NAME

access - Postfix SMTP server access table

SYNOPSIS

postmap /etc/postfix/access

postmap -q "*string***" /etc/postfix/access**

postmap -q - /etc/postfix/access <*inputfile*

DESCRIPTION

This document describes access control on remote SMTP client information: host names, network addresses, and envelope sender or recipient addresses; it is implemented by the Postfix SMTP server. See **header_checks(5)** or **body_checks(5)** for access control on the content of email messages.

Normally, the **access(5)** table is specified as a text file that serves as input to the **postmap(1)** command. The result, an indexed file in **dbm** or **db** format, is used for fast searching by the mail system. Execute the command "**postmap /etc/postfix/access**" to rebuild an indexed file after changing the corresponding text file.

When the table is provided via other means such as NIS, LDAP or SQL, the same lookups are done as for ordinary indexed files.

Alternatively, the table can be provided as a regular-expression map where patterns are given as regular expressions, or lookups can be directed to TCP-based server. In those cases, the lookups are done in a slightly different way as described below under "REGULAR EXPRESSION TABLES" or "TCP-BASED TABLES".

CASE FOLDING

The search string is folded to lowercase before database lookup. As of Postfix 2.3, the search string is not case folded with database types such as regexp: or pcre: whose lookup fields can match both upper and lower case.

TABLE FORMAT

The input format for the **postmap(1)** command is as follows:

pattern action
: When *pattern* matches a mail address, domain or host address, perform the corresponding *action*.

blank lines and comments
: Empty lines and whitespace-only lines are ignored, as are lines whose first non-whitespace character is a ‘#’.

multi-line text
: A logical line starts with non-whitespace text. A line that starts with whitespace continues a logical line.

EMAIL ADDRESS PATTERNS

With lookups from indexed files such as DB or DBM, or from networked tables such as NIS, LDAP or SQL, patterns are tried in the order as listed below:

user@domain
: Matches the specified mail address.

domain.tld
: Matches *domain.tld* as the domain part of an email address.

  The pattern *domain.tld* also matches subdomains, but only when the string **smtpd_access_maps** is listed in the Postfix **parent_domain_matches_subdomains** configuration setting.

.domain.tld
: Matches subdomains of *domain.tld*, but only when the string **smtpd_access_maps** is not listed in the Postfix **parent_domain_matches_subdomains** configuration setting.

user@ Matches all mail addresses with the specified user part.

Note: lookup of the null sender address is not possible with some types of lookup table. By default, Postfix uses <> as the lookup key for such addresses. The value is specified with the **smtpd_null_access_lookup_key** parameter in the Postfix **main.cf** file.

EMAIL ADDRESS EXTENSION

When a mail address localpart contains the optional recipient delimiter (e.g., *user+foo@domain*), the lookup order becomes: *user+foo@domain*, *user@domain*, *domain*, *user+foo@*, and *user@*.

HOST NAME/ADDRESS PATTERNS

With lookups from indexed files such as DB or DBM, or from networked tables such as NIS, LDAP or SQL, the following lookup patterns are examined in the order as listed:

domain.tld

Matches *domain.tld*.

The pattern *domain.tld* also matches subdomains, but only when the string **smtpd_access_maps** is listed in the Postfix **parent_domain_matches_subdomains** configuration setting.

.domain.tld

Matches subdomains of *domain.tld*, but only when the string **smtpd_access_maps** is not listed in the Postfix **parent_domain_matches_subdomains** configuration setting.

net.work.addr.ess

net.work.addr

net.work

net Matches the specified IPv4 host address or subnetwork. An IPv4 host address is a sequence of four decimal octets separated by ".".

Subnetworks are matched by repeatedly truncating the last ".octet" from the remote IPv4 host address string until a match is found in the access table, or until further truncation is not possible.

NOTE 1: The access map lookup key must be in canonical form: do not specify unnecessary null characters, and do not enclose network address information with "[]" characters.

NOTE 2: use the **cidr** lookup table type to specify network/netmask patterns. See **cidr_table(5)** for details.

net:work:addr:ess

net:work:addr

net:work

net Matches the specified IPv6 host address or subnetwork. An IPv6 host address is a sequence of three to eight hexadecimal octet pairs separated by ":".

Subnetworks are matched by repeatedly truncating the last ":octetpair" from the remote IPv6 host address string until a match is found in the access table, or until further truncation is not possible.

NOTE 1: the truncation and comparison are done with the string representation of the IPv6 host address. Thus, not all the ":" subnetworks will be tried.

NOTE 2: The access map lookup key must be in canonical form: do not specify unnecessary null characters, and do not enclose network address information with "[]" characters.

NOTE 3: use the **cidr** lookup table type to specify network/netmask patterns. See **cidr_table(5)** for details.

IPv6 support is available in Postfix 2.2 and later.

ACCEPT ACTIONS

OK Accept the address etc. that matches the pattern.

all-numerical

An all-numerical result is treated as OK. This format is generated by address-based relay authorization schemes such as pop-before-smtp.

For other accept actions, see "OTHER ACTIONS" below.

REJECT ACTIONS

Postfix version 2.3 and later support enhanced status codes as defined in RFC 3463. When no code is specified at the beginning of the *text* below, Postfix inserts a default enhanced status code of "5.7.1" in the case of reject actions, and "4.7.1" in the case of defer actions. See "ENHANCED STATUS CODES" below.

4*NN text*

5*NN text*

Reject the address etc. that matches the pattern, and respond with the numerical three-digit code and text. **4***NN* means "try again later", while **5***NN* means "do not try again".

The following responses have special meaning for the Postfix SMTP server:

421 *text* (Postfix 2.3 and later)

521 *text* (Postfix 2.6 and later)

After responding with the numerical three-digit code and text, disconnect immediately from the SMTP client. This frees up SMTP server resources so that they can be made available to another SMTP client.

Note: The "521" response should be used only with botnets and other malware where interoperability is of no concern. The "send 521 and disconnect" behavior is NOT defined in the SMTP standard.

REJECT *optional text...*

Reject the address etc. that matches the pattern. Reply with "**$access_map_reject_code** *optional text...*" when the optional text is specified, otherwise reply with a generic error response message.

DEFER *optional text...*

Reject the address etc. that matches the pattern. Reply with "**$access_map_defer_code** *optional text...*" when the optional text is specified, otherwise reply with a generic error response message.

This feature is available in Postfix 2.6 and later.

DEFER_IF_REJECT *optional text...*

Defer the request if some later restriction would result in a REJECT action. Reply with "**$access_map_defer_code 4.7.1** *optional text...*" when the optional text is specified, otherwise reply with a generic error response message.

Prior to Postfix 2.6, the SMTP reply code is 450.

This feature is available in Postfix 2.1 and later.

DEFER_IF_PERMIT *optional text...*

Defer the request if some later restriction would result in a an explicit or implicit PERMIT action. Reply with "**$access_map_defer_code 4.7.1** *optional te xt...*" when the optional text is specified, otherwise reply with a generic error response message.

Prior to Postfix 2.6, the SMTP reply code is 450.

This feature is available in Postfix 2.1 and later.

For other reject actions, see "OTHER ACTIONS" below.

OTHER ACTIONS

restriction...
Apply the named UCE restriction(s) (**permit**, **reject**, **reject_unauth_destination**, and so on).

BCC *user@domain*
Send one copy of the message to the specified recipient.

If multiple BCC actions are specified within the same SMTP MAIL transaction, only the last action will be used.

This feature is not part of the stable Postfix release.

DISCARD *optional text...*
Claim successful delivery and silently discard the message. Log the optional text if specified, otherwise log a generic message.

Note: this action currently affects all recipients of the message. To discard only one recipient without discarding the entire message, use the transport(5) table to direct mail to the discard(8) service.

This feature is available in Postfix 2.0 and later.

DUNNO
Pretend that the lookup key was not found. This prevents Postfix from trying substrings of the lookup key (such as a subdomain name, or a network address subnetwork).

This feature is available in Postfix 2.0 and later.

FILTER *transport:destination*
After the message is queued, send the entire message through the specified external content filter. The *transport* name specifies the first field of a mail delivery agent definition in master.cf; the syntax of the next-hop *destination* is described in the manual page of the corresponding delivery agent. More information about external content filters is in the Postfix FILTER_README file.

Note 1: do not use $*number* regular expression substitutions for *transport* or *destination* unless you know that the information has a trusted origin.

Note 2: this action overrides the main.cf **content_filter** setting, and affects all recipients of the message. In the case that multiple **FILTER** actions fire, only the last one is executed.

Note 3: the purpose of the FILTER command is to override message routing. To override the recipient's *transport* but not the next-hop *destination*, specify an empty filter *destination* (Postfix 2.7 and later), or specify a *transport:destination* that delivers through a different Postfix instance (Postfix 2.6 and earlier). Other options are using the recipient-dependent **transport_maps** or the sender-dependent **sender_dependent_default_transport_maps** features.

This feature is available in Postfix 2.0 and later.

HOLD *optional text...*
Place the message on the **hold** queue, where it will sit until someone either deletes it or releases it for delivery. Log the optional text if specified, otherwise log a generic message.

Mail that is placed on hold can be examined with the **postcat(1)** command, and can be destroyed or released with the **postsuper(1)** command.

Note: use "**postsuper -r**" to release mail that was kept on hold for a significant fraction of **$maximal_queue_lifetime** or **$bounce_queue_lifetime**, or longer. Use "**postsuper -H**" only for mail that will not expire within a few delivery attempts.

Note: this action currently affects all recipients of the message.

This feature is available in Postfix 2.0 and later.

PREPEND *headername: headervalue*
Prepend the specified message header to the message. When more than one PREPEND action executes, the first prepended header appears before the second etc. prepended header.

Note: this action must execute before the message content is received; it cannot execute in the context of **smtpd_end_of_data_restrictions**.

This feature is available in Postfix 2.1 and later.

REDIRECT *user@domain*
After the message is queued, send the message to the specified address instead of the intended recipient(s).

Note: this action overrides the FILTER action, and currently affects all recipients of the message.

This feature is available in Postfix 2.1 and later.

WARN *optional text...*
Log a warning with the optional text, together with client information and if available, with helo, sender, recipient and protocol information.

This feature is available in Postfix 2.1 and later.

ENHANCED STATUS CODES

Postfix version 2.3 and later support enhanced status codes as defined in RFC 3463. When an enhanced status code is specified in an access table, it is subject to modification. The following transformations are needed when the same access table is used for client, helo, sender, or recipient access restrictions; they happen regardless of whether Postfix replies to a MAIL FROM, RCPT TO or other SMTP command.

- When a sender address matches a REJECT action, the Postfix SMTP server will transform a recipient DSN status (e.g., 4.1.1-4.1.6) into the corresponding sender DSN status, and vice versa.
- When non-address information matches a REJECT action (such as the HELO command argument or the client hostname/address), the Postfix SMTP server will transform a sender or recipient DSN status into a generic non-address DSN status (e.g., 4.0.0).

REGULAR EXPRESSION TABLES

This section describes how the table lookups change when the table is given in the form of regular expressions. For a description of regular expression lookup table syntax, see **regexp_table(5)** or **pcre_table(5)**.

Each pattern is a regular expression that is applied to the entire string being looked up. Depending on the application, that string is an entire client hostname, an entire client IP address, or an entire mail address. Thus, no parent domain or parent network search is done, *user@domain* mail addresses are not broken up into their *user@* and *domain* constituent parts, nor is *user+foo* broken up into *user* and *foo*.

Patterns are applied in the order as specified in the table, until a pattern is found that matches the search string.

Actions are the same as with indexed file lookups, with the additional feature that parenthesized substrings from the pattern can be interpolated as **$1**, **$2** and so on.

TCP-BASED TABLES

This section describes how the table lookups change when lookups are directed to a TCP-based server. For a description of the TCP client/server lookup protocol, see **tcp_table(5)**. This feature is not available up to and including Postfix version 2.4.

Each lookup operation uses the entire query string once. Depending on the application, that string is an entire client hostname, an entire client IP address, or an entire mail address. Thus, no parent domain or parent network search is done, *user@domain* mail addresses are not broken up into their *user@* and *domain* constituent parts, nor is *user+foo* broken up into *user* and *foo*.

Actions are the same as with indexed file lookups.

EXAMPLE

The following example uses an indexed file, so that the order of table entries does not matter. The example permits access by the client at address 1.2.3.4 but rejects all other clients in 1.2.3.0/24. Instead of **hash** lookup tables, some systems use **dbm**. Use the command "**postconf -m**" to find out what lookup tables Postfix supports on your system.

/etc/postfix/main.cf:
smtpd_client_restrictions =
check_client_access hash:/etc/postfix/access

/etc/postfix/access:
1.2.3 REJECT
1.2.3.4 OK

Execute the command "**postmap /etc/postfix/access**" after editing the file.

BUGS

The table format does not understand quoting conventions.

SEE ALSO

postmap(1),
Postfix lookup table manager
smtpd(8),
SMTP server
postconf(5),
configuration parameters
transport(5),
transport:nexthop syntax

README FILES

Use "**postconf readme_directory**" or "**postconf html_directory**" to locate this information.
SMTPD_ACCESS_README, built-in SMTP server access control
DATABASE_README, Postfix lookup table overview

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