opFlow 3 Installation Guide

Before You Begin

Prerequisites

- NMIS installed on the same server that opFlow is being installed (NMIS version >=8.5.6G).
- The individual performing this installation has a small bit of Linux experience.
- Root access is available.
- Internet access is required for installing any missing but required software packages.
- opFlow License (evaluation available here).
- All licenses are added/updated at https://<hostname>/omk/opLicense .

Preparation

- If you do not yet have a working installation of NMIS in your server, please follow the procedure in the NMIS 8 Installation Guide.
- Download opFlow from the Opmantek website.
- If you have opFlow 2.X installed please see the upgrade documentation

Installation Steps

As of February 2016, opFlow is distributed in a self-extracting download format that simplifies the installation process quite a bit. More information on running the installer can be found HERE: The Opmantek Installer

Transfer the opFlow installer onto the server in question, either by direct download from the Opmantek website, or from your desktop with `scp` or `sftp` or a similar file transfer tool.
Make a record of where you put the tarball (`root`'s home directory or /tmp are good locations).

- Start the interactive installer and follow its instructions:

```
sudo sh
./opFlow-Linux-x86_64-3.0.2.run

++++++++++++++++++++++++++++++++++++++++++++++++++++++
opFlow (3.0.2) Installation script
++++++++++++++++++++++++++++++++++++++++++++++++++++++

This installer will install opFlow into /usr/local/omk.
To select a different installation location please rerun the
installer with the -t option.
...
```

- The installer will interactively guide you through the steps of installing opFlow. Please make sure to read the on-screen prompts carefully.
- When the installer finishes, opFlow is installed into `/usr/local/omk`, and the default configuration files are in `/usr/local/omk/conf`, ready for your initial config adjustments.
- A detailed log of the installation process is saved as `/usr/local/omk/install.log`, and subsequent upgrades or installations of other Opmantek products will add to that logfile.
- For detailed information about the interactive installer please check the Opmantek Installer page.

Initial Configuration

After installation you may need/want to change the directories that flows are stored in, the ports the flows are coming in on, etc. Please read the sections below for more.

nfdump

On most platforms nfdump uses the classic init script /etc/init.d/nfdump, normally accessed via the `service` helper, e.g. `service nfdump stop` or `start`
.
The init script contains defaults for the most essential options for the `nfdump`/`nfcapd` programs.

It is recommended that you *do not modify* this init script, as upgraded nfdump packages may very well replace it.

Instead you should make use of the override file that is appropriate for your platform, and add values for (only) those options that you want to change.

On CentOS/RedHat, you need to create or modify `/etc/sysconfig/nfdump`, on Debian/Ubuntu the correct file is `/etc/default/nfdump`. Please note that this override file wins over the defaults that the init script sets.

Here is a list of the defaults as provided by the init script:

```
# best way to configure these is via /etc/default/nfdump or /etc/sysconfig/nfdump,
# DATA_BASE_DIR needs to be the same as "<opflow_dir>" in opCommon.nmis
DATA_BASE_DIR="/var/lib/nfdump"
DATA_ROTATE_INTERVAL=300
NETFLOW_PORT=9995
PIDFILE=/var/run/$NAME.pid
```

To to change port and spool directory to your preferred settings, edit `/etc/sysconfig/nfdump` rsp. `/etc/default/nfdump` so that it contains the following entries:

```
# non-standard config settings for nfdump
# this directory was used by opFlow 2.X
DATA_BASE_DIR=/data/opflow
NETFLOW_PORT=12345
```

When that's done, you need to restart the `nfdump` service to activate your configuration: `sudo service nfdump restart`.

Additional required steps If your OS is Debian or Ubuntu, and you are using systemd:

The most recent nfdump packages in Debian come with a problematic systemd service file (see bug Debian Bug 843602) which completely ignores /etc/default/nfdump.
Until that is resolved, we recommend that you disable the nfdump systemd service and have the system fall back to using sysv init scripts, combined with the nfdump init script that was shipped with opFlow (which is available as `/usr/local/omk/install/nfdump.init.d`).

A symptom of that issue would be that `nfcapd` is running with data directory `/var/cache/nfdump`, is listening on a port that is neither 9995 nor your NETFLOW_PORT from /etc/default/nfdump, does not include the "`-T all`" argument to enable netflow extensions, and does not include the `-t` argument for data rotation.

```
ps ax|fgrep nfcapd
# good: that one honours custom settings as it should
1583 ?        S      0:47 /usr/bin/nfcapd -D -T all -l /data/opflow -t 120 -P /var/run/nfcapd.pid -p 12345
# BAD: that's an nfcapd with undesireable hardcoded arguments
1257 ?        S      0:00 /usr/bin/nfcapd -D -l /var/cache/nfdump -P /var/run/nfcapd.pid -p 2055
```

The forced switch to SysV init script can be made by running the following commands as `root` (ie. under `sudo bash` or the like):

```
service nfdump stop
dpkg-divert --rename --divert /lib/systemd/system/nfdump.service.disabled --add /lib/systemd/system/nfdump.service
rm -f /etc/systemd/system/nfdump.service /etc/systemd/system/multi-user.target.wants/nfdump.service
systemctl daemon-reload
# note that this will only work fully if you use the nfdump init script from /usr/local/omk/install/nfdump.init.d!
service nfdump start
```

opCommon

The following changes can be made in the opCommon configuration file /usr/local/omk/conf/opCommon.nmis

opflowd/ndfump

It is **important** that the <opflow_dir> in opCommon.nmis matches the DATA_BASE_DIR in the nfdump configuration

```
    '<opflow_dir>' => '/data/opflow', # or '/var/lib/nfdump' to match the default shipping config
```

opCharts/NMIS integration

NMIS integration enables the resolution of Interface indexes to Interface Names. The association to an NMIS node enables opFlow to look up the interface indexes which the traffic is flowing to and from. Note the agents are a list of the IP addresses from which flows are received. opFlow will automatically update Agent->Node links once an hour, at this time interface information will also be updated, the update can also be triggered from the GUI using System->Sync Agent/Node Data. Associating to an NMIS node enables opFlow to look up the interface indexes which the traffic is flowing to and from.

Linking with opCharts/NMIS can be done to an NMIS instance on the same server (Local) or can integrate to a remote instance of opCharts. If you are running opCharts3 as the remote it must not be a Primary instance it must be a normal poller instance. If you are running opCharts4 the remote server can be a poller or a Primary.

If you are linking to a local omkd **do not** use a remote connection.

Local NMIS integration

If the config setting 'opflow_opcharts_url_base' is left blank, opFlow will attempt to load node information from a local NMIS server found at 'nmis_dir' => '/usr/local/nmis8'

Remote NMIS/opCharts integration

Remote integration requires setting 3 config items, these are used so the opFlow server can access an opCharts server. When this is working the GUI will show ifDescr and Descriptions in the agent selector, and when filtering on an agent/interface will display the interface info panel.

The two servers must have the same value for <omk_url_base> (which is not often changed)

```
# NOTE: no trailing slash
'opflow_opcharts_url_base' => "http://someserver.tld", # base for omk, do not connect to localhost this way, use local nmis integration
'opflow_opcharts_user' => "nmis",      # needs ro-access
'opflow_opcharts_password' => "nm1888",
```

High volume settings

There are two high volume controls for opFlow, one for the backend and one for the frontend.

```
'opflow_high_volume' => 1,
'opflow_gui_high_flow_volume' => 1,
'opflow_gui_no_flows_over_time_graph' => 1,
'opflow_gui_display_other' => 0,
```

opflow_high_volume will cause opflowd to insert pre-aggregated flows if set, raw flows if not. Currently the GUI has no way of displaying raw flows so this is enabled by default.

opflow_gui_high_flow_volume will force the GUI to show a simplified/optimized index page, it can also be viewed by setting ?simple=1 on the index page, it is enabled by default.

opflow_gui_no_flows_over_time_graph will remove the flows over time graph from the index page, this is off by default.

opflow_gui_display_other tells opFlow if all flows outside of the TopN should be summarised into an "other" entry, this is off by default

Graph display settings

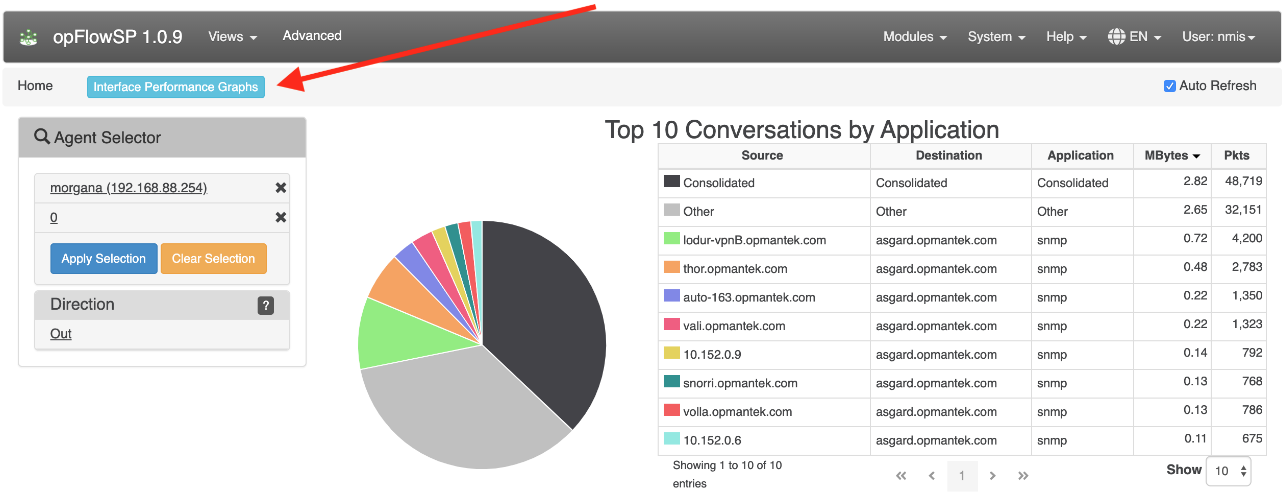
The graph that show flows over time can display 2 modes: the default shows the number of octets/packets in the current time slice, the second mode makes the graph display the data in octets/second or packets/second. To enable the second mode change the following config variable to 1:

```
         'opflow_gui_graph_over_time_per_sec' => 1
```

opFlowSP 1.0.9 introduced 3 new configuration items:

```
      'opflow_gui_hide_interface_performance_graphs' => 0,
      # Custom agent button
      #'opflow_gui_agent_custom_button_text' => 'Button Text',
      #'opflow_gui_agent_custom_button_url' =>'https://example.com/omk/opCharts/inventory/interfaces',
```

opflow_gui_hide_interface_performance_graphs is used to hide or show the button "Interface Performance Graphs". Default is 0 to show the button. Set to 1 to hide the button.



Top 10 Conversations by Application

Source	Destination	Application	MBytes	Pkts
Consolidated	Consolidated	Consolidated	2.82	48,719
Other	Other	Other	2.65	32,151
lodur-vpnB.opmantek.com	asgard.opmantek.com	snmp	0.72	4,200
thor.opmantek.com	asgard.opmantek.com	snmp	0.48	2,783
auto-163.opmantek.com	asgard.opmantek.com	snmp	0.22	1,350
vali.opmantek.com	asgard.opmantek.com	snmp	0.22	1,323
10.152.0.9	asgard.opmantek.com	snmp	0.14	792
snorri.opmantek.com	asgard.opmantek.com	snmp	0.13	768
volla.opmantek.com	asgard.opmantek.com	snmp	0.13	786
10.152.0.6	asgard.opmantek.com	snmp	0.11	675

Showing 1 to 10 of 10 entries

Show 10

opflow_gui_agent_custom_button_text and opflow_gui_agent_custom_button_url are set together to add a button with a custom link to be visible to the right of "Interface Performance Graphs".

Possibility to set the octet format to MegaBytes (MB) or Megabits (Mbits) using the configuration item opflow_gui_octet_display_multiplier.

```
     'opflow_gui_octet_display_multiplier' => 0.000000953674316,
     'opflow_gui_octet_display_multiplier' => 0.000008,
```

Restart the daemons

After making changes to the config make sure to restart all opFlow daemons.

```
service nfdump restart
service omkd restart
service opflowd restart
```

Configuring your Flow exporters

A basic router configuration guide for exporting flow data is available here.

DNS

opFlow attempts to resolve all ip address so DNS settings must be correct. Be sure to verify that DNS settings are appropriate:

```
cat /etc/resolv.conf
# verify the  listed nameservers and search order works,
# using dig, nslookup or host
```

If you have very large numbers of distinct IP addresses in your flows you should DISABLE DNS lookup, change 'opflow_resolve_endpoint_dns' => 'true', to false in /usr/local/omk/conf/opCommon.nmis to speed up performance. Each of the opflow processes will have to wait for each of the DNS lookups which means you will have a large number processes waiting for DNS to return information. This is especially true on internet traffic as resolution will require a PTR lookup through to the SOA for that IP which could take a while.