NAME

sudo − execute a command as another user

SYNOPSIS

sudo −V | **−h** | **−l** | **−L** | **−v** | **−k** | **−K** | **−s** | [**−H**] [**−P**] [**−S**] [**−b**] | [**−p** *prompt*] [**−c** *class*|−] [**−a** *auth_type*] [**−u** *username*|*#uid*] *command*

DESCRIPTION

sudo allows a permitted user to execute a *command* as the superuser or another user, as specified in the *sudoers* file. The real and effective uid and gid are set to match those of the target user as specified in the passwd file (the group vector is also initialized when the target user is not root). By default, **sudo** requires that users authenticate themselves with a password (NOTE: by default this is the user's password, not the root password). Once a user has been authenticated, a timestamp is updated and the user may then use sudo without a password for a short period of time (5 minutes unless overridden in *sudoers*).

sudo determines who is an authorized user by consulting the file */etc/sudoers*. By giving **sudo** the **−v** flag a user can update the time stamp without running a *command.* The password prompt itself will also time out if the user's password is not entered within 5 minutes (unless overridden via *sudoers*).

If a user who is not listed in the *sudoers* file tries to run a command via **sudo**, mail is sent to the proper authorities, as defined at configure time or the *sudoers* file (defaults to root). Note that the mail will not be sent if an unauthorized user tries to run sudo with the **−l** or **−v** flags. This allows users to determine for themselves whether or not they are allowed to use **sudo**.

sudo can log both successful and unsuccessful attempts (as well as errors) to *syslog* (3), a log file, or both. By default **sudo** will log via *syslog* (3) but this is changeable at configure time or via the *sudoers* file.

OPTIONS

sudo accepts the following command line options:

−V The **−V** (*version*) option causes **sudo** to print the version number and exit. If the invoking user is already root the **−V** option will print out a list of the defaults **sudo** was compiled with as well as the machine's local network addresses.

−l The **−l** (*list*) option will list out the allowed (and forbidden) commands for the user on the current host.

−L The **−L** (*list* defaults) option will list out the parameters that may be set in a *Defaults* line along with a short description for each. This option is useful in conjunction with *grep* (1).

−h The **−h** (*help*) option causes **sudo** to print a usage message and exit.

−v If given the **−v** (*validate*) option, **sudo** will update the user's timestamp, prompting for the user's password if necessary. This extends the **sudo** timeout for another 5 minutes (or whatever the timeout is set to in *sudoers*) but does not run a command.

−k The **−k** (*kill*) option to **sudo** invalidates the user's timestamp by setting the time on it to the epoch. The next time **sudo** is run a password will be required. This option does not require a password and was added to allow a user to revoke **sudo** permissions from a .logout file.

−K The **−K** (sure *kill*) option to **sudo** removes the user's timestamp entirely. Likewise, this option does not require a password.

−b The **−b** (*background*) option tells **sudo** to run the given command in the background. Note that if you use the **−b** option you cannot use shell job control to manipulate the process.

−p The **−p** (*prompt*) option allows you to override the default password prompt and use a custom one. The following percent ('%') escapes are supported:

- %u expanded to the invoking user's login name
- %U expanded to the login name of the user the command will be run as (defaults to root)
- %h expanded to the local hostname without the domain name
- %H expanded to the local hostname including the domain name (on if the machine's hostname is fully qualified or the *fqdn* sudoers option is set)

%% two consecutive % characters are collaped into a single % character

−c The **−c** (*class*) option causes **sudo** to run the specified command with resources limited by the specified login class. The *class* argument can be either a class name as defined in /etc/login.conf, or a single '−' character. Specifying a *class* of − indicates that the command should be run restricted by the default login capabilities for the user the command is run as. If the *class* argument specifies an existing user class, the command must be run as root, or the **sudo** command must be run from a shell that is already root. This option is only available on systems with BSD login classes where **sudo** has been configured with the −−with−logincap option.

−a The **−a** (*authentication type*) option causes **sudo** to use the specified authentication type when validating the user, as allowed by /etc/login.conf. The system administrator may specify a list of sudo-specific authentication methods by adding an ''auth−sudo'' entry in /etc/login.conf. This option is only available on systems that support BSD authentication where **sudo** has been configured with the −−with−bsdauth option.

−u The **−u** (*user*) option causes **sudo** to run the specified command as a user other than *root*. To specify a *uid* instead of a *username*, use *#uid*.

−s The **−s** (*shell*) option runs the shell specified by the *SHELL* environment variable if it is set or the shell as specified in *passwd* (5).

−H The **−H** (*HOME*) option sets the HOME environment variable to the homedir of the target user (root by default) as specified in *passwd* (5). By default, **sudo** does not modify HOME.

−P The **−P** (*preserve group vector*) option causes **sudo** to preserve the user's group vector unaltered. By default, **sudo** will initialize the group vector to the list of groups the target user is in. The real and effective group IDs, however, are still set to match the target user.

−S The **−S** (*stdin*) option causes **sudo** to read the password from standard input instead of the terminal device.

−− The −− flag indicates that **sudo** should stop processing command line arguments. It is most useful in conjunction with the **−s** flag.

RETURN VALUES

Upon successful execution of a program, the return value from **sudo** will simply be the return value of the program that was executed.

Otherwise, **sudo** quits with an exit value of 1 if there is a configuration/permission problem or if **sudo** cannot execute the given command. In the latter case the error string is printed to stderr. If **sudo** cannot *stat* (2) one or more entries in the user's PATH an error is printed on stderr. (If the directory does not exist or if it is not really a directory, the entry is ignored and no error is printed.) This should not happen under normal circumstances. The most common reason for *stat* (2) to return ''permission denied'' is if you are running an automounter and one of the directories in your PATH is on a machine that is currently unreachable.

SECURITY NOTES

sudo tries to be safe when executing external commands. Variables that control how dynamic loading and binding is done can be used to subvert the program that **sudo** runs. To combat this the LD_*, _RLD_*, SHLIB_PATH (HP−UX only), and LIBPATH (AIX only) environment variables are removed from the environment passed on to all commands executed. **sudo** will also remove the IFS, ENV, BASH_ENV, KRB_CONF, KRBCONFDIR, KRBTKFILE, KRB5_CONFIG, LOCALDOMAIN, RES_OPTIONS, HOSTALIASES, NLSPATH, PATH_LOCALE, TERMINFO, TERMINFO_DIRS and TERMPATH variables as they too can pose a threat. If the TERMCAP variable is set and is a pathname, it too is ignored. Additionally, if the LC_* or LANGUAGE variables contain the / or % characters, they are ignored. If **sudo** has been compiled with SecurID support, the VAR_ACE, USR_ACE and DLC_ACE variables are cleared as well. The list of environment variables that **sudo** clears is contained in the output of sudo −V when run as root.

To prevent command spoofing, **sudo** checks ''.'' and "" (both denoting current directory) last when searching for a command in the user's PATH (if one or both are in the PATH). Note, however, that the actual PATH environment variable is *not* modified and is passed unchanged to the program that **sudo** executes.

For security reasons, if your OS supports shared libraries and does not disable user-defined library search paths for setuid programs (most do), you should either use a linker option that disables this behavior or link **sudo** statically.

sudo will check the ownership of its timestamp directory (*/var/run/sudo* by default) and ignore the directory's contents if it is not owned by root and only writable by root. On systems that allow non-root users to give away files via *chown* (2), if the timestamp directory is located in a directory writable by anyone (e.g.: */tmp*), it is possible for a user to create the timestamp directory before **sudo** is run. However, because **sudo** checks the ownership and mode of the directory and its contents, the only damage that can be done is to ''hide'' files by putting them in the timestamp dir. This is unlikely to happen since once the timestamp dir is owned by root and inaccessible by any other user the user placing files there would be unable to get them back out. To get around this issue you can use a directory that is not world-writable for the timestamps (*/var/adm/sudo* for instance) or create */var/run/sudo* with the appropriate owner (root) and permissions (0700) in the system startup files.

sudo will not honor timestamps set far in the future. Timestamps with a date greater than current_time + 2 * `TIMEOUT` will be ignored and sudo will log and complain. This is done to keep a user from creating his/her own timestamp with a bogus date on systems that allow users to give away files.

Please note that **sudo** will only log the command it explicitly runs. If a user runs a command such as `sudo su` or `sudo sh`, subsequent commands run from that shell will *not* be logged, nor will **sudo**'s access control affect them. The same is true for commands that offer shell escapes (including most editors). Because of this, care must be taken when giving users access to commands via **sudo** to verify that the command does not inadvertently give the user an effective root shell.

EXAMPLES

Note: the following examples assume suitable *sudoers* (5) entries.

To get a file listing of an unreadable directory:

```
% sudo ls /usr/local/protected
```

To list the home directory of user yazza on a machine where the filesystem holding ~yazza is not exported as root:

```
% sudo -u yazza ls ~yazza
```

To edit the *index.html* file as user www:

```
% sudo -u www vi ~www/htdocs/index.html
```

To shutdown a machine:

```
% sudo shutdown -r +15 "quick reboot"
```

To make a usage listing of the directories in the /home partition. Note that this runs the commands in a subshell to make the `cd` and file redirection work.

```
% sudo sh -c "cd /home ; du -s * | sort -rn > USAGE"
```

ENVIRONMENT

sudo utilizes the following environment variables:

PATH	Set to a sane value if SECURE_PATH is set
SHELL	Used to determine shell to run with -s option
USER	Set to the target user (root unless the -u option is specified)
HOME	In -s or -H mode (or if sudo was configured with the --enable-shell-sets-home option), set to homedir of the target user.
SUDO_PROMPT	Used as the default password prompt
SUDO_COMMAND	Set to the command run by sudo
SUDO_USER	Set to the login of the user who invoked sudo
SUDO_UID	Set to the uid of the user who invoked sudo
SUDO_GID	Set to the gid of the user who invoked sudo
SUDO_PS1	If set, PS1 will be set to its value

FILES

/etc/sudoers	List of who can run what
/var/run/sudo	Directory containing timestamps

AUTHORS

Many people have worked on **sudo** over the years; this version consists of code written primarily by:

Todd Miller
Chris Jepeway

See the HISTORY file in the **sudo** distribution or visit http://www.sudo.ws/sudo/history.html for a short history of **sudo**.

BUGS

If you feel you have found a bug in sudo, please submit a bug report at http://www.sudo.ws/sudo/bugs/

DISCLAIMER

Sudo is provided ''AS IS'' and any express or implied warranties, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed. See the LICENSE file distributed with **sudo** for complete details.

CAVEATS

There is no easy way to prevent a user from gaining a root shell if that user has access to commands allowing shell escapes.

If users have sudo ALL there is nothing to prevent them from creating their own program that gives them a root shell regardless of any '!' elements in the user specification.

Running shell scripts via **sudo** can expose the same kernel bugs that make setuid shell scripts unsafe on some operating systems (if your OS supports the /dev/fd/ directory, setuid shell scripts are generally safe).

SEE ALSO

grep (1), *su* (1), *stat* (2), *login_cap* (3), *sudoers* (5), *passwd* (5), *visudo* (8)