Monitorización con Raspberry Pi

Monitorización con Raspberry Pi

- Guía para la conexión a la red y configuración del dispositivo.
- Instalación del agente y del Pandora FMS Satellite server en un dispositivo Raspberry.
- Creación automática del usuario `pandora` y asegurar el protocolo SSH.

Componentes hardware

Raspberry

Un dispositivo Raspberry es un computador de placa reducida, computador de placa única o computador de placa simple (SBC) de bajo coste. Su sistema operativo oficial es una versión Open Source adaptada de Debian, denominada Raspbian.

Software

Imagen Pandora FMS para Raspberry

La imagen distribuida se basa en el sistema operativo Raspbian. Contiene el agente, el satélite, el cliente de eHorus, los paquetes para instalar una sonda NetFlow y todas las dependencias de estos.

Instalación

Grabar imagen en la tarjeta SD

Descargar imagen oficial de Pandora FMS para Raspberry

El paso inicial de instalación es descargar la imagen oficial de Pandora FMS para Raspberry en su página de descargas oficial:

https://sourceforge.net/projects/pandora/files/Raspberry-PandoraFMS/

Consiste en un archivo en formato IMG que se debe grabar en la tarjeta de almacenamiento SD de 4 gigabytes (o más) de capacidad.

Descargar Etcher

Para grabar el fichero imagen anterior, use el software Etcher, que puede ser descargado en Etcher y que funciona de manera similar tanto en Windows® como en Linux®.

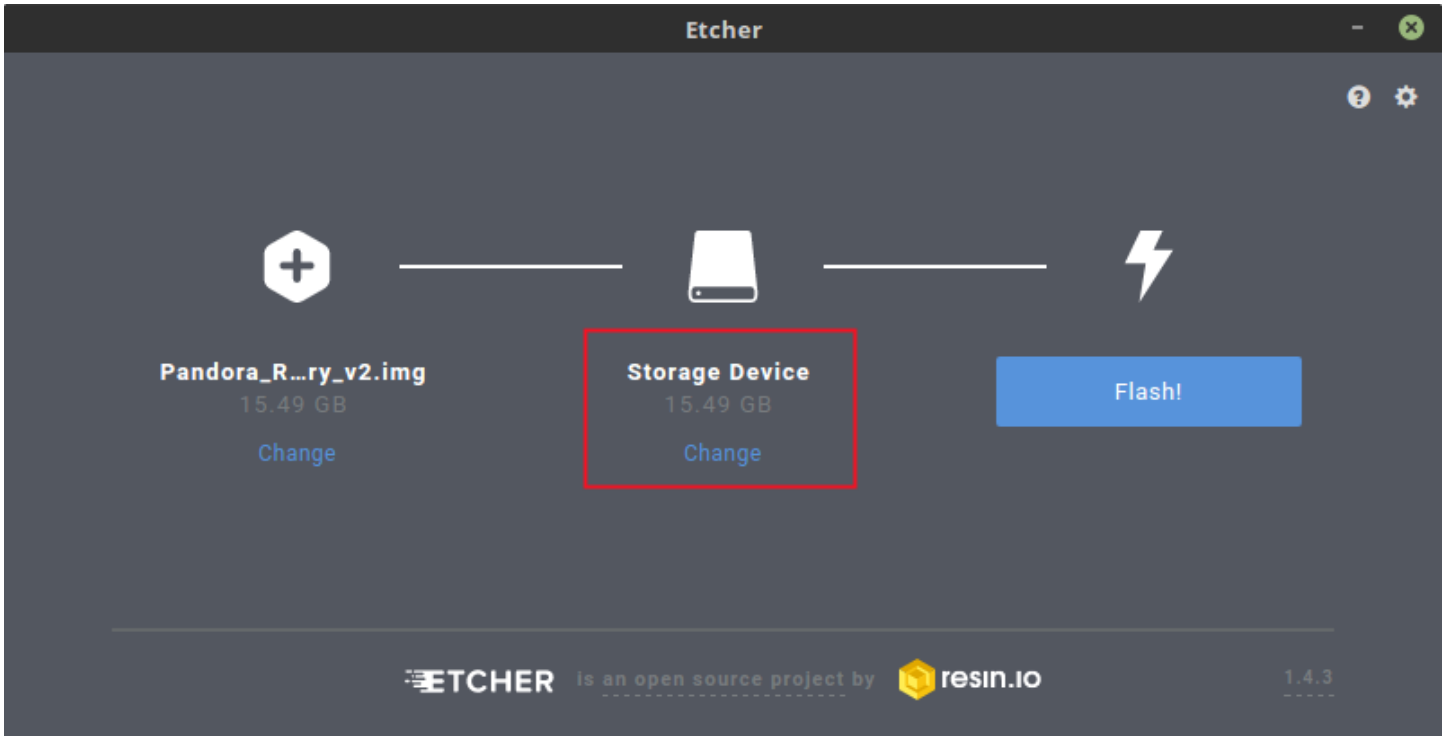
https://etcher.balena.io/

Proceso para grabar la imagen en la tarjeta SD

Coloque la tarjeta de almacenamiento SD en su ordenador, el cual debe contar con un lector especial para dicho tipo de tarjetas. Ejecute el programa Etcher.

Pulse en Select image. Esto abrirá el explorador de archivos para que seleccione la imagen de Pandora FMS previamente descargada.

Seleccione la tarjeta SD previamente insertada en el ordenador. Si la tarjeta es la que aparece por defecto, déjela tal como está; sino pulse en Change y seleccione la tarjeta SD deseada.



Pulse en el botón de Flash! para montar la imagen en la tarjeta.

Posteriormente extraiga la tarjeta de forma segura según las instrucciones de su sistema operativo.

Conexión hardware

En este paso conectará todos los componentes para encender la Raspberry:

- Introduzca la tarjeta SD en el compartimento de la parte inferior de la caja.
- Conecte el teclado a cualquier puerto USB.
- Conecte el cable HDMI al monitor y al puerto HDMI de la Raspberry.
- Conecte el cable de alimentación al dispositivo y a la corriente eléctrica.

Configuración de red

En el monitor muestra cómo se inicia el dispositivo y tras esto aparecerá un instalador en el que podrá seleccionar qué interfaz desea configurar.

Cableado DHCP

Seleccione `Eth0` para configurar la interfaz de red por cable.

A la pregunta si desea cambiar la configuración de la interfaz `Eth0` responda positivamente, en caso de que tenga un servidor DHCP en la red, seleccione DHCP.

Tras esto aparecerá un mensaje de que la red cableada ha sido configurada correctamente.

Cableado Estático

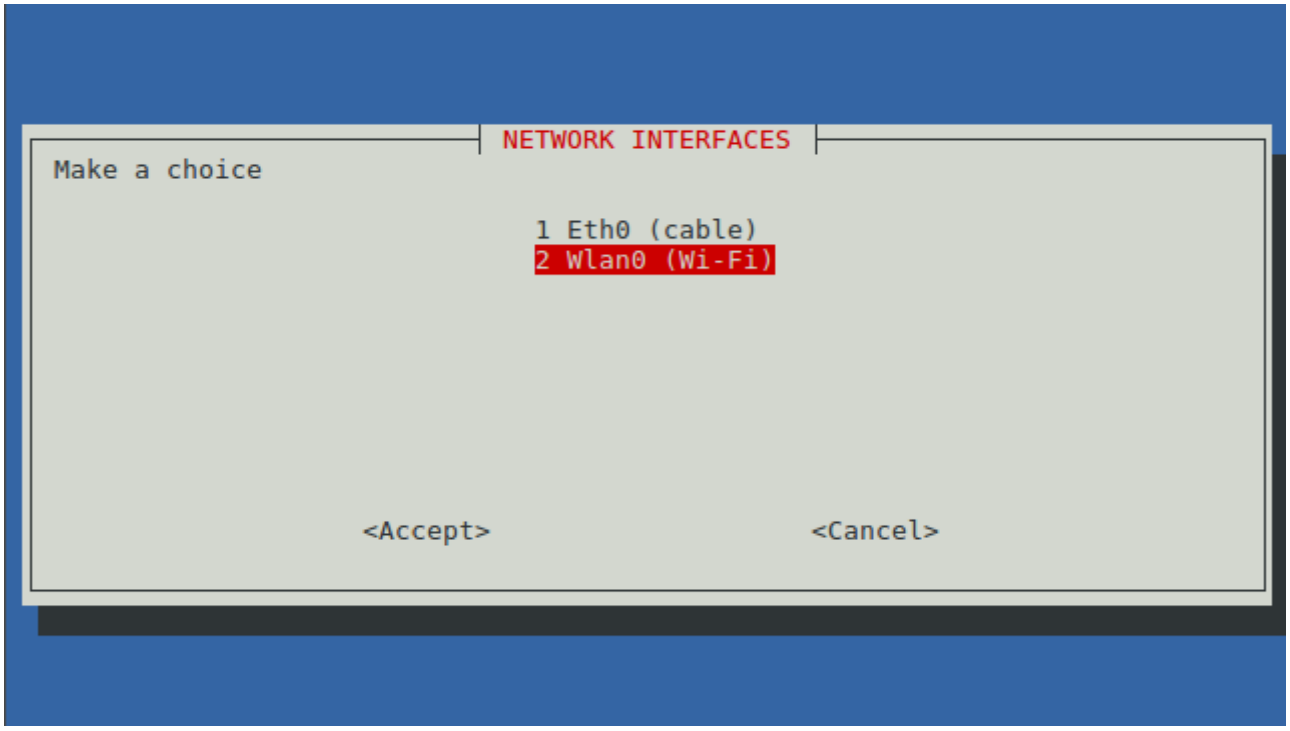
Seleccione IP STATIC si desea configurar la interfaz cableada manualmente. Introduzca la dirección IP estática de la Raspberry.

Introduzca la dirección del Gateway de red. Introduzca la máscara de red correspondiente. Introduzca el DNS público.

Obtendrá un mensaje de que la configuración se ha realizado con éxito.

Inalámbrica DHCP

Seleccione Wlan0 para configurar la interfaz de red inalámbrica.



A la pregunta si desea cambiar la configuración de la interfaz Wlan0 responda positivamente. En caso de que tenga un servidor DHCP en la red, seleccione DHCP.

Escoja en la lista el nombre del punto de acceso. Introduzca la clave del punto de acceso. Obtendrá un mensaje de que la configuración se ha realizado correctamente.

Inalámbrica Estática

- Seleccione WIFI STATIC si desea configurar la interfaz inalámbrica manualmente.
- Elija de la lista el nombre del punto de acceso. Introduzca la clave del punto de acceso.
- Introduzca la dirección IP estática del dispositivo Raspberry.
- Introduzca la máscara de red correspondiente.
- Introducimos la dirección del Gateway del punto de acceso.
- Se obtendrá un mensaje indicando que la configuración se ha realizado con éxito.

Configuración de Agente y de Satélite

Agente

- Para instalar el agente seleccione AGENT en el menú.
- Introduzca la dirección IP del servidor Pandora FMS al que apuntará el Agente.
- Se Introduce el grupo existente en el servidor Pandora FMS al cual añadirá el Agente.

Satélite

- Para instalar el satélite seleccione SATELLITE en el menú.
- Introduzca la dirección IP del servidor Pandora FMS al que apuntará el Satélite.
- Introduzca el rango y máscara de la red que monitorizará.

- Introducimos la comunidad o lista de comunidades SNMP de los dispositivos de red a monitorizar.
- Introduzca el usuario o lista de usuarios para hacer consultas WMI a los equipos de la red a monitorizar.

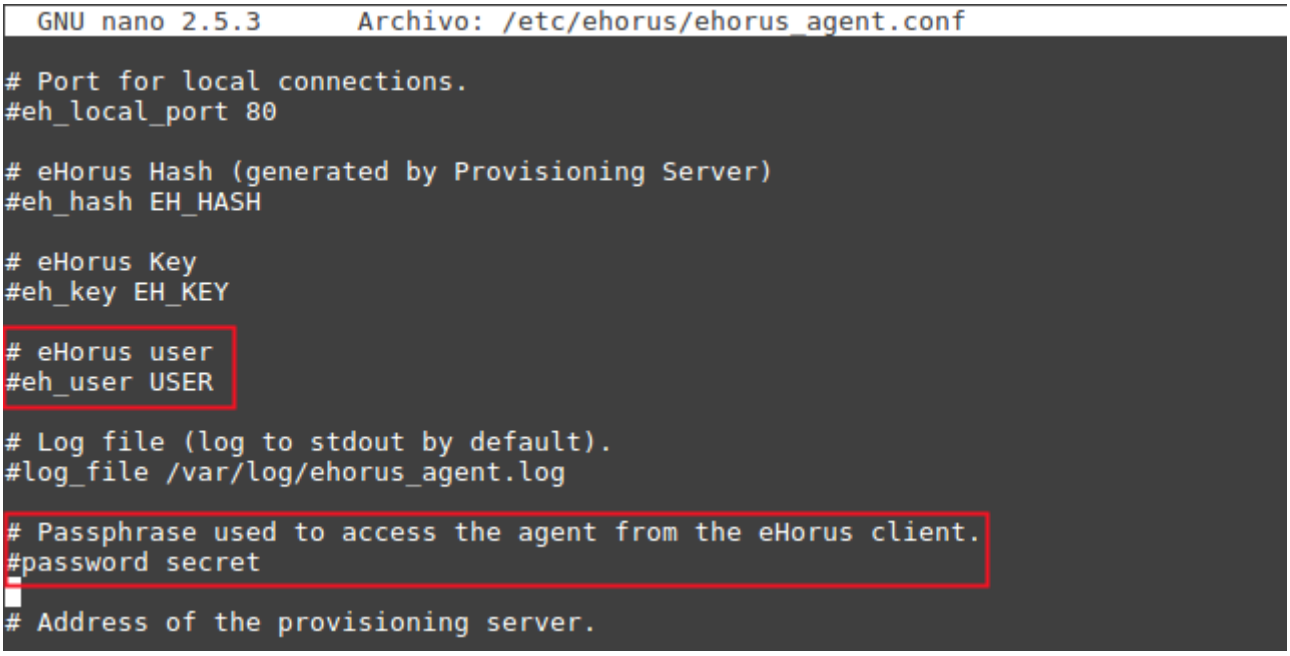
Postinstalación

Configuración del cliente eHorus

Edite el fichero con el editor de texto nano:

```
/etc/ehorus/ehorus.conf
```

Reemplace el *token* `eh_user` por su nombre de usuario en eHorus. En la línea `#password secret` borre el numeral que indica inicio de comentario (*descomente la línea*) y reemplace la palabra "secret" por una contraseña para acceder a su Agente desde eHorus.



Si necesita ver el entorno gráfico debe instalar la dependencia de x11vnc:

```
apt-get install x11vnc
```

Inicie el servicio de eHorus con:

```
/etc/init.d/ehorus_agent_daemon start
```

Sonda NetFlow

Su funcionamiento se basa en la utilización de varios componentes:

- Un dispositivo con compatibilidad NetFlow, generalmente un hardware de red tipo *switch* o *router*, que genera paquetes de información, o bien una sonda NetFlow.
- Un colector NetFlow, que recibe los paquetes generados por el dispositivo anterior, almacenándolos y procesándolos. Suele ser una herramienta o servidor con estas capacidades.

Pandora FMS utiliza una herramienta *OpenSource* llamada nfcapd para procesar todo el tráfico NetFlow. Este demonio lo levanta de forma automática el servidor de Pandora FMS. Este sistema almacena los datos en ficheros binarios, en una ubicación determinada. Debe instalar nfcapd en su sistema antes de poder trabajar con NetFlow en Pandora FMS. El demonio nfcapd por defecto escucha en el puerto 9995/UDP, por lo que tendrá que tenerlo en cuenta si tiene *firewalls* para abrir este puerto y a la hora de configurar sus sondas NetFlow.

Sonda NetFlow por software

Si no dispone de un *router* con NetFlow pero el tráfico "pasa" por un sistema Linux, puede instalar un software que actúe de sonda y envíe información de tráfico NetFlow al colector. En Linux existe un programa llamado fprobe que captura el tráfico y lo reenvía a un servidor NetFlow. Con él puede generar tráfico NetFlow, de todo el tráfico de red que pasa por sus interfaces.

Primero debe instalar fprobe:

```
apt-get install fprobe
```

Al momento de instalar preguntará qué interfaz necesita monitorizar y a qué dirección IP y puerto enviar la información recabada. Si luego desea reconfigurar puede ejecutar el siguiente comando:

```
/usr/sbin/fprobe -i <interfaz_monitorizar> -fip <ip_colector>:<puerto>
```

En el ejemplo siguiente se enviará todo el tráfico del interfaz eth0 al colector NetFlow escuchando en el puerto 9995 de la dirección IP 192.168.70.185:

```
/usr/sbin/fprobe -i eth0 -fip 192.168.70.185:9995
```

Una vez generado tráfico, podrá ver estadísticas de este tráfico en el colector NetFlow con el comando:

```
nfdump -R /var/spool/pandora/data_in/netflow
```

Hay que habilitar NetFlow para que sea accesible desde los menús Operación y Administración:
Habilitar NetFlow

Una vez configurado el NetFlow, habrá que reiniciar el servidor de Pandora FMS para que levante el servidor nfcapd. Este debe estar correctamente instalado antes de intentar arrancarlo. Compruebe los *logs* del servidor ante cualquier duda.

Sonda NetFlow con Port Mirroring

Explicado en la sección: Netflow Port Mirroring

Volver a Indice de Documentación Pandora FMS