Scalable Flow Monitoring for Data Center Network

A Project Report Submitted in the partial fulfillment of the requirements for the award of degree of

Master of Technology
in
Computer Science

By
Nirmoy Das

School of Computer and Information Sciences
University of Hyderabad
Hyderabad, India

June, 2013

May 25, 2013

Contents

1 Related Work **2**

1.1 EMC2[5] 2

1.1.1 Architecture 2

1.1.2 Modules 2

1.1.2.1 Flow-Table 3

1.1.2.2 NetFlowParser/sFlowParser 3

1.1.2.3 NetFlowCollector/sFlowCollector 4

1.1.3 Advantages and Limitations 4

Bibliography **6**

Chapter 1

Related Work

Flow monitoring protocols like NetFlow[1] and sFlow[2] can provide important information about traffic that passes through a network. However contemporary computer networking is out-spacing out ability to monitor them efficiently. As data centers are getting virtualized with virtual software switches and scaling to thousands of node, it is our immediate requirement to have monitoring system that can scale efficiently. There are few solutions that provide some methods to have scalable flow monitoring in data center networks.

1.1 EMC2[5]

Edge Monitoring and Collection for Cloud (EMC2) is a scalable network wide monitoring service for data centers. EMC2 stays inside host computer to monitor virtual switches. Monitoring at virtual switch is scalable due to its distributed nature.

1.1.1 Architecture

Figure 1.1 shows the architecture of EMC2

1.1.2 Modules

EMC2 is a multi-threaded application that contains following modules

- Flow-Table : Flow-Table is in-memory 2-level hash table.
- NetFlowParser : It parse NetFlow datagrams and update Flow-Table.
- sFlowParser : Its parse sFlow datagrams and update Flow-Table.

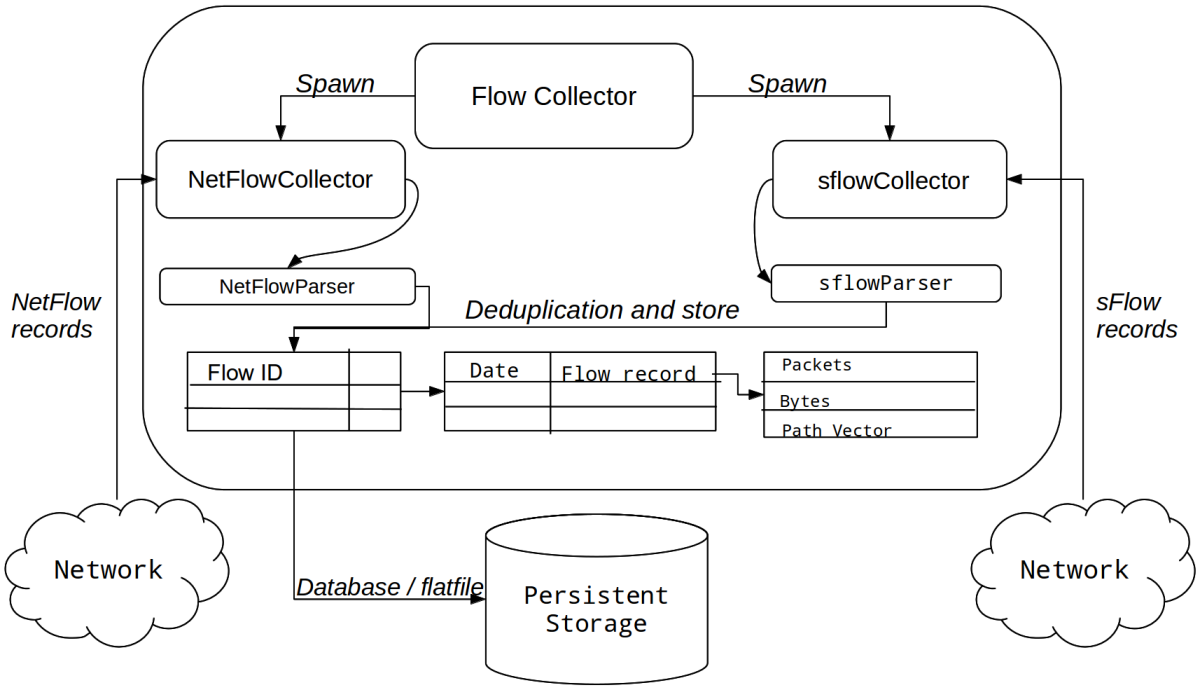

Figure 1.1: Architecture of EMC2.

- NetFlowCollector : It accept NetFlow datagrams and create parser thread upon receiving NetFlow datagrams.
- sFlowCollector : It does the same task like NetFlowCollector for sFlow datagrams.
- FlowCollector : It invoke two thread, NetFlowCollector and sFlowCollector for accepting flow datagrams.

1.1.2.1 Flow-Table

Flow-Table is a 2-level in-memory hash table. Layer-3 source and destination address forms Flow-ID that acts as primary key for in-memory hash table. Flow-ID maps to another hash table where timestamp is the key and flow record is value. Flow record contains number of packets, number of bytes and optional path vector.

1.1.2.2 NetFlowParser/sFlowParser

NetFlowCollector/sFlowCollector creates these two parser threads upon receiving a NetFlow/sFlow datagram. Parser threads parse the datagram and update the Flow-Table. Parser threads also performs two important tasks:

- Deduplication.
- Data rate prediction in presence of sampling.

Deduplication: Deduplication avoids duplicate flow records to be added in Flow-Table. It uses the following algorithm.

Algorithm 1: Detect Duplicate Flow

```
if flow − ID not exist then
    add flow to the flow table.
    return
else
    if Same exporter then
        update the flow table.
        return
    else
        report duplicate flow.
        update path vector.
        return
    end if
end if
```

Data Rate Prediction in Presence of Sampling: Sampling rate is specified in flow datagrams. Parser thread predict data rate by multiplying sampling rate with length of the packet.

1.1.2.3 NetFlowCollector/sFlowCollector

NetFlowCollector/sFlowCollector are collector thread that waits for new NetFlow or sFlow datagrams and spawn a new NetFlowParser/sFlowParser thread upon receiving a datagram.

1.1.3 Advantages and Limitations

Claimed Advantages of EMC2

- Scalable monitoring as EMC2 monitors host Vswitches which are distributed in nature.

Disadvantages are

- Lack of scalable storage.
- Centralized monitoring will be difficult as it requires to fetch from distributed flats files.

Bibliography

[1] **Cisco IOS NetFlow**. `http://www.cisco.com/en/US/products/ps6601/products_ios_protocol_group_home.html`.

[2] **sFlow Official Site**. `http://www.sflow.org`.

[3] *Fifth International Conference on Communication Systems and Networks, COMSNETS 2013, Bangalore, India, January 7-10, 2013*. IEEE, 2013.

[4] Yeonhee Lee and Youngseok Lee. **Toward scalable internet traffic measurement and analysis with Hadoop**. *SIGCOMM Comput. Commun. Rev.*, **43**(1):5–13, January 2012.

[5] Vijay Mann, Anilkumar Vishnoi, and Sarvesh Bidkar. **Living on the edge: Monitoring network flows at the edge in cloud data centers**. In *COMSNETS* [3], pages 1–9.