth); destination(d_auth); };
log { source(s_sys); filter(f_mail); destination(d_mail); };
log { source(s_sys); filter(f_emergency); destination(d_emergency); };
log { source(s_sys); filter(f_boot); destination(d_boot); };
log { source(s_sys); filter(f_cron); destination(d_cron); };
log { source(s_sys); filter(f_vsftpd); destination(d_vsftpd); };

# Connect and Store your system log sources to the remote server
log { source(s_sys); filter(f_kernel); destination(remote); };
log { source(s_sys); filter(f_default); destination(remote); };
log { source(s_sys); filter(f_auth); destination(remote); };
log { source(s_sys); filter(f_mail); destination(remote); };
log { source(s_sys); filter(f_emergency); destination(remote); };
log { source(s_sys); filter(f_boot); destination(remote); };
log { source(s_sys); filter(f_cron); destination(remote); };
log { source(s_sys); filter(f_vsftpd); destination(remote); };

# apache log
filter f_apache { program("apache") and level(info); };
destination d_apache { file("/var/log/httpd/access_log"); };
log {
   source(s_sys);
```

```
   filter(f_apache);
   destination(d_apache);
   destination(remote);
};

filter f_apache_err { program("apache") and level(err); };
destination d_apache_err { file("/var/log/httpd/error_log"); };
log {
   source(s_sys);
   filter(f_apache_err);
   destination(d_apache_err);
   destination(remote);
};
```

หรือดาวน์โหลดไฟล์คอนฟิกได้จาก http://ftp.ku.ac.th/pub/syslog-ng/linux/syslog-ng.conf

```
# cd  /etc
# wget  http://ftp.ku.ac.th/pub/syslog-ng/linux/syslog-ng.conf
```

4. แก้ไขค่าคอนฟิกของ Apache web server (/etc/httpd/conf/httpd.conf)

```
#   nano -w   /etc/httpd/conf/httpd.conf
       LogFormat "%v %h %l %u %t \"%r\" %>s %b \"%{Referer}i\"" privacy_format


       ErrorLog "| logger -t apache -p daemon.err"
       CustomLog "| logger -t apache -p daemon.info" privacy_format
```

และสั่งให้โพรแซส httpd เริ่มการทำงานใหม่

```
#  service  httpd  restart
```

5. แก้ไขค่าคอนฟิกของ FTP server (/etc/vsftpd/vsftpd.conf)

```
#   nano -w    /etc/vsftpd/vsftpd.conf
       syslog_enable=YES
       xferlog_enable=YES
       xferlog_file=/var/log/vsftpd.log
```

และสั่งให้โพรแซส httpd เริ่มการทำงานใหม่

```
# service vsftpd restart
```

6. เพิ่มค่าคอนฟิกของ Stunnel เพื่อใช้ในการเข้ารหัสข้อมูลก่อนส่งไปยัง Centralized Log Server

```
# nano -w /etc/stunnel/stunnel.conf
    # Stunnel of syslog-ng-client configuration
    client = yes
    debug = debug
    output = /etc/stunnel/stunnel.log
    [syslog-ng]
        accept = 127.0.0.1:514
        connect = 158.108.5.154:61514
```

หรือดาวน์โหลดไฟล์คอนฟิกได้จาก http://ftp.ku.ac.th/pub/syslog-ng/linux/stunnel.conf

```
# cd /etc/stunnel
# wget http://ftp.ku.ac.th/pub/syslog-ng/linux/stunnel.conf
```

สร้างไฟล์เก็บล๊อกการทำงานของโปรแกรม Stunnel

```
# cd /etc/stunnel
# touch /etc/stunnel/stunnel.log
```

เริ่มการทำงานของโปรแกรม Stunnel

```
# stunnel /etc/stunnel/stunnel.conf
```

และกำหนดให้เซิร์ฟเวอร์เริ่มการทำงานทุกครั้งบูทเครื่องขึ้นมาใหม่

```
# nano -w /etc/rc.local
    stunnel /etc/stunnel/stunnel.conf
```

7. สั่งให้ syslog-ng เริ่มทำงาน

```
# service syslog-ng start
```

คำสั่งหยุดการทำงานของโปรแกรม syslog-ng

```
# service syslog-ng stop
```

คำสั่งหยุดและเริ่มการทำงานของโปรแกรม syslog-ng ใหม่

```
# service syslog-ng  restart
```

และกำหนดให้โปรแกรม syslog-ng เริ่มการทำงานใหม่ทุกครั้งที่บูทเครื่อง

```
# chkconfig  --level 2345  syslog-ng on
```

8. ตรวจสอบโพรแซสของ syslog-ng ด้วยคำสั่ง

```
# ps –aux | grep syslog
```

9. ทดสอบการส่งล๊อกไฟล์

```
#  logger "Send log from local server"
```