LabSheet 08:

การติดตั้งโปรแกรม Syslog-ng บนเซิร์ฟเวอร์ที่มีระบบปฏิบัติการ Sun Solaris-based 10 SPARC/x86_84

Date: 21 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. ดาวน์โหลดโปรแกรมจาก http://ftp.ku.ac.th/syslog-ng/solaris/
   - eventlog-0.2.7-sol10-x86-local.gz
   - glib-2.14.1-sol10-x86-local.gz
   - libgcc-3.4.6-sol10-x86-local.gz
   - libiconv-1.11-sol10-x86-local.gz
   - syslogng-2.0.9-sol10-x86-local.gz

2. ปิดการใช้งาน syslog และ shell SMF services

```
# svcadm disable svc:/system/system-log:default    หรือ      # svcadm disable system-log
# svcadm disable svc:/network/shell:default
```

3. เพิ่มพอร์ตให้บริการของ syslog-ng

```
#  vi  /etc/services
     syslog-ng      514/tcp                  # syslog-ng
```

4. ติดตั้งโปรแกรม

```
# gunzip *.gz
# pkgadd -d eventlog-0.2.7-sol10-sparc-local
# pkgadd -d libgcc-3.4.6-sol10-sparc-local
# pkgadd -d glib-2.14.1-sol10-sparc-local
# pkgadd -d libol-0.3.18-sol10-sparc-local
# pkgadd -d libiconv-1.11-sol10-sparc-local
# pkgadd -d syslogng-2.0.9-sol10-sparc-local
```

5. สร้างไฟล์ start/stop services ของโปรแกรม syslog-ng

```
# cp /usr/local/doc/syslogng/contrib/init.d.solaris  /etc/init.d/syslog-ng
# chmod 744 /etc/init.d/syslog-ng
# chown root:sys /etc/init.d/syslog-ng
# cd /etc/rc2.d/
# ln -s ../init.d/syslog-ng S98syslog-ng
```

6. แก้ไขไฟล์ /etc/logadm.conf

```
# cp /etc/logadm.conf /etc/logadm.conf.orig
# vi /etc/logadm.conf
    ----------
    แก้ไขจาก
     -HUP `cat /var/run/syslog.pid`'
    เป็น
    -HUP `cat /etc/syslog-ng/syslog-ng.pid`'
   ----------
```

7. สร้างไฟล์คอนฟิกและแก้ไขค่าคอนฟิก ดังตัวอย่าง

```
# mkdir -p /etc/syslog-ng
# vi /etc/syslog-ng/syslog-ng.conf
      ########################################################################
      # $Id: solaris-conf.txt,v 1.6 2003/03/13 02:28:36 nate Exp $
      #
      # This is for syslog-ng 1.5.x The only things I think you'd have to cut
      # out to use this on 1.4.x are log_msg_size() and bad_hostname().
      ########################################################################

      options {
            long_hostnames(off);

            # doesn't actually help on Solaris, log(3) truncates at 1024 chars
            log_msg_size(8192);
```

```
        # buffer just a little for performance
        sync(1);

        # memory is cheap, buffer messages unable to write (like to loghost)
        log_fifo_size(2048);

        # I hate Vignette StoryServer
        bad_hostname("^(ctld.|cmd|tmd|last)$");

        # The time to wait before a dead connection is reestablished (seconds)
        time_reopen(10);

        use_fqdn (yes);
        use_dns (no);
        create_dirs (no);
        keep_hostname (yes);
};
########################################################################
# The source stream, use sun-stream on solaris, and don't forget #
# the door at /etc/.syslog_door                                  #
########################################################################
source src {
        sun-stream("/dev/log" door("/etc/.syslog_door"));
        internal();
};
########################################################################
# Destination logfile setups (include your net setups here)   #
########################################################################
destination syslog {
        file("/var/log/syslog");
};
destination messages {
        file("/var/adm/messages");
};
```

```
destination loginlog {
        file("/var/adm/loginlog");
};
destination remote {
        tcp("127.0.0.1" port(514));
};
########################################################################
# Filters for mimicking Solaris syslogd                 #
########################################################################
filter f_syslog {
        facility(mail) or (facility(daemon) and priority(notice));
};
filter f_messages {
        priority(err)
        or facility(kern)
        or (facility(user) and priority(err))
        or (facility(daemon) and priority(notice))
        or (facility(mail) and priority(crit));
};
filter f_auth {
        facility (auth);
};
########################################################################
# Tie it all together                                   #
########################################################################
log {
        source(src);
        filter(f_syslog);
        destination(syslog);
};
log {
        source(src);
        filter(f_messages);
        destination(messages);
```

```
};
log {
        source(src);
        filter(f_auth);
        destination(loginlog);
};
log {
        source(src);
        #filter(f_syslog);
        #filter(f_messages);
        #filter(f_auth);
        destination(remote);
};
#####################################################################
```

เริ่มการทำงานของโปรแกรม syslog-ng

```
# /etc/init.d/syslog-ng  start
```

8. แก้ไขค่าคอนฟิกของโปรแกรม FTP

```
# vi /etc/ftpd/ftpaccess
    # เอาเครื่อง # หน้า log ออก
    log        commands       real,guest,anonymous
    log        security       real,guest,anonymous
    log        transfers      real,guest,anonymous    inbound,outbound
    xferlog     format  %T %Xt %R %Xn %XP %Xy %Xf %Xd %Xm %U ftp %Xa %u %Xc %Xs %Xr
```

เริ่มการทำงานของโปรแกรม FTP ใหม่

```
# svcadm -v restart ftp
```

9. ติดตั้งโปรแกรม Stunnel เพื่อใช้ในการเข้ารหัสข้อมูลก่อนส่งไปยัง Centralized Log Server (ดาวน์โหลดได้จาก http://www.stunnel.org และไฟล์ที่ได้มาจะอยู่ในรูปของ Tar ball – Source code installation เช่น stunnel-4.05.tar.gz)

```
# /usr/sbin/groupadd -g 122 stunnel
# /usr/sbin/useradd -c stunnel -d /nonexistent -m -g 122 -u 122 stunnel

# wget http://www.stunnel.org/download/stunnel/src/stunnel-4.05.tar.gz
# gunzip stunnel-4.05.tar.gz
# tar xvf  stunnel-4.05.tar
# cd stunnel-4.05

# ./configure --localstatedir=/var/run/stunnel \
 --with-pem-dir=/usr/local/etc/openssl/certs --datadir=/usr/local
# make
```

*Country Name (2 letter code) [PL]:**TH***

*State or Province Name (full name) [Some-State]:**Bangkok***

*Locality Name (eg, city) []:**Chatujak***

*Organization Name (eg, company) [Stunnel Developers Ltd]:**Kasetsart University***

*Organizational Unit Name (eg, section) []:**Office of Computer Services***

*Common Name (FQDN of your server) [localhost]:**pirun.ku.ac.th***

```
# make install
```

เพิ่มค่าคอนฟิกของ Stunnel

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

สร้างไฟล์เก็บล๊อกการทำงานของโปรแกรม Stunnel

```
# cd   /usr/local/etc/stunnel
```

```
# touch  stunnel.log
```

สร้างไดเร็กทอรี่เก็บหมายเลข process id ของโปรแกรม stunnel

```
# mkdir –p  /var/run/stunnel/run
```

และสร้างไฟล์ script ให้เริ่มการทำงานของโปรแกรม Stunnel อัตโนมัติเมื่อบูทเครื่องใหม่

```
# cd   /etc/init.d
# vi   stunnel
```

```
#!/bin/sh
# Startup script for stunnel
RETVAL=0

start() {
        # Start daemons.
        echo "Starting stunnel:"
        if [ ! -f /var/run/stunnel/run ]; then
          mkdir -p  /var/run/stunnel/run
        fi

        /usr/local/sbin/stunnel /usr/local/etc/stunnel/stunnel.conf
        echo
        return $RETVAL
}

stop() {
        # Stop daemons.
        echo "Shutting down stunnel:"
        /usr/bin/pkill -x -u 0 stunnel
        echo
        return $RETVAL
}

case "$1" in
```

```
        start)
            start
            ;;
        stop)
            stop
            ;;
        *)
            echo "$0 {start|stop}"
            exit 1
    esac
    exit 0
```

```
# chown root:sys stunnel
# chmod 755 stunnel
# cd /etc/rc2.d/
# ln -s ../init.d/stunnel  S99stunnel
```

-เริ่มการทำงานของโปรแกรม Stunnel

```
# /etc/init.d/stunnel start
```

-ตรวจดูการทำงานของโปรแกรม Stunnel

```
# ps -ef |grep stunnel
  root  5878    1   0 15:27:40 ?   0:00 /usr/local/sbin/stunnel /usr/local/etc/stunnel/stunnel.conf
```

10. ทดสอบการส่งล๊อกไฟล์

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