Configurare un server mail

exim + dovecot FTW

Alessandro Di Federico

ale@clearmind.me

EA2F 42F5 173F 63D9 1C0A
2695 BEFD AF3D 6FDC B177

Corsi Linux Avanzati 2015
Politecnico Open unix Lab

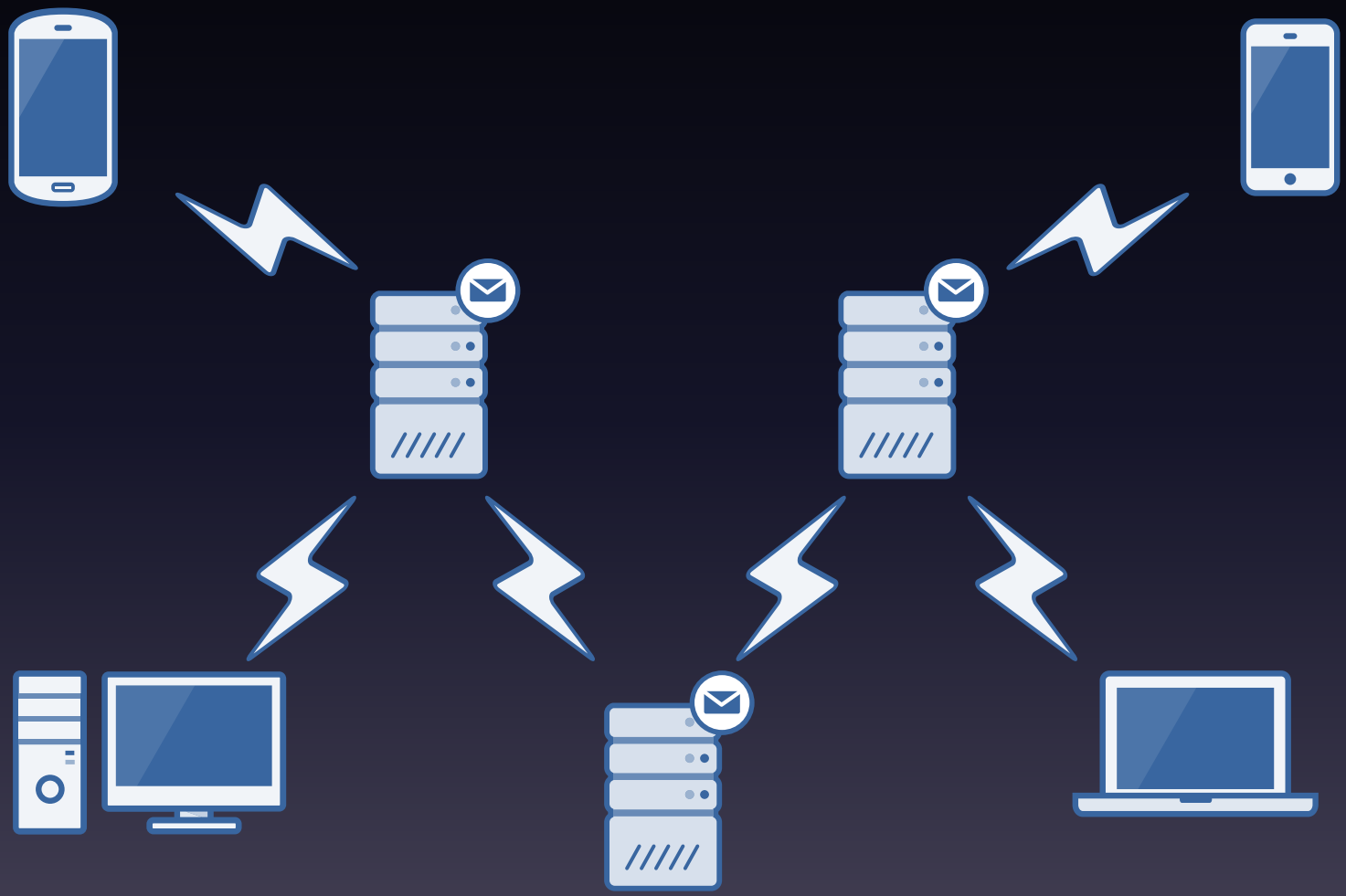
31 marzo 2015

Indice

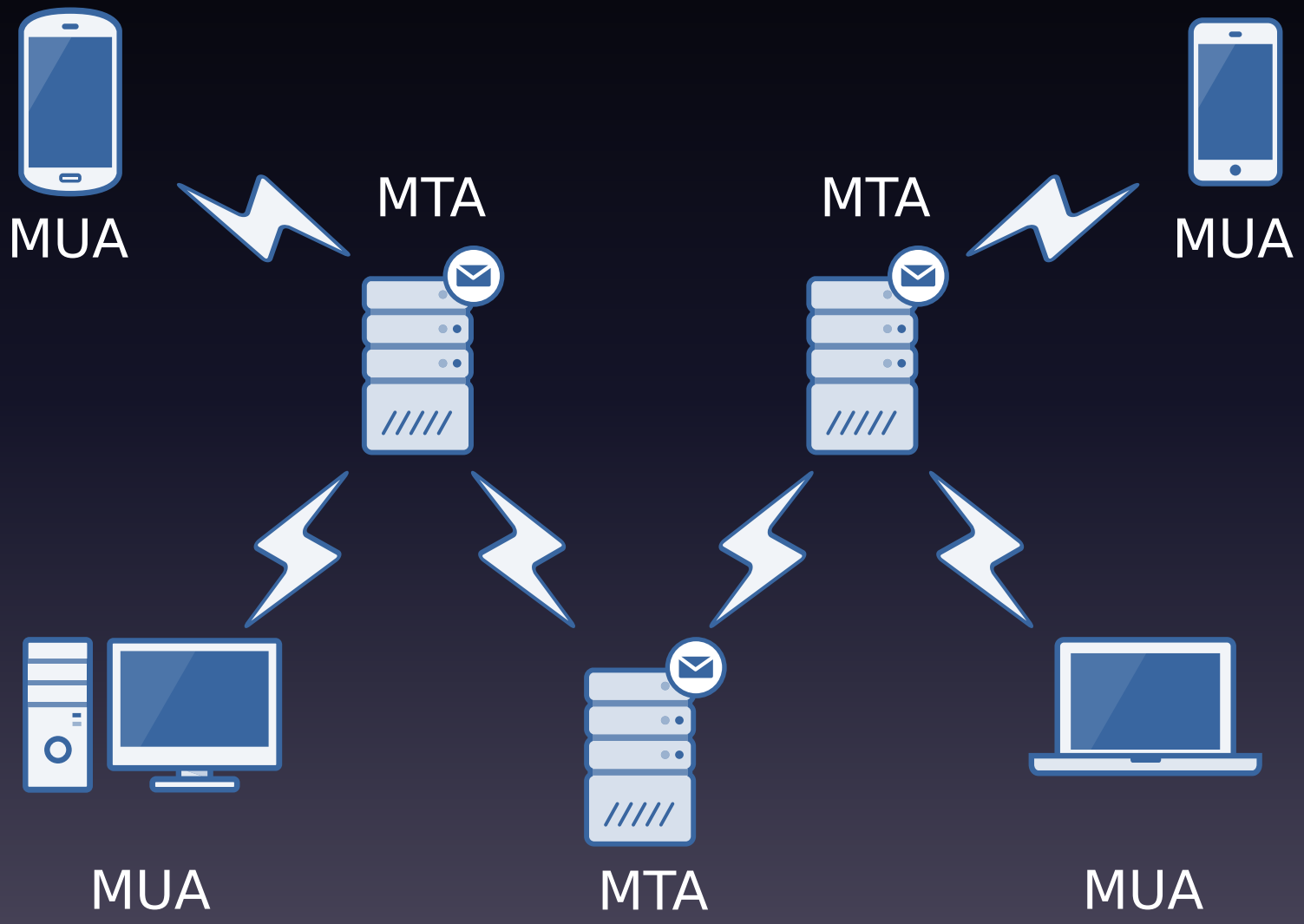
Cosa faremo oggi

- Impareremo a configurare un server e-mail
- Potremo ricevere ed inviare e-mail
- Offrire caselle di posta per gli utenti
- Vedremo come evitare di essere classificati spam

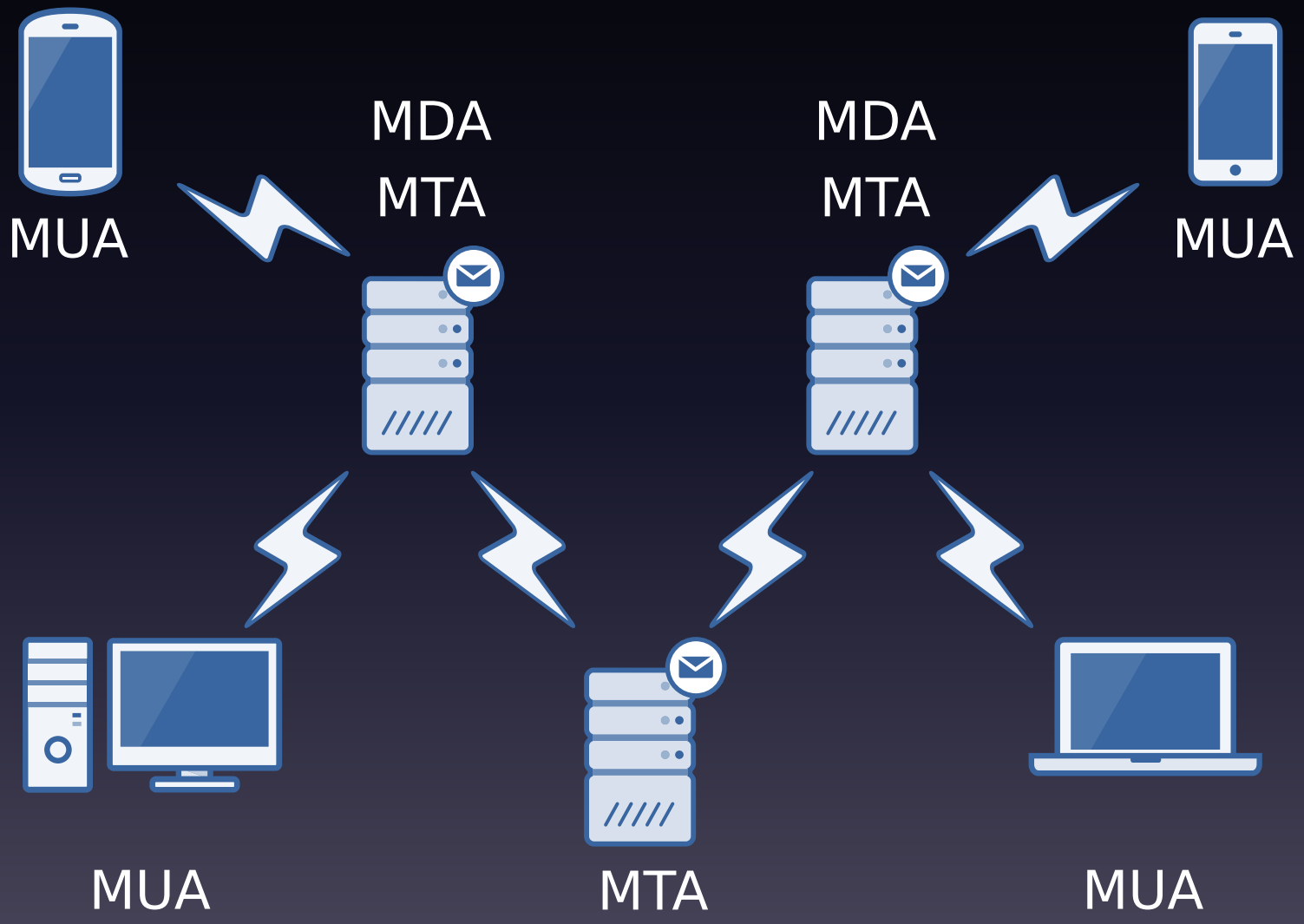
Panoramica sulla posta elettronica



Panoramica sulla posta elettronica



Panoramica sulla posta elettronica



Ricapitolando

- Il Mail User Agent (MUA) è il client utilizzato dell'utente
- Il Mail Transfer Agent (MTA) riceve e inoltra la posta
- Il Mail Delivery Agent (MDA) stocca la posta per il MUA

I protocolli

Attori	Operazione	Protocollo	Porte
MTA $\leftrightarrow$ MTA	Inoltro	SMTP[1]	25 o 465
MUA $\leftrightarrow$ MTA	Invio		
MUA $\leftrightarrow$ MDA	Ricezione	POP3[2]	110 o 995
		IMAP[3]	143 o 993

[1] Simple Mail Transfer Protocol (RFC 5321)
[2] Post Office Protcol 3 (RFC 1939)
[3] Internet Message Access Protocol (RFC 3501)

Cosa accade quando si invia un messaggio?

1. Il client si collega al server SMTP

smtp.clearmind.me

2. Il client chiede di inviare una mail a info@poul.org

From: Ale <ale@clearmind.me>
To: POuL <info@poul.org>
Subject: Saluti

smtp.clearmind.me

3. Il server ottiene il record MX per poul.org

MX for poul.org?

smtp.clearmind.me

dns.opennic.org

3. Il server ottiene il record MX per poul.org

smtp.poul.org

smtp.clearmind.me

dns.opennic.org

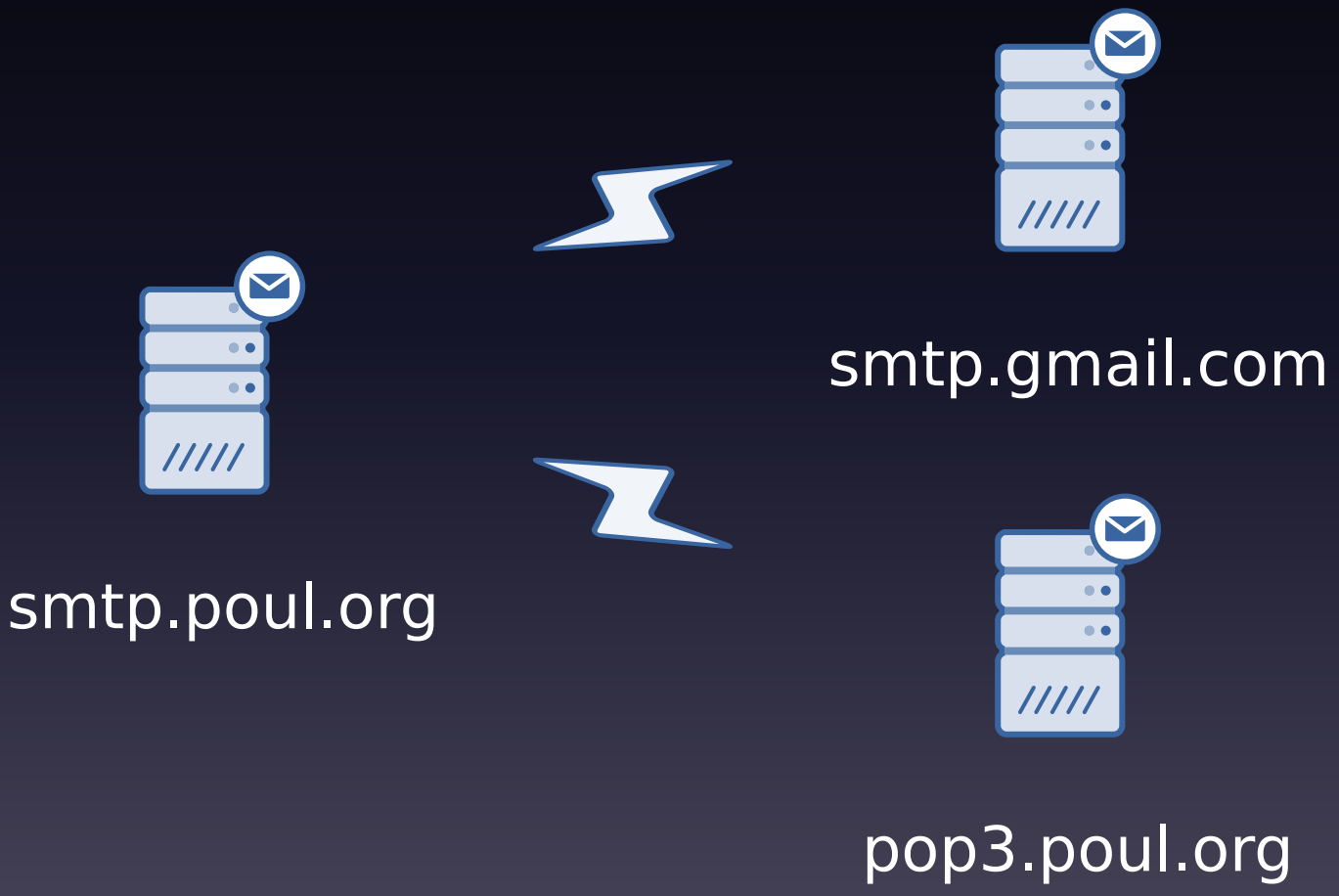
4. Il server si collega a smtp.poul.org e consegna l'e-mail

From: Ale <ale@clearmind.me>
To: POuL <info@poul.org>
Subject: Saluti

smtp.clearmind.me

smtp.poul.org

5. Il server SMTP di destinazione decide se:
    1. Inoltrare la mail ad un altro MTA
    2. Passare la mail al MDA perché la immagazzini



Demo

Indice

Exim

- Exim è un server SMTP:
  - Rilasciato sotto licenza GPL
  - Ricco di feature e configurabile
  - Affidabile e leggero

Cosa c’è da configurare

/etc/exim/exim.conf

- La configurazione di default è un ottima partenza[4]
- Configureremo:
  - Dominio, IP e porte da utilizzare
  - TLS
  - Autenticazione
  - Come archiviare la posta

[4] Assumeremo di partire dalla configurazione di default ufficiale: https://github.com/Exim/exim/blob/master/src/src/configure.default

Coordinate del server

```
# Nome della macchina su cui gira il demone
primary_hostname = poul.org

# Domini da accettare come locali, ovvero
# gestiti dalla nostra istanza di exim.
domainlist local_domains = @

# Indirizzi IP su cui ascoltare
local_interfaces = 91.121.220.9

# Porte da utilizzare
daemon_smtp_ports = 25

remote_smtp:
  driver = smtp
  # Forza uno specifico IP per la posta in uscita
  interface = 91.121.220.9
```

TLS, chi è costui?

SSL? STARTLS? TLS?

Abilitare TLS

1. Ottenere un certificato da una CA[5]
2. Concatenare in formato PEM in un unico file:
    1. chiave segreta
    2. certificato per poul.org
    3. certificati intermedi
3. Salvarlo in /etc/ssl/private/poul-org-key-crt-ca.pem[6]

[5] StartSSL offre certificati riconosciuti gratuitamente

[6] Purtroppo, per come è strutturato exim, questo file non può essere leggibile solo da root, ma anche l'utente di exim deve potervi accedere

Abilitare TLS

```
# Permetti a tutti i client di utilizzare TLS
tls_advertise_hosts = *

# Ascolta anche sulla porta 465
daemon_smtp_ports = 25 : 465

# Utilizza esclusivamente TLS sulla 465
tls_on_connect_ports = 465
```

Configurare TLS

```
# Crypto voodoo
# Ulteriori informazioni:
# https://bettercrypto.org/
openssl_options = +all +no_sslv2 +no_compression +
    cipher_server_preference +no_sslv3
tls_require_ciphers = EECDH+aRSA+AESGCM:EDH+aRSA+
    AESGCM:EECDH+aRSA+SHA384:EECDH+aRSA+SHA256:EECDH:
    EDH+aRSA:CAMELLIA:AES:!RC4:!SEED:!aNULL:!eNULL:!
    LOW:!3DES:!MD5:!EXP:!PSK:!SRP:!DSS:!DES

tls_certificate = /etc/ssl/private/key-crt-ca.pem
```

Autenticazione tramite file

- Di default ogni utente del sistema ha un account
- Talvolta questo non è desiderabile
- Vediamo come gestire gli utenti tramite un file:

```
# /etc/mail/passwd
# user:password_md5::
# Per calcolare l'hash MD5 della password:
# printf password | md5sum
ale:08cf56a1e2c7d2da70c03b861e6dd506::
ff:58ee09937d51f3886dcd0c0ea91c053e::
admiral0:d94250c8428a6181d209eb5aa3eb8cdf::
```

Modificare il driver localuser

```
localuser:
  driver = accept
  local_parts = lsearch;/etc/mail/passwd
# check_local_user
# local_part_suffix = +* : -*
# local_part_suffix_optional
  transport = local_delivery
  cannot_route_message = Unknown user
```

Modificare l'autenticazione PLAIN

```
plain_server:
  driver = plaintext
  public_name = PLAIN
  server_prompts = :
  server_set_id = $auth2

  # Exim voodoo
  server_condition = "\
    ${if exists{/etc/mail/passwd}\
      {${lookup{$2}lsearch{/etc/mail/passwd}\
        {${if crypteq{$3}{\\\{md5\\\}\
          ${extract{1}{:}{$value}{$value}fail}}\
          {true}{false} }}\
        fail }}\
      fail }"
```

Archiviare la posta in maildir

- Di default exim usa il formato mailbox
- Tutta la posta in un singolo file:
  - enorme e poco gestibile
  - ricerche lente
  - soggetto a corruzione
- Il formato maildir salva un file per messaggio

Archiviare la posta in maildir

```
local_delivery:
  driver = appendfile
  # Directory delle caselle
  directory = /var/mail/$local_part
  # Utilizziamo maildir
  maildir_format = true
  delivery_date_add
  envelope_to_add
  return_path_add
  # Utilizziamo l'utente "mail"
  user = mail
  group = mail
  mode = 0660
```

Impostare il record MX!

And we’re good to go
/etc/init.d/exim start

Demo

Indice

Cos’è dovecot?

- È un server POP3 e IMAP
- Rilasciato sotto licenze MIT e LGPLv2
- Vedremo come configurare POP3
- Utilizzeremo lo stesso file di autenticazione di exim

Configurazione di base

/etc/dovecot/dovecot.conf

```
# Protocols we want to be serving.
protocols = pop3

# A comma separated list of IPs or hosts where to
# listen in for connections.
listen = 5.135.157.69

# Greeting message for clients.
login_greeting = YOLO.
```

Abilitiamo POP3

/etc/dovecot/conf.d/10-master.conf

```
service pop3-login {
  inet_listener pop3 {
    port = 110
  }
}
```

Caselle e-mail

Stessa directory e utente di exim:

/etc/dovecot/conf.d/10-mail.conf

```
mail_location = maildir:/var/mail/%u

# Impostiamo l'utente da usare per accedere alle
# caselle. 8 e 12 sono gli identificativi dell'utente
# e del gruppo "mail". Per verificare quali sono:
# sudo -u mail id

first_valid_uid = 8
last_valid_uid = 8
first_valid_gid = 12
last_valid_gid = 12
mail_uid = mail
mail_gid = mail
```

Autenticazione da /etc/mail/passwd

/etc/dovecot/conf.d/10-auth.conf

```
# Abilitiamo l'autenticazione in chiaro
disable_plaintext_auth = no

# ...

# Disabilitiamo il login tramite utente di sistema
#!include auth-system.conf.ext
# ...
# Abilitiamo il login tramite /etc/mail/passwd
!include auth-passwdfile.conf.ext
```

Autenticazione da /etc/mail/passwd

/etc/dovecot/conf.d/auth-passwdfile.conf.ext

```
passdb {
  driver = passwd-file
  args = scheme=PLAIN-MD5 username_format=%u /etc/mail
      /passwd
}

userdb {
  driver = passwd-file
  args = username_format=%u /etc/mail/passwd
}
```

TLS

/etc/dovecot/conf.d/10-ssl.conf

/etc/dovecot/conf.d/10-ssl.conf

Esercizio al lettore

Demo

Indice

Non vogliamo essere classificati come spam

Tre cose da fare:

1. SPF
2. DKIM
3. rDNS

Non vogliamo essere classificati come spam

Tre cose da fare:

1. SPF
2. DKIM
3. rDNS
4. Non mandare spam

Sender Policy Framework (SPF)

- Associazione tra un dominio e i suoi server SMTP
- Informazione codificata in un record DNS di tipo TXT
- Microsoft offre un buon wizard[7]
- Policy suggerita[8]:

  v=spf1 mx -all

  O in fase di test:

  v=spf1 mx ~all

[7] https://www.microsoft.com/mscorp/safety/content/technologies/senderid/wizard/
[8] Documentazione sintassi: http://www.openspf.org/SPF_Record_Syntax

DomainKeys Identified Mail (DKIM)

- DKIM permette firmare digitalmente un messaggio
- Nota: la firma è apposta dal server SMTP
- È necessario creare una chiave per la firma digitale

Setup della chiave DKIM

- Creiamo la chiave ed esportiamola

```
cd /etc/exim

# Creazione della chiave
openssl genrsa -out dkim.key 1024 -outform PEM

# Esportiamo la parte pubblica
openssl rsa -in dkim.key -out dkim.pub \
          -pubout -outform PEM
```

- Creiamo un record TXT per dkim._domainkey.poul.org:

```
printf 'v=DKIM1\; k=rsa\; p=' && grep -v 'PUBLIC KEY'
    dkim.pub | awk '{print}' ORS=''; echo
```

Abilitare la firma con DKIM

```
remote_smtp:
  driver = smtp

  interface = 91.121.220.9
  dkim_domain = poul.org
  dkim_selector = dkim
  dkim_private_key = /etc/exim/dkim.key
  dkim_canon = relaxed
```

Il reverse DNS

- Ogni IP ha un nome canonico associato
- Noto anche come reverse DNS (o rDNS)
- Il rDNS del server SMTP deve corrispondere al suo nome
- Può essere verificato con il comando `host`

```
$ host 91.121.220.9
9.220.121.91.in-addr.arpa domain name pointer poul.org
    .
```

Funzionerà?

Verifica della funzionalità

Due servizi chiave:

- Domain Health Check di dnsqueries.com
- Scrivere una mail a check-auth@verifier.port25.com

Tenere lontano lo spam

- Due misure per tenere lontano lo spam:
  - Controllare le black list
  - Verificare i record SPF
- Faremo greylisting, ovvero aggiungeremo solo un avviso

Tenere lontano lo spam

```
acl_check_rcpt:
  # ...
  warn dnslists = zen.spamhaus.org : \
                  psbl.surriel.com : \
                  b.barracudacentral.org
       add_header = X-Warning: $sender_host_address is
          in a black list at $dnslist_domain

  warn spf = fail
       add_header = X-Warning: $sender_host_address is
          not allowed to send mail from
          $sender_address_domain
```

Indice

Alias

- Exim supporta gli alias per un account
- Possono essere creati da /etc/mail/aliases
- Basta inserire una coppia “alias: account”:

```
otacon22: daniele
fabrizio: ff
```

Alias esterni e multipli

- È anche possibile reindirizzare verso un account esterno
- O reindirizzare verso multipli account

```
otacon22: otacon22@gmail.com
info: andreagus@gmail.com,izzo@bobby.com,ff
```

Alias tramite suffissi

- È anche possibile avere alias automatici
- Ad esempio far puntare tutti gli indirizzi

  bino+qualcosa@poul.org

  a

  bino@poul.org

- Non è obbligatorio usare il + come separatore

Alias tramite suffissi

```
localuser:
  driver = accept
  local_parts = lsearch;/etc/mail/passwd
  #check_local_user

  # Abilita gli alias automatici tramite suffisso
  local_part_suffix = +* : -*
  local_part_suffix_optional
  transport = local_delivery
  cannot_route_message = Unknown user
```

Note finali

1. Non usare autenticazione PLAIN senza TLS

[9] http://dmarc.org/

Note finali

1. Non usare autenticazione PLAIN senza TLS
2. Salvare password in MD5 senza sale non è ideale

[9] http://dmarc.org/

Note finali

1. Non usare autenticazione PLAIN senza TLS
2. Salvare password in MD5 senza sale non è ideale

Utilizzare password complesse!

[9] http://dmarc.org/

Note finali

1. Non usare autenticazione PLAIN senza TLS
2. Salvare password in MD5 senza sale non è ideale

   Utilizzare password complesse!
3. DMARC[9]: coordina DKIM e SPF

[9] http://dmarc.org/

Licenza