Messagerie Internet

(Exim)

Introduction (1)

- Messagerie électronique
  - Application la plus populaire de l'Internet
- Plus qu'un échange d'informations entre 2 personnes n'importe où dans le monde.
- Utile pour joindre une multitude d'individus à la fois et en un temps record

Introduction (2)

- Définition :
  - Courrier électronique = message, document, fichier multimédia stocké dans un ordinateur et envoyé à un autre ordinateur par le biais d'Internet.
  - e-mail (pays anglophones), courriel (Québec)
  - Mél : abréviation officielle en France

Introduction (3)

- Pour accéder à une messagerie électronique, il faut avoir :
  - un compte (par votre ISP, votre entreprise, ou un service gratuit) et donc une adresse.
  - un logiciel spécifique (Eudora, Thunderbird) ou une boîte aux lettres Web (gmail, Yahoo, Hotmail).

Introduction (4)

- Le fonctionnement du courrier électronique :
  - très voisin de celui de la vie réelle.
  - s'appuie sur des "bureaux de poste", des expéditeurs et des destinataires.
- Un bureau de poste doit être disponible et sûr
- 2 types de protocoles pour l'acheminement et la réception de courriers :
  - Transport de messages : SMTP
  - Dialogue entre gestionnaire d'email et client de messagerie : POP3 et IMAP

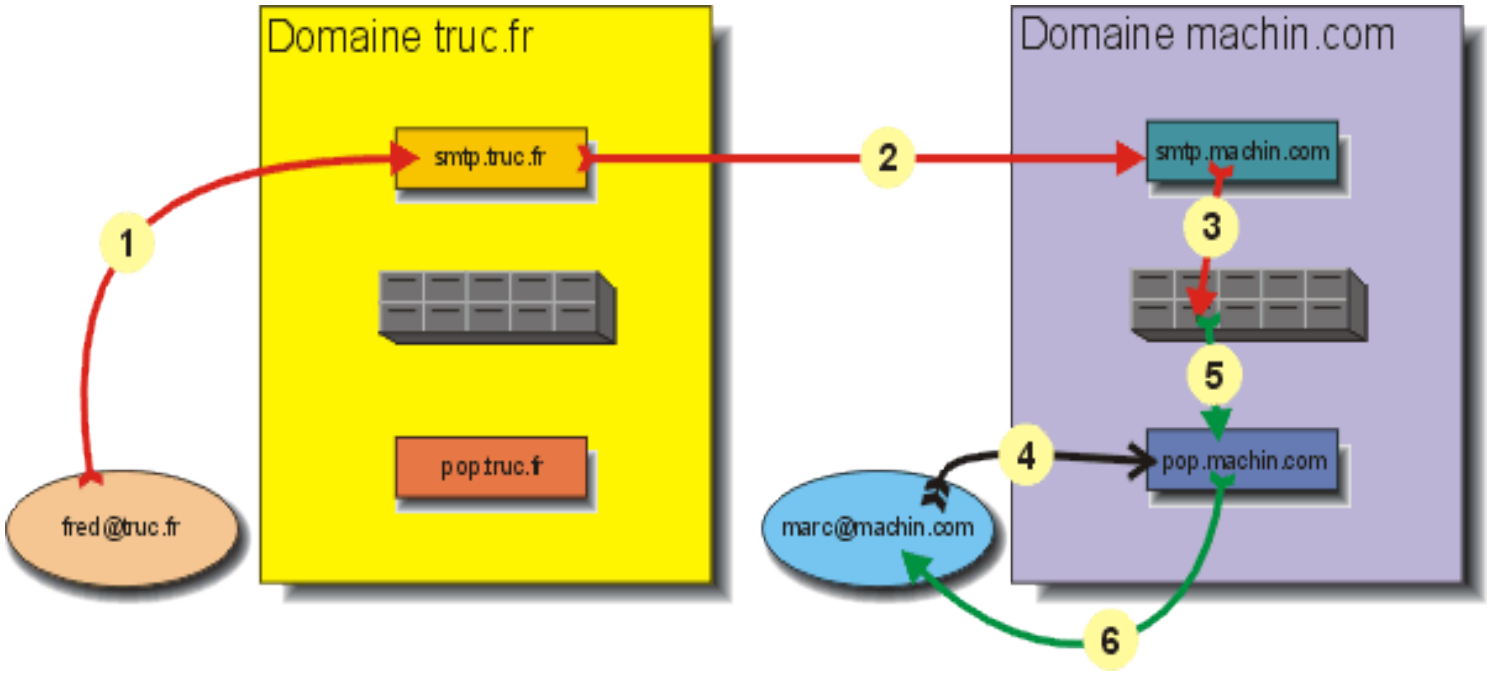
SMTP

- Simple Mail Transfer Protocol
- Un des protocoles les plus fondamentaux de l'Internet
- Permet de véhiculer du courrier électronique
- C'est la messagerie de l'Internet

Itinéraire d'un message électronique (1)

- Supposons un cas simple (et cependant courant).
  - Soit un utilisateur abonné chez "truc" et ayant pour adresse électronique: **fred@truc.fr**.
  - Soit un autre utilisateur abonné chez "machin" et ayant pour adresse électronique **marc@machin.com**.
  - truc dispose des serveurs:
    - smtp.truc.fr
    - pop.truc.fr
  - machin dispose des serveurs:
    - smtp.machin.com
    - pop.machin.com
  - Fred doit envoyer un message à Marc.

Itinéraire d'un message électronique (2)



Itinéraire d'un message électronique (3)

1. Fred compose le message avec son outil de messagerie, et clique sur le bouton "envoyer". Le message est envoyé sur le serveur smtp.truc.fr
2. smtp.truc.fr reçoit le message, constate que le destinataire n'est pas dans son domaine, recherche un serveur de messagerie dans le domaine machin.com, et envoie le message à smtp.machin.com.
3. Le serveur smtp.machin.com reçoit le message, constate que le destinataire est bien dans son domaine, et range le message dans la boîte aux lettres de Marc.
4. Un jour, Marc décide de regarder s'il n'a pas de messages. Il envoie donc une requête à son serveur pop.machin.com, au moyen de son outil de messagerie.
5. Le serveur pop consulte alors la boîte aux lettres de Marc, constate qu'il y a un message.
6. Il l'envoie à l'outil de messagerie de Marc qui, par défaut, demandera à pop.machin.com de le supprimer de la boîte aux lettres. Il est possible de demander à ne pas effacer les messages. Cette fonction est utile lorsque l'on désire consulter sa messagerie de divers endroits sans avoir à se renvoyer un message si on veut le relire ailleurs.

Questions ???

Mécanismes mis en jeu (1)

- SMTP :
  - Protocole applicatif de transport des messages sur internet.
  - Sait acheminer un message jusqu'à une boîte aux lettres.
- POP3 (Post Office Protocol 3) :
  - Dialogue entre client (outlook) et serveur de messagerie (sendmail par exemple).
  - Il ne fait pas de transport
  - Permet à l'utilisateur de gérer son courrier.

Mécanismes mis en jeu (2)

- MUA (Mail User Agent) :
- Interagit directement avec l'utilisateur final
  - Pine, mutt, mail, Eudora, Marcel, Mailstrom,
  - Mulberry, Pegasus, Simeon, Netscape, Outlook, thunderbird, evolution, ...
- Les MUA sont nombreux sur un système – l'utilisateur final choisit
- MTA = Mail Transfer Agent
- Reçoit et délivre des messages électroniques
  - Sendmail, Smail, PP, MMDF, Charon, Exim, qmail, Postfix, ...
- Un MTA par système – sysadmin choisit

Format de message (1)

From: Philip Hazel <ph10@cus.cam.ac.uk>
To: Julius Caesar <julius@ancient-rome.net>
Cc: Mark Anthony <MarkA@cleo.co.uk>
Subject: How Internet mail works

Julius,
  I'm going to be running a course on ...

- Le format est à l'origine défini par RFC 822 en 1982
- Maintenant remplacé par RFC 2822
- Le message se compose de :
  - Des lignes d'en-tête
  - Un interligne
  - Des lignes du corps de message

Format de message (2)

- Une adresse se compose d' une *partie locale* et d'un *domaine*

  roger@*refer.sn*

- Un corps de message de base est non structuré

- D'autres RFC (MIME, 2045) ajoutent des entêtes additionnelles qui définissent la structure pour le corps

- MIME supportent des attachements de diverses sortes et dans divers codages

- Créer/décoder les attachements est le travail des MUA

Un message en transit (1)

- Des en-têtes sont ajoutés par le MUA avant l'envoi

From: Philip Hazel <ph10@cus.cam.ac.uk>

To: Julius Caesar <julius@ancient-rome.net>

cc: Mark Anthony <MarkA@cleo.co.uk>

Subject: How Internet mail works

Date: Fri, 10 May 2002 11:29:24 +0100 (BST)
Message-ID: <Pine.SOL.3.96.990117111343.
19032A-100000@taurus.cus.cam.ac.uk>
MIME-Version: 1.0
Content-Type: TEXT/PLAIN; charset=US-ASCII

The Tueur,

Je serai à l'heure au cours ...

Un message en transit (2)

- Des en-têtes sont ajoutées par les MTA

```
Received: from taurus.cus.cam.ac.uk
      ([192.168.34.54] ident=exim)
      by mauve.csi.cam.ac.uk with esmtp
      (Exim 4.00) id 101qxX-00011X-00;
      Fri, 10 May 2002 11:50:39 +0100
    Received: from ph10 (helo=localhost)
      by taurus.cus.cam.ac.uk with local-smtp
      (Exim 4.10) id 101qin-0005PB-00;
      Fri, 10 May 2002 11:50:25 +0100
    From: Philip Hazel <ph10@cus.cam.ac.uk>
    To: Julius Caesar <julius@ancient-rome.net>
    cc: Mark Anthony <MarkA@cleo.co.uk>
    ...
```

Un message en transit(3)

- Un message est transmis par une *enveloppe*

  MAIL FROM:<ph10@cus.cam.ac.uk>

  RCPT TO:<aalain@trstech.net>

- *L'enveloppe est séparée du message RFC 2822*

- *les champs de l'enveloppe (RFC 2821) n'ont pas besoin d'être identiques aux champs de l'en-tête (RFC 2822)*

- *Les MTA (principalement) sont concernés par des enveloppes*
  - *Juste comme la poste...*
- *Les messages d'erreur (“rebond”) ont un champ expéditeur nul*

  MAIL FROM:<>

Questions ???

Détails de l’entête d’un message (1)

- Return-Path **:** C'est l'adresse qui sera utilisée pour :
  - la réponse (la fonction répondre à l'expéditeur)
  - Le renvoi du message s'il ne peut arriver au destinataire.
- Received : Cette ligne est un peu particulière. Chaque MTA qui reçoit le message y inscrit le nom du MTA qui le lui a envoyé, ainsi que le sien. Il est ainsi possible de retracer complètement la route qu'a suivi le message de l'expéditeur jusqu'au destinataire.
- Message-ID : C'est un identifiant unique du message. Il est attribué par le premier MTA qui reçoit le message.

Détails de l’entête d’un message (2)

- From : L'adresse de l'expéditeur, par défaut recopiée dans le "return path".
- To : C'est l'adresse du (ou des) destinataire(s)
- Subject : L'objet du message
- Date : La date d'émission écrite par le MUA de l'émetteur
- MIME-Version : Version du mode de codage des données.
- Content-Type : Type de codage utilisé (plain/text, base 64, HTML).

Utilité de l'en-tête

- L'en-tête contient donc toutes les informations nécessaires pour :
  - Identifier l'auteur du message
  - Identifier le destinataire
  - Savoir à qui il faut répondre
  - Retrouver le chemin suivi par le message
  - Savoir le type de codage du message.

Une session de SMTP (1)

```
telnet relay.ancient-rome.net 25
220 relay.ancient-rome.net ESMTP Exim ...
EHLO taurus.cus.cam.ac.uk
250-relay.ancient-rome.net ...
250-SIZE 10485760
250-PIPELINING
250 HELP
MAIL FROM:<ph10@cus.cam.ac.uk>
250 OK
RCPT TO:<julius@ancient-rome.net>
250 Accepted
DATA
354 Enter message, ending with “.”
Received: from ...
     (slide suivant)
```

Une session de SMTP(2)

From: ...

To: ...

etc...

.

250 OK id=10sPdr-00034H-00

quit

221 relay.ancient-rome.net closing conn...

Les codes retour de SMTP

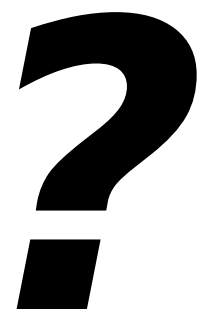
2xx ok

3xx envoyez plus de données

4xx Echec temporaire

5xx Echec permanent

Questions ???



Utilisation du DNS pour le courrier électronique (1)

- Deux types d'enregistrement DNS sont utilisés pour le courrier
- *L'enregistrement Mail Exchange (MX) fait correspondre les domaines du courrier aux serveurs, et fourni une liste de serveurs avec des préférences:*

  hermes.cam.ac.uk. MX 5 green.csi.cam.ac.uk.
  MX 7 ppsw3.csi.cam.ac.uk.
  MX 7 ppsw4.csi.cam.ac.uk.

- *Les enregistrements adresse (A) font correspondre les noms aux adresses IP :*

  green.csi.cam.ac.uk. A 131.111.8.57
  ppsw3.csi.cam.ac.uk. A 131.111.8.38
  ppsw4.csi.cam.ac.uk. A 131.111.8.44

Utilisation du DNS pour le courrier électronique(2)

- Les enregistrements MX ont été ajoutés au DNS après son déploiement initial

- Règle de compatibilité :

  Si aucun enregistrement MX n'est trouvé, recherchez un enregistrement A, et si c'est trouvé, traitez le comme un MX avec la préférence 0.

- Les enregistrements MX ont été inventés pour des passages à d'autres systèmes de courrier, mais sont maintenant fortement utilisés pour manipuler des domaines génériques de courrier

Erreurs communes de DNS

- Points finaux manquant sur des noms dans l'enregistrement MX
- Les enregistrements MX pointent vers des aliases au lieu des noms canoniques.

  Cela devrait fonctionner, mais est inefficace et désapprouvé
- Les enregistrements MX pointent vers des machines inexistantes
- Les enregistrements MX contiennent une adresse IP au lieu d'un nom sur le côté droit

  Malheureusement quelques MTA acceptent ça
- Les enregistrements MX ne contiennent pas une valeur préférentielle
- Certains serveurs de nom donnent une erreur de serveur pour des requêtes de MX inexistant

Sécurité : Problèmes

- Divers problèmes:
  - pertes de messages
    - par l ’agent de transport (le MTA)
    - par l ’utilisateur
    - par un incident matériel
  - Ecoute des messages
  - Falsification des messages

Questions ???

Sécurité : Solutions (2)

- Réponses
  - Informer l'expéditeur sur ce qui est arrivé au message.
  - Chaque relais sait indiquer si le message est envoyé correctement ou non au relais suivant.
  - Limitation possible du nombre de relais par SMTP
  - Utilisation du Chiffrement entre les serveurs

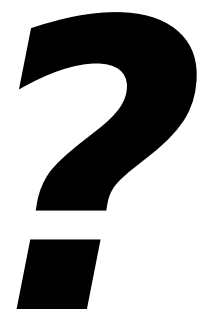
SPAM : Problème

- Courrier non sollicité envoyé à plusieurs personnes.
- Les adresses sont récupérées via les News, les listes de diffusion, les pages Web (analyse des champs mailto).
- Apparu avec l'explosion du nombre d'utilisateurs de l'Internet (solutions apparues en 1997).
- Un commerce florissant (vente de fichiers d'utilisateurs…)

SPAM - Solutions

- Reconnaître l'auteur d'un SPAM
- Filtrage au niveau personnel
- Filtrage au niveau d 'un site
  - liste noir des « spammeurs » connus
  - liste blanche
  - Liste grise
  - interdire le relayage
  - refuser les adresses invalides
  - refuser les adresses IP d'expéditeurs non valides

Questions ???



Exim

Exim - Introduction (1)

- Serveur de messagerie électronique (MTA)
- 1ère version écrite en 1995 par Phil Hazel à l'université de Cambridge.
- Basé au départ sur smail, il a largement évolué pour devenir l'un des MTA les plus flexbiles et robustes.
- Exim est un logiciel libre
- MTA par défaut de Debian

Exim – Introduction (2)

- Il est donc parfaitement adapté aux grosses entreprises.
- Très fiable, il n'a connu à ce jour aucun bogue critique majeur.
- Son développement est très actif pour suivre les différentes normes, et ajouter de nouvelles fonctionnalités.

Fichier de configuration de Exim (1)

- Exim dispose d'un fichier de configuration unique découpé en plusieurs parties.
- Chaque partie correspond aux différentes actions réalisées sur un message.
- La syntaxe utilisée est semblable à du langage de scripts shell.
- Il est possible d'utiliser des affectations, des exécutions de programmes, …
- Exim permet aux administrateurs de suivre pas à pas l'acheminement du message à chaque étape de l'envoi du mail ==> débogage rapide de la configuration

Fichier de configuration de Exim (2)

- Section générale du fichier : options globales du programme, comme le nom de la machine, les domaines locaux, précision de l'antivirus et de l'antispam, …
- Toutes les autres sections commencent par le mot clé « *begin* ».
- Elles sont optionnelles, et peuvent apparaître dans n'importe quel ordre.
- *Les paramètres optionnels peuvent se rapporter aux fichiers de données auxiliaires, par exemple, un fichier d'alias (habituellement /etc/aliases)*

Fichier de configuration de Exim (3)

- *Les commentaires, les macros, et les inclusions sont disponibles.*
- Section des ACLs : pour la vérification des messages entrant. Chaque ACL est une série d'instructions qui permet d'accepter ou de rejeter un message.
- Section des Routers : Permet de router les messages (vers un utilisateur local ou distant). Les routeurs sont exécutés de façon séquentielle. ➔ Ordre des routers est très important. Lorsque les conditions d'un routeur sont remplies, il peut faire appel à un transport.

Fichier de configuration de Exim (4)

- Section des Transports : 1 transport est appelé lorsque le message doit être délivré à une destination finale (boîte à lettres locale, une adresse vers un autre domaine ou un programme). La configuration se fait en utilisant des pilotes existant pouvant être configurés.
- Section de retransmission : Algorithme de retransmission des messages en queue.
- Section des Réécritures : permet de changer l'émetteur d'un message (à l'envoi) ou le récepteur d'un message (à la réception)
- Deux autres sections pour définir des méthodes d'authentification et pour le scannage local.

Fichier de configuration de Exim (4)

Paramétrage options globales

`begin ACL`

Listes de contrôles d'accès

`begin routers`

Configuration du routeur(router)

`begin transports`

Configuration du transport

`begin retry`

Règles des tentatives

`begin rewrite`

Règles de réécritures

`begin authenticators`

Configuration d'authentification

Requis pour SMTP entrant

Requis pour la livraison de message

Les routeurs de Exim 4

- Exim contient un certain nombre de routeurs

  Exemple: *le routeur dnslookup fait le traitement DNS*

  le routeur redirect fait la redirection d'adresse

  (l'aliasing et le forwarding)

- *La configuration définit quels routeurs sont utilisés, dans quel ordre, et dans quelles conditions*

  Exemple: les routeurs sont souvent limités à des domaines spécifiques

- *Le même routeur peut apparaître plus d'une fois, habituellement avec différentes configurations*
- *L'ordre dans lequel les routeurs sont définis est très important*

Configuration de routage simple

- Vérifiez le domaine non-local : exécutez le routeur 'dnslookup'
  - Accepter: Queue pour le transport smtp
  - Rejeter:Si “no_more” défini => rebond
- Vérifiez les aliases système: le routeur 'redirect'
  - Accepter: génère de nouvelle(s) adresse(s)
  - Rejeter: passé au prochain routeur
- Vérifiez les forward des utilisateurs locaux : autre routeur 'redirect'
  - Accepter: génère nouvelle(s) adresse(s)
  - Rejeter: passé au prochain routeur
- Vérifiez les utilisateurs locaux: exécutez le routeur 'accept'
  - Accepter: file d'attente pour le transport 'appendfile'
- Plus de routeurs => rebond

Transports de Exim

- Les transports sont les composants de Exim qui délivrent réellement les copies des messages
  - Le transport 'smtp' délivre sur TCP/IP aux sites distants
  - Le transport 'appendfile' écrit dans un fichier local
  - Le transport 'pipe' écrit vers autre processus via un pipe
  - Le transport 'lmtp' fait de même, en utilisant LMTP
  - Le transport 'Autoreply' est anormal, parce qu'il crée une réponse automatique au lieu de faire une vraie livraison
- L'ordre dans lequel des transports sont définis est sans importance
- Un transport est utilisé uniquement si référencé par un routeur
- Des transports sont exécutés dans des sous-processus, sous leur propre uid, après le routage

Questions ???

Les routeurs par défaut (1)

- Le premier routeur gère les domaines non locaux

```
dnslookup:
  driver = dnslookup
  domains = ! +local_domains
  ignore_target_hosts = 127.0.0.0/8
  transport = remote_smtp
  no_more
```

- Des pré-conditions verifiées pour un domaine non local
- Des entrées DNS “idiotes” sont ignorées
- Si le domaine est trouvé dans le DNS, mettre en queue pour **remote_smtp**
- Dans le cas contraire, **no_more** transforme le “rejet” en “echec”

Les routeurs par défaut (2)

- Le deuxième routeur manipule les aliases système

```
system_aliases:
   driver = redirect
   data = ${lookup{$local_part}lsearch\
         {/etc/aliases}}
   allow_fail
   allow_defer
   pipe_transport = address_pipe
   file_transport = address_file
   user = exim
```

Les routeurs par défaut(4)

- Le routeur final manipule les boîtes aux lettres des utilisateurs locaux :

```
localuser:
  driver = accept
  check_local_user
  transport = local_delivery
```

- Récapitulation - une adresse est routée comme ceci:
  - Adresse distante => remote_smtp transport
  - System_aliases => nouvelle adress(es), fail, defer
  - Utilisateur local => local_delivery transport
  - adresse non routable => rebond
- Juste un cas de configuration parmi tant d'autres

Routage vers les “smarthosts

- Remplacer le premier routeur par ceci

```
send_to_smarthost:
  driver = manualroute
  domains = ! +local_domains
  route_list = * smart-host1.example:\
                 smart-host2.example
  transports = route_smtp
```

- La règle route_list contient deux éléments séparés :
  - Le premier représente le domaine : * correspond à n'importe quel domaine
  - Le second est une liste de machines pour les domaines correspondants

Transports par défaut (1)

- Principaux transports

```
remote_smtp:
  driver = smtp


local_delivery:
  driver = appendfile
  file = /var/mail/$local_part
  delivery_date_add
  return_path_add
  envelope_to_add
# group = mail
# mode = 0660
```

- Le défaut suppose un répertoire avec “sticky bit”
  - Le paramétrage du groupe et du mode est une approche alternative

Transports par défaut(2)

- Transports auxiliaires

```
address_pipe:
  driver = pipe
  return_output

address_file:
  driver = appendfile
  delivery_data_add
  return_path_add
  envelope_to_add

address_reply:
  driver = autoreply
```

Les listes nommées

```
domainlist local_domains = @ : plc.com
hostlist   relay_hosts   = 192.168.32.0/24
```

- NB : la liste est spécifiée à un seul endroit
  Les références sont plus courtes et plus faciles à comprendre
- Optimisation: des correspondances dans les listes nommées sont mises en cache
  Exemple: plusieurs routeurs examinant la même liste de domaines
- Une liste nommée est référencée en mettant '+ ' devant son nom

```
hosts = 127.0.0.1 : +relay_hosts
```

- Une liste nommée peut être inversée
  domains = !+local_domains
  Ceci n'est pas possible avec les macros

ACLs

- Les ACL s'appliquent seulement aux SMTP entrants
  - Mais ils s'appliquent aussi aux SMTP locaux
- Pour les messages SMTP entrants
  - acl_smtp_rcpt définit le ACL à exécuter pour chaque RCPT
  - Le defaut est “deny”
  - acl_smtp_data définit le ACL à exécuter après DATA
  - Le défaut est “accept”
- Les tests sur le contenu de message peuvent seulement être faits après DATA
- D'autres ACLs peuvent être utilisés pour AUTH, ETRN, EXPN, VRFY

Un simple ACL

```
acl_smtp_rcpt = acl_check_rcpt

begin acl

acl_check_rcpt:
  accept   local_parts = postmaster
           domains     = +my_domains

  require  verify      = sender

  accept   domains     = +my_domains
           verify      = recipient
```

- Implicitement “deny” à la fin

Les modificateurs de ACL

- **Message définissant un message personalisé pour un refus ou un avertissement**

```
deny    message  = You are black listed at \
                   $dnslist_domain
        dnslists = rbl.mail-abuse.org : ...
```

- **log_message définit un message journal personalisé**

```
require log_message = Recipient verify failed
        verify      = recipient
```

- **"endpass" est utilisé avec le verbe "accept" pour des résultats spécifiques**

```
accept  domains  = +local_domains
        endpass
        verify   = recipient
```

  - **Au dessus de "endpass", l'échec cause l'éxecution de la prochaine déclaration**
  - **Au dessous de "endpoint", l'échec cause le rejet**

Les déclarations de ACL

- Chaque déclaration contient un « verbe » et une liste de conditions

```
verb      condition 1      (une par ligne)
          condition 2
          ...
```

- Si toutes les conditions sont remplies
  - “accept” Permet l'éxécution de la commande SMTP
  - “deny” Rejet (sinon passe)
  - “require” Passe (sinon rejet)
  - “warn” exécute une action d'avertissement (par exemple : écrire des journaux ou ajouter des entêtes) : Passe toujours

ACLs par défaut

```
acl_check_rcpt:
  accept  hosts         = :
  deny    local_parts = ^.*[@%!|/] : ^\\.
  accept  local_parts = postmaster
          domains       = +local_domains
  require verify        = sender
  accept  domains       = +local_domains
          endpass
          message       = unknown user
          verify        = recipient
  accept  domains       = +relay_to_domains
          endpass
          message       = unrouteable address
          verify        = recipient
  accept  hosts         = +relay_from_hosts
  accept  authenticated = *
  deny    message       = relay not permitted
```

Questions ???

Quelques commandes Exim

- exim –bp : voir la queue des messages.
- exim –Rff <domain> : forcer les messages pour <domain> à partir.
- exim –Mrm <idf> : suppression du message dont l'identifiant est <idf>
- exim –bh <hote> : vérifier le relayage pour <hote>
- mailq : pareil que exim -bp

Les journaux d'Exim

- Pour une installation à partir de sources (compilation), l'emplacement et les noms des fichiers log sont paramétrables.
- Pour notre exim4 de lenny, il s'agit de 3 fichiers :
  - mainlog : le traitement des mails (entrant et sortant)
  - rejectlog : les rejets de mails
  - paniclog : des problèmes d'exécution

Grandes installations

- Utilisez un serveur de nom local avec beaucoup de mémoire
- Exim est limité par les entrés/sorties disque
  - Utilisez un système disque rapide
  - Utiliser le **split_spool_directory**
  - Utilisez plusieurs répertoires pour les boîtes aux lettres
- Évitez les fichiers au mot de passe linéaire
- Utilisez le format maildir pour permettre les livraisons parallèles
- Projetez d'agrandir le système avec des serveurs parallèles
  - Ceci aide aussi à ajouter plus de capacité disque

Questions ???