NetFlow Optimizer™

Overview

Version 2.4.9 (Build 2.4.9.0.3)

May 2017

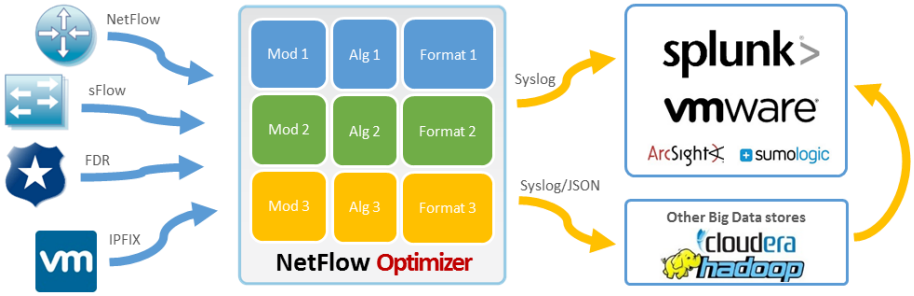
Contents

About NetFlow Optimizer 2
What is NetFlow Optimizer 2
NetFlow Optimizer Core Features 3
Compatibility with other systems 3
Components 3
Core 3
Integration with Splunk 4
Integration with VMware vRealize Log Insight 4
NetFlow Optimizer Deployments 5
Deployment with Splunk Enterprise 5
Combined indexer/search head 5
Separate Indexers, Search Heads, and Universal Forwarders 6
Multi-instance Indexers, Search Heads, Clusters, and Forwarders 7
Deployment with Splunk Cloud 8
Deployment with VMware vRealize Log Insight 9
Ingest flow data directly from NFO 9
Ingest flow data with Log Insight Agent 10

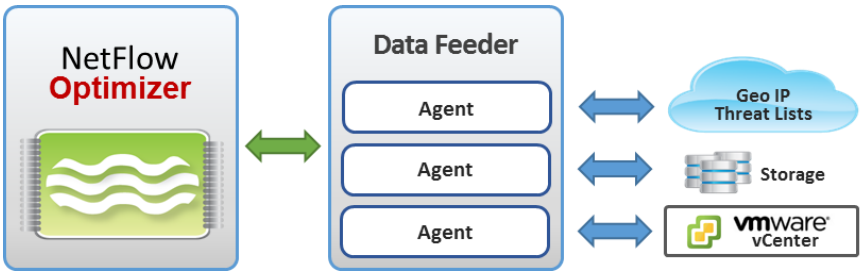
About NetFlow Optimizer

What is NetFlow Optimizer

NetFlow Optimizer (NFO) is a software-only processing engine for network flow data: NetFlow, IPFIX, sFlow, J-Flow, etc. **NFO is not a NetFlow collector**. It uses patented streaming technology that accepts network flow data from network devices (routers, switches, firewalls), applies map-reduce algorithms to the data to extract the information needed to address desired use cases, converts the processed data to syslog (or other formats such as JSON), then sends that useful information to your visualization platform or SIEM.



External Data Feeder for NFO (EDFN) is a remote component which serves as a knowledge base of information outside of the NetFlow domain. Its task is to provide NetFlow Optimizer with information generally unavailable in the data streams supplied by NetFlow/IPFIX exporters. It enables automatic updates of security threat lists, Geo IP information, and VM names for VMWare vCenter integration.



EDFN is comprised of a Platform and a collection of Agents each of which is designed to obtain information of a certain kind. The Platform provides a common interface for the Agents' configuration and data exchange and serves as a conduit for delivering information collected by the Agents to the NetFlow Optimizer. Typically External Data Feeder for NFO is installed on a separate server with access to the internet. (Must be downloaded separately from NetFlow Logic's web site – www.netflowlogic.com/download/).

NetFlow Optimizer Core Features

- **NFO is a software solution**. No investment in expensive proprietary hardware is required;
- **Unique real-time consolidation** technology optimizes the flow data sent to the SIEM, without losing the accuracy of the information;
- **Identifies security threats** and traces current known threat sources;
- **Enriches flow data** with real-time DNS, SNMP information, current Reputation, and GeoIP information;
- **Monitors network devices and interface loads**. Measures bandwidth consumption for capacity planning. Identifies applications and users that consume bandwidth.
- **Multiple destinations**. NFO can send output to multiple destinations. The outputs can be configured to send pre-processed consolidated flows, original flows translated from binary to syslog or JSON one-to-one, and an original flow data in binary format to other flow collectors;
- **Enables actionable virtual and physical network monitoring**. Identifies VMs affected by physical network outages and interface failures. Visualizes virtual and physical network data paths. Supports point-to-point communication tracing: VM – VM, VM – physical host, VM – VM over VXLAN;
- **NFO provides unmatched performance** and can process up to 500,000 records per second on an 8-core machine with 12GB of memory. Millions of flow records per second can be processed if multiple instances of NFO are deployed;
- **NFO can be deployed in a virtual** environment and scales horizontally and vertically with the growth of the enterprise network.

Compatibility with other systems

As NetFlow Optimizer outputs flow data in standard syslog format, it is easily consumed by any syslog analyzer or SIEM system. In the sections below you will find details about various components available from NetFlow Logic for integration with Splunk and VMware vRealize Log Insight.

Components

Core

NetFlow Optimizer receives flow data from network devices, consumes and enriches flow information with other data, translates it to syslogs, and sends it to other systems where it is then correlated with other machine data and visualized. (Downloadable from NetFlow Logic's web site – www.netflowlogic.com/download/).

External Data Feeder for NFO (EDFN) enables automatic updates of threat lists, GeoIP information, and VM names for VMWare vCenter integration. This component feeds this information to NFO. (Downloadable from NetFlow Logic's web site – www.netflowlogic.com/download/).

Integration with Splunk

Technology Add-on for NetFlow must be installed on Splunk indexers and search heads in order for NFO to work with Splunk. It collects flow data processed by NetFlow Optimizer, and then this data is visualized by the Netflow Analytics for Splunk App. You need to have NetFlow Optimizer installed prior to installing this and all other NetFlow Logic Apps and Technology Add-ons. (The Technology Add-on for NetFlow is downloadable from Splunkbase at https://splunkbase.splunk.com/app/1838/).

NetFlow Analytics for Splunk App must be installed on Splunk search heads. It contains visualization dashboards and information for alerting. You need to have NetFlow Optimizer installed prior to installing this and all other NetFlow Logic Apps and Technology Add-ons. (Downloadable from Splunkbase at https://splunkbase.splunk.com/app/489/).

V2P Network Visibility Solution has two components. **V2P Network Visibility for Splunk App** and **V2P Network Visibility Module** together provide information for virtual and physical networks correlation. They enable virtual infrastructure administrators to determine whether a problem in virtual network communications is caused by a physical network device problem.

V2P Network Visibility for Splunk App must be installed in your Splunk environment. (Downloadable from https://splunkbase.splunk.com/app/2824/).

The V2P Network Visibility Module must be installed in your NFO. (Downloadable from NetFlow Logic's web site – www.netflowlogic.com/download/).

Integration with VMware vRealize Log Insight

NetFlow Logic Network Metrics Content Pack must be installed on VMware vRealize Log Insight. It contains visualization dashboards and fields for search and correlation of flow information with other machine data. You need to have NetFlow Optimizer installed prior to installing this component. (Downloadable from NetFlow Logic's web site – www.netflowlogic.com/download/).

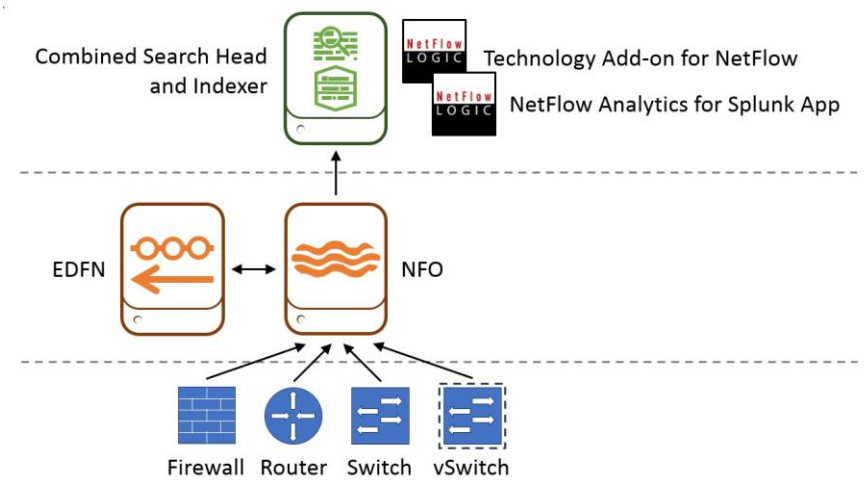
NetFlow Optimizer Deployments

NetFlow Optimizer receives flow data from your network devices, typically sent over UDP protocol. NetFlow analytics and/or original flow data are sent from NFO to any system capable of receiving syslogs over UDP protocol, such as Splunk indexers or Splunk forwarders, rsyslog or syslog-ng, VMware vRealize Log Insight, Sumo Logic, Elastic stack (ELK), or any other SIEM system. These systems store flow information where it can be correlated with other machine data, visualized in dashboards, searched and used for creating alerts.

Deployment with Splunk Enterprise

Combined indexer/search head

In single-instance Splunk Enterprise deployments, where one instance handles everything from input through indexing to search, NFO should be installed on a different server or virtual machine (VM) than the one on which the combined search head / indexer is installed. EDFN could be installed on the same server or VM on which NFO is installed or on a different one. This diagram shows where the processing components reside on the various processing tiers. This type of deployment is suitable for a department or a small enterprise.

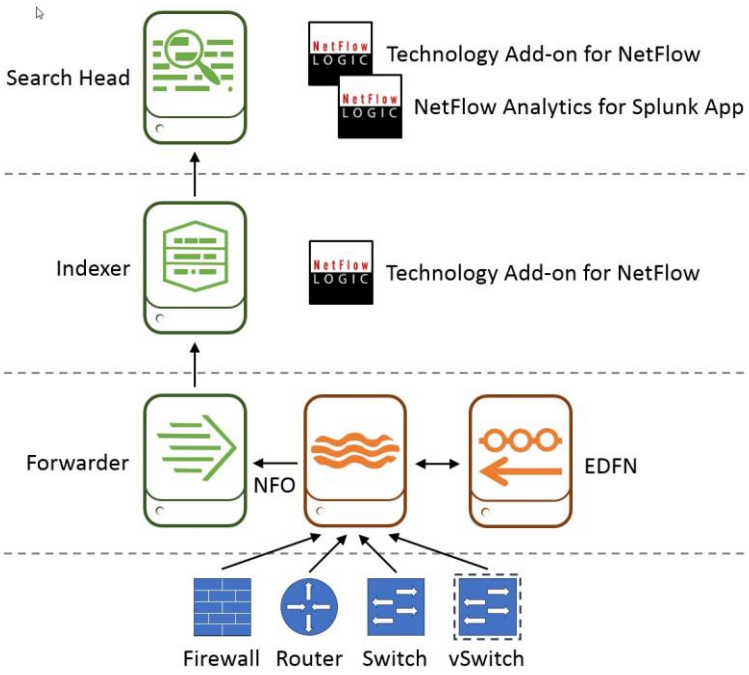


In this diagram, starting from the bottom up:

- **Network device tier.** Configure your routers, switches, firewalls, and virtual switches to send flow data to NFO.
- **NFO / EDFN tier.** NFO receives flow data, performs preprocessing and optimization, enriches it with external data provided by EDFN, and sends it to Splunk indexer for storage and indexing.
- **Splunk tier.** You need to install both Technology Add-on for Netflow (TA) and NetFlow Analytics for Splunk and other Apps here. TA defines all the necessary field names and tags for flow data to be CIM-compliant. The Apps provide dashboards, drill downs, searches, and alerting.

Separate Indexers, Search Heads, and Universal Forwarders

In distributed Splunk Enterprise deployments, you may add indexers and search heads to boost performance, and forwarders to ingest data. Typically, in these deployments, universal forwarder (UF) is the right choice. UF can be co-located on the machines that are generating data.

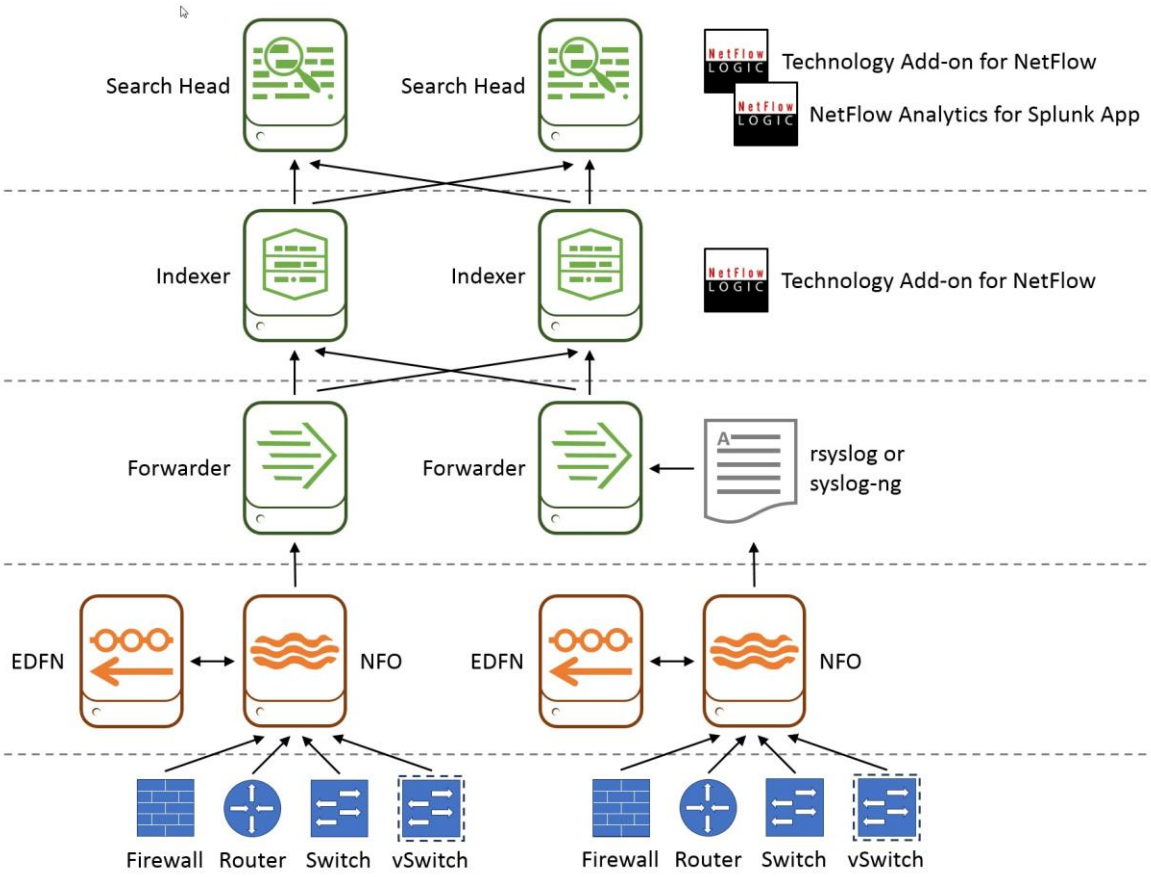


In this diagram, starting from the bottom up:

- **Network device tier.** Configure your routers, switches, firewalls, and virtual switches to send flows data to NFO. Picture firewall and vds
- **NFO / EDFN /Splunk UF tier.** NFO receives flow data, performs preprocessing and optimization, enriches it with external data provided by EDFN, and sends it to Splunk universal forwarder (UF). UF then forwards data to an indexer.
- **Splunk indexing tier.** Technology Add-on for Netflow (TA) is installed here. TA defines all the necessary field names and tags for flow data to be CIM-compliant.
- **Splunk search head tier.** You need to install both Technology Add-on for Netflow (TA) and NetFlow Analytics for Splunk and other Apps here. Note that you install the Technology Add-on for Netflow both here and in splunk indexing tier.

Multi-instance Indexers, Search Heads, Clusters, and Forwarders

In a large enterprise deployment you may have several search heads or a search cluster, several indexers or an index cluster, and many forwarders. You may also have an rsyslog or syslog-ng infrastructure for high availability ingestion of syslog data.

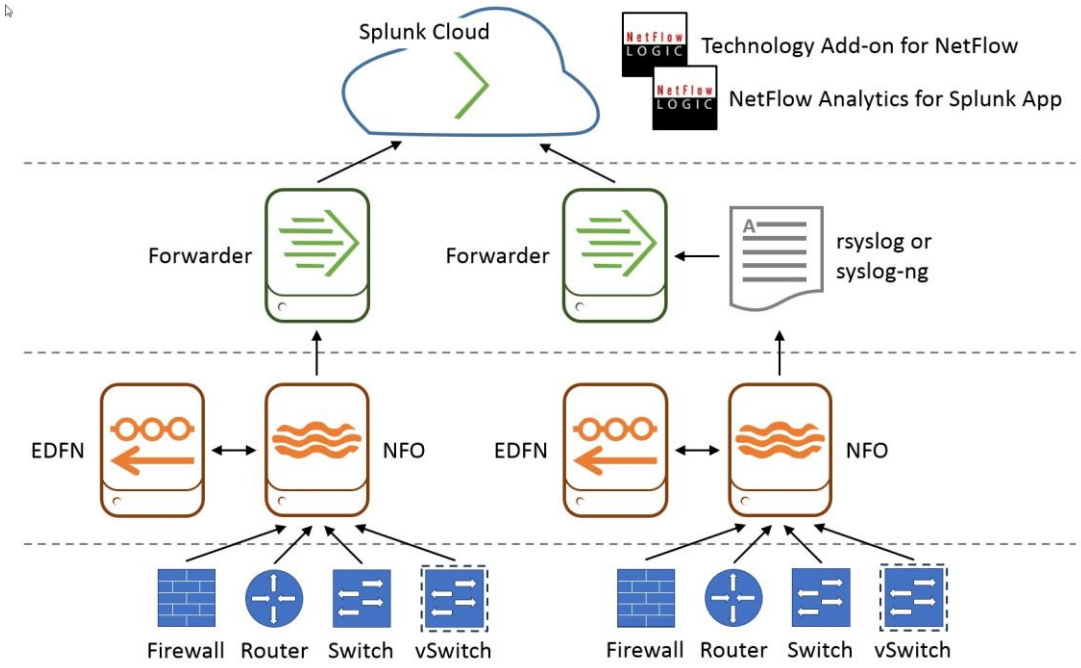


In this diagram, starting from the bottom up:

- **Network device tier.** Configure your routers, switches, firewalls, and virtual switches to send flows data to NFO.
- **NFO / EDFN tier.** NFO receives flow data, performs preprocessing and optimization, enriches it with external data provided by EDFN, and sends it to Splunk forwarder or rsyslog or syslog-ng.
- **Splunk forwarder / rsyslog / syslog-ng tier.** This is the data input for Splunk tier. In this tier you may have Splunk universal or heavy forwarders, and rsyslog / syslog-ng infrastructure.
- **Splunk indexing tier.** Technology Add-on for Netflow (TA) is installed here. TA defines all the necessary field names and tags for flow data to be CIM-compliant.
- **Splunk search head tier.** You need to install both Technology Add-on for Netflow (TA) and NetFlow Analytics for Splunk and other Apps here. Note that you install the Technology Add-on for Netflow both here and in splunk indexing tier.

Deployment with Splunk Cloud

NetFlow Logic's Technology Add-on for NetFlow and NetFlow Analytics for Splunk App both certified and vetted for Splunk Cloud deployment. Whether your organization has self-service or managed Splunk Cloud deployment, you need to install NFO and EDFN in your data center. Splunk forwarders are used to ingest data to Splunk Cloud. Select one of the above scenarios with universal forwarder or heavy forwarder that matches your syslog collection infrastructure.



In this diagram, starting from the bottom up:

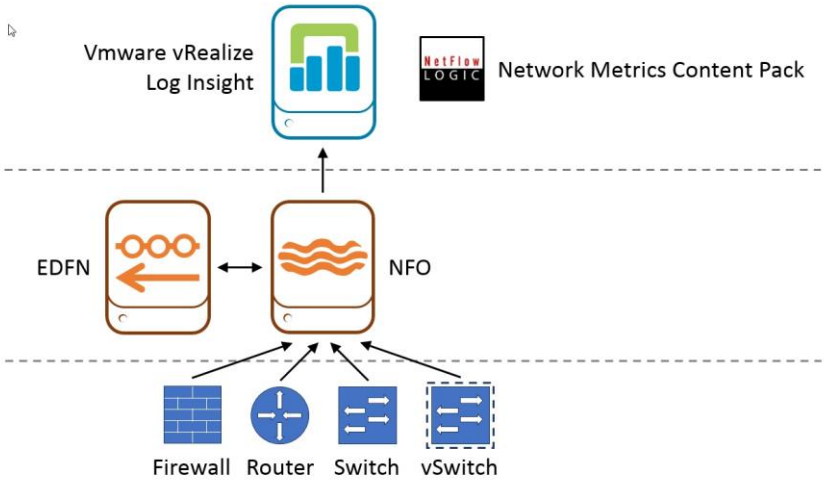
- **Network device tier.** Configure your routers, switches, firewalls, and virtual switches to send flows data to NFO.
- **NFO / EDFN tier.** NFO receives flow data, performs preprocessing and optimization, enriches it with external data provided by EDFN, and sends it to Splunk forwarder or rsyslog or syslog-ng.
- **Splunk forwarder / rsyslog / syslog-ng tier.** This is the data input for Splunk tier. In this tier you may have Splunk universal or heavy forwarders, and rsyslog / syslog-ng infrastructure.
- **Splunk Cloud tier.** You need to install both Technology Add-on for Netflow (TA) and NetFlow Analytics for Splunk and other Apps here.

Deployment with VMware vRealize Log Insight

VMware vRealize Log Insight ingests streaming syslogs directly over UDP protocol, or from Log Insight Agents. NetFlow Logic provides Network Metrics Content Pack for Log Insight, which should be installed in Log Insight server. The Content Pack provides dashboards, tables, and intuitive graphs for security and operational intelligence on both physical and virtual networks.

Ingest flow data directly from NFO

NFO should be installed on a different virtual machine (VM) than the one on which the Log Insight is installed. EDFN could be installed on the same VM on which NFO is installed or on a different one.

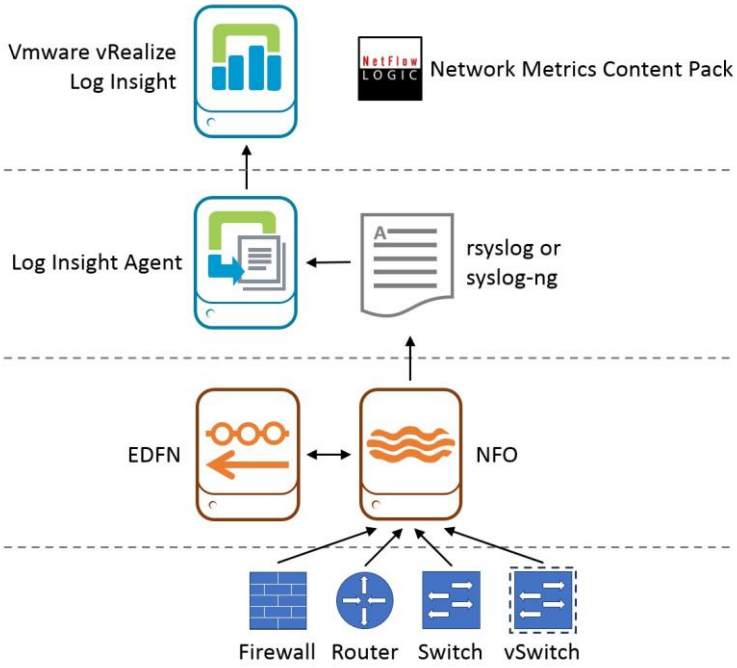


In this diagram, starting from the bottom up:

- **Network device tier.** Configure your routers, switches, firewalls, and virtual switches to send flows data to NFO.
- **NFO / EDFN tier.** NFO receives flow data, performs preprocessing and optimization, enriches it with external data provided by EDFN, and sends it to Splunk forwarder or rsyslog or syslog-ng.
- **Log Insight server tier.** Network Metrics Content Pack for Log Insight is installed here.

Ingest flow data with Log Insight Agent

Your organization may have an rsyslog or syslog-ng infrastructure for high availability ingestion of syslog data. NFO should be installed on a different virtual machine (VM) than the one on which the Log Insight is installed. EDFN could be installed on the same VM on which NFO is installed or on a different one.



In this diagram, starting from the bottom up:

- **Network device tier.** Configure your routers, switches, firewalls, and virtual switches to send flows data to NFO.
- **NFO / EDFN tier.** NFO receives flow data, performs preprocessing and optimization, enriches it with external data provided by EDFN, and sends it to Splunk forwarder or rsyslog or syslog-ng.
- **Log Insight Agent / rsyslog / syslog-ng tier.** This is the data input for Log Insight server tier. In this tier you may have Linux or Windows LI Agents, and rsyslog / syslog-ng infrastructure.
- **Log Insight server tier.** Network Metrics Content Pack for Log Insight is installed here.