NAME

anvil - Postfix session count and request rate control

SYNOPSIS

anvil [generic Postfix daemon options]

DESCRIPTION

The Postfix **anvil(8)** server maintains statistics about client connection counts or client request rates. This information can be used to defend against clients that hammer a server with either too many simultaneous sessions, or with too many successive requests within a configurable time interval. This server is designed to run under control by the Postfix **master(8)** server.

In the following text, **ident** specifies a (service, client) combination. The exact syntax of that information is application-dependent; the **anvil(8)** server does not care.

CONNECTION COUNT/RATE CONTROL

To register a new connection send the following request to the **anvil(8)** server:

request=connect
ident=*string*

The **anvil(8)** server answers with the number of simultaneous connections and the number of connections per unit time for the (service, client) combination specified with **ident**:

status=0
count=*number*
rate=*number*

To register a disconnect event send the following request to the **anvil(8)** server:

request=disconnect
ident=*string*

The **anvil(8)** server replies with:

status=0

MESSAGE RATE CONTROL

To register a message delivery request send the following request to the **anvil(8)** server:

request=message
ident=*string*

The **anvil(8)** server answers with the number of message delivery requests per unit time for the (service, client) combination specified with **ident**:

status=0
rate=*number*

RECIPIENT RATE CONTROL

To register a recipient request send the following request to the **anvil(8)** server:

request=recipient
ident=*string*

The **anvil(8)** server answers with the number of recipient addresses per unit time for the (service, client) combination specified with **ident**:

status=0
rate=*number*

TLS SESSION NEGOTIATION RATE CONTROL

The features described in this section are available with Postfix 2.3 and later.

To register a request for a new (i.e. not cached) TLS session send the following request to the **anvil(8)** server:

request=newtls
ident=*string*

The **anvil(8)** server answers with the number of new TLS session requests per unit time for the (service, client) combination specified with **ident**:

status=0
rate=*number*

To retrieve new TLS session request rate information without updating the counter information, send:

request=newtls_report
ident=*string*

The **anvil(8)** server answers with the number of new TLS session requests per unit time for the (service, client) combination specified with **ident**:

status=0
rate=*number*

SECURITY

The **anvil(8)** server does not talk to the network or to local users, and can run chrooted at fixed low privilege.

The **anvil(8)** server maintains an in-memory table with information about recent clients requests. No persistent state is kept because standard system library routines are not sufficiently robust for update-intensive applications.

Although the in-memory state is kept only temporarily, this may require a lot of memory on systems that handle connections from many remote clients. To reduce memory usage, reduce the time unit over which state is kept.

DIAGNOSTICS

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

Upon exit, and every **anvil_status_update_time** seconds, the server logs the maximal count and rate values measured, together with (service, client) information and the time of day associated with those events. In order to avoid unnecessary overhead, no measurements are done for activity that isn't concurrency limited or rate limited.

BUGS

Systems behind network address translating routers or proxies appear to have the same client address and can run into connection count and/or rate limits falsely.

In this preliminary implementation, a count (or rate) limited server process can have only one remote client at a time. If a server process reports multiple simultaneous clients, state is kept only for the last reported client.

The **anvil(8)** server automatically discards client request information after it expires. To prevent the **anvil(8)** server from discarding client request rate information too early or too late, a rate limited service should always register connect/disconnect events even when it does not explicitly limit them.

CONFIGURATION PARAMETERS

On low-traffic mail systems, changes to **main.cf** are picked up automatically as **anvil(8)** processes run for only a limited amount of time. On other mail systems, 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.

anvil_rate_time_unit (60s)
The time unit over which client connection rates and other rates are calculated.

anvil_status_update_time (600s)
How frequently the **anvil(8)** connection and rate limiting server logs peak usage information.

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.

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.

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

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

README FILES

Use "**postconf readme_directory**" or "**postconf html_directory**" to locate this information.
TUNING_README, performance tuning

LICENSE

The Secure Mailer license must be distributed with this software.

HISTORY

The anvil service is available in Postfix 2.2 and later.

AUTHOR(S)

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