LabSheet 09:

การติดตั้งโปรแกรม Syslog-ng บนเซิร์ฟเวอร์ที่มีระบบปฏิบัติการ FreeBSD-based 6.2 Release

Date: 25 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. ติดตั้งโปรแกรมผ่าน Ports Collection ในกรณีที่ยังไม่ได้ติดตั้งโปรแกรม Ports Collection มีขั้นตอนดังนี้

```
# sysinstall
# ที่หน้าจอ Sysinstall Main Memu เลือก Configure --> Distributions --> Ports
การติดตั้งโปแกรม Ports Collection จำเป็นต้องมีแผ่น Installation CD แผ่นที่ 1
```

2. ติดตั้งโปรแกรม syslog-ng

```
-- ติดตั้ง --
#  cd /usr/ports/sysutils/syslog-ng
#   make & make install

-- แก้ไขไฟล์ /etc/rc.conf เพื่อกำหนดให้เรียกใช้ syslog-ng แทน syslogd โดยเพิ่มข้อมูลดังนี้ --
# vi /etc/rc.conf
syslogd_enable="NO"
syslog_ng_enable="YES"
-- Stop Process syslogd --
# kill `cat /var/run/syslog.pid`

-- ปรับแต่งค่า syslog-ng --
# cp /usr/local/etc/syslog-ng/syslog-ng.conf.sample /usr/local/etc/syslog-ng/syslog-ng.conf
# cd /usr/local/etc/syslog-ng
# vi syslog-ng.conf
```

```
#
# This sample configuration file is essentially equilivent to the stock
# FreeBSD /etc/syslog.conf file.
#
```

```
#
# options
#
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);
};

#
# sources
#
source src { unix-dgram("/var/run/log");
             unix-dgram("/var/run/logpriv" perm(0600));
             udp(); internal(); file("/dev/klog"); };

#
# destinations
#
destination messages { file("/var/log/messages"); };
destination security { file("/var/log/security"); };
destination authlog { file("/var/log/auth.log"); };
destination maillog { file("/var/log/maillog"); };
destination lpd-errs { file("/var/log/lpd-errs"); };
destination xferlog { file("/var/log/xferlog"); };
destination cron { file("/var/log/cron"); };
destination debuglog { file("/var/log/debug.log"); };
```

```
destination consolelog { file("/var/log/console.log"); };
destination all { file("/var/log/all.log"); };
destination newscrit { file("/var/log/news/news.crit"); };
destination newserr { file("/var/log/news/news.err"); };
destination newsnotice { file("/var/log/news/news.notice"); };
destination slip { file("/var/log/slip.log"); };
destination ppp { file("/var/log/ppp.log"); };
destination console { file("/dev/console"); };
destination allusers { usertty("*"); };
#destination loghost { udp("loghost" port(514)); };
destination remote { tcp("127.0.0.1" port(514)); };

#
# log facility filters
#
filter f_auth { facility(auth); };
filter f_authpriv { facility(authpriv); };
filter f_not_authpriv { not facility(authpriv); };
filter f_console { facility(console); };
filter f_cron { facility(cron); };
filter f_daemon { facility(daemon); };
filter f_ftp { facility(ftp); };
filter f_kern { facility(kern); };
filter f_lpr { facility(lpr); };
filter f_mail { facility(mail); };
filter f_news { facility(news); };
filter f_security { facility(security); };
filter f_user { facility(user); };
filter f_uucp { facility(uucp); };
filter f_local0 { facility(local0); };
filter f_local1 { facility(local1); };
filter f_local2 { facility(local2); };
filter f_local3 { facility(local3); };
```

```
filter f_local4 { facility(local4); };
filter f_local5 { facility(local5); };
filter f_local6 { facility(local6); };
filter f_local7 { facility(local7); };

#
# log level filters
#
filter f_emerg { level(emerg); };
filter f_alert { level(alert..emerg); };
filter f_crit { level(crit..emerg); };
filter f_err { level(err..emerg); };
filter f_warning { level(warning..emerg); };
filter f_notice { level(notice..emerg); };
filter f_info { level(info..emerg); };
filter f_debug { level(debug..emerg); };
filter f_is_debug { level(debug); };

#
# program filters
#
filter f_ppp { program("ppp"); };
filter f_slip { program("startslip"); };

#
# *.err;kern.warning;auth.notice;mail.crit              /dev/console
#
log { source(src); filter(f_err); destination(console); };
log { source(src); filter(f_kern); filter(f_warning); destination(console); };
log { source(src); filter(f_auth); filter(f_notice); destination(console); };
log { source(src); filter(f_mail); filter(f_crit); destination(console); };

#
```

```
# *.notice;authpriv.none;kern.debug;lpr.info;mail.crit;news.err /var/log/messages
#
log { source(src); filter(f_notice); filter(f_not_authpriv); destination(messages); };
log { source(src); filter(f_kern); filter(f_debug); destination(messages); };
log { source(src); filter(f_lpr); filter(f_info); destination(messages); };
log { source(src); filter(f_mail); filter(f_crit); destination(messages); };
log { source(src); filter(f_news); filter(f_err); destination(messages); };

#
# security.*                                    /var/log/security
#
log { source(src); filter(f_security); destination(security); };

#
# auth.info;authpriv.info                       /var/log/auth.log
log { source(src); filter(f_auth); filter(f_info); destination(authlog); };
log { source(src); filter(f_authpriv); filter(f_info); destination(authlog); };

#
# mail.info                                     /var/log/maillog
#
log { source(src); filter(f_mail); filter(f_info); destination(maillog); };

#
# lpr.info                                      /var/log/lpd-errs
#
log { source(src); filter(f_lpr); filter(f_info); destination(lpd-errs); };

#
# ftp.info                                      /var/log/xferlog
#
log { source(src); filter(f_ftp); filter(f_info); destination(xferlog); };
```

```
#
# cron.*                                  /var/log/cron
#
log { source(src); filter(f_cron); destination(cron); };


#
# *.=debug                                /var/log/debug.log
#
log { source(src); filter(f_is_debug); destination(debuglog); };


#
# *.emerg                                 *
#
log { source(src); filter(f_emerg); destination(allusers); };


#
# uncomment this to log all writes to /dev/console to /var/log/console.log
# console.info                            /var/log/console.log
#
#log { source(src); filter(f_console); filter(f_info); destination(consolelog); };


#
# uncomment this to enable logging of all log messages to /var/log/all.log
# touch /var/log/all.log and chmod it to mode 600 before it will work
# *.*                                     /var/log/all.log
#
#log { source(src); destination(all); };


#
# uncomment this to enable logging to a remote loghost named loghost
# *.*                                     @loghost
#
#log { source(src); destination(loghost); };
```

```
#
# uncomment these if you're running inn
# news.crit                             /var/log/news/news.crit
# news.err                              /var/log/news/news.err
# news.notice                             /var/log/news/news.notice
#
#log { source(src); filter(f_news); filter(f_crit); destination(newscrit); };
#log { source(src); filter(f_news); filter(f_err); destination(newserr); };
#log { source(src); filter(f_news); filter(f_notice); destination(newsnotice); };

#
# !startslip
# *.*                                   /var/log/slip.log
#
log { source(src); filter(f_slip); destination(slip); };

#
# !ppp
# *.*                                   /var/log/ppp.log
#
log { source(src); filter(f_ppp); destination(ppp); };

#
# Remote
log { source(src); filter(f_ftp); filter(f_info); destination(remote); };
log { source(src); filter(f_notice); filter(f_not_authpriv); destination(remote); };
log { source(src); filter(f_mail); filter(f_info); destination(remote); };
```

-- Start / Stop --

```
# /usr/local/etc/rc.d/syslog-ng stop
# /usr/local/etc/rc.d/syslog-ng start
```

3. ติดตั้งโปรแกรม Stunnel

-- ตรวจสอบโปรแกรม Stunnel --

```
# cd /usr/ports/
# make search key=stunnel
```

```
Port:   stunnel-4.18_1
Path:   /usr/ports/security/stunnel
```

-- ติดตั้งโปรแกรม --

```
# cd /usr/ports/security/stunnel
# make install
```

-- ปรับแต่งค่า --

```
# cd /usr/local/etc/stunnel/
# cp stunnel.conf-sample stunnel.conf
# vi stunnel.conf
```

```
# Stunnel of syslog-ng-client configuration
pid =  /var/run/stunnel.pid
debug = debug
output = /var/log/stunnel.log
client = yes

[syslog-ng]
accept  = 127.0.0.1:514
connect = 158.108.5.154:61514
```

```
# touch /var/run/stunnel.pid
# touch /var/log/stunnel.log
```

-- แก้ไขไฟล์ /etc/rc.conf เพื่อกำหนดให้เรียกใช้ Stunnel ทุกครั้งที่ Boot เครื่อง --

```
# vi /etc/rc.conf
```

```
stunnel_enable="YES"
```

-- แก้ไขไฟล์ Start / Stop Service Stunnel --

cd /usr/local/etc/rc.d/

vi stunnel.sh

```
#!/bin/sh
#
# A sample stunnel startup script written by martti.kuparinen@ericsson.com
#
# $FreeBSD: ports/security/stunnel/files/stunnel.sh,v 1.2 2002/09/20 09:29:11 roam Exp $
#

# Where is the program
STUNNEL="/usr/local/sbin/stunnel"

case "$1" in
   start)
      ${STUNNEL} /usr/local/etc/stunnel/stunnel.conf
      ;;

   stop)
      killall `basename ${STUNNEL}`
      ;;

   *)
      echo ""
      echo "Usage: basename $0 { start | stop }"
      echo ""
      ;;
esac
```

/usr/local/etc/rc.d/stunnel.sh start

-- ตรวจสอบ Service --

```
# ps -ax |grep stunnel
  671  ??  Is     0:00.16 /usr/local/sbin/stunnel /usr/local/etc/stunnel/stunnel.conf
```