NAME

proxymap − Postfix lookup table proxy server

SYNOPSIS

proxymap [generic Postfix daemon options]

DESCRIPTION

The **proxymap**(8) server provides read−only or read−write table lookup service to Postfix processes. These services are implemented with distinct service names: **proxymap** and **proxywrite**, respectively. The purpose of these services is:

- To overcome chroot restrictions. For example, a chrooted SMTP server needs access to the system passwd file in order to reject mail for non−existent local addresses, but it is not practical to maintain a copy of the passwd file in the chroot jail. The solution:

  ```
  local_recipient_maps =
    proxy:unix:passwd.byname $alias_maps
  ```

- To consolidate the number of open lookup tables by sharing one open table among multiple processes. For example, making mysql connections from every Postfix daemon process results in "too many connections" errors. The solution:

  ```
  virtual_alias_maps =
    proxy:mysql:/etc/postfix/virtual_alias.cf
  ```

  The total number of connections is limited by the number of proxymap server processes.

- To provide single−updater functionality for lookup tables that do not reliably support multiple writers (i.e. all file−based tables).

The **proxymap**(8) server implements the following requests:

open *maptype:mapname flags*
: Open the table with type *maptype* and name *mapname*, as controlled by *flags*. The reply includes the *maptype* dependent flags (to distinguish a fixed string table from a regular expression table).

lookup *maptype:mapname flags key*
: Look up the data stored under the requested key. The reply is the request completion status code and the lookup result value. The *maptype:mapname* and *flags* are the same as with the **open** request.

update *maptype:mapname flags key value*
: Update the data stored under the requested key. The reply is the request completion status code. The *maptype:mapname* and *flags* are the same as with the **open** request.

  To implement single−updater maps, specify a process limit of 1 in the master.cf file entry for the **proxywrite** service.

  This request is supported in Postfix 2.5 and later.

delete *maptype:mapname flags key*
: Delete the data stored under the requested key. The reply is the request completion status code. The *maptype:mapname* and *flags* are the same as with the **open** request.

  This request is supported in Postfix 2.5 and later.

sequence *maptype:mapname flags function*
: Iterate over the specified database. The *function* is one of DICT_SEQ_FUN_FIRST or DICT_SEQ_FUN_NEXT. The reply is the request completion status code and a lookup key and result value, if found.

This request is supported in Postfix 2.9 and later.

The request completion status is one of OK, RETRY, NOKEY (lookup failed because the key was not found), BAD (malformed request) or DENY (the table is not approved for proxy read or update access).

There is no **close** command, nor are tables implicitly closed when a client disconnects. The purpose is to share tables among multiple client processes.

SERVER PROCESS MANAGEMENT

proxymap(8) servers run under control by the Postfix **master**(8) server. Each server can handle multiple simultaneous connections. When all servers are busy while a client connects, the **master**(8) creates a new **proxymap**(8) server process, provided that the process limit is not exceeded. Each server terminates after serving at least **$max_use** clients or after **$max_idle** seconds of idle time.

SECURITY

The **proxymap**(8) server opens only tables that are approved via the **proxy_read_maps** or **proxy_write_maps** configuration parameters, does not talk to users, and can run at fixed low privilege, chrooted or not. However, running the proxymap server chrooted severely limits usability, because it can open only chrooted tables.

The **proxymap**(8) server is not a trusted daemon process, and must not be used to look up sensitive information such as UNIX user or group IDs, mailbox file/directory names or external commands.

In Postfix version 2.2 and later, the proxymap client recognizes requests to access a table for security−sensitive purposes, and opens the table directly. This allows the same main.cf setting to be used by sensitive and non−sensitive processes.

Postfix−writable data files should be stored under a dedicated directory that is writable only by the Postfix mail system, such as the Postfix−owned **data_directory**.

In particular, Postfix−writable files should never exist in root−owned directories. That would open up a particular type of security hole where ownership of a file or directory does not match the provider of its content.

DIAGNOSTICS

Problems and transactions are logged to **syslogd**(8).

BUGS

The **proxymap**(8) server provides service to multiple clients, and must therefore not be used for tables that have high−latency lookups.

The **proxymap**(8) read−write service does not explicitly close lookup tables (even if it did, this could not be relied on, because the process may be terminated between table updates). The read−write service should therefore not be used with tables that leave persistent storage in an inconsistent state between updates (for example, CDB). Tables that support "sync on update" should be safe (for example, Berkeley DB) as should tables that are implemented by a real DBMS.

CONFIGURATION PARAMETERS

On busy mail systems a long time may pass before **proxymap**(8) relevant changes to **main.cf** are picked up. 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.

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.

ipc_timeout (3600s)
The time limit for sending or receiving information over an internal communication channel.

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_read_maps (see 'postconf -d' output)
The lookup tables that the **proxymap**(8) server is allowed to access for the read−only service.

Available in Postfix 2.5 and later:

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

proxy_write_maps (see 'postconf -d' output)
The lookup tables that the **proxymap**(8) server is allowed to access for the read−write service.

SEE ALSO

postconf(5), configuration parameters
master(5), generic daemon options

README FILES

Use "**postconf readme_directory**" or "**postconf html_directory**" to locate this information.
DATABASE_README, Postfix lookup table overview

LICENSE

The Secure Mailer license must be distributed with this software.

HISTORY

The proxymap service was introduced with Postfix 2.0.

AUTHOR(S)

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