

Raspberry: Instalar y ejecutar el servidor Blynk local

1 Descarga Blynk

Crea una carpeta en tu directorio home, por ejemplo Blynk

mkdir Blynk

Y descarga Blynk :

```
wget "https://github.com/Peterkn2001/blynk-server/releases/download/v0.41.16/server-0.41.16-java8.jar"
```

El enlace <https://github.com/Peterkn2001/blynk-server/releases/download/v0.41.16/server-0.41.16-java8.jar> conviene actualizarlo, recomendamos visitar la página <https://github.com/Peterkn2001/blynk-server#blynk-server> y coger la última versión de aquí

GETTING STARTED

Blynk server

Blynk Server is an Open-Source [Netty](#) based Java server, responsible for forwarding messages between Blynk mobile application and various microcontroller boards and SBCs (i.e. Arduino, Raspberry Pi. etc).

Download latest server build [here](#).

release **v0.41.17** downloads **6.2k**

Requirements

- Java 8/11 required (OpenJDK, Oracle)
- Any OS that can run java
- At least 30 MB of RAM (could be less with tuning)
- Open ports 9443 (for app and hardware with ssl), 8080 (for hardware without ssl)

2 Configurar server.properties

Necesitamos crear un fichero de configuración para las diferentes opciones que queremos en nuestro servidor Blynk.

Entra en la carpeta creada Blynk y crea el fichero *server.properties*.

cd Blynk

sudo nano server.properties

A continuación se muestra un posible contenido de server.properties.

```
initial.energy=1000000
allow.reading.widget.without.active.app=false
user.message.quota.limit=100
logs.folder=./logs
user.dashboard.max.limit=100
lcd.strings.pool.size=6
server.ssl.key=./server_embedded.key
webhooks.response.size.limit=96
hardware.mqtt.port=8440
table.rows.pool.size=100
terminal.strings.pool.size=25
admin.email=admin@blynk.cc
admin.rootPath=/admin
user.widget.max.size.limit=20
listen.address=
blocking.processor.thread.pool.limit=6
stats.print.worker.period=60000
enable.db=false
force.port.80.for.csv=false
enable.raw.db.data.store=true
restore.host=blynk-cloud.com
csv.export.data.points.max=43200
restore=false
user.profile.max.size=256
allow.store.ip=true
allowed.administrator.ips=0.0.0.0/0,::/0
net.interface=eth
webhooks.frequency.user.quota.limit=1000
http.port=8080
```

```
web.request.max.size=524288
user.devices.limit=50
async.logger.ring.buffer.size=2048
user.tags.limit=100
server.ssl.key.pass=
admin.pass=admin
hard.socket.idle.timeout=10
product.name=Blynk
data.folder=/Path
map.strings.pool.size=25
profile.save.worker.period=60000
https.port=9443
log.level=info
server.ssl.cert=./server_embedded.crt
force.port.80.for.redirect=true
notifications.queue.limit=2000
notifications.frequency.user.quota.limit=5
server.host=192.168.137.1
app.ssl.port=8443
hardware.default.port=8442
hardware.ssl.port=8441
hardware.mqtt.port=8440
```

Para la explicación de cada línea, aconsejo consultar esta [página](#) en el apartado *Configuración avanzada del servidor local*

3 Ejecutar el servidor Blynk local

En la Raspberry por comandos SSH, entramos en la carpeta donde hemos creado el servidor Blynk

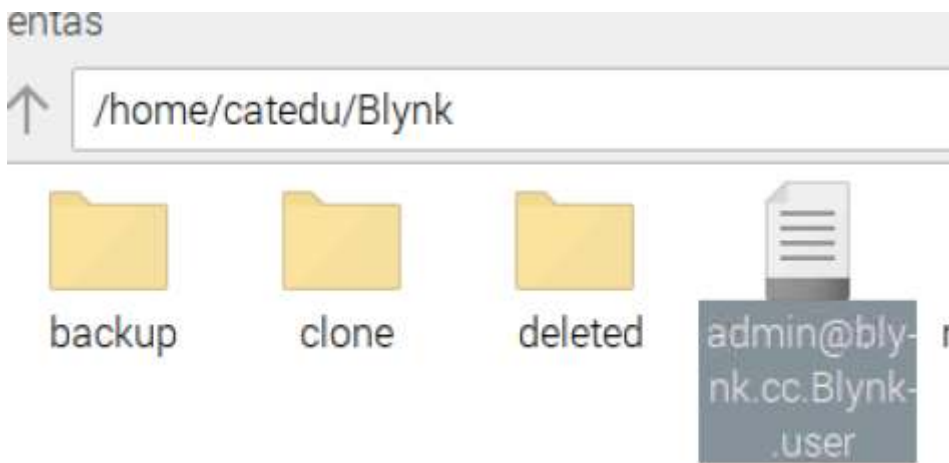
cd Blynk

Y ejecutamos el servidor Blynk instalado, pero que cargue la configuración de server.properties que en nuestro caso como el la Raspberry el usuario se llama catedu la carpeta es catedu:

java -jar server-0.41.16-java8.jar -dataFolder /home/catedu/Blynk -serverConfig /home/catedu/Blynk/server.properties

Curiosamente la primera vez que ejecutas esta instrucción te sale los datos del usuario

admin@blynk.cc y su contraseña sin encriptar que por defecto es admin. Si no has tomado nota, ejecutar la instrucción anterior no sirve de nada pues ya ha creado el fichero texto de este usuario.



La única forma de que te vuelva a mostrar la contraseña es borrar el fichero texto y ejecutar otra vez la orden `java -jar server....`

4 Que la orden de ejecución se haga automáticamente cada vez que se reinicie la Raspberry

Para no repetir estos dos comandos `cd Blynk` y `java -jar server-0.41.16-java8.jar -dataFolder /home/catedu/Blynk -serverConfig /home/catedu/Blynk/server.properties` cada vez que reiniciamos la Raspberry puedes generar un script para que lo ejecute automáticamente, puedes ver buenos tutoriales en Internet.

En internet puedes ver varios métodos:

Método1 es entrar en `/etc` y editar el fichero `rc.local` y añadir esta línea

```
java -jar server-0.41.16-java8.jar -dataFolder /home/catedu/Blynk -serverConfig /home/catedu/Blynk/server.properties &
```

Método 2 usar el comando `crontab -e` y poner al final la siguiente línea `@reboot java java -jar server-0.41.16-java8.jar -dataFolder /home/catedu/Blynk -serverConfig /home/catedu/Blynk/server.properties`

5 Probarlo

Si la IP de la Raspberry es 192.168.1.112 entonces entramos en:

<https://192.168.1.112:9443/admin>

Vale, ya estoy ¿y ahora qué?

Seguramente te saldrá la siguiente advertencia por el certificado SSL, dale a **Configuración avanzada** y luego a **Acceder a (la IP del servidor Blynk Legacy) sitio no seguro**



La conexión no es privada

Es posible que los atacantes estén intentando robar tu información de **192.168.43.111** (por ejemplo, contraseñas, mensajes o tarjetas de crédito). [Más información](#)

NET::ERR_CERT_AUTHORITY_INVALID



Para disfrutar del máximo nivel de seguridad en Chrome, [activa la protección mejorada](#).

Ocultar configuración avanzada

1

Volver para estar a salvo

Este servidor no ha podido probar que su dominio es **192.168.43.111**, el sistema operativo de tu ordenador no confía en su certificado de seguridad. Este problema puede deberse a una configuración incorrecta o a que un atacante haya interceptado la conexión.

[Acceder a 192.168.43.111 \(sitio no seguro\)](#)

2

Si quieres generar certificados SSL propios para que no salga la anterior pantalla consulta [aquí](#)

Tienes que entrar con el usuario y contraseña fijada en **server.properties** :

```
# Default admin name and password. Will be created on initial server start
admin.email=admin@blynk.cc
admin.pass=admin
```

Si quieres cambiar la contraseña, tienes que hacerlo como un usuario normal en la página de administración tal y como hemos visto en el capítulo [Entrando en el Blynk local: El panel de control](#)

6 Para saber más :

- <https://github.com/Peterkn2001/blynk-server#blynk-server>
- [Intalación de Blynk : How to Install a Blynk Local Server on Raspberry Pi](#)
- [Configuración de server.properties.](#)

7 Para saber más : Configurar mail.properties

Este aparatado ya comentamos que no lo aconsejamos, pues los alumnos no suelen tener email y la APP ya no permite crear usuarios con email, pero si queremos que envíe los tokens por email, hay que crear este fichero para que el servidor envíe por email los tokens de los proyectos

Entra en la carpeta creada Blynk y crea el fichero *mail.properties*.

cd Blynk

sudo nano mail.properties

A continuación se muestra una muestra del posible contenido de mail.properties :

```
mail.smtp.auth=true
mail.smtp.starttls.enable=true
mail.smtp.host=smtp.gmail.com
mail.smtp.port=587
mail.smtp.username=Your EMAIL ID
mail.smtp.password=Password
```

Utilizando **Your EMAIL ID** y **Password** los datos de una cuenta de gmail tuya. En esa cuenta tienes que permitir accesos no seguros. Aquí se muestra dónde está en la pantalla de configuración de Gmail :

The image is a screenshot of the Google Account settings interface. On the left is a navigation menu with the following items: 'Inicio' (highlighted with a red box and a red circle with the number 1), 'Información personal', 'Datos y personalización', 'Seguridad' (highlighted with a red box and a red circle with the number 2), 'Contactos e información compartida', 'Pagos y suscripciones', and 'Información general'. The main content area on the right has a header 'Gestionar dispositivos' and another partially visible 'Gestionar...'. Below this is a section titled 'Acceso de aplicaciones poco seguras' (highlighted with a red box and a red circle with the number 3). The text in this section reads: 'Tu cuenta es vulnerable porque permites el acceso de aplicaciones y dispositivos que utilizan una tecnología de inicio de sesión poco segura. Para mantener tu cuenta protegida, Google desactivará automáticamente este ajuste si no se utiliza.' Below this text is a toggle switch labeled 'Activado' (highlighted with a red box and a red circle with the number 4). At the bottom of this section is a link that says 'Desactivar acceso (opción recomendada)'.

Inicio ¹

Información personal

Datos y personalización

Seguridad ²

Contactos e información compartida

Pagos y suscripciones

Información general

Gestionar dispositivos

Gestionar i

Acceso de aplicaciones poco seguras ³

Tu cuenta es vulnerable porque permites el acceso de aplicaciones y dispositivos que utilizan una tecnología de inicio de sesión poco segura. Para mantener tu cuenta protegida, Google desactivará automáticamente este ajuste si no se utiliza.

! Activado ⁴

[Desactivar acceso \(opción recomendada\)](#)

Para saber más

- [Configuración mail](#)

Revision #5

Created 1 February 2022 12:51:22 by Equipo CATEDU

Updated 7 December 2022 13:48:47 by Javier Quintana