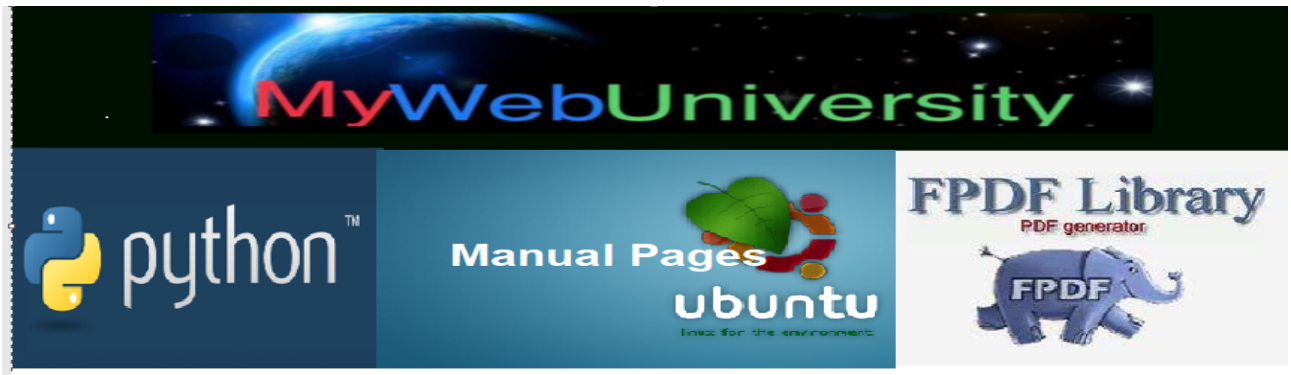

Full credit is given to the above companies including the OS that this PDF file was generated!

Linux Ubuntu 26.04 Manual Pages on command 'aa-exec.1'

$ man aa-exec.1

AA-EXEC(1) AppArmor AA-EXEC(1)

NAME

aa-exec - confine a program with the specified AppArmor profile

SYNOPSIS

aa-exec [options] [--] [<command> ...]

DESCRIPTION

aa-exec is used to launch a program confined by the specified profile and or namespace. If both a profile and namespace are specified command will be confined by profile in the new policy namespace. If only a namespace is specified, the profile name of the current confinement will be used. If neither a profile or namespace is specified command will be run using standard profile attachment (ie. as if run without the aa-exec command).

If the arguments are to be pasted to the <command> being invoked by aa-exec then -- should be used to separate aa-exec arguments from the command.

aa-exec -p profile1 -- ls -l

OPTIONS aa-exec accepts the following arguments:

-p PROFILE, --profile=PROFILE

confine <command> with PROFILE. If the PROFILE is not specified use the current profile name (likely unconfined).

-n NAMESPACE, --namespace=NAMESPACE

use profiles in NAMESPACE. This will result in confinement transitioning to using the new profile namespace.

-i, --immediate

transition to PROFILE before doing executing <command>. This subjects the running of

<command> to the exec transition rules of the current profile.

-v, --verbose

show commands being performed

-d, --debug

show commands and error codes

-- Signal the end of options and disables further option processing. Any arguments after the -- are treated as arguments of the command. This is useful when passing arguments to the <command> being invoked by aa-exec.

RESTRICTIONS

aa-exec uses aa_change_profile(3) to change application confinement. The use of aa_change_profile(3) may be restricted by policy in ways that will cause failure or results different than expected.

Even when using aa-exec from unconfined restrictions in policy can causes failure or the confinement entered to be different than requested

See the unpriviled unconfined restriction documentation for more detail.

https://gitlab.com/apparmor/apparmor/-/wikis/unprivileged_unconfined_restriction

STACKING

aa-exec can be used to setup a stack of profiles as confinement. When an application is confined by a stack, all profiles in the stack are checked as if they were the profile confining the application. The resulting mediation is the intersection of what is allowed by each profile in the stack.

The profiles in a stack are treated independently. Each profile can have its own flags and profile transitions. During an exec each profile gets to specify its transition and the results brought together to form a new canonicalized stack.

The profile separator indicating a stack is the character sequence //&. Thus a stack can be expressed using

```
$ aa-exec -p "unconfined//&firefox" -- bash
$ ps -Z
LABEL                          PID TTY          TIME CMD
unconfined                   30714 pts/12   00:00:00 bash
firefox//&unconfined (unconfined) 31160 pts/12   00:00:00 bash
firefox//&unconfined (unconfined) 31171 pts/12   00:00:00 ps
```

NAMESPACES

aa-exec can be used to enter confinement in another policy namespace if the policy namespaces exists, is visible, and the profile exists in the namespace. Note applications launched within the namespace will not be able to exit the namespace, and may be restricted by additional confinement around namespacing. Files and resources visible to the parent that launches the application may not be visible in the policy namespace resulting in access denials.

To enter a policy namespace the profile is prefixed with the namespace's name, using a : prefix and suffix.

Eg.

```
$ aa-exec -p :ex1:unconfined -- bash
$ ps -Z
LABEL                          PID TTY          TIME CMD
-                            30714 pts/12   00:00:00 bash
unconfined                   34372 pts/12   00:00:00 bash
unconfined                   34379 pts/12   00:00:00 ps
```

Confinement of processes outside of the namespace may not be visible in which case the confinement will be represented with a -. If policy is stacked only part of the confinement might be visible. However confinement is usually fully visible from the parent policy namespace.

Eg. the confinement of the child can be queried in the parent to see

```
$ ps -Z 34372
LABEL                          PID TTY      STAT   TIME COMMAND
:ex1:unconfined                 34372 pts/12   S+     0:00 bash
```

And in the case of stacking with namespaces

```
$ aa-exec -p "unconfined//&:ex1:unconfined" -- bash
$ ps -Z
LABEL                          PID TTY          TIME CMD
-                            30714 pts/12   00:00:00 bash
unconfined                   36298 pts/12   00:00:00 bash
unconfined                   36305 pts/12   00:00:00 ps
```

while from the parent namespace the full confinement can be seen

```
$ ps -Z 36298
LABEL                          PID TTY      STAT   TIME COMMAND
```

unconfined//&:ex1:unconfined 36298 pts/12 S+ 0:00 bash

BUGS

If you find any bugs, please report them at <https://gitlab.com/apparmor/apparmor/-/issues>

SEE ALSO

apparmor(7), apparmor.d(5), aa_change_profile(3), aa_change_onexec(3) and <https://wiki.apparmor.net>.