NAME

hosts.hfaxd − *HylaFAX* client access control list

DESCRIPTION

The ASCII file **etc/hosts.hfaxd** in the *HylaFAX* spooling area specifies the hosts and users that are permitted to access services through the *hfaxd*(8C) process. This file must exist for client access; if it is not present then *hfaxd* will deny all requests for service. Note also that this file must be readable only by the ''fax'' user; i.e. it should have mode 600 and be owned by ''fax''.

Each newline-terminated entry is a set of colon (:) separated fields, all but the first of which are optional. Trailing null fields and their separators may be omitted. The most general form is:

client:uid:passwd:adminwd

client is a regular expression to be matched against a string ''*user@host*'' that is formed from the *user* string passed to *hfaxd* with the **USER** command and the official *host* name or the DARPA Internet address, specified in ''dot notation''. If *client* does not contain an ''*@*'' then, for backwards compatibility, it is treated as a host for which any user may have access; i.e. it is automatically converted to the regular expression ''^.*@*client*$''.

Comments are introduced with the ''#'' character and extend to the end of the line. Any whitespace immediately preceding a comment is also ignored.

If *client* has a leading ''!'', then it is interpreted as a class of hosts and users to which access is to be **disallowed**. That is, if the pattern matches the client information, then access is denied.

Note that regular expressions are **not** anchored. That is, a regular expression may match a substring of the ''*user@host*'' string. Thus '*pb@.*\.cl\.cam\.ac\.uk*' matches '*cpb@mc.cl.cam.ac.uk.esd.sgi.com*'. Use ''^'' to match the start of the string and ''$'' to match the end.

Fields following *client* are optional and specify the following:

uid The numerical user ID to assign to clients that use the entry for access. *hfaxd* uses the *uid* to control access to server resources such as jobs and documents (the value is used to set the group ID of files created by a client).

Multiple clients/users may share the same *uid* or unique IDs may be created for each client. User IDs may be any number in the range [0..60002] with 60002 used, by convention, for entries that do not have a *uid* specified.

passwd The encrypted password. If this field is empty (null) then no password will be demanded when a client logs in; i.e. the **USER** command does not need to be followed by a **PASS** command.

adminwd The encrypted password for this user to gain administrative privileges. If this field is empty (null) then the user is not permitted to have administrative privileges.

EXAMPLE

The following is a sample hosts.hfaxd file. Note that the first entry that matches is taken, so more-specific entries should be placed first.

```
^pb@[^.]*\.cl\.cam\.ac\.uk$:::hFy8zXq2KaG8s
                        # pb on a machine directly in cl.cam.ac.uk can
                        # administer if an admin pw is given
127.0.0.1               # anyone on local host uses the default uid
^sam@flake.*sgi\.com$   # Sam on his work machine
^sam@oxford.*Berkeley.*# Sam on any machine starting oxford and containing
                        # Berkeley, e.g. sam@oxfordberkeley.cl.cam.ac.uk
^.*@.*.\.esd\.          # anyone in an esd domain
!^tom@                  # Tom Davis is denied access
.*\.sgi\.com$           # but anyone else at sgi is ok
```

SEE ALSO

sendfax(1), *hfaxd*(8C), *hylafax-server*(5F)