PNNL-SA-120800
PNNL-18428, Rev. 4

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

FLOWER Installation Guide

FLOWER Version 06 (flr06)

October 2017

DS Curtis

U.S. DEPARTMENT OF ENERGY

Prepared for the U.S. Department of Energy
under Contract DE-AC06-76RL01830
with Battelle Memorial Institute

DISCLAIMER

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
email: orders@ntis.gov <http://www.ntis.gov/about/form.aspx>
Online ordering: http://www.ntis.gov

This document was printed on recycled paper.
(8/2010)

PNNL-SA-120800
PNNL-18428, Rev. 4

FLOWER Installation Guide

DS Curtis

October 2017

Prepared for
the U.S. Department of Energy
under Contract DE-AC06-76RL01830
with Battelle Memorial Institute

Pacific Northwest National Laboratory
Richland, Washington 99352

Acknowledgments

 PNNL-SA-120800

Battelle IPID: 17042-E

Prime Contract No.: DE-AC06-76RL01830 with Battelle Memorial Institute

Acronyms and Abbreviations

FLOWER	FLOW analyzer
GCC	GNU Compiler Collection
pcap	packet capture files
PNNL	Pacific Northwest National Laboratory

Contents

1.0 Introduction

The FLOWER (FLOW analyzER) application is designed to start at boot time from as a Linux systemd service running on RedHat 7.x, CentOS 7.x, or Ubuntu 16.04 to summarize network flows. FLOWER can also be used to read packets from a network interface or from packet capture (pcap) files that can be processed with the libpcap system library.

2.0 System Requirements

2.1 Hardware Requirements

The minimum and recommended hardware requirements outlined here are based on a typical small to medium sized installation. The exact requirements vary between deployments based on network traffic load.

Resource	Minimum	Recommended
CPU	Intel i3	Intel i7
Memory	4 GB of system RAM	16 GB of system RAM
Hard Disk	50 GB of locally accessible, writable, disk space	250 GB of locally accessible, writable, disk space
Network Interface	1 Network Interface Card (NIC) with bandwidth of at least 1 Gbps	1 Network Interface Card (NIC) with bandwidth of 10-40 Gbps

2.2 Operating System Requirements

FLOWER runs on Linux operating systems and versions using systemd.

Linux	Version
CentOS	7.x
RedHat	7.x
Ubuntu	16.04

NOTE: In general, FLOWER will not run on a Linux system where selinux is enabled.

2.3 External Library Requirements

FLOWER is a dynamically linked executable that requires external libraries to run.

Library	Version
GNU C++ runtime	5.3 for RedHat and CentOS
	5.4 for Ubuntu
BOOST C++ libraries	1.60 (or higher) for RedHat and CentOS
	1.58 for Ubuntu
PCAP development library	1.5 (or higher) for RedHat and CentOS
	0.8 (or higher) for Ubuntu

2.4 GNU C++ Runtime Libraries on RedHat of CentOS 7.x

To get the GNU C++ runtime libraries on your RedHat/CentOS systems you can use one of the following options:

- Install the `gcc-5.3-0.x86-64.rpm` that comes with the FLOWER rpm:
  ```
  # rpm –i gcc-5.3-0.x86-64.rpm -y
  ```

- Follow the instructions in Appendix A of the FLOWER_Build_Guide_FLR06.pdf to install the libraries in the directory, `/usr/local/gcc`.

2.5 GNU C++ Runtime Libraries on Ubuntu 16.04

To get the GNU C++ runtime libraries on your Ubuntu systems you can use one of the following options:

- Install GNU C++ from your Ubuntu repository:
  ```
  # apt-get install gcc-5 g++-5 -y
  ```

- Follow the instructions in Appendix A of the FLOWER_Build_Guide_FLR06.pdf to install the libraries in the directory `/usr/local/gcc`.

2.6 BOOST Runtime Libraries on RedHat of CentOS 7.x

To get the BOOST runtime libraries on your RedHat/CentOS systems you can use one of the following options:

- Install the `boost-1.60-0.x86-64.rpm` that comes with the FLOWER rpm:
  ```
  # rpm –i boost-1.60-0.x86-64.rpm -y
  ```

- Follow the instructions in Appendix B of the FLOWER_Build_Guide_FLR06.pdf to install the libraries in the directory, `/usr/local/boost`.

2.7 BOOST Runtime Libraries on Ubuntu 16.04

To get the BOOST runtime libraries on your Ubuntu systems you can use one of the following options:

- Install GNU C++ from your Ubuntu repository:
  ```
  # apt-get install libboost-all-dev –y
  ```

- Follow the instructions in Appendix B of the FLOWER_Build_Guide_FLR06.pdf to install the libraries in the direction, `/usr/local/boost`.

2.8 PCAP Development Libraries on RedHat of CentOS 7.x

To get the PCAP development libraries on your RedHat/CentOS systems you can run the following:

- Install the `libpcap-devel package`
  ```
  # rpm –i libpcap-devel -y
  ```

2.9 PCAP Development Libraries on Ubuntu 16.04

To get the PCAP development libraries on your Ubuntu systems you can run the following:

- Install libpcap-dev from your Ubuntu repository:
  ```
  # apt-get install libpcap-dev -y
  ```

NOTE: Because Ubuntu does not have a version 1.0 of the shared object file for libpcap.so, we need to create one with the following command:

```
# ln –s /usr/lib/x86_64-linux-gnu/libpcap.so \
        /usr/lib/x86_64-linux-gnu/libpcap.so.1
```

3.0 Install FLOWER

3.1 Install FLOWER

By default, FLOWER will be installed in the directory, `/opt/flower`, where:

- binaries located in `/opt/flower/bin`
- libraries located in `/opt/flower/lib`
- the configuration file will be `/opt/flower/conf/flower.conf`
- data files will be generated in `/opt/flower/data`

3.1.1 Install FLOWER on RedHat of CentOS 7.x

To get the PCAP development libraries on your RedHat/CentOS systems you can run the following:

```
# rpm –i flower-6.0-0.x86-64.rpm –y
```

To install FLOWER in a directory other than /opt/flower you can use the relocate option with the rpm command to install FLOWER in another directory. If you would like to install FLOWER in /usr/local/flower you can run the following:

```
# rpm –r /usr/local/flower –i flower-6.0-0.x86-64.rpm –y
```

3.1.2 Install FLOWER on Ubuntu 16.04

To get the PCAP development libraries on your RedHat/CentOS systems you can run the following:

```
# dpkg -i flower_6.0-0_amd64.deb -y
```

3.2 Install FLOWER systemd Service

For FLOWER to start collecting data from a network interface, you need to configure the software to tell the flower binary which network interface to use and to start up the systemd service. If you installed FLOWER in the default location, `/opt/flower`, then you would run the following command as the root user or using `sudo`:

```
# /opt/flower/bin/create-flower-config.sh
```

NOTE: If you installed FLOWER in another directory, you will have to adjust the command above.

The create-flower-config.sh script will prompt you for the network interface to collect data from (e.g. `eth0`) and the sitename (e.g. the name you want for this installation of FLOWER software to write in each output file).

The script will create the /opt/flower/conf/flower.conf file, enable the flower as a daemon, enable the flower service, and start the flower software.

NOTE: If you make changes to the flower.conf file, you will need to restart the flower daemon and flower software.

4.0 Configure FLOWER After Installation

4.1 Configuring FLOWER

Please refer to the FLOWER_Ops_Guide_FLR06 document on how to configure and run the flower binary.

5.0 Disable Operating System and Hardware Optimizations

5.1 Disable Operating System and Hardware Optimizations

Newer versions of Linux have the ability to take advantage of Network Interface Card (NIC) optimizations such as TCP Segmentation Offload (TSO), Large Send Offload (LSO), and Generic Segmentation Offload (GSO). There is a good explanation of these NIC optimizations and how they work at LoveMyTool.com.

If you know you will be running FLOWER on interfaces on your system that have TSO, LSO, and GSO capabilities you will see errors in `/var/log/messages` so you will want to disable these optimizations.

5.2 Disable Network Optimizations on RedHat of CentOS 7.x

To disable the networking optimizations, you can add the following line to the file, `/etc/sysconfig/network-scripts/ifcfg-<interface_name>:`

```
ETHTOOL_OPTS="-K ${DEVICE} rx off tx off sg off tso off ufo off gso
off gro off lro off rxvlan off txvlan off ntuple off rxhash off"
```

5.3 Disable Network Optimizations on Ubuntu 16.04

To disable the networking optimizations, you can add the following line to the file, `/etc/network/interfaces:`

```
pre-up /sbin/ethtool –K <interface_name> rx off tx off sg off tso off
ufo off gso off gro off lro off rxvlan off txvlan off ntuple off
rxhash off
```

6.0 Troubleshooting

6.1 FLOWER is not producing any files

If the flower process is not producing files but is still running, there are a few things you can do to find out what might be wrong. If the --use-ring=1 command line or configuration file option is being used then files should always be produced even if there are no packets on the wire.

Find out how many system resources `flower` is being used with the following commands:

```
ps --no-heading -C flower
lsof -p `ps --no-heading -C flower | awk '{print $1}'`
free –mt
grep flower /var/log/messages*
```

Find the raw packets that might have caused the problem by creating a pcap file in the output directory using the command:

```
kill -SIGSEGV $(ps --no-heading -C flower | awk '{print $1}')
```

You can use Wireshark to analyze any `*.pcap` files left in the FLOWER data directory that was specified in the `flower.conf` file or specified as a command line option.

6.2 FLOWER is producing warning messages

Refer to section 5.0 for disabling optimizations if FLOWER is producing error messages in `/var/log/messages` that look like the following:

```
Oct 23 03:36:00 host flower: FATAL ERROR:
Oct 23 03:36:00 host flower: File:
./include/PacketParser.hpp(line:832)
Oct 23 03:36:00 host flower: Class:  PacketParser
Oct 23 03:36:00 host flower: Function:  setTotalBytes
Oct 23 03:36:00 host flower: Message:  Error Code=RangeError
Oct 23 03:36:00 host flower: Adjust TotalBytes
Oct 23 03:36:00 host flower: Expected total bytes (2863) to be less
than or equal to bytes on the wire (1982)
```

7.0 Reporting Bugs

Please submit bug reports to `flower-support@pnnl.gov` and include as much information as possible to describe the problem.

Please include the output from the commands in the "Troubleshooting" section and the output from `flower -v` up to the copyright message. For example:

```
network packet FLOW analizER (flower)

flower version:           5.1.0
Compiled on:              Jun  9 2017, 14:38:43 (1497044321)
Compiled with:            gcc version 5.3.0 (GCC)
  Optimize Level:         -O3
  Debug:                  -g
  Boost library version:  /usr/local/boost
  pcap  library version:  libpcap version 1.5.3
  Data Guide version:       flr06
```

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by **Battelle** *Since 1965*

U.S. DEPARTMENT OF
ENERGY

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99352
1-888-375-PNNL (7665)

www.pnnl.gov