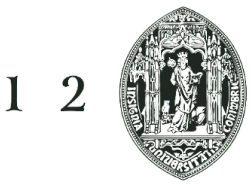

UNIVERSIDADE D
COIMBRA

Trabalho 2

Configuração de Serviço de Email com autenticação LDAP

Duarte Manuel Bento Dias 2018293526
André Pinto Dias 2020209083

Índice

Introdução e objetivo

Este trabalho foi realizado no âmbito da cadeira GISI com intuito de configurar um serviço de correio eletrónico.
Foi usada como base a topologia de rede montada no primeiro trabalho prático. Assim sendo, o serviço de email encontra-se na DMZ de Coimbra. O serviço LDAP foi adicionado ao servidor que contém os serviços de DNS e DHCP (Router) . Adicionalmente foi configurado o serviço de email (Postfix) num cliente secundário na rede do cliente1, para testar o envio de emails, usando o protocolo SMTP.

Ferramentas e Software

Neste trabalho foram utilizadas as seguintes packages:

- Postfix - MTA
- Dovecot-imapd dovecot-pop3d dovecot-lmtpd dovecot-ldap MDA (e respetivas extensões)
- slapd ldap-utils - LDAP para servidores
- spamassassin e spamc
- mutt - MUA

Arquitetura de Rede

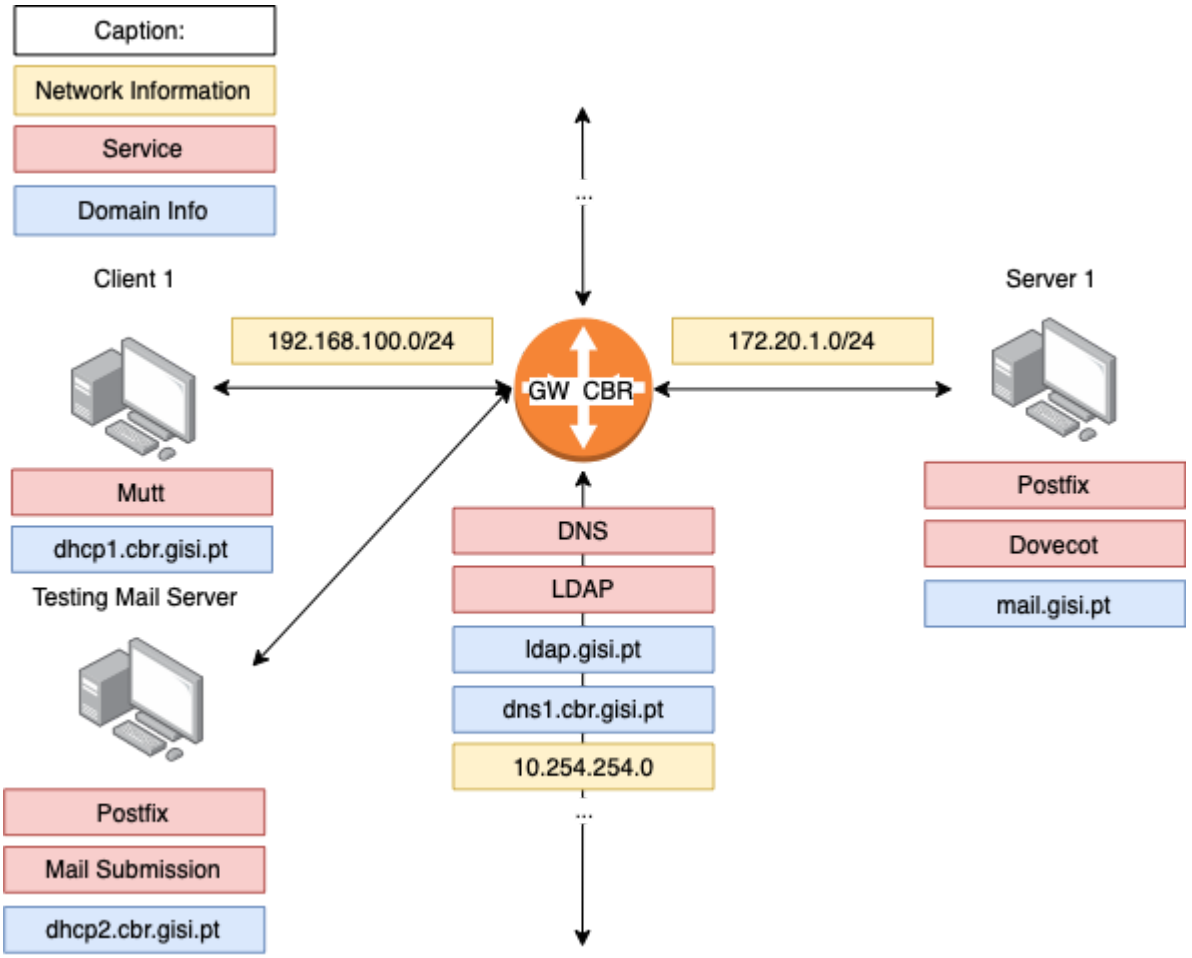

Fig.1 Arquitetura de Rede

DNS

Na configuração de DNS, apenas foram necessárias pequenas mudanças, dado que, este ficheiro já tinha sido criado no primeiro trabalho. Desta forma, foram alterados os seguintes ficheiros:

```
# File /etc/bind/gisi.db in machine - GW CGR (ONLY PART OF THE FILE)
            IN   MX   10 mail
mail        IN   A     172.20.1.5
ldap        IN  CNAME dns1
pop         IN   CNAME mail
imap        IN   CNAME mail
```

```
# File /etc/bind/cbr1_rev.db in machine - GW CGR (ONLY PART OF THE FILE)
5            IN  PTR    mail.gisi.pt.
```

LDAP

O serviço LDAP (Lightweight Directory Access Protocol) é um protocolo que permite ter autenticação centralizada para diversos serviços. Como mencionado acima, este serviço encontra-se no gateway de Coimbra. Como pedido, esta base de dados é composta por dois grupos e quatro utilizadores distintos.

Os comandos abaixo permitem a criação de utilizadores, grupos e OUs a partir de ficheiros:

```
ldapmodify -a -x -D "cn=admin,dc=gisi,dc=pt" -W -H ldapi:// -f ous.ldif
ldapmodify -a -x -D "cn=admin,dc=gisi,dc=pt" -W -H ldapi:// -f
users.ldif
ldapmodify -a -x -D "cn=admin,dc=gisi,dc=pt" -W -H ldapi:// -f
groups.ldif
```

Os ficheiros acima mencionados contêm:

```
# File Ous.ldif (NOT Complete file)
dn: ou=people, dc=gisi, dc=pt
ou: people
objectClass: organizationalUnit
```

```
# File groups.ldif (NOT Complete file)
dn: cn=managers,ou=group,dc=gisi,dc=pt
objectClass: top
objectClass: posixGroup
gidNumber: 1010
```

```
# File groups.ldif (NOT Complete file)
dn: uid=dante,ou=people,dc=gisi,dc=pt
objectClass: top
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
cn: dante
uidNumber: 101010
gidNumber: 1010
homeDirectory: /home/dante
loginShell: /bin/bash
```

```
userPassword: {SSHA}/zVHrFptcBxI5Ts6CPJc0wTNCmV7gcJm
```

Nota: Para gerar as passwords de utilizador foi utilizado o comando slappasswd.

Para efetuar a validação do serviço LDAP, o comando ldapsearch pode ser usado, para verificar o correto funcionamento da base de dados.

```
Router-CBR:/etc/ldap# ldapsearch -D "cn=admin,dc=gisi,dc=pt" -W -b "dc=gisi,dc=pt" "(cn=deve*)"
Enter LDAP Password:
# extended LDIF
#
# LDAPv3
# base <dc=gisi,dc=pt> with scope subtree
# filter: (cn=deve*)
# requesting: ALL
#

# developers, group, gisi.pt
dn: cn=developers,ou=group,dc=gisi,dc=pt
objectClass: top
objectClass: posixGroup
gidNumber: 10006
cn: developers

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

Fig.2 Resposta do LDAP

Email

O serviço de email foi configurado recorrendo ao serviço Postfix, para envio e receção de email, e ao Dovecot para armazenamento dos emails nas mailboxes dos diferentes utilizadores.

A arquitetura do serviço de email é demonstrada abaixo.

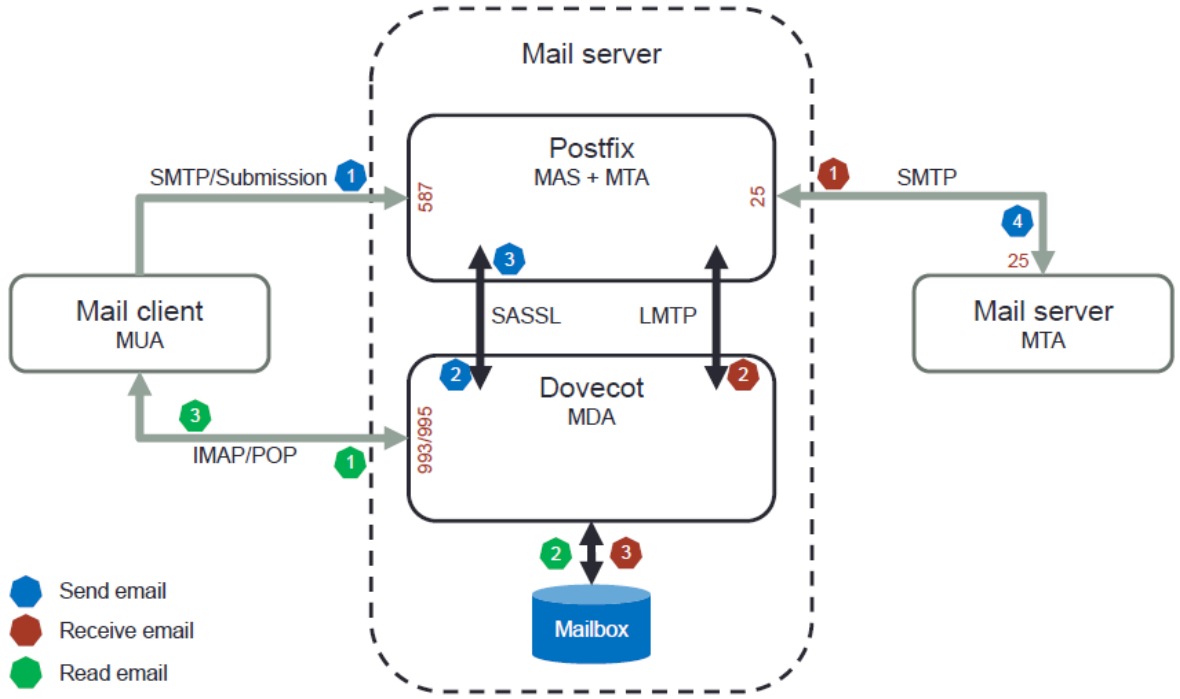

Fig 3 Arquitetura de email

Postfix

Como pode ser visto acima, o Postfix trata da recepção dos emails e de todo o fluxo de transporte. Por outro lado, os serviços de autenticação e gestão das caixas de email ficam a cargo do Dovecot.

As configurações utilizadas foram as seguintes:

```
#In file etc/postfix/main.cf  (Not total file shown)
#LMTP
mailbox_transport = lmtp:unix:private/dovecot-lmtp #Handle local
transport

# SASL
smtpd_sasl_type = dovecot  #SASL Type
smtpd_sasl_path = private/auth
smtpd_sasl_auth_enable = yes
broken_sasl_auth_clients = yes
```

```
home_mailbox = mailbox/  #Not used since dovecot handles maildirs


#LDAP Integration
virtual_transport = dovecot
virtual_mailbox_domains = hash:/etc/postfix/virtual_domains
virtual_mailbox_maps =
proxy:ldap:/etc/postfix/ldap_virtual_recipients.cf
virtual_alias_maps = proxy:ldap:/etc/postfix/ldap_virtual_aliases.cf
#
#SMTP connection restrictions
#Restrictions related to MUA clients
smtpd_restriction_classes = mua_sender_restrictions,
mua_client_restrictions, mua_helo_restrictions smtpd_helo_restrictions
    permit_mynetworks,
    permit_sasl_authenticated,
    permit
mua_client_restrictions = permit_sasl_authenticated, reject
mua_sender_restrictions = permit_sasl_authenticated, reject
mua_helo_restrictions = permit_mynetworks, permit
```

Para ativar os serviços do Postfix mudaram-se também as configurações no ficheiro master.cf

```
submission inet n       -       y       -       -       smtpd
```

Dovecot

No que diz respeito ao Dovecot, foram feitas alterações em quatro ficheiros, sendo estes o 10-auth (que faz a ligação com o LDAP), 10-mail (que configura as mailboxes), 10-logging (não obrigatório, mas importante para efeitos de debugging) e 10-master (ficheiro principal de configuração de email)

```
#In file etc/dovecot/conf.d/10-auth.conf  (Not total file shown)
auth_mechanisms = plain login
auth_username_format = %Ln
!include auth-ldap.conf.ext ## For LDAP Authentication
#include auth-system.conf.ext ## For Regular local authentication
```

```
#In file etc/dovecot/conf.d/10-logging.conf  (Not total file shown)
log_path = syslog
syslog_facility = mail
auth_debug = yes
```

```
#In file etc/dovecot/conf.d/10-mail.conf  (Not total file shown)
mail_location = maildir:/home/mail/%u/MailDir
```

```
#In file etc/dovecot/conf.d/10-master.conf  (Not total file shown)
service imap-login {
 inet_listener imap {
   port = 143
 }
 inet_listener imaps {
   port = 993
   ssl = yes
 }
service pop3-login {
 inet_listener pop3 {
   port = 110
 }
 inet_listener pop3s {
   port = 995
   ssl = yes
 }
}
service lmtp {
  unix_listener lmtp {
    #mode = 0666
  }
  unix_listener /var/spool/postfix/private/dovecot-lmtp {
        group = postfix
        mode = 0666
        user = postfix
    }
}
service auth {
 unix_listener auth-userdb {
   #mode = 0666
   #user =
   #group =
 }

#Postfix smtp-auth
unix_listener /var/spool/postfix/private/auth {
   mode = 0666
   user = postfix
   group = postfix
 }
}
```

Foi ainda necessário criar os seguintes ficheiros:

```
#In file etc/dovecot/dovecot-ldap.conf.ext  (Not total file shown)
hosts = ldap.gisi.pt
dn = cn=admin,dc=gisi,dc=pt
# Password for LDAP server, if dn is specified.
dnpass = admin
tls = no
auth_bind = yes
# LDAP protocol version to use. Likely 2 or 3.
ldap_version = 3
# LDAP base. %variables can be used here.
base = ou=people,dc=gisi,dc=pt
# Search scope: base, onelevel, subtree
scope = subtree
user_attrs = homeDirectory=home,uidNumber=uid,gidNumber=gid
user_filter = (&(objectClass=posixAccount)(|(uid=%n)(maildrop=%u)))
```

```
#In file /etc/postfix/ldap_virtual_recipients.cf
bind = yes
bind_dn = cn=admin,dc=gisi,dc=pt
bind_pw = admin
server_host = 172.20.1.1
server_port= 389
search_base = ou=people,dc=gisi,dc=pt
scope = sub
domain = mail.gisi.pt
```

```
Apr  6 10:47:39 Server1 dovecot: auth: Debug: auth client connected (pid=49445)
Apr  6 10:47:40 Server1 dovecot: auth: Debug: client in: AUTH#0111#011LOGIN#011service=imap#011secured=tls#011session=VniZQPnb2q
p=192.168.100.11#011lport=993#011rport=42714#011local_name=mail.gisi.pt
Apr  6 10:47:40 Server1 dovecot: auth: Debug: client passdb out: CONT#0111#011VXNlcm5hbWU6
Apr  6 10:47:40 Server1 dovecot: auth: Debug: client in: CONT<hidden>
Apr  6 10:47:40 Server1 dovecot: auth: Debug: client passdb out: CONT#0111#011UGFzc3dvcmQ6
Apr  6 10:47:40 Server1 dovecot: auth: Debug: client in: CONT<hidden>
Apr  6 10:47:40 Server1 dovecot: auth: Debug: ldap(lancelot,192.168.100.11,<VniZQPnb2qbAqGQL>): Performing passdb lookup
Apr  6 10:47:40 Server1 dovecot: auth: Debug: ldap(lancelot,192.168.100.11,<VniZQPnb2qbAqGQL>): Finished passdb lookup
Apr  6 10:47:40 Server1 dovecot: auth: Debug: auth(lancelot,192.168.100.11,<VniZQPnb2qbAqGQL>): Auth request finished
Apr  6 10:47:40 Server1 dovecot: auth: Debug: client passdb out: OK#0111#011user=lancelot
Apr  6 10:47:40 Server1 dovecot: auth: Debug: master in: REQUEST#0114194566145#01149445#0111#011d662bab5afd196907a137705aa705943
st_auth_token
Apr  6 10:47:40 Server1 dovecot: auth: Debug: ldap(lancelot,192.168.100.11,<VniZQPnb2qbAqGQL>): Performing userdb lookup
Apr  6 10:47:40 Server1 dovecot: auth: Debug: ldap(lancelot,192.168.100.11,<VniZQPnb2qbAqGQL>): user search: base=ou=people,dc=g
=(&(objectClass=posixAccount)(|(uid=lancelot)(maildrop=lancelot))) fields=homeDirectory,uidNumber,gidNumber
Apr  6 10:47:40 Server1 dovecot: auth: Debug: ldap(lancelot,192.168.100.11,<VniZQPnb2qbAqGQL>): result: uidNumber=101014 gidNumb
ncelot; homeDirectory,uidNumber,gidNumber unused
Apr  6 10:47:40 Server1 dovecot: auth: Debug: ldap(lancelot,192.168.100.11,<VniZQPnb2qbAqGQL>): Finished userdb lookup
Apr  6 10:47:40 Server1 dovecot: auth: Debug: master userdb out: USER#0114194566145#011lancelot#011home=/home/lancelot#011uid=10
LOGIN#011auth_token=91a5126d3496b5d5c3c72ce8904b94cdbec1ef19
Apr  6 10:47:40 Server1 dovecot: imap-login: Login: user=<lancelot>, method=LOGIN, rip=192.168.100.11, lip=172.20.1.5, mpid=4944
GQL>
```

Fig 4 Login e autenticação com LDAP

SpamAssassin

Finalmente, foi também efetuada a configuração do spamassassin. Esta ferramenta permite a filtragem dos emails que são considerados spam.
Feita a instalação, como mencionado em software e packages, é necessário proceder a configuração do spamassassin.
O ficheiro /etc/default/spamassassin contém as configurações do spamassassin por default. Assim sendo, foram feitas as seguintes modificações.

```
# In file /etc/default/spamassassin
SAHOME="/var/log/spamassassin/"

OPTIONS="--create-prefs --max-children 5 --username spamd
--helper-home-dir /home/spamd/ -s /home/spamd/spamd.log"

# Pid file
PIDFILE="/var/run/spamd.pid"

# Set nice level of spamd
#NICE="--nicelevel 15"

# Cronjob

CRON=1
```

Em vez do antigo “ENABLE=1” utilizou-se a tool update-rc.d.

```
update-rc.d spamassassin enable
```

Foi ainda necessário efetuar as seguintes mudanças no postfix:

- Adicionar o serviço ao master.cf
- Adicionar o serviço como mail filter (i.e. milter no main.cf)

```
#In file /etc/postfix/master.cf
smtp      inet  n       -       y       -       -       smtpd
        -o content_filter=spamassassin

spamassassin unix -     n       n       -       -       pipe
        user=spamd argv=/usr/bin/spamc -f -e
        /usr/sbin/sendmail -oi -f ${sender} ${recipient}
```

```
#In file /etc/postfix/main.cf
smtpd_milters = unix:/spamass/spamass.sock
milter_connect_macros = j {daemon_name} v {if_name} _
milter_default_action = tempfail
```

É ainda necessário configurar o SpamAssassin para reescrever os headers, bem como para

```
# In file /etc/spamassassin/local.cf
required_score 5.0 #Legitimate message = lower score
rewrite_header Subject [***** SPAM _SCORE_ *****]
```

Do lado do servidor, vê-se a seguinte comunicação (já com o spamassassin).

```
Apr  5 23:28:31 Server1 postfix/smtps/smtpd[48954]: A2F5523D06: client=dhcp2.cbr.gisi.pt[192.168.100.11], sasl
_method=LOGIN, sasl_username=lancelot
Apr  5 23:28:31 Server1 postfix/cleanup[48959]: A2F5523D06: message-id=<YkzCjhWPWY/EgFP0@client1>
Apr  5 23:28:31 Server1 spamd[26665]: spamd: connection from ::1 [::1]:50524 to port 783, fd 5
Apr  5 23:28:31 Server1 spamd[26665]: spamd: processing message <YkzCjhWPWY/EgFP0@client1> for lancelot:1002
Apr  5 23:28:32 Server1 spamd[26665]: spamd: clean message (-1.0/5.0) for lancelot:1002 in 0.9 seconds, 597 by
tes.
Apr  5 23:28:32 Server1 spamd[26665]: spamd: result: . -1 - ALL_TRUSTED scantime=0.9,size=597,user=lancelot,ui
d=1002,required_score=5.0,rhost=::1,raddr=::1,rport=50524,mid=<YkzCjhWPWY/EgFP0@client1>,autolearn=ham autolea
rn_force=no
Apr  5 23:28:32 Server1 postfix/qmgr[48727]: A2F5523D06: from=<lancelot@mail.gisi.pt>, size=517, nrcpt=1 (queu
e active)
Apr  5 23:28:32 Server1 postfix/smtps/smtpd[48954]: disconnect from dhcp2.cbr.gisi.pt[192.168.100.11] ehlo=1 a
uth=1 mail=1 rcpt=1 data=1 quit=1 commands=6
```

Fig.5 Processamento do servidor (Postfix, Dovecot e spamassasin)

```
Return-Path: <lancelot@mail.gisi.pt>
Delivered-To: lancelot@mail.gisi.pt
Received: from MailServer.cbr.gisi.pt
        by Server1 with LMTP
        id lDVUEPppTGLdmQAAm+WwGQ
        (envelope-from <lancelot@mail.gisi.pt>)
        for <lancelot@mail.gisi.pt>; Tue, 05 Apr 2022 17:10:34 +0100
Received: from client1 (dhcp2.cbr.gisi.pt [192.168.100.11])
        by MailServer.cbr.gisi.pt (Postfix) with ESMTPSA id D207923940
        for <lancelot@mail.gisi.pt>; Tue,  5 Apr 2022 17:10:25 +0100 (WEST)
Date: Tue, 5 Apr 2022 17:10:24 +0100
From: Brave Lancelot <lancelot@mail.gisi.pt>
To: lancelot@mail.gisi.pt
Subject: [***** SPAM 999.0 *****] with the thing
Message-ID: <Ykxp8NmnAssgYIwb@client1>
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="----------=_624C69FA.B0E3BC51"
Content-Disposition: inline
X-Spam-Flag: YES
X-Spam-Status: Yes, score=999.0 required=5.0 tests=ALL_TRUSTED,GTUBE
        autolearn=no autolearn_force=no version=3.4.6
X-Spam-Level: **************************************************
X-Spam-Checker-Version: SpamAssassin 3.4.6 (2021-04-09) on Server1

[-- Attachment #1 --]
[-- Type: text/plain, Encoding: 8bit, Size: 0.7K --]
Content-Type: text/plain; charset=iso-8859-1
Content-Disposition: inline
Content-Transfer-Encoding: 8bit

Spam detection software, running on the system "Server1",
has identified this incoming email as possible spam.  The original
message has been attached to this so you can view it or label
similar future email.  If you have any questions, see
@@CONTACT_ADDRESS@@ for details.

Content preview:  XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X
```

Fig.6 Comportamento do SpamAssassin aquando a detecção de um email com spam

Testing

Mail User Agent

Como cliente de email foi utilizado o Mutt. Este serviço é bastante simples e necessita de pouca configuração. No ficheiro .muttrc foram efetuadas as seguintes configurações.

```
#In file .muttrc
set imap_user = "lancelot"
set imap_pass = "admin"
set smtp_url = "smtps://$imap_user@mail.gisi.pt:465/"
set smtp_pass = $imap_pass
set folder = "imaps://mail.gisi.pt:993/"
set spoolfile = "+INBOX"
set from = "Brave Lancelot <lancelot@mail.gisi.pt>"
set move = no
mailboxes "+INBOX"
set record = +Sent
```

O envio de um email através de smtp resulta num email com o seguinte header.

```
Return-Path: <tldart@Server1>
Delivered-To: lancelot@mail.gisi.pt
Received: from MailServer.cbr.gisi.pt
        by Server1 with LMTP
        id FQFiHlw/S2LWbAAAm+WwGQ
        (envelope-from <tldart@Server1>)
        for <lancelot@mail.gisi.pt>; Mon, 04 Apr 2022 19:56:28 +0100
Received: by MailServer.cbr.gisi.pt (Postfix, from userid 1000)
        id 7746E23CF0; Mon,  4 Apr 2022 19:56:28 +0100 (WEST)
Subject: Testing
To: lancelot@mail.gisi.pt
X-Mailer: mail (GNU Mailutils 3.10)
Message-Id: <20220404185628.7746E23CF0@MailServer.cbr.gisi.pt>
Date: Mon,  4 Apr 2022 19:56:28 +0100 (WEST)
From: tldart <tldart@Server1>

PEPEW
```

Fig.7 Envio de email SMTP

Testing Mail Server

Para realizar testes de comunicação SMTP entre servidores, instanciou-se uma outra máquina, neste caso localizada na mesma rede do cliente 1. Nesta máquina utilizou-se um servidor de postfix minimamente configurado.

```
# In /etc/postfix/main.cf (Not full file)
smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated
defer_unauth_destination
myhostname = debian.cbr.gisi.pt
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination = debian.cbr.gisi.pt, test.example.com, debian,
localhost.localdomain, localhost
relayhost = mail.gisi.pt
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
inet_protocols = all
```

Denote-se a utilização do parâmetro “relayhost” de forma a efetuar o transporte do postfix. O envio de email faz-se através do método submission.

```
echo "Testing Relay" | mail -s "test relay" lancelot@mail.gisi.pt
```

Do lado do cliente o header to email contém informação sobre ambos os servidores.

```
Return-Path: <root@debian>
Delivered-To: lancelot@mail.gisi.pt
Received: from MailServer.cbr.gisi.pt
        by Server1 with LMTP
        id JN8MEUq4TGInvwAAm+WwGQ
        (envelope-from <root@debian>)
        for <lancelot@mail.gisi.pt>; Tue, 05 Apr 2022 22:44:42 +0100
Received: by MailServer.cbr.gisi.pt (Postfix, from userid 1002)
        id 433F023D06; Tue,  5 Apr 2022 22:44:42 +0100 (WEST)
X-Spam-Checker-Version: SpamAssassin 3.4.6 (2021-04-09) on Server1
X-Spam-Level:
X-Spam-Status: No, score=-1.0 required=5.0 tests=ALL_TRUSTED
        autolearn=unavailable autolearn_force=no version=3.4.6
Received: from debian.cbr.gisi.pt (unknown [192.168.100.13])
        by MailServer.cbr.gisi.pt (Postfix) with ESMTPS id 2ACD42393F
        for <lancelot@mail.gisi.pt>; Tue,  5 Apr 2022 22:44:42 +0100 (WEST)
Received: by debian.cbr.gisi.pt (Postfix, from userid 0)
        id 1E571237CC; Tue,  5 Apr 2022 22:44:42 +0100 (WEST)
Subject: test relay
To: lancelot@mail.gisi.pt
X-Mailer: mail (GNU Mailutils 3.10)
Message-Id: <20220405214442.1E571237CC@debian.cbr.gisi.pt>
Date: Tue,  5 Apr 2022 22:44:42 +0100 (WEST)
From: root <root@debian>

Testing Relay
```

Fig.8 Relay de servidores SMTP

References

- 2-LDAP-managed-mail-server-with-Postfix-and-Dovecot-for-multiple-domains
- install-spamassassin-with-postfix-dovecot
- how-to-get-spamassassin-working-with-postfix-as-a-milter
- how-to-install-spamassassin-with-postfix-on-ubuntu