



Akvorado,  
collect and  
visualise flows  
the easy way

Will van Gulik

presenting  
Vincent Bernat & Free's work

Swinog #38



# Bio & Agenda

- Will van Gulik :
  - Network Engineer and associate at Nimag Networks,
  - Committee member of RomandIX,
  - Ripe's Connect WG co-chair,
  - generally having fun with friends, Internet, books and music in not particular order
- Akvorado :
  - Developed by Vincent Bernat and Free (French ISP)
  - <https://www.akvorado.net> , licensed under AGPLv3
- Disclaimer :
  - This is not my work, I'm just a preacher, don't shoot me yet, read the docs, and then the troubleshooting guide, it's amazing and precise.
- Agenda :
  0. Intro, Bio, Agenda (*Done*)
  1. Reminder and Prerequisite
  2. Connect, Start the deployment
  3. ~~Talk while magic happens~~ Words of advice
  4. Demo (Hopefully show the working website)
  5. Links to resources, Cordialement, bisous.

# Reminder and Prerequisite

- Akvorado
  - “ receives flows ([...] Netflow/IPFIX and sFlow), enriches them with interface names (using SNMP), geo information (using MaxMind), and exports them to Kafka, then ClickHouse. It also exposes a web interface to browse the collected data. “
- Previously done (before the install) :
  - Prepared my 2 routers (VXR w/G2) to send netflow to the Akvoradhost
  - Modified my docker storage path to /opt/docker in /etc/docker/daemon.json,
  - Downloaded the quickstart's tgz, uncompressed it and docker pulled.
- The scripts I created are simple, dirty and I'm not a developer. You're more than welcome to suggest improvements .

# Start the deployment

- My script used in this demo :
  - Moves to the Akvorado directory
  - Removes the demo parameters from the config files (2 files)
  - Modifies the SNMP community to match my routers (1 file)
  - Insert a default sampling rate (needed by my old G2s) (1 file)
  - Adds the export / import filters that I modified to match my infra.
  - Starts Akvorado

# Words of advice ...

- RTFM. Really.
  - Forget the old ways of NFsen because ...
  - ... It's simple as hell, if you follow the documentation,
  - Before bugging the dev team, use the troubleshooting guide, I fixed most of my issue using it, and the rest of my problems by re-reading the docs,
- Requirements :
  - SNMP reachability of your routers by the Akvoradhost
  - Some flows reaching your Akvoradhost (example in the docs for Juniper, Cisco, and more)
  - Not so much storage
    - At Nimag, collecting since 22.10.22, 22G used, sampling rate of 1/1024 (less than 5Gbps avg.)
    - In my lab, collecting since 22.03.23, 24G used, sampling rate of 1/10 (less than 10Mbps avg.)



# ... and links

- Akvorado :
  - <https://www.akvorado.net>
- My scripts / docs :
  - <https://p.under.ch/Scripts/>
  - <https://www.porcus.ch/blog/>
- No questions, it's a lightning talk, come bug me later.



- Cordialement, bisous.

# Failover Screenshot

