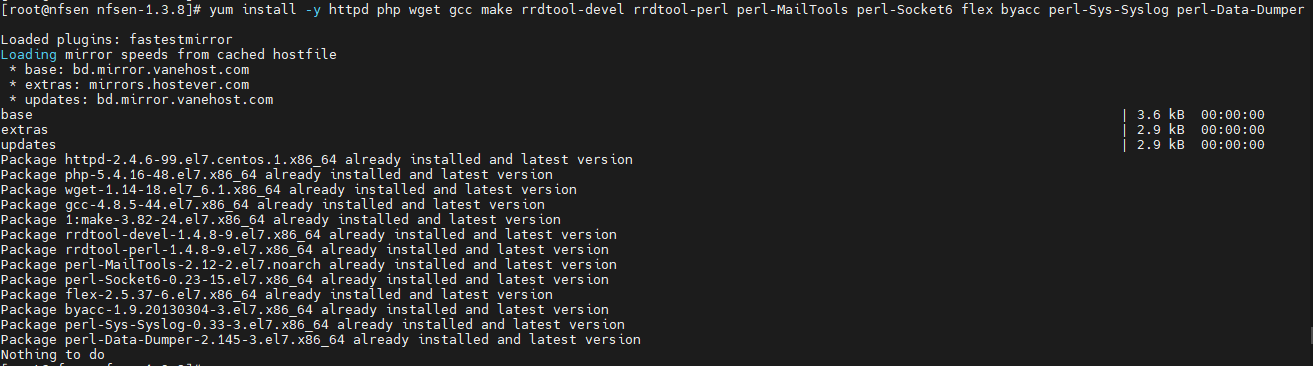
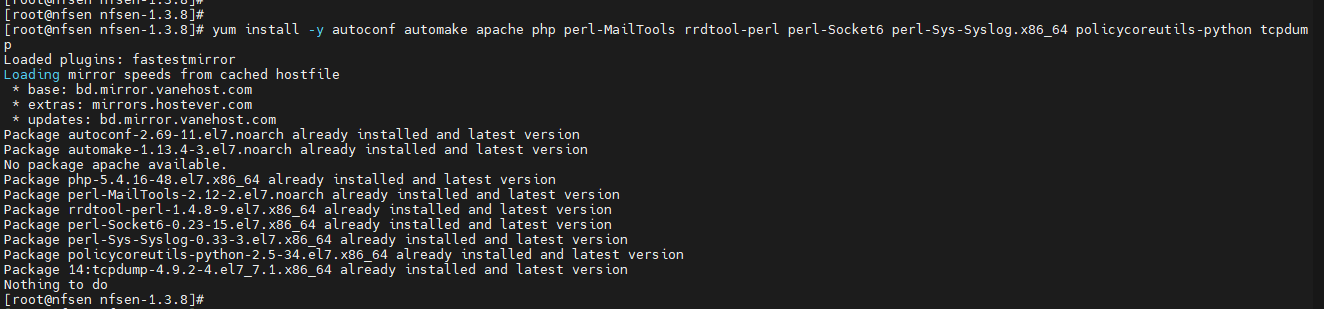
[root@nfsen nfsen-1.3.8]# yum install -y httpd php wget gcc make rrdtool-devel rrdtool-perl perl-MailTools perl-Socket6 flex byacc perl-Sys-Syslog perl-Data-Dumper



[root@nfsen nfsen-1.3.8]# yum install -y autoconf automake apache php perl-MailTools rrdtool-perl perl-Socket6 perl-Sys-Syslog.x86\_64 policycoreutils-python tcpdump



[root@nfsen nfsen-1.3.8]# echo "date.timezone = Asia/Dhaka" > /etc/php.d/timezone.ini yum update -y

[root@nfsen nfsen-1.3.8]# useradd netflow -G apache

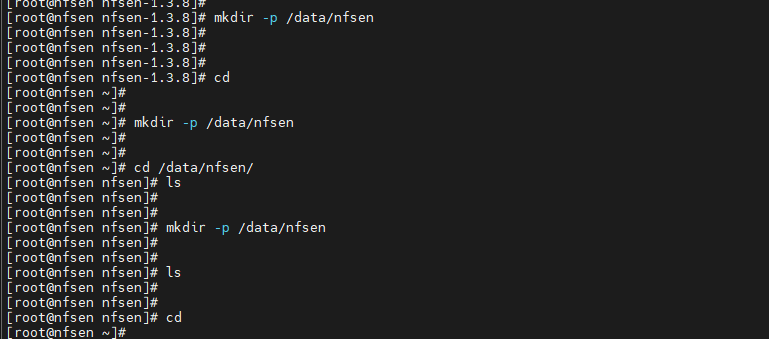
[root@nfsen nfsen-1.3.8]# mkdir -p /data/nfsen

[root@nfsen nfsen-1.3.8]# cd

[root@nfsen ~]# mkdir -p /data/nfsen

[root@nfsen ~]# cd /data/nfsen/

[root@nfsen nfsen]# mkdir -p /data/nfsen



[root@nfsen ~]# cd /data/nfsen/

[root@nfsen nfsen]# ls

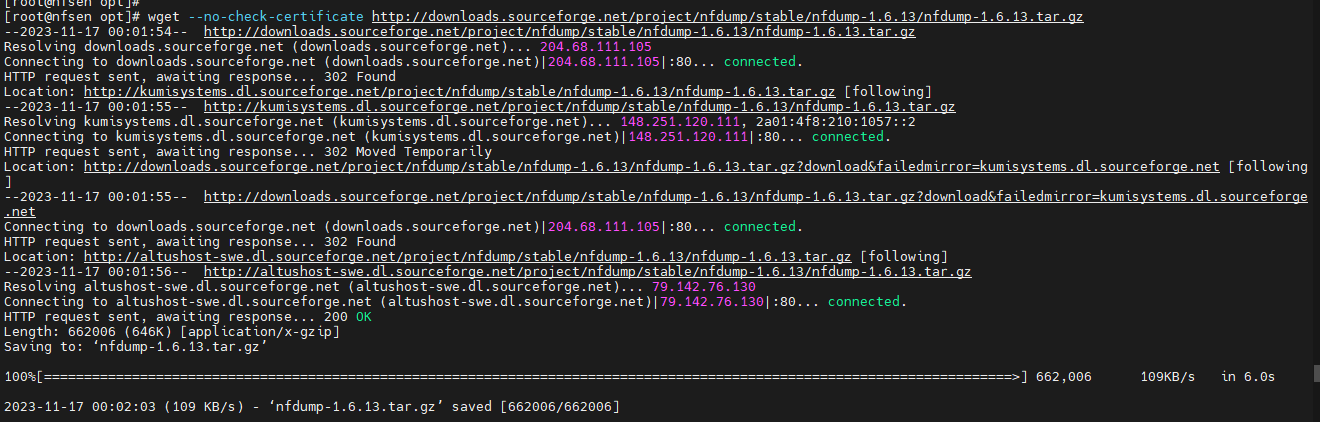
[root@nfsen nfsen]# mkdir -p /data/nfsen

[root@nfsen nfsen]# cd

[root@nfsen ~]# mkdir -p /var/www/html/nfsen

[root@nfsen ~]# cd /opt/

[root@nfsen opt]# wget --no-check-certificate <http://downloads.sourceforge.net/project/nfdump/stable/nfdump-1.6.13/nfdump-1.6.13.tar.gz>



[root@nfsen opt]# wget <https://sourceforge.net/projects/nfsen/files/stable/nfsen-1.3.8/nfsen-1.3.8.tar.gz>

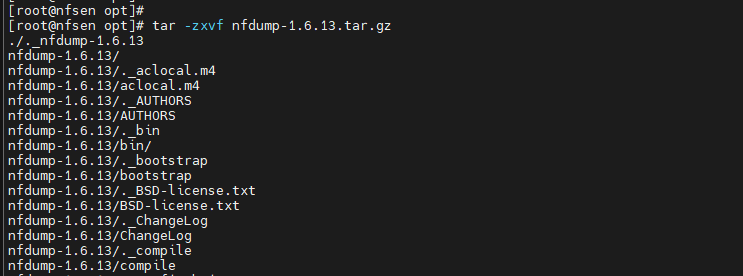


[root@nfsen opt]# service httpd start

Redirecting to /bin/systemctl start httpd.service

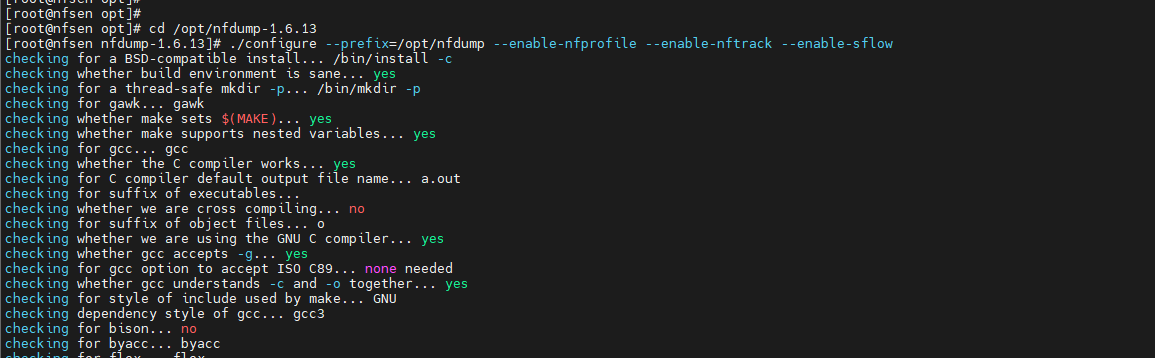
[root@nfsen opt]#

[root@nfsen opt]# tar -zxvf nfdump-1.6.13.tar.gz



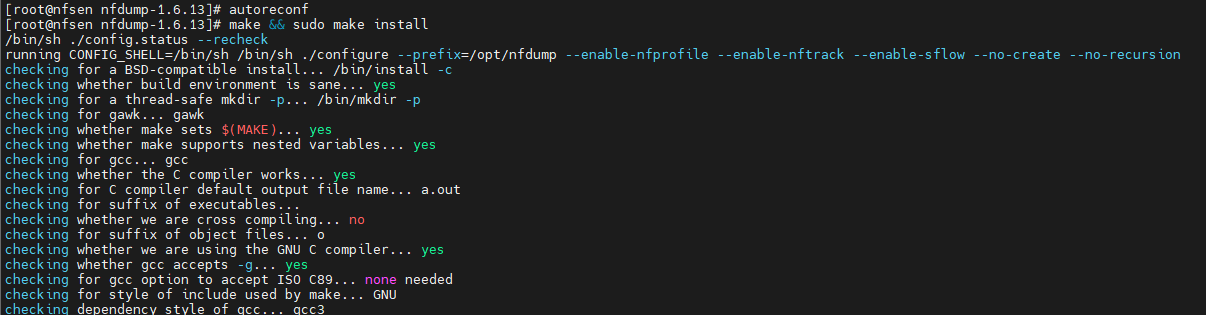
[root@nfsen opt]# cd /opt/nfdump-1.6.13

[root@nfsen nfdump-1.6.13]# ./configure --prefix=/opt/nfdump --enable-nfprofile --enable-nftrack --enable-sflow



[root@nfsen nfdump-1.6.13]# autoreconf

[root@nfsen nfdump-1.6.13]# make && sudo make install



[root@nfsen nfdump-1.6.13]# cd ..

[root@nfsen opt]# cd /opt/

[root@nfsen opt]# ls

nfdump nfdump-1.6.13 nfdump-1.6.13.tar.gz nfsen-1.3.8.tar.gz

[root@nfsen opt]# tar -zxvf nfsen-1.3.8.tar.gz

[root@nfsen opt]# ls

nfdump nfdump-1.6.13 nfdump-1.6.13.tar.gz nfsen-1.3.8 nfsen-1.3.8.tar.gz

[root@nfsen opt]# cd nfsen-1.3.8

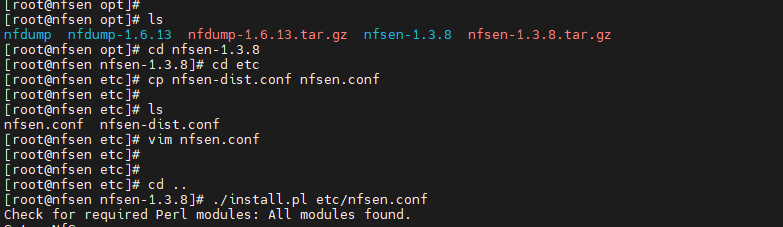
[root@nfsen nfsen-1.3.8]# cd etc

[root@nfsen etc]# cp nfsen-dist.conf nfsen.conf

[root@nfsen etc]# ls

nfsen.conf nfsen-dist.conf

[root@nfsen etc]# vim nfsen.conf



Edit the nfsen.conf file with at least the changes below. Make sure all data path variables are set correctly:

$BASEDIR= "/data/nfsen";

$HTMLDIR = "/var/www/nfsen"; 'change to' --> $HTMLDIR = "/var/www/html/nfsen";

$PREFIX = '/usr/local/bin'; 'change to' --> '$PREFIX = '/opt/nfdump/bin';

$WWWUSER = "www"; 'change to' --> $WWWUSER = "apache"; $WWWGROUP = "www"; 'change to' --> $WWWGROUP = "apache";

You can change the following if you know all the hosts: Duplicate the 'router-1' line for each different host. Change the Name, Port and Color for each different line. Comment out lines by using "#" at the beginning of the line

%sources = (

'router-1' => { 'port' => '9030', 'col' => '#0000ff', 'type' => 'netflow' },

'firewall-1' => { 'port' => '9031', 'col' => '#9093ff', 'type' => 'netflow' },

);

The next section we will add the "flowdoh" plugin which we will install and configure after NFSEN and NFDUMP are up and running.

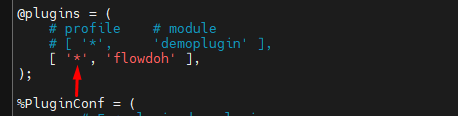
@plugins = ( # profile # module

# [ '', 'demoplugin' ],

[ '', 'flowdoh' ], )

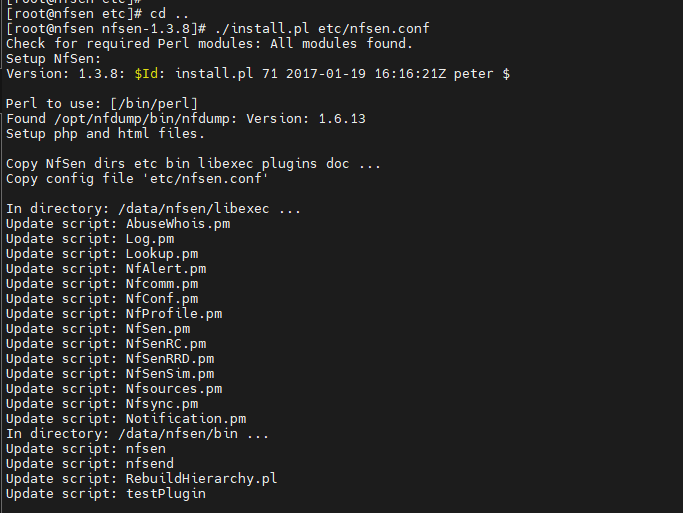
Need TO Add

[ '\*', 'flowdoh' ],



[root@nfsen etc]# cd ..

[root@nfsen nfsen-1.3.8]# ./install.pl etc/nfsen.conf



[root@nfsen nfsen-1.3.8]# ls

bin BSD-license.txt ChangeLog contrib etc helpers html installer-items install.pl libexec plugins README README.plugins

[root@nfsen nfsen-1.3.8]# vim etc/nfsen.conf

[root@nfsen nfsen-1.3.8]#

[root@nfsen nfsen-1.3.8]#

[root@nfsen nfsen-1.3.8]# vim /etc/init.d/nfsen

#!/bin/bash

#chkconfig: - 50 50

#description: nfsen

DAEMON=/data/nfsen/bin/nfsen

case "$1" in

start)

$DAEMON start

;;

stop)

$DAEMON stop

;; status)

$DAEMON status

;;

restart)

$DAEMON stop

sleep 1

$DAEMON start

;;

\*)

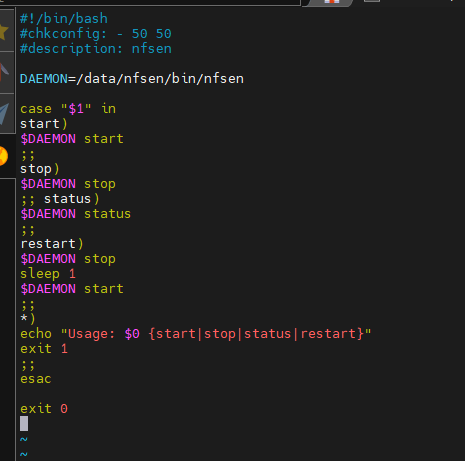
echo "Usage: $0 {start|stop|status|restart}"

exit 1

;;

esac

exit 0



[root@nfsen nfsen-1.3.8]#

[root@nfsen nfsen-1.3.8]#

[root@nfsen nfsen-1.3.8]# vim /etc/init.d/nfsen

[root@nfsen nfsen-1.3.8]#

[root@nfsen nfsen-1.3.8]#

[root@nfsen nfsen-1.3.8]# chmod +x /etc/init.d/nfsen

[root@nfsen nfsen-1.3.8]#

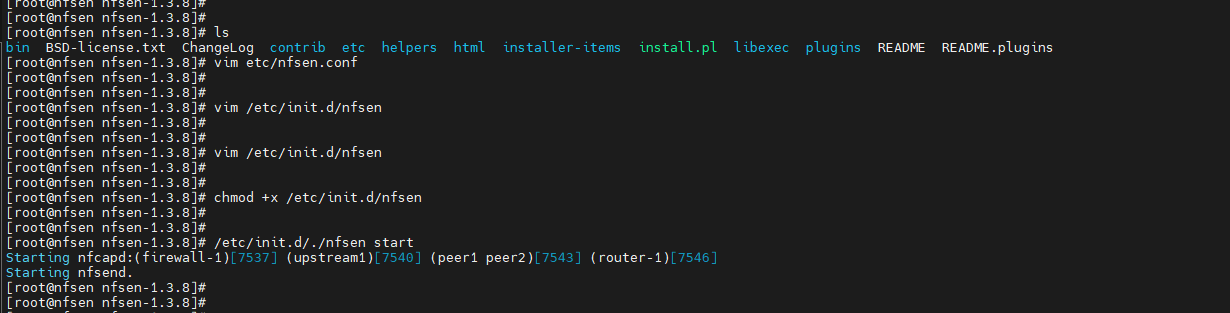
[root@nfsen nfsen-1.3.8]#

[root@nfsen nfsen-1.3.8]# /etc/init.d/./nfsen start

Starting nfcapd:(firewall-1)[7537] (upstream1)[7540] (peer1 peer2)[7543] (router-1)[7546]

Starting nfsend.

[root@nfsen nfsen-1.3.8]#



[root@nfsen nfsen-1.3.8]# /etc/init.d/nfsen restart

Shutdown nfcapd: ()[7537]. ()[7540]. ()[7543]. ()[7546]. .

Shutdown nfsend:[7548]..

Starting nfcapd:(firewall-1)[7566] (upstream1)[7569] (peer1 peer2)[7572] (router-1)[7575]

Starting nfsend.

[root@nfsen nfsen-1.3.8]# systemctl stop firewalld

[root@nfsen nfsen-1.3.8]# systemctl disable firewalld

Removed symlink /etc/systemd/system/multi-user.target.wants/firewalld.service.

Removed symlink /etc/systemd/system/dbus-org.fedoraproject.FirewallD1.service.

[root@nfsen nfsen-1.3.8]#

[root@nfsen nfsen-1.3.8]#

[root@nfsen nfsen-1.3.8]#

[root@nfsen nfsen-1.3.8]#

[root@nfsen nfsen-1.3.8]# /etc/init.d/nfsen restart

Shutdown nfcapd: ()[7566]. ()[7569]. ()[7572]. ()[7575]. .

Shutdown nfsend:[7577]..

Starting nfcapd:(firewall-1)[7664] (upstream1)[7667] (peer1 peer2)[7670] (router-1)[7673]

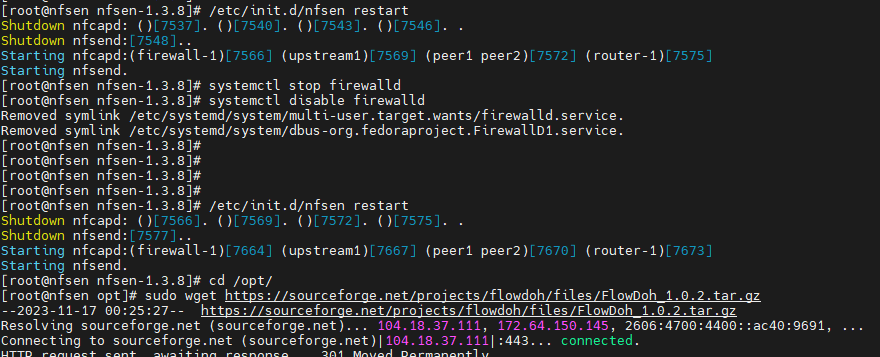
Starting nfsend.

Go to <http://127.0.0.1/nfsen/nfsen.php> (in place of 127.0.0.1" use your server IP.)

**Installing Plugins:**

**FLOWDOH:**

[root@nfsen nfsen-1.3.8]# cd /opt/



[root@nfsen nfsen-1.3.8]# cd /opt/

[root@nfsen opt]# sudo wget <https://sourceforge.net/projects/flowdoh/files/FlowDoh_1.0.2.tar.gz>

[root@nfsen opt]# sudo tar -zxvf FlowDoh\_1.0.2.tar.gz

[root@nfsen opt]# cd /opt/flowdoh/backend/

[root@nfsen backend]#

[root@nfsen backend]# cp -avr flowdoh/ /data/nfsen/plugins/

‘flowdoh/’ -> ‘/data/nfsen/plugins/flowdoh’

‘flowdoh/alerts’ -> ‘/data/nfsen/plugins/flowdoh/alerts’

‘flowdoh/flowdoh.conf.defaults’ -> ‘/data/nfsen/plugins/flowdoh/flowdoh.conf.defaults’

[root@nfsen backend]# cp flowdoh.pm /data/nfsen/plugins/

[root@nfsen backend]# cd /data/nfsen/plugins/flowdoh

[root@nfsen flowdoh]# cp flowdoh.conf.defaults flowdoh.conf

[root@nfsen flowdoh]# cd /data/nfsen/plugins

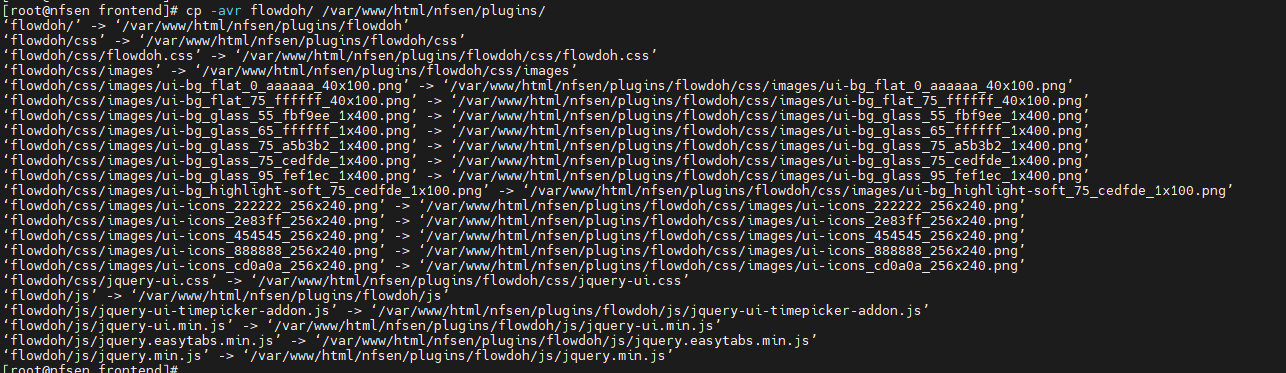
[root@nfsen plugins]# chmod 777 flowdoh

[root@nfsen plugins]# chmod 777 flowdoh.pm

[root@nfsen plugins]# cd /opt/flowdoh/frontend/

[root@nfsen frontend]# cp flowdoh.php /var/www/html/nfsen/plugins/

[root@nfsen frontend]# cp -avr flowdoh/ /var/www/html/nfsen/plugins/



[root@nfsen frontend]# cd /var/www/html/nfsen/plugins

[root@nfsen plugins]# chmod 777 flowdoh

[root@nfsen plugins]# chmod 777 flowdoh.php

[root@nfsen plugins]# /etc/init.d/nfsen restart

Shutdown nfcapd: ()[7664]. ()[7667]. ()[7670]. ()[7673]. .

Shutdown nfsend:[7675]..

Starting nfcapd:(firewall-1)[7809] (upstream1)[7812] (peer1 peer2)[7815] (router-1)[7818]

Starting nfsend.

[root@nfsen plugins]# vim /data/nfsen/etc/nfsen.conf

[root@nfsen plugins]# /etc/init.d/nfsen reconfig

Usage: /etc/init.d/nfsen {start|stop|status|restart}

[root@nfsen plugins]# /etc/init.d/./nfsen start

NfSen is already running!

[root@nfsen plugins]# vim /data/nfsen/etc/nfsen.conf

[root@nfsen plugins]# /data/nfsen/bin/nfsen reconfig

[root@nfsen plugins]# cd /data/nfsen/profiles-data/live/

# cd /opt/

# sudo wget https://sourceforge.net/projects/flowdoh/files/FlowDoh\_1.0.2.tar.gz

# sudo tar -zxvf FlowDoh\_1.0.2.tar.gz

Backend: (/data/nfsen/plugins/)

# cd /opt/flowdoh/backend/

# cp -avr flowdoh/ /data/nfsen/plugins/

# cp flowdoh.pm /data/nfsen/plugins/

# cd /data/nfsen/plugins/flowdoh

# cp flowdoh.conf.defaults flowdoh.conf

# cd /data/nfsen/plugins

# chmod 777 flowdoh

# chmod 777 flowdoh.pm

FrontEnd: (/var/www/html/nfsen/plugins/)

# cd /opt/flowdoh/frontend/

# cp flowdoh.php /var/www/html/nfsen/plugins/

# cp -avr flowdoh/ /var/www/html/nfsen/plugins/

# cd /var/www/html/nfsen/plugins

# chmod 777 flowdoh

# chmod 777 flowdoh.php

Restart NFSEN to add the FLOWDOH Plugin.

# /etc/init.d/nfsen restart

**Firewall enabled**

[root@nfsen live]# firewall-cmd --add-port=9995/tcp --permanent

success

[root@nfsen live]# firewall-cmd --add-port=9995/udp --permanent

success

[root@nfsen live]# firewall-cmd --add-port=80/tcp --permanent

success

[root@nfsen live]# firewall-cmd --add-port=80/udp --permanent

success

[root@nfsen live]# firewall-cmd --add-port=443/udp --permanent

success

[root@nfsen live]# firewall-cmd --add-port=443/tcp --permanent

success

[root@nfsen live]# firewall-cmd --reload

success

[root@nfsen live]# firewall-cmd --list-all

[root@nfsen ~]# firewall-cmd --remove-service=ssh --permanent

[root@nfsen ~]# firewall-cmd --remove-port=40/tcp --permanent

echo "date.timezone = Asia/Dhaka" > /etc/php.d/timezone.ini yum update –y

sudo timedatectl set-timezone Asia/Dhaka

/data/nfsen/bin/nfsen reconfig