Linuxwochen 2006 - Eisenstadt - 27. Mai

Skalierbares Mailsystem mit Postfix, Cyrus und OpenLDAP

René Pfeiffer

pfeiffer@luchs.at

26. Mai 2006

http://web.luchs.at/, Vienna, AT

You have new mail.

- Email wichtigster Dienst bei ISPs und Firmen
- Email verbraucht mehr und mehr Speicherplatz
- Emailtransport immer mehrstufig
- Emailsysteme wachsen mit den Benutzern
- Emailsysteme müssen flexibel sein

Ausgangspunkt

- proprietärer Mailserver (CommuniGate Pro)
- POP3/IMAP Zugriff auf Mailboxen
- ca. 2500+ aktive Benutzerkonten
- ca. 400 Mailinglisten
- mehr als 80000 Mailtransaktionen pro Tag
- mehr als 20-60 GB Mailvolumen pro Monat

Die Mailtransaktionen sind inklusive Spam und Viren angegeben.

Migration auf Freies System

- Umstellung auf LDAP-Verwaltung

  Anpassungen gleich aufwendig wie die Konfiguration eines neuen Systems

- Vergrößerung des Speicherplatzes

  Umstieg auf Linux Logical Volume Manager (LVM)

- Austausch des Basissystems

  Wechsel der GNU/Linux Distribution aus organisatorischen Gründen

  Wechsel der Hardware (64-Bit Revolution ;)

- Änderungen in der Lizenzpolitik des CGate Pro

Komponenten

- Postfix MTA

  ein Mail Transport Agent für Mail Routing und Mailempfang via ESMTP/SMTP

- Cyrus IMAP

  für Verwaltung der Mailboxen und Export via POP3/IMAPv4

- OpenLDAP
  - eine Master Instanz auf seperatem Server
  - eine Slave Instanz pro abfragendem Server

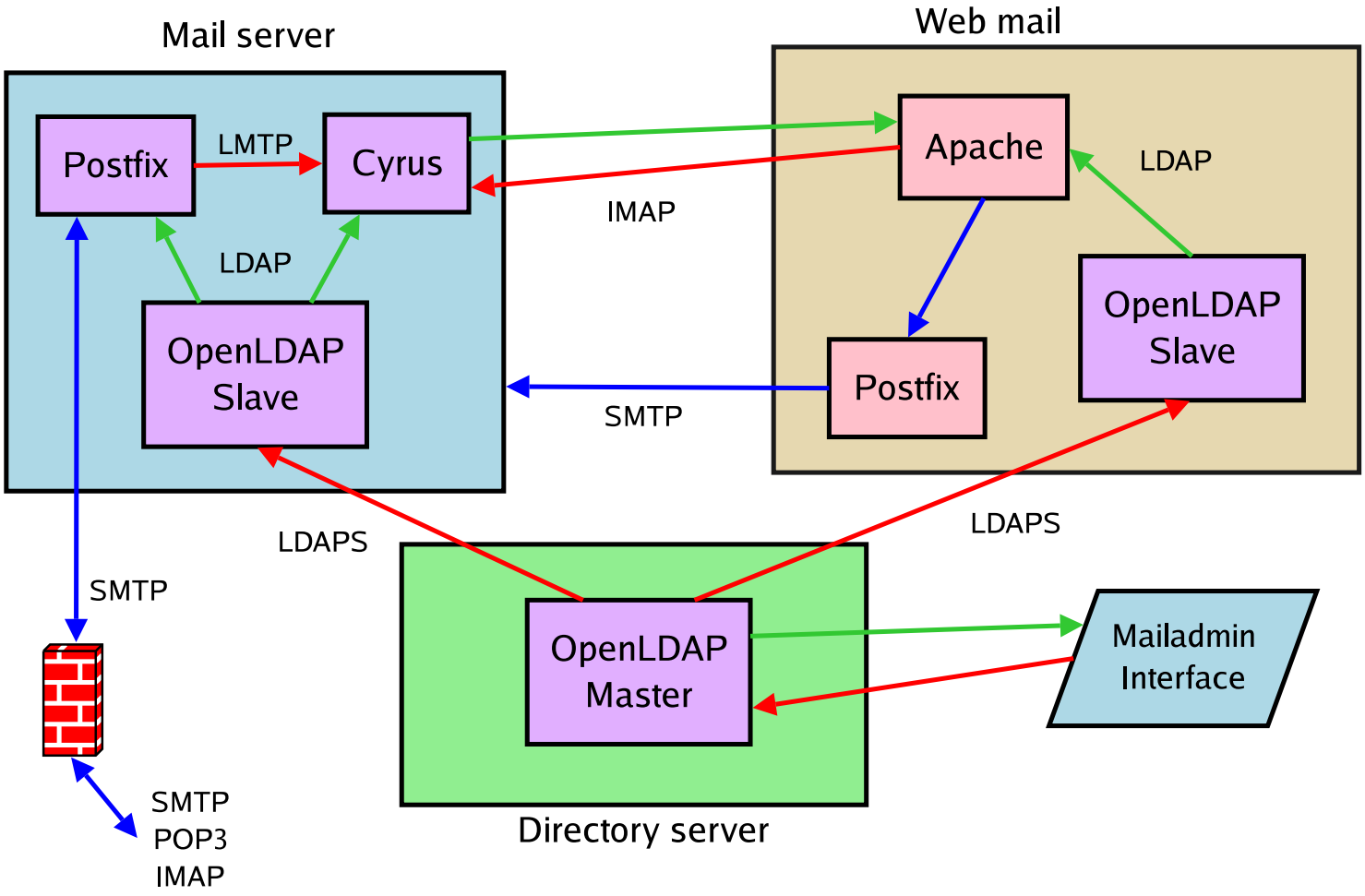
- OpenSSL

  für verschlüsselte Kommunikation der Komponenten via SSLv3/TLS

- Perl

  für Importe und Verwaltung im LDAP Baum

Übersicht Infrastruktur



Vorbereitungen

- Benutzerstruktur in LDAP abbilden

  grundsätzliche Designfragen klären

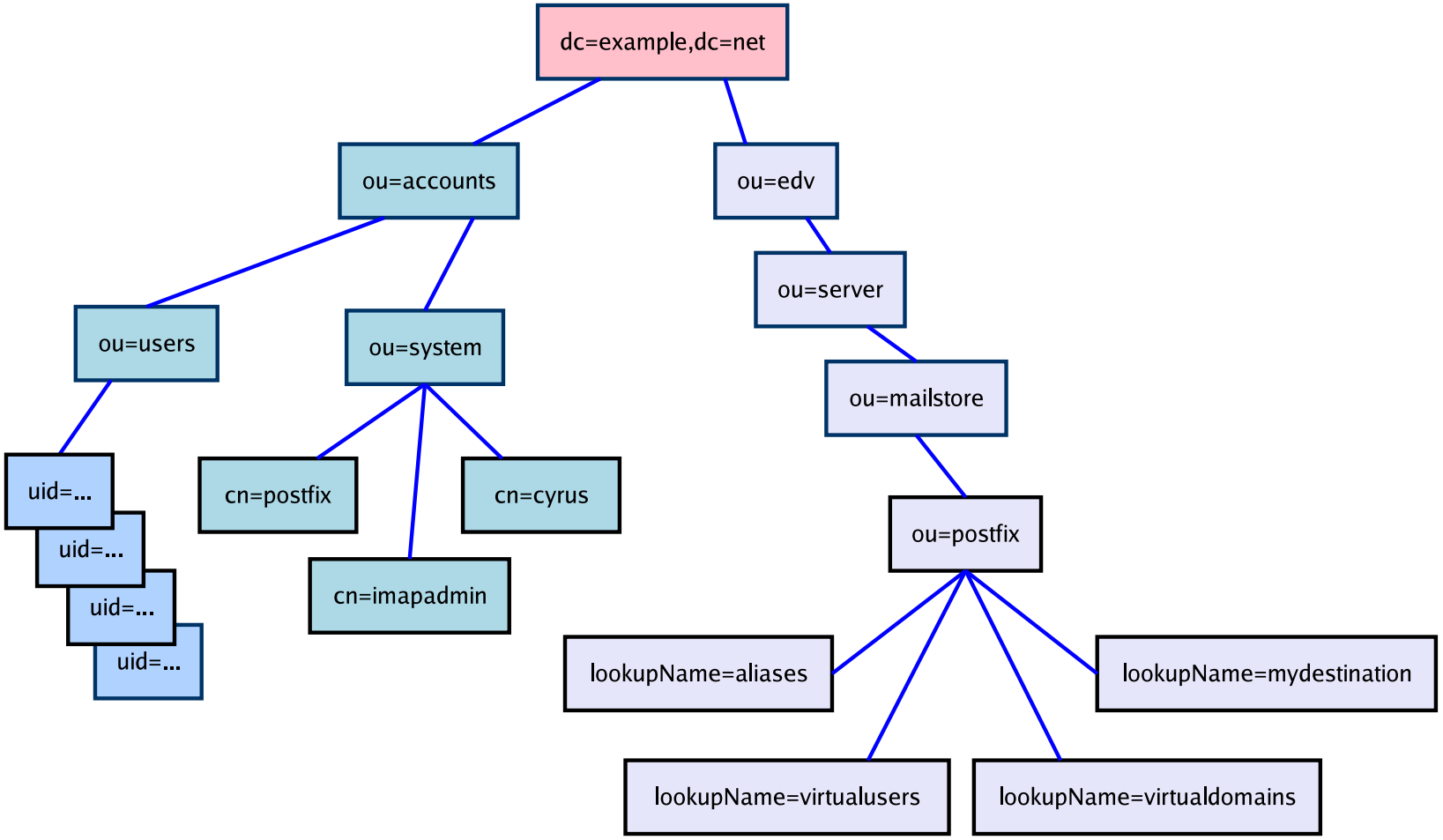
- Benutzerkonten übertragen
  - Logins, Paßworte, Aliase und Mailinglisten liegen am CGate Pro in Textdateien
  - Mailboxen können später mittels IMAP synchronisiert werden

  Perlskripte für die Konfigurationen und Tool `imapsync` für die Mailboxen wurden verwendet.

- eigene Certificate Authority für SSLv3/TLS anlegen

  - OpenSSL bietet alle Werkzeuge dafür
  - Verwaltung der CA mit eigenem Makefile und Subversion

Teil der LDAP Struktur



LDAP-Container für Benutzer

- ou=accounts,dc=example,dc=net
  - ou=system,ou=accounts,dc=example,dc=net
    - cn=cyrus,ou=system,ou=accounts,dc=example,dc=net
    - cn=postfix,ou=system,ou=accounts,dc=example,dc=net
    - cn=webmail,ou=system,ou=accounts,dc=example,dc=net
  - ou=users,ou=accounts,dc=example,dc=net
- ou=edv,dc=example,dc=net
  - ou=server,ou=edv,dc=example,dc=net
    - cn=mailstore,ou=server,ou=edv,dc=example,dc=net
      - cn=postfix,cn=mailstore,ou=server,ou=edv,dc=example,dc=net
        1. lookupName=aliases,cn=postfix,cn=mailstore,ou=server,ou=edv,dc=example,dc=net
        2. lookupName=mydestination,cn=postfix,cn=mailstore,ou=server,ou=edv,dc=example,dc=net
        3. lookupName=virtualdomains,cn=postfix,cn=mailstore,ou=server,ou=edv,dc=example,dc=net
        4. lookupName=virtualusers,cn=postfix,cn=mailstore,ou=server,ou=edv,dc=example,dc=net

Benutzerrepräsentation

- LDAP Objektklassen
  - *account* - Login, Name und Paßwort
  - *greenUser* - zentral für Postfix und Cyrus
  - *pkiUser* - optional für PKI Informationen
  - *posixAccount*, *sambaSamAccount*, *shadowAccount* - optional für lokale Anbindungen
- Benutzer beschrieben durch
  - *cn* - voller Name des Benutzers
  - *mail* - volle Emailadresse
  - *mailAlternateAddress* - Aliasadressen
  - *mailForwardingAddress* - Weiterleitungen von Email
  - *mailQuotaSize* - maximale Größe der Mailbox am Cyrus Server
  - *uid* - Login
  - *userPassword* - das Benutzerpaßwort

greenUser ist eine geringfügige Modifikation des `qmail` LDAP Schemas.

Anbindung des Postfix

- MTAs müssen oft Informationen nachschlagen
  - Informationen über lokale Domains
  - Emailadressen
  - Aliase
  - Mailboxen
  - Weiterleitungen

  „Lookups” oder „lookup table” ist die Abkürzung dafür
- Anbindung an LDAP-Server durch Erweiterung
  - Hauptkonfiguration verweist auf Datei mit LDAP Parametern
  - pro Nachschlagetabelle eine Textdatei
  - LDAP Suchabfragen beliebig konfigurierbar

„Lookups” im Detail

- Postfix Konfiguration für lokale Empfänger

```
local_recipient_maps = ldap:/etc/postfix/local_recipient_maps.cf \
                       $alias_maps \
                       $virtual_alias_maps
```

- Inhalt von `local_recipient_maps.cf`
  - definiert Verbindung zum LDAP Server
  - enthält LDAP Filter für die Suchabfrage

Beispiel: local_recipient_maps.cf

```
server_host = 127.0.0.1
server_port = 389
search_base = ou=users,ou=accounts,dc=example,dc=net
scope       = sub
timeout     = 30
bind        = yes
bind_dn     = cn=postfix,ou=system,ou=accounts,dc=example,dc=net
bind_pw     = XXXXXXXXXXXX
version     = 3

start_tls        = no
tls_ca_cert_file = /etc/ldap/openldap/collected_cas.pem
query_filter     = (&(uid=%u)(accountStatus=aktiv))
result_attribute = mail
```

Kandidaten für Lookup Tabellen

- `alias_maps` - Aliase
- `mydestination` - eigene (Sub)Domains
- `local_recipient_maps` - lokale Empfänger
- `virtual_alias_domains` - Domains mit virtuellen Adressen
- `virtual_alias_maps` - Aliase für virtuelle Adressen

Schema für simple Lookups

- Lookups sind Abbildungen $a \longrightarrow b$
- einfaches LDAP Schema ausreichend
- Definition von zwei neuen Objektklassen
  - *lookupName*
  - *lookupTableEntry*

    führt Abbildung $lookupKey \longrightarrow lookupValue$ durch

Anbindung von Cyrus

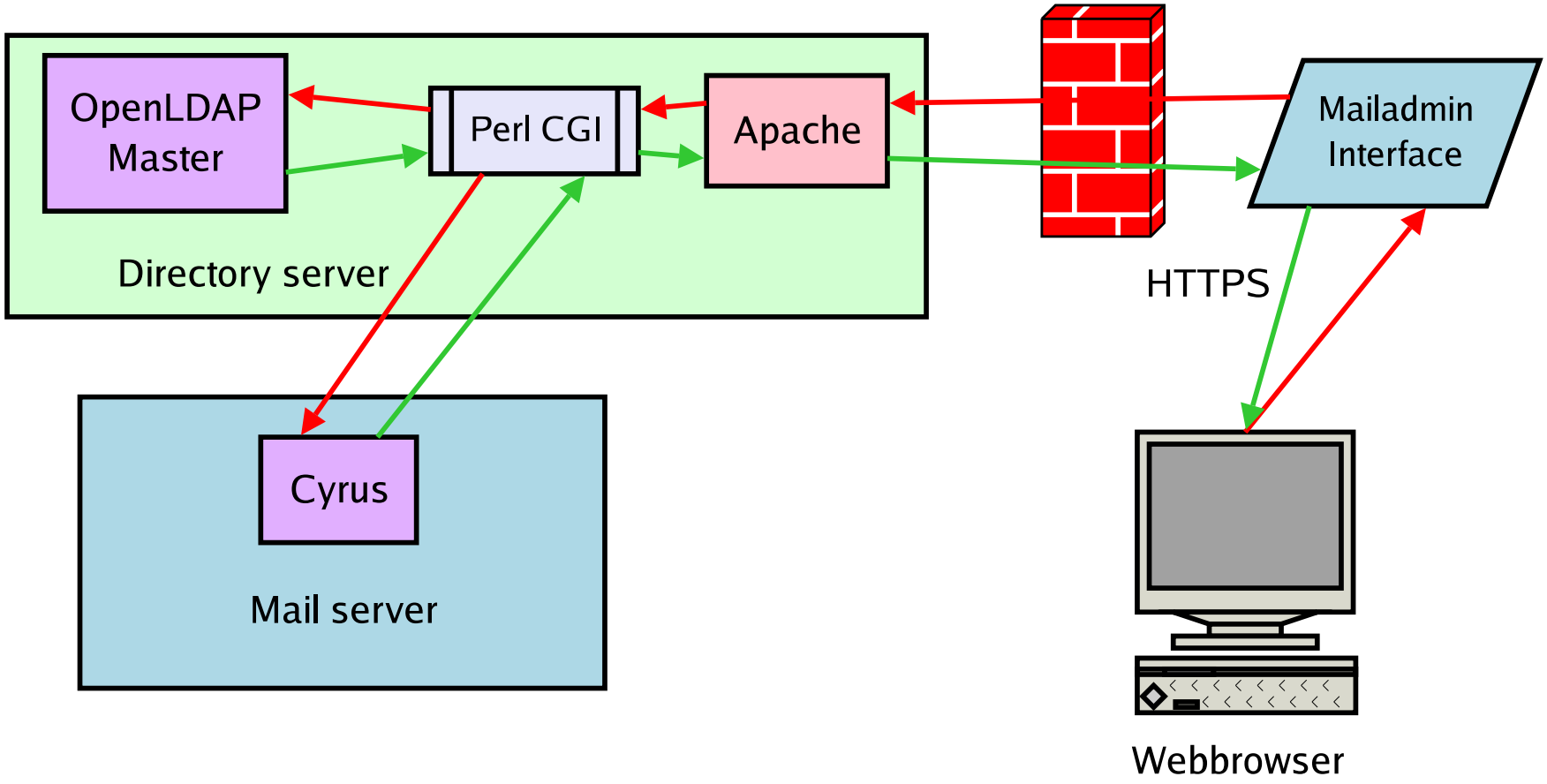
- Cyrus benötigt Login/Paßwort Test
- Cyrus kennt mehrere Authentifizierungen
  - lokale Simple Authentication and Security Layer (SASL) Datenbank
  - LDAP
  - Pluggable Authentication Modules (PAM)
  - Kerberos
- Mailquoten und -boxen verwaltet Cyrus selbst
  - Synchronisierung Quoten und Konten mittels Perlskripte
  - Cyrus biete eigenes CPAN Modul `Cyrus::IMAP`

SASL AUTH mit OpenLDAP

`/etc/saslauthd.conf` benötigt Datenquelle für Login/Paßwort:

```
ldap_servers: ldap://127.0.0.1/
ldap_version: 3
ldap_timeout: 10
ldap_time_limit: 10
ldap_cache_ttl: 30
ldap_cache_mem: 32768
ldap_scope: sub
ldap_search_base: ou=accounts,dc=example,dc=net
ldap_auth_method: custom
ldap_bind_dn: cn=ldaproot,dc=example,dc=net
ldap_password: 6202f430d9c9a97da8d041946847643f
ldap_filter: uid=%U
```

Administratorenzugang



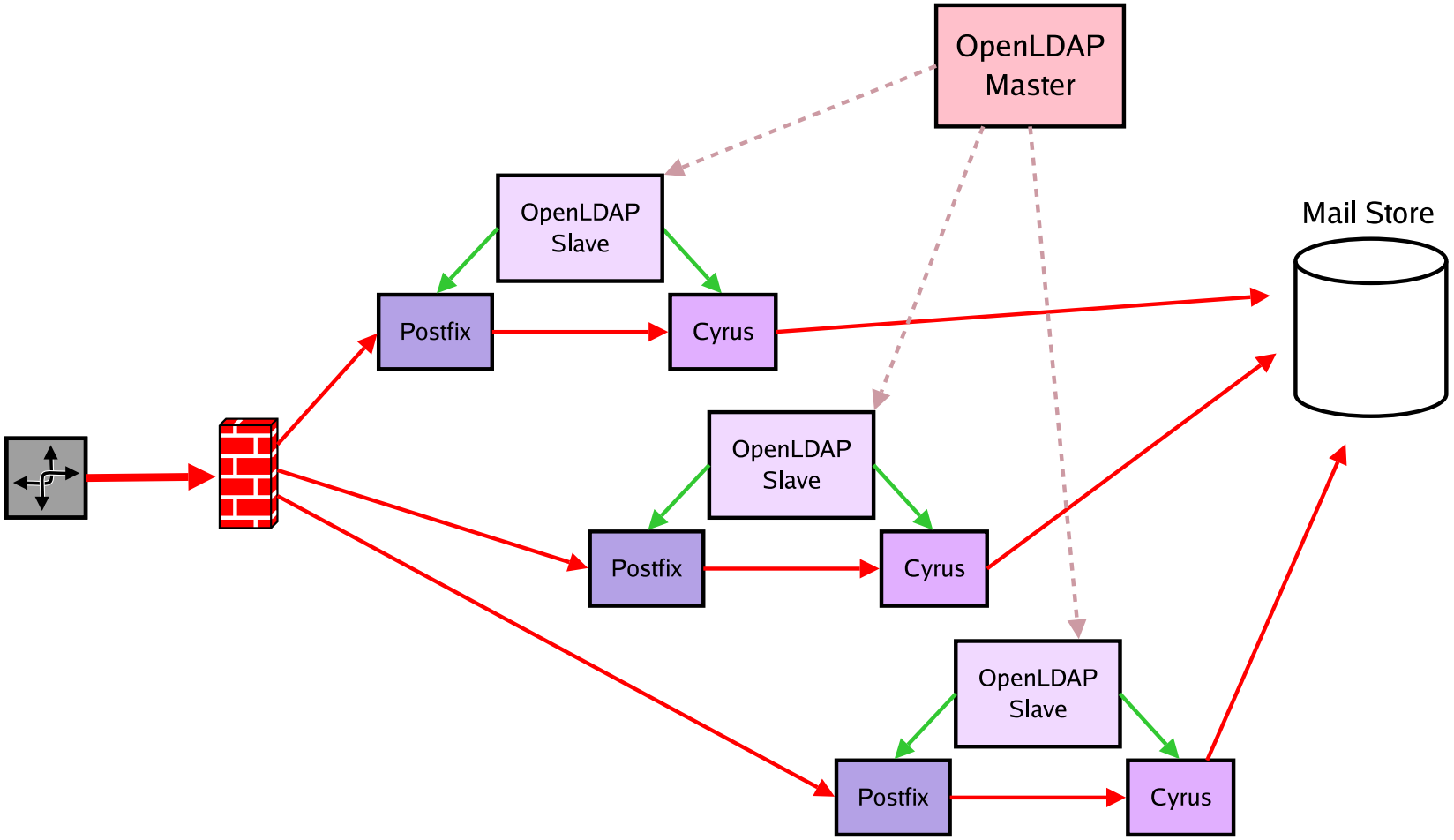
Verbindung Postfix zu Cyrus

- Postfix nimmt Emails vom AV/AS-Filter entgegen
- Postfix dekodiert Aliase und lokale Benutzer
- lokale Mails gehen via LMTP zu Cyrus
- Cyrus speichert Emails in lokale Boxen

Vorzüge des Systems

- komplettes Mailrouting durch LDAP Baum
- sämtliche Konfigurationen im LDAP Baum
- Postfix und Cyrus können daher entkoppeln
- zusätzliche Server leicht zu konfigurieren

Skalierbarkeit



Nützliche Tools

- imapsync *http://www.linux-france.org/prj/imapsync/*
- JXplorer *http://jxplorer.org*
- OpenSSL Certificate Authority Setup *http://sial.org/howto/openssl/ca/*
- phpLDAPadmin *http://phpldapadmin.sourceforge.net/*
- Perl LDAP *http://ldap.perl.org/*
- SmartSieve *http://smartsieve.sourceforge.net/*

Rat für Systemmigrationen

Among the maxims on Lord Naoshige's wall, there was this one: "Matters of great concern should be treated lightly."

Master Ittei commented, "Matters of small concern should be treated seriously."

— *Hagakure*

Über dieses Dokument

- Autor: René Pfeiffer
- Erstellt mit LaTeX und FoilTeX
- Dokumentensammlung unter

  http://web.luchs.at/information/docs.php