
Spam!
Spam!
Spam!
Spam!
Spam!
Spam!
Spam!
CLOUD
CLOUD
Oops!
BERLIN
heinlein
ORIGINAL 1KML
DDOS
PEST
CCC
shutdown -h now
PHP OR PYTHON
MASSAGE STUDIO
CAN MAN SCHON SO MACHEN, ABER DANN FÄLLT HAL RACCE
git commit -m "Nixes Fenster"
TABS OR SPACES? Hm! Hm! Hm!
CRIT
FUCKS
XXL
Bar
DOOM
IRON
Code of Conduct
atari teenage RIOT
LINUX
42
SACK MEHL
MEHLBOTORKE
RUHE!
ANMELDUNG
EINGANG
Snacks
LOG IN:
EIN ROOT FÜR ALLE FÄLLE.
#heinlein

heinlein

Peer Heinlein <p.heinlein@heinlein-support.de>

Dovecot 2.3:

Viele tolle neue Sachen

Peer Heinlein <p.heinlein@heinlein-support.de>

Geht's um E-Mail-Security...

- Heinlein Support GmbH / Peer Heinlein
  - Linux Security Consultant seit 1995
  - Spezialist für Mailserver und Anti-Spam/Anti-Virus seit 1992
  - Diplom-Jurist
  - Kunden:
    - ISPs > 100.000 Kunden und > 1.000.000 Kunden
    - Universitäten, Forschungseinrichtungen
    - diverse Landesrechenzentren (ITDZ, Stuttgart, Baden-Franken, Thüringen)
    - Massenversender
    - Eigene E-Mail ISPs: mailbox.org (Stiftung Warentest Testsieger)
  - Heinlein Support GmbH: 35 Mitarbeiter mit Sitz in Berlin

Post-Snowden Mail-Security 2016
[SLAC 2018]
Peer Heinlein <p.heinlein@heinlein-support.de>

Sharding auf dem Director

Peer Heinlein <p.heinlein@heinlein-support.de>

Zum Unterschied zwischen Director und Proxy

- „Dovecot Director“:

  Mehrere Logins des gleichen Users werden immer an das gleiche Backend weitergegeben – Source-IP egal.
  - Wichtig für Caching und insb. bei Object Storage!

- „Dovecot Proxy“:

  Der User wird anhand seines Host-Attributes in der Datenbank zu seinem Host mit seinen Postfächern weitergeleitet
  - Wichtig für Scale Out: Nicht jeder Host kennt jeden Nutzer
  - Dateisysteme bleiben klein, Last wird aufgeteilt
  - So auch: Perdition

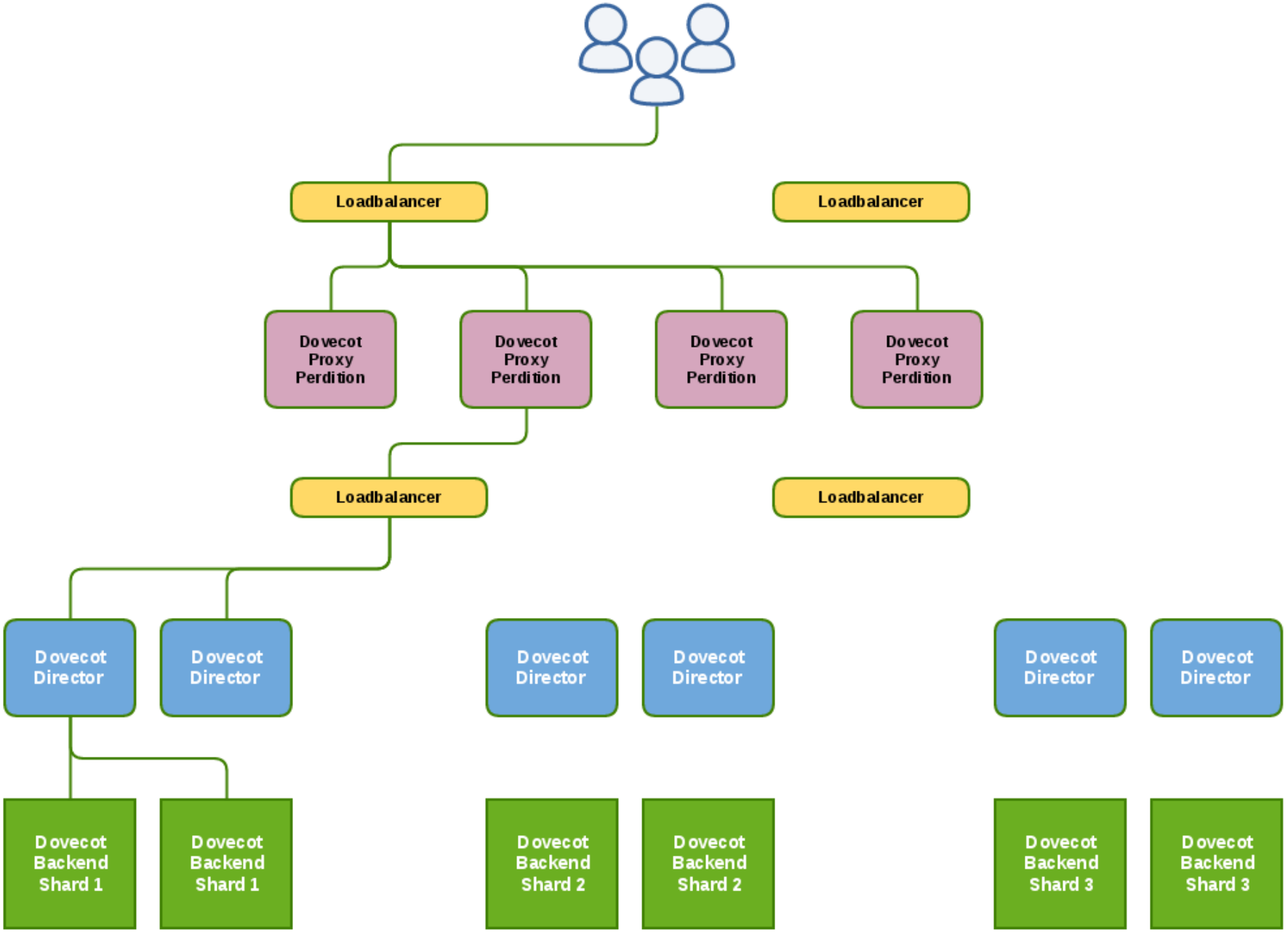
Peer Heinlein <p.heinlein@heinlein-support.de>

Viel Aufwand zum Scale-Out

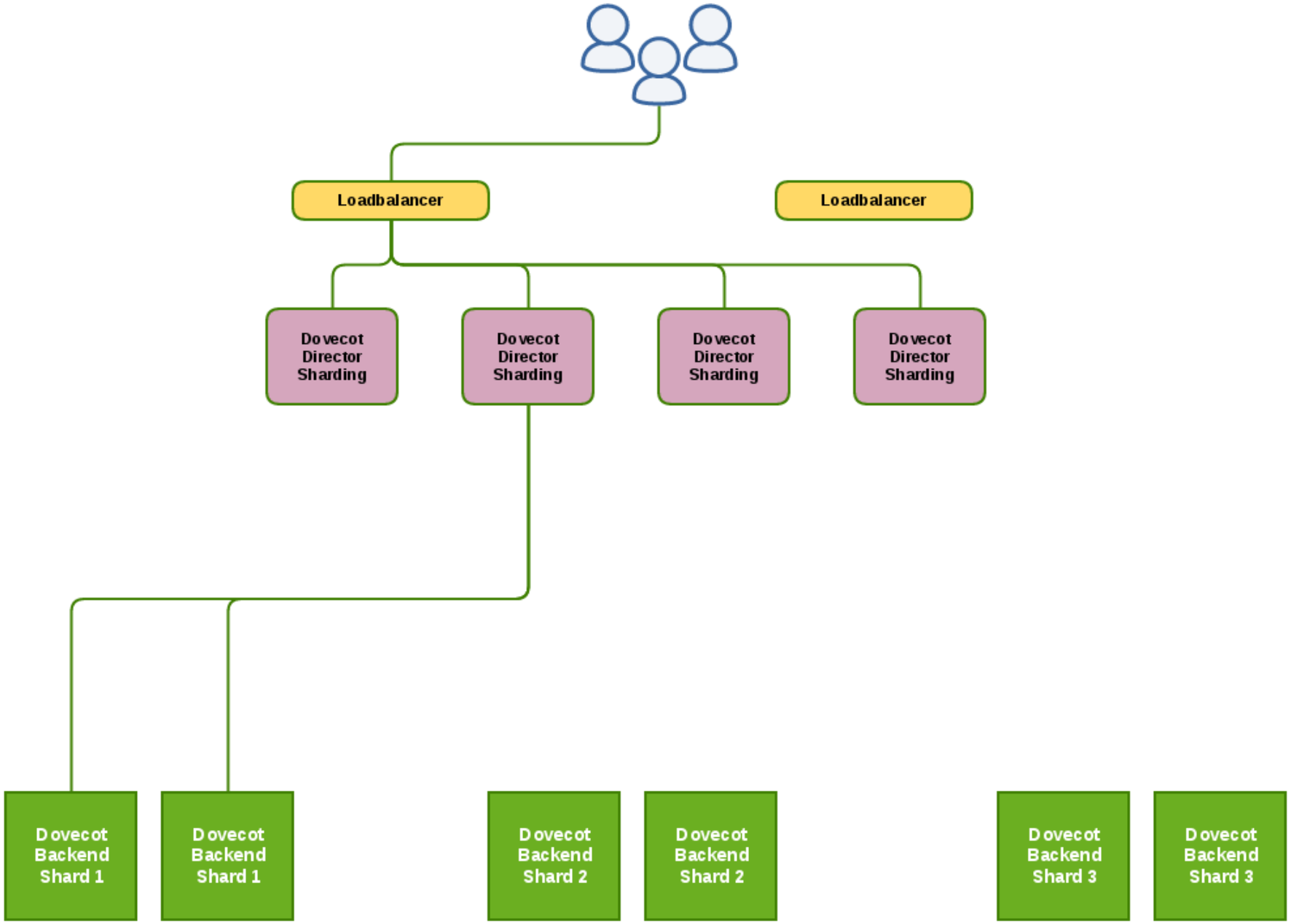
- Typisches Setup:

  Ein Proxy-Server verteilt über Loadbalancer auf Directoren-Gruppen
  - Die Directoren einer Gruppe bündeln die Userlogins auf das gleiche Backend.
  - Machbar, üblich, aber kompliziert.

- Neu: Director + Proxy-Funktionalität in einem Rutsch!


Loadbalancer
Loadbalancer
Dovecot Proxy Perdition
Dovecot Proxy Perdition
Dovecot Proxy Perdition
Dovecot Proxy Perdition
Loadbalancer
Loadbalancer
Dovecot Director
Dovecot Director
Dovecot Director
Dovecot Director
Dovecot Director
Dovecot Director
Dovecot Backend Shard 1
Dovecot Backend Shard 1
Dovecot Backend Shard 2
Dovecot Backend Shard 2
Dovecot Backend Shard 3
Dovecot Backend Shard 3

Post-Snowden Mail-Security 2016
[SLAC 2018]
Peer Heinlein <p.heinlein@heinlein-support.de>



Peer Heinlein <p.heinlein@heinlein-support.de>

Sharding – so geht‘s

- Alle Backends erhalten auf den Directoren einen Shard-Tag

```
director_mail_servers =  192.168.10.11@shard1 192.168.10.12@shard1
                         192.168.10.21@shard2 192.168.10.22@shard2
                         192.168.10.1@shard0
```

- „doveadm director“-Kommandos bereits aktiver Hosts brauchen keine Angabe des Shard-Tags mehr.

```
# doveadm director add 192.168.10.31@shard3

# doveadm director update 192.168.10.31 50
```

Peer Heinlein <p.heinlein@heinlein-support.de>

Sharding in der Authentifizierung

- Statt eines fixen Host haben die User einen „Shard-Tag“ in den Userdaten

```
user_attrs =[…] =proxy=y,=director_tag=shard%{ldap:ImapShard:1},=starttls=any-cert
pass_attrs =[…] =proxy=y,=director_tag=shard%{ldap:ImapShard:1},=starttls=any-cert
```

- User werden nur noch an die zu ihrem Shard-Tag passenden Backends weitergeleitet (=Proxy) dann aber gleiche Logins immer zum gleichen Backend (=Director).

Peer Heinlein <p.heinlein@heinlein-support.de>

Tipps für die Backends

- Tipp: Auf dem einzelnen Backend den Shard-Tag in dessen Config als Filter aufnehmen
  - user_filter, pass_filter, iterate_query

- Nur hier aktive User können sich einloggen / werden gefunden
  - Auch ein „doveadm user '*' " liefert nur die hier aktive Userliste

Peer Heinlein <p.heinlein@heinlein-support.de>

Anwendungsbeispiele

- Test-Cluster
  - Einen Shard-Tag „0“ als Test-Cluster reservieren
  - Test-User diesem Shard zuordnen => und dann einfach benutzen.
  - Gut auch für VIP-User oder Friendly-User-Tests (FUT)

- Migrationen
  - Alter-Cluster wird als „Shard 1“ bezeichnet
  - Direktoren werden in Stellung gebracht und dazwischengeschaltet
  - Ab dann einfache One-by-One-Migration möglich
    - User sperren
    - User umziehen
    - Shard-Tag des Users aktualisieren
    - User entsperren

Peer Heinlein <p.heinlein@heinlein-support.de>

Doveadm auf dem Director

Peer Heinlein <p.heinlein@heinlein-support.de>

Was Direktoren so alles können...

- Die Directoren verteilen nicht nur POP3, IMAP, LMTP, ManageSieve...

  ...sondern auch doveadm-Kommandos.

- Der Admin kann erledigt seine Aufgaben zentral auf dem Director
  - Er muß nicht prüfen, wo der User lokalisiert ist

- Bspw:
  - Quota-Abfrage
  - Management von Sieve-Scripten
  - Abfragen und Manipulationen an IMAP-Foldern
  - Status-Abfragen zur mailbox des Nutzers

Peer Heinlein <p.heinlein@heinlein-support.de>

Admin-Zugriff für das Helpdesk

- Helpdesk-Agents könnten einen eigenen Director-Server bekommen
  - Zugriff auf alle doveadm-Kommandos ohne SSH-Root-Zugriff auf die Server haben zu müssen!

heinlein

Peer Heinlein <p.heinlein@heinlein-support.de>

Doveadm per HTTP-API

Peer Heinlein <p.heinlein@heinlein-support.de>

Dovecot goes HTTP

- Doveadm kann per HTTP-API abgefragt werden
  - Früher: Ausführen von doveadm-Kommandos per SSH-Login
- Eine Einbindung in ein User-Verwaltungsinterfaces einfach möglich
  - Live-Anzeige der Quota-Auslastung im Userportal
  - Liste existierender IMAP-Folder als Zielordner für Spamfilterung
  - Urlaubsresponder auf Sieve-Basis selber programmieren

HTTP-API: So geht's

- Aktivieren des HTTP-Interfaces:

```
service doveadm {
   inet_listener http {
      port = 8080
      #ssl = yes # uncomment to enable https
   }
}
doveadm_password = chemnitzseaside
```

HTTP-API: So geht‘s

- Alle Abfragen sind per Shared Key gesichert
  - Base64 berechnen – Achtung: „echo -n“ verwenden!

```
echo -n doveadm:chemnitzseaside | base64
ZG92ZWFkbTpwYXNzd29yZA==
```

  - Aufrufe müssen Authorization-Headereinhalten:

```
Authorization: Basic ZG92ZWFkbTpjaGVtbml0enNlYXNpZGU=
```

- Mit curl geht das aber auch einfacher…

```
curl -v -X POST -u doveadm:doveadm_password -H "Content-Type: application/json"
http://localhost:8080/doveadm/v1
```

Peer Heinlein <p.heinlein@heinlein-support.de>

HTTP-API Dokumentation

- API-Schnittstelle bietet Doku:

```
# curl -k -H "Authorization: Basic ZG92ZWFkbTpjaGVtbml0enNlYXNpZGU="
https://127.0.0.1:8081/doveadm/v1

[...]
    {"command":"quotaGet", "parameters":[
                {"name":"allUsers","type":"boolean"},
                {"name":"socketPath","type":"string"},
                {"name":"user","type":"string"},
                {"name":"userFile","type":"string"}
        ]},
[...]
```

HTTP-API: So geht‘s

- Mit curl geht das aber auch einfacher…

```
curl -v -X POST -u doveadm:doveadm_password -H "Content-Type: application/json"
-d '[["mailboxStatus", {"field": ["messages"], "mailboxMask": ["INBOX"], "user":
"test@example.org"}, "c01"]]'  http://localhost:8080/doveadm/v1
```

- Weitere Doku:
  https://wiki2.dovecot.org/Design/DoveadmProtocol/HTTP

heinlein

Post-Snowden Mail-Security 2016
[SLAC 2018]
Peer Heinlein <p.heinlein@heinlein-support.de>

Submission and BURL support in Dovecot

Peer Heinlein <p.heinlein@heinlein-support.de>

Eigentlich nur folgerichtig...

- Dovecot 2.3 bietet ab sofort auch einen Submission-Dämon
  - Eigentlich nur folgerichtig: Mailversand (Submission), Mailabruf (POP3/IMAP)
  - Zumal auch bei Postfix & Co zur Authentifizierung stets Dovecot im Spiel war
- Der Submission-Server ist kein vollwertiger MTA
  - Arbeitet nur als SMTP-Proxy und forwarded die Verbindung live an Postfix
  - Quasi analog zu „smtpd_proxy_filter“
- Die Vorteile:
  - Einfache Anbindung an die in Dovecot vorhandene Authentifizierung
  - Einfache Integration in Anti-Abuse-Shield
  - Das Dovecot „penalty“-System blockt auch bei submission Brute Force-Logins

Das Henne-Ei-Problem hat nun die Henne

- Aktuell wird BURL nur Trojita unterstützt
- Weitere Kandidaten sind Mobile Apps wie K-9 Mail u.a.
- Stephan Bosch: „Das Huhn ist da, nun fehlt noch das Ei.“

Peer Heinlein <p.heinlein@heinlein-support.de>

Statistik: Wissen, was läuft

Peer Heinlein <p.heinlein@heinlein-support.de>

Dynamische Statistiken über alles

- Dovecot 2.3 hat ein neues Statistik-Modul
  - Altes „stats“-Modul nur noch im Legacy-Support, siehe Upgrade-README
- Alle Statistik-Daten basieren auf Log-Events
  - Quasi alles kann gezählt werden.
- Filter definieren, was gezählt wird
- „doveadm stats dump“ liefert Daten
  - Interessant: Auch Performance-Daten wie Lock-Times u.a.!
- Anbindung an Big Data-Systeme möglich

Peer Heinlein <p.heinlein@heinlein-support.de>

```
metric imap_select_no_notfound {
  event_name = imap_command_finished
  filter {
    name = SELECT
    tagged_reply = NO*Mailbox doesn't exist:*
  }
}


metric storage_http_gets {
  event_name = http_request_finished
  categories = storage
  filter {
    method = get
  }
}
```

heinlein

Peer Heinlein <p.heinlein@heinlein-support.de>

Sieve-Filter auch unter IMAP anwenden

Peer Heinlein <p.heinlein@heinlein-support.de>

Sieve geht auch beim Upload

- Sieve-Scripte werden normalerweise beim Speichern per LMTP ausgeführt
  - Mails können vom User aber auch per IMAP hochgeladen werden
- In Abhängigkeit vom Foldernamen kann Dovecot Sieve-Filter auf hochgeladene E-Mails anwenden
  - So greift der Filter auch bei verschobenen E-Mails
  - Hochgeladene Spam-Mails können zum Training an ein Spam-Utility geben?

Peer Heinlein <p.heinlein@heinlein-support.de>

```
plugin {
    sieve_plugins = sieve_imapsieve sieve_extprograms

    # From elsewhere to Spam folder
    imapsieve_mailbox1_name = Spam
    imapsieve_mailbox1_causes = COPY
    imapsieve_mailbox1_before = file:/var/vmail/sieve/global/learn-spam.sieve

    # From Spam folder to elsewhere
    imapsieve_mailbox2_name = *
    imapsieve_mailbox2_from = Spam
    imapsieve_mailbox2_causes = COPY
    imapsieve_mailbox2_before = file:/var/vmail/sieve/global/learn-ham.sieve

    sieve_pipe_bin_dir = /usr/bin
    sieve_global_extensions = +vnd.dovecot.pipe
}
```

```
require ["vnd.dovecot.pipe", "copy", "imapsieve"];
pipe :copy "rspamc" ["learn_spam"];
```

```
require ["vnd.dovecot.pipe", "copy", "imapsieve"];
pipe :copy "rspamc" ["learn_ham"];
```

heinlein

Peer Heinlein <p.heinlein@heinlein-support.de>

FTS: Volltextsuche unter Dovecot

Warum Ordnung wenn man suchen kann?

- User haben den Anspruch auch große Mailarchive per Volltext in Echtzeit zu durchsuchen
  - Warum in IMAP-Ordner sortieren wenn man doch suchen kann?
  - Volltextsuchen über mehrere Gbyte Mail-Daten dauern und können jeden IMAP-Server-Boliden in die Knie zwingen.
  - User verstehen das nicht.
- Volltextsuche per Lucene, Solr & Co sind für Dovecot verfügbar
  - Haben aber in allen meinen Tests nicht zufriedenstellend funktioniert.
  - Dovecot bringt eigenes FTS-Backend mit
  - Volltextsuche in wenigen Handgriffen aufgesetzt.
- Achtung: Kommerzielle Dovecot-Pro-Lizenz notwendig => $$$.

Peer Heinlein <p.heinlein@heinlein-support.de>

Ach, das Leben kann so einfach sein...

- Im lizensierten Enterprise-Repo sind „dovecot-fts“-Pakete
- Wenn das „fts“-Plugin aktiv ist, indiziert Dovecot neue Mails
  - Alte Mails über „doveadm index rescan“ nachpflegen lassen
  - Der FTS-Index liegt im Dateiform im User-Homeverzeichnis
  - Auch Attachments können indiziert werden (pdf2text & Co grüßen)
- FTS out-of-the-box mit Dovecot
  - Keine aufwändige SOLR/Lucene-Installation notwendig
  - Zusätzlicher Speicherverbrauch i.d.R. unter +5%
- Ab sofort Volltextsuche in Roundcube, OX & Co in „Echtzeit“

Peer Heinlein <p.heinlein@heinlein-support.de>

Der Unterschied ist enorm

```
[root@host ~]# time doveadm search -u p.heinlein@mailbox.org text TESTPATTERN

real    0m32.832s
user    0m28.276s
sys     0m2.528s
```

```
[root@host ~]# time doveadm -o "mail_plugins=zlib fts fts_dovecot" search -u
p.heinlein@mailbox.org text TESTPATTERN

real    0m4.022s
user    0m2.372s
sys     0m0.168s
```

Peer Heinlein <p.heinlein@heinlein-support.de>

Willkommens-Kultur

Das welcome-Script klärt „Dinge“

- Das „welcome“-Plugin führt eine Aktion aus, sobald sich ein User zum ersten mal angelegt wird
  - D.h.: sein Home-Directory erzeugt wird
- Bei mailbox.org nutzen wir welcome-Scripte u.a. um...
  - Special Use-Folder von vornherein anzulegen
  - Verschiedene Begrüßungs- und Support-Mails dem User zuzustellen

Peer Heinlein <p.heinlein@heinlein-support.de>

So geht's: welcome-Scripte

```
mail_plugins = $mail_plugins welcome

plugin {
 welcome_script = welcome %u
}

service welcome {
 executable = script /usr/local/bin/NewUserSpecialFolderCreate.sh
 unix_listener welcome {
   user = vmail
 }
 user = vmail
}
```

Peer Heinlein <p.heinlein@heinlein-support.de>

Haben wollen. Und nun?

Peer Heinlein <p.heinlein@heinlein-support.de>

Nicht zu früh freuen...

- Kritischer Einsatz der 2.3? Naja. Vorsicht.
  - Gut abgehangene Software ist auch was feines.
  - Die nächsten Wochen sicher noch mehr Bugs als normal.

- Fertige Pakete u.a.
  - http://repo.dovecot.org
  - http://xi.dovecot.fi (Nachfolger von Stephan Bosch xi.rename-it.nl)
  - Dovecot 2.3 im SuSE-Buildservice in server:mail schon verfügbar.

Upgrade? Vorsicht.

- Upgrade-README beachten!
  https://wiki2.dovecot.org/Upgrading/2.3

- Verschiedene neue Default-Werte
- Altes Statistik-Plugin nur noch im Legacy-Betrieb
- SSL/Diffie-Hellman mit geändertem Verhalten
- Auch Hosts in login_trusted_networks kriegen Penalty!

Peer Heinlein <p.heinlein@heinlein-support.de>

Community oder Enterprise?

Peer Heinlein <p.heinlein@heinlein-support.de>

Features der kommerziellen Lizenz

- Dovecot unterliegt der GPL, Pakete sind frei verfügbar.
  - „dovecot-ee-*“-Pakete von Dovecot mit QA veröffentlicht

- „Enterprise“-Features sind nicht Public und unterliegen Lizenz:
  - Native Volltextsuche (FTS)
  - REST API
  - Object Storage
  - Lawful Interception
  - Anti-Abuse-Shield
  - Support/Maintenance

Peer Heinlein <p.heinlein@heinlein-support.de>

Das Pricing der kommerziellen Lizenz

- Seit Januar 2018 ist Dovecot auch ohne AppSuite lizensierbar

- Repo-Access deb/rpm-Pakete + Enterprise-Features
  - 100 – 1.000 User: 5,- EUR / Jahr
  - 10.000 – 20.000 User: 3,- EUR / Jahr
  - >20.000 User: Projektpreis

  - 25% Rabatt für Non-Profit
  - 40% Rabatt für EDU/Academic

- Natürlich und gerne stehe ich Ihnen jederzeit mit Rat und Tat zur Verfügung und freue mich auf neue Kontakte.

Peer Heinlein

Mail: p.heinlein@heinlein-support.de

Telefon: 030/40 50 51 – 42

- Wenn's brennt:
  - Heinlein Support 24/7 Notfall-Hotline: 030/40 505 - 110

heinlein

Post-Snowden Mail-Security 2016
[SLAC 2018]
Peer Heinlein <p.heinlein@heinlein-support.de>

Ja, diese Folien stehen auch als PDF im Netz...
http://www.heinlein-support.de/vortrag

Peer Heinlein <p.heinlein@heinlein-support.de>

Soweit, so gut.

Gleich sind Sie am Zug:
Fragen und Diskussionen!

Peer Heinlein <p.heinlein@heinlein-support.de>

Wir suchen:
Admins, Consultants, Trainer!

Wir bieten:
Spannende Projekte, Kundenlob, eigenständige Arbeit, keine Überstunden, Teamarbeit

...und natürlich: Linux, Linux, Linux...

http://www.heinlein-support.de/jobs

Peer Heinlein <p.heinlein@heinlein-support.de>

Und nun...

- Vielen Dank für's Zuhören...
- Schönen Tag noch...
- Und viel Erfolg an der Tastatur...

Bis bald.

heinlein

Peer Heinlein <p.heinlein@heinlein-support.de>

Heinlein Support hilft bei allen Fragen rund um Linux-Server

HEINLEIN AKADEMIE

Von Profis für Profis: Wir vermitteln in Training und Schulung die oberen 10% Wissen: geballtes Wissen und umfangreiche Praxiserfahrung.

HEINLEIN HOSTING

Individuelles Business-Hosting mit perfekter Maintenance durch unsere Profis. Sicherheit und Verfügbarkeit stehen an erster Stelle.

HEINLEIN CONSULTING

Das Backup für Ihre Linux-Administration: LPIC-2-Profis lösen im CompetenceCall Notfälle, auch in SLAs mit 24/7-Verfügbarkeit.

HEINLEIN ELEMENTS

Hard- und Software-Appliances für Archivierung, IMAP und Anti-Spam und speziell für den Serverbetrieb konzipierte Software rund ums Thema E-Mail.


Spam!
Spam!
Spam!
Spam!
Spam!
Spam!
Spam!
CLOUD
CLOUD
Oops!
BERLIN
heinlein
ORIGINAL 1KML
DDOS
PEST
CCC
shutdown -h now
PHP OR PYTHON
MASSAGE STUDIO
CAN MAN SCHON SO MACHEN, ABER DANN FÄLLT HAL RACCE
git commit -m "Nixes Fenster"
TABS OR SPACES? Hm! Hm! Hm!
CRIT
FUCKS
XXL
Bar
DOOM
IRON
Code of Conduct
atari teenage RIOT
LINUX
42
SACK MEHL
MEHLBOTORKE
RUHE!
ANMELDUNG
EINGANG
Snacks
LOG IN:
EIN ROOT FÜR ALLE FÄLLE.
#heinlein