Конфигурация на POSTFIX SMTP сървър със SASL автентикация през LDAP сървър

Ивелин Велков
Румен Рачков

София
2008

Съдържание:

Необходими неща

Инсталираме следните пакети:

```
postfix-ldap-2.4.5-2mdv2008.0
postfix-2.4.5-2mdv2008.0
libpostfix1-2.4.5-2mdv2008.0
libsasl2-plug-login-2.1.22-23mdv2008.0
libsasl2-2.1.22-23mdv2008.0
libsasl2-plug-plain-2.1.22-23mdv2008.0
libsasl2-plug-digestmd5-2.1.22-23mdv2008.0
libsasl2-plug-ldapdb-2.1.22-23mdv2008.0
cyrus-sasl-2.1.22-23mdv2008.0
```

Нужно ни е да имаме инсталиран и LDAP сървър.

В този пример използваните LDAP схеми ще са:

```
include /usr/share/openldap/schema/core.schema
include /usr/share/openldap/schema/cosine.schema
include /usr/share/openldap/schema/corba.schema
include /usr/share/openldap/schema/inetorgperson.schema
include /usr/share/openldap/schema/java.schema
include /usr/share/openldap/schema/krb5-kdc.schema
include /usr/share/openldap/schema/kerberosobject.schema
#include        /usr/share/openldap/schema/misc.schema
include /usr/share/openldap/schema/nis.schema
include /usr/share/openldap/schema/openldap.schema
include /usr/share/openldap/schema/autofs.schema
include /usr/share/openldap/schema/samba.schema
include /usr/share/openldap/schema/kolab.schema
include /usr/share/openldap/schema/evolutionperson.schema
include /usr/share/openldap/schema/calendar.schema
include /usr/share/openldap/schema/sudo.schema
include /usr/share/openldap/schema/dnszone.schema
include /usr/share/openldap/schema/dhcp.schema
#include /usr/share/openldap/schema/rfc822-MailMember.schema
#include /usr/share/openldap/schema/pilot.schema
include /usr/share/openldap/schema/qmail.schema
#include /usr/share/openldap/schema/mull.schema
#include /usr/share/openldap/schema/netscape-profile.schema
#include /usr/share/openldap/schema/trust.schema
include /etc/openldap/schema/local.schema
```

схемите които реално използваме са:

- qmail.schema,
- core.schema,
- cosine.schema,
- nis.schema

Използване на schema атрибутите:

- "mail" тук са mail псевдонимите.
- "mailAlternateAddress" тук са истинските мейл адреси.

- "accountStatus" - активен/неактивен mail account
- uid= автентикация на потребител
- userPassword – парола за тази автентикация
- objectClass трябва да съдържа qmailUser

Конфигурация на Postfix

Въведение:

Конфигурационните файлове на Postfix се намират в /etc/postfix. Има два основни конфигурационни файла. Единият е /etc/postfix/master.cf, а другия е /etc/postfix/main.cf.

/etc/postfix/master.cf

Това е таблицата на процесите на Postfix. Всички негови процеси се описват в нея. Обикновенно тя се редактира само ако се дебъгва. За да дебъгвате единична postfix услуга добавете аргумент –v към командата.

Пример:

```
#==========================================================================
# service type  private unpriv  chroot  wakeup  maxproc command + args
#               (yes)   (yes)   (yes)   (never) (100)
#==========================================================================
smtp    inet    n       -       y       -       -       smtpd -v
```

/etc/postfix/main.cf

Виртуални LDAP псевдоними

Тук ще ви предоставим нашите настройки в /etc/postfix/main.cf:

```
virtual_alias_maps = $alias_maps, ldap:/etc/postfix/ldap-aliases.cf
virtual_gid_maps = static:5001
virtual_mailbox_base = /var/spool/mail/
virtual_mailbox_limit = 0
```

и настройките в /etc/postfix/ldap-aliases.cf:

```
[root@ivelin postfix]# cat ldap-aliases.cf
bind = yes
bind_dn = cn=Manager,dc=test,dc=com
bind_pw = secret
version = 3
timeout = 20
size_limit = 1
expansion_limit = 0
start_tls = no
#tls_require_cert = no
server_host = ldap://sveto.active-lynx.com
search_base = ou=accounts,dc=test,dc=com
scope = sub
query_filter = (&(objectClass=qmailUser)(mail=%s)(accountStatus=active))
result_attribute = mailAlternateAddress
special_result_filter=%s@%d
```

virtual_alias_maps (default: $virtual_maps)

Опционални lookup таблици, които дават псевдоним на мейл адрес или домейн към друг локален адрес или домейн. Ако използвате тази възможност подсигурете се че ще пуснете: postmap /etc/postfix/virtual, след като промените файла.

Примери:
virtual_alias_maps = dbm:/etc/postfix/virtual
virtual_alias_maps = hash:/etc/postfix/virtual

virtual_gid_maps (default: empty)

Lookup таблици с получателското group id за virtual mailbox получаванията. В lookup таблицата, посочете "@domain.tld" отляво да се мачва с потребител в домейна, който няма веведен "user@domain.tld".

virtual_mailbox_base (default: empty)

Указва къде да отиват mailboховете. Това е от причини за сигурност за да се подсигурим че няма да се пръснат навсякъде из файловата система.

Пример: virtual_mailbox_base = /var/mail

virtual_mailbox_limit (default: 51200000)

Максималния размер в байтове на mailbox. (ако го сложим 0 става безлимитен)

Рестрикции

smtpd_helo_restrictions

Според SMTP мейл трансфера започва след изпращането на HELO/EHLO команда. Това е мястото където невалидните връзки могат да бъдат ограничени. Ето един пример как можете да настроите `smtpd_helo_restrictions`:

```
smtpd_helo_restrictions =
        reject_invalid_hostname,
        reject_unknown_hostname,
        reject_non_fqdn_hostname
```

reject_invalid_helo_hostname (with Postfix < 2.3: reject_invalid_hostname)

Отхвърля request-а ако хоста на HELO/EHLO е невалиден.

reject_unknown_helo_hostname (with Postfix < 2.3: reject_unknown_hostname)

Отхвърля request-а ако хоста на HELO/EHLO няма DNS A или MX запис.

reject_non_fqdn_helo_hostname (with Postfix < 2.3: reject_non_fqdn_hostname)

Отхвърля request-а ако хоста на HELO/EHLO не е в fully-qualified domain form (fqdn) както се изисква от RFC.

Ето един пример как тези рестрикции работят:

Клиентски терминал:

```
[ivo@ivelin ~]$ telnet localhost 25
Trying 127.0.0.1...
Connected to ivelin (127.0.0.1).
Escape character is '^]'.
220 ivelin.active-lynx.com ESMTP Postfix (2.4.5) (Mandriva Linux)
ehlo ivo
450 4.7.1 <ivo>: Helo command rejected: Host not found
^]
telnet> close
Connection closed.
```

postfix log:

```
Nov  9 11:59:15 ivelin postfix/smtpd[6692]: connect from ivelin[127.0.0.1]
Nov  9 11:59:15 ivelin postfix/smtpd[6692]: match_list_match: ivelin: no match
Nov  9 11:59:15 ivelin postfix/smtpd[6692]: match_list_match: 127.0.0.1: no match
Nov  9 11:59:15 ivelin postfix/smtpd[6692]: match_list_match: ivelin: no match
Nov  9 11:59:15 ivelin postfix/smtpd[6692]: match_list_match: 127.0.0.1: no match
Nov  9 11:59:15 ivelin postfix/smtpd[6692]: match_hostname: ivelin ~? 127.0.0.1
Nov  9 11:59:15 ivelin postfix/smtpd[6692]: match_hostaddr: 127.0.0.1 ~? 127.0.0.1
Nov  9 11:59:15 ivelin postfix/smtpd[6692]: > ivelin[127.0.0.1]: 220 ivelin.active-
lynx.com ESMTP Postfix (2.4.5) (Mandriva Linux)
Nov  9 11:59:17 ivelin postfix/smtpd[6692]: < ivelin[127.0.0.1]: ehlo ivo
Nov  9 11:59:17 ivelin postfix/smtpd[6692]: >>> START Helo command RESTRICTIONS <<<
Nov  9 11:59:17 ivelin postfix/smtpd[6692]: generic_checks:
name=reject_invalid_hostname
Nov  9 11:59:17 ivelin postfix/smtpd[6692]: reject_invalid_hostname: ivo
Nov  9 11:59:17 ivelin postfix/smtpd[6692]: generic_checks:
name=reject_invalid_hostname status=0
Nov  9 11:59:17 ivelin postfix/smtpd[6692]: generic_checks:
name=reject_unknown_hostname
Nov  9 11:59:17 ivelin postfix/smtpd[6692]: reject_unknown_hostname: ivo
Nov  9 11:59:17 ivelin postfix/smtpd[6692]: lookup ivo type A flags 0
Nov  9 11:59:17 ivelin postfix/smtpd[6692]: dns_query: ivo (A): Host not found
Nov  9 11:59:17 ivelin postfix/smtpd[6692]: lookup ivo type AAAA flags 0
Nov  9 11:59:17 ivelin postfix/smtpd[6692]: dns_query: ivo (AAAA): Host not found
Nov  9 11:59:17 ivelin postfix/smtpd[6692]: lookup ivo type MX flags 0
Nov  9 11:59:17 ivelin postfix/smtpd[6692]: dns_query: ivo (MX): Host not found
Nov  9 11:59:17 ivelin postfix/smtpd[6692]: NOQUEUE: reject: EHLO from
ivelin[127.0.0.1]: 450 4.7.1 <ivo>: Helo command rejected: Host not found;
proto=SMTP helo=<ivo>
Nov  9 11:59:17 ivelin postfix/smtpd[6692]: generic_checks:
name=reject_unknown_hostname status=2
Nov  9 11:59:17 ivelin postfix/smtpd[6692]: > ivelin[127.0.0.1]: 450 4.7.1 <ivo>:
Helo command rejected: Host not found
Nov  9 11:59:28 ivelin postfix/smtpd[6692]: smtp_get: EOF
Nov  9 11:59:28 ivelin postfix/smtpd[6692]: match_hostname: ivelin ~? 127.0.0.1
Nov  9 11:59:28 ivelin postfix/smtpd[6692]: match_hostaddr: 127.0.0.1 ~? 127.0.0.1
Nov  9 11:59:28 ivelin postfix/smtpd[6692]: lost connection after EHLO from
ivelin[127.0.0.1]
Nov  9 11:59:28 ivelin postfix/smtpd[6692]: disconnect from ivelin[127.0.0.1]
Nov  9 11:59:28 ivelin postfix/smtpd[6692]: master_notify: status 1
Nov  9 11:59:28 ivelin postfix/smtpd[6692]: connection closed
Nov  9 11:59:28 ivelin postfix/smtpd[6692]: proxymap stream disconnect
```

smtpd_sender_restrictions:

Ето и един примерен postgix log за изпращане на мейл от ограничен мейл на изпращача:

```
Nov  9 12:05:05 ivelin postfix/smtpd[6732]: > ivelin[127.0.0.1]: 220 ivelin.active-lynx.com
ESMTP Postfix (2.4.5) (Mandriva Linux)
Nov  9 12:05:05 ivelin postfix/smtpd[6732]: < ivelin[127.0.0.1]: EHLO ivelin.active-lynx.com
Nov  9 12:05:05 ivelin postfix/smtpd[6732]: >>> START Helo command RESTRICTIONS <<<
Nov  9 12:05:05 ivelin postfix/smtpd[6732]: generic_checks: name=reject_invalid_hostname
Nov  9 12:05:05 ivelin postfix/smtpd[6732]: reject_invalid_hostname: ivelin.active-lynx.com
Nov  9 12:05:05 ivelin postfix/smtpd[6732]: generic_checks: name=reject_invalid_hostname
status=0
Nov  9 12:05:05 ivelin postfix/smtpd[6732]: generic_checks: name=reject_unknown_hostname
Nov  9 12:05:05 ivelin postfix/smtpd[6732]: reject_unknown_hostname: ivelin.active-lynx.com
Nov  9 12:05:05 ivelin postfix/smtpd[6732]: lookup ivelin.active-lynx.com type A flags 0
Nov  9 12:05:05 ivelin postfix/smtpd[6732]: dns_query: ivelin.active-lynx.com (A): OK
Nov  9 12:05:05 ivelin postfix/smtpd[6732]: dns_get_answer: type A for ivelin.active-lynx.com
Nov  9 12:05:05 ivelin postfix/smtpd[6732]: generic_checks: name=reject_unknown_hostname
status=0
Nov  9 12:05:05 ivelin postfix/smtpd[6732]: generic_checks: name=reject_non_fqdn_hostname
Nov  9 12:05:05 ivelin postfix/smtpd[6732]: reject_non_fqdn_hostname: ivelin.active-lynx.com
Nov  9 12:05:05 ivelin postfix/smtpd[6732]: generic_checks: name=reject_non_fqdn_hostname
status=0
Nov  9 12:05:05 ivelin postfix/smtpd[6732]: >>> END Helo command RESTRICTIONS <<<
Nov  9 12:05:05 ivelin postfix/smtpd[6732]: > ivelin[127.0.0.1]: 250-ivelin.active-lynx.com
Nov  9 12:05:05 ivelin postfix/smtpd[6732]: > ivelin[127.0.0.1]: 250-PIPELINING
Nov  9 12:05:05 ivelin postfix/smtpd[6732]: > ivelin[127.0.0.1]: 250-SIZE 10240000
Nov  9 12:05:05 ivelin postfix/smtpd[6732]: > ivelin[127.0.0.1]: 250-VRFY
Nov  9 12:05:05 ivelin postfix/smtpd[6732]: > ivelin[127.0.0.1]: 250-ETRN
Nov  9 12:05:05 ivelin postfix/smtpd[6732]: > ivelin[127.0.0.1]: 250-AUTH LOGIN PLAIN
Nov  9 12:05:05 ivelin postfix/smtpd[6732]: match_list_match: ivelin: no match
Nov  9 12:05:05 ivelin postfix/smtpd[6732]: match_list_match: 127.0.0.1: no match
Nov  9 12:05:05 ivelin postfix/smtpd[6732]: > ivelin[127.0.0.1]: 250-AUTH=LOGIN PLAIN
Nov  9 12:05:05 ivelin postfix/smtpd[6732]: > ivelin[127.0.0.1]: 250-ENHANCEDSTATUSCODES
Nov  9 12:05:05 ivelin postfix/smtpd[6732]: > ivelin[127.0.0.1]: 250-8BITMIME
Nov  9 12:05:05 ivelin postfix/smtpd[6732]: > ivelin[127.0.0.1]: 250 DSN
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: < ivelin[127.0.0.1]: AUTH PLAIN AGl2ZWxpbgBh
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: xsasl_cyrus_server_first: sasl_method PLAIN,
init_response AGl2ZWxpbgBh
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: xsasl_cyrus_server_first: decoded initial response
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: > ivelin[127.0.0.1]: 235 2.0.0 Authentication
successful
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: < ivelin[127.0.0.1]: MAIL FROM:<ivelin@mail.bg>
SIZE=325
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: extract_addr: input: <ivelin@mail.bg>
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: smtpd_check_addr: addr=ivelin@mail.bg
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: connect to subsystem private/rewrite
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: send attr request = rewrite
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: send attr rule = local
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: send attr address = ivelin@mail.bg
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: private/rewrite socket: wanted attribute: flags
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: input attribute name: flags
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: input attribute value: 0
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: private/rewrite socket: wanted attribute: address
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: input attribute name: address
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: input attribute value: ivelin@mail.bg
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: private/rewrite socket: wanted attribute: (list
terminator)
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: input attribute name: (end)
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: rewrite_clnt: local: ivelin@mail.bg ->
ivelin@mail.bg
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: send attr request = resolve
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: send attr sender =
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: send attr address = ivelin@mail.bg
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: private/rewrite socket: wanted attribute: flags
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: input attribute name: flags
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: input attribute value: 0
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: private/rewrite socket: wanted attribute:
transport
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: input attribute name: transport
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: input attribute value: smtp
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: private/rewrite socket: wanted attribute: nexthop
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: input attribute name: nexthop
```

```
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: input attribute value: mail.bg
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: private/rewrite socket: wanted attribute:
recipient
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: input attribute name: recipient
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: input attribute value: ivelin@mail.bg
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: private/rewrite socket: wanted attribute: flags
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: input attribute name: flags
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: input attribute value: 4096
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: private/rewrite socket: wanted attribute: (list
terminator)
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: input attribute name: (end)
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: resolve_clnt: `' -> `ivelin@mail.bg' ->
transp=`smtp' host=`mail.bg' rcpt=`ivelin@mail.bg' flags= class=default
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: ctable_locate: install entry key ivelin@mail.bg
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: extract_addr: in: <ivelin@mail.bg>, result:
ivelin@mail.bg
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: >>> START Sender address RESTRICTIONS <<<
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: generic_checks: name=check_sender_access
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: check_mail_access: ivelin@mail.bg
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: ctable_locate: leave existing entry key
ivelin@mail.bg
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: check_access: ivelin@mail.bg
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: dict_ldap_lookup: In dict_ldap_lookup
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: dict_ldap_lookup: No existing connection for LDAP
source /etc/postfix/ldap-check-sender-email.cf, reopening
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: dict_ldap_connect: Connecting to server
ldap://sveto.active-lynx.com
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: dict_ldap_connect: Actual Protocol version used is
3.
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: dict_ldap_connect: Binding to server
ldap://sveto.active-lynx.com as dn cn=Manager,dc=test,dc=com
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: dict_ldap_connect: Successful bind to server
ldap://sveto.active-lynx.com as cn=Manager,dc=test,dc=com
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: dict_ldap_connect: Cached connection handle for
LDAP source /etc/postfix/ldap-check-sender-email.cf
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: dict_ldap_lookup: /etc/postfix/ldap-check-sender-
email.cf: Searching with filter (&(objectClass=qmailUser)(mail=ivelin)(accountStatus=active))
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: dict_ldap_get_values[1]: Search found 0 match(es)
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: dict_ldap_get_values[1]: Leaving
dict_ldap_get_values
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: dict_ldap_lookup: Search returned nothing
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: check_domain_access: mail.bg
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: dict_ldap_lookup: In dict_ldap_lookup
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: dict_ldap_lookup: Using existing connection for
LDAP source /etc/postfix/ldap-check-sender-email.cf
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: dict_ldap_lookup: /etc/postfix/ldap-check-sender-
email.cf: Searching with filter (&(objectClass=qmailUser)(mail=mail.bg)(accountStatus=active))
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: dict_ldap_get_values[1]: Search found 0 match(es)
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: dict_ldap_get_values[1]: Leaving
dict_ldap_get_values
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: dict_ldap_lookup: Search returned nothing
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: dict_ldap_lookup: In dict_ldap_lookup
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: dict_ldap_lookup: Using existing connection for
LDAP source /etc/postfix/ldap-check-sender-email.cf
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: dict_ldap_lookup: /etc/postfix/ldap-check-sender-
email.cf: Searching with filter (&(objectClass=qmailUser)(mail=bg)(accountStatus=active))
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: dict_ldap_get_values[1]: Search found 0 match(es)
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: dict_ldap_get_values[1]: Leaving
dict_ldap_get_values
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: dict_ldap_lookup: Search returned nothing
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: check_access: ivelin@
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: dict_ldap_lookup: In dict_ldap_lookup
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: dict_ldap_lookup: Using existing connection for
LDAP source /etc/postfix/ldap-check-sender-email.cf
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: dict_ldap_lookup: /etc/postfix/ldap-check-sender-
email.cf: Searching with filter (&(objectClass=qmailUser)(mail=ivelin)(accountStatus=active))
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: dict_ldap_get_values[1]: Search found 0 match(es)
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: dict_ldap_get_values[1]: Leaving
dict_ldap_get_values
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: dict_ldap_lookup: Search returned nothing
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: generic_checks: name=check_sender_access status=0
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: generic_checks: name=reject_unknown_sender_domain
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: reject_unknown_address: ivelin@mail.bg
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: ctable_locate: leave existing entry key
ivelin@mail.bg
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: reject_unknown_mailhost: mail.bg
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: lookup mail.bg type MX flags 0
```

```
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: dns_query: mail.bg (MX): OK
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: dns_get_answer: type MX for mail.bg
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: dns_get_answer: type MX for mail.bg
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: generic_checks: name=reject_unknown_sender_domain
status=0
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: generic_checks: name=reject_non_fqdn_sender
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: reject_non_fqdn_address: ivelin@mail.bg
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: generic_checks: name=reject_non_fqdn_sender
status=0
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: generic_checks: name=reject
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: NOQUEUE: reject: MAIL from ivelin[127.0.0.1]: 554
5.7.1 <ivelin@mail.bg>: Sender address rejected: Access denied; from=<ivelin@mail.bg>
proto=ESMTP helo=<ivelin.active-lynx.com>
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: generic_checks: name=reject status=2
Nov  9 12:05:08 ivelin postfix/smtpd[6732]: > ivelin[127.0.0.1]: 554 5.7.1 <ivelin@mail.bg>:
Sender address rejected: Access denied
```

Проверките на mail sender-а започват точно след mail from командата (тази команта се изпраща от клиента към сървъра). В този пример писмото е отхвърлено, защото не е намерено в базата данни на LDAP. Ще обсъдим интегрирането на Postfix с LDAP малко по-късно.

Ето и smtpd_sender_restrictions правилата настроени в `/etc/postfix/main.cf`:

```
smtpd_sender_restrictions =
        check_sender_access  ldap:/etc/postfix/ldap-check-sender-email.cf,
        reject_unknown_sender_domain,
        reject_non_fqdn_sender,
        reject
```

Тук можете да намерите обясненията за използване на рестрикциите:
http://www.postfix.org/postconf.5.html#smtpd_sender_restrictions

check_sender_access type:table

Преглежда посочена база данни за достъп за mail from адреса, домейна, домейни-бащи или localpart@, и изпълнява посочено действие. В нашия случай таблицата е ldap скрипт.

reject_unknown_sender_domain

Отхвърля заявката ако mail from адреса няма DNS A или MX запис, или фалшив MX запис.

reject_non_fqdn_sender

Отхвърля request-а ако хоста на HELO/EHLO не е в fully-qualified domain form (fqdn) както се изисква от RFC.

reject

Отхвърля заявката. Тази рестрикция е полезна на края на списъка със рестрикции, да действа като по default.

ldap-check-sender-email.cf

```
[root@ivelin postfix]# cat ldap-check-sender-email.cf
bind = yes
bind_dn = cn=Manager,dc=test,dc=com
bind_pw = secret
version = 3
timeout = 20
size_limit = 0
expansion_limit = 1
start_tls = no
#tls_require_cert = no
server_host = ldap://sveto.active-lynx.com
search_base = ou=accounts,dc=test,dc=com
scope = sub
query_filter = (&(objectClass=qmailUser)(mail=%u)(accountStatus=active))
result_attribute = title
```

bind (default: yes)

Да или да не се bind-не към LDAP сървъра. Новите версии на LDAP не се нуждаят клиентите да се „свързват", което спестява време.
Например:
bind = no
Ако не се нуждаете от bind-ване, може да предпочетете да конфигурирате Postfix да се свързва към локалната машина на порт, който е SSL тунел към вашия LDAP сървър. Ако вашия LDAP сървър не поддържа SSL, можете да направите тунел и на тази машина също. Това ще предотврати паролата да преминава през мрежата в чист вид.

bind_dn (default: empty)

Ако трабва да използвате bind, използвайте го с това име.
Пример:
bind_dn= uid=postfix, dc=your, dc=com

bind_pw (default: empty)

Паралота за горното. Ако искате да използвате това трябва да направите конфигурационния файл да е достъпен само за Postfix потребителя. Когато използвате ldap: ldapsource синтаксиса с map параметрите в main.cf, не е възможно да запазите bind паролата на сигурно място. Това е защото main.cf има нужда да бъде четим от всички за да имат възможност локалните потребители да изпращат поща от sendmail командата.
Пример:
bind_pw=парола

timeout (default: 10 seconds)

Времето в секунди през което търсенето да продължи преди да таймаутне.

size_limit (default: $expansion_limit)

Лимит на броя на LDAP резултатите върнати от единично LDAP търсене. Ако е 0 – нямаме лимит.

expansion_limit (default: 0)

Лимит на всичките елементи които се връщат от lookup според картата. Ако е 0 – отново нямаме лимит. Lookup-а фейлва с грешка ако лимита е превишен. Ако настроим лимита на 1 си гарантираме, че lookupа няма да връща много стойности.

server_host (default: localhost)

Името на стартирания (или стартираните в зависимост от версията на LDAP клиента може и да са няколко и порт може да се слага и т.н.) LDAP сървър.
Пример:
server_host=ldap.alabala.com

server_host = ldap.example.com:1444

server_host = ldap://ldap.example.com:1444

ldap://ldap2.example.com:1444 (това с OpenLDAP)

start_tls (default: no)

Да използваме или да не използваме STARTTLS при връзка към сървъра. НЕ използвайте това с LDAP SSL (SSL сесията тръгва автоматично при отваряне на TCP връзката).

search_base (No default; you must configure this)

RFC22553 базовото домейн име в което да се води търсенето:

search_base = dc=your, dc=com

От postfix 2.2+ този параметър поддържа следните '%' разширения:

%% - се символа %

%s – input key
Използват се и кавички за да се подсигурим че input key-а не е метасимвол.

%u – когато input key-а е адрес на формата.
user@domain, %u се заменя с локалната част на адреса. В противен случай се заменя с целя стринг от търсенето. Ако локалната част е празна, търсенето не връща резултати.

%d – когато input key-а е адрес на формата.
user@domain, %d – връща домейн частта на адреса. Иначе вне връща резултат.

%[SUD] - Главните букви еквивалентни на малките използвани по-горе се държат по същия начин.

%[1-9] Параметрите %1, %2,... %9 се използват за да се вземат важните части от домейна на input key-а. За да стане по-ясно какво се има предвид нека вземем за пример: user@mail.example.com – тогава %1 е com, %2 е example, %3 е mail.

scope (default: sub)

Областта на търсене на LDAP (sub, base или one) съответно:
LDAP_SCOPE_SUBTREE
LDAP_SCOPE_BASE
LDAP_SCOPE_ONELEVEL

query_filter (default: mailacceptinggeneralid=%s)

RFC2254 филтър използван за претърсване на директорията, където %s е субституция за адреса, който Postfix се опитва да резолвне. Например:

query_filter = (&(mail=%s)(paid_up=true))

От postfix 2.2+ този параметър поддържа следните '%' разширения:

%% - се символа %

%s – input key
Използват се и кавички за да се подсигурим че input key-а не е метасимвол.

%u – когато input key-а е адрес на формата.
user@domain, %u се заменя с локалната част на адреса. В противен случай се заменя с целя стринг от търсенето. Ако локалната част е празна, търсенето не връща резултати.

%d – когато input key-а е адрес на формата.
user@domain, %d – връща домейн частта на адреса. Иначе вне връща резултат.

%[SUD] - Главните букви еквивалентни на малките използвани по-горе се държат по същия начин.

%[1-9] Параметрите %1, %2,... %9 се използват за да се вземат важните части от домейна на input key-а. За да стане по-ясно какво се има предвид нека вземем за пример: user@mail.example.com – тогава %1 е com, %2 е example, %3 е mail.

Важно: НЕ поставяйте кавички около query_filter параметъра.

result_attribute (default: maildrop)

Атрибутите, които Postfix чете от който е да е резултат от директория върнат от lookup-а за да бъде резолвнат в е-мейл адрес.

result_attribute = mailbox, maildrop

smtpd_recipient_restrictions

Тези ограничение се изпълняват от Postfix сървъра, когато е получена команда rcpt to.

Ето ограниченията, които ще използваме ние:

```
smtpd_recipient_restrictions =
        permit_sasl_authenticated,
        permit_mynetworks,
        check_relay_domains,
        reject
```

а ето и обяснение на правилата, които използваме:

permit_sasl_authenticated

Позволяваме заявката, когато клиента се е автентикирал успешно през RFC4954 (AUTH) протокола.

permit_mynetworks

Позволяваме заявката, когато ИП адреса на клиента се съдържа в някоя от мрежите записани в $mynetworks.

check_relay_domains

Позволяваме заявката, когато хоста на клиента се намира в $relay_domains или когато резолвнатия краен адрес се намира в $relay_domains, иначе отказ.

reject

Отхвърля заявката. Тази рестрикция е полезна на края на списъка със рестрикции, да действа като по default.

Други полезни ограничения

```
smtpd_helo_required = yes
smtpd_delay_reject = no
strict_rfc821_envelopes = yes
```

и отново описание:

smtpd_helo_required (default: no)

Изисква това отдалечения SMTP клиент да се представи преди да започне SMTP сесия с HELO или EHLO команда.

Пример: smtpd_helo_required = yes

smtpd_delay_reject (default: yes)

Изчаква до RCPT TO командата преди да оцени: $smtpd_client_restrictions, $smtpd_helo_restrictions или $smtpd_sender_restrictions, или изчаква до ETRN команда преди да оцени $smtpd_client_restrictions, $smtpd_helo_restrictions.

Това ограничение има едно много важно предимство, че логва адреса на получателя преди да го отхвърли. Така в логовете можете да проверите кои адреси са били отхвърлени.

strict_rfc821_envelopes (default: no)

Изисква адресите получени в SMTP MAIL FROM и RCPT TO командите да са заключени с < >, и тези адреси да не съдържат коментари и фрази в стил RFC822. Това предотвратява получаване на поща от лошо написан софтуер. По принцип Postfix SMTP сървъра получава RFC 822 синтаксис в MAIL FROM и RCPT TO адресите.

Postfix автентикация (SASL базирана)

Можете да проверите дали Postfix поддържа cyrus sasl като стартирате postconf –a

Пример:

```
[ivo@ivelin ~]$ sudo postconf -a
cyrus
dovecot
```

тук използваме SASL базирана автентикация.

Следващите няколко настройки казват на Postfix да използва SASL автентикация:

```
smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
smtpd_sasl_local_domain =
```
broken_sasl_auth_clients = yes

Описание на тези настройки:

smtpd_sasl_auth_enable (default: no)

Позволява SASL автентикация в Postfix SMTP сървърът. По подразбиране Postfix SMTP сървърът не поддържа автентикация.

Ако външен SMTP клиент е аутентикиран,
permit_sasl_authenticated може да бъде използван за relay access,
по следния начин:

smtpd_recipient_restrictions =

permit_mynetworks, permit_sasl_authenticated, ...

За да се забранят всички SMTP връзки от неаутентикирани клиенти, се използва smtpd_delay_reject = yes (което е по подразбиране) и:

smtpd_client_restrictions = permit_sasl_authenticated, reject

Вижте SASL_README файлът за SASL настройки:

- *smtpd_sasl_security_options (подразбиране: noanonymous)*

  Postfix SMTP сървър SASL security options;

  от Postfix 2.3 настройките зависят от имплементацията на SASL която е избрана със smtpd_sasl_type.

  Следните настройки са дефинирани за cyrus имплементацията.

  noplaintext

  Забранява методи които използват plaintext.

  noanonymous

  Забранява методите които използват анонимна аутентикация.

  forward_secrecy

  Only allow methods that support forward secrecy (Dovecot only).

  mutual_auth

  Разрешава само методи които използват споделена аутентикация.

  По подразбиране Postfix SMTP сървърът поддържа plaintext пароли, но не поддържа анонимни потребители.

  Внимание: Повечето клиенти изпробват различните методи за аутентикация в реда препоръчан от сървъра (e.g., PLAIN ANONYMOUS CRAM-MD5) което означава, че ако се забрани PLAIN клиентите ще се аутентикират анонимно, дори когато те би трябвало да използват CRAM-MD5. И така ако забраните PLAIN, забранете и анонимна аутентикация.

  Пример

  smtpd_sasl_security_options = noanonymous, noplaintext

- *smtpd_sasl_local_domain (подразбиране: празно)*

  Името на локалния домейн.

  Пример:

  smtpd_sasl_local_domain = $mydomain smtpd_sasl_local_domain = $myhostname

- *broken_sasl_auth_clients (default: no)*

  Спеицифицирайте "broken_sasl_auth_clients = yes" за да се предлойите AUTH подръжка по нестандартен начин. (Някой клиенти работят работят с такава спецификация на AUTH командата: Microsoft Outlook Express version 4 и Microsoft Exchange version 5.0.)

SASL настройките

/etc/sasl2/smtpd.conf

В този файл се намират настройки за SASL. Настройте mech_list параметърът на plain login, pwdcheck метода и saslauthd_path.

Ето моят конфигурационен файл:

```
[ivo@ivelin ~]$ cat /etc/sasl2/smtpd.conf
# SASL library configuration file for postfix
# all parameters are documented into:
# /usr/share/doc/cyrus-sasl/options.html

# The mech_list parameters list the sasl mechanisms to use,
# default being all mechs found.
mech_list:         plain login

# To authenticate using the separate saslauthd daemon, (e.g. for
# system or ldap users). Also see /etc/sysconfig/saslauthd.
pwcheck_method:    saslauthd
saslauthd_path:    /var/lib/sasl2/mux

# To authenticate against users stored in sasldb.
#pwcheck_method:    auxprop
#auxprop_plugin:    sasldb
#sasldb_path:       /var/lib/sasl2/sasl.db
```

/etc/sysconfig/saslatuhd

В този файл са записани настройктие за saslauthd service. Тези настройки включват: тип на аутентикация и настройки на типа на аутентикация. Сложете тези настройки като мите ако искате да използвате ldap аутентеикация.

```
[ivo@ivelin ~]$ cat /etc/sysconfig/saslauthd
# $Id: saslauthd.sysconfig,v 1.1 2001/05/02 10:55:48 wiget Exp $
# Authentications mechanism (for list see saslauthd -v)
SASL_AUTHMECH=ldap

# Hostname for remote IMAP server (if rimap auth mech is used)
# Ldap configuration file (if ldap auth mech is used)
SASL_MECH_OPTIONS=/etc/saslauthd.conf

# Extra options (for list see saslauthd -h)
#SASLAUTHD_OPTS=-O /etc/saslauthd.conf
```

/etc/saslauthd.conf

В този файл са записани настройките свързани със ldap аутентикацията.

Ето моите настройки:

```
[ivo@ivelin ~]$ cat /etc/saslauthd.conf
```

```
ldap_servers: ldap://sveto.active-lynx.com/
ldap_bind_dn: cn=Manager, dc=test, dc=com
ldap_bind_pw: secret
ldap_search_base: ou=accounts, dc=test, dc=com
ldap_filter: (&(objectClass=qmailUser)(uid=%u)(accountStatus=active))
```

- *ldap_servers*

  ldap_servers посочва интернет адреса на ldap сървъра.

Валидни формати са:

ldap://somehost.domain, ldap://ip.address, ldap://ip.address:server_port, ldap://hostname:server_port.

ldap_bind_dn

Ако тази настройка е въведена то, saslauthd модулът ще се аутентикира със ldap_bind_dn и ldap_bind_pw когато прави заявки, в противен случай ще използва анонимна аутентикация.

- *ldap_bind_pw*

  Паролата използвана в горепосочената настройка.

- *ldap_search_base*

  Базовият DN от който ще търсим.

- *ldap_filter*

  Филтърът посредством който ще търсим.

Имайки в предвид тези настройки аутентикацията протича на следните стъпки:

1. Клиент се връзва към postfix smtp сървисът и изпраща helo/ehlo.
2. postfix проверява домейнът специфициран от helo/ehlo.
3. Клиентът изпраща команда за аутентикация.
4. SASL енджинът претърсва за потребителското име в LDAP сървърът, ако намери той се опитва да се аутентикира с потребителското име и въведената от клиента парола. Ако това е успешно, то клиентът е аутентикиран.

Използвана литература и източници:

www.postfix.org
http://www.postfix.org/LDAP_README.html
http://bg.wikipedia.org/wiki/LDAP
http://www.hmug.org/man/3/ldap.php
http://linux.die.net/man/8/saslauthd
http://linux.die.net/man/1/postfix