zentraler informatik dienst

universität wien

EHLO

November 2012

Wolfgang Breyha

zentraler informatik dienst

universität wien

SPAM Workshop Teil 1

Vorstellung:

- Wolfgang Breyha
- root am ZID der Universität Wien
- Verantwortlich für Entwicklung und Betrieb des Linux Mailsystems

zentraler informatik dienst

universität wien

Mailsystem der Universität Wien

- ~ 80.000 Mailboxen
- Exim mit LDAP routing
    - 4 MX, 3 MSA, 1 relay
- Cyrus Murder
    - 3 frontends, 6 backends (~25TB)
- IPv6 enabled (seit 2006)
- ~600.000 Connections/Tag
- ~150.000 Mails/Tag

Was kommt nun auf Sie/Dich zu?

Themenüberblick

- SMTP/Submission
- Mailserver Setup – DNS, Ports, IPv6, ...
- best practices
- ESMTP – die wichtigsten/gängisten Erweiterungen

DNS Basics

- A Resource Record (RR):
  fqdn => IPv4

```
# host -t a zidmx1.univie.ac.at
zidmx1.univie.ac.at has address 131.130.3.100
```

- PTR RR:
  IP => fqdn

```
# host -t ptr 131.130.3.100
100.3.130.131.in-addr.arpa domain name pointer ray.univie.ac.at.
```

- MX RR:
  mail domain => fqdn

```
# host -t mx univie.ac.at
univie.ac.at mail is handled by 10 zidmx1.univie.ac.at.
```

- AAAA RR
  fqdn => Ipv6

```
# host -t aaaa zidmx1.univie.ac.at
zidmx1.univie.ac.at has IPv6 address 2001:62a:4:25::25:100
```

```
# host -t ptr 2001:62a:4:25::25:100
0.0.1.0.5.2.0.0.0.0.0.0.0.0.0.0.5.2.0.0.4.0.0.0.a.2.6.0.1.0.0.2.ip6.arpa
domain name pointer zidmx1.univie.ac.at.
```

- CNAME RR
  fqdn => fqdn

... besser kein Beispiel;-)

SMTP - Grundlagen

```
$ telnet zidmx1.univie.ac.at 25
Trying 2001:62a:4:25::25:100...
Connected to zidmx1.univie.ac.at.
Escape character is '^]'.
220 ray.univie.ac.at ESMTP Exim 4.77 Fri, 13 Apr 2012 23:09:43 +0200
EHLO pcwb.cc.univie.ac.at
250-ray.univie.ac.at Hello pcwb.cc.univie.ac.at [2001:62a:4:202::193]
250-SIZE 52428800
250-DSN
250-PIPELINING
250-STARTTLS
250 HELP
MAIL FROM:<wolfgang.breyha@univie.ac.at>
250 OK
RCPT TO:<echo@univie.ac.at>
250 Accepted
DATA
354 Enter message, ending with "." on a line by itself
Subject: Test

Test
.
250 OK id=1SInm8-00053F-1X
QUIT
221 ray.univie.ac.at closing connection
Connection closed by foreign host.
```

Befehle und Antworten

- Befehle:
  EHLO, MAIL FROM, RCPT TO, DATA,
  QUIT, VRFY, ETRN, RSET, NOOP

- Antworten – Statuscodes
  2xx ok
  3xx intermediate ok (zB. DATA)
  4xx temporary error
  5xx permanent error

HELO/EHLO <FQDN>

```
HELO => keine Erweiterungen
EHLO <host.domain.tld>
EHLO [131.130.3.100]
EHLO [IPv6:2001:62a:4:25::25:100]
```

ganz falsch

```
EHLO <server fqdn>
EHLO <server ip>
```

Adresskommandos

```
MAIL FROM:<blafasel@blafasel.at>
250 OK

MAIL FROM:<>
250 OK

RCPT TO:<blafasel@blafasel.at>
250 Accepted

VRFY <blafasel@blafasel.at>
250 <blafasel@blafasel.at> is deliverable
....
252 Administrative prohibition

EXPN blafasel@blafasel.at
250-<adr1@blafasel.at>
250 <adr2@blafasel.at>
```

sonstige Kommandos

```
RSET
250 OK

NOOP bla
250 OK

QUIT
221 joan.univie.ac.at closing connection
```

Schwachpunkte

- unauthentizierte submission
- authorization auf IP- und Mailadressen Basis

RFC 4409 – Message Submission

- Port 587 statt 25
- verpflichtende Unterstützung für Authentizierung
- darf fehlende Header ergänzen
- funktioniert auch bei port 25 Blockade in Fremdnetzen
- spezialisierbar auf MUA Bedürfnisse
- Trennung MSA und MTA generell von Vorteil

- im Unterschied zu 2010 mittlerweile meistens unterstützt in .at

Mailrouting Basics

- MX lookup auf Domain der Empfängeradresse
  - wenn CNAME, dann Antwort übernehmen und weitersuchen
  - wenn MX RR(s) dann Zustellung nach Priorität gereiht
    Vorsicht vor Einträgen wie 127.0.0.1, ::1
- kein MX Record, dann A RR lookup und Zustellung

robustness principle vs. SPAM

- RFC 761:
  Be conservative in what you do;
  be liberal in what you accept from others.
- Interessenskonflikt mit Spamfiltern
- “liberal” für Mailserver kaum mehr zutreffend
- Fehler im Setup führen unweigerlich zu Problemen
- schlechtesten Falls lange Zeit unbemerkt
- www.rfc-ignorant.org als Leitfaden

Mailhost Setup

- Hostname
  - generischer Name: mail, mx01....
  - freies Namenschema mit aliases
- IP => PTR => FQDN => A => IP stimmig
- Keine CNAMEs!
- Alternativ weitere A RRs
  mail.domain.tld => 1.2.3.4 => FQDN
  zB: zidmx1.univie.ac.at => 131.130.3.100 => ray.univie.ac.at
- client HELO immer mit (externem) FQDN

MX Records

- keine MX RRs auf CNAMEs!
- secondary MX nicht mehr zweckmäßig
- besser mehrere gleichrangige MX hosts
  oder load balancer
- jeder MX host muß alle lokalen User verifizieren können
  (LDAP, DB, callouts, ...)

SMTP behaviour

- queues immer vom selben host abarbeiten lassen
- keine late bounces
    - annehmen wenn Zustellbarkeit sichergestellt oder
    - ablehnen
    - bei relaying recipient verification mittels SMTP callouts
- sender verification callouts sind “unfreundlich”
- großzügig definierte timeouts einhalten
- Queueruns auf greylisting abstimmen

Firewalls vs. Mailserver

- Vertrauensproblem Netzwerker <=> Mailadmin?
- Layer 7 extrem problematisch (zB. CISCO “fixups”)
    - schränken Extensions ein
    - kein STARTTLS
    - schwer zu debuggen bei Problemen (zB. DKIM)

logging & Visualisierung / monitoring

- keine Inhalte (auch kein Subject)
- sinnvolle technische Daten loggen
- “on the fly” auswerten und aufbereiten
- aussagekräftige Grafiken

- ausgehende IP auf DNSBL?

  http://multirbl.valli.org/

IPv6 Erfahrungen

- September 2008: 62 unique hosts
- Mai 2009: 210 unique hosts
- März 2010: 454 unique hosts
- April 2012: 406 unique hosts
- selbst Profis machen alte Fehler

Neuerungen RFC 2821->5321

- submission auf port 587 empfohlen
- 550 am Ende von DATA offiziell erlaubt
- Schutz gegen Harvester erlaubt
- Bounce Vermeidung wird nahegelegt

http://blog.mailchannels.com/2008/10/update-to-email-standards.html

http://tools.ietf.org/rfcdiff?url1=rfc2821&url2=rfc5321

zentraler informatik dienst

universität wien

Pause?!

swaks

- Swiss Army Knife SMTP – Testfälle leicht gemacht
  http://jetmore.org/john/code/swaks/

```
$ ./swaks -q rcpt -f mash@funkzwerg.blafasel.at  -t wb@univie.ac.at
=== Trying zidmx1.univie.ac.at:25...
=== Connected to zidmx1.univie.ac.at.
<-  220 ray.univie.ac.at ESMTP Exim 4.77 Sun, 15 Apr 2012 15:46:24 +0200
 -> EHLO mash
<-  250-ray.univie.ac.at Hello funkzwerg.blafasel.at [131.130.7.186]
<-  250-SIZE 52428800
<-  250-8BITMIME
<-  250-DSN
<-  250-PIPELINING
<-  250-STARTTLS
<-  250 HELP
 -> MAIL FROM:<mash@funkzwerg.blafasel.at>
<-  250 OK
 -> RCPT TO:<wb@univie.ac.at>
<-  250 Accepted
 -> QUIT
<-  221 ray.univie.ac.at closing connection
=== Connection closed with remote host.
```

SMTP Extensions - ESMTP

- früher eigenständige RFC 1869
- jetzt in RFC 2821/5321 definiert
- Ankündigung über Schlüsselwort in der EHLO Antwort
- zusätzliche Parameter für MAIL und RCPT
- zusätzliche Kommandos

verbreitete Erweiterungen

- "8BITMIME", RFC 1652
- "SIZE", RFC 1870
- "ETRN", RFC 1985
- "ENHANCEDSTATUSCODES“, RFC 2034
- "PIPELINEING", RFC 2920
- "STARTTLS, RFC 3207
- "AUTH", RFC 4954

"8BITMIME", RFC 1652

- EMail default = 7Bit
- ermöglicht MIME-Messages in 8Bit Transfer Encoding
- Server verpflichtet sich Übersetzung 8->7 Bit zu unterstützen. Optional 7->8Bit.
- gespaltene Welt “8bit clean” vs. “8bitMIME”
  http://cr.yp.to/smtp/8bitmime.html
- exim?
  http://bugs.exim.org/show_bug.cgi?id=817

```
EHLO ymir.claremont.edu
250-dbc.mtview.ca.us says hello
250 8BITMIME
MAIL FROM:<ned@ymir.claremont.edu> BODY=8BITMIME
```

"SIZE", RFC 1870

- SIZE [max. Mailgröße]
- MAIL Parameter SIZE=<vermutliche Mailgröße>
- ermöglicht reject bevor Daten übertragen wurden
- ermöglicht individuellen reject pro Empfänger

```
EHLO ymir.claremont.edu
250 SIZE 1000000
MAIL FROM:<ned@thor.innosoft.com> SIZE=500000
```

"ETRN", RFC 1985

- startet queuerun auf Server
- früher oft verwendet mit secondary MX/dial up setup
- ETRN <domain>, ETRN @<domain>

```
EHLO ymir.claremont.edu
250 ETRN
ETRN @blafasel.at
250 Ok
```

"ENHANCEDSTATUSCODES, RFC 2034/3463

- Server antwortet für alle 2xx, 4xx und 5xx mit erweiterten Statuscodes im Format “x.y.z”.
- Die Kategorie (1. Stelle) der alten Codes wird beibehalten.
- Codes wie in RFC 3463 definiert

```
EHLO bla.blafasel.at
250-mx0.gmx.net GMX Mailservices
250 ENHANCEDSTATUSCODES
mail from:<>
250 2.1.0 ok {mx088}
```

RFC 3463 Beispiele

5.1.1 Bad destination mailbox address

5.2.2 Mailbox full

5.2.3 Message length exceeds administrative limit.

4.4.1 No answer from host

5.5.2 Syntax error

5.5.4 Invalid command arguments

"PIPELINEING", RFC 2920

- erlaubt “command grouping”

```
C: EHLO dbc.mtview.ca.us
S: 250-innosoft.com
S: 250 PIPELINING
C: MAIL FROM:<mrose@dbc.mtview.ca.us>
C: RCPT TO:<dan@innosoft.com>
C: RCPT TO:<kvc@innosoft.com>
C: DATA
S: 250 sender <mrose@dbc.mtview.ca.us> OK
S: 250 recipient <dan@innosoft.com> OK
S: 250 recipient <kvc@innosoft.com> OK
S: 354 enter mail, end with line containing only "."
  ...
C: .
C: QUIT
S: 250 message sent
S: 221 goodbye
```

"STARTTLS, RFC 3207

- stellt eine SSL/TLS Verbindung her
- Ersatz für implizites SSL auf port 465
- zum Testen:

```
openssl s_client -connect mail.univie.ac.at:25 -starttls smtp
gnutls-cli -p 25 -s mail.univie.ac.at
smtptest -p 587 -t "" mail.univie.ac.at
swaks -tls -p 25 -s mail.univie.ac.at -q TLS
```

"AUTH", RFC 4954

- essentiell für Message Submission

```
250-joan.univie.ac.at Hello funkzwerg.blafasel.at [131.130.7.186]
250-STARTTLS
250-AUTH=LOGIN
250 AUTH LOGIN PLAIN
```

- clear text nur nach STARTTLS verpflichtend
- PLAIN over TLS ist verpflichtend

noch mehr Extensions

- "CHECKPOINT", RFC 1845
- "DELIVERBY", RFC 2852
- "DSN", RFC 3461
- "MTRK", RFC 3885
- "UTF8SMTP", RFC 5336
- Lemonade, RFC 4550
    - "CHUNKING"/"BINARYMIME", RFC 3030
    - "BURL", RFC 4468

"CHECKPOINT", RFC 1845

```
C: EHLO ymir.claremont.edu
S: 250-dbc.mtview.ca.us says hello
S: 250 CHECKPOINT
C: MAIL FROM:<ned@ymir.claremont.edu> TRANSID=<12345@claremont.edu>
S: 355 6135 is the transaction offset
C: DATA
S: 354 Send previously checkpointed message starting at octet 6135
C: <message data minus first 6135 octets sent>
```

"DELIVERBY", RFC 2852

```
C: EHLO bigbiz.com
S: 250-acme.net
S: 250 DELIVERBY
C: MAIL FROM:<eljefe@bigbiz.com> BY=120;R
S: 250 <eljefe@bigbiz.com> sender ok
```

"DSN" – Delivery Status Notifications, RFC 3461
"MTRK", RFC 3885

- Nur bedingt nützlich, weil durchgehender end2end Support notwendig

"UTF8SMTP", RFC 5336

- MAIL FROM/RCPT TO in UTF8 möglich
- downgrade auf ALT-ADDRESS falls vorhanden

"CHUNKING"/"BINARYMIME", RFC 3030

```
S: EHLO ymir.claremont.edu
R: 250-cnri.reston.va.us says hello
R: 250-PIPELINING
R: 250-BINARYMIME
R: 250 CHUNKING
S: MAIL FROM:<ned@ymir.claremont.edu> BODY=BINARYMIME
S: RCPT TO:<gvaudre@cnri.reston.va.us>
S: RCPT TO:<jstewart@cnri.reston.va.us>
R: 250 <ned@ymir.claremont.edu>... Sender and BINARYMIME ok
R: 250 <gvaudre@cnri.reston.va.us>... Recipient ok
R: 250 <jstewart@cnri.reston.va.us>... Recipient ok
S: BDAT 100000
S: (First 10000 octets of canonical MIME message data)
S: BDAT 324
S: (Remaining 324 octets of canonical MIME message data)
S: BDAT 0 LAST
R: 250 100000 octets received
R: 250 324 octets received
R: 250 Message OK, 100324 octets received
```

"BURL", RFC 4468

```
C: EHLO potter.example.com
S: 250-owlry.example.com
S: 250-8BITMIME
S: 250-BURL imap
S: 250-AUTH PLAIN
S: 250-DSN
S: 250 ENHANCEDSTATUSCODES
C: AUTH PLAIN aGFycnkAaGFycnkAYWNjaW8=
S: 235 2.7.0 PLAIN authentication successful.
C: MAIL FROM:<harry@gryffindor.example.com>
S: 250 2.5.0 Address Ok.
C: RCPT TO:<ron@gryffindor.example.com>
S: 250 2.1.5 ron@gryffindor.example.com OK.
C: BURL imap://harry@gryffindor.example.com/outbox
        ;uidvalidity=1078863300/;uid=25;urlauth=submit+harry
        :internal:91354a473744909de610943775f92038 LAST
S: 250 2.5.0 Ok.
```

zentraler informatik dienst

universität wien

Fragen?