NAME

smtp – Postfix SMTP+LMTP client

SYNOPSIS

smtp [generic Postfix daemon options]

DESCRIPTION

The Postfix SMTP+LMTP client implements the SMTP and LMTP mail delivery protocols. It processes message delivery requests from the queue manager. Each request specifies a queue file, a sender address, a domain or host to deliver to, and recipient information. This program expects to be run from the **master**(8) process manager.

The SMTP+LMTP client updates the queue file and marks recipients as finished, or it informs the queue manager that delivery should be tried again at a later time. Delivery status reports are sent to the **bounce**(8), **defer**(8) or **trace**(8) daemon as appropriate.

The SMTP+LMTP client looks up a list of mail exchanger addresses for the destination host, sorts the list by preference, and connects to each listed address until it finds a server that responds.

When a server is not reachable, or when mail delivery fails due to a recoverable error condition, the SMTP+LMTP client will try to deliver the mail to an alternate host.

After a successful mail transaction, a connection may be saved to the **scache**(8) connection cache server, so that it may be used by any SMTP+LMTP client for a subsequent transaction.

By default, connection caching is enabled temporarily for destinations that have a high volume of mail in the active queue. Connection caching can be enabled permanently for specific destinations.

SMTP DESTINATION SYNTAX

SMTP destinations have the following form:

domainname

domainname:*port*

> Look up the mail exchangers for the specified domain, and connect to the specified port (default: **smtp**).

[*hostname*]

[*hostname*]:*port*

> Look up the address(es) of the specified host, and connect to the specified port (default: **smtp**).

[*address*]

[*address*]:*port*

> Connect to the host at the specified address, and connect to the specified port (default: **smtp**). An IPv6 address must be formatted as [**ipv6**:*address*].

LMTP DESTINATION SYNTAX

LMTP destinations have the following form:

unix:*pathname*

> Connect to the local UNIX−domain server that is bound to the specified *pathname*. If the process runs chrooted, an absolute pathname is interpreted relative to the Postfix queue directory.

inet:*hostname*

inet:*hostname*:*port*

inet:[*address*]

inet:[*address*]:*port*

> Connect to the specified TCP port on the specified local or remote host. If no port is specified, connect to the port defined as **lmtp** in **services**(4). If no such service is found, the **lmtp_tcp_port** configuration parameter (default value of 24) will be used. An IPv6 address must be formatted as [**ipv6**:*address*].

SECURITY

The SMTP+LMTP client is moderately security−sensitive. It talks to SMTP or LMTP servers and to DNS servers on the network. The SMTP+LMTP client can be run chrooted at fixed low privilege.

STANDARDS

RFC 821 (SMTP protocol)
RFC 822 (ARPA Internet Text Messages)
RFC 1651 (SMTP service extensions)
RFC 1652 (8bit−MIME transport)
RFC 1870 (Message Size Declaration)
RFC 2033 (LMTP protocol)
RFC 2034 (SMTP Enhanced Error Codes)
RFC 2045 (MIME: Format of Internet Message Bodies)
RFC 2046 (MIME: Media Types)
RFC 2554 (AUTH command)
RFC 2821 (SMTP protocol)
RFC 2920 (SMTP Pipelining)
RFC 3207 (STARTTLS command)
RFC 3461 (SMTP DSN Extension)
RFC 3463 (Enhanced Status Codes)
RFC 4954 (AUTH command)
RFC 5321 (SMTP protocol)
RFC 6531 (Internationalized SMTP)
RFC 6533 (Internationalized Delivery Status Notifications)

DIAGNOSTICS

Problems and transactions are logged to **syslogd**(8). Corrupted message files are marked so that the queue manager can move them to the **corrupt** queue for further inspection.

Depending on the setting of the **notify_classes** parameter, the postmaster is notified of bounces, protocol problems, and of other trouble.

BUGS

SMTP and LMTP connection caching does not work with TLS. The necessary support for TLS object passivation and re−activation does not exist without closing the session, which defeats the purpose.

SMTP and LMTP connection caching assumes that SASL credentials are valid for all destinations that map onto the same IP address and TCP port.

CONFIGURATION PARAMETERS

Before Postfix version 2.3, the LMTP client is a separate program that implements only a subset of the functionality available with SMTP: there is no support for TLS, and connections are cached in−process, making it ineffective when the client is used for multiple domains.

Most smtp_*xxx* configuration parameters have an lmtp_*xxx* "mirror" parameter for the equivalent LMTP feature. This document describes only those LMTP−related parameters that aren't simply "mirror" parameters.

Changes to **main.cf** are picked up automatically, as **smtp**(8) processes run for only a limited amount of time. Use the command "**postfix reload**" to speed up a change.

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

COMPATIBILITY CONTROLS

ignore_mx_lookup_error (no)
> Ignore DNS MX lookups that produce no response.

smtp_always_send_ehlo (yes)
> Always send EHLO at the start of an SMTP session.

smtp_never_send_ehlo (no)
> Never send EHLO at the start of an SMTP session.

smtp_defer_if_no_mx_address_found (no)
> Defer mail delivery when no MX record resolves to an IP address.

smtp_line_length_limit (998)
> The maximal length of message header and body lines that Postfix will send via SMTP.

smtp_pix_workaround_delay_time (10s)
> How long the Postfix SMTP client pauses before sending ".<CR><LF>" in order to work around the PIX firewall "<CR><LF>.<CR><LF>" bug.

smtp_pix_workaround_threshold_time (500s)
> How long a message must be queued before the Postfix SMTP client turns on the PIX firewall "<CR><LF>.<CR><LF>" bug workaround for delivery through firewalls with "smtp fixup" mode turned on.

smtp_pix_workarounds (disable_esmtp, delay_dotcrlf)
> A list that specifies zero or more workarounds for CISCO PIX firewall bugs.

smtp_pix_workaround_maps (empty)
> Lookup tables, indexed by the remote SMTP server address, with per−destination workarounds for CISCO PIX firewall bugs.

smtp_quote_rfc821_envelope (yes)
> Quote addresses in Postfix SMTP client MAIL FROM and RCPT TO commands as required by RFC 5321.

smtp_reply_filter (empty)
> A mechanism to transform replies from remote SMTP servers one line at a time.

smtp_skip_5xx_greeting (yes)
> Skip remote SMTP servers that greet with a 5XX status code.

smtp_skip_quit_response (yes)
> Do not wait for the response to the SMTP QUIT command.

Available in Postfix version 2.0 and earlier:

smtp_skip_4xx_greeting (yes)
> Skip SMTP servers that greet with a 4XX status code (go away, try again later).

Available in Postfix version 2.2 and later:

smtp_discard_ehlo_keyword_address_maps (empty)
> Lookup tables, indexed by the remote SMTP server address, with case insensitive lists of EHLO keywords (pipelining, starttls, auth, etc.) that the Postfix SMTP client will ignore in the EHLO response from a remote SMTP server.

smtp_discard_ehlo_keywords (empty)
> A case insensitive list of EHLO keywords (pipelining, starttls, auth, etc.) that the Postfix SMTP client will ignore in the EHLO response from a remote SMTP server.

smtp_generic_maps (empty)
> Optional lookup tables that perform address rewriting in the Postfix SMTP client, typically to transform a locally valid address into a globally valid address when sending mail across the

Internet.

Available in Postfix version 2.2.9 and later:

smtp_cname_overrides_servername (version dependent)
> When the remote SMTP servername is a DNS CNAME, replace the servername with the result from CNAME expansion for the purpose of logging, SASL password lookup, TLS policy decisions, or TLS certificate verification.

Available in Postfix version 2.3 and later:

lmtp_discard_lhlo_keyword_address_maps (empty)
> Lookup tables, indexed by the remote LMTP server address, with case insensitive lists of LHLO keywords (pipelining, starttls, auth, etc.) that the Postfix LMTP client will ignore in the LHLO response from a remote LMTP server.

lmtp_discard_lhlo_keywords (empty)
> A case insensitive list of LHLO keywords (pipelining, starttls, auth, etc.) that the Postfix LMTP client will ignore in the LHLO response from a remote LMTP server.

Available in Postfix version 2.4.4 and later:

send_cyrus_sasl_authzid (no)
> When authenticating to a remote SMTP or LMTP server with the default setting "no", send no SASL authoriZation ID (authzid); send only the SASL authentiCation ID (authcid) plus the authcid's password.

Available in Postfix version 2.5 and later:

smtp_header_checks (empty)
> Restricted **header_checks**(5) tables for the Postfix SMTP client.

smtp_mime_header_checks (empty)
> Restricted **mime_header_checks**(5) tables for the Postfix SMTP client.

smtp_nested_header_checks (empty)
> Restricted **nested_header_checks**(5) tables for the Postfix SMTP client.

smtp_body_checks (empty)
> Restricted **body_checks**(5) tables for the Postfix SMTP client.

Available in Postfix version 2.6 and later:

tcp_windowsize (0)
> An optional workaround for routers that break TCP window scaling.

Available in Postfix version 2.8 and later:

smtp_dns_resolver_options (empty)
> DNS Resolver options for the Postfix SMTP client.

Available in Postfix version 2.9 and later:

smtp_per_record_deadline (no)
> Change the behavior of the smtp_*_timeout time limits, from a time limit per read or write system call, to a time limit to send or receive a complete record (an SMTP command line, SMTP response line, SMTP message content line, or TLS protocol message).

smtp_send_dummy_mail_auth (no)
> Whether or not to append the "AUTH=<>" option to the MAIL FROM command in SASL−authenticated SMTP sessions.

Available in Postfix version 2.11 and later:

smtp_dns_support_level (empty)
> Level of DNS support in the Postfix SMTP client.

Available in Postfix version 3.0 and later:

smtp_delivery_status_filter ($default_delivery_status_filter)

Optional fi lter for the **smtp**(8) delivery agent to change the delivery status code or explanatory text of successful or unsuccessful deliveries.

smtp_dns_reply_filter (empty)

Optional fi lter for Postfi x SMTP client DNS lookup results.

MIME PROCESSING CONTROLS

Available in Postfi x version 2.0 and later:

disable_mime_output_conversion (no)

Disable the conversion of 8BITMIME format to 7BIT format.

mime_boundary_length_limit (2048)

The maximal length of MIME multipart boundary strings.

mime_nesting_limit (100)

The maximal recursion level that the MIME processor will handle.

EXTERNAL CONTENT INSPECTION CONTROLS

Available in Postfi x version 2.1 and later:

smtp_send_xforward_command (no)

Send the non−standard XFORWARD command when the Postfi x SMTP server EHLO response announces XFORWARD support.

SASL AUTHENTICATION CONTROLS

smtp_sasl_auth_enable (no)

Enable SASL authentication in the Postfi x SMTP client.

smtp_sasl_password_maps (empty)

Optional Postfi x SMTP client lookup tables with one username:password entry per remote hostname or domain, or sender address when sender−dependent authentication is enabled.

smtp_sasl_security_options (noplaintext, noanonymous)

Postfi x SMTP client SASL security options; as of Postfi x 2.3 the list of available features depends on the SASL client implementation that is selected with **smtp_sasl_type**.

Available in Postfi x version 2.2 and later:

smtp_sasl_mechanism_filter (empty)

If non−empty, a Postfi x SMTP client fi lter for the remote SMTP server's list of offered SASL mechanisms.

Available in Postfi x version 2.3 and later:

smtp_sender_dependent_authentication (no)

Enable sender−dependent authentication in the Postfi x SMTP client; this is available only with SASL authentication, and disables SMTP connection caching to ensure that mail from different senders will use the appropriate credentials.

smtp_sasl_path (empty)

Implementation−specifi c information that the Postfi x SMTP client passes through to the SASL plug−in implementation that is selected with **smtp_sasl_type**.

smtp_sasl_type (cyrus)

The SASL plug−in type that the Postfi x SMTP client should use for authentication.

Available in Postfi x version 2.5 and later:

smtp_sasl_auth_cache_name (empty)

An optional table to prevent repeated SASL authentication failures with the same remote SMTP server hostname, username and password.

smtp_sasl_auth_cache_time (90d)

The maximal age of an smtp_sasl_auth_cache_name entry before it is removed.

smtp_sasl_auth_soft_bounce (yes)

When a remote SMTP server rejects a SASL authentication request with a 535 reply code, defer mail delivery instead of returning mail as undeliverable.

Available in Postfix version 2.9 and later:

smtp_send_dummy_mail_auth (no)

Whether or not to append the "AUTH=<>" option to the MAIL FROM command in SASL−authenticated SMTP sessions.

STARTTLS SUPPORT CONTROLS

Detailed information about STARTTLS configuration may be found in the TLS_README document.

smtp_tls_security_level (empty)

The default SMTP TLS security level for the Postfix SMTP client; when a non−empty value is specified, this overrides the obsolete parameters smtp_use_tls, smtp_enforce_tls, and smtp_tls_enforce_peername.

smtp_sasl_tls_security_options ($smtp_sasl_security_options)

The SASL authentication security options that the Postfix SMTP client uses for TLS encrypted SMTP sessions.

smtp_starttls_timeout (300s)

Time limit for Postfix SMTP client write and read operations during TLS startup and shutdown handshake procedures.

smtp_tls_CAfile (empty)

A file containing CA certificates of root CAs trusted to sign either remote SMTP server certificates or intermediate CA certificates.

smtp_tls_CApath (empty)

Directory with PEM format Certification Authority certificates that the Postfix SMTP client uses to verify a remote SMTP server certificate.

smtp_tls_cert_file (empty)

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

smtp_tls_mandatory_ciphers (medium)

The minimum TLS cipher grade that the Postfix SMTP client will use with mandatory TLS encryption.

smtp_tls_exclude_ciphers (empty)

List of ciphers or cipher types to exclude from the Postfix SMTP client cipher list at all TLS security levels.

smtp_tls_mandatory_exclude_ciphers (empty)

Additional list of ciphers or cipher types to exclude from the Postfix SMTP client cipher list at mandatory TLS security levels.

smtp_tls_dcert_file (empty)

File with the Postfix SMTP client DSA certificate in PEM format.

smtp_tls_dkey_file ($smtp_tls_dcert_file)

File with the Postfix SMTP client DSA private key in PEM format.

smtp_tls_key_file ($smtp_tls_cert_file)

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

smtp_tls_loglevel (0)

Enable additional Postfix SMTP client logging of TLS activity.

smtp_tls_note_starttls_offer (no)
> Log the hostname of a remote SMTP server that offers STARTTLS, when TLS is not already enabled for that server.

smtp_tls_policy_maps (empty)
> Optional lookup tables with the Postfix SMTP client TLS security policy by next−hop destination; when a non−empty value is specified, this overrides the obsolete smtp_tls_per_site parameter.

smtp_tls_mandatory_protocols (!SSLv2, !SSLv3)
> List of SSL/TLS protocols that the Postfix SMTP client will use with mandatory TLS encryption.

smtp_tls_scert_verifydepth (9)
> The verification depth for remote SMTP server certificates.

smtp_tls_secure_cert_match (nexthop, dot−nexthop)
> How the Postfix SMTP client verifies the server certificate peername for the "secure" TLS security level.

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.

smtp_tls_verify_cert_match (hostname)
> How the Postfix SMTP client verifies the server certificate peername for the "verify" TLS security level.

tls_daemon_random_bytes (32)
> The number of pseudo−random bytes that an **smtp**(8) or **smtpd**(8) process requests from the **tlsmgr**(8) server in order to seed its internal pseudo random number generator (PRNG).

tls_high_cipherlist (ALL:!EXPORT:!LOW:!MEDIUM:+RC4:@STRENGTH)
> The OpenSSL cipherlist for "HIGH" grade ciphers.

tls_medium_cipherlist (ALL:!EXPORT:!LOW:+RC4:@STRENGTH)
> The OpenSSL cipherlist for "MEDIUM" or higher grade ciphers.

tls_low_cipherlist (ALL:!EXPORT:+RC4:@STRENGTH)
> The OpenSSL cipherlist for "LOW" or higher grade ciphers.

tls_export_cipherlist (ALL:+RC4:@STRENGTH)
> The OpenSSL cipherlist for "EXPORT" or higher grade ciphers.

tls_null_cipherlist (eNULL:!aNULL)
> The OpenSSL cipherlist for "NULL" grade ciphers that provide authentication without encryption.

Available in Postfix version 2.4 and later:

smtp_sasl_tls_verified_security_options ($smtp_sasl_tls_security_options)
> The SASL authentication security options that the Postfix SMTP client uses for TLS encrypted SMTP sessions with a verified server certificate.

Available in Postfix version 2.5 and later:

smtp_tls_fingerprint_cert_match (empty)
> List of acceptable remote SMTP server certificate fingerprints for the "fingerprint" TLS security level (**smtp_tls_security_level** = fingerprint).

smtp_tls_fingerprint_digest (md5)
> The message digest algorithm used to construct remote SMTP server certificate fingerprints.

Available in Postfix version 2.6 and later:

smtp_tls_protocols (!SSLv2, !SSLv3)
>   List of TLS protocols that the Postfix SMTP client will exclude or include with opportunistic TLS encryption.

smtp_tls_ciphers (medium)
>   The minimum TLS cipher grade that the Postfix SMTP client will use with opportunistic TLS encryption.

smtp_tls_eccert_file (empty)
>   File with the Postfix SMTP client ECDSA certificate in PEM format.

smtp_tls_eckey_file ($smtp_tls_eccert_file)
>   File with the Postfix SMTP client ECDSA private key in PEM format.

Available in Postfix version 2.7 and later:

smtp_tls_block_early_mail_reply (no)
>   Try to detect a mail hijacking attack based on a TLS protocol vulnerability (CVE−2009−3555), where an attacker prepends malicious HELO, MAIL, RCPT, DATA commands to a Postfix SMTP client TLS session.

Available in Postfix version 2.8 and later:

tls_disable_workarounds (see 'postconf -d' output)
>   List or bit−mask of OpenSSL bug work−arounds to disable.

Available in Postfix version 2.11 and later:

smtp_tls_trust_anchor_file (empty)
>   Zero or more PEM−format files with trust−anchor certificates and/or public keys.

smtp_tls_force_insecure_host_tlsa_lookup (no)
>   Lookup the associated DANE TLSA RRset even when a hostname is not an alias and its address records lie in an unsigned zone.

tls_dane_trust_anchor_digest_enable (yes)
>   RFC 6698 trust−anchor digest support in the Postfix TLS library.

tlsmgr_service_name (tlsmgr)
>   The name of the **tlsmgr**(8) service entry in master.cf.

Available in Postfix version 3.0 and later:

smtp_tls_wrappermode (no)
>   Request that the Postfix SMTP client connects using the legacy SMTPS protocol instead of using the STARTTLS command.

OBSOLETE STARTTLS CONTROLS

The following configuration parameters exist for compatibility with Postfix versions before 2.3. Support for these will be removed in a future release.

smtp_use_tls (no)
>   Opportunistic mode: use TLS when a remote SMTP server announces STARTTLS support, otherwise send the mail in the clear.

smtp_enforce_tls (no)
>   Enforcement mode: require that remote SMTP servers use TLS encryption, and never send mail in the clear.

smtp_tls_enforce_peername (yes)
>   With mandatory TLS encryption, require that the remote SMTP server hostname matches the information in the remote SMTP server certificate.

smtp_tls_per_site (empty)
>   Optional lookup tables with the Postfix SMTP client TLS usage policy by next−hop destination and by remote SMTP server hostname.

smtp_tls_cipherlist (empty)
> Obsolete Postfix < 2.3 control for the Postfix SMTP client TLS cipher list.

RESOURCE AND RATE CONTROLS

smtp_destination_concurrency_limit ($default_destination_concurrency_limit)
> The maximal number of parallel deliveries to the same destination via the smtp message delivery transport.

smtp_destination_recipient_limit ($default_destination_recipient_limit)
> The maximal number of recipients per message for the smtp message delivery transport.

smtp_connect_timeout (30s)
> The Postfix SMTP client time limit for completing a TCP connection, or zero (use the operating system built−in time limit).

smtp_helo_timeout (300s)
> The Postfix SMTP client time limit for sending the HELO or EHLO command, and for receiving the initial remote SMTP server response.

lmtp_lhlo_timeout (300s)
> The Postfix LMTP client time limit for sending the LHLO command, and for receiving the initial remote LMTP server response.

smtp_xforward_timeout (300s)
> The Postfix SMTP client time limit for sending the XFORWARD command, and for receiving the remote SMTP server response.

smtp_mail_timeout (300s)
> The Postfix SMTP client time limit for sending the MAIL FROM command, and for receiving the remote SMTP server response.

smtp_rcpt_timeout (300s)
> The Postfix SMTP client time limit for sending the SMTP RCPT TO command, and for receiving the remote SMTP server response.

smtp_data_init_timeout (120s)
> The Postfix SMTP client time limit for sending the SMTP DATA command, and for receiving the remote SMTP server response.

smtp_data_xfer_timeout (180s)
> The Postfix SMTP client time limit for sending the SMTP message content.

smtp_data_done_timeout (600s)
> The Postfix SMTP client time limit for sending the SMTP ".", and for receiving the remote SMTP server response.

smtp_quit_timeout (300s)
> The Postfix SMTP client time limit for sending the QUIT command, and for receiving the remote SMTP server response.

Available in Postfix version 2.1 and later:

smtp_mx_address_limit (5)
> The maximal number of MX (mail exchanger) IP addresses that can result from Postfix SMTP client mail exchanger lookups, or zero (no limit).

smtp_mx_session_limit (2)
> The maximal number of SMTP sessions per delivery request before the Postfix SMTP client gives up or delivers to a fall−back relay host, or zero (no limit).

smtp_rset_timeout (20s)
> The Postfix SMTP client time limit for sending the RSET command, and for receiving the remote SMTP server response.

Available in Postfix version 2.2 and earlier:

lmtp_cache_connection (yes)
> Keep Postfix LMTP client connections open for up to $max_idle seconds.

Available in Postfix version 2.2 and later:

smtp_connection_cache_destinations (empty)
> Permanently enable SMTP connection caching for the specified destinations.

smtp_connection_cache_on_demand (yes)
> Temporarily enable SMTP connection caching while a destination has a high volume of mail in the active queue.

smtp_connection_reuse_time_limit (300s)
> The amount of time during which Postfix will use an SMTP connection repeatedly.

smtp_connection_cache_time_limit (2s)
> When SMTP connection caching is enabled, the amount of time that an unused SMTP client socket is kept open before it is closed.

Available in Postfix version 2.3 and later:

connection_cache_protocol_timeout (5s)
> Time limit for connection cache connect, send or receive operations.

Available in Postfix version 2.9 and later:

smtp_per_record_deadline (no)
> Change the behavior of the smtp_*_timeout time limits, from a time limit per read or write system call, to a time limit to send or receive a complete record (an SMTP command line, SMTP response line, SMTP message content line, or TLS protocol message).

Available in Postfix version 2.11 and later:

smtp_connection_reuse_count_limit (0)
> When SMTP connection caching is enabled, the number of times that an SMTP session may be reused before it is closed, or zero (no limit).

SMTPUTF8 CONTROLS
Preliminary SMTPUTF8 support is introduced with Postfix 3.0.

smtputf8_enable (yes)
> Enable preliminary SMTPUTF8 support for the protocols described in RFC 6531..6533.

smtputf8_autodetect_classes (sendmail, verify)
> Detect that a message requires SMTPUTF8 support for the specified mail origin classes.

TROUBLE SHOOTING CONTROLS
debug_peer_level (2)
> The increment in verbose logging level when a remote client or server matches a pattern in the debug_peer_list parameter.

debug_peer_list (empty)
> Optional list of remote client or server hostname or network address patterns that cause the verbose logging level to increase by the amount specified in $debug_peer_level.

error_notice_recipient (postmaster)
> The recipient of postmaster notifications about mail delivery problems that are caused by policy, resource, software or protocol errors.

internal_mail_filter_classes (empty)
> What categories of Postfix−generated mail are subject to before−queue content inspection by non_smtpd_milters, header_checks and body_checks.

notify_classes (resource, software)
> The list of error classes that are reported to the postmaster.

MISCELLANEOUS CONTROLS

best_mx_transport (empty)

Where the Postfix SMTP client should deliver mail when it detects a "mail loops back to myself" error condition.

config_directory (see 'postconf -d' output)

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

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.

delay_logging_resolution_limit (2)

The maximal number of digits after the decimal point when logging sub−second delay values.

disable_dns_lookups (no)

Disable DNS lookups in the Postfix SMTP and LMTP clients.

inet_interfaces (all)

The network interface addresses that this mail system receives mail on.

inet_protocols (all)

The Internet protocols Postfix will attempt to use when making or accepting connections.

ipc_timeout (3600s)

The time limit for sending or receiving information over an internal communication channel.

lmtp_assume_final (no)

When a remote LMTP server announces no DSN support, assume that the server performs final delivery, and send "delivered" delivery status notifications instead of "relayed".

lmtp_tcp_port (24)

The default TCP port that the Postfix LMTP client connects to.

max_idle (100s)

The maximum amount of time that an idle Postfix daemon process waits for an incoming connection before terminating voluntarily.

max_use (100)

The maximal number of incoming connections that a Postfix daemon process will service before terminating voluntarily.

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.

proxy_interfaces (empty)

The network interface addresses that this mail system receives mail on by way of a proxy or network address translation unit.

smtp_address_preference (any)

The address type ("ipv6", "ipv4" or "any") that the Postfix SMTP client will try first, when a destination has IPv6 and IPv4 addresses with equal MX preference.

smtp_bind_address (empty)

An optional numerical network address that the Postfix SMTP client should bind to when making an IPv4 connection.

smtp_bind_address6 (empty)

An optional numerical network address that the Postfix SMTP client should bind to when making an IPv6 connection.

smtp_helo_name ($myhostname)
>The hostname to send in the SMTP HELO or EHLO command.

lmtp_lhlo_name ($myhostname)
>The hostname to send in the LMTP LHLO command.

smtp_host_lookup (dns)
>What mechanisms the Postfix SMTP client uses to look up a host's IP address.

smtp_randomize_addresses (yes)
>Randomize the order of equal−preference MX host addresses.

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".

Available with Postfix 2.2 and earlier:

fallback_relay (empty)
>Optional list of relay hosts for SMTP destinations that can't be found or that are unreachable.

Available with Postfix 2.3 and later:

smtp_fallback_relay ($fallback_relay)
>Optional list of relay hosts for SMTP destinations that can't be found or that are unreachable.

Available with Postfix 3.0 and later:

smtp_address_verify_target (rcpt)
>In the context of email address verification, the SMTP protocol stage that determines whether an email address is deliverable.

SEE ALSO

generic(5), output address rewriting
header_checks(5), message header content inspection
body_checks(5), body parts content inspection
qmgr(8), queue manager
bounce(8), delivery status reports
scache(8), connection cache server
postconf(5), configuration parameters
master(5), generic daemon options
master(8), process manager
tlsmgr(8), TLS session and PRNG management
syslogd(8), system logging

README FILES

Use "**postconf readme_directory**" or "**postconf html_directory**" to locate this information.
SASL_README, Postfix SASL howto
TLS_README, Postfix STARTTLS howto

LICENSE

The Secure Mailer license must be distributed with this software.

AUTHOR(S)

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

Command pipelining in cooperation with:

Jon Ribbens
Oaktree Internet Solutions Ltd.,
Internet House,
Canal Basin,
Coventry,
CV1 4LY, United Kingdom.

SASL support originally by:
Till Franke
SuSE Rhein/Main AG
65760 Eschborn, Germany

TLS support originally by:
Lutz Jaenicke
BTU Cottbus
Allgemeine Elektrotechnik
Universitaetsplatz 3–4
D–03044 Cottbus, Germany

Revised TLS and SMTP connection cache support by:
Victor Duchovni
Morgan Stanley