Installation of Apresa on an existing Debian machine

When renting a virtual machine in a data center with any (cloud) service provider, usually you do not have the option to install Apresa using the installation ISO. Instead you are probably given access to an already installed instance of Debian Linux. In this document, the procedure is described to install Apresa in such an environment.

Notice that since the virtual machine is not set up and fully controlled by the Apresa installation, we cannot guarantee the same functionality.

Retrieving and validating the installation package

- When creating the virtual machine, select Debian Linux version 10 (other distributions and versions are not supported currently)
- Get access to the shell, and login
- Retrieve the installation package from the internet

  `wget https://www.vidicode.com/support/apresa-install-debian10.tgz`

  If it says "command not found", then first install wget (**`apt-get install wget`**)
- The signature of the installation package can be used to verify if the package is from Vidicode.

  `wget https://www.vidicode.com/support/apresa-install-debian10.tgz.sig`
  `gpg apresa-install-debian10.tgz.sig`

  The public key of Vidicode is found at the following places:

  - /usr/share/apresa/vididev.pubkey on any existing Apresa installation
  - On a key server: **`gpg --recv-keys 4442F1408963693A`**
  - https://www.vidicode.com/support/vididev.pubkey

Installation

- Extract the installation pack

  `tar xzf apresa-install-debian10.tgz`

  If it says “command not found”, then first install tar (**`apt-get install tar`**).
- Run the installation (this step has to be done as root)

  `apresa-install/run.sh`

  After the installation process, you will be prompted to enter a new admin password for the web interface.

Security measures

Consider applying the following security measures, especially when Apresa is on the public internet.

- Restrict access using a firewall on Apresa or outside of it, based on IP address or other rules, or give access only through a VPN tunnel. Disable remote access to SSH, or allow access to

SSH (port 22) only for your own IP address. This might be configurable in the network settings of your virtual machine as provided by your cloud service provider (e.g. Azure).

- Configure automatic security updates of Debian Linux (Tools > System > Software update)
- Use strong passwords for the web interface and use a strong password or key-based logon for SSH
- Enable two-factor authentication using email (System settings > System > Log on Verification Code)