Manual de administrador

USBSecurity version 4.x.x

El control de los puertos USB es una necesidad recurrente cuando se tienen ordenadores a disposicion de usuarios. Bloquear los puertos no es factible cuendo se quieren establecer permisos de acceso a los mismos. Existen diversos programas de bloqueo, quizas tambien de control de acceso.

La idea es un sistema para controlar el acceso a los puertos USB, que sea administrable, que funcione desde un servidor centralizado y sea multiplataforma. USBSecurity es un conjunto de programas para gestionar el control de acceso a nivel de usuarios, dispositivos y ordenador. Es multiplataforma funciona en Linux y Windows e independiente de la arquitectura del procesador. Por defecto funciona en modo local pero con pocas configuraciones puede funcionar desde un servidor centralizado.

USBSecurity

Es un conjunto de programas para gestionar el control de acceso a los puertos USB. Esta compuesto por los siguientes programas:

- usbsecurity-server
- usbsecurity-monitor
- usbsecurity-gui

usbsecurity-server

Es el programa web que para administrar los permisos a los puertos. Por defecto funciona en modo local en la direccion 127.0.0.1 tras el puerto 8888. Para mas informacion ejecutar desde un terminal:

$ usbsecurity-server –h | --help

usbsecurity-monitor

Es el programa que monitorea los puertos USB. Por defecto funciona en modo local bloqueando los puertos como politica inicial. Por defecto los permisos son gestionados por usbsecurity-server pero puede configurarse para usar un tercero a traves de una API REST.

Para mas informacion ejecutar desde un terminal:

$ usbsecurity-monitor –h | --help

usbsecurity-gui

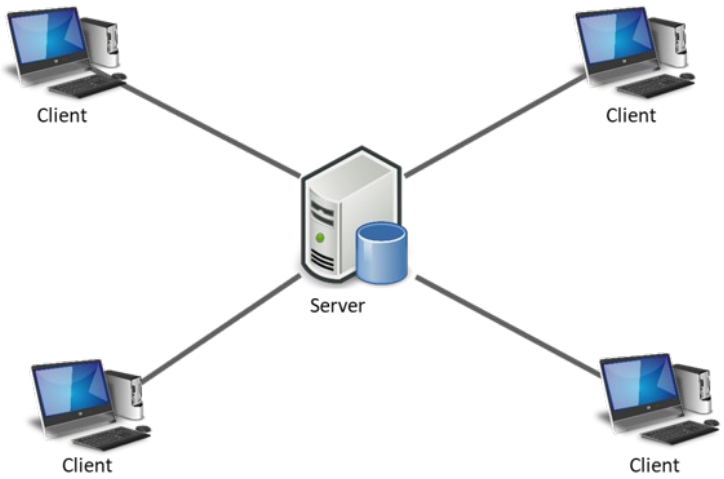
Es el programa que ofrece una interface grafica. Por defecto funciona en modo local conectado a la direccion 127.0.0.1 puerto 8888. Para mas informacion ejecutar desde un terminal:

$ usbsecurity-gui –h | --help

Servidor centralizado

USBSecurity funciona como una arquitectura cliente-servidor. De esta forma cada programa es un proceso independiente y se comunican entre si a traves de la capa de red.

Partiendo de este comportamiento nativo se ofrece la posibilidad de servir USBSecurity desde un servidor centralizado.



Configuracion

Suponiendo que el servicor corre en la red con las siguientes caracteristicas:

HOST: 192.168.1.1

PORT: 8888

Servidor

usbsecurity-server –host 192.168.1.1 –port 8888

Cliente

usbsecurity-monitor –host 192.168.1.1 –port 8888

usbsecurity-gui –host 192.168.1.1 –port 8888

Permisos de terceros

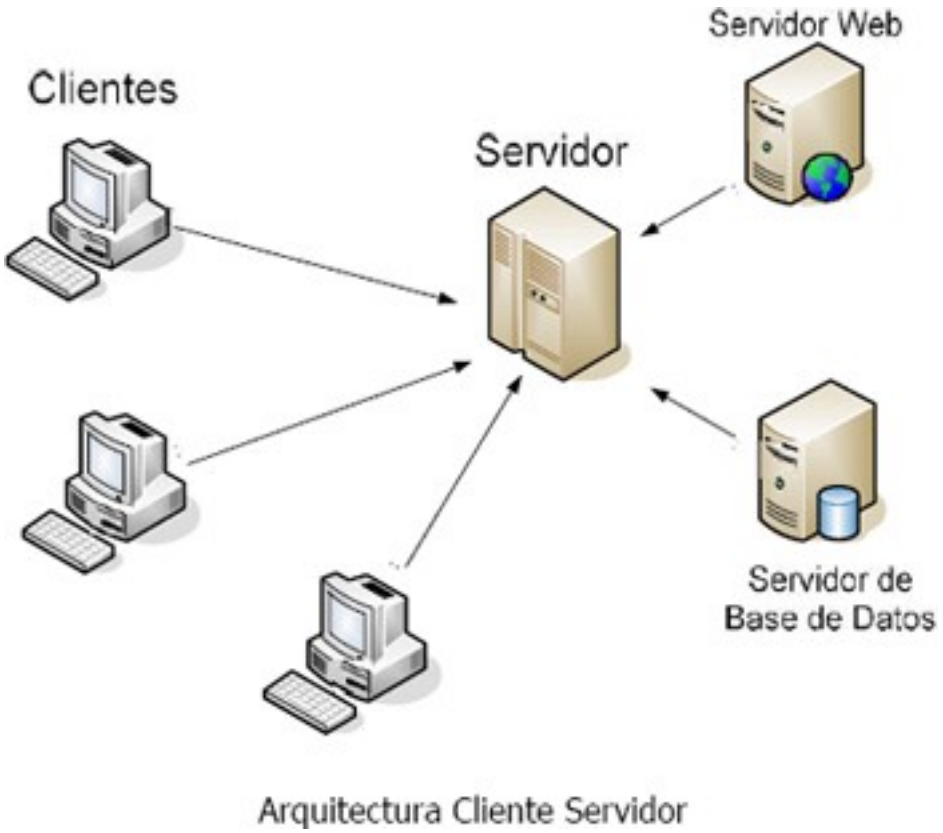
USBSecurity permite gestionar los permisos a partir de un tercero. La forma de comunicarse es a travez d eun API REST. La aplicación usbsecurity-monitor tiene un parametro –url-api para tal fin que debe esperar dos parameteros: ‘action’ y ‘id’.

Parametro ‘action’

En este parametro se pasa el evento ocurrido en el puerto USB.

Parametro ‘id’

En este parametro se pasa el id del dispositivo que desencadeno la accion.



Arquitectura Cliente Servidor

Configuracion

Suponiendo que el servicor corre en la red con las siguientes caracteristicas:

HOST: 192.168.1.1

PORT: 8888

y la api del servidor de terceros gestiona los permisos a traves de la siguiente URL:

URL: http://192.168.1.2:8889/api/action/{action}/{id}

Cliente

usbsecurity-monitor –host 192.168.1.1 –port 8888 –url-api http://192.168.1.2:8889/api/action/{action}/{id}

* Es necesario los parametros en la URL con las llaves: {parametro}.

Administracion

Por defecto USBSecurity se administra localmente desde el navegador y la URL http://127.0.0.1:888/admin. Con un servidor centralizado accede desde http[*s*]://*ip_servidor*:*puerto*/admin. Desde usbsecurity-gui puede acceder directamente.

Credenciales por defecto

Usuario: admin

Contraseña: usbsecurity

* Dado que el manual es publico y muestra las credenciales por defecto es re **recomendable cambiar la contraseña la primera vez que acceda**.

Opciones de administracion

La interface de administracion es intuitiva y flexible. Puede realizar las siguientes configuraciones:

- Crear cuentas de usuarios, colectivas o personales.
- Crear permisos por cuentas.
- Crear permisos por dispositivos.
- Crear permisos por ordenador.
- Crear permisos por cuentas y dispositivos.
- Crear permisos por ordenador y dispositivos.
- Ver y editar las sesiones de usuarios en los ordenadores.