opFlow V2 (deprecated since v3) Installation Guide

For V3 (current version) Install Guide please refer to opFlow 3 Installation Guide

- For V3 (current version) Install Guide please refer to opFlow 3 Installation Guide
  - Version 2 - Installation Prerequisites
- Version 2 - Installation Steps
- Data Storage Size
- Alternate Installation Directory
- Install flowd NetFlow Daemon
  - Install Required Packages
  - Compiling Flowd
- Install MongoDB
- Opmantek Setup for Flowd
- Opmantek Setup for MongoDB
- Installing the Opmantek License and Accepting the EULA
- opFlow Setup
- Configuring mongod on a remote server
- Starting the opFlow Daemon
- Access opFlow Web Page

Version 2 - Installation Prerequisites

- The individual performing this installation has some Linux experience.
- Free disk space
- NMIS8 is installed on the same server where opFlow will be installed
- NMIS8 is installed in /usr/local/nmis8
- opFlow will be installed into /usr/local/opmantek
- Root access is available (not always needed but much easier)
- **RRDtool 1.4.7 installed in /usr/local/rrdtool**

Version 2 - Installation Steps

- Download opFlow from the Opmantek website.
- Copy the opFlow tarball to the server (a tarball is a GZIP'd tar file, e.g. opFlow-Linux-x86_64-1.0.tar.gz)
  1. You may need to use SCP or FTP to get the file onto the server.
- The file will now likely be in the users home directory.
- If the installation directory does not already exist
- Change into the directory where the tarball was copied
- Untar the file

```
cd /usr/local
tar xvf ~/opFlow-Linux-x86_64-<version>.tar.gz
cd opmantek/
cp install/opCommon.nmis conf/
cp install/opFlow.nmis conf/
bin/opfixperms.pl
cp install/01opmantek.conf /etc/httpd/conf.d/
service httpd restart
```

Debian/Ubuntu

```
cp install/01opmantek.conf /etc/apache2/conf.d/
service apache2 restart
```

Data Storage Size

NetFlow data can get away on you, there could be several Gigabytes of NetFlow data each hour, day or month, this is all very dependant on where you are generating netflow from, the number of active users and the types of applications they are using, you will want to consider storing the MongoDB database and the NetFlow data into a filesystem with 50 gigabytes or more. During development we found 20 gigabytes was enough for our purposes, but caused problems with the flow files mainly. If you are using the Opmantek NMIS8 Virtual Machine please check out our instructions on Resizing NMIS VMs.

Size

opFlow uses fixed sizes for raw flows and conversations, when the setup tool (opflow_setup.pl) is run the database files will immediately be pre-allocated to the configured size and will never grow after this. It is important that the sizes you choose fit on the partition you choose, the setup tool will warn you if they will not fit. The default settings are: (found in /usr/local/opmantek/conf/opFlow.nmis)

```
'opflow_db_conversation_collection_size' => 16106127360, #15G
'opflow_db_flow_collection_size' => 5368709120 # 5G
```

Please adjust them appropriately before running the setup tool. (which is done later in the instructions)

The output from the setup tool may tell you to run it again after adjusting your config with force=1 (opflow_setup.pl setup=db_config force=1) # again, only if required

Location

opFlow is highly configurable and customisable, so it is easy to just have the flowd data be a seperate filesystem and update the configuration accordingly.

If you are going to use a different directory, Modify the opFlow.nmis file and edit the <opflow_dir>

```
'<opflow_dir>' => '/data/opflow',
```

Edit the file /etc/init.d/mongod and change the correct directory, look for this line

```
mongodbpath=/data/mongodb
```

Edit the file /usr/local/etc/flowd.conf, and modify the entry for logfile.

```
logfile "/data/opflow/flowd"
```

Alternate Installation Directory

opFlow can be installed into another directory if required, e.g. /opt/opmantek, the same process applies, but a few files will need to be changed.

Edit opFlow.nmis and opCommon.nmis and change the <omk_base> to be the new, e.g.

```
'<omk_base>' => '/opt/opmantek',
```

Edit the Apache include file, which if already copied to /etc/httpd/conf.d will be /etc/httpd/conf.d/01opmantek.conf and change the following lines to the new installation location

```
Alias /opmantek/ "/usr/local/opmantek/htdocs/"

ScriptAlias /cgi-omk/ "/usr/local/opmantek/cgi-bin/"

<Directory "/usr/local/opmantek/cgi-bin">
```

Install flowd NetFlow Daemon

You will need to compile the NetFlow Daemon flowd, the source code is included with opFlow.

Install Required Packages

```
yum install byacc
```

Debian/Ubuntu

```
apt-get install byacc
```

Compiling Flowd

```
cd /usr/local/opmantek/source
tar xvf flowd-0.9.1.tar.gz
cd flowd-0.9.1
./configure
make
make install
cd ../../
```

Install MongoDB

Please follow the instructions on the MongoDB Installation page to install the latest supported version of MongoDB.

Opmantek Setup for Flowd

Now that you have the binaries for flowd we have a bunch of Opmantek goodness to make it work easily. The following commands get this running

```
adduser _flowd
\cp /usr/local/opmantek/install/flowd.conf /usr/local/etc/flowd.conf
cp /usr/local/opmantek/install/flowd.init.d /etc/init.d/flowd
mkdir /usr/local/var
mkdir /usr/local/var/run
mkdir /var/opflow/
chkconfig flowd on
service flowd start
```

Debian/Ubuntu
When trying to add the _flowd user, you will get the following error message:

```
adduser: Please enter a username matching the regular expression configured
via the NAME_REGEX[_SYSTEM] configuration variable. Use the `--force-badname'
option to relax this check or reconfigure NAME_REGEX.
```

```
adduser --force _flowd
```

Debian/Ubuntu follow the LSB (Linux Standard Base) specification, init script functions be available at /lib/lsb/init-functions.

Edit /etc/init.d/flowd

```
#change this line:
. /etc/init.d/functions
#to this:
. /lib/lsb/init-functions
```

The start flowd

```
sysv-rc-conf flowd on
service flowd start
```

Opmantek Setup for MongoDB

The following commands get MongoDB running (before doing this make sure to read the section above on considerations for storage). The last command here starts MongoDB, the first time it runs it can take some time to do its pre-allocation of database and journal files. This will depend on the performance of your storage.

```
cp /usr/local/opmantek/install/mongod.init.d /etc/init.d/mongod
chkconfig mongod on
service mongod start
```

Debian/Ubuntu
Edit /etc/init.d/mongod

```
#change this line:
. /etc/init.d/functions
#to this:
. /lib/lsb/init-functions
```

The start mongod

```
sysv-rc-conf mongod on
service mongod start
```

Installing the Opmantek License and Accepting the EULA

If you haven't already obtained a commercial or evaluation license from Opmantek, now is the time to do so, this will be a license key which is an encrypted string.

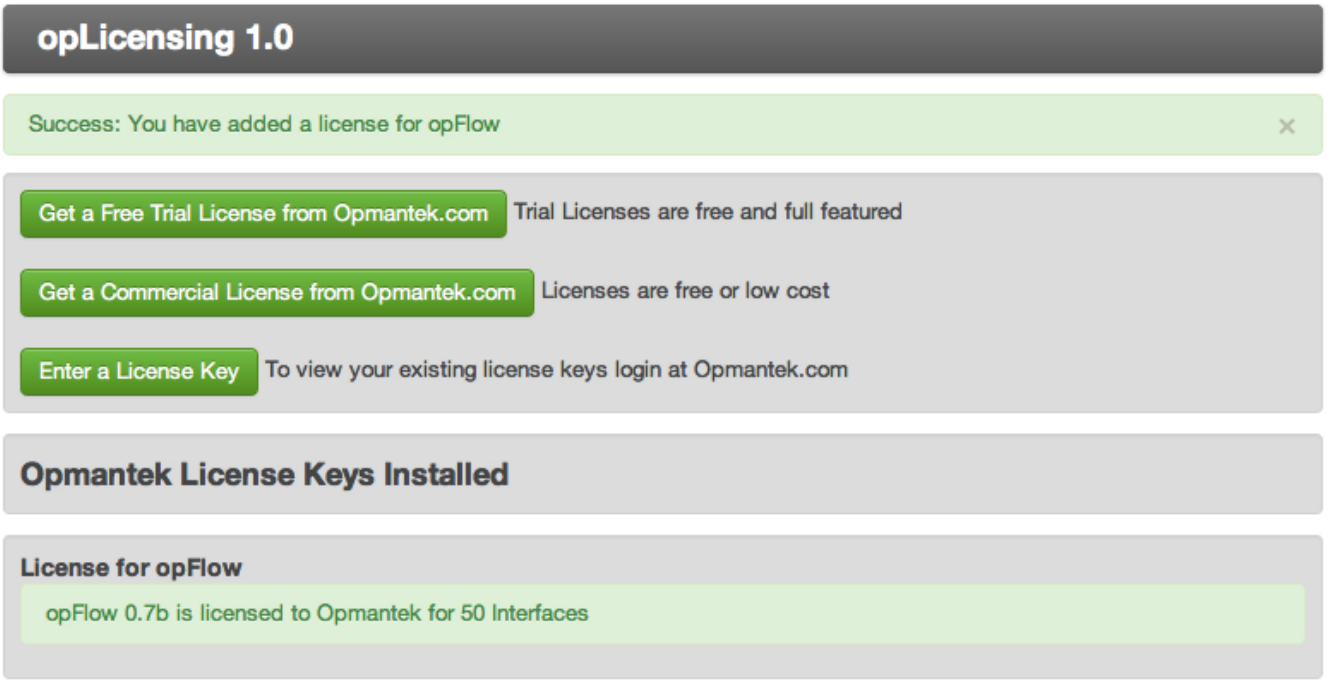
At this point you should be able to access the opFlow GUI which will be at a URL like this http://server.domain.com/cgi-omk/opFlow.pl

Access the web page and login in with your NMIS username and password, which by default is nmis/nm1888

opFlow will likely have a message like "A valid license file was not found", and there is a button "View and Enter Licenses" under it, which you should click.

If you have your license key, click on "Enter a License Key" and paste the license key into the text box and click on "Add License".

You should now see a screen which says "Success: You have added a license for opFlow"



You can return to the opFlow page a refresh it, you will be now asked to review the EULA (End User License Agreement) and click on the "Accept EULA" button at the bottom.

Once that is done, opFlow GUI will start.

opFlow Setup

To initialise the database, create the default application definitions and many more things, you will need to run opflow_setup.pl, this will also generate a crontab entries for adding to your Cron setup.

Make sure you stop/kill any mongod processes before your run these commands.

```
/usr/local/opmantek/bin/opfixperms.pl
/usr/local/opmantek/bin/opflow_setup.pl setup=all
```

You can ignore this message: "chmod: cannot access ‘/usr/local/opmantek/conf/credential_sets.nmis’: No such file or directory". The credentials_sets.nmis configuration file will not be present if the opConfig module has not been previously installed.

When the crontab entries are displayed, you can copy and paste these into crontab,

```
/usr/local/opmantek/bin/opflow_setup.pl setup=cron

#######################################################
# opFlow Cronfig
#######################################################
# Run the DNS resolution every 15 minutes
*/15 * * * * /usr/local/opmantek/bin/opflowd.pl type=endpoints
# Purge the old Flows every 24 hours
0 0 * * * /usr/local/opmantek/bin/opflowd.pl type=purge
30 0 * * * /usr/local/opmantek/bin/opflow_purge_raw_files.sh /var/opflow 7
#######################################################
# Check to rotate the logs 4:05AM every day
5 4 * * * /usr/sbin/logrotate /usr/local/opmantek/conf/oplogrotate.conf
#######################################################
# opFlow Reports
# hourly - every hour 3 minutes after the hour
3 * * * * /usr/local/opmantek/bin/opFlowReports-hourly.sh
# daily - every day at 1am
0 1 * * * /usr/local/opmantek/bin/opFlowReports-daily.sh
crontab -e

Insert the above text, then save and quit.
```

Configuring mongod on a remote server

If you not are running your mongo db server on the same server as opFlow mongo database authentication will need to be done manually.

1. Ensure mongod is not running with the --auth switch, **if you are using the mongod.init.d script included in opFlow** run:

   ```
   /etc/init.d/mongod stop;
   /etc/init.d/mongod start_no_auth;
   ```

2. Create the user, currently the opFlow user requires access to both the admin database and it's own. Start up the mongo shell and type these commands:

   ```
   use admin;
   db.addUser('opUserRW', 'op42flow42'); // these are the defaults, change them as well as your opFlow.nmis
   file
   use nmis; // again this is a default, it doesn't need to be changed
   db.addUser('opUserRW', 'op42flow42'); // these are the defaults, change them as well as your opFlow.nmis
   file, it should match the above user command
   ```

3. Restart the mongo server with authentication, --auth (again, only if you are using the mongod.init.d script included in opFlow)

   ```
   /etc/init.d/mongod stop;
   /etc/init.d/mongod start;
   ```

Starting the opFlow Daemon

With the license now installed, we can complete the setup of opFlow.

```
cp /usr/local/opmantek/install/opflowd.init.d /etc/init.d/opflowd
chkconfig opflowd on
service opflowd start
```

Debian/Ubuntu
Edit /etc/init.d/opflowd

```
#change this line:
. /etc/init.d/functions
#to this:
. /lib/lsb/init-functions
```

The start opflowd

```
sysv-rc-conf opflowd on
service opflowd start
```

Access opFlow Web Page

The default URL to access opFlow is http://nmis.domain.com/cgi-omk/opFlow.pl

Any authentication challenges will be the same as to login to your NMIS8 system.