Purpose

This document describes how to choose, install, and configure netflow exporters for Windows operating systems.

Target Audience

This document is intended for use by admins looking to collect netflow information from Windows workstations and servers.

Choosing An Exporter

An exporter is a third party application that will send netflow data from your Windows machine to your Nagios Network Analyzer server. There are a number of different exporters available for Windows. Unfortunately, most are commercial offerings only and the few free options have a number of known issues. If you have any suggestions for other flow exporters for Windows, please open a thread at http://support.nagios.com/forum/ to let us know! The current options are:

- nProbe
  - http://www.ntop.org/products/netflow/nprobe/
  - Trial allows for 25,000 flow exports
  - Download the latest nprobe-x64-x.x.x.zip package from: http://packages.ntop.org/Windows
  - Only Windows x64 version is supported
- FlowTraq Flow Export
  - https://www.flowtraq.com/product/flow-exporter/
  - This website requires registration before the download link is available
  - The demo does not have any restrictions, but requires it to be licensed for commercial / production use
  - Requires WinPcap to be installed on Windows, available here: http://www.winpcap.org/

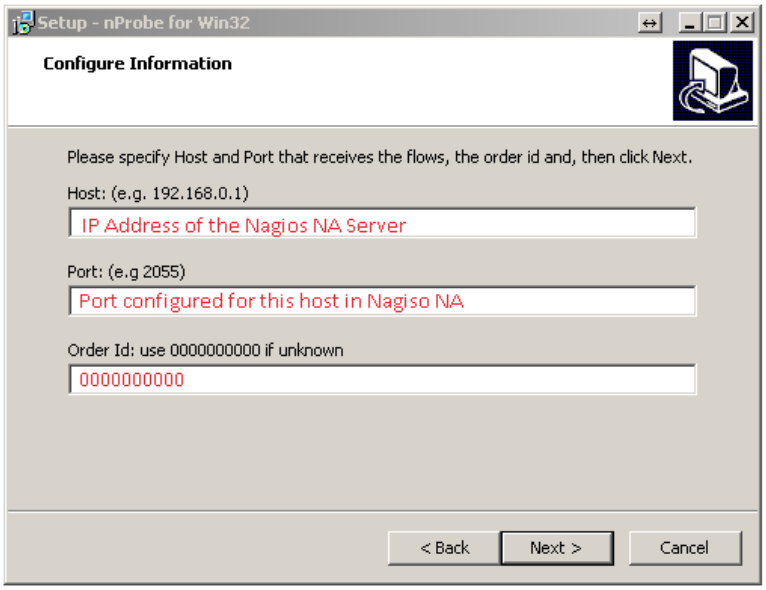
Network Analyzer Source

When you install nProbe or FlowTraq you will be required to provide the network port that the Nagios Network Analyzer server will be listening on. This assumes you already have a Source created for this traffic. Please refer to the following documentation on creating a source:

Understanding Sources And Source Groups In Network Analyzer

Installing nProbe

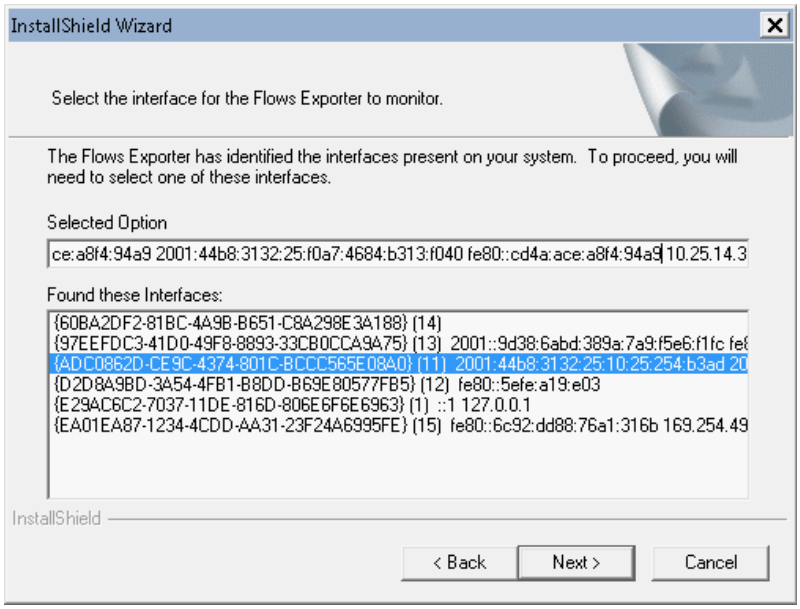
- Download nProbe and run the installer
- Enter the necessary setup information:
  - **Host:** The ip address of your Nagios Network Analyzer server
  - **Port:** The port the Nagios Network Analyzer server is listening for flow data, as configured in the source
  - **Order ID:** Use 10 zeros: `0000000000`
- Finish up the Installation, the default options should be fine from this point onward. You may be prompted to install additional libraries, please install these as well.



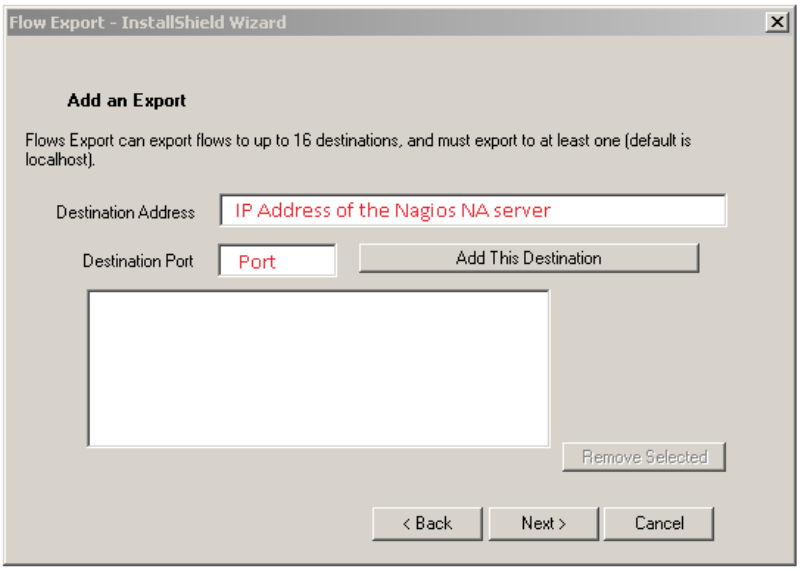
- Open `services.msc` and start the nProbe service
  - If the nProbe service cannot be located, run the install again and it should exist after the second attempt.

Installing FlowTraq Flow Export

- Install WinPcap first, accept all defaults
- Run the Flow Export installer, accept the EULA, default locations and then click Install
- Choose the interface from which to collect flows
  - There will be a number to choose from and if you have IPv6 it may be hard to determine the right adapter.
  - The easiest way to identify which interface is to select an interface in the bottom window and then click the selected field at the top. Press **End** on your keyboard and the IPv4 address will be at the end of the field.



- Now you need to add the details of your Nagios Network Analyzer server
  - **Destination Address:** The ip address of your Nagios Network Analyzer server
  - **Destination Port:** The port the Nagios Network Analyzer server is listening for flow data, as configured in the source
  - Click the **Add This Destination** button
  - Click Next and finish the installation
  - A new service called ProQueSys Flow Export has been created and will have been started



Check Flow Data

It can take about minutes before the netflow data will appear under your source in Nagios Network Analyzer. If you want to confirm the data is being received you can use the `tcpdump` program. To do this, establish a terminal session to your Nagios Network Analyzer server.

Install `tcpdump` with this command:

```
yum install -y tcpdump
```

Watch the network traffic with this command:

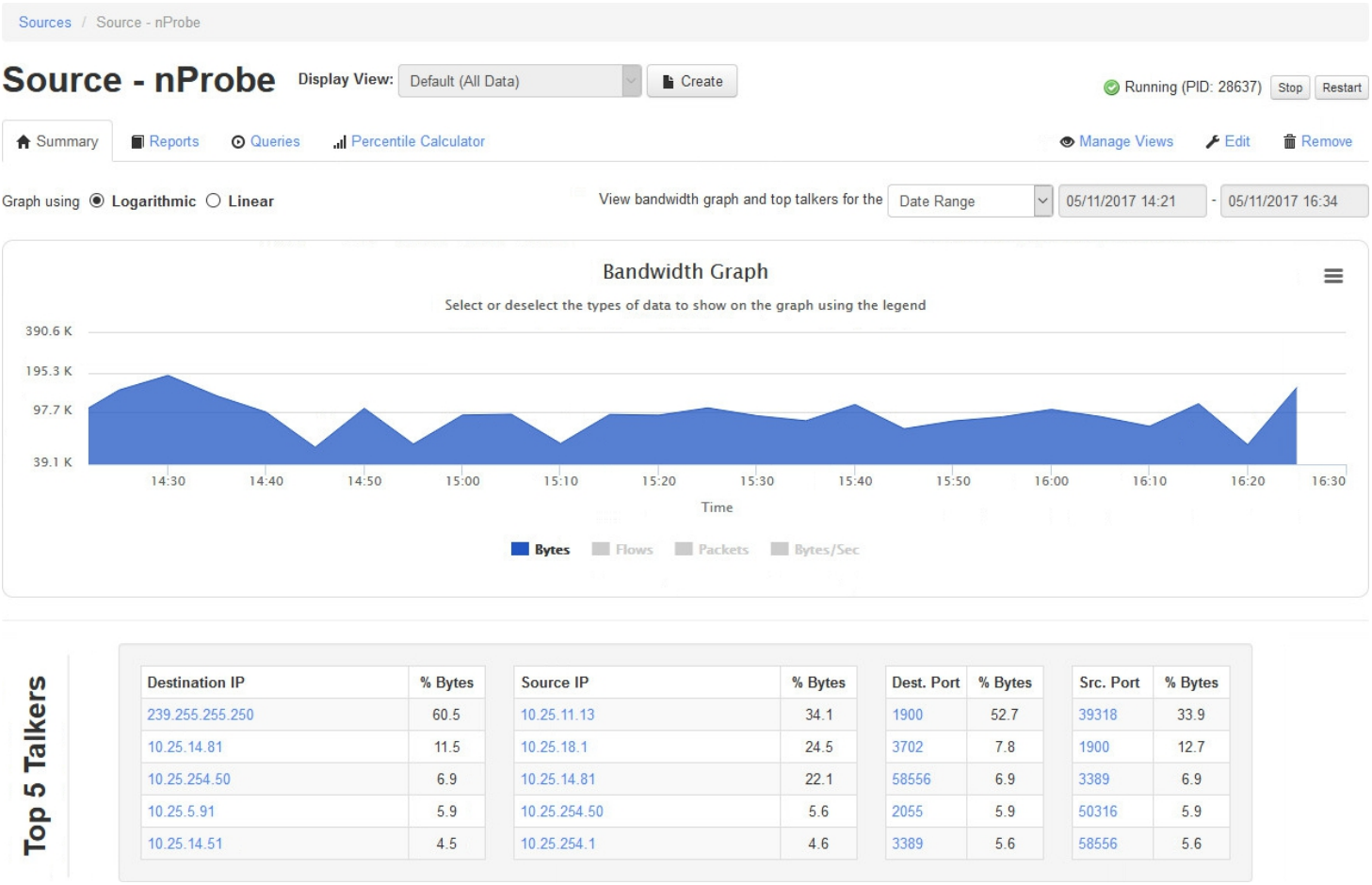
```
tcpdump -nnvvS -i eth0 src host 10.25.14.81 and dst host 10.25.5.91
```

You will need to change `-i` to the network interface to listen on and the `src host` and `dst host` addresses relevant to your situation. You should see traffic come in that looks something like:

```
15:11:09.212599 IP (tos 0x0, ttl 128, id 17861, offset 0, flags [none], proto
UDP (17), length 532)
    10.25.14.81.50316 > 10.25.5.91.2055: [udp sum ok] UDP, length 504
15:11:18.050608 IP (tos 0x0, ttl 128, id 17864, offset 0, flags [DF], proto UDP
(17), length 1492)
    10.25.14.81.50316 > 10.25.5.91.2055: [udp sum ok] UDP, length 1464
15:11:20.090137 IP (tos 0x0, ttl 128, id 17865, offset 0, flags [DF], proto UDP
(17), length 1492)
    10.25.14.81.50316 > 10.25.5.91.2055: [udp sum ok] UDP, length 1464
```

You can see the port the traffic is coming in on is 2055, which is what was configured on the Windows machine and matches the source that was created in Nagios Network Analyzer.

The following screenshot is an example of the netflow data received in Nagios Network Analyzer. It will take at least five minutes for enough data to be collected before you see data for the source appear.



Top 5 Talkers

Destination IP	% Bytes	Source IP	% Bytes	Dest. Port	% Bytes	Src. Port	% Bytes
239.255.255.250	60.5	10.25.11.13	34.1	1900	52.7	39318	33.9
10.25.14.81	11.5	10.25.18.1	24.5	3702	7.8	1900	12.7
10.25.254.50	6.9	10.25.14.81	22.1	58556	6.9	3389	6.9
10.25.5.91	5.9	10.25.254.50	5.6	2055	5.9	50316	5.9
10.25.14.51	4.5	10.25.254.1	4.6	3389	5.6	58556	5.6

Finishing Up

This completes the documentation on installing and configuring netflow exporters for Windows.

If you have additional questions or other support related questions, please visit us at our Nagios Support Forums:

https://support.nagios.com/forum

The Nagios Support Knowledgebase is also a great support resource:

https://support.nagios.com/kb