EXILOG

Exim logs and Queue management Tool
AFNOG Workshop
May 30, 2008
Frank A. Kuse

What is Exilog?

- Exilog is an open source tool to centralize and visualize Exim logs across multiple Exim Servers.
- It is used in addition to Exim's standard or syslog logging.
- It does not require changing Exim or its logging style and doesn't require restarting Exim Daemon.

Features of Exilog

- Search for addresses, hosts (names and IP addresses), message Ids and ident strings.
- Filter by event types: Arrival, Deliveries, Deferrals, Errors, Rejects and messages that are still on-queue.
- Message actions: Force deliveries, cancel and delete
- Filter by time range, servers and server groups
- See basic host statistics, message sizes, message transfer times

Features of Exilog -- Continue

- Point-and-click on message Ids, IP addresses, hostnames to get different filtering results.
- Track messages across servers by header message ID.

Exilog Target Audience

- This tool is used for Postmasters who want to be able to troubleshoot email delivery across their Exim installations, no matter if used as relays or backend IMAP and POP toasters.
- It's very good for Postmasters who want to offload email support to staff who are less proficient with grep, sed and awk.

LABS

Installing Exilog

- Prerequisite for installing Exilog is Mysql Server with installation step as below
- Cd /usr/ports/databases/mysql50-server
  make install clean
- Cd /usr/ports/mail/exilog
  make install clean

Setting up exilog Mysql Database

- Enabling mysql server

  ```
  vi /etc/rc.conf
    mysql_enable=”YES”
  ```

- Creating an account for exilog on mysql server

  ```
  mysql -uroot
  create database exilog ;
  grant all on exilog.* to exilog identified by 'password'
  ```

- Install the initial exilog database

  ```
  cd /usr/local/share/docs/exilog
  mysql -uexilog -ppassword exilog < mysql-db-script.sql
  ```

Configuring Exilog

- Cp /usr/local/etc/exilog-dist /usr/local/etc/exilog.conf
- Vi /etc/local/etc/exilog.conf

  ```
  #Example for local MySQL server
  'type'     => 'mysql',
  'DBI'      => 'DBI:mysql:database=exilog;',
  'user'     => 'exilog',
  'pass'     => 'password'
  ```

Configuring Exilog -- Continue

- 'logs' => [
  '/var/spool/exim/log/mainlog',
  '/var/spool/exim/log/rejectlog'
  ],
- # Path to your Exim binary
  'exim' => '/usr/exim/bin/exim',

Configuring Apache server

```
vi /usr/local/etc/apache22/httpd.conf
# Virtual hosts
Include etc/apache22/extra/httpd-vhosts.conf

vi /usr/local/etc/apache22/extra/httpd-vhosts.conf

<VirtualHost *:80>
    ServerAdmin gofori@stapee.afnogws.gh
    DocumentRoot /usr/local/www/exilog
    ServerName exilog.stapee.afnogws.gh
    ErrorLog /var/log/exilog.stapee.afnogws.gh-
error_log
```

```
 CustomLog
/var/log/exilog.stapee.afnogws.gh_log common
      ScriptAlias /exilog_cgi.pl
/usr/local/www/exilog/exilog_cgi.pl
          <Directory "/usr/local/www/exilog/">
            AllowOverride AuthConfig
            Options +ExecCGI
            Order allow,deny
            Allow from all
          </Directory>
      Alias /exilog "/usr/local/www/exilog/"
```

```
     </Directory>
   Alias /exilog "/usr/local/www/exilog/"
     <Directory "/usr/local/www/exilog">
      Options None
      AllowOverride AuthConfig
      Order allow,deny
      Allow from all
     </Directory>
</VirtualHost>
vi /usr/local/etc/apache22/httpd.conf

# Modify DirectoryIndex to look like as below

 DirectoryIndex exilog_cgi.pl index.html
```

Creating Credential Access

- vi /usr/local/www/exilog/.htaccess

  ```
  AuthName "Exilog Access"
  AuthType Basic
  AuthUserFile /usr/local/www/exilog/htpasswd.users
  require valid-user
  ```

- htpasswd -c /usr/local/www/exilog/htpasswd.users exilog

Running Exilog

- Vi /etc/rc.conf
  exilog_enable=”YES”
- Chmod 644 /usr/local/etc/exilog.conf
- /usr/local/etc/rc.d/exilog start
- http://exilog.stapee.afnogws.gh

Documentation

- Download Exilog source http://duncanthrax.net/exilog/
- Sample Exilog screenshoots

  http://duncanthrax.net/exilog/screenshots/