Es un M.A.C. creado por la NSA y Red Hat.

Una aplicación supervisada por SELinux posee acceso únicamente a los recursos que están definidos en una política de seguridad. Los procesos, puertos, archivos y directorios está controlados por un contexto de seguridad que consta de tres campos obligatorios y uno opcional: **`user:role:type[:nivel]`**

Para el sistema de ficheros agregamos unas "etiquetas" adicionales que podremos modificar para definir el contexto necesario, podremos mostrarlo con la opción **`-Z`** de **`ls`**.

Ejemplo: **`system_u:object_r:file_t:s0 Fichero_ejemplo.txt`**

Tiene 2 modos de funcionamiento:

- Enforcing : Denegar todos los accesos no autorizados, según las políticas de seguridad.
- Permissive Permitir todos los accesos no autorizados, pero mostrar alertas sobre ellos.

Elementos del contexto de seguridad

- **Usuarios**: Por defecto es `unconfined_u`
- **Roles**: Un usuario de puede tener varios roles. Su significado estará definido en la política de seguridad. Por defecto los elementos tendrán el rol `object_r`
- **Tipos**: Los tipos son el factor principal para decidir si se puede acceder a los recursos. Suelen tener una `_t` al final
- **Nivel**: Se utiliza sólo con políticas avanzadas multi-nivel (MLS) o multi-categoría (MCS). Son extensiones que permiten un control aún más preciso mediante un etiquetado adicional con dos entidades: *sensibilidad* y *categoría*.

Algunos módulos de SELinux exportan opciones booleanas que se pueden ajustar para alterar el comportamiento del sistema. Son directivas que sólo pueden tener el valor de verdadero o falso. Conviene revisarla para estar seguros de que no entran en conflicto con otras configuraciones del sistema.

Comandos

- **selinux-activate**: Activa SELinux una vez que se han instalado los paquetes necesarios. Es equivalente a activarlo en las opciones del GRUB y actualizar su configuración.
- **sestatus**: Información sobre el estado actual de SELinux. Con `-v` muestra más detalles.
- **getenforce**: Nos indica en qué modo está operando, enforcing o permisivo
- **setenforce**: Cambia a enforcing (con el parámetro 1) o a permissive (0)
- **semanage**: Herramienta de gestión de las políticas y el contexto. Como primer parámetro le pasamos sobre qué vamos a trabajar (fcontext, user, login, module, port, interface, node, etc.)
- **getsebool**: Lista los valores de las políticas booleanas con -a, o el valor de una si le pasamos su nombre
- **setsebool**: Modifica una política booleana

Para instalarlo en Debian/Ubuntu se necesitan los paquetes `selinux-basics selinux-policy-default`