

# Applications DHCP et Mails – Sommaire

## Service DHCP DHCP

## Services mails

Courrier électronique, principe, agents, et Mime  
SMTP, POP, IMAP  
Serveurs mails

# DHCP

- *Dynamic Host Configuration Protocol (RFC 2131)*
- offrir dynamiquement pour une durée choisie à une machine qui ne possède pas d'adresse IP, une configuration réseau comprenant :
  - adresse IP, masque
  - routeur par défaut
  - nom d'hôte
  - adresses des serveurs DNS
  - adresse de serveur SMTP
- boot depuis le réseau
- interaction DNS

## Problème

- comment communiquer sans adresse IP ?
  - Adresse MAC identifiant unique présent dans les interfaces 802.X et donc dans celle du client
  - Utilisation de la diffusion de niveau 2 (ff:ff:ff:ff:ff:ff)
  - Utilisation des adresse IP réservées 0.0.0.0 et 255.255.255.255
  - Utilisation d'UDP
- Comment réutiliser les adresses déjà utilisées ?
  - allocation pour une durée fixée : un bail
  - utilisation d'option : Requested IP Address

## DHCP : protocole

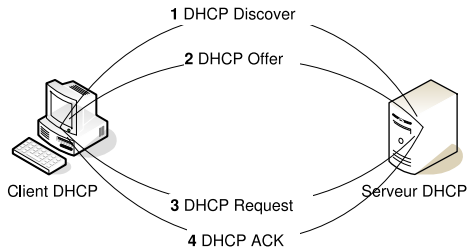


Figure: Protocole DHCP

## DHCP : protocole

- DHCP Discover : trouver un serveur DHCP dont l'adresse IP est inconnue :
  - Niveau 2 (@MAC vers ff:ff:ff:ff:ff:ff)
  - Niveau 3 (0.0.0.0 vers 255.255.255.255)
  - Niveau 4 (UDP 68 vers 67)
  - Niveau 7 (Info sur son adresse MAC, la dernière @IP obtenue, )
- DHCP Offer : le ou les serveurs de DHCP proposent :
  - Un bail et l'adresse IP du serveur DHCP avec un identifiant de transaction

## DHCP : protocole

- DHCP Request : le client répond à tous les serveurs pour indiquer quelle offre il accepte :
  - Niveau 2 (@MAC vers ff:ff:ff:ff:ff:ff)
  - Niveau 3 (0.0.0.0 vers 255.255.255.255)
  - Niveau 4 (UDP 68 vers 67)
  - Niveau 7 (@MAC Client, @IP Client, @IP Serveur, identifiant de transaction)
- DHCP ACK : le client accepte définitivement le bail et le serveur peut marquer l'adresse comme étant utilisée

## DHCP : capture résumée

```
1  0.000000      0.0.0.0 → 255.255.255.255
DHCP 342 DHCP Discover - Transaction ID 0x964a3437
2  0.000281 04:8d:38:cf:7d:cd → Broadcast
ARP 42 Who has 10.0.42.10? Tell 10.0.42.42
3  0.998684 04:8d:38:cf:7d:cd → Broadcast
ARP 42 Who has 10.0.42.10? Tell 10.0.42.42
4  1.001508 10.0.42.42 → 10.0.42.10
DHCP 342 DHCP Offer    - Transaction ID 0x964a3437
5  1.005558      0.0.0.0 → 255.255.255.255
DHCP 342 DHCP Request  - Transaction ID 0x964a3437
6  1.005767 10.0.42.42 → 10.0.42.10
DHCP 342 DHCP ACK      - Transaction ID 0x964a3437
```

## DHCP : détail Discover

Ethernet II, Src: 04:8d:38:cf:7d:41, Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255

User Datagram Protocol, Src Port: 68, Dst Port: 67

Dynamic Host Configuration Protocol (Discover)

Message type: Boot Request (1)

Client IP address: 0.0.0.0

Your (client) IP address: 0.0.0.0

Next server IP address: 0.0.0.0

Relay agent IP address: 0.0.0.0

Client MAC address: 04:8d:38:cf:7d:41 (04:8d:38:cf:7d:41)

Server host name not given      Boot file name not given

Option: (53) DHCP Message Type (Discover)

Option: (12) Host Name : debian

Option: (55) Parameter Request List

Parameter Request List Item: (1) Subnet Mask

Parameter Request List Item: (28) Broadcast Address

Parameter Request List Item: (2) Time Offset

Parameter Request List Item: (3) Router

Parameter Request List Item: (15) Domain Name

Parameter Request List Item: (6) Domain Name Server

Parameter Request List Item: (119) Domain Search

Parameter Request List Item: (12) Host Name

Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server



## DHCP : détail Offer

```
Ethernet II, Src: 04:8d:38:cf:7d:cd, Dst: 04:8d:38:cf:7d:41
Internet Protocol, Src: 10.0.42.42 (10.0.42.42), Dst: 10.0.42.10 (10.0.42.10)
User Datagram Protocol, Src Port: 67, Dst Port: 68
Dynamic Host Configuration Protocol (Offer)
  Message type: Boot Reply (2)
  Client IP address: 0.0.0.0
  Your (client) IP address: 10.0.42.10
  Next server IP address: 0.0.0.0
  Relay agent IP address: 0.0.0.0
  Client MAC address: 04:8d:38:cf:7d:41 (04:8d:38:cf:7d:41)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  Option: (53) DHCP Message Type (Offer)
  Option: (54) DHCP Server Identifier: 10.0.42.42
  Option: (51) IP Address Lease Time: (600s) 10 minutes
  Option: (1) Subnet Mask: 255.255.255.0
  Option: (3) Router: 10.0.42.254
  Option: (15) Domain Name: fai.com
  Option: (6) Domain Name Server: 192.168.0.254
  Option: (255) End
```

## DHCP : détail Request

Ethernet II, Src: 04:8d:38:cf:7d:41, Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255

User Datagram Protocol, Src Port: 68, Dst Port: 67

Dynamic Host Configuration Protocol (Request)

Message type: Boot Request (1)

Client IP address: 0.0.0.0 Your (client) IP address: 0.0.0.0

Next server IP address: 0.0.0.0 Relay agent IP address: 0.0.0.0

Client MAC address: 04:8d:38:cf:7d:41 (04:8d:38:cf:7d:41)

Server host name not given Boot file name not given

Option: (53) DHCP Message Type (Request)

Option: (54) DHCP Server Identifier: 10.0.42.42

Option: (50) Requested IP Address: 10.0.42.10

Option: (12) Host Name: debian

Option: (55) Parameter Request List

Parameter Request List Item: (1) Subnet Mask

Parameter Request List Item: (28) Broadcast Address

Parameter Request List Item: (2) Time Offset

Parameter Request List Item: (3) Router

Parameter Request List Item: (15) Domain Name

Parameter Request List Item: (6) Domain Name Server

Parameter Request List Item: (119) Domain Search

Parameter Request List Item: (12) Host Name

Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server

## DHCP : détail ACK

```
Ethernet II, Src: 04:8d:38:cf:7d:cd, Dst: 04:8d:38:cf:7d:41
Internet Protocol Version 4, Src: 10.0.42.42, Dst: 10.0.42.10
User Datagram Protocol, Src Port: 67, Dst Port: 68
Dynamic Host Configuration Protocol (ACK)
  Message type: Boot Reply (2)
  Client IP address: 0.0.0.0
  Your (client) IP address: 10.0.42.10
  Next server IP address: 0.0.0.0
  Relay agent IP address: 0.0.0.0
  Client MAC address: 04:8d:38:cf:7d:41 (04:8d:38:cf:7d:41)
  Server host name not given
  Boot file name not given
  Option: (53) DHCP Message Type (ACK)
  Option: (54) DHCP Server Identifier: 10.0.42.42
  Option: (51) IP Address Lease Time: (600s) 10 minutes
  Option: (1) Subnet Mask: 255.255.255.0
  Option: (3) Router: 10.0.42.254
  Option: (15) Domain Name: fai.com
  Option: (6) Domain Name Server: 192.168.0.254
  Option: (255) End
```

## Gestion du bail

- pour ne pas épuiser le stock d'adresses IPs disponibles, les serveurs les allouent pour un temps donné
- un client doit toujours avoir une adresse IP  $\Rightarrow$  (Selon les clients)
  - à 50% du bail le client demande au serveur qui a fourni le bail de le renouveler  $\Rightarrow$  DHCP REQUEST + DHCP ACK
  - à 87,5% du bail le client demande un nouveau bail auprès de tous les serveurs  $\Rightarrow$  possibilité de changer d'adresse IP

## Architecture DHCP

- des clients
- des serveurs
- des relais (sur les routeurs)
- + tolérance aux pannes (redondance des serveurs)

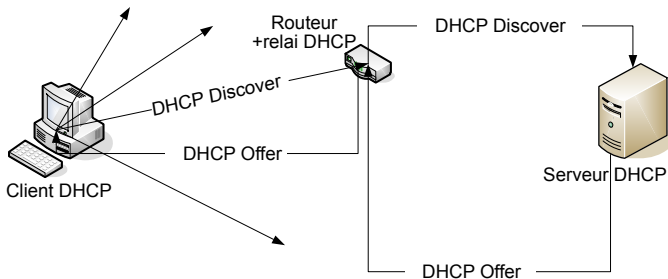


Figure: Architecture DHCP

## Éléments de configuration (client)

```
#send host-name "andare.fugue.com";
#send dhcp-client-identifier 1:0:a0:24:ab:fb:9c;
#send dhcp-lease-time 3600;
#supersede domain-name "fugue.com home.vix.com"; # on va utiliser ça
request subnet-mask, broadcast-address, time-offset, routers,
        domain-name, domain-name-servers, host-name,
        netbios-name-servers, netbios-scope; # on voudrait
require subnet-mask, domain-name-servers; # on exige
timeout 60; # tps avant de considérer que personne ne répond
retry 60; # délai avant nouvelle tentative
reboot 10; # si reboot, on veut la même ip sinon, délai avant demande new
select-timeout 5; # délai avant d'accepter une autre offre
#script "/etc/dhcp3/dhclient-script"; # script à exécuter
#reject 192.33.137.209; # on ne veut pas d'offre de cette ip
#lease { # bail par défaut si je n'arrive pas à contacter un serveur
#   interface "eth0";
#   fixed-address 192.33.137.200;
#   option host-name "andare.swiftmedia.com";
#   option subnet-mask 255.255.255.0;
#   option broadcast-address 192.33.137.255;
#   option routers 192.33.137.250;
#   option domain-name-servers 127.0.0.1;
#   renew 2 2000/1/12 00:00:01;
```

## Éléments de configuration (serveur)

```
option domain-name "example.org"; # Nom de domaine
option domain-name-servers 192.168.10.1 ; #serveurs dns
default-lease-time 600 ;# Duree par default de l'attribution d'adresse
max-lease-time 7200; # Duree maximale de l'attribution d'adresse

subnet 10.254.239.0 netmask 255.255.255.224 {
    range 10.254.239.10 10.254.239.20;
    option routers rtr-239-0-1.example.org, rtr-239-0-2.example.org;
}
subnet 192.168.10.0 netmask 255.255.255.0 {
    range 192.168.10.26 192.168.10.30;
    option domain-name-servers ns1.internal.example.org;
    option domain-name "internal.example.org";
    option routers 192.168.10.254;
}
host fantasia {
    hardware ethernet 08:00:07:26:c0:a5;
    fixed-address 192.168.10.10;}
host passacaglia {
    hardware ethernet 0:0:c0:5d:bd:95;
    filename "vmunix.passacaglia";
    server-name 192.168.10.2;}
```

## Courrier électronique

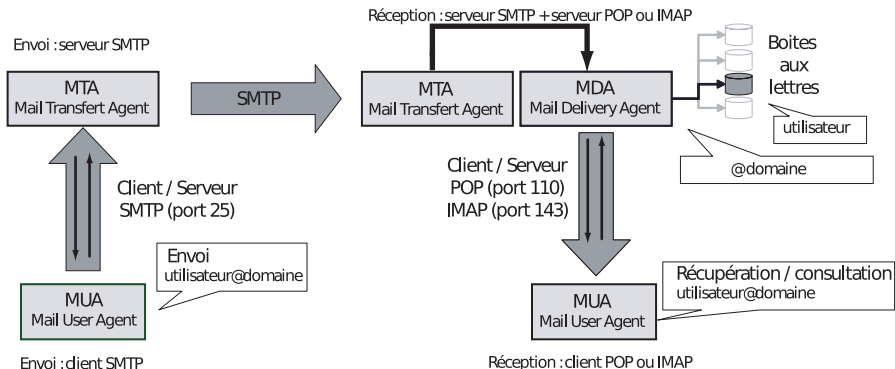
- un des premiers services d'Internet
- adresses FQDN :  
nom@domaine  
ex : Jean-Francois.Remm@univ-nantes.fr
- exemple de mail type :

```
To: Jean-Francois.Remm@univ-nantes.fr  
From: Guillaume.Connand@somewhere.co.uk  
Subject: I miss you
```

```
How are you ?
```



# Principe



## Agents du mail

- le service de mail est constitué de plusieurs fonctions :
  - MTA : Un *Mail Transfert Agent* envoie, reçoit, route les messages suivant le protocole SMTP.
  - MDA : L'écriture des messages dans les boîtes aux lettres se fait par les *Mail Delivery Agent*.
  - MUA : Les logiciels de messagerie qui permettent de rédiger des messages ou consulter sa boîte aux lettres sont des *Mail User Agent*. Bien souvent, les MUA consultent les boîtes aux lettres sur des machines distantes par les protocoles POP ou IMAP.
- le service est organisé de manière à ne pas perdre de message. L'expéditeur ne reçoit de notification que lorsque la délivrance au destinataire n'a pu se faire.

## Contenu du mail

- Un courrier se compose :
  - d'une enveloppe utilisée par l'agent de transfert
  - d'un message lui-même subdivisé en :
    1. entête (header)
    2. corps (body)[1] utilisés par l'agent utilisateur
- documenté par la RFC 822
- puis MIME (RFC 1341 à 1345, puis RFC 2045 à 2049).

<b>Enveloppe</b> MAIL From: origine RCPT To: destination
<b>En-tête</b> - Received: - Message-Id: - From: - Date: - Reply-To: - To: - Cc: copie - Bcc: copie secrète - Subject:
<b>corps</b>

# MIME

- à l'origine un courrier ne comportait que du texte (ASCII)
- besoin d'envoyer des caractères non ASCII (accentués), des contenus non textuels, des contenus multiples
- définition d'entêtes supplémentaires :
  - `MIME-Version` : encore 1.0 pour "annoncer" la suite
  - `Content-Type` : 7 types principaux : `text`, `image`, `audio`, `video`, `application`, `multipart`, `message` et des sous-types (d'où `text/plain`, `image/jpeg`, `multipart/form-data`,...).
  - `Content-Transfert-Encoding` : `Quoted-Printable`, `Base64`, `7bit`

## SMTP

- le protocole SMTP est le protocole de transport des mails. Les messages sortant font appel à SMTP pour passer de l'ordinateur client à l'ordinateur serveur, d'où ils partent pour leur destination finale. Ce protocole permet à deux serveurs de messagerie différents de communiquer.
- SMTP *Simple Mail Transert Protocol* RFC 821 (1982) puis maintenant RFC 5321 (2008)
  - base de SMTP : ouverture/ fermeture de transaction : HELO, QUIT
  - commandes d'envoi d'un mail : RCPT TO, MAIL FROM, DATA
  - obsolète ? VRFY : verification du nom d'un utilisateur ; EXPN : expansion d'une mailing list
  - pas vraiment prévu pour le spam : aucune authentification de base !
- ESMTP RFC 1869 : ajout d'extensions.
  - Un client débute une transaction par EHLO
  - le serveur répond (code 250) par la liste des extensions prise en charge.

## Dialogue SMTP (Simple)

```
$ telnet smtp.mazone.com smtp
Trying smtp.mazone.com...
Connected to smtp.mazone.com
Escape character is '^]'.
220 smtp.mazone.com ESMTP Postfix (Release-XXXX)
EHLO tp.mazone.fr
250-smtp.mazone.com
250-PIPELINING
250-SIZE 10240000
250-ETRN
250 8BITMIME
MAIL FROM:<moi@labas.fr>
250 Ok
RCPT TO:<user@mazone.com>
250 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
bonjour,
comment ça va?
je suis en train de faire des tests sur SMTP
bon, j'arrête...
.
250 Ok: queued as 4AEC610332
```

## Dialogue SMTP (Capture réelle)

```
220 smtp.houla.com ESMTP Service (7.2.060.1) ready
EHLO [192.168.2.100]
250-smtp.houla.com
250-DSN
250-8BITMIME
250-PIPELINING
250-HELP
250-AUTH=LOGIN
250-AUTH LOGIN CRAM-MD5 DIGEST-MD5 PLAIN
250-DELIVERBY 300
250 SIZE 10485760
AUTH CRAM-MD5
334 PENGmzi4NzBMOU3NTBFmjg1OUFCMzREN0IwMOZBMOBzbxRwaW4ubGFwb3NOZS5uZXQ+
amVhbi1mcmFuY21pcy5yZW1tIGQxNTJhNWVmNTlhYmE1MWRmNmQ2YTQyZTczOGIyNDcy
235 CRAM-MD5 authentication successful
```

## Dialogue SMTP (Capture réelle)

```
MAIL FROM:<jean.martin@houla.com> SIZE=388
250 MAIL FROM:<jean.martin@houla.com> OK
RCPT TO:<jean.martin@houla.com>
250 RCPT TO:<jean.martin@houla.com> OK
DATA
354 Start mail input; end with <CRLF>.<CRLF>
Message-ID: <456357A2.8070706@houla.com>
Date: Tue, 21 Nov 2006 20:46:42 +0100
From: =?ISO-8859-1?Q?Jean_Martin?=
    <jean.martin@houla.com>
User-Agent: Thunderbird X.Y.Z.T (Windows/AAAAMMJJ)
MIME-Version: 1.0
To: jean.martin@houla.com
Subject: Test
Content-Type: text/plain; charset=ISO-8859-1; format=flowed
Content-Transfer-Encoding: 7bit
```

Test

```
.
250 <4562233E00008C5D> Mail accepted
```



## Consultation

- consultation locale : à l'origine le MDA écrivait les mails dans un espace accessible à l'utilisateur (dans son HOME)
- consultation distante :
  1. POP (Post Office Protocol)
  2. IMAP (Internet Message Access Protocol)

# POP

- POP3 *Post Office Protocol* RFC 1225
  - permet de se connecter, déconnecter, supprimer des messages, de charger des courriers d'un serveur distant en les recopiant en local
  - utilise le port 110 (995 pour le Pop3s)

## Dialogue POP (Simple)

```
$ telnet pop.mazone.fr pop3
Trying pop.mazone.fr...
Connected to pop.mazone.fr
Escape character is '^]'.
+OK Qpopper (version 4.0.5) at pop.mazone.com starting.
user user
+OK Password required for user.
pass user
+OK user has 5 visible messages (0 hidden) in 2179 octets.
list
+OK 5 visible messages (2179 octets)
1 441
2 441
3 451
4 440
5 406
.
```

## Dialogue POP (Simple)

```
retr 2
+OK 441 octets
Return-Path: <moi@labas.fr>
Delivered-To: user@mazone.com
Received: from toto (localhost.localdomain [127.0.0.1])
    by smtp.mazone.com (Postfix) with ESMTP id B31581AAD4
    for <user@mazone.com>; Thu, 6 Dec 2001 15:30:16 -0500 (EST)
Message-Id: <20011206203016.B31581AAD4@smtp.mazone.com>
Date: Thu, 6 Dec 2001 15:30:16 -0500 (EST)
From: moi@labas.fr
To: undisclosed-recipients:;
X-UIDL: 6*F!!V4W!!"pZ!!M"a!!
Status: U
```

Message...

```
.
```

```
delete 2
+OK Message 2 has been deleted.
noop
+OK
rset
+OK Maildrop has 5 messages (2179 octets)
```

## Dialogue POP (Capture réelle)

```
+OK POP3 server ready (7.2.060.1) <E65E3A20B4DB76BC524571F5996D6C5E3DF4F129@mx.
CAPA
+OK Capability list follows
TOP
RESP-CODES
USER
SASL CRAM-MD5 DIGEST-MD5 PLAIN
PIPELINING
UIDL
IMPLEMENTATION CPMS-7.2.060.1
AUTH-RESP-CODE
.
AUTH PLAIN
+ go ahead
dXNlcmB1c2VyAG1vdGRlcGFzc2VDb21wbG1xdWU=
+OK 1 messages
STAT
+OK 1 1001
LIST
+OK
1 1001
.
UIDL
```

## Dialogue POP (Capture réelle)

RETR 1

+OK 1001 bytes

Return-Path: <jean.martin@houla.com>

Received: from smtp.houla.com (10.150.9.41) by mx.houla.com (7.2.060.1)

id 455B90E1005E27BD for jean.martin@houla.com; Tue, 21 Nov 2006 20:59:1

Received: from smtp.houla.com (10.150.9.73) by smtp.houla.com (7.3.105.2)

id 455CB19700554532 for jean.martin@houla.com; Tue, 21 Nov 2006 20:59:1

Received: from [192.168.2.100] (84.6.84.85) by smtp.houla.com (7.2.060.1) (auth

id 456222D000008FF0 for jean.martin@houla.com; Tue, 21 Nov 2006 20:59:1

Message-ID: <45635A93.5060504@houla.com>

Date: Tue, 21 Nov 2006 20:59:15 +0100

From: =?ISO-8859-1?Q?Jean\_Martin?=  
<jean.martin@houla.com>

User-Agent: Thunderbird 1.5.0.4 (Windows/20060516)

MIME-Version: 1.0

To: jean.martin@houla.com

Subject: Test

Content-Type: text/plain; charset=ISO-8859-1; format=flowed

Content-Transfer-Encoding: 7bit

Test

.

DELE 1

## IMAP

- IMAP *Internet Message Access Protocol* RFC 1024 (V4 RFC3501 2003)
  - plus évolué
  - les mails peuvent être classés dans différents dossiers créés sur le serveur.
  - tous les mails sont conservés sur le serveur, ils sont donc tous accessible depuis différents endroits avec différents clients mails.
  - la connexion entre le client et le serveur mail est persistante, ce qui permet au client de savoir instantanément si de nouveaux messages sont arrivés sur le serveur.
  - utilise le port 143 (993 pour IMAPs)

## Dialogue IMAP (Capture réelle)

```
* OK IMAP4 server ready (7.2.060.1)
1 capability
* CAPABILITY IMAP4 IMAP4rev1 UIDPLUS IDLE NAMESPACE QUOTA CHILDREN AUTH=CRAM-MD
  AUTH=DIGEST-MD5 AUTH=PLAIN
1 OK capabilities listed
2 authenticate plain
+ go ahead
dXNlcbG1c2VyAG1vdGRlcGFzc2VDb21wbGlxdWU=
2 OK login successful
3 namespace
* NAMESPACE ((" " /")) NIL NIL
3 OK NAMESPACE completed
4 lsub "" "*"
* LSUB (\HasNoChildren) "/" "Courriers Suspects"
4 OK LSUB completed
5 list "" "INBOX"
* LIST (\NoInferiors) NIL INBOX
5 OK LIST completed
6 list "" "Trash"
* LIST (\HasNoChildren) "/" Trash
6 OK LIST completed
7 create "Trash"
7 NO mailbox already exists
```



## Principaux serveurs

- Sendmail : historique, difficile à configurer
- exim
- postfix
- microsoft
- ...

## Configuration Serveur (Postfix)

- postfix se configure essentiellement dans un fichier `/etc/postfix/mail.cf`
- les principales informations à paramétrer sont :
  - `myorigin` : domaine qui apparaît dans le courrier envoyé à partir de cette machine (défaut : `$myhostname`) souvent remplacé par `$mydomain`)
  - `mydestination` : liste des domaines mail avec délivrance locale (ex : `domain.com`, etc.) plutôt qu'une retransmission à une autre machine
  - `myhostname` : nom pleinement qualifié du serveur
  - `mydomain` : nom du domaine principal du serveur
  - `inet_interface` : sur quelles interfaces on écoute (`all`, `localhost`, `$myhostname`)
  - `mynetworks` : contient la liste des IP/réseaux qui sont autorisés à envoyer des mails à partir de ce serveur (pour l'antirelais)
  - ...

## Exemple

```
queue_directory = /var/spool/postfix
command_directory = /usr/sbin
daemon_directory = /usr/libexec/postfix
mail_owner = postfix
mydomain = exemple.fr
myorigin = $mydomain
mydestination = $mydomain, machine.exemple.fr
sender_canonical_maps = hash:/etc/postfix/revaliases
alias_maps = hash:/etc/postfix/aliases, hash:/var/mailman/data/aliases
alias_database = hash:/etc/postfix/aliases, hash:/var/mailman/data/aliases
mynetworks = 195.18.103.0/24, 127.0.0.0/8
local_destination_concurrency_limit = 2
default_destination_concurrency_limit = 10
debug_peer_level = 2
content_filter= vscan:
default_mailbox_size = 20480000
mailbox_size_limit = 20480000
message_size_limit = 20480000
```