gentoo linux (/) **Wiki**

AppArmor

From Gentoo Wiki

AppArmor is a MAC (Mandatory Access Control) system, implemented upon LSM (Linux Security Modules).

Resources
Home (http://wiki.apparmor.net)
Wikipedia (https://en.wikipedia.org/wiki/AppArmor)
GitWeb (http://bazaar.launchpad.net/~apparmor-dev/apparmor/master/files)
`#apparmor` (https://webchat.freenode.net/?channels=apparmor)

Contents

Installation

Kernel

While the Linux kernel has supported AppArmor for quite some time, some recent changes have been made that make working with AppArmor profiles much more user friendly. It is therefore highly recommended to use >=sys-kernel/hardened-sources (https://packages.gentoo.org/packages/sys-kernel/hardened-sources)-3.10 or any other kernel >=3.12.

Activate the following kernel options:

KERNEL

```
Security options  --->
    [*] Enable different security models
    [*] AppArmor support
    (1)   AppArmor boot parameter default value
    [*]   Enable AppArmor 2.4 compatability
          Default security module (AppArmor)  --->
```

Note that the *Enable AppArmor 2.4 compatability* option is only required with hardened-sources before 3.12

Emerge

Install the userspace tools. It contains the profile parser and init script:

```
root # emerge --ask                    (https://packages.gentoo.org/packages/sys-apps/apparmor)
```

Emerging the following package is recommended, but not required. This package contains additional userspace utilities to assist with profile management:

```
root # emerge --ask                        (https://packages.gentoo.org/packages/sys-apps/apparmor-utils)
```

Additional software

- sys-libs/libapparmor (https://packages.gentoo.org/packages/sys-libs/libapparmor) - The core library to support the userspace utilities
- sec-policy/apparmor-profiles (https://packages.gentoo.org/packages/sec-policy/apparmor-profiles) - A collection of pre-built profiles contributed by the AppArmor community

Configuration

Enabling AppArmor

If you did not select AppArmor as the default security module and set the boot parameter default value in the kernel configuration, you will need to enable AppArmor manually at boot time.

GRUB

FILE `/boot/grub/grub.conf` **Example GRUB config for AppArmor with simple kernel**

```
title=Gentoo with AppArmor
root (hd0,0)
kernel /vmlinuz root=/dev/sda2 apparmor=1 security=apparmor
```

GRUB 2

FILE `/etc/default/grub` **Enabling AppArmor with GRUB 2**

```
GRUB_CMDLINE_LINUX_DEFAULT="apparmor=1 security=apparmor"
```

Apply changes by running:

```
root # grub2-mkconfig -o /boot/grub2/grub.cfg
```

securityfs

securityfs is the filesystem used by Linux kernel security modules. The init script mounts it automatically if it is not already, but some may prefer to do it manually:

FILE `/etc/fstab` **securityfs entry for fstab**

```
none     /sys/kernel/security securityfs defaults           0      0
```

Services

OpenRC

Adding it to boot runlevel:

```
root # rc-update add apparmor boot
```

Working with profiles

Profiles are stored as simple text files in `/etc/apparmor.d`. They may take any name, and may be stored in subdirectories - you may organised them however it suits you.

```
root # ls /etc/apparmor.d
```

```
abstractions  program-chunks  usr.lib.apache2.mpm-prefork.apache2  usr.lib.dovecot.managesieve-login  usr.sbin.dovecot  usr.sbin.nsc
apache2.d     sbin.klogd      usr.lib.dovecot.deliver              usr.lib.dovecot.pop3               usr.sbin.identd   usr.sbin.ntp
bin.ping      sbin.syslog-ng  usr.lib.dovecot.dovecot-auth         usr.lib.dovecot.pop3-login         usr.sbin.lspci    usr.sbin.smb
disable       sbin.syslogd    usr.lib.dovecot.imap                 usr.sbin.avahi-daemon              usr.sbin.mdnsd    usr.sbin.smb
local         tunables        usr.lib.dovecot.imap-login           usr.sbin.dnsmasq                   usr.sbin.nmbd     usr.sbin.tra
```

Profiles are referred to by name, including any parent subdirectories if present.

Automatic control

The init script will automatically load all profiles located in your profile directory. Unless specifically specified otherwise, each profile will be loaded in enforce mode.

Manual control

To activate a profile, simply set it to enforce mode:

```
root # aa-enforce usr.sbin.dnsmasq
```

```
Setting /etc/apparmor.d/usr.sbin.dnsmasq to enforce mode.
```

Similarly, to deactivate a profile, simply set it to complain mode.

```
root # aa-complain usr.sbin.dnsmasq
```

```
Setting /etc/apparmor.d/usr.sbin.dnsmasq to complain mode.
```

The current status of your profiles may be viewed using `aa-status`:

```
root # aa-status
```

```
# aa-status
apparmor module is loaded.
6 profiles are loaded.
5 profiles are in enforce mode.
   /bin/ping
   /sbin/klogd
   /sbin/syslog-ng
   /usr/sbin/dnsmasq
   /usr/sbin/identd
1 profiles are in complain mode.
   /usr/sbin/lspci
1 processes have profiles defined.
1 processes are in enforce mode.
   /usr/sbin/dnsmasq (12905)
0 processes are in complain mode.
0 processes are unconfined but have a profile defined.
```


Categories (/wiki/Special:Categories):
Pages with syntax highlighting errors (/index.php?title=Category:Pages_with_syntax_highlighting_errors&action=edit&redlink=1)
Security (/wiki/Category:Security)

- This page was last modified on 10 December 2015, at 22:24.