Centralized System Logging With A Database

Manitoba UNIX User Group

Kevin McGregor

February 13, 2007

The Situation

- Multiple hosts and devices are logging stuff
- Log files are scattered
- Reports and analyses are being requested

Requirements And Constraints

- I’d prefer free software (gratis/libre)
- Open standards
- Must work with available equipment

My Solution

- Send information from all syslog devices to a syslog server, which stores the logs in a database for future reporting
- Servers run Ubuntu Server 6.06.1 LTS
- PostgreSQL 8.1
- Syslog-ng

What Is syslog?

- Three things, really:
  - A method of general system logging on UNIX via system calls
  - A log format
  - A network log transmission mechanism with three roles:
    - syslog device
      - A source of syslog messages
    - syslog relay
      - Relays some or all messages to a syslog server
    - syslog server
      - Final destination of syslog messages
  - Note: Many ways to structure the three roles

Why syslog-ng?

- Use TCP along with UDP
- Filtering based on message content
- Support for encryption, tunneling, firewalls
- Can run in chroot environment

Which Databases Can We Use?

- Using this method, any database with a Linux client:
  - MySQL
  - PostgreSQL
  - SQL Server
  - Sybase ASE
  - Oracle
  - DB2
  - Others

Set Up A Test Machine

- For Windows XP, get and install Kiwi SyslogGen for testing, pgAdmin for general database management (both free)
- For this demo, add to c:\windows\system32\drivers\etc\hosts:

```
192.168.182.128   loghost
192.168.182.129   db
```

Loghost Configuration (1 of 3)

- Install syslog-ng, postgresql-client-8.1, openssh-server, openntp
- Check logs (/var/log/{daemon.log,syslog})
- Create pipe (“`mkfifo /var/run/pgsql.pipe`” or “`mknod /var/run/pgsql.pipe p`”)
- `chmod 700 /var/run/pgsql.pipe`

Loghost Configuration (2 of 3)

- Add to /etc/syslog-ng/syslog-ng.conf:

```
source s_net {
     udp();
};
destination dp_pgsql {
   pipe(
     “/var/run/pgsql.pipe”
     template(“INSERT INTO logs
       (rcvd,sent,fac,lev,pri,tag,host,sourceip,program,msg)
       VALUES( ‘$R_ISODATE’, ’$S_ISODATE’, ’$FACILITY’,
       ’$LEVEL’, ’$PRI’, ’$TAG’, ’$HOST’, ’$SOURCEIP’,
       ’$PROGRAM’, ’$MSGONLY’ );\n”)
     template_escape(yes)
   );
};
log {
     source(s_net);
     destination(dp_pgsql);
};
```

Loghost Configuration (3 of 3)

- Signal syslog-ng to re-read syslog-ng.conf
  - `kill –HUP <syslog-ng_processid>`
- Check pipe contents:
  - `cat </var/run/pgsql.pipe`
- Send a test log message to loghost with SyslogGen

Database Host Configuration (1 of 2)

Install the necessary software

```
apt-get install postgresql-8.1 openssh-server openntp
```

Configure PostgreSQL:

Add to /etc/postgresql/8.1/main/pg_hba.conf:

```
host syslogdemo sysloguser 192.168.182.0/24 trust
host all postgres 192.168.182.0/24 trust
```

Change in /etc/postgresql/8.1/main/postgresql.conf:

```
listen addresses = ‘*’
```

Database Host Configuration (2 of 2)

Set up the database, user, table and permissions:

```
su postgres
createdb syslogdemo
psql -d syslogdemo
create role sysloguser login;
CREATE TABLE logs (
     rcvd timestamp with time zone,
     sent timestamp with time zone,
     fac character varying(10),
     lev character varying(10),
     pri integer,
     tag character(2),
     host character varying(32),
     sourceip inet,
     program text,
     msg text,
     entry serial NOT NULL,
     PRIMARY KEY (entry)  ) ;
ALTER TABLE logs OWNER TO postgres;
GRANT ALL ON TABLE logs TO postgres;
GRANT INSERT ON TABLE logs TO sysloguser;
GRANT UPDATE ON SEQUENCE logs_entry_seq TO sysloguser;
```

Back To Loghost

Add to inittab:

```
sl:2345:respawn:/usr/local/bin/syslog-ng-pgsql-pipe.sh
```

Create /usr/local/bin/syslog-ng-pgsql-pipe.sh:

```
[[ -p /var/run/pgsql.pipe ]] || /bin/mknod /var/run/pgsql.pipe p
exec /usr/bin/psql –U sysloguser –d syslogdemo –h db
   </var/run/pgsql.pipe
```

Don’t forget to

```
chmod 700 /usr/local/bin/syslog-ng-pgsql-pipe.sh
```

Add to loghost’s /etc/hosts:

```
192.168.182.129 db
```

Then ‘telinit q’ to have init re-read inittab and start everything going.

Issues, Concerns, Enhancements

- Database security (Research this)
- Database structure/design (See links)
- Database optimization (PostgreSQL defaults not good for large number of records)
- Web reporting (Probably Apache/PHP)
- Log Squid-cache, Apache (Large amount of data!)

Links

Syslog-ng (http://www.balabit.com/products/syslog_ng/)
PostgreSQL (http://www.postgresql.org/)
Ubuntu (http://www.ubuntu.com/)
Kiwi Logger (http://www.kiwisyslog.com/index.php)
Snare EventLog Agent for Windows (http://www.intersectalliance.com/projects/SnareWindows/)
pgAdmin (http://www.pgadmin.org/)
VMware (http://www.vmware.com/)
RFC 3164 (http://www.ietf.org/rfc/rfc3164.txt)

Some sites you'd find via Google anyway:
http://www.campin.net/syslog-ng/faq.html
http://ben.muppethouse.com/SYSLOG-DOC.html
http://www.kdough.net/docs/syslog_postgresql/
http://www.whitemiceconsulting.com/node/103
http://community.seattleserver.com/viewtopic.php?p=33&