OpenTap is a software defined networking interface to network tap devices. Network tap devices are devices that can capture data plane traffic in a network. This data can be collected in various formats such as pcap (packet capture) or NetFlow (flow records in CSV). OpenTap configuration is set by an administrator through the opentap.conf file.

The OpenTap interface is a remote invocation service that can be implemented on top of other protocols such as SSH or HTTP (via REST API). The invocations supported are:

capture

arguments: type start stop observationpt

type – data type

start – start time of capture

stop – stop time of capture

observationpt – observation point identifier (0 for default)

return: id (used for retrieval)

REST: /capture/type?start=xx&stop=xx&observationpt=xx

retrieve

arguments: id

id – retrieval id (returned from capture invocation)

return: captured data

REST: /retrieve?id=xx

capabilities

arguments: none

return: supported data type list, observation point identifier list, capture length limit, retention period limit

REST: / or /capabilities

Data types currently supported:

Network data types: **netflow**, **ethernet**

Environmental data types: **temperature**

Observation points:

Each OpenTap device can support multiple observation points for each data type. The OpenTap device administrator can associate meaningful IDs with system specific IDs for the data collection devices (network interface card identifiers, Phidgets sensor identifiers). This is setup in an opentap.conf file found in /etc/opentap. The installer will solicit input to auto-generate this file.

Installing OpenTap:

Uncompress the OpenTap tarball:

tar -zxf ./opentap.tgz

Execute the installation script:

cd opentap
sudo ./installer.sh

The installation script will install of the necessary files for OpenTap and then solicit input from you to setup operating parameters and observation point identifiers (currently only for the network interfaces).

OpenTap will be installed in /opt/opentap.

OpenTap consists of two perpetually executing programs (a python script Web server that hosts the REST API, and a bash script Garbage collector that purges old data).

Starting OpenTap:

sudo /opt/opentap/bin/start_opentap.sh

Shutting down OpenTap:

sudo /opt/opentap/bin/stop_opentap.sh

Using OpenTap:

The quickest way to use OpenTap is with the OpenTap Python module found in ***demo/opentap.py*** along with the demo script ***demo/opentapdemo.py***. The ***opentap.py*** module contains functions to initiate data capture tasks and retrieve the data into PANDAS data frames. At the top of this file (***opentap.py***) you will want to create a Python dictionary for each of your OpenTap devices. The dictionary will need a name and contain three fields (**name** – the name of the device, **ipaddr** – the IP address of the OpenTap device REST API, and **portnum** – the port number of the OpenTap device REST API). Here is an example for our OpenTap device that is monitoring our Virgo cluster:

VIRGO = { 'name': 'virgo', 'ipaddr': '129.108.40.76', 'portnum': '50080' }

The demo script (***opentapdemo.py***) shows an example of how to capture NetFlow data and retrieve this data into a PANDAS data frame.