

3.12 Pi alert. ¿Intrusos en tu red?

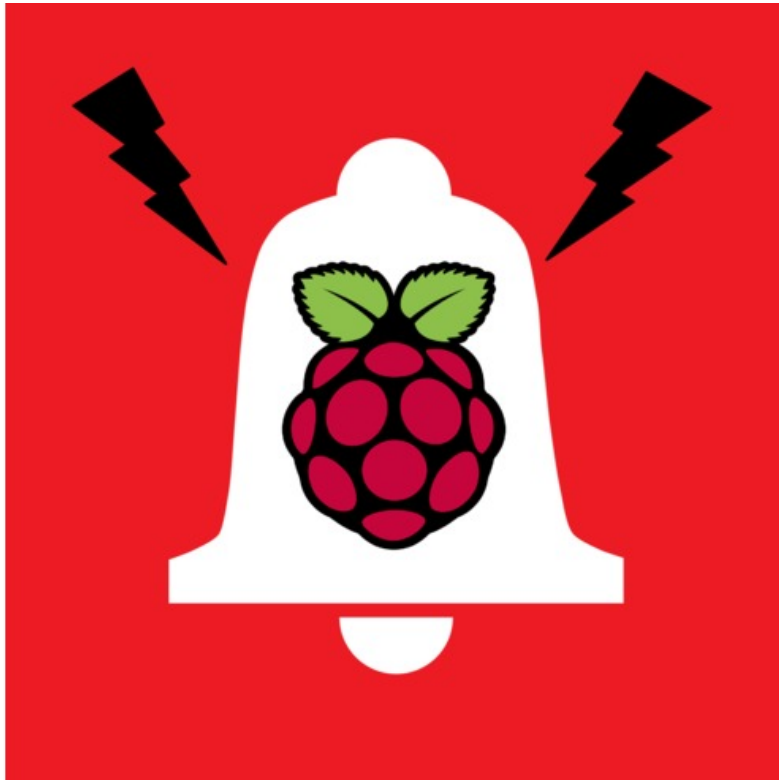


Imagen obtenida de <https://devpost.com/software/pialert>

Este proyecto lleva mas de 2 años sin ser actualizado

Esta herramienta sirve para...

detectar nuevos equipos conectados en nuestra red de modo que si aparece algún equipo nuevo del cuál no estamos al tanto detectaremos una conexión no permitida.

Web de proyecto y otros enlaces de interés

Repositorio de código original: <https://github.com/pucherot/Pi.Alert>

Imagen que utilizaremos: <https://registry.hub.docker.com/r/jokobsk/pi.alert>

Despliegue

Como en ocasiones anteriores vamos a hacer con docker-compose para ello accedemos al terminal y escribimos

```
cd $HOME  
mkdir pialert  
cd pialert  
nano docker-compose.yml
```

y dentro del fichero escribiremos el siguiente contenido

```
version: "3"  
services:  
  pialert:  
    image: jokobsk/pi.alert  
    ports:  
      - "20211:20211/tcp"  
    environment:  
      - TZ=Europe/Madrid  
    restart: unless-stopped  
    volumes:  
      - ./pialert_db:/home/pi/pialert/db  
      - ./config/pialert.conf:/home/pi/pialert/config/pialert.conf
```

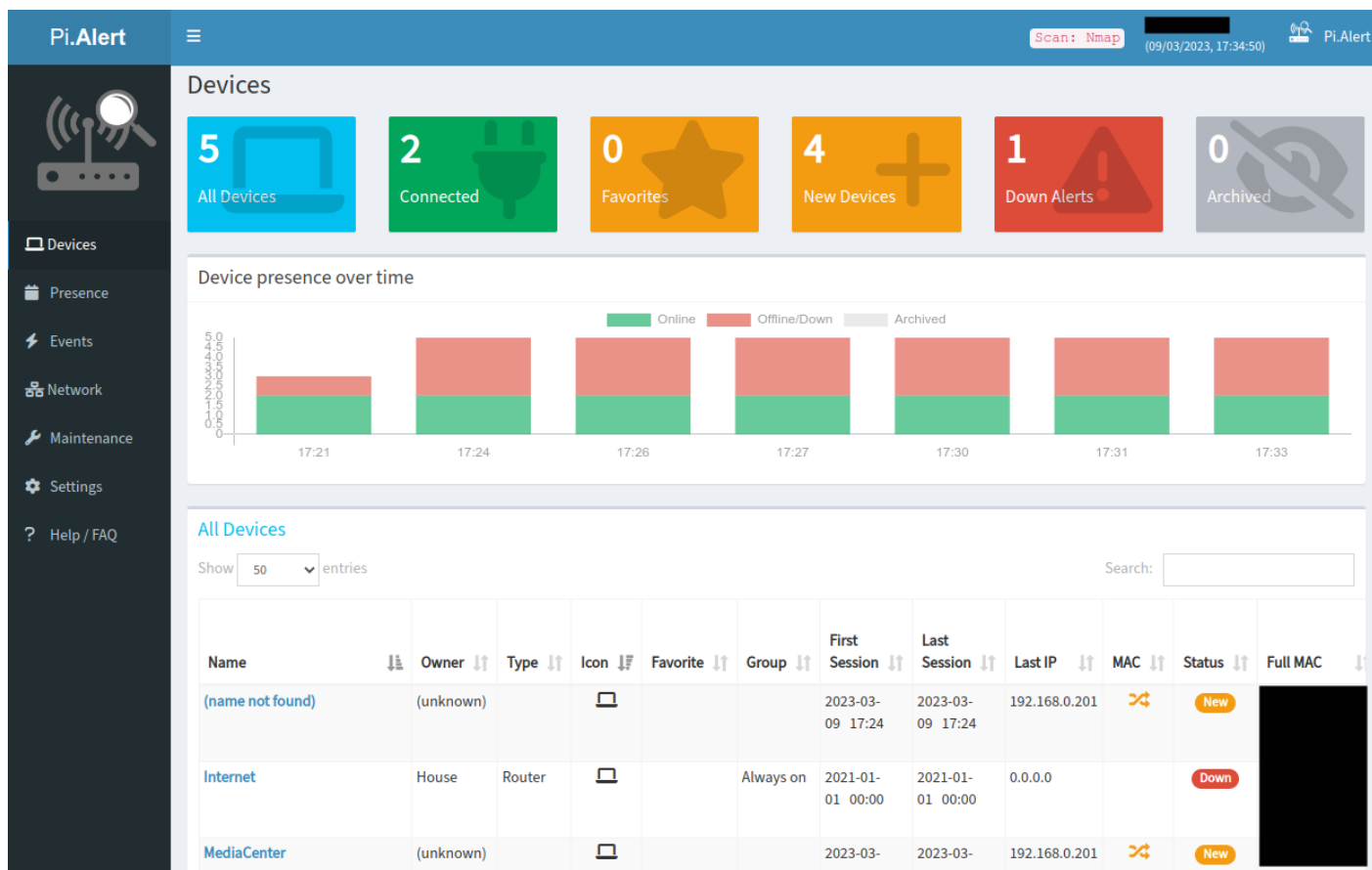


como en ocasiones anteriores, para guardar los cambios pulsaremos control + x y cuando nos pregunte aceptaremos. Una vez volvamos a estar en el terminal, escribiremos `docker compose up -d` para lanzar los servicios ubicados dentro del fichero docker-compose. Veremos algo similar a:

```
pi@mediacenter:/etc/docker $ cd $HOME
mkdir pialert
cd pialert
nano docker-compose.yml
pi@mediacenter:~/pialert $ docker-compose up -d
Pulling pialert (jokobsk/pi.alert:latest)...
latest: Pulling from jokobsk/pi.alert
934ce60d1040: Pull complete
d7da1afcf2bf: Pull complete
58d607f924cb: Pull complete
c9b26a498401: Pull complete
cecde2be4312: Pull complete
Digest: sha256:9a2472cd37540a5f2be1f3c5bf1a14912e80063adab80d1530efc7d76216bcf9
Status: Downloaded newer image for jokobsk/pi.alert:latest
Creating pialert ... done
pi@mediacenter:~/pialert $ ls -la
total 24
drwxr-xr-x  5 pi   pi   4096 mar  9 16:50 .
drwxr-xr-x 28 pi   pi   4096 mar  9 16:43 ..
drwxr-xr-x  2 root root 4096 mar  9 16:50 config
drwxr-xr-x  2 root root 4096 mar  9 16:50 db
-rw-r--r--  1 pi   pi    415 mar  9 16:43 docker-compose.yml
drwxr-xr-x  2 root root 4096 mar  9 16:50 logs
```

Elaboración propia

Si accedéis en vuestro navegador a la IP de la raspberry y al puerto que hemos establecido (20211). En mi caso sería `http://192.168.0.201:20211` deberíais ver algo como:




Elaboración propia

Funcionamiento

Nada mas acceder accederás a una pantalla como la anterior. En la mismas verás 4 partes claramente delimitadas:

- un menú lateral a la izquierda
- una parte central dividida en 3 franjas horizontales:
 - botonera de dispositivos
 - gráfica con las horas y dispositivos encontrados (conectados y no conectados)
 - listado de elementos encontrados (nombre, tipo, IP, MAC, estado,...)

Del menú lateral nos interesará acceder a la sección de Configuración (Settings).



- Dispositivos
- Historial
- Eventos
- Red
- Mantenimiento
- Configuración**
- Ayuda / FAQ

Configuración ⌵

Last time settings were imported from the pialert.conf file: 09/03/2023, 21:59:03


General

Enable ARP scan <small>ENABLE_ARPSCAN</small>	Arp-scan is a command-line tool that uses the ARP protocol to discover and fingerprint IP hosts on the local network. An alternative to ARP scan is to enable the PIHOLE_ACTIVE PiHole integration settings .	<input checked="" type="checkbox"/>
Subnets to scan <small>SCAN_SUBNETS</small>	The arp-scan time itself depends on the number of IP addresses to check. The number of IPs to check depends on the network mask you set here. For example, a <code>/24</code> mask results in 256 IPs to check, where as a <code>/16</code> mask checks around 65,536. Every IP takes a couple seconds. This means that with an incorrect configuration the arp-scan will take hours to complete instead of seconds. <ol style="list-style-type: none"> Specify the network mask. For example, the filter <code>192.168.1.0/24</code> covers IP ranges 192.168.1.0 to 192.168.1.255. Run <code>iwconfig</code> in your container to find your interface name(s) (e.g.: <code>eth0</code>, <code>eth1</code>). 	<div style="display: flex; align-items: center;"> <input style="width: 100px;" type="text" value="192.168.1.0/24"/> <input style="width: 100px;" type="text" value="eth0"/> <input type="button" value="Add"/> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> 192.168.0.0/24 --interface=eth0 </div> <div style="text-align: right; margin-top: 5px;"> <input type="button" value="Remove all"/> </div>
Print additional logging <small>PRINT_LOG</small>	This setting will enable more verbose logging. Useful for debugging events writing into the database.	<input type="checkbox"/>
Time zone <small>TIMEZONE</small>	Time zone to display stats correctly. Find your time zone here .	<input style="width: 100px;" type="text" value="Europe/Madrid"/>
Enable login <small>PIALERT_WEB_PROTECTION</small>	When enabled a login dialog is displayed. Read below carefully if you get locked out of your instance.	<input type="checkbox"/>
Login password <small>PIALERT_WEB_PASSWORD</small>	The default password is <code>123456</code> . To change the password run <code>/home/pi/pialert/back/pialert-cli</code> in the container	<input style="width: 100px;" type="password"/>
Notify on <small>INCLUDED_SECTIONS</small>	Specifies which events trigger notifications. Remove the event type(s) you don't want to get notified on. This setting overrides device-specific settings in the UI. (CTRL + Click to select / deselect).	<div style="border: 1px solid #ccc; padding: 5px;"> internet new_devices down_devices events </div>
Scan cycle delay <small>SCAN_CYCLE_MINUTES</small>	The delay between scans. If using arp-scan, the scan time itself depends on the number of IP addresses to check. This is influenced by the network mask set in the SCAN_SUBNETS setting at the top. Every IP takes a couple seconds to	<input style="width: 50px;" type="text" value="5"/>

Elaboración propia

En este menú debes prestar especial atención a la opción que dice **Subnets to scan**, es decir, subredes a escanear. En mi caso, la red de mi casa es la 192.168.0.0/24 ¡ojo, lo habitual suele ser 192.168.1.0/24! y la interface de red que usa mi raspberry es eth0 de ahí mi configuración. En otras opciones que aparecen mas abajo podéis cambiar el idioma o configurar que os lleguen alertas de intrusión por email, MQTT (lo veremos en el apartado 4 de domótica). Webhooks u otras opciones.

Si pincháis en el nombre de un dispositivo aparecerá una pantalla como la siguiente



- Dispositivos
- Historial
- Eventos
- Red
- Mantenimiento
- Configuración
- Ayuda / FAQ

MediaCenter ((unknown)) Hoy

Offline
Estado actual

1
Sesiones

0 h.
Historial

0
Alerta(s) de caída(s)

Detalles Nmap Sesiones Historial Eventos Pholus

3 / 5

Información principal

MAC [REDACTED]

Nombre MediaCenter

Propietario (unknown)

Tipo

Icon laptop

Proveedor (Unknown: locally administered)

Favorito

Grupo

Ubicación

Comentario

Información de sesión

Estado Offline

1ra. sesión 2023-03-09 17:21

Última sesión 2023-03-09 17:21

Última IP 192.168.0.201

IP estática

Network

Hardware de Red (ID) Internet

Puerto de Red HW

Configuración de eventos y alertas

Ciclo de escaneo yes

Alerta a todos los eventos

Alerta de caída

Omitir notificaciones repetidas durante 0 h (notify all event)

Nuevo dispositivo:

Archivada:

MAC al azar:

Delete Events Eliminar dispositivo Restablecer cambios Guardar

Elaboración propia

En la cual podréis establecer algunas características del dispositivo como su nombre. Esto os ayudará en el futuro, en las estadísticas, a identificar el dispositivo.

Revision #8

Created 4 February 2023 10:07:35 by Pablo Ruiz

Updated 20 July 2023 18:05:30 by Pablo Ruiz