NAME

tlsmgr − Postfix TLS session cache and PRNG manager

SYNOPSIS

tlsmgr [generic Postfix daemon options]

DESCRIPTION

The **tlsmgr**(8) manages the Postfix TLS session caches. It stores and retrieves cache entries on request by **smtpd**(8) and **smtp**(8) processes, and periodically removes entries that have expired.

The **tlsmgr**(8) also manages the PRNG (pseudo random number generator) pool. It answers queries by the **smtpd**(8) and **smtp**(8) processes to seed their internal PRNG pools.

The **tlsmgr**(8)'s PRNG pool is initially seeded from an external source (EGD, /dev/urandom, or regular file). It is updated at configurable pseudo−random intervals with data from the external source. It is updated periodically with data from TLS session cache entries and with the time of day, and is updated with the time of day whenever a process requests **tlsmgr**(8) service.

The **tlsmgr**(8) saves the PRNG state to an exchange file periodically and when the process terminates, and reads the exchange file when initializing its PRNG.

SECURITY

The **tlsmgr**(8) is not security−sensitive. The code that maintains the external and internal PRNG pools does not "trust" the data that it manipulates, and the code that maintains the TLS session cache does not touch the contents of the cached entries, except for seeding its internal PRNG pool.

The **tlsmgr**(8) can be run chrooted and with reduced privileges. At process startup it connects to the entropy source and exchange file, and creates or truncates the optional TLS session cache files.

With Postfix version 2.5 and later, the **tlsmgr**(8) no longer uses root privileges when opening cache files. These files should now be stored under the Postfix−owned **data_directory**. As a migration aid, an attempt to open a cache file under a non−Postfix directory is redirected to the Postfix−owned **data_directory**, and a warning is logged.

DIAGNOSTICS

Problems and transactions are logged to the syslog daemon.

BUGS

There is no automatic means to limit the number of entries in the TLS session caches and/or the size of the TLS cache files.

CONFIGURATION PARAMETERS

Changes to **main.cf** are not picked up automatically, because **tlsmgr**(8) is a persistent processes. Use the command "**postfix reload**" after a configuration change.

The text below provides only a parameter summary. See **postconf**(5) for more details including examples.

TLS SESSION CACHE

lmtp_tls_loglevel (0)
: The LMTP−specific version of the smtp_tls_loglevel configuration parameter.

lmtp_tls_session_cache_database (empty)
: The LMTP−specific version of the smtp_tls_session_cache_database configuration parameter.

lmtp_tls_session_cache_timeout (3600s)
: The LMTP−specific version of the smtp_tls_session_cache_timeout configuration parameter.

smtp_tls_loglevel (0)
: Enable additional Postfix SMTP client logging of TLS activity.

smtp_tls_session_cache_database (empty)
Name of the file containing the optional Postfix SMTP client TLS session cache.

smtp_tls_session_cache_timeout (3600s)
The expiration time of Postfix SMTP client TLS session cache information.

smtpd_tls_loglevel (0)
Enable additional Postfix SMTP server logging of TLS activity.

smtpd_tls_session_cache_database (empty)
Name of the file containing the optional Postfix SMTP server TLS session cache.

smtpd_tls_session_cache_timeout (3600s)
The expiration time of Postfix SMTP server TLS session cache information.

PSEUDO RANDOM NUMBER GENERATOR

tls_random_source (see 'postconf -d' output)
The external entropy source for the in-memory **tlsmgr**(8) pseudo random number generator (PRNG) pool.

tls_random_bytes (32)
The number of bytes that **tlsmgr**(8) reads from $tls_random_source when (re)seeding the in-memory pseudo random number generator (PRNG) pool.

tls_random_exchange_name (see 'postconf -d' output)
Name of the pseudo random number generator (PRNG) state file that is maintained by **tlsmgr**(8).

tls_random_prng_update_period (3600s)
The time between attempts by **tlsmgr**(8) to save the state of the pseudo random number generator (PRNG) to the file specified with $tls_random_exchange_name.

tls_random_reseed_period (3600s)
The maximal time between attempts by **tlsmgr**(8) to re-seed the in-memory pseudo random number generator (PRNG) pool from external sources.

MISCELLANEOUS CONTROLS

config_directory (see 'postconf -d' output)
The default location of the Postfix main.cf and master.cf configuration files.

data_directory (see 'postconf -d' output)
The directory with Postfix-writable data files (for example: caches, pseudo-random numbers).

daemon_timeout (18000s)
How much time a Postfix daemon process may take to handle a request before it is terminated by a built-in watchdog timer.

process_id (read-only)
The process ID of a Postfix command or daemon process.

process_name (read-only)
The process name of a Postfix command or daemon process.

syslog_facility (mail)
The syslog facility of Postfix logging.

syslog_name (see 'postconf -d' output)
The mail system name that is prepended to the process name in syslog records, so that "smtpd" becomes, for example, "postfix/smtpd".

SEE ALSO

smtp(8), Postfix SMTP client
smtpd(8), Postfix SMTP server
postconf(5), configuration parameters
master(5), generic daemon options
master(8), process manager

syslogd(8), system logging

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

This service was introduced with Postfix version 2.2.

AUTHOR(S)

Lutz Jaenicke
BTU Cottbus
Allgemeine Elektrotechnik
Universitaetsplatz 3−4
D−03044 Cottbus, Germany

Adapted by:
Wietse Venema
IBM T.J. Watson Research
P.O. Box 704
Yorktown Heights, NY 10598, USA