Postfix

Postfix è il Mail Transfer Agent (MTA) predefinito di Ubuntu. Cerca di essere facile da amministrare e sicuro ed è compatibile con l'MTA **sendmail**. Questa sezione espone come installare e configurare **postfix** e anche come configurare un server SMTP utilizzando un collegamento sicuro (per l'invio di email in sicurezza).

Installazione

Per installare **postfix** con SMTP AUTH e TLS (Transport Layer Security) eseguire il seguente comando:

```
sudo apt-get install postfix
```

Premere Invio a ogni domanda posta durante il processo di installazione, la configurazione viene svolta al passo successivo.

Configurazione di base

Per configurare **postfix** eseguire il seguente comando:

```
sudo dpkg-reconfigure postfix
```

Sarà visualizzata l'interfaccia grafica. A ogni schermata selezionare i seguenti valori:

- Ok
- Internet Site
- NONE
- mail.example.com
- mail.example.com, localhost.localdomain, localhost
- No
- 127.0.0.0/8
- Sì
- 0
- +
- tutti

Sostituire mail.example.com con il nome del proprio host server.

Autenticazione SMTP

I passi successivi sono la configurazione di **postfix** per l'uso di SASL per SMTP AUTH. Invece di modificare i file di configurazione manulamente, è possibile utilizzare lo strumento **postconf** per impostare tutti i parametri di **postfix**. I parametri di configurazione vengono salvati nel file `/etc/postfix/main.cf`. Per riconfigurare un particolare parametro è possibile utilizzare nuovamente il comando precedente o modificare il file a mano.

1. Configurare Postfix per eseguire SMTP AUTH usando SASL (saslauthd):

```
postconf -e 'smtpd_sasl_local_domain ='
postconf -e 'smtpd_sasl_auth_enable = yes'
postconf -e 'smtpd_sasl_security_options = noanonymous'
postconf -e 'broken_sasl_auth_clients = yes'
postconf -e 'smtpd_recipient_restrictions =
permit_sasl_authenticated,permit_mynetworks,reject_unauth_destination'
postconf -e 'inet_interfaces = all'
```

Aprire il file `/etc/postfix/sasl/smtpd.conf` e aggiungere le seguenti righe alla fine del file:

```
pwcheck_method: saslauthd
mech_list: plain login
```

2. In seguito, configurare il certificato digitale per TLS. Quando vengono fatte delle domande, seguire le istruzioni e rispondere di conseguenza.

```
openssl genrsa -des3 -rand /etc/hosts -out smtpd.key 1024
chmod 600 smtpd.key
openssl req -new -key smtpd.key -out smtpd.csr
openssl x509 -req -days 365 -in smtpd.csr -signkey smtpd.key -out
smtpd.crt
openssl rsa -in smtpd.key -out smtpd.key.unencrypted
mv -f smtpd.key.unencrypted smtpd.key
openssl req -new -x509 -extensions v3_ca -keyout cakey.pem -out cacert.pem
-days 3650
sudo mv smtpd.key /etc/ssl/private/
sudo mv smtpd.crt /etc/ssl/certs/
sudo mv cakey.pem /etc/ssl/private/
sudo mv cacert.pem /etc/ssl/certs/
```

Si può ottenere il certificato digitale da un'autorità di certificazione. In alternativa, è possibile creare il proprio certificato autonomamente. Per maggiori informazioni, consultare Creare un certificato auto-firmato.

3. Configurare Postfix affinché esegua la cifratura TLS sia per le email in arrivo sia per quelle in uscita:

```
postconf -e 'smtpd_tls_auth_only = no'
postconf -e 'smtp_use_tls = yes'
postconf -e 'smtpd_use_tls = yes'
postconf -e 'smtp_tls_note_starttls_offer = yes'
postconf -e 'smtpd_tls_key_file = /etc/ssl/private/smtpd.key'
postconf -e 'smtpd_tls_cert_file = /etc/ssl/certs/smtpd.crt'
postconf -e 'smtpd_tls_CAfile = /etc/ssl/certs/cacert.pem'
postconf -e 'smtpd_tls_loglevel = 1'
postconf -e 'smtpd_tls_received_header = yes'
postconf -e 'smtpd_tls_session_cache_timeout = 3600s'
postconf -e 'tls_random_source = dev:/dev/urandom'
postconf -e 'myhostname = mail.example.com'
```

Una volta eseguiti tutti i comandi, SMTP AUTH è configurato per **postfix**. Il certificato auto-firmato è creato per TLS ed è configurato per l'uso con **postfix**.

Ora, il file `/etc/postfix/main.cf` dovrebbe essere simile a questo.

La configurazione iniziale di postfix è completata. Eseguire il seguente comando per avviare il demone postfix:

```
sudo /etc/init.d/postfix start
```

Ora il demone **postfix** è installato, configurato e funziona correttamente. **Postfix** supporta anche SMTP AUTH come descritto in RFC2554. È basato su SASL, ma è necessario abilitare l'autenticazione SASL prima di poter utilizzare SMTP.

Configurare SASL

libsasl2, **sasl2-bin** e **libsasl2-modules** sono necessari per abilitare SMTP AUTH usando SASL. È possibile installare queste applicazioni se non sono già state installate:

```
sudo apt-get install libsasl2 sasl2-bin
```

È necessario apportare alcune modifiche prima di un corretto funzionamento. Questo perché **Postfix** viene eseguito in chroot su `/var/spool/postfix`, **SASL** necessita di essere configurato per poter girare nella falsa root (`/var/run/saslauthd` diventa `/var/spool/postfix/var/run/saslauthd`):

```
mkdir -p /var/spool/postfix/var/run/saslauthd
rm -rf /var/run/saslauthd
```

Per attivare **saslauthd**, modificare il file `/etc/default/saslauthd` e cambiare o aggiungere la variabile START. Per configurare **saslauthd** affinché possa girare nella falsa root, aggiungere le variabili PWDIR, PIDFILE e PARAMS. Infine configurare la variabile MECHANISMS a piacere. Il file dovrebbe essere all'incirca come questo:

```
# This needs to be uncommented before saslauthd will be run
# automatically
START=yes

PWDIR="/var/spool/postfix/var/run/saslauthd"
PARAMS="-m ${PWDIR}"
PIDFILE="${PWDIR}/saslauthd.pid"

# You must specify the authentication mechanisms you wish to use.
# This defaults to "pam" for PAM support, but may also include
# "shadow" or "sasldb", like this:
# MECHANISMS="pam shadow"

MECHANISMS="pam"
```

> È possibile utilizzare **shadow** al posto di **pam**. Questo utilizzerà il trasferimento delle password con l'hashing MD5 ed è perfettamente sicuro. Il nome utente e la password necessari per l'autenticazione sono quelle dell'utente nel sistema in uso.

Aggiornare lo «stato» di `/var/spool/portfix/var/run/saslauthd`. Lo script init di saslauthd utilizza queste impostazioni per creare la directory mancante con i permessi appropriati:

```
dpkg-statoverride --force --update --add root sasl
755 /var/spool/postfix/var/run/saslauthd
```

Test

La configurazione di SMTP AUTH è completata. Ora è necessario avviare il tutto ed eseguire dei test. Per avviare il demone SASL utilizzare il seguente comando:

```
sudo /etc/init.d/saslauthd start
```

Per controllare se SMTP AUTH e TLS funzionano perfettamente, eseguire il seguente comando:

```
telnet mail.example.com 25
```

Una volta stabilito il collegamento con il server postfix, digitare:

```
ehlo mail.example.com
```

Se compaiono le seguenti righe, allora tutto è a posto. Digitare **quit** per uscire.

```
250-STARTTLS
250-AUTH LOGIN PLAIN
250-AUTH=LOGIN PLAIN
250 8BITMIME
```