

# How to config Netflow monitor

## DOCUMENT VERSION HISTORY

VERSION	DATE	DESCRIPTION	AUTHOR/EDITOR
0.9	10/01/2024	1 <sup>st</sup> . version	Jacky.zou, Spencer.hung Nickle.Wu, Double.lin

## Contents


1	Configure flowview monitor.....	2
1.1	Configure flowview generator simulator .....	2
1.2	Configure listeners.....	4
1.3	Configure filters .....	5
1.4	Statistical Report.....	6
1.5	Check DB size & Row numbers .....	6
1.6	Sample flow export configuration on Cisco SW & Fortigate.....	6


# 1 Configure flowview monitor

Steps: Configure Netflow Generator (simulator) Listener => Configure filter => view flow status

## 1.1 Configure flowview generator simulator

Download and Configure NetFlow Generator to create test flow source traffic on UDP port 9099, version 9


NetFlow Generator


**NetFlow Generator** *free tool*

## Configuration

### Orion server

IP address or hostname
Port

172.17.32.14 <=Cacti IP
9099 <=Listen port

☒ **Node simulation**

### IP addresses

☒ Single or CIDR
☐ Range

IP address or CIDR

172.16.15.99 <=Desktop IP which run this flow generator

### SNMP interfaces

Number of interfaces

8

### Traffic level

Average flows per second

10 <=Reduce to 10 to lower traffic.(default is 100)

### Flow settings

**Flow type**

NetFlow V9 <= Select v5,v9, IPFIX types.

NetFlow V5

**NetFlow V9**

SFlow V5

IPFIX

### Endpoints

+ Add endpoints

Source


Src. ports

Destination

Dest. ports

Protocol

192.168.99.1/32
9099
192.168.99.2/32
443
TCP
⋮



Start generating flow v9 traffics...

Running status

Statistics

Packets sent
Bytes sent
Flow records sent
Packets per second

7,890
45.15 MB
15,780
5.00

Orion server
172.17.32.14:9099

Node simulation
Enabled

Simulated nodes
172.16.15.99

Average flows per second
10

SNMP interfaces
8

Flow type
NetFlow V9

Sampling rate
1:1

NBAR 2
Disabled

Source endpoints
Source ports
Destination endpoints
Destination ports
Protocol

192.168.99.1/32
9099
192.168.99.2/32
443
TCP

Stop generator

## 1.2 Configure listeners

Configure folwview generator to create test flow traffic on UDP port 9099 (v9)

Main Console
Create
Management
Data Collection
Templates
Automation
Presets
Import/Export
FlowView
Listeners
Filters
Schedules
Databases

General
Templates

Listener [edit: zz\_Simulate\_9099]

Listener Name
zz\_Simulate\_9099

Allowed Host Range
172.16.15.99

Port
9099

Protocol
UDP Protocol

Enabled

AUTO start this new listener

Return
Save

Inbound Streams and Status
Verify status is UP. Version, Last Updated

Name	Address	Status	Version	Templates	Last Updated
Stream [172.16.15.99]	172.16.15.99	Up	v9	1	2024-09-30 17:24:06

4

FlowView Listeners										
Search <input type="text" value="Enter a search term"/> <input type="button" value="Go"/> <input type="button" value="Clear"/>										
All 1 Listeners										
Name	Method	Allowed From	Port	Protocol	Status	Observed Listen	Backlog	Streams	Stream Versions	Last Updated
zz_Simulate_9099	Cacti	172.16.15.99	9099	UDP	Up	0.0.0.0:9099	0	1	v9	2024-09-30 17:29:07
All 1 Listeners										
Choose an action										<input type="button" value="Go"/>

systemctl status flow-capture

```

flow-capture.service - Flow Capture Service for Cacti
Loaded: loaded (/etc/systemd/system/flow-capture.service; enabled; preset: disabled)
Active: active (running) since Mon 2024-09-30 17:10:10 CST; 24min ago
Main PID: 2499 (php)
Tasks: 2 (limit: 153762)
Memory: 40.5M
CPU: 13.356s
CGroup: /system.slice/flow-capture.service
└─2499 /usr/bin/php -q /usr/share/cacti/plugins/flowview/service/flow-capture --systemd
    └─2501 /usr/bin/php -q /usr/share/cacti/plugins/flowview/flow_collector.php --listener-id=1

Sep 30 17:10:10 twtprsvhq014.tpvaoc.com systemd[1]: Started Flow Capture Service for Cacti.
Sep 30 17:10:11 twtprsvhq014.tpvaoc.com php[2499]: NOTE: Starting Flow Collection
Sep 30 17:10:11 twtprsvhq014.tpvaoc.com php[2499]: NOTE: Launching cacti-flow-capture as '/usr/share/cacti/plugins/flowview/flow_collector.php --listener-id=1'
Sep 30 17:15:11 twtprsvhq014.tpvaoc.com php[2499]: NOTE: Checking for new or gone listeners
Sep 30 17:20:11 twtprsvhq014.tpvaoc.com php[2499]: NOTE: Checking for new or gone listeners
Sep 30 17:25:11 twtprsvhq014.tpvaoc.com php[2499]: NOTE: Checking for new or gone listeners
Sep 30 17:30:11 twtprsvhq014.tpvaoc.com php[2499]: NOTE: Checking for new or gone listeners

```

### 1.3 Configure filters

Create filters map to listeners, “Stream Address” IP & Max. Row “Top 15” must be assigned to increase stability.

Main Console

Create

Management

Data Collection

Templates

Automation

Presets

Import/Export

FlowView

Listeners

Filters

Schedules

Databases

Syslog Settings

Configuration

Utilities

Troubleshooting

Filter: [new]

General Filters

Filter ?

zz\_Simulate\_9099

Listener ?

zz\_Simulate\_9099

Flow Template ID ?

All

Stream Address ?

Stream [172.16.15.99]

Presets ?

Last Day

Detailed Filter Criteria

Report Type ?

Statistical

Statistical Report ?

Source/Destination IP

Range Rules ?

End Time in Range (fast)

Resolve IP's ?

Yes

Sort Field ?

Bytes

Maximum Rows ?

Top 15

Minimum Bytes ?

No Limit

Result

Filter Name	Listener	Report Type	ID	Sort Field	Resolution
zz_Simulate_9099	zz_Simulate_9099	Source/Destination IP	1	Bytes	Y
All 1 Filters					

## 1.4 Statistical Report

Click "FlowView" => Select Filter & Listener => Click "GO" => Click "Table"

Statistical Report: Source/Destination IP [ Including overrides as specified below ]

Filter: **zz\_Simulate\_9099** Listener: **zz\_Simulate\_9099** **Go** Clear New Edit Save Save As Rename Delete

Report: Statistical: Source/Destination IP Sort Field: Bytes Lines: Top 200 Exclude: None Octets: No Limit ☒ Domains/Hostnames Only

Timespan: Last Half Hour From: 2024-09-30 16:46 To: 2024-09-30 17:16 30 Min

Graph: Bar Height: 300 Pixels Show/Hide: ☒ Table ☐ Bytes ☐ Packets ☐ Flows Export

Source DNS	Dest DNS	Source IP	Dest IP	Flows	Bytes	Packets	Bytes/Packet
ip-192-168-99-1.private.net	ip-192-168-99-2.private.net	192.168.99.1	192.168.99.2	1,418	4,254,000	14,180	300

## 1.5 Check DB size & Row numbers

#Show flowview DB table size & row number

```
mysql -uroot -e "SELECT t.table_name AS `Table`, ROUND(((t.data_length + t.index_length) / 1024 / 1024), 2) AS `Size (MB)`, t.table_rows AS `Rows` FROM information_schema.tables t WHERE t.table_schema = 'flowview' ORDER BY (t.data_length + t.index_length) DESC;"
```

Table	Size (MB)	Rows
plugin_flowview_irr_inetnum	6468.88	6076708
plugin_flowview_irr_route	1099.82	4165912
plugin_flowview_raw_202421511	675.35	2458674
plugin_flowview_raw_202421510	669.52	2433973
plugin_flowview_raw_202421500	669.21	2435004
plugin_flowview_raw_202421509	666.79	2422586
plugin_flowview_raw_202421508	666.03	2419226
plugin_flowview_raw_202421507	662.62	2404484
plugin_flowview_raw_202421505	661.58	2400437
plugin_flowview_raw_202421504	661.52	2400879
plugin_flowview_raw_202421506	661.32	2399050
plugin_flowview_raw_202421501	660.09	2398581
plugin_flowview_raw_202421502	657.93	2389060
plugin_flowview_raw_202421503	655.13	2378987
plugin_flowview_raw_202421423	515.02	1878653
plugin_flowview_irr_domain	485.66	1183215
plugin_flowview_irr_role	68.68	146182

## 1.6 Sample flow export configuration on Cisco SW & Fortigate

**Cisco Switch:**

```

flow record TPV-Flow-Record
match ipv4 destination address
match ipv4 source address
match transport source-port
match transport destination-port
match ipv4 protocol
match interface input
match ipv4 tos
match flow direction
collect counter bytes long
collect counter packets long
collect transport tcp flags
collect timestamp absolute first
collect timestamp absolute last
collect interface output
!
!
flow record TPV-Flow-Record-OUT
match ipv4 destination address
match ipv4 source address
match transport source-port
match transport destination-port
match ipv4 protocol
match interface output
match ipv4 tos
match flow direction
collect counter bytes long
collect counter packets long
collect transport tcp flags
collect timestamp absolute first
collect timestamp absolute last
collect interface input
!
!
flow exporter FNFexp
destination 172.17.32.16
source Vlan99
transport udp 2055
!
!
flow exporter test
destination 172.17.32.14
source Vlan99
transport udp 2055
!

```



```

!
flow monitor FlowMonitor1
exporter FNFexp
exporter test
record TPV-Flow-Record
!
!
flow monitor FlowMonitorOUT
exporter FNFexp
exporter test
record TPV-Flow-Record-OUT
!
!
sampler sampler1
description sample at 50%
mode random 1 out-of 2
!
!
interface GigabitEthernet1/1/2
switchport trunk allowed vlan 99
switchport mode trunk
ip flow monitor FlowMonitor1 sampler sampler1 input
ip flow monitor FlowMonitorOUT sampler sampler1 output
channel-group 2 mode active

interface GigabitEthernet2/1/2
switchport trunk allowed vlan 99
switchport mode trunk
ip flow monitor FlowMonitor1 sampler sampler1 input
ip flow monitor FlowMonitorOUT sampler sampler1 output
channel-group 2 mode active

```

## **Fortigate Firewall:**

```

FG3H1E5819903613 (global) # show system netflow
config system netflow
    set collector-ip 172.17.32.14
    set collector-port 9005
    set source-ip 172.17.32.100
    set active-flow-timeout 60
    set inactive-flow-timeout 10
end

```

```

FG3H1E5819903613 (global) # show system interface "port3"
config system interface

```

```
edit "port3"  
  set vdom "root"  
  set ip 172.17.32.100 255.255.255.0  
  set allowaccess ping https snmp  
  set type physical  
  set netflow-sampler both  
  set sflow-sampler enable  
  set sample-rate 50  
  set explicit-web-proxy enable  
  set description "LAN"  
  set alias "lan"  
  set device-identification enable  
  set role lan  
  set snmp-index 5  
next  
end
```