Fixing Zimbra Tidak dapat Mengirim ke Luar

Di salah satu mail server klien kami terdapat kendala tidak dapat mengirimkan email keluar, namun mail server tersebut dapat menerima email dari luar (gmail,zoho,dll). Sebelumnya email dapat terkirim dengan baik. Tentu yang perlu saya lakukan adalah memeriksa log di mail server berbasis zimbra tersebut.

```
tail -n 500 /var/log/zimbra.log
```

opsi `-n 500` agar saya leluasa melihat lebih banyak log ketimbang hanya 10 baris saja tanpa opsi tersebut. Hasilnya diketahui bahwa mail server tidak dapat terhubung ke relay. Karena memang mail server ini memanfaatkan relay yang ditawarkan oleh ISP yang digunakan. Terbukti dengan log yang berbunyi:

```
Jul 30 18:33:07 mail postfix/smtp[19382]: connect to smtp.relay-
isp.net.id[ip-relay-isp]:25: Connection timed out
```

> **Catatan:** di sini nama ISP dan alamat emailnya saya samarkan.

Saya sedikit curiga kalau salah satu akun di mail server ini melakukan spamming. Kecurigaan saya pun mulai terasa menguat setelah saya menemukan bukti di log:

```
....
Jul 30 18:31:53 mail postfix/qmgr[2538]: AADC94721281: from=<terdeteksi-
spammer@samsulkab.go.id>, size=116949, nrcpt=1 (queue active)
Jul 30 18:31:53 mail postfix/qmgr[2538]: B1DE64A3407D: from=<terdeteksi-
spammer@samsulkab.go.id>, size=71643, nrcpt=1 (queue active)
Jul 30 18:31:53 mail postfix/qmgr[2538]: B1D90422FD0E: from=<terdeteksi-
spammer@samsulkab.go.id>, size=97540, nrcpt=1 (queue active)
Jul 30 18:31:53 mail postfix/qmgr[2538]: 5EF404706463: from=<terdeteksi-
spammer@samsulkab.go.id>, size=90976, nrcpt=1 (queue active)
.....
```

Ada banyak sekali queue yang aktif dari 1 alamat email tersebut. Ditambah saya temukan pula alamat email tujuannya juga ngacak:

```
Jul 30 18:33:07 mail postfix/smtp[19383]: B1D90422FD0E:
to=<xxxzakaria.ras@hotmail.fr>, relay=smtp.relay-
isp.net.id[202.162.213.139]:25, delay=198415, delays=198340/0.09/74/0,
dsn=4.4.2, status=deferred (lost connection with smtp.relay-
isp.net.id[202.162.213.139] while receiving the initial server greeting)
Jul 30 18:33:07 mail postfix/smtp[19380]: 9DF314A3407C:
to=<xxxxluigiderosa68@gmail.com>, relay=smtp.relay-
isp.net.id[202.162.213.139]:25, delay=55401, delays=55326/0.07/74/0,
dsn=4.4.2, status=deferred (lost connection with smtp.relay-
isp.net.id[202.162.213.139] while receiving the initial server greeting)
Jul 30 18:33:07 mail postfix/smtp[19379]: 8D42B4A33728:
to=<xxxibor64@gmail.com>, relay=none, delay=56943, delays=56868/0.06/74/0,
```

```
dsn=4.4.1, status=deferred (connect to smtp.relay-isp.net.id[ip-relay-
isp]:25: Connection timed out)
Jul 30 18:33:07 mail postfix/smtp[19382]: B1DE64A3407D:
to=<xxxluigicuore56@gmail.com>, relay=none, delay=55401,
delays=55326/0.08/74/0, dsn=4.4.1, status=deferred (connect to smtp.relay-
isp.net.id[ip-relay-isp]:25: Connection timed out)
Jul 30 18:33:07 mail postfix/smtp[19381]: AADC94721281:
to=<xxxpascal.lasseur@free.fr>, relay=none, delay=198088,
delays=198013/0.07/74/0, dsn=4.4.1, status=deferred (connect to smtp.relay-
isp.net.id[ip-relay-isp]:25: Connection timed out)
Jul 30 18:33:07 mail postfix/error[20301]: 5EF404706463:
to=<oz-2010@live.fr>, relay=none, delay=197979, delays=197905/75/0/0.01,
dsn=4.4.1, status=deferred (delivery temporarily suspended: connect to
smtp.relay-isp.net.id[ip-relay-isp]:25: Connection timed out)
Jul 30 18:33:07 mail postfix/error[20301]: 60E3E4A32FAD:
to=<xxxsatanqueta69@gmail.com>, relay=none, delay=200057,
delays=199983/75/0/0, dsn=4.4.1, status=deferred (delivery temporarily
suspended: connect to smtp.relay-isp.net.id[ip-relay-isp]:25: Connection
timed out)
Jul 30 18:33:07 mail postfix/error[20302]: 5EA944A33755:
to=<xxxmaximumfusillo@gmail.com>, relay=none, delay=59717,
delays=59643/74/0/0.01, dsn=4.4.1, status=deferred (delivery temporarily
suspended: connect to smtp.relay-isp.net.id[ip-relay-isp]:25: Connection
timed out)
Jul 30 18:33:07 mail postfix/error[20303]: E4CD84A32FAF:
to=<lxxxucabarone@gmail.com>, relay=none, delay=57620,
delays=57545/74/0/0.07, dsn=4.4.1, status=deferred (delivery temporarily
suspended: connect to smtp.relay-isp.net.id[ip-relay-isp]:25: Connection
timed out)
Jul 30 18:33:07 mail postfix/error[20301]: 6EE2F4A32FAB:
to=<pxxxaulami69@gmail.com>, relay=none, delay=200434,
delays=200360/75/0/0.08, dsn=4.4.1, status=deferred (delivery temporarily
suspended: connect to smtp.relay-isp.net.id[ip-relay-isp]:25: Connection
timed out)
Jul 30 18:33:07 mail postfix/error[20304]: E2D434A34062:
to=<xxah856465@gmail.com>, relay=none, delay=56867, delays=56792/75/0/0,
dsn=4.4.1, status=deferred (delivery temporarily suspended: connect to
smtp.relay-isp.net.id[ip-relay-isp]:25: Connection timed out)
Jul 30 18:33:07 mail postfix/error[20302]: 6667A4A3409A:
to=<xxxbilling@ptdes.net>, relay=none, delay=34580, delays=34506/74/0/0.08,
dsn=4.4.1, status=deferred (delivery temporarily suspended: connect to
smtp.relay-isp.net.id[ip-relay-isp]:25: Connection timed out)
Jul 30 18:33:07 mail postfix/error[20301]: D4A314A33757:
to=<jxxxxuanquis@outlook.it>, relay=none, delay=59530,
delays=59455/75/0/0.01, dsn=4.4.1, status=deferred (delivery temporarily
suspended: connect to smtp.relay-isp.net.id[ip-relay-isp]:25: Connection
timed out)
Jul 30 18:33:07 mail postfix/error[20305]: E31614A34078:
to=<jxxx.folletto@libero.it>, relay=none, delay=55601,
delays=55526/75/0/0.04, dsn=4.4.1, status=deferred (delivery temporarily
```

```
suspended: connect to smtp.relay-isp.net.id[ip-relay-isp]:25: Connection
timed out)
Jul 30 18:33:07 mail postfix/error[20306]: 118F54A32FBC:
to=<txxxxhierryanger@hotmail.fr>, relay=none, delay=198533,
delays=198458/75/0/0.03, dsn=4.4.1, status=deferred (delivery temporarily
suspended: connect to smtp.relay-isp.net.id[ip-relay-isp]:25: Connection
timed out)
Jul 30 18:33:07 mail postfix/error[20302]: 6667A4A3409A:
to=<financexxx@ptdes.net>, relay=none, delay=34580, delays=34506/74/0/0.11,
dsn=4.4.1, status=deferred (delivery temporarily suspended: connect to
smtp.relay-isp.net.id[ip-relay-isp]:25: Connection timed out)
```

Kecurigaan saya tersebut segera saya konfirmasi dengan memeriksa mail queue yang ada dengan langkah sebagai berikut:

masuk sebagai user `zimbra`

```
su - zimbra
```

lalu dengan user zimbra tersebut, cek mail queue

```
[zimbra@mail ~]$ postqueue -p
-Queue ID-  --Size-- ----Arrival Time---- -Sender/Recipient-------
7CF854A34060    71108 Fri Jul 30 02:54:10  terdeteksi-
spammer@samsulkab.go.id
     (connect to smtp.relay-isp.net.id[ip-relay-isp]:25: Connection timed
out)
                                        danieleiftodi@gmail.com

71B0A4A32FB7    97146 Wed Jul 28 11:18:10  terdeteksi-
spammer@samsulkab.go.id
     (connect to smtp.relay-isp.net.id[ip-relay-isp]:25: Connection timed
out)
                                        scro31@sfr.fr

72A1F4A3406B    76589 Fri Jul 30 02:53:01  terdeteksi-
spammer@samsulkab.go.id
(lost connection with smtp.relay-isp.net.id[ip-relay-isp] while receiving
the initial server greeting)
                                        constantiniulian123456@gmail.com
dst. dst. dst.
```

Saya coba cek ada berapa sih jumlah email yang belum terkirim dari email tersebut:

```
/opt/zimbra/common/sbin/postqueue -p | awk 'BEGIN { RS = "" } { if ($7 ==
"terdeteksi-spammer@samsulkab.go.id" ) print $1 }' | tr -d '!*' | wc -l
91
```

Wah, ternyata ada 91. Saya pun tidak sempat memeriksa ada berapa email yang telah berhasil dikirimkan, tapi saat ini kita tahu ada 91 email yang belum berhasil dikirimkan oleh email tersebut sebagai spam.

Selanjutnya saya sampaikan kepada klien beberapa langkah yang perlu dilakukan untuk mengangani ini adalah sebagai berikut:

1. bersihkan mail queue khusus dari email tersebut
2. ubah password akun email tersebut
3. setelah itu baru sampaikan ke relay-isp bahwa kita kita telah menangani akun yang spamming, lalu tolong dibuka kembali untuk akses relay-nya...

Langkah 1 & 2 saya bantu eksekusi, sedangkan langkah 3 akan dieksekusi oleh klien sendiri. Nah, untuk eksekusi langkah 1 tersebut saya hanya perlu eksekusi perintah berikut:

```
/opt/zimbra/common/sbin/postqueue -p | awk 'BEGIN { RS = "" } { if ($7 ==
"terdeteksi-spammer@samsulkab.go.id" ) print $1 }' | tr -d '!*' |
/opt/zimbra/common/sbin/postsuper -d -
postsuper: 7595F4A32FB5: removed
postsuper: 77BA64A3374F: removed
postsuper: 7F0824A32F9E: removed
postsuper: 7CF854A34060: removed
postsuper: 71B0A4A32FB7: removed
postsuper: 72A1F4A3406B: removed
dst. dst. dst.
postsuper: Deleted: 92 messages
```

Oiya, perintah tersebut perlu dieksekusi sebagai root, jadi perlu `exit` dulu dari user zimbra tadi.

Sekarang queue email tersebut telah kita hapus, lanjut ke langkah 2, kita buatkan email tersebut password baru yang lebih rumit.

```
zmprov sp terdeteksi-spammer@samsulkab.go.id "passwordyangsangatrumit"
```

Password telah dibuat dengan yang baru. Lalu saya laporkan ke klien bahwa task sudah saya eksekusi.

Catatan dari saya adalah, baiknya untuk password akun email menggunakan yang rumit dan sulit ditebak. Karena jika salah satu akun email saja dapat ditebak dan ditemukan oleh attacker dia dapat menggunakan akun tersebut untuk melakukan spamming. Dampaknya tentu saja berbengaruh ke seluruh akun yang ada di mail server tersebut menjadi tidak dapat mengirimkan email.

Demikian catatan ini, semoga bermanfaat.

Referensi

- https://wiki.zimbra.com/wiki/Managing-The-Postfix-Queues
- https://wiki.zimbra.com/wiki/Reset_an_User_or_Administrator_password

From:
https://wiki.samsul.web.id/ - **Samsul Maarif**

Permanent link:
https://wiki.samsul.web.id/linux/Fixing.Zimbra.Tidak.dapat.Mengirim.ke.Luar

Last update: **2021/07/30 15:23**