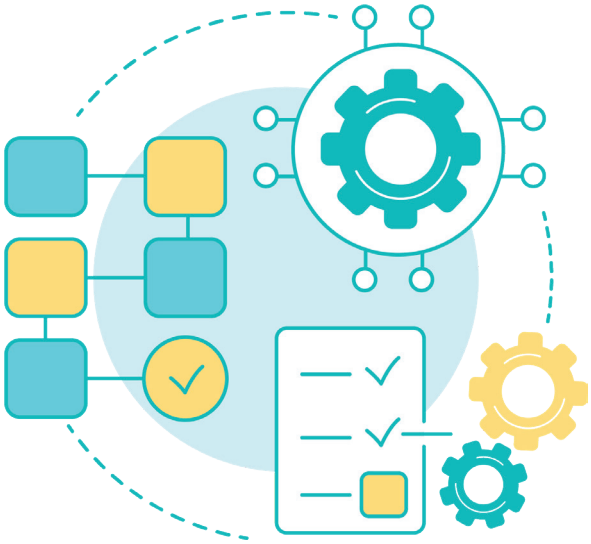
WiFiMon

FEEL, SEE AND UNDERSTAND YOUR WIFI

QUICKSTART INSTALLATION MANUAL

GÉANT

AUTOMATED INSTALLATION PROCESS



WiFiMon relies on Ansible to simplify complex component installation:

1. WiFiMon Analysis Server - WAS
2. WiFiMon Test Server - WTS

Playbooks for WAS and WTS can be run from:

- The WiFiMon Administrator local environment;
- The WAS and WTS command line.

REQUIREMENTS

A. Machine where the playbook is run:

- ✓ Ansible version 2.10 or greater.
- ✓ SSH access to the WAS/WTS “root” user
  - ✓ We advise against password-based SSH authentication. We suggest key-based SSH authentication to “root” or disabling SSH to “root” after WiFiMon installation.

B. DNS Records:

1. WiFiMon Analysis Server: The following A-type records, all pointing to the IP address of the WiFiMon Analysis Server:
   - ✓ was_hostname.was_domainsuffix *)
   - ✓ was_hostname-**ui**.was_domainsuffix
   - ✓ was_hostname-**elastic**.was_domainsuffix
   - ✓ was_hostname-**kibana**.was_domainsuffix
   - ✓ was_hostname-**flask**.was_domainsuffix

*) instead of domainsuffix put the domain of your institution

2. WiFiMon Test Server: The following A-type record pointing to the IP address of the WiFiMon Test Server:

✓ wts_hostname-**wts.**wts_domainsuffix

e.g. “wifimon.example.com”, “wifimon**-ui**.example.com”

Note: The WAS and WTS may be installed on the same machine. In this case, all DNS records will point to the same IP address. However, DNS records should be as described above.

C. Firewall Requirements for WAS and WTS

TCP ports 80 and 443 must be accessible to the monitored devices and the WiFiMon administrator

INSTALLATION

A. Running the Playbook

Clone the Playbook repository to the machine hosting Ansible:

git clone https://gitlab.grena.ge/nugzar/wifimon-ansible.git

Edit file: hosts.cfg in the “wifimon-ansible” directory.

Specify WAS (entries starting with WAS_*) and WTS reachability details. IP addresses or domain names can be used.

If WAS and WTS are installed in the same machine, the same IP address can be specified. However, if domain names are used instead of IP addresses, they should be specified as described in the “Requirements” section..

Edit file “main.yml” in the “wifimon-ansible/vars” directory.
Based on the “DNS Records” section given names, fill in these lines:

1 was_server_hostname: **was_hostname**
2 was_server_domainname: **was_domainsuffix**
3 wts_server_hostname: **wts_hostname-wts**

(**bold letters:** Input from the WiFiMon administrator)

Set the email that will be used to access the WiFiMon UI:
<wifimon_admin_email>

Then:

1. Set the email used for Lets Encrypt certificates: <letsencrypt_admin_email>.
2. Set the credentials used for securing WiFiMon. These may be randomized strings, consisting of English letters and digits.

Fill in the following lines:

- ✓ “wifimon_database_user_pass”
- ✓ “wifimon_admin_pass”
- ✓ “elastic_elasticsearch_password”
- ✓ “kibana_elasticsearch_password”
- ✓ “logstash_system_user_password”
- ✓ “logstash_writer_user_password”
- ✓ “fingerprint_key”

Remaining lines should be left as is.

B. Run the following command to install WAS/WTS:

- ✓ ansible-playbook wifimon.yml

The WiFiMon UI may be accessed using the following link:
https://<was_hostname>-ui.<was_domainsuffix>
Example: https://wifimon-ui.example.com

Using the “wifimon_admin_email” and the “wifimon_admin_pass” credentials.

CONFIGURATIONS

WiFiMon Test Server Configuration

HTML files for crowdsourced tests are in the paths (in WTS):

- **NetTest:** /var/www/wts/wifimon/measurements/nettest.html
- **Boomerang:** /var/www/wts/wifimon/measurements/boomerang.html
- **LibreSpeed:** /var/www/wts/wifimon/measurements/speedworker.html
  /var/www/wts/wifimon/js/speedworker.html

These files are already prepared for crowdsourced measurements during WTS installation.

You may change the attribute “testServerLocation” in each of them to indicate the WTS location. The HTML code of these files may be copied to a frequently visited website to monitor end users.

Constructing the files for hardware probe performance measurements is based on the HTML code of the above files and the name you wish to use for describing your probe. Any string can be used for naming the probes, e.g. “1”, “wifimon-1”, etc. In the following, we will denote this string with bold letters, i.e. **probename**.

Copy nettest.html, boomerang.html and speedworker.html (both files) to the same directory. The target files should be named:

- nettest**probename.**html
- boomerang**probename.**html
- speedworker**probename.**html

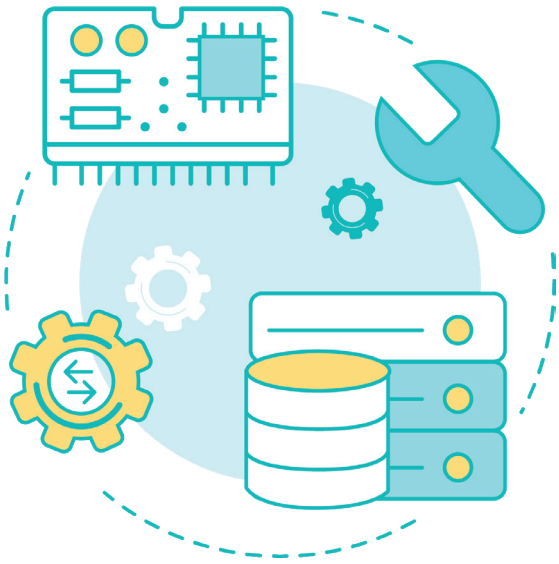
Change the name of the “testtool” attribute in each file to:

- NetTest-**probename**
- boomerang-**probename**
- speedtest-**probename**

Hyphens (-) are necessary to differentiate between the testtool used and the probe name.

For example, if the probe name is “1”, Boomerang file should be named as “boomerang1.html”, whereas “testtool” should be “boomerang-**1**”. If the probe name is “wifimon-1”, Boomerang file should be named as “boomerang**wifimon-1**.html”, whereas “testtool” should be “boomerang-**wifimon-1**”.

HARDWARE PROBE CONFIGURATION



1. Download the WiFiMon Hardware Probe (WHP) image from https://s3.grena.ge/raspbarry-image/whpv8.img.gz.

2. Uncompress the downloaded raspberry image before the installation by running 'gunzip whpv8.img.gz'

3. Install it on a Raspberry Pi v3 or v4 device

4. Edit the last line of files:
   /usr/local/bin/{nettest.sh, boomerang.sh, speedtest.sh}
   based on the configuration of the previous section.

   A. - If the name of the probe is "1" and HTTPS is used, the last line of "nettest.sh" should be:
   - timeout 60 firefox-esr
   - new-tab: https://wts_hostname-wts.wts_domainsuffix/wifimon/measurements/nettest1.html

B. - If the probe name is “wifimon-1” and HTTPS is used, the last line of “nettest.sh” should be:
   - timeout 60 firefox-esr
   - new-tab: https://wts_hostname-wts.wts_domainsuffix/wifimon/measurements/nettestwifimon-1.html

4. Repeat for files “boomerang.sh” and “speedtest.sh”.

5. Edit files: /root/twping_parser.py and /root/wireless.py
   By replacing capital words with the suitable content as described in: https://wiki.geant.org/pages/viewpage.action?pageId=631443696

HARDWARE PROBE DISTRIBUTED CONTROL AND CONFIGURATION

Optionally, WHP distributed configuration and control may be enabled. Salt is required for application layer communication between WHP’s and the WAS, which facilitates control of WHP’s behind NAT networks. Salt can be installed on WHP’s via:

- – apt-get install -y salt-minion

- Edit file “/etc/salt/minion”:
  In line “master” specify the WAS name, i.e. was_hostname.was_domainsuffix

- Edit file “/etc/salt/minion_id”:

Specify the name of the WHP, e.g. “1” or “wifimon-1”, based on the examples of the previous section.

- In WAS: Accept the WHP Salt key with the command “salt-key -A”

- Control the probes by accessing the WiFiMon UI in WAS through the tab “Configuration -> Control Probes”