Les mails

Configuration des clients:

SMTP

mail.ppsfleet.navy, 587 (tls)

IMAP

mail.ppsfleet.navy, ssl/tls, 993

Le serveur

Le serveur est composé de

- ~~Opensmtpd~~ Exim - serveur smtp (envoi/reception de mail)
- Dovecot - serveur imap (pour stocker les mails, et lire ses mails avec un client)
- Sieve (dans dovecot): rules pour trier les mails dans des dossiers etc...
- Dkimfilter - signe les mails avec la clé public du serveur
- Des champs dns - `/var/named/ppsfleet.navy.d/ppsfleet.navy.mail.include`

Tout est géré via systemd, installé sur l'auth

Dovecot

/etc/dovecot/dovecot.conf

Les fichiers dans /etc/dovecot/conf.d ne sont pas lues...

```
ssl = required
ssl_cert = </etc/letsencrypt/live/mail.ppsfleet.navy/fullchain.pem
ssl_key = </etc/letsencrypt/live/mail.ppsfleet.navy/privkey.pem

ssl_min_protocol = TLSv1.2
ssl_prefer_server_ciphers = yes
ssl = required
disable_plaintext_auth = yes

protocols = lmtp imap sieve


service lmtp {
        unix_listener lmtp {
                user  = vmail
                group = vmail
        }
}

protocol lmtp {
  mail_plugins = $mail_plugins sieve
}

service managesieve-login {
  inet_listener sieve {
    port = 4190
  }

  #inet_listener sieve_deprecated {
  #  port = 2000
  #}

  # Number of connections to handle before starting a new process. Typically
  # the only useful values are 0 (unlimited) or 1. 1 is more secure, but 0
  # is faster. <doc/wiki/LoginProcess.txt>
  service_count = 1

  # Number of processes to always keep waiting for more connections.
  process_min_avail = 0
```

```
  # If you set service_count=0, you probably need to grow this.
  vsz_limit = 64M
}



service imap-login {
        inet_listener imap {
                port = 143
        }
        inet_listener imaps {
                port = 993
        }
}

service auth {
  # SASL
  unix_listener auth-client {
    mode = 0600
    user = mail
    group = mail
  }
}



passdb {
        driver = passwd-file
        args = scheme=SHA512-CRYPT /etc/mails/passwd.txt
}



userdb {
    args   = uid=vmail gid=vmail home=/data/mails/mailbox/%d/%n
    driver = static
}




#userdb {
#       driver = passwd-file
#       args = /etc/dovecot/users.txt
```

```
#       override_fields = uid=vmail gid=vmail home=/home/vmail/%n
#}

namespace inbox {
  # Namespace type: private, shared or public
  type = private

  # Hierarchy separator to use. You should use the same separator for all
  # namespaces or some clients get confused. '/' is usually a good one.
  # The default however depends on the underlying mail storage format.
  separator = '/'

  inbox = yes

}

mail_location = maildir:/data/mails/mailbox/%d/%n
```

Exim

La conf exim est divisé en plusieurs section. https://www.exim.org/exim-html-current/doc/html/spec_html/ch-the_default_configuration_file.html

Les paramètre globaux (en haut), tel que les certificats et d'autres truc generaux

la section **begin acl.** Vérifie si on accepte d'envoyer le mail selon l'emetteur, a qui on l'envoi, le type mime etc...

On a configuré les sections via ces lignes:

```
acl_smtp_mail =         acl_check_mail
acl_smtp_rcpt =         acl_check_rcpt
.ifdef _HAVE_PRDR
acl_smtp_data_prdr =    acl_check_prdr
.endif
acl_smtp_data =         acl_check_data
acl_smtp_mime =         acl_check_mime
```

la section **begin routers.**

> The routers that you find under 'routers configuration' contain conditions that determine under which conditions 'something' happens to the mail. What happens next is determined by the transports under 'transport configuration'.

```
system_aliases:
  driver = redirect
  allow_fail
  allow_defer
  data = ${lookup{$local_part@$domain}lsearch{/etc/mails/aliases.txt}}
# user = exim
  file_transport = address_file
  pipe_transport = address_pipe



localuser:
  debug_print = "R: local_user for $local_part@$domain"
  driver = accept
  domains = +local_domains
# local_part_suffix = +* : -*
# local_part_suffix_optional
  transport = dovecot_lmtp
  cannot_route_message = Unknown user
```

la section **begin transports**

la section **begin retry**. Règle de retry

la section **begin rewrite**. vide

la section **begin authenticators**. Pour l'authentification.
On utilise dovecot.

```
begin authenticators


dovecot_plain:
  driver = dovecot
  public_name = PLAIN
  server_socket = /var/run/dovecot/auth-client
  server_set_id              = $auth1
```

Pour que ca fonctionne on doit avoir exim lancé avec le groupe mail. C'est dans le fichier `/etc/sysconfig/exim`

Sieve

Pour avoir sieve, il faut installer le paquet *dovecot-pigeonhole.* Puis tout se joue dans dovecot. La conf du dessus est configuré pour sieve.

https://doc.dovecot.org/2.3/configuration_manual/sieve/configuration/

Il faut aussi configurer l'interface web dans */etc/roundcubemail/managesieve.inc.php.dist*

> $config['managesieve_host'] = 'localhost:4190'; (pour correspondre à la conf de dovecot)

Les utilisateurs:

Il y a 3 fichiers:

- Les noms de domaines: `/etc/mails/domains.txt`
- Les mot de passe: `/etc/mails/passwd.txt`
- Les alias (reception): `/etc/mails/aliases.txt`

Pour générer le hash du mot de passe: `doveadm pw -s SHA512-CRYPT`

todo: unifier tout ça, avec auth.ppsfleet.navy si possible

Révision #26
Créé 2021-01-18 13:22:10 UTC par tjiho
Mis à jour 2025-12-24 14:06:02 UTC par tjiho