NAME

access.conf − the login access control table file

DESCRIPTION

The /etc/security/access.conf file specifies (*user/group*, *host*), (*user/group*, *network/netmask*), (*user/group*, *tty*), (*user/group*, *X−$DISPLAY−value*), or (*user/group*, *pam−service−name*) combinations for which a login will be either accepted or refused.

When someone logs in, the file access.conf is scanned for the first entry that matches the (*user/group*, *host*) or (*user/group*, *network/netmask*) combination, or, in case of non−networked logins, the first entry that matches the (*user/group*, *tty*) combination, or in the case of non−networked logins without a tty, the first entry that matches the (*user/group*, *X−$DISPLAY−value*) or (*user/group*, *pam−service−name/*) combination. The permissions field of that table entry determines whether the login will be accepted or refused.

Each line of the login access control table has three fields separated by a ":" character (colon):

permission:*users/groups*:*origins*

The first field, the *permission* field, can be either a "+" character (plus) for access granted or a "−" character (minus) for access denied.

The second field, the *users/group* field, should be a list of one or more login names, group names, or *ALL* (which always matches). To differentiate user entries from group entries, group entries should be written with brackets, e.g. *(group)*.

The third field, the *origins* field, should be a list of one or more tty names (for non−networked logins), X *$DISPLAY* values or PAM service names (for non−networked logins without a tty), host names, domain names (begin with "."), host addresses, internet network numbers (end with "."), internet network addresses with network mask (where network mask can be a decimal number or an internet address also), *ALL* (which always matches) or *LOCAL*. The *LOCAL* keyword matches if and only if **pam_get_item**(3), when called with an *item_type* of *PAM_RHOST*, returns NULL or an empty string (and therefore the *origins* field is compared against the return value of **pam_get_item**(3) called with an *item_type* of *PAM_TTY* or, absent that, *PAM_SERVICE*).

If supported by the system you can use *@netgroupname* in host or user patterns. The *@@netgroupname* syntax is supported in the user pattern only and it makes the local system hostname to be passed to the netgroup match call in addition to the user name. This might not work correctly on some libc implementations causing the match to always fail.

The *EXCEPT* operator makes it possible to write very compact rules.

If the **nodefgroup** is not set, the group file is searched when a name does not match that of the logged−in user. Only groups are matched in which users are explicitly listed. However the PAM module does not look at the primary group id of a user.

The "#" character at start of line (no space at front) can be used to mark this line as a comment line.

EXAMPLES

These are some example lines which might be specified in /etc/security/access.conf.

User *root* should be allowed to get access via *cron*, X11 terminal *:0*, *tty1*, ..., *tty5*, *tty6*.

+:root:crond :0 tty1 tty2 tty3 tty4 tty5 tty6

User *root* should be allowed to get access from hosts which own the IPv4 addresses. This does not mean that the connection have to be a IPv4 one, a IPv6 connection from a host with one of this IPv4 addresses does work, too.

+:root:192.168.200.1 192.168.200.4 192.168.200.9

+:root:127.0.0.1

User *root* should get access from network 192.168.201. where the term will be evaluated by string matching. But it might be better to use network/netmask instead. The same meaning of 192.168.201. is

192.168.201.0/24 or *192.168.201.0/255.255.255.0*.

+:root:192.168.201.

User *root* should be able to have access from hosts *foo1.bar.org* and *foo2.bar.org* (uses string matching also).

+:root:foo1.bar.org foo2.bar.org

User *root* should be able to have access from domain *foo.bar.org* (uses string matching also).

+:root:.foo.bar.org

User *root* should be denied to get access from all other sources.

−:root:ALL

User *foo* and members of netgroup *admins* should be allowed to get access from all sources. This will only work if netgroup service is available.

+:@admins foo:ALL

User *john* and *foo* should get access from IPv6 host address.

+:john foo:2001:db8:0:101::1

User *john* should get access from IPv6 net/mask.

+:john:2001:db8:0:101::/64

Disallow console logins to all but the shutdown, sync and all other accounts, which are a member of the wheel group.

−:ALL EXCEPT (wheel) shutdown sync:LOCAL

All other users should be denied to get access from all sources.

−:ALL:ALL

NOTES

The default separators of list items in a field are space, ',', and tabulator characters. Thus conveniently if spaces are put at the beginning and the end of the fields they are ignored. However if the list separator is changed with the *listsep* option, the spaces will become part of the actual item and the line will be most probably ignored. For this reason, it is not recommended to put spaces around the ':' characters.

SEE ALSO

pam_access(8), **pam.d**(5), **pam**(7)

AUTHORS

Original **login.access**(5) manual was provided by Guido van Rooij which was renamed to **access.conf**(5) to reflect relation to default config file.

Network address / netmask description and example text was introduced by Mike Becher <mike.becher@lrz−muenchen.de>.