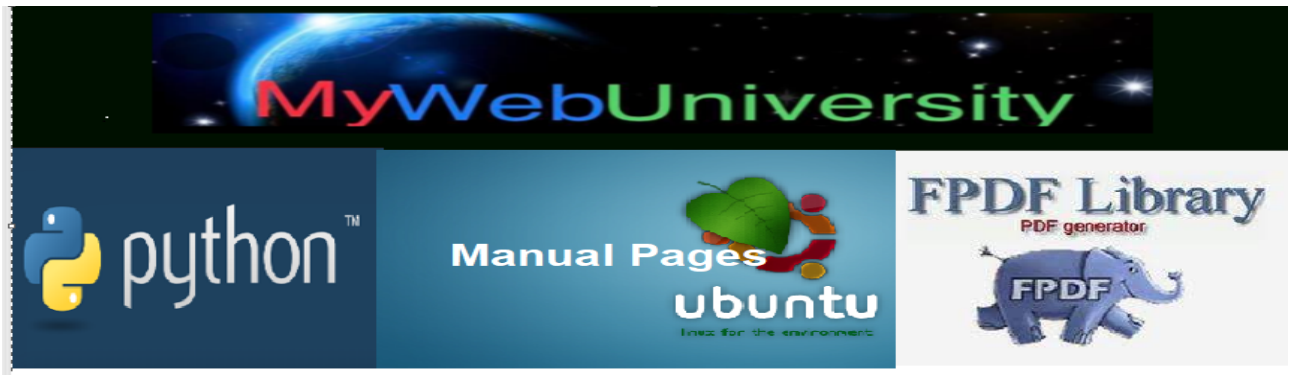

Full credit is given to the above companies including the OS that this PDF file was generated!

Linux Ubuntu 26.04 Manual Pages on command 'postfix-tls.1'

$ man postfix-tls.1

POSTFIX-TLS(1) General Commands Manual POSTFIX-TLS(1)

NAME

postfix-tls - Postfix TLS management

SYNOPSIS

postfix tls subcommand

DESCRIPTION

The "postfix tls subcommand" feature enables opportunistic TLS in the Postfix SMTP client or server, and manages Postfix SMTP server private keys and certificates.

The following subcommands are available:

enable-client [-r randsource]

Enable opportunistic TLS in the Postfix SMTP client, if all SMTP client TLS settings are at their default values. Otherwise, suggest parameter settings without making any changes.

Specify randsource to update the value of the tls_random_source configuration parame? ter (typically, /dev/urandom). Prepend dev: to device paths or egd: to EGD socket paths.

See also the all-default-client subcommand.

enable-server [-r randsource] [-a algorithm] [-b bits] [hostname...]

Create a new private key and self-signed server certificate and enable opportunistic TLS in the Postfix SMTP server, if all SMTP server TLS settings are at their default values. Otherwise, suggest parameter settings without making any changes.

The randsource parameter is as with enable-client above, and the remaining options are as with new-server-key below.

See also the all-default-server subcommand.

new-server-key [-a algorithm] [-b bits] [hostname...]

Create a new private key and self-signed server certificate, but do not deploy them.

Log and display commands to deploy the new key and corresponding certificate. Also log and display commands to output a corresponding CSR or TLSA records which may be needed to obtain a CA certificate or to update DNS before the new key can be de? ployed.

The algorithm defaults to rsa, and bits defaults to 2048. If you choose the ecdsa algorithm then bits will be an EC curve name (by default secp256r1, also known as prime256v1). Curves other than secp256r1, secp384r1 or secp521r1 are unlikely to be widely interoperable. When generating EC keys, use one of these three. DSA keys are obsolete and are not supported.

Note: ECDSA support requires OpenSSL 1.0.0 or later and may not be available on your system. Not all client systems will support ECDSA, so you'll generally want to de? ploy both RSA and ECDSA certificates to make use of ECDSA with compatible clients and RSA with the rest. If you want to deploy certificate chains with intermediate CAs for both RSA and ECDSA, you'll want at least OpenSSL 1.0.2, as earlier versions may not handle multiple chain files correctly.

The first hostname argument will be the CommonName of both the subject and issuer of the self-signed certificate. It, and any additional hostname arguments, will also be listed as DNS alternative names in the certificate. If no hostname is provided the value of the myhostname main.cf parameter will be used.

For RSA, the generated private key and certificate files are named key-yyyymmdd-hh? mmss.pem and cert-yyyymmdd-hhmmss.pem, where yyyymmdd is the calendar date and hhmmss is the time of day in UTC. For ECDSA, the file names start with eckey- and eccert- instead of key- and cert- respectively.

Before deploying the new key and certificate with DANE, update the DNS with new DANE TLSA records, then wait for secondary nameservers to update and then for stale records in remote DNS caches to expire.

Before deploying a new CA certificate make sure to include all the required interme? diate issuing CA certificates in the certificate chain file. The server certificate must be the first certificate in the chain file. Overwrite and deploy the file with the original self-signed certificate that was generated together with the key.

new-server-cert [-a algorithm] [-b bits] [hostname...]

This is just like new-server-key except that, rather than generating a new private key, any currently deployed private key is copied to the new key file. Thus if you're publishing DANE TLSA "3 1 1" or "3 1 2" records, there is no need to update DNS records. The algorithm and bits arguments are used only if no key of the same algorithm is already configured.

This command is rarely needed, because the self-signed certificates generated have a 100-year nominal expiration time. The underlying public key algorithms may well be obsoleted by quantum computers long before then.

The most plausible reason for using this command is when the system hostname changes, and you'd like the name in the certificate to match the new hostname (not required for DANE "3 1 1", but some needlessly picky non-DANE opportunistic TLS clients may log warnings or even refuse to communicate).

deploy-server-cert certfile keyfile

This subcommand deploys the certificates in certfile and private key in keyfile (which are typically generated by the commands above, which will also log and display the full command needed to deploy the generated key and certificate). After the new certificate and key are deployed any obsolete keys and certificates may be removed by hand. The keyfile and certfile filenames may be relative to the Postfix configura? tion directory.

output-server-csr [-k keyfile] [hostname...]

Write to stdout a certificate signing request (CSR) for the specified keyfile.

Instead of an absolute pathname or a pathname relative to $config_directory, keyfile may specify one of the supported key algorithm names (see "postconf -T public-key-al? gorithms"). In that case, the corresponding setting from main.cf is used to locate the keyfile. The default keyfile value is rsa.

Zero or more hostname values can be specified. The default hostname is the value of myhostname main.cf parameter.

output-server-tlsa [-h hostname] [keyfile...]

Write to stdout a DANE TLSA RRset suitable for a port 25 SMTP server on host hostname with keys from any of the specified keyfile values. The default hostname is the value of the myhostname main.cf parameter.

Instead of absolute pathnames or pathnames relative to $config_directory, the keyfile

list may specify names of supported public key algorithms (see "postconf -T pub?lic-key-algorithms"). In that case, the actual keyfile list uses the values of the corresponding Postfix server TLS key file parameters. If a parameter value is empty or equal to none, then no TLSA record is output for that algorithm.

The default keyfile list consists of the two supported algorithms rsa and ecdsa.

AUXILIARY COMMANDS

all-default-client

Exit with status 0 (success) if all SMTP client TLS settings are at their default values. Otherwise, exit with a non-zero status.

This is typically used as follows:

postfix tls all-default-client &&
    postfix tls enable-client

all-default-server

Exit with status 0 (success) if all SMTP server TLS settings are at their default values. Otherwise, exit with a non-zero status.

This is typically used as follows:

postfix tls all-default-server &&
    postfix tls enable-server

CONFIGURATION PARAMETERS

The "postfix tls subcommand" feature reads or updates the following configuration parame?ters.

command_directory (see 'postconf -d' output)

The location of all postfix administrative commands.

config_directory (see 'postconf -d' output)

The default location of the Postfix main.cf and master.cf configuration files.

openssl_path (openssl)

The location of the OpenSSL command line program openssl(1).

smtp_tls_loglevel (0)

Enable additional Postfix SMTP client logging of TLS activity.

smtp_tls_security_level (empty)

The default SMTP TLS security level for the Postfix SMTP client.

smtp_tls_session_cache_database (empty)

Name of the file containing the optional Postfix SMTP client TLS session cache.

smtpd_tls_cert_file (empty)

File with the Postfix SMTP server RSA certificate in PEM format.

smtpd_tls_eccert_file (empty)

File with the Postfix SMTP server ECDSA certificate in PEM format.

smtpd_tls_eckey_file ($smtpd_tls_eccert_file)

File with the Postfix SMTP server ECDSA private key in PEM format.

smtpd_tls_key_file ($smtpd_tls_cert_file)

File with the Postfix SMTP server RSA private key in PEM format.

smtpd_tls_loglevel (0)

Enable additional Postfix SMTP server logging of TLS activity.

smtpd_tls_received_header (no)

Request that the Postfix SMTP server produces Received: message headers that include information about the protocol and cipher used, as well as the remote SMTP client CommonName and client certificate issuer CommonName.

smtpd_tls_security_level (empty)

The SMTP TLS security level for the Postfix SMTP server; when a non-empty value is specified, this overrides the obsolete parameters smtpd_use_tls and smtpd_en? force_tls.

tls_random_source (see 'postconf -d' output)

The external entropy source for the in-memory tlsmgr(8) pseudo random number genera? tor (PRNG) pool.

SEE ALSO

master(8) Postfix master program

postfix(1) Postfix administrative interface

README FILES

Use "postconf readme_directory" or "postconf html_directory" to locate this information.

TLS_README, Postfix TLS configuration and operation

LICENSE

The Secure Mailer license must be distributed with this software.

HISTORY

The "postfix tls" command was introduced with Postfix version 3.1.

AUTHOR(S)

Viktor Dukhovni