Postfix, DOVECOT, Anti-Spam

Sei Dein eigener Mail-Admin!

Jan Büren

FrOSCon 2015
22. / 23. 8. 2015
Hochschule Rhein / Sieg

Richardson & Büren

Worum geht es in diesen Vortrag ...

... (erstmal)NICHT!!!

- Kein weiteres HowTo
- Keine Schulung
- Nicht um E-Mail-Server
- Nicht um Linux

Richardson & Büren

Es geht um:

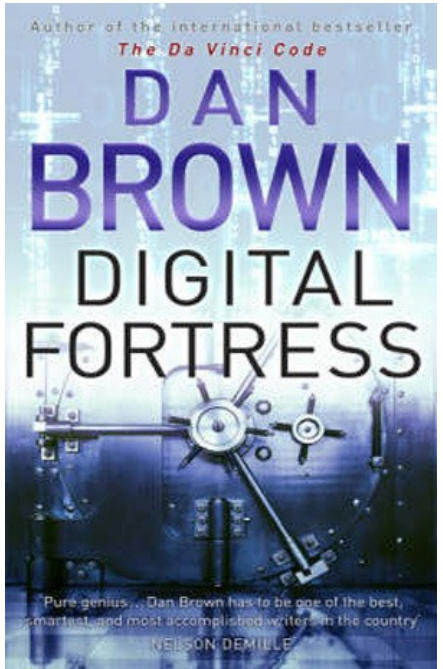
- Unabhängigkeit
- Sicherheit
- Freiheit
- Freundschaft
- Technische Leidenschaft

Meine E-Mail Status 1999

fd1919@meine-hochschule.de

Webmailer mit https!!

https://urd.informatik.meine-hochschule.de



Richardson & Büren

E-Mails sind wie Postkarten!

Richardson & Büren

… mit vielen Kopien!!

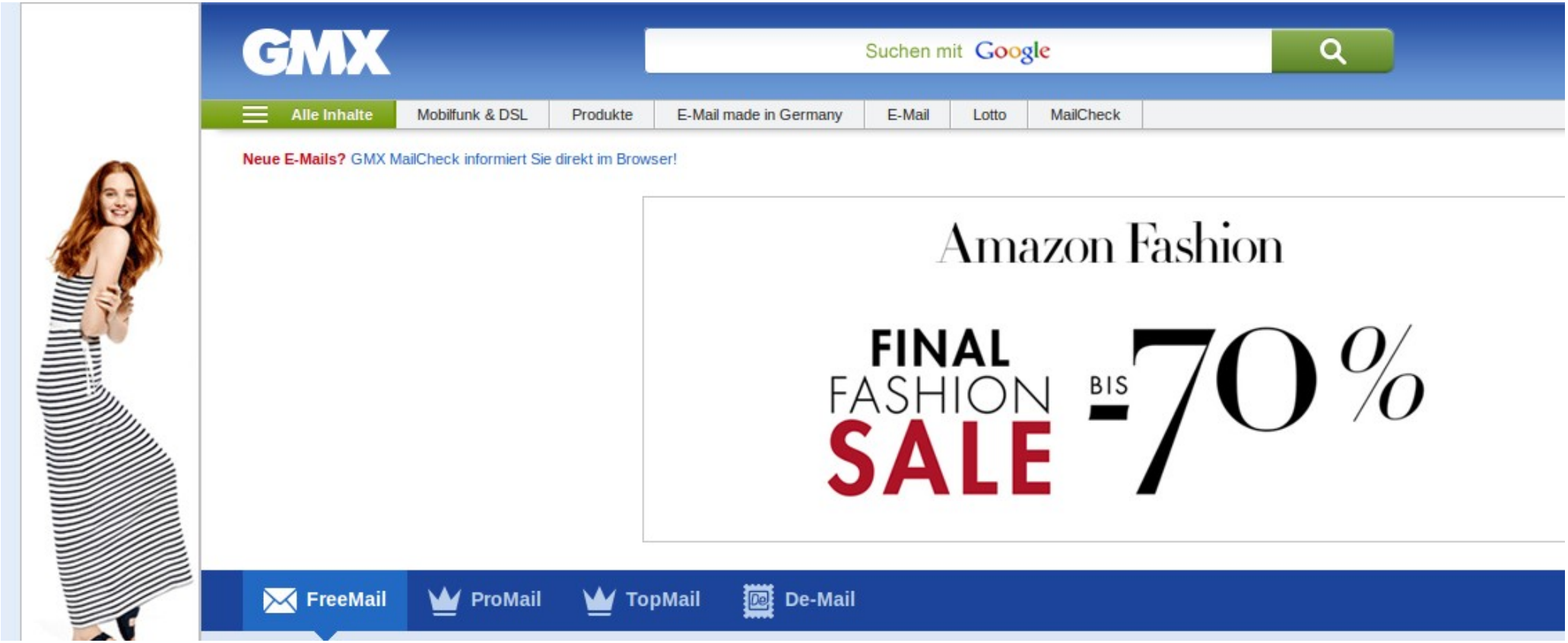
Virenscanner

E-Mail-Hoster

MX-Gateways

Lokaler E-Mail-Client

Alternative Freemailer ...



- Nicht wirklich free (Werbung?)
- Nur POP
- Speicherplatz
- Wo sind meine Daten?
- Wer hat Zugriff?

Richardson & Büren

Permanente E-Mail-Adresse

- Arbeit?
- Hochschule?
- Verein?
- gmx?
- …

stunteltje@gmail.com

Alles doof! Heimwerker-King!

- **Nur Transportverschlüsselte Verbindungen**
- **KEIN (!!!) POP**
- **VIEL Speicherplatz**
- **Zugriff hat: Geoff, Jan, Nick und Kube**
- **Kosten 7,95 € / Monat + Arbeitszeit**

https://web.archive.org/web/20040318215917/http://vlinux.de/

Richardson & Büren

Die Zusage:

- Virtueller Raum
- Ortsunabhängig
- Wissensspeicher
- International
- IMMER SICHER!
- Client-Freiheit

MediaGlyphs.org

Proto-Indo-European Roots

Root/Stem:	****weid-***
Meaning:	to know, to see

Ort und Team 2004

- **Drei Nationalitäten (englisch, deutsch italienisch)**
- **Drei Orte (Westfalen, Nord-Italien, China)**

SMTP-DSL-Relay Italien

- Mediaglyphs.org → SMTP Service
- „alte“ Mail-Adressen → fetchmail / .forward

$ dig mx mediaglyphs.org

Richardson & Büren

Neujahrsgrüße 2014!!!

Neujahrsgrüße 2014 – ling. hacker

Con "extra-super-frizzanti" augurissimi per un eccezionale 2015!!

With our most bubbly and sparkling wishes for an amazing 2015!!

祝您特别精彩的新一年!!

Ikiro, Uriel, AlilA
Cat & Jos
14 XII 24

Nachgefragt, immer noch alles i.O.?

Hi Jan!
Nice hearing from you
You are welcome to use my photo in your presentation
And yes, I am a long time fan&advocate of privacy and security. In fact
I even wish people would send each other gpg encrypted emails... (which
I only managed with one correspondent, looong time ago, and with noone else)
I guess you are using only secured mail transport services, therefore,
Definitely
at least in our case, this image has never touched any insecure
transport line neither was there a force to publish this in a dropbox /
facebook storage.
True.
Although it has been published on my children blog as well as being sent
by email.
And while their blog is also accessible by https, I guess most people
used http to access it, so the photo DID travel on unsecure channels as
well
elsewhere, ok, but from our point of view, this was secure)
true
There is another faint idea, if I remember correctly you were running a
own smtp-service via the dsl at your local town in italy, maybe this can
be expanded for a nice secure network scenario ...
I still do operate the smtp (although it's almost never used) and since
that time I also set up my own secure sync services to replace the
google & dropbox operated ones .
I have (together with my own ssh, https, ampache and so on) an owncloud
installation and I sync my android contacts and calendars across all
devices using davdroid connected to that owncloud.
I can also transfer files using owncloud webdav but I found a better
solution which basically replaced (or complemented) dropbox: encfs
encrypted folders which are kept in sync across all my devices on
multiple platforsm (windows, linux and android) using a combination of
opensource and proprietary software (dropbox, owncloud, foldersync,
encdroid, encfs..)
How were you thinking to expand "for a nice secure network scenario"?
Ciao!
Best,
    Jos
PS: have you tried yet the videogame(s) I designed?

- pgp
- owncloud
- encfs
- NO facebook
- NO dropbox

my bad → hacking my own server

Weiterbildung hilft!
Heinlein Mail Conference 2009

```
smtpd_recipient_restrictions = permit_tls_clientcerts,
        permit_mynetworks,
        permit_sasl_authenticated,
        reject_unauth_destination,
        reject_unlisted_recipient,
        check_sender_access hash:/etc/postfix/access_sender,
        reject_unverified_recipient,
        reject_non_fqdn_sender,
        reject_unknown_sender_domain,
#        reject_unverified_sender,   # auskommentiert aufgrund von der 4. mailserver-konferenz peer heinlein
        reject_multi_recipient_bounce,
        reject_non_fqdn_recipient,
        reject_unknown_recipient_domain,
        reject_rbl_client ix.dnsbl.manitu.net,
        reject_rbl_client zen.spamhaus.org,
         check_policy_service inet:[::1]:10023
```

https://www.heinlein-support.de/slac/film-zur-konferenz-2009

my very bad - lazy certifcate man.

Ausgestellt für

Allgemeiner Name (CN)	weitan.org
Organisation (O)	Richardson & Büren
Organisationseinheit (OU)	<kein Teil des Zertifikats>
Seriennummer	06

Ausgestellt von

Allgemeiner Name (CN)	weitan.org
Organisation (O)	Richardson & Büren
Organisationseinheit (OU)	weitan

Gültigkeitsdauer

Beginnt mit	20.04.2004
Läuft ab am	18.04.2014

Fingerabdrücke

SHA-256-Fingerabdruck	EE:9E:69:F7:EF:82:9C:23:47:43:F8:69:26:D8:60:F9:9A:26:A0:7D:8A:A0:D3:EA:61:9B:6F:EE:8E:C1:24:7E
SHA1-Fingerabdruck	A1:80:E2:88:96:94:70:29:85:05:19:5E:5D:76:C3:6F:EC:2A:2E:03

```
New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES256-GCM-SHA384
Server public key is 1024 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : ECDHE-RSA-AES256-GCM-SHA384
```

Best practice – DNS!

$ dig mx meine-domain.de

$ dig mail.meine-domain.de

$ dig -x 89.89.231.13

```
jan@kranich:~$ dig -x 31.15.66.237

; <<>> DiG 9.9.5-3ubuntu0.4-Ubuntu <<>> -x 31.15.66.237
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19063
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;237.66.15.31.in-addr.arpa.     IN      PTR

;; ANSWER SECTION:
237.66.15.31.in-addr.arpa. 3600 IN      PTR     www.volker-rademacher.de.
```

Open relay check SMTP

http://mxtoolbox.com

✓	SMTP Reverse DNS Mismatch	OK - 80.244.242.139 resolves to weitan.org
✓	SMTP Banner Check	OK - Reverse DNS matches SMTP Banner
✓	SMTP TLS	OK - Supports TLS.
✓	SMTP Connection Time	1.031 seconds - Good on Connection time
✓	SMTP Open Relay	OK - Not an open relay.
✓	SMTP Transaction Time	3.360 seconds - Good on Transaction Time

Check EICAR (Anti-Virus)

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

http://www.eicar.org/86-0-Intended-use.html

Check EICAR (Anti-Spam)

XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X

http://www.eicar.org/86-0-Intended-use.html

Check IMAPs / SMTPs protocol

- openssl s_client

```
openssl s_client -host lvps46-163-78-219.dedicated.hosteurope.de  -port 25 -starttls smtp
```

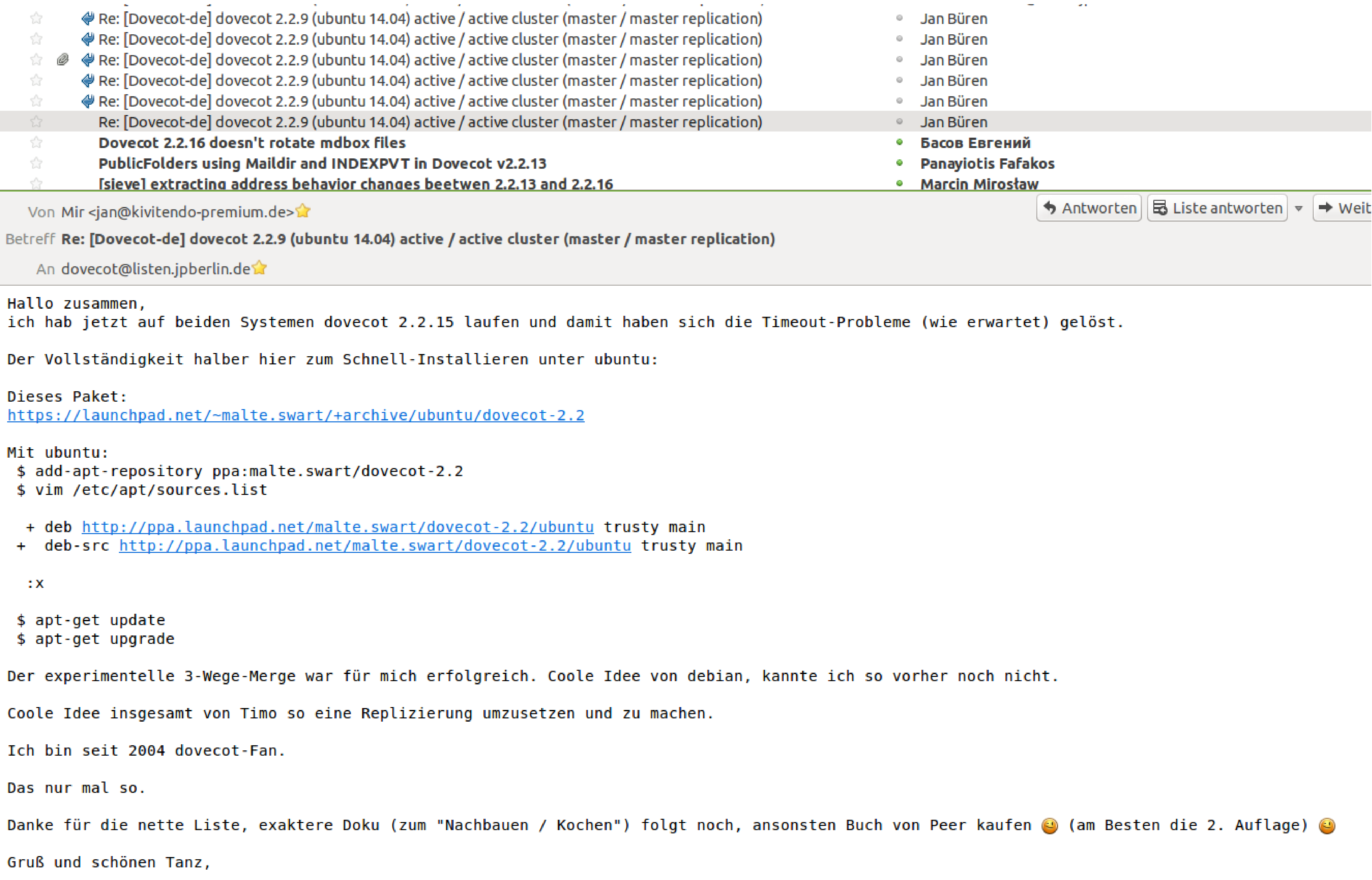
Richardson & Büren

View E-Mail header!!!!

```
Return-Path: <insana@mediaglyphs.org>
X-Original-To: jan@weitan.org
Delivered-To: jan@weitan.org
Received: from localhost (localhost [127.0.0.1])
    by weitan.org (Postfix) with ESMTP id 45D1CE0075;
    Thu, 25 Dec 2014 00:06:03 +0100 (CET)
X-Virus-Scanned: Debian amavisd-new at weitan.org
Received: from weitan.org ([127.0.0.1])
    by localhost (localhost [127.0.0.1]) (amavisd-new, port 10024)
    with ESMTP id w4V+owlezUPn; Thu, 25 Dec 2014 00:06:03 +0100 (CET)
Received: from [192.168.1.44] (unknown [95.233.178.175])
    (using TLSv1 with cipher DHE-RSA-AES128-SHA (128/128 bits))
    (No client certificate requested)
    by weitan.org (Postfix) with ESMTPSA id 44333E006C;
    Thu, 25 Dec 2014 00:05:41 +0100 (CET)
Message-ID: <549B46C9.4090309@mediaglyphs.org>
Date: Thu, 25 Dec 2014 00:05:45 +0100
From: Dr Giuseppe Insana <insana@mediaglyphs.org>
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Thunderbird/31.3.0
MIME-Version: 1.0
To: undisclosed-recipients:;
Subject: For a wonderful new year
OpenPGP: id=CD84801E;
    url=http://www.insana.net/i/contact.html
Content-Type: multipart/signed; micalg=pgp-sha256;
 protocol="application/pgp-signature";
 boundary="7RjelnE87roljMnq9t6xLt5JtqrwnJnwI"

This is an OpenPGP/MIME signed message (RFC 4880 and 3156)
--7RjelnE87roljMnq9t6xLt5JtqrwnJnwI
Content-Type: multipart/mixed;
```

Mailinglisten



Re: [Dovecot-de] dovecot 2.2.9 (ubuntu 14.04) active / active cluster (master / master replication)	Jan Büren
Re: [Dovecot-de] dovecot 2.2.9 (ubuntu 14.04) active / active cluster (master / master replication)	Jan Büren
Re: [Dovecot-de] dovecot 2.2.9 (ubuntu 14.04) active / active cluster (master / master replication)	Jan Büren
Re: [Dovecot-de] dovecot 2.2.9 (ubuntu 14.04) active / active cluster (master / master replication)	Jan Büren
Re: [Dovecot-de] dovecot 2.2.9 (ubuntu 14.04) active / active cluster (master / master replication)	Jan Büren
Re: [Dovecot-de] dovecot 2.2.9 (ubuntu 14.04) active / active cluster (master / master replication)	Jan Büren
Dovecot 2.2.16 doesn't rotate mdbox files	**Басов Евгений**
PublicFolders using Maildir and INDEXPVT in Dovecot v2.2.13	**Panayiotis Fafakos**
[sieve] extracting address behavior changes beetwen 2.2.13 and 2.2.16	**Marcin Mirosław**

Von Mir <jan@kivitendo-premium.de>

Betreff **Re: [Dovecot-de] dovecot 2.2.9 (ubuntu 14.04) active / active cluster (master / master replication)**

An dovecot@listen.jpberlin.de

Hallo zusammen,
ich hab jetzt auf beiden Systemen dovecot 2.2.15 laufen und damit haben sich die Timeout-Probleme (wie erwartet) gelöst.

Der Vollständigkeit halber hier zum Schnell-Installieren unter ubuntu:

Dieses Paket:
https://launchpad.net/~malte.swart/+archive/ubuntu/dovecot-2.2

Mit ubuntu:

```
 $ add-apt-repository ppa:malte.swart/dovecot-2.2
 $ vim /etc/apt/sources.list

  + deb http://ppa.launchpad.net/malte.swart/dovecot-2.2/ubuntu trusty main
 +  deb-src http://ppa.launchpad.net/malte.swart/dovecot-2.2/ubuntu trusty main

  :x

 $ apt-get update
 $ apt-get upgrade
```

Der experimentelle 3-Wege-Merge war für mich erfolgreich. Coole Idee von debian, kannte ich so vorher noch nicht.

Coole Idee insgesamt von Timo so eine Replizierung umzusetzen und zu machen.

Ich bin seit 2004 dovecot-Fan.

Das nur mal so.

Danke für die nette Liste, exaktere Doku (zum "Nachbauen / Kochen") folgt noch, ansonsten Buch von Peer kaufen 🙂 (am Besten die 2. Auflage) 🙂

Gruß und schönen Tanz,

Dovecot imaps only

```
service imap-login {
  inet_listener imap {
    port = 0
  }
}
```

```
  inet_listener imaps {
    #port = 993
    #ssl = yes
  }
```

Postfix smtps (starttls) only

```
#sasl
smtpd_sasl_auth_enable = yes
smtpd_sasl_local_domain =
broken_sasl_auth_clients = yes
smtpd_sasl_security_options = noanonymous
smtpd_sasl_type = dovecot
smtpd_sasl_path = private/auth
smtpd_use_tls=yes
```

Dovecot active / active cluster tcps

```
service replicator {
  process_min_avail = 1
  unix_listener replicator-doveadm {
    mode = 0660
    group = vmail
  }
}

service doveadm {
  inet_listener {
    port = 7070
    ssl = yes
  }
}
```

netstat -plunt

```
(Für "-p": geteuid()=1000 konnte keine Information gelesen werden; sie sollten Root sein.)
Aktive Internetverbindungen (Nur Server)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:5432          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:25              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:7070            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:4190            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:993             0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:10023         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:10024         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:10025         0.0.0.0:*               LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       0      0 :::25                   :::*                    LISTEN      -
tcp6       0      0 :::443                  :::*                    LISTEN      -
tcp6       0      0 :::7070                 :::*                    LISTEN      -
tcp6       0      0 :::4190                 :::*                    LISTEN      -
tcp6       0      0 :::993                  :::*                    LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
```

Richardson & Büren

10 Jahre Erfahrung - Fazit

- Postfix (1.x → 2.x)
- Dovecot (0.99beta → 2.2.15)
- Amavis
- Spamassassin
- Squirrelmail → Roundcube
- Procmail → Sieve
- Keine relationale DB → max. LDAP

Richardson & Büren

Meine 2 Cent / Tipps

- Kein LDA (Local Delivery Agent)
  → **LMTP** (Light Message Transport Protocol)
- Lokal nur unix_listener (postfix ↔ dovecot)
- Keine SQL-DB für Nutzer!
- **Keine Postfix Nutzerverwaltung!!!!**
  → auch keine system user (root)

Weiterführende Links und empfehlenswerte HowTos ….

https://www.exratione.com/2014/05/a-mailserver-on-ubuntu-1404-postfix-dovecot-mysql/

http://blog.serverbiz.de/debian-hostname-dauerhaft-andern-fqdn-anpassen

http://www.postfix.org/

http://www.dovecot.org

http://www.dovecot-buch.de/

http://spamassassin.apache.org/

https://www.heinlein-support.de/blog/news/aktuelle-spamassassin-regeln-von-heinlein-support

https://help.ubuntu.com/community/PostfixAmavisNew

http://www.unixwitch.de/de/sysadmin/tools/imap-mit-ssl-testen

postconf -n

```
rademacher@www:~$ postconf -n
alias_database = hash:/etc/aliases
alias_maps = hash:/etc/aliases
append_dot_mydomain = no
biff = no
bounce_size_limit = 70000
broken_sasl_auth_clients = yes
config_directory = /etc/postfix
content_filter = smtp-amavis:127.0.0.1:10024
header_size_limit = 402400
inet_interfaces = all
inet_protocols = all
mailbox_size_limit = 0
message_size_limit = 140240000
mydestination = localhost
myhostname = www.meinedomain.de
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
myorigin = /etc/mailname
readme_directory = no
recipient_delimiter = +
relay_domains = hash:/etc/postfix/relay_domains
relayhost =
smtp_tls_mandatory_protocols = !SSLv2 !SSLv3
smtp_tls_protocols = !SSLv2, !SSLv3
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache
```

postconf -n

```
smtpd_recipient_restrictions = permit_tls_clientcerts, permit_mynetworks,
permit_sasl_authenticated, reject_unauth_destination, reject_unlisted_recipient,
reject_unverified_recipient, reject_non_fqdn_sender, reject_unknown_sender_domain,
reject_multi_recipient_bounce, reject_non_fqdn_recipient, reject_unknown_recipient_domain,
reject_rbl_client ix.dnsbl.manitu.net, reject_rbl_client zen.spamhaus.org, check_policy_service
inet:127.0.0.1:10023
smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated defer_unauth_destinatior
smtpd_sasl_auth_enable = yes
smtpd_sasl_local_domain =
smtpd_sasl_path = private/auth
smtpd_sasl_security_options = noanonymous
smtpd_sasl_type = dovecot
smtpd_tls_cert_file = /etc/ssl/certs/www.snakeoil.pem
smtpd_tls_key_file = /etc/ssl/private/www.snakeoil.key
smtpd_tls_mandatory_protocols = !SSLv2 !SSLv3
smtpd_tls_protocols = !SSLv2 !SSLv3
smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache
smtpd_use_tls = yes
soft_bounce = no
strict_rfc821_envelopes = yes
transport_maps = hash:/etc/postfix/transport, $relay_domainssmtpd_banner = $myhostname
ESMTP $mail_name (Ubuntu)
smtpd_data_restrictions = reject_multi_recipient_bounce, reject_unauth_pipelining
```

Postfix master.conf

```
# 10025 is the port that amavis sends to after checking
127.0.0.1:10025         inet n  -       n       -       10      smtpd   -o content_filter=    -o
local_recipient_maps=   -o receive_override_options=no_address_mappings
#postfix amavis
smtp-amavis unix -      -       n       -       2       smtp    -o smtp_data_done_timeout=1200 -o
smtp_send_xforward_command=yes   -o disable_dns_lookups=yes
```

doveconf -n

```
# 2.2.15: /etc/dovecot/dovecot.conf
# Pigeonhole version 0.4.6 (3e924b1b6c5c+)
# OS: Linux 3.13.0-62-generic x86_64 Ubuntu 14.04.3 LTS
auth_mechanisms = plain login
doveadm_password = sehrgeheimmein
doveadm_port = 7070
mail_location = maildir:~/Maildir
mail_plugins = " notify replication"
managesieve_notify_capability = mailto
managesieve_sieve_capability = fileinto reject envelope encoded-character vacation
subaddress comparator-i;ascii-numeric relational regex imap4flags copy include
variables body enotify environment mailbox date ihave duplicate
```

doveconf -n

```
namespace inbox {
  inbox = yes
  location =
  mailbox Drafts {
    special_use = \Drafts
  }
  mailbox Junk {
    special_use = \Junk
  }
  mailbox Sent {
    special_use = \Sent
  }
  mailbox "Sent Messages" {
    special_use = \Sent
  }
  mailbox Trash {
    special_use = \Trash
  }
  prefix =
}
passdb {
  args = scheme=CRYPT username_format=%Lu /etc/dovecot/users
  driver = passwd-file
}
```

doveconf -n

```
plugin {
  mail_replica = tcps:intern.meinedomain.de
  sieve = file:~/sieve;active=~/.dovecot.sieve
  sieve_before = /var/vmail/sieve/spam-global.sieve
}
protocols = " imap lmtp sieve"
replication_max_conns = 4
service aggregator {
  fifo_listener replication-notify-fifo {
    user = vmail
  }
  unix_listener replication-notify {
    user = vmail
  }
}
service auth {
  unix_listener /var/spool/postfix/private/auth {
    mode = 0666
  }
  unix_listener auth-userdb {
    mode = 0777
  }
}
```

doveconf -n

```
service doveadm {
  inet_listener {
    port = 7070
    ssl = yes
  }
}
service imap-login {
  inet_listener imap {
    port = 0
  }
}
service lmtp {
  unix_listener /var/spool/postfix/private/lmtp-dovecot {
    group = postfix
    user = postfix
  }
}
service replicator {
  process_min_avail = 1
  unix_listener replicator-doveadm {
    group = vmail
    mode = 0660
  }
}
```

doveconf -n

```
ssl_ca = </etc/ssl/certs/www.meinedomain.de-intermediate.crt
ssl_cert = </etc/ssl/certs/www.meinedomain.de.crt
ssl_client_ca_dir = /etc/ssl/certs
ssl_key = </etc/ssl/private/www.meinedomain.de.key
ssl_protocols = !SSLv2 !SSLv3
userdb {
  args = username_format=%Lu /etc/dovecot/users
  driver = passwd-file
}
protocol lmtp {
  mail_plugins = " notify replication sieve replication"
  postmaster_address = postmaster@localhost
}
```

Amavisd-new

```
use strict;

# You can modify this file to re-enable SPAM checking through
spamassassin
# and to re-enable antivirus checking.

#
# Default antivirus checking mode
# Please note, that anti-virus checking is DISABLED by
# default.
# If You wish to enable it, please uncomment the following lines:


@bypass_virus_checks_maps = (
   \%bypass_virus_checks, \@bypass_virus_checks_acl, \
$bypass_virus_checks_re);

# Default SPAM checking mode
# Please note, that anti-spam checking is DISABLED by
@bypass_spam_checks_maps = (
   \%bypass_spam_checks, \@bypass_spam_checks_acl, \
$bypass_spam_checks_re);
```

Anhang / Nachtrag

Empfehlungen aus dem Publikum:

- https://bettercrypto.org
- https://www.ssllabs.com/

reject_unverified_sender (backscatter-Problematik besser erklärt):

- http://www.backscatterer.org/?target=sendercallouts
- http://www.postfix.org/BACKSCATTER_README.html#wtf