Monitorización del sistema de archivos con systemd

Introducción

Uno de los aspectos más importantes de la seguridad informática de sistemas es la monitorización. Monitorizar es realizar una supervisión activa de un recurso, recopilando información de su uso y, si es el caso, tomando acciones en respuesta a eventos relacionados con el recurso.

Los sistemas de archivos almacenan la información de los usuarios y la empresa, por tanto serán elementos fundamentales a monitorizar. Pueden plantearse cuestiones como:

- ¿Quién ha accedido a determinado archivo o directorio?
- ¿En qué momento se ha producido el acceso?
- ¿De qué tipo ha sido el acceso? ¿Se ha borrado o modificado información?
- ¿Ha intentando acceder alguien a un recurso del sistema de archivos para el que no tiene autorización.
- Etc.

Las cuestiones anteriores son de suma importancia en al administración de sistemas, concretamente en el área de monitorización, la cual constituye una base necesaria para la auditoría de sistemas.

Monitorización del sistema de archivos con systemd

Utilizando los units de tipo **path** podemos implementar un sencillo y eficiente mecanismo de monitorización para el sistema de archivos.

El funcionamiento básico consiste en

- Definir el elemento del sistema de archivos a monitorizar, para ello definiremos una unit de tipo **path**
- Definir la respuesta o acción a llevar a cabo cuando se detecte algún evento sobre el elemento del sistema de archivos monitorizado. Lo normal en este caso será definir una unit de tipo **service**

Vamos a verlo mediante un ejemplo.

Supongamos que tengo un directorio, **/var/confidencial**, que me interesaría monitorizar para detectar cualquier tipo de acceso no autorizado al mismo. La idea es que si alguien accede e intenta modificar algún elemento, el administrador obtenga notificación del evento correspondiente.

Para implementarlo tendremos que definir

- Un **unit de tipo service** con la acción a tomar a cabo al detectar el evento
- Un **pequeño script** que será invocado por el service
- Un **unit de tipo path** que definirá el elemento del sistema de archivos a supervisar

Empecemos definiendo el service. Crearemos el archivo **/etc/systemd/system/monitorconfidencial.service**

```
[Unit]
Description= Inicia el registro de acceso a /var/confidencial
Documentation= man:systemd.service
[Service]
Type=oneshot
ExecStart=/usr/bin/monitorconfidencial.sh
```

Vamos a continuación con el script, que crearemos en **/usr/bin/monitorconfidencial.sh**

Es importante tener en cuenta las directivas de la sección Service

- **Type=oneshot** indica como se ejecutará el servicio, en este caso ejecuta el comando asociado y termina
- **ExecStart=/usr/bin/monitorconfidencial.sh** indica el script invocado por el servicio

El contenido será muy simple

```
#!/bin/bash
echo `date` 'Atención! Alguien ha modificado /var/confidencial!' >> /var/log/monitorconfidencial.log
```

El script simplemente escribe una línea en el archivo de log /**var**/**log**/**monitorconfidencial.log**, indicando la fecha y hora del evento.

Es importante conceder permiso de ejecución al script

```
chmod +x /usr/bin/monitorconfidencial.sh
```

Por último definimos el unit de tipo path para definir el elemento del sistema de archivos a supervisar

Definimos la unit en /**etc**/**systemd**/**system**/**monitorconfidencial.path**

```
[Unit]
Description= Lanza el servicio que supervisa /var/confidencial.
Documentation= man:systemd.path
[Path]
PathModified=/var/confidencial
[Install]
WantedBy=multi-user.target
```

La sección a tener en cuenta en este caso es **Path** que en este caso, mediante la directiva **PathModified** indica el elemento del sistema de archivos a supervisar, concretamente el directorio /**var**/**confidencial**

NOTA: Para vincular el service con el path, sin especificarlo explícitamente en la definición del path (mediante una directiva Unit en la sección Path), en este ejemplo utilizamos el mismo nombre para el service que para el path. De este modo vinculamos la acción a invocar, el service, cuando se produzca un evento supervisado por la unit del path.

Vamos a comprobar que funciona.

En primer lugar arrancamos el service de tipo path

```
systemctl start monitorconfidencial.path
```

Modificamos el directorio supervisado, creando un archivo en él:

```
touch /var/confidencial/archivo
```

Comprobamos que, efectivamente, se ha guardado registro del evento, para ello accedemos al archivo /**var**/**log**/**monitorconfidencial.log**, en el que se escribían el script que respondía a los eventos supervisados por la unit monitorconfidencial.path

```
cat /var/log/monitorconfidencial.log
```

Muestra:

```
mié nov 29 19:03:42 CET 2017 : Atención! Alguien ha modificado /var/confidencial!
```

Volver

JavierFP 17:44 11 dec 2017 (CET)