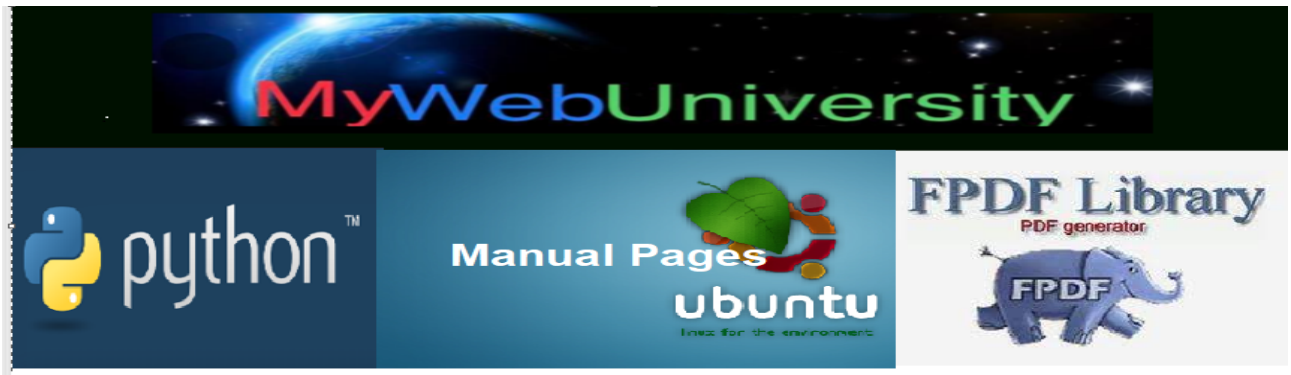

Full credit is given to the above companies including the OS that this PDF file was generated!

Linux Ubuntu 26.04 Manual Pages on command 'run0.1'

$ man run0.1

RUN0(1) run0 RUN0(1)

NAME

run0 - Elevate privileges

SYNOPSIS

run0 [OPTIONS...] [COMMAND...]

DESCRIPTION

run0 may be used to temporarily and interactively acquire elevated or different privileges.

It serves a similar purpose as sudo(8), but operates differently in a couple of key areas:

? No execution or security context credentials are inherited from the caller into the invoked commands, as they are invoked from a fresh, isolated service forked off by the service manager.

? Authentication takes place via polkit[1], thus isolating the authentication prompt from the terminal (if possible).

? An independent pseudo-tty is allocated for the invoked command, detaching its lifecycle and isolating it for security.

? No SetUID/SetGID file access bit functionality is used for the implementation.

Altogether this should provide a safer and more robust alternative to the sudo mechanism, in particular in OS environments where SetUID/SetGID support is not available (for example by setting the NoNewPrivileges= variable in systemd-system.conf(5)).

Any session invoked via run0 will run through the "systemd-run0" PAM stack.

Note that run0 is implemented as an alternative multi-call invocation of systemd-run(1).

That is, run0 is a symbolic link to systemd-run executable file, and it behaves as run0 if it is invoked through the symbolic link, otherwise behaves as systemd-run.

OPTIONS

The following options are understood:

--unit=

Use this unit name instead of an automatically generated one.

Added in version 256.

--property=

Sets a property of the service unit that is created. This option takes an assignment in the same format as systemctl(1)'s set-property command.

Added in version 256.

--description=

Provide a description for the service unit that is invoked. If not specified, the command itself will be used as a description. See Description= in systemd.unit(5).

Added in version 256.

--slice=

Make the new .service unit part of the specified slice, instead of user.slice.

Added in version 256.

--slice-inherit

Make the new .service unit part of the slice the run0 itself has been invoked in. This option may be combined with --slice=, in which case the slice specified via --slice= is placed within the slice the run0 command is invoked in.

Example: consider run0 being invoked in the slice foo.slice, and the --slice= argument is bar. The unit will then be placed under foo-bar.slice.

Added in version 256.

--user=, -u, --group=, -g

Switches to the specified user/group. If not specified defaults to "root", unless --area= or --empower are used (see below), in which case this defaults to the invoking user.

Added in version 256.

--nice=

Runs the invoked session with the specified nice level.

Added in version 256.

--chdir=, -D

Runs the invoked session with the specified working directory. If not specified defaults

to the client's current working directory if switching to the root user, or the target user's home directory otherwise.

Added in version 256.

--via-shell

Invokes the target user's login shell and runs the specified command (if any) via it.

Added in version 258.

-i

Shortcut for --via-shell --chdir='~'.

Added in version 258.

--setenv=NAME[=VALUE]

Runs the invoked session with the specified environment variable set. This parameter may be used more than once to set multiple variables. When "=" and VALUE are omitted, the value of the variable with the same name in the invoking environment will be used.

Added in version 256.

--background=COLOR

Change the terminal background color to the specified ANSI color as long as the session lasts. If not specified, the background will be tinted in a reddish tone when operating as root, and in a yellowish tone when operating under another UID, as reminder of the changed privileges. The color specified should be an ANSI X3.64 SGR background color, i.e. strings such as "40", "41", ..., "47", "48;2;...", "48;5;...". See ANSI Escape Code (Wikipedia)[2] for details. Set to an empty string to disable.

Example: "--background=44" for a blue background.

Added in version 256.

--pty, --pty-late, --pipe

Request allocation of a pseudo TTY for the run0 session (in case of --pty or --pty-late), or request passing the caller's STDIO file descriptors directly through (in case of --pipe). --pty-late is very similar to --pty but begins the TTY processing only once unit startup is complete, leaving input to any passwords/polkit agents until that time. If neither switch is specified, or if both --pipe and one of --pty/--pty-late are specified, the mode will be picked automatically: if standard input, standard output, and standard error output are all connected to a TTY then a pseudo TTY is allocated (in --pty-late mode unless --no-ask-password is specified in which case --pty is selected), otherwise the relevant file descriptors are passed through directly.

--pty and --pipe were added in v257.

--pty-late was added in v258.

--shell-prompt-prefix=STRING

Set a shell prompt prefix string. This ultimately controls the $SHELL_PROMPT_PREFIX environment variable for the invoked program, which is typically imported into the shell prompt. By default ? if emojis are supported ?, a superhero emoji is shown (?). This default may also be changed (or turned off) by passing the $SYSTEMD_RUN_SHELL_PROMPT_PREFIX environment variable to run0, see below. Set to an empty string to disable shell prompt prefixing.

Added in version 257.

--lightweight=BOOLEAN

Controls whether to activate the per-user service manager for the target user. By default if the target user is "root" or a system user the per-user service manager is not activated as effect of the run0 invocation, otherwise it is.

This ultimately controls the $XDG_SESSION_CLASS environment variable pam_systemd(8) respects.

Added in version 258.

--area=AREA

Controls the "area" of the target account to log into. Areas are secondary home directories within the primary home directory of the target user, i.e. logging into area "foobar" of an account translates to $HOME being set to ~/Areas/foobar on login.

If this option is used, the default user to transition to changes from root to the calling user's (but --user= takes precedence, see above). Or in other words, just specifying an area without a user is a mechanism to create a new session of the calling user, just with a different area.

This ultimately controls the $XDG_AREA environment variable pam_systemd(8) respects.

For details on the area concept see pam_systemd_home(8).

Added in version 258.

--empower

If specified, run0 will elevate the privileges of the selected user (using --user=) or the current user if no user is explicitly selected. Currently this means we give the invoked process all available capabilities and add the "empower" group as a supplemental group (for which all polkit actions are allowed by default), but other privileges may be

granted in the future as well when using this option.

Note that other (unprivileged) processes of the selected user will have privileges over the invoked process. Consider not using this option in an environment where there might be malicious processes running as the selected user.

Added in version 259.

--same-root-dir

Execute the run0 session in the same root directory that the run0 command is executed in.

Added in version 259.

--machine=

Execute operation in a local container. Specify a container name to connect to.

Added in version 256.

--no-ask-password

Do not query the user for authentication for privileged operations.

-h, --help

Print a short help text and exit.

--version

Print a short version string and exit.

All command line arguments after the first non-option argument become part of the command line of the launched process. If no command line is specified an interactive shell is invoked. The shell to invoke may be controlled through --via-shell - when specified the target user's shell is used - or --setenv=SHELL=.... By default, the originating user's shell is executed if operating locally, or /bin/sh when operating with --machine=.

Note that unlike sudo, run0 always spawns shells with login shell semantics, regardless of -i.

EXIT STATUS

On success, 0 is returned. If run0 failed to start the session or the specified command fails, a non-zero return value will be returned.

ENVIRONMENT VARIABLES

As with systemd-run, the session will inherit the system environment from the service manager. In addition, the following environment variables will be set:

$TERM

Copied from the $TERM of the caller. Can be overridden with --setenv=

Added in version 256.

$SUDO_USER

Set to the username of the originating user.

Added in version 256.

$SUDO_UID

Set to the numeric UNIX user id of the originating user.

Added in version 256.

$SUDO_GID

Set to the primary numeric UNIX group id of the originating session.

Added in version 256.

$SHELL_PROMPT_PREFIX

By default, set to the superhero emoji (if supported), but may be overridden with the $SYSTEMD_RUN_SHELL_PROMPT_PREFIX environment variable (see below), or the --shell-prompt-prefix= switch (see above).

Added in version 257.

The following variables may be passed to run0:

$SYSTEMD_RUN_SHELL_PROMPT_PREFIX

If set, overrides the default shell prompt prefix that run0 sets for the invoked shell (the superhero emoji). Set to an empty string to disable shell prompt prefixing.

Added in version 257.

SEE ALSO

systemd(1), systemd-run(1), sudo(8), machinectl(1), pam_systemd(8)

NOTES

1. polkit

   https://www.freedesktop.org/wiki/Software/polkit

2. ANSI Escape Code (Wikipedia)

   https://en.wikipedia.org/wiki/ANSI_escape_code#SGR_(Select_Graphic_Rendition)_parameters