

8.1.2 MRlv2-ROUTER routet Mails falsch

Am Tag nach der Einführung ist aufgefallen, dass im MRlv2-Proxy ungewöhnlich viele (6750) Mails angekommen sind. Hier sollten eigentlich nur Nicht-Domain-Aufträge landen oder nicht parsebare Mails. Tatsächlich liegen hier aber auch unzählige Domainaufträge (5473), die scheinbar vom Router nicht geparkt werden konnten, vom MRlv2-Proxy aber fehlerfrei ausgeführt wurden. Die Aufträge sind somit in der falschen Queue unter Missachtung von First come, first served über sehr zeitnah durchgeführt worden.

Eine Prüfung der Aufträge hat ergeben, dass trotz der falschen Einsortierung alle Aufträge in der richtigen zeitlichen Reihenfolge bearbeitet wurden. Es konnte keine Verletzung von First come, first served festgestellt werden.

Wie kann dieser Fehler verhindert werden können?

Die Entwicklungsabteilung hatte gesagt, dass im Router die gleichen Komponenten wie im MRlv2-Proxy und RRI stecken. Daher war davon auszugehen, dass der Router alle Mails parsen kann, die MRlv2 auch parsen kann. Aufgrund dieser Annahme und des Zeitdrucks wurden keine diesbezüglichen Tests durchgeführt.

Ob der Fehler bei Test aufgefallen wäre ist allerdings fraglich, da einige der Aufträge ein sehr pathologisches Format (auch nach DENIC-24 ungenügend, aber durch die Implementierung toleriert) hatten. Während der Mitglieder-Testphase gab es nur am 22.10. nur ein einziges Mal einen Auftrag unter über 8000 Aufträgen, der fehlschlug:

```
Content-Type: text/plain; charset=utf-8
Content-Transfer-Encoding: quoted-printable
X-DENIC-ProviderID: 375
X-DENIC-NCC-RegID: de.DENIC-375
X-DENIC-ProviderFull: Domain Services Rotterdam B.V.
X-DENIC-KeyID: D72D64FA

-----BEGIN PGP SIGNED MESSAGE-----
0D=0AHash: SHA256=0D=0A=0D=0AAction:=
CREATE=0D=0AVersion: 2.0=0D=0AActid: 8004acf7-a9bc-49f9-92b1-98f4ab304b0f=
=0D=0ADomain: on.de=0D=0ADomain-ace: =0D=0AHolder: DENIC-375-DSRDE=0D=0AAdmin-c:
=
DENIC-375-SIV=0D=0ATech-c: DENIC-375-DSR=0D=0AZone-c: DENIC-375-DSR=0D=0ANserve
r:=
ns.tellus.nl=0D=0ANserver: ns2.tellus.nl=0D=0A=0D=0A-----BEGIN PGP SIGNATURE---
---
=0D=0AVersion: BCPG C# v1.5.0.0=0D=0A=0D=0AiJcEAREIAD8FAkrgO3Y4HERFTk1DLTM3NSBQc
m9kdWN0aW9uIETleSAoUm9ib3Qt=
=0D=0Aa2V5KSA8REVOSUNAdGVsbHVzLmNvbT4ACgkQKjwKp9ctZPrmvAEA7wxvi3rYN9UR=0D=0AYHEJ
sJh6owIbaAQjUpe0c3p1G2kHP3MA/j1x9HV0ZSXj8msaroFO2Ky1AL3lS379=
=0D=0AmUL8lXww2Bz0=0D=0A=3DFKmd=0D=0A-----END PGP SIGNATURE-----
```

Ein derartiges Format wird derzeit durch das aktuelle Testsystem nicht simuliert und wird deswegen vermutlich nicht aufgefallen. Dies wird zukünftige Tests implementiert.

8.1.3 No_early-Problematik

Es wurde berichtet, dass Mitglieder in einer Minute mehr als 4 Aufträge durchbekommen können. Bei genauer Betrachtung ist dies aus mehrerlei Hinsicht tatsächlich möglich.

1. Ursache: Mailer

Die ACL im Exim greift nachdem der Client den Mail-Envelope geschrieben hat, also nach dem HELO, MAIL, RCPT. Der Timestamp wird aber erst nach der vollständigen Mail (mit dem Punkt) erstellt. Viele Mitglieder haben schon vor 9 Uhr die Verbindung aufgemacht, den Envelope und auch die Mail gesendet, bis auf den finalen Punkt. Damit wurde der Auftrag in der ACL um 08:59 Uhr gezählt, der Timestamp aber um 09:00 geschrieben. Dadurch waren in dieser Minute theoretisch 5 Aufträge möglich. Dieser Effekt kann auch in folgenden Zeitminuten auftreten, wenn eine Mail um xx:59 die Prüfung passieren, aber erst in der Folgeminute wird die Datensektion abgeschlossen und das received geschrieben wird, sehen wir ebenfalls für E-Mails für diese Minute aber nur drei für die Vorminute

2. Ursache: MySQL-ACL

Es sind zwei MySQL-Aktionen hintereinander notwendig, die nicht innerhalb einer Transaktion laufen. In der ersten wird der Counter hochgezählt, in der zweiten geprüft, ob er ≤ 4 ist. Zwischen Schritt 1 und 2 kann die Minute umspringen, wodurch der zweite Query 0 zurückgibt und in dieser Minute dann 5 Aufträge ermöglichen würde. Die Wahrscheinlichkeit ist gering, unter hoher Last aber sicher deutlich höher.

Eine Verknüpfung der Logfiles hat ergeben, dass von keiner IP aus mehr als 5 Aufträge in einer Minute gesendet wurden. Weiterhin wurde festgestellt, dass der Effekt bei keiner IP in zwei aufeinander folgenden Minuten auftrat. Der Effekt wurde aber in der Tat nachdem die Last zurückging beobachtet und zwar erstmalig in um 9:22 Uhr. Insgesamt wurde der Effekt 87 mal beobachtet.

```
5 194.50.187.234 09:22
5 212.16.224.130 09:35
5 79.140.49.61 09:35
5 213.158.112.122 09:36
5 87.233.214.195 09:37
5 87.233.214.196 09:37
5 87.237.120.2 09:37
5 95.130.18.4 09:37
5 195.60.208.6 09:38
5 87.233.215.82 09:38
5 213.187.75.33 09:39
5 79.125.18.193 09:39
5 87.233.215.92 09:39
5 95.130.18.5 09:39
5 193.19.92.23 09:40
5 195.226.65.133 09:40
5 212.12.32.70 09:40
5 81.95.11.198 09:40
5 85.190.44.85 09:40
5 86.109.254.39 09:40
5 95.130.18.6 09:40
5 188.94.248.210 09:41
5 192.55.84.85 09:41
5 212.40.189.15 09:41
5 212.89.98.4 09:41
5 217.148.181.10 09:41
5 217.173.140.40 09:41
5 217.188.240.180 09:41
5 82.198.95.20 09:41
5 213.128.128.130 09:42
5 78.46.96.9 09:42
5 80.190.147.81 09:42
5 81.3.3.8 09:42
5 217.173.140.40 09:43
5 62.128.1.62 09:43
5 79.125.18.193 09:43
5 87.233.214.203 09:43
5 95.130.18.4 09:43
5 195.60.208.6 09:44
5 212.123.34.101 09:44
```

```

5 212.204.60.58 09:44
5 212.6.120.2 09:44
5 212.89.98.4 09:44
5 217.188.240.180 09:44
5 85.10.200.86 09:44
5 87.233.214.208 09:44
5 212.79.49.139 09:45
5 82.98.99.3 09:45
5 85.119.206.26 09:45
5 217.13.193.102 09:46
5 87.233.214.206 09:46
5 213.128.128.130 09:47
5 80.190.147.81 09:47
5 85.10.200.86 09:47
5 89.146.235.235 09:49
5 89.146.235.235 09:51
5 89.146.235.235 10:02
5 89.146.235.235 10:04
5 62.214.75.4 10:05
5 89.146.235.235 10:09
5 62.80.102.230 10:12
5 88.198.184.4 10:12
5 89.146.235.235 10:17
5 62.214.75.4 10:18
5 88.198.184.4 10:20
5 89.146.235.235 10:21
5 88.198.184.4 10:25
5 193.138.108.27 10:26
5 212.223.223.82 10:26
5 62.214.75.4 10:26
5 62.80.102.230 10:26
5 78.46.96.9 10:28
5 213.218.0.130 10:30
5 217.148.181.10 10:31
5 89.146.235.235 10:35
5 78.46.96.9 10:37
5 78.46.96.9 10:39
5 78.46.96.9 10:41
5 62.214.75.4 10:45
5 62.214.75.4 10:47
5 62.80.102.230 10:48
5 78.46.96.9 10:49
5 62.80.102.230 10:51
5 193.138.108.27 10:54
5 62.214.75.4 10:54
5 78.46.96.9 10:54
5 78.46.96.9 10:58

```

8.1.4 Doppelte Antwortmails

In einigen Fällen sind Antwortmails doppelt an die Mitglieder gegangen. Die Ursache dafür ist noch unklar, es wird aber vermutet, dass bcc-Mails an DBS schuld sind. Diese Problematik ist im Vorfeld nicht aufgetreten, auch während der Mitglieder-Test phase hat kein Mitglied von diesem Problem berichtet.

Vor Produktionsbeginn wurden die Adressen in den MRlv2-Proxies von Test auf Produktion umgestellt, womit auch die bcc-Adresse eine andere war.

Bis zur vollständigen Klärung der Ursache ist ungewiss, ob dieser Fehler nicht verhindert werden kann.

8.2 Organisatorische Probleme

8.2.1 Poolbildung

Einige DENIC-Mitglieder scheinen sich während der Einführungsphase zu Pools zusammengeschlossen zu haben, um durch Aussortieren von Dubletten den gemeinsamen Registrierungserfolg zu maximieren. Wie viele Pools es gab mit wie vielen Mitgliedern teilgenommen hatten, ist nicht bekannt.

Es kam aber vor, dass Mitglieder über ihre IP-Adresse Auftragsmail anderer Mitglieder schickten, genauso wie es dem Anschein nach vorkam, dass Mitglieder, zwar die eigenen Auftragssignierung nutzen, aber die Aufträge im Vorfeld zur Erhöhung der gemeinsamen Chancen abstimmten.

Beide Vorgehensweisen sind seitens DENICs nicht grundsätzlich ausschließbar, da es sich um Verhaltensweisen handelt, welche im Verantwortungsbereich der jeweiligen Mitglieder liegen. Seitens DENIC wurde allerdings sichergestellt, dass nur von jedem Mitglied nur eine von diesem mitgeteilte IP-Adresse (signiert mit dem Master-Key des Mitglieds) und nur Aufträge, welche von einem Mitglied signiert waren, entgegen genommen wurden.

Die Anzahl von RegAccs je Mitglied spielte keine Rolle.

8.2.2 Keys von einzelnen Mitgliedern waren beim RollOut defekt

Während des RollOuts meldeten sich zwei DENIC-Mitglieder, deren PGP-Keys nicht für die Teilnahme am RollOut freigeschaltet waren. Beide Mitglieder konnten mit den betroffenen Keys am Mitgliedertest teilnehmen und die Probleme traten erstmalig beim RollOut der neuen Domains auf.

Hier eine Historie der entsprechenden Vorgänge

DENIC-325 (TMG)

23.10.2009, 09:22:53 Ticket 2009102343001322	Mitglied schreibt, sein Key funktioniert nicht Status: bisher unbeantwortet, ist leider untergegangen, da noch aus dem Vortagen viele Mails zu den Massentests vorlagen
23.10.2009, ca. 09:40 Anruf des Mitglieds	Mitglied beschreibt Problem mit Keys -> Eskalation an KT in War-Room -> Mitglied erstmalig vertreten, wg. Fehlersuche
23.10.2009, 10:15:50 Ticket 2009102343001895	Mitglied fordert eine Reaktion seitens Vorstand -> Mail wird im 10:37:17 beantwortet: Mitglied wird vertreten mit Hinweis, dass Vorgang bei Frau Dolderer liegt
23.10.2009, ca. 09:40 Ticket 2009102343001895	Nachfrage des Mitglieds, wann mit einer Aussage zu rechnen ist
23.10.2009, 10:56:58 Ticket 2009102343001895	Antwort an Mitglied: weiterer Hinweis auf Problemsuche und dass der Vorgang beim Vorstand liegt
23.10.2009, 11:16:22 Ticket 2009102343001895	Fristsetzung vom Mitglied (11:45:00) zur Klärung des Sachverhalts
23.10.2009, ca. 11:20:00	Lösung des Problems durch manuellen Import des Keys auf den Maschinen - Mitteilung per Jabber
23.10.2009, ca. 11:28:00	Bestätigung des Mitglieds, dass Key funktioniert

23.10.2009, ca. 11:40 Anruf des Mitglieds	Mitglied verträgt und Anruf von MSC versprochen
23.10.2009, ca. 11:45 Anruf beim Mitglied	MSC telefoniert mit Mitglied
23.10.2009, 13:30:57 Ticket 2009102343005686	Mitglied sehr verärgert und setzt weitere Frist
23.10.2009, 13:30:57 Antwort auf Ticket 2009102343005686	Mitglied beruhigt und Anruf des Vorstand gegen 15:00 Uhr zugesichert
23.10.2009, ca. 15:00 Anruf beim Mitglied	JOS ruft Mitglied an

Zwischen den einzelnen Aktionen fanden diverse Telefonate und Jabber-Kontakte statt. In diesen wurde das Mitglied immer wieder verträgt und auf Recherche verwiesen. Die Brisanz des Problems und dass Probleme bei DENIC die Ursache waren wurden zu spät erkannt.

Ursache des Problems:

Beim Einbinden eines davorliegenden Keys fehlte das Carriage Return in der letzten Zeile. Dadurch konnte der Key des Mitglieds (325) nicht gelesen werden. Der Fehler konnte vom Mitglied durch einen Test der Live-Umgebung nicht erkannt werden, da Einbindung des problem-verursachenden Keys erst nach dem letzten Massentest erfolgte (Key hinterlegt 17:19 (2009102043006734), auf die Maschinen kopiert 17:15 und 17:53)). Hatte das Mitglied aber einen Auftrag in die reguläre produktive Umgebung gesendet, so wurde auch dieser mit einem Fehler abgewiesen worden.

DENIC-259 (Secura)

23.10.2009, 09:49:36 Ticket 2009102343001608	Mitglied schreibt, sein Key funktioniert nicht Status: bisher unbeantwortet, ist leider untergegangen, da noch aus dem Vortagen viele Mails zu den Massentests vorlagen
23.10.2009, 15:01:24 Ticket 2009102343006658	Mitglied sendet Hilfeanfragen mit Fehlermeldungen Status: bisher unbeantwortet, ist leider untergegangen, durch die Problematik mit TMG Mitglied sendet Anfrage auf Grund der Mail von TMG auf der hostmaster-l Status: bisher unbeantwortet, zum Einen durch die Brisanz des Themas durch TMG, als auch die Auswertung bezüglich der Anfrage noch nicht vorliegt.

Zwischen den Tickets können Telefonate mit Herrn Oswald geführt worden sein, leider erinnert sich keiner im Team genau daran

Ursache des Problems:

