MELACAK LALULINTAS EMAIL PADA ZIMBRA

Identitas Dokumen

Tipe	:	**PETUNJUK KERJA**	
No.	:		
Versi	:	1.0	Tgl Berlaku: 27 April 2011
Lokasi	:	Googlegroups	

Kontak untuk Minta Keterangan

Jika ada pertanyaan tentang dokumen ini, dapat menghubungi:

Telepon : +62 21 70760276
E-mail : toni@stiawan.web.id

Daftar Isi

Daftar Gambar

1. PENDAHULUAN

1.1 Ruang Lingkup

Ruang lingkup dari dokumen ini adalah:

1) Mencari transaksi ID untuk satu tujuan pengiriman
2) Menampilkan transaksi email secara lengkap
3) Menampilkan transaksi email dengan awk
4) Menyiapkan database mysql
5) Menyiapkan skrip PHP

Penulis menggunakan distro linux Ubuntu 8.04 dan Zimbra 6.06 sebagai bahan acuan. Apabila terdapat perbedaan lokasi path, Anda butuh menyesuaikan lokasi path sesuai kondisi pada linux Anda.

1.2 Kebutuhan awal

Untuk menjalankan beberapa perintah pada dokumentasi ini, dibutuhkan :

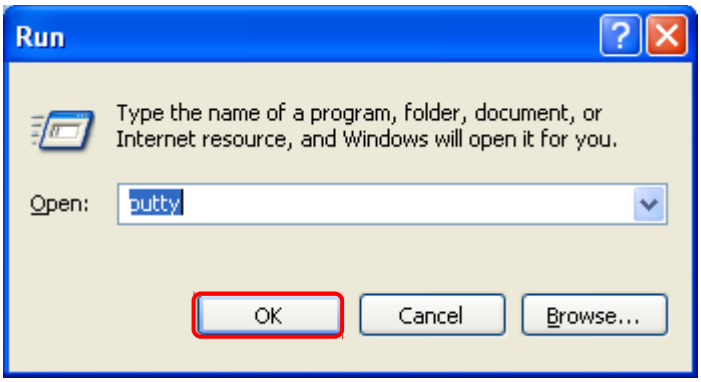
1) Akses root konsol linux
2) Akses root mysql
3) Mengetahui lokasi path log zimbra-postfix
4) Mengetahui perintah dasar linux untuk operasi file.

2. MENCARI TRANSAKSI ID UNTUK SATU TUJUAN PENGIRIMAN

2.1 Mengakses Server Linux

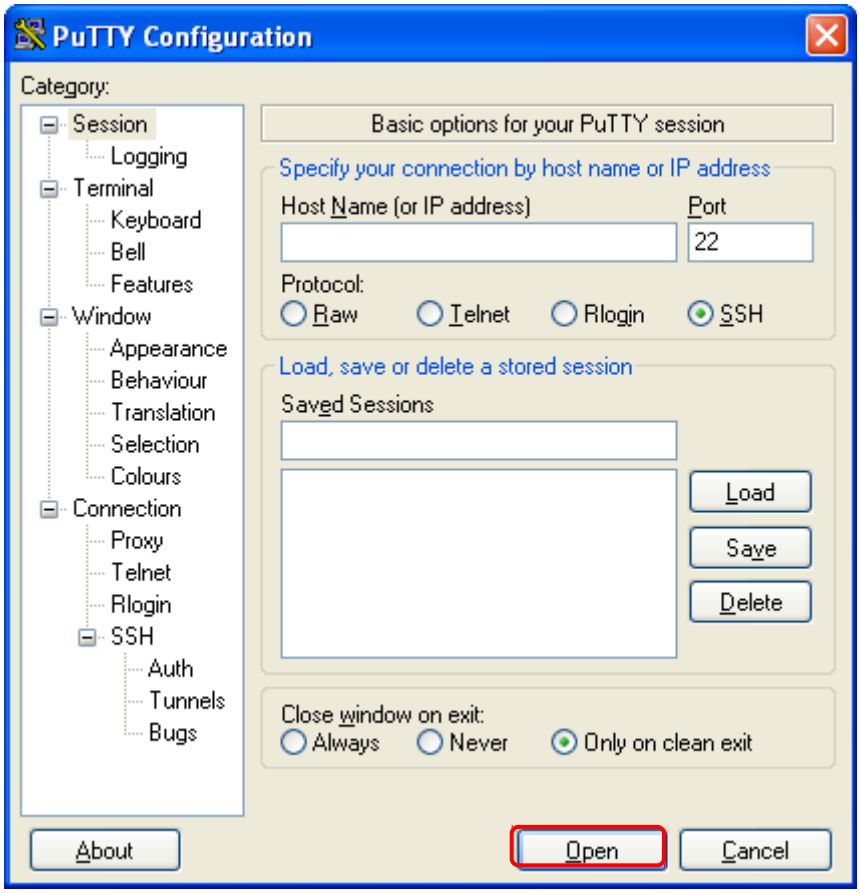
Agar dapat melakukan pencarian Transaksi ID suatu email, Anda perlu mengakses ke dalam konsol Linux untuk menjalankan beberapa perintah pencarian.

1. Jalankan putty atau aplikasi terminal lainnya.



Gambar 1 – Membuka putty

2. Kemudian klik tombol “Open”.



Gambar 2 – Mengakses mailserver dengan putty

2.2 Mengakses Zimbra Postfix Log

1. Secara default, zimbra akan menyimpan aktivitas pengiriiman dan penerimaan email pada /var/log/zimbra.log

2. Untuk melihat log aktivitas postfix, dapat menggunakan perintah tail seperti berikut :

   # tail –f /var/log/zimbra.log

2.3 Memahami Struktur Log

Pada Zimbra Postfix log terdapat bermacam catatan aktivitas postfix seperti :

- Smtpd

- Smtp

- Cleanup

- Qmgr

- Lmtp

- Scache, dll

Contoh Zimbra Postfix log dapat seperti berikut :

```
Apr 26 06:34:34 mailserver postfix/smtp[29776]: 4BE137CC477:
to=<wisnoe.irawan@example.stiawan.web.id>, relay=127.0.0.1[127.0.0.1]:10024, delay=0.49,
delays=0.12/0/0/0.37, dsn=2.0.0, status=sent (250 2.0.0 Ok, id=19755-12, from
MTA([127.0.0.1]:10025): 250 2.0.0 Ok: queued as A5F207CC47F)
Apr 26 06:34:34 mailserver postfix/qmgr[3796]: 4BE137CC477: removed
Apr 26 06:34:52 mailserver postfix/cleanup[29244]: AB66C7CC47F: warning: header Subject:
Delivered: Re: [Milis-dm] Cranes operation balance for shift III-26/06.00 hrs from
mx1.example.stiawan.web.id[192.168.2.4];
```

Bila mengacu pada contoh log di atas, setiap baris log akan menyimpan :

- Tanggal proses : Apr 26 xx:xx:xx

- Nama email server : mailserver

- Proses pada postfix beserta ID proses : postfix/xxxxx [yyyy]

- ID Transaksi : 4BE137CC477

- Content log transaksi

2.4 Melacak Status Pengiriman Email

Aktivitas pengiriman email pada zimbra akan dicatatkan pada log postfix. Jadi apabila ada permintaan untuk mengetahui status pengiriman email, Anda dapat membaca log postfix untuk mengetahui status pengiriman.

Untuk mencari informasi pada log file, Anda dapat menggunakan tools grep dengan format :

```
# grep –iE “smtp” /var/log/zimbra.log|grep -iE "to=.<user_tujuan>"
```

Contoh perintah grep di atas untuk mencari aktivitas email untuk tujuan “toni.stiawan”.

```
# grep –iE “smtp” /var/log/zimbra.log|grep -iE "to=.toni\.stiawan"
```

Anda dapat menyesuaikan perintah ini sesuai kebutuhan.

Bila kriteria yang dituliskan pada perintah grep tersebut ada pada log Zimbra Postfix, maka akan ditampilkan ke layar komputer. Dan Anda dapat mencatat ID Transaksi yang tampil pada layar untuk melakukan langkah selanjutnya.

3. MENAMPILKAN TRANSAKSI EMAIL SECARA LENGKAP

Setelah Anda mengetahui ID Transaksi, Anda dapat mencari kembali pada log file berdasarkan ID Transaksi. Perintah yang digunakan untuk mencari ID Transaksi adalah :

grep -i "<id-transaksi>:" /var/log/zimbra.log

Contoh perintah grep untuk mencari ID Transaksi 8280F7CC464 :

grep -i "8280F7CC464:" /var/log/zimbra.log

Apr 26 22:51:41 mailserver postfix/smtpd[12299]: **8280F7CC464**: client=mx2.example.stiawan.web.id[192.168.2.5]

Apr 26 22:51:41 mailserver postfix/cleanup[4695]: **8280F7CC464**: warning: header Subject: IronPort Report: Outgoing Mail Daily Report (ironport2.example.stiawan.web.id) from mx2.example.stiawan.web.id[192.168.2.5]; from=<toni.stiawan@example.stiawan.web.id> to=<toni.stiawan@example.stiawan.web.id> proto=ESMTP helo=<mx2.example.stiawan.web.id>

Apr 26 22:51:41 mailserver postfix/cleanup[4695]: **8280F7CC464**: message-id=<20110426155141.8280F7CC464@mx1-zimbra.example.stiawan.web.id>

Apr 26 22:51:41 mailserver postfix/qmgr[3796]: **8280F7CC464**: from=<toni.stiawan@example.stiawan.web.id>, size=275989, nrcpt=1 (queue active)

Apr 26 22:51:50 mailserver postfix/smtp[4564]: **8280F7CC464**: to=<toni.stiawan@example.stiawan.web.id>, relay=127.0.0.1[127.0.0.1]:10024, delay=8.6, delays=0.18/0/0/8.4, dsn=2.0.0, status=sent (250 2.0.0 Ok, id=26355-15, from MTA([127.0.0.1]:10025): 250 2.0.0 Ok: queued as 072CA7CC4EA)

Apr 26 22:51:50 mailserver postfix/qmgr[3796]: **8280F7CC464**: removed

4. MENAMPILKAN TRANSAKSI EMAIL DENGAN AWK

Agar tampilan transaksi email dapat dibaca lebih baik, Anda dapat memanfaatkan utility awk yang terdapat pada linux. Untuk memastikan utility ini terinstall pada linux, gunakan perintah whereis seperti berikut :

whereis gawk

Apabila pada linux terinstall gawk, maka akan ditampilkan path direktori utility ini

gawk: /usr/bin/gawk /usr/share/man/man1/gawk.1.gz

Penulis telah membuat satu skrip awk yang akan melakukan pengaturan tampilan transaksi email menjadi lebih baik dan enak dilihat. Letakan file gawk2.awk pada direktori /root

Skrip ini dipanggil bersamaan dengan perintah grep yang akan melakukan pencarian log email. Berikut ini baris perintah grep yang dikombinasikan dengan gawk :

grep -iE "postfix/(cleanup|smtp|qmgr)\[" /var/log/zimbra.log | /usr/bin/gawk -f /root/gawk2.awk | less

Perintah di atas akan menghasilkan tampilan

```
---------------------------------
| Transaction ID :  00F097CC365  |
---------------------------------
00F097CC365 || from || from=<edifact@example.stiawan.web.id>
00F097CC365 || ipsender ||  unknown[172.16.241.208];
00F097CC365 || size ||  size=2147
00F097CC365 || status ||  status=sent (250 2.0.0 Ok
00F097CC365 || subject || Subject: EDI Notification - COARRI Message to HJS from
unknown[172.16.241.208];
00F097CC365 || tglkirim || Apr 27 08:01:54
00F097CC365 || to-1534 || to=<edi_jkt@bumilaut.co.id>
00F097CC365 || to-1535 || to=<eqrpt_logjkt@bumilaut.co.id>
00F097CC365 || to-1536 || to=<edimail@hanjin.com>
```

5. MENYIAPKAN DATABASE MYSQL

Setelah informasi mengenai transaksi email dapat ditampilkan dengan rapi, selanjutnya Anda dapat menyimpan informasi tersebut ke dalam database MySQL. Pada tahap ini dibutuhkan server MySQL yang terinstall pada linux dan juga membutuhkan php5 terinstall pada linux sebagai shell skrip.

Penulis sudah menyiapkan beberapa skrip yang akan digunakan di petunjuk kerja ini. Kode sumber yang disertakan masih dalam kondisi dikompress.

5.1 Menyiapkan direktori kerja

Penulis telah menyiapkan kode sumber yang siap di pecah (extract). Adapun kondisi environment kerja :

- Operating System : ubuntu 8.04
- Zimbra : Community Edition 6.06
- Webserver : apache2
- Scripting language : php5
- Scripting output format : awk
- Postfix log path : /var/log/zimbra.log
- Web root path : /var/www

Untuk melakukan perintah-perintah di bawah ini, Anda butuh privileges root.

```
# mkdir /var/www/maillogs
# tar xvjf maillogs.tar.bz2 -C /var/www/maillogs
# cd /var/www/maillogs
```

5.2 Membuat database mail_stat

Setelah langkah 5.1 selesai dilaksanakan, selanjutnya menyiapkan database MySQL untuk menampung aktivitas Zimbra Postfix Log. Adapun langkah membuat database pada mysql

```
# mysqladmin -u root -p create mail_stat
# mysql –u root –p mail_stat < /var/www/maillogs/tools/mail_stat.sql
```

5.3 Membuat scheduler untuk menyimpan log transaksi.

Pada kode sumber yang disertakan Penulis, telah disertakan skrip yang butuh dipanggil dari scheduler (crontab). Untuk itu dibutuhkan beberapa pengaturan agar skrip tersebut berjalan baik.

- **Mengkonfigurasi koneksi database**

Anda perlu mengkonfigurasi nama database, username dan password untuk koneksi ke database MySQL pada file db.php. Nama database MySQL yang dicantumkan pada file db.php adalah nama database yang dilakukan pada langkah 5.2 (mysqladmin).

- **Menyesuaikan path skrip**

Anda juga perlu menyesuaikan path agar skrip dapat berfungsi baik. Adapun path yang perlu disesuaikan berada pada file :

Nama file	Teks asli	Diganti menjadi
Cron.run	./tools/trace-email-status.awk	/var/www/maillogs/tools/trace-email-status.awk
Cron.run	mail_stat.input	/var/www/maillogs/mail_stat.input
Parse-log.php	$fteks=file("mail_stat.input");	$fteks=file("/var/www/maillogs/mail_stat.input");

- **Mencoba fungsi skrip cron.run**

Setelah konfigurasi koneksi database telah dilakukan, selanjutnya mencoba skrip cron.run dijalankan secara langsung dari konsol linux :

./cron.run

Bila telah dapat dijalankan secara baik dan pada database telah terisi record log aktivitas Zimbra – Postfix berarti skrip telah berfungsi secara benar.

- **Menyisipkan ke scheduler crontab**

Agar setiap periode tertentu database terus ter-update, untuk itu perlu disisipkan scheduler yang memanggil skrip cron.run. Langkah menyisipkan ke scheduler :

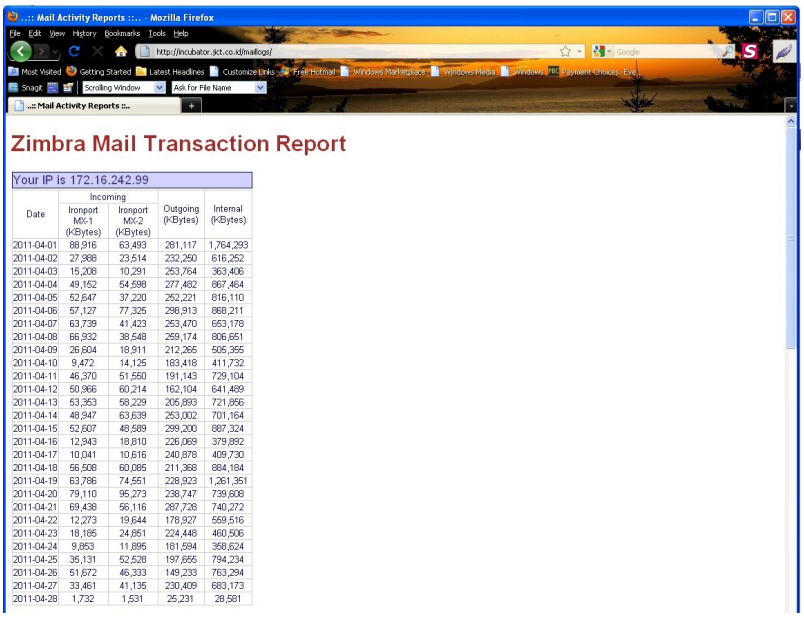
echo “* 0-23/2 * * * root /root/cron.run” >> /etc/crontab

Contoh scheduler di atas untuk menjalankan cron.run setiap 2 jam.

6. MENYIAPKAN SKRIP PHP

Skrip PHP yang akan dikonfigurasi berikut ini sebagai interface web based untuk menampilkan isi database mail_stat yang berisi aktivitas lalulintas email Zimbra Postfix. Untuk itu dibutuhkan Apache webserver, libapache2-mod-php5 dan extension mysql.so pada php5.

Pada skrip index.php baris ke-2, dibutuhkan penyesuaian nama domain seperti yang Anda gunakan. Setelah disesuikan dengan nama domain Anda, selanjutnya Anda dapat memanggil script tersebut dengan alamat http://<ip_server>/maillogs/ menggunakan web browser.



Date	Incoming Ironport MX-1 (KBytes)	Incoming Ironport MX-2 (KBytes)	Outgoing (KBytes)	Internal (KBytes)
2011-04-01	88,916	63,493	281,117	1,764,293
2011-04-02	27,988	23,514	232,250	616,252
2011-04-03	15,208	10,291	253,764	363,406
2011-04-04	49,152	54,598	277,482	867,464
2011-04-05	52,647	37,220	252,221	816,110
2011-04-06	57,127	77,325	298,913	868,211
2011-04-07	63,739	41,423	263,470	653,178
2011-04-08	66,932	38,548	269,174	806,651
2011-04-09	26,604	18,911	212,265	505,365
2011-04-10	9,472	14,125	183,418	411,732
2011-04-11	46,370	51,550	191,143	729,104
2011-04-12	50,966	60,214	162,104	641,489
2011-04-13	53,353	58,229	205,893	721,856
2011-04-14	48,947	63,639	253,002	701,164
2011-04-15	52,607	48,589	299,200	887,324
2011-04-16	12,943	18,810	226,069	379,892
2011-04-17	10,041	10,616	240,878	409,730
2011-04-18	56,508	60,085	211,368	884,184
2011-04-19	63,786	74,551	228,923	1,261,351
2011-04-20	79,110	95,273	238,747	739,608
2011-04-21	69,438	56,116	287,728	740,272
2011-04-22	12,273	19,644	178,927	559,516
2011-04-23	18,186	24,851	224,448	460,506
2011-04-24	9,853	11,895	181,594	358,624
2011-04-25	35,131	52,528	197,655	794,234
2011-04-26	51,672	46,333	149,233	763,294
2011-04-27	33,461	41,135	230,409	683,173
2011-04-28	1,732	1,531	25,231	28,581

Gambar 3 – Tampilan interface web