



Patrick Ni
RedAnt IT Support Inc.
December, 2009

Debian Postfix SMTP AUTH configuration using Cyrus SASL and TLS

Status of this memo

Postfix Server

- * Operating system: Debian Lenny
- * Postfix: 2.5.5-1.1
- * SASL: 2.1.22

Postfix Client

- * Operating system: Debian Etch
- * Postfix: 2.3.8-2
- * SASL: 2.1.22

Thunderbird Client

- * Operating system: Windows XP Professional Version 2002 SP3
- * Thunderbird: 2.0.0.23 (20090812)

Packages needed

- * postfix
- * sasl2-bin
- * libsasl2
- * libsasl2-modules

Abstract

This document is to share my experiences and hopefully it helps make SMTP AUTH work at your site

1. Prerequisite

- *PAM on your Debian is working

*Postfix is working with basic configuration as a NULL client, except `inet_interfaces = all`, this is important, because

- o "trusted" SMTP clients are allowed to relay mail through Postfix
- o As a NULL client, only localhost can relay mail through Postfix
- o To prove SMTP AUTH work, we will test from another SMTP client on the same LAN
 - +We will add `permit_sasl_authenticated` to `smtpd_recipient_restrictions`, i.e.,
 - +`smtpd_recipient_restrictions = permit_sasl_authenticated, permit_mynetworks, reject_unauth_destination`
- o That is why Postfix has to listen on the LAN network interface as well

2. Check whether Postfix is running chrooted or not

- * Read the `/etc/init.d/postfix` file
- * If the fifth column is either "-", "y" or "Y", that means Postfix is to run chrooted
- * In our case, Postfix is running chrooted.

3. SASL authentication on the Postfix SMTP server

3.1 `/etc/postfix/main.cf`

- *`smtpd_sasl_auth_enable = yes`
- *`smtpd_recipient_restrictions = permit_sasl_authenticated, permit_mynetworks, reject_unauth_destination`
- *`broken_sasl_auth_clients = yes`
- *`smtpd_sasl_authenticated_header = yes`
 - o Once SMTP Auth working, you can get the following header from the recipient's e-mail header
 - o Received: from [192.168.0.100] (unknown [192.168.0.100]) (Authenticated sender:pni) by river.redant.ca (Postfix) with ESMTPA id 02FBB76772 for a11024@yahoo.com; Sat, 19 Dec 2009 22:40:01 -0800 (PST)
- *`smtpd_sasl_path = smtpd`
- *`smtpd_sasl_security_options = noanonymous`
- *`smtpd_sasl_type = cyrus`

3.2 `/etc/postfix/sasl/smtpd.conf`

- *`pwcheck_method: saslauthd`
- *`mech_list: PLAIN LOGIN`

3.3 `/etc/default/saslauthd`

- *`START=yes`
- *`MECHANISMS="pam"`
- *`OPTIONS="-c -m /var/spool/postfix/var/run/saslauthd"`

3.4 `/etc/init.d/postfix`

- *Add `etc/postfix/sasl/smtpd.conf` to the FILES line, like this
 - o `FILES="etc/localtime etc/services etc/resolv.conf etc/hosts \`

etc/nsswitch.conf etc/postfix/sasl/smtpd.conf"

3.5 Chroot related configurations

```
*mv /var/run/saslauthd /var/spool/postfix/var/run/saslauthd
*ln -s /var/spool/postfix/var/run/saslauthd /var/run/saslauthd
```

3.6 Error message: warning: SASL authentication failure: cannot connect to saslauthd server: No such file or directory

*Check chroot configuration. It means Postfix as the SASL client, can not find the communication socket mux

3.7 Error message: warning: SASL authentication failure: cannot connect to saslauthd server: Permission denied

```
*adduser postfix sasl
```

4. SASL authentication on the Postfix SMTP client

```
*smtp_sasl_auth_enable = yes
*smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd
*smtp_sasl_type = cyrus
*relayhost = [192.168.0.2]
*smtp_sasl_security_options = noanonymous
```

5. TLS configuration on the Postfix server

```
*smtpd_tls_cert_file = /etc/postfix/RAtls/river.redant.ca.crt
*smtpd_tls_key_file = /etc/postfix/RAtls/river.redant.ca.key
*smtpd_tls_CAfile = /etc/postfix/RAtls/ca.crt
*smtpd_tls_security_level = may (may work too. I changed to encrypt later.)
*smtpd_tls_security_level = encrypt
*smtpd_tls_ask_ccert = no
*smtpd_tls_req_ccert = no
*smtpd_tls_auth_only = yes
*smtpd_tls_session_cache_database = btree:/var/lib/postfix/smtpd_scache
*smtpd_tls_session_cache_timeout = 3600s
```

6. TLS configuration on the Postfix client

```
*smtp_tls_CAfile = /etc/postfix/RAtls/ca.crt
*smtp_tls_session_cache_database = btree:/var/lib/postfix/smtp_scache
*smtp_tls_session_cache_timeout = 3600s
*smtp_tls_security_level = may (may work too. I changed to encrypt later.)
*smtp_tls_security_level = encrypt
```

7. Normative References

RFC 4954, SMTP Service Extension for Authentication

8. Author's Address

Patrick Ni
RedAnt IT Support Inc.

Phone: 778 988 3178
Email: Patrick.Ni@RedAnt.ca