

NetFlow - PortTracker Exercises

Optional Tasks

Installing the PortTracker plugin (Optional or as reference)

First, connect to your virtual machine and become root:

```
~~~~~  
ssh sysadm@pcN.ws.nsrc.org  
$ sudo bash  
#  
~~~~~
```

We have installed the nfdump package, but we still need to get the source package, as it contains extra files required to enable PortTracker.

```
~~~~~  
# cd /usr/local/src  
# wget http://noc.ws.nsrc.org/downloads/nfdump-1.6.6.tar.gz  
# tar xvzf nfdump-1.6.6.tar.gz  
# cd nfdump-1.6.6  
~~~~~
```

* Make a directory for the nftrack data

```
~~~~~  
# mkdir -p /var/log/netflow/porttracker  
# chown www-data /var/log/netflow/porttracker  
~~~~~
```

* Set the nftrack data directory in the PortTracker.pm module:

```
~~~~~  
# editor extra/PortTracker.pm
```

Find the line:

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

and change it to:

```
my $PORTSDBDIR = "/var/log/netflow/porttracker";  
~~~~~
```

Save and exit from the file.

* Install the plugin into the NfSen distribution

```
~~~~~  
# cp extra/PortTracker.pm /var/nfsen/plugins/  
~~~~~
```

* Add the plugin definition to the nfsen.conf configuration

```
~~~~~  
# cd /var/nfsen/etc  
# editor etc/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 www-data nftack -I -d /var/log/netflow/porttracker
~~~~~
```

(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.

```
~~~~~
# chown -R netflow:www-data /var/log/netflow/porttracker
# chmod -R 775 /var/log/netflow/porttracker
~~~~~
```

* Restart NfSen

```
~~~~~
# service nfsen stop
# service nfsen start
~~~~~
```

* 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 to the nfsen GUI

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

... and select the Plugins tab.

```
*****
* You may get an error that "No plugins installed!" or
* "Error reading stats"...
*
* Don't worry, you need to wait a few minutes before NfSen will begin to
* show the PortTracker plugin and its graphs.
*****
```

At this point you are done. Congratulations!

Troubleshooting

If you get an error "Cannot Read Stats file", check the /var/log/netflow/porttracker \ directory for 2 additional files: portstat24.txt and portstat.txt like this:

```
~~~~~  
# ls -l /var/log/netflow/porttracker/portstat*  
-rw-r--r-- 1 netflow www-data      677 2011-11-17 14:30 /var/log/netflow/\  
porttracker/portstat24.txt  
-rwxrwxr-x 1 netflow www-data      638 2011-11-17 14:30 /var/log/netflow/\  
porttracker/portstat.txt  
~~~~~
```

Make sure that nfsen can write in that directory.