Contents

NetFlow - PortTracker Exercises

1 Optional Tasks

1.1 Installing the PortTracker plugin (Optional or as reference)

This exercise assumes you already built nfdump from source with options `--enable-nfprofile` and `--enable-nftrack`, with nftrack installed under /usr/local/bin. If not, see exercise2-install-nfdump-nfsen.

- Make a directory for the nftrack data

```
$ sudo mkdir /var/ports-db
$ sudo chown netflow /var/ports-db
```

- Set the nftrack data directory in the PortTracker.pm module (which is under the nfsen source)

```
$ cd
$ cd nfsen-1.3.6p1/contrib/PortTracker
$ editor PortTracker.pm

    Find the line:

my $PORTSDBDIR = "/data/ports-db";

    and change it to:

my $PORTSDBDIR = "/var/ports-db";
```

Save and exit from the file.

- Install the plugin into the NFSen distribution

```
$ sudo cp PortTracker.pm /var/nfsen/plugins/
$ sudo cp PortTracker.php /var/www/nfsen/plugins/
```

- Add the plugin definition to the nfsen.conf configuration

```
$ cd /var/nfsen/etc
$ sudo editor nfsen.conf
```

- Find the plugins section and make it look like this:

```
@plugins = (
   [ 'live', 'PortTracker'],
);
```

Save and exit from the file.

- Initialize the PortTracker database files

```
$ sudo -u netflow nftrack -I -d /var/ports-db
```

(This can take a LONG time! - 8 GB worth of files will be created)

- Set the permissions so the netflow user running nfsen, and the www-data user running the Web interface, can access the porttracker data.

```
$ sudo chown -R netflow:www-data /var/ports-db
$ sudo chmod 775 /var/ports-db
$ sudo chmod 664 /var/ports-db/*
```

- Restart NfSen

```
$ sudo service nfsen reload
```

- Check for success:

```
$ grep -i 'porttracker.*success' /var/log/syslog
Oct 12 13:19:35 pc1 nfsen[28005]: Loading plugin 'PortTracker': Success
Oct 12 13:19:35 pc1 nfsen[28005]: Initializing plugin 'PortTracker': Success
```

- Wait some minutes, and go the the nfsen GUI

```
http://pcX.ws.nsrc.org/nfsen/nfsen.php
```

... and select the Plugins tab.

> You may get an error that "No plugins available!": if so, quit and re-start your browser.
>
> You may get "Error reading stat". You will need to wait a few minutes before NfSen will begin to show the graphs.

At this point you are done. Congratulations!

1.2 Troubleshooting

If you get "Error reading stat", check the /var/ports-db directory for 2 additional files: portstat24.txt and portstat.txt like this:

```
$ ls -l /var/ports-db/portstat*
-rw-r--r-- 1 netflow www-data     512 Jul 17 21:20 /var/ports-db/portstat24.txt
                                                   /var/ports-db/portstat.txt
```

If either is missing then this will cause the problem. Make sure that nfsen can write in that directory.

You can get additional debugging by setting `$DEBUG = 1` in /var/www/nfsen/conf.php, and then looking in /var/tmp/nfsen.log