

Es un MAC (Mandatory Access Control o sistema de control obligatorio de acceso). Es un módulo a nivel de núcleo, que preguntará a AppArmor antes de cada llamada del sistema para saber si un proceso está autorizado a realizar la operación que se solicita.

Su funcionamiento se basa en "**perfiles**" para cada programa que se desea controlar. El perfil depende de la ruta de instalación del programa y se guarda en /etc/apparmor.d/. Está compuesto por una lista de rutas y los permisos que tiene el programa para utilizar dichos recursos. Cada perfil se puede cargar bien en modo estricto (**enforcing**) o bien en modo relajado (**complaining**). El modo estricto aplica las reglas y registra el intento de violación, mientras que en el modo relajado sólo se registran pero no se bloquean

Para obtener más perfiles se pueden instalar los paquetes **apparmor-profiles** y **apparmor-profiles-extra**. En algunas distribuciones hay que instalar **apparmor-utils** para disponer de todos los comandos

Comandos

- **aa-status**: comprueba el estado de AppArmor. Muestra una lista de los perfiles cargados y si hay procesos que los estén utilizando
- **apparmor_parser**: carga perfiles. Con -r los recarga para actualizar cambio en el perfil.
- **aa-enforce**: Carga un perfil en modo enforce
- **aa-complain**: Carga un perfil en modo complain
- **aa-disable**: Deshabilita un perfil