Gigamon Metadata Application for Splunk Deployment Guide

This page is intentionally left blank

Table of Contents

Overview

IPFIX and CEF are powerful standards-based technology that are gaining momentum in the network security space for forensics, trend analysis, and anomaly detection. They looks at raw network packets and derives sophisticated flow-based metadata such as records of conversations between endpoints, duration of conversations, and channels of communications.

Gigamon centralizes the function of generating these flow records so that this can be done consistently across heterogeneous and disparate infrastructure. The flow records can be served up to a variety of security solutions that analyze flow metadata. Gigamon has also extended the metadata to include URL information, providing insight into HTTP and SIP traffic. Other enterprise extensions for metadata are HTTP, DNS, and SSL certificates, which provide metadata that can be used for security analysis.

The Gigamon Security Delivery Platform with metadata Generation:

- provides unsampled metadata record generation to detect “low-and-slow” attacks
- filters records based on configurable parameters to predetermined tools
- offloads metadata record generation from the overloaded network infrastructure
- enables end-to-end security enforcement with visibility into every flow
- provides advanced information elements

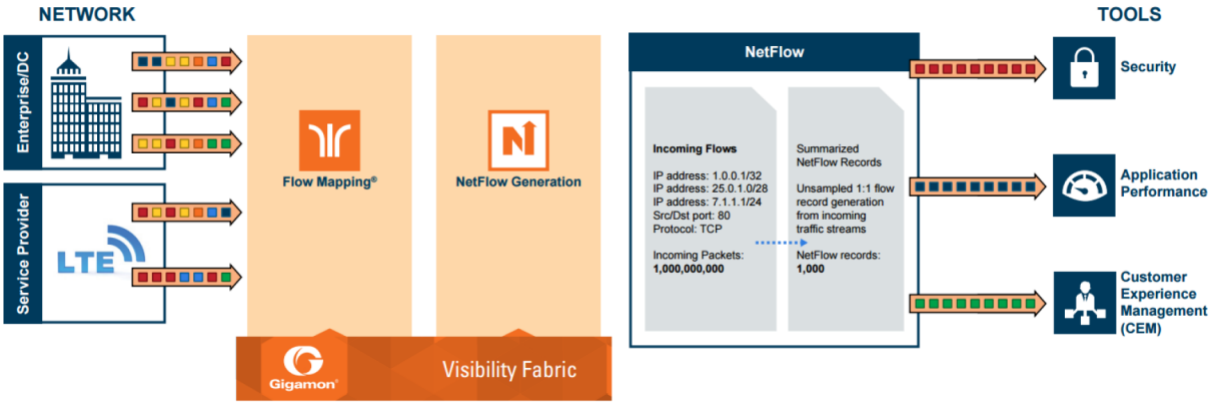


Figure 1: IPFIX/CEF Generation using Gigamon Visibility Platform

Incoming packets from network(s) enter the Gigamon Visibility Platform and are directed by maps to GigaSMART engine for metadata generation. Metadata generation process examines the incoming packets and converts the packets of choice into flow records. Specific flows are then forwarded to specific tools, such as Security, Application Performance, and Customer Experience Management (CEM) tools.

Gigamon Metadata Application for Splunk

The Gigamon Metadata Application for Splunk allows customers to extract, index and display network metadata generated by the GigaSECURE Security Delivery Platform. The application comes packaged with dashboards, demo views, and tutorial to make deployment simple and intuitive.

The Gigamon GigaSECURE Security Delivery Platform allows users to extract and consolidate metadata from monitored network traffic flows, package them into NetFlow IPFIX/CEF records, then send them to collectors like Splunk SIEM for indexing and analysis. Gigamon has enriched the IPFIX/CEF records with information like URL information, HTTP/HTTPS return codes, and DNS query/response information, all of which can provide the ability to rapidly diagnose security events for use cases such as, identifying rogue DNS services, spotting potential Command and Control server communications using high entropy domains and detecting use of non-trusted or self-signed certificates for SSL-decrypted traffic that could indicate nefarious activity.

See Appendix for Use cases available with Gigamon's custom metadata elements
For more information on Gigamon's NetFlow and Metadata Generation see:

https://www.gigamon.com/products/traffic-intelligence/gigasmart/metadata-generation.html

Audience

This guide is intended for users who have basic understanding of Splunk. This document expects users to be familiar with Splunk administration, installation of additional Splunk components, administrative permissions to restart services and edit configuration files.
This deployment guide covers installation and configuration of a single-instance deployment, where one Splunk instance serves as both the search head and indexer running on Linux- based servers.

Notes

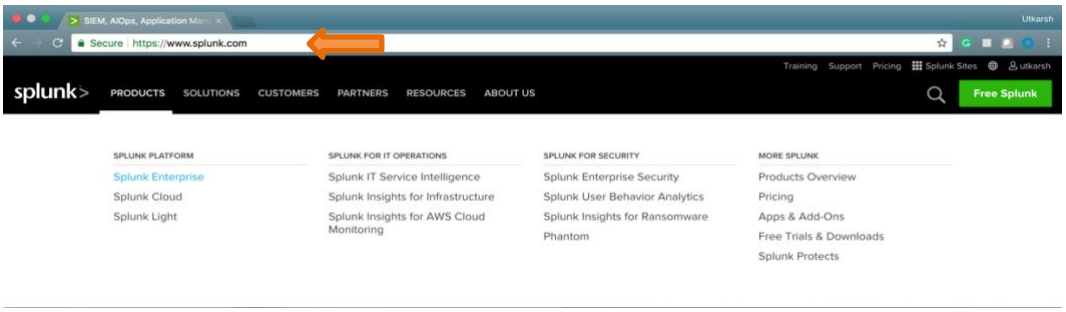
The below notes apply to GigaVUE visibility node running GigaVUE-OS 5.0.

- Maximum of five records can be added to single monitor with all the records having same match fields but can differ in collect fields
- Only one monitor can be configured per GigaSMART Group
- GigaSMART Operation can only be assigned to GigaSMART Group consisting of single engine port.
- For more than one monitors, multiple engine ports must be bound to separate GigaSMART Groups and different monitors can be assigned to each of them.
- Maximum number of exporters supported by a tunnel is six

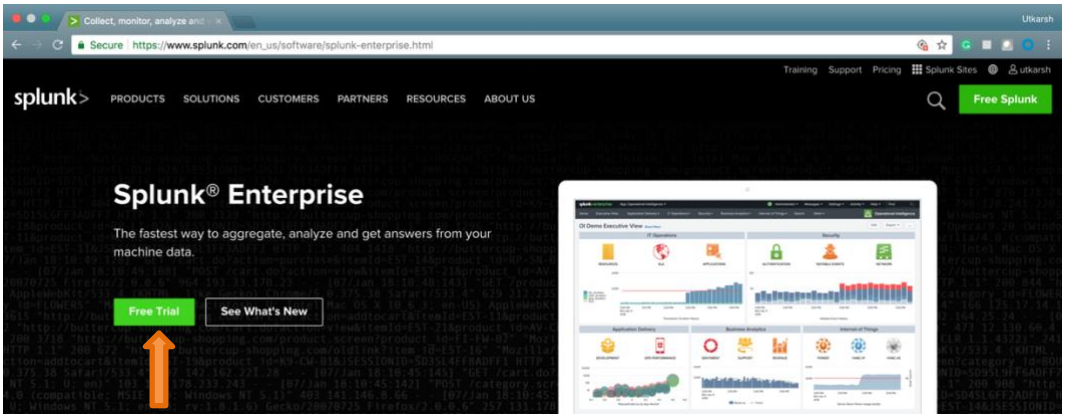
Setting up Splunk

Downloading the Splunk SIEM

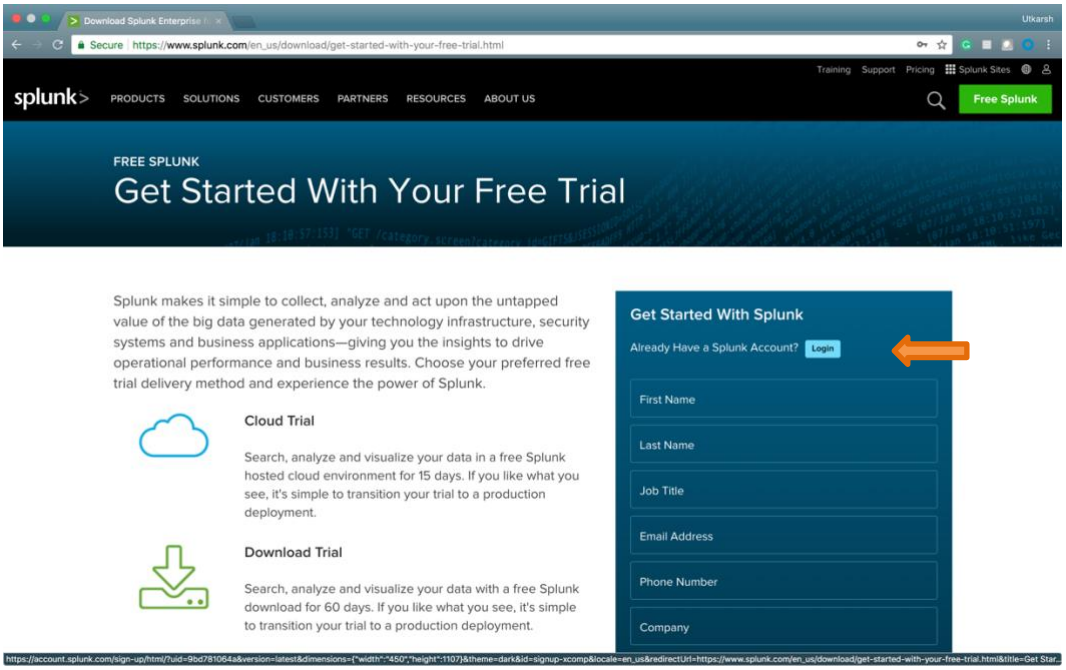
Go to https://www.splunk.com/



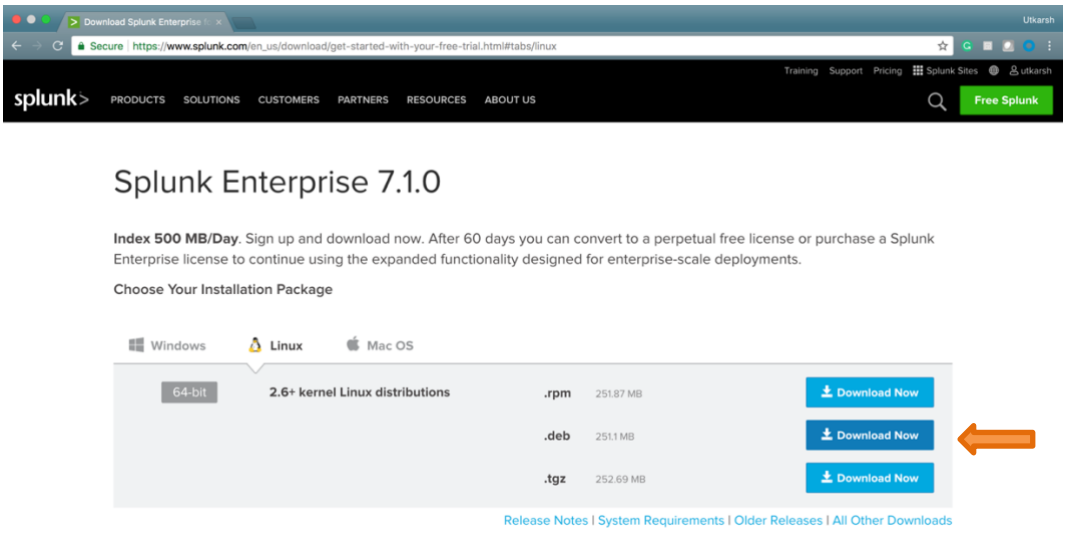
Click the free trial option



Sign-in or Login into your Splunk account to download Splunk.

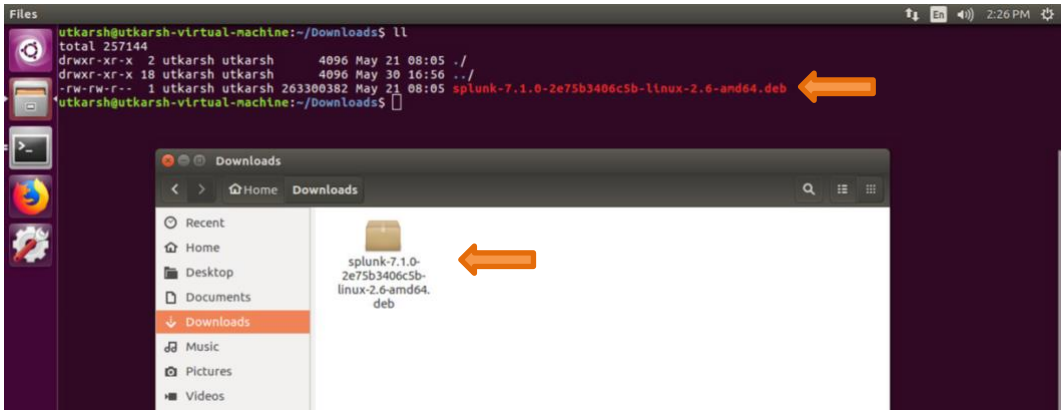


Now, download the Splunk Enterprise as per your OS. For Ubuntu machines, download .deb as shown below:



Installing the Splunk SIEM

Splunk setup would be downloaded in the “Downloads” directory

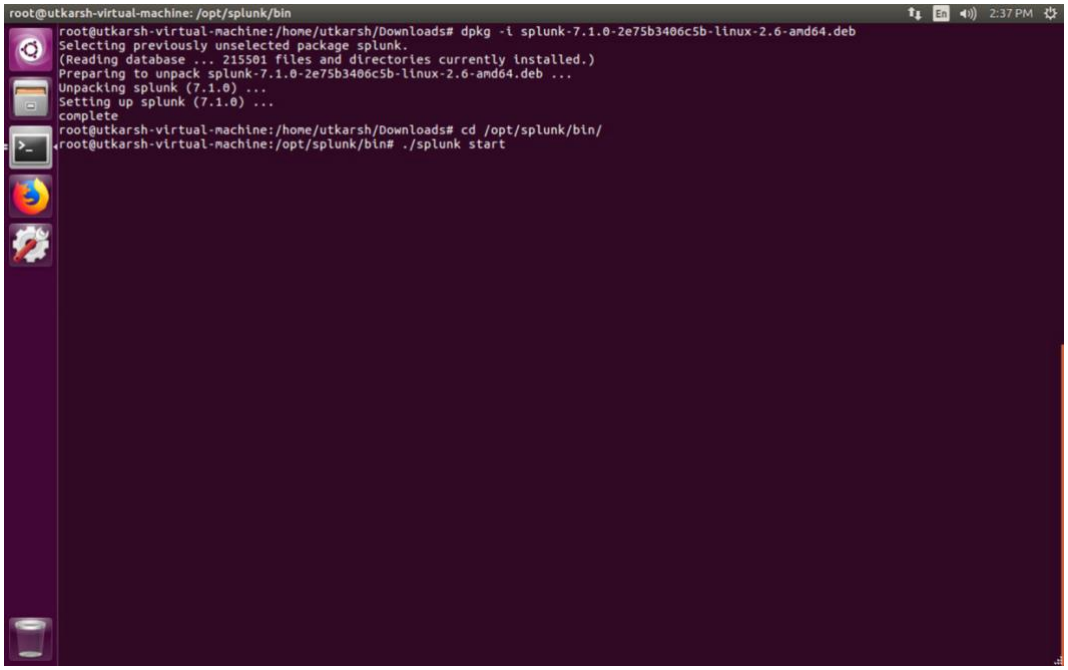


You might need superuser permissions to perform the below commands. You can use:

$ sudo -i

Use the below command to install splunk on ubuntu:

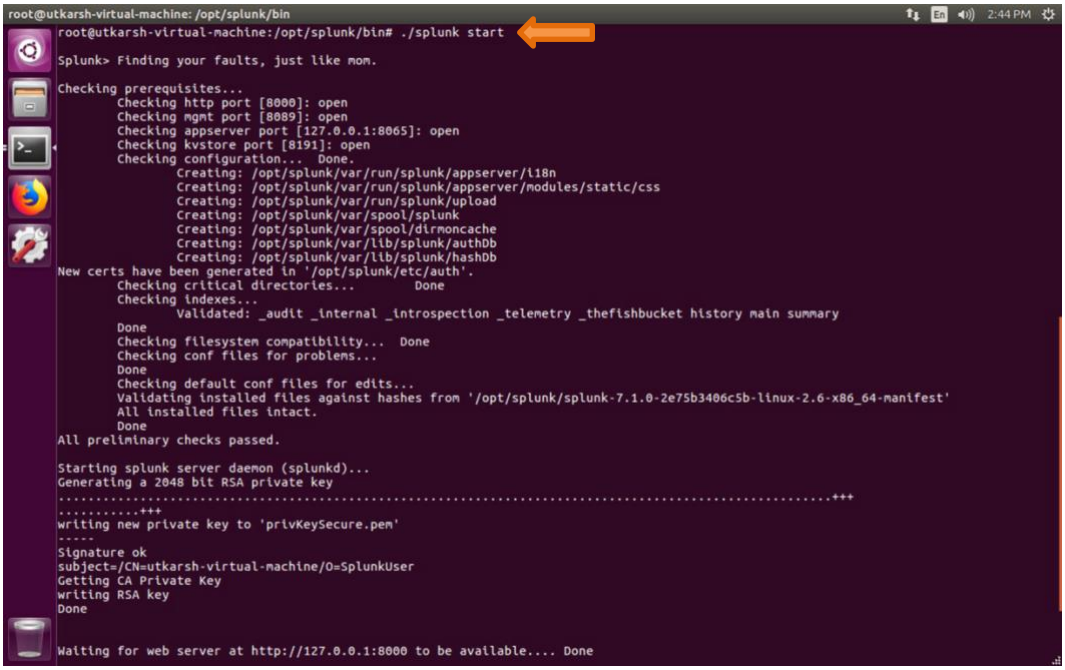
$ dpkg -I <package_name>



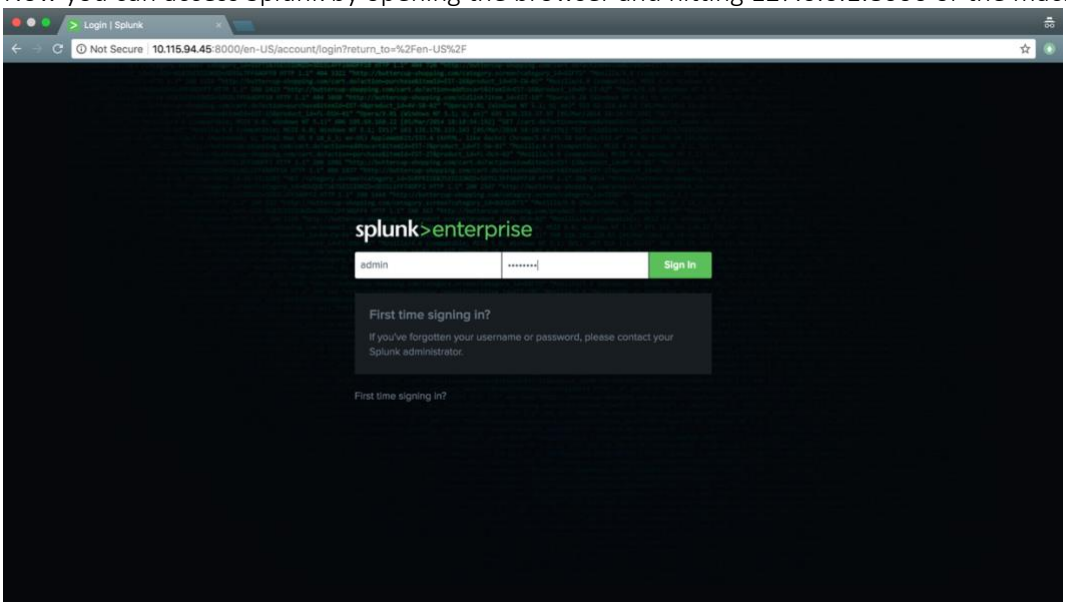
Splunk is installed in the '/opt' directory:
To start Splunk use the below command

$ cd /opt/splunk/bin
$ ./splunk start

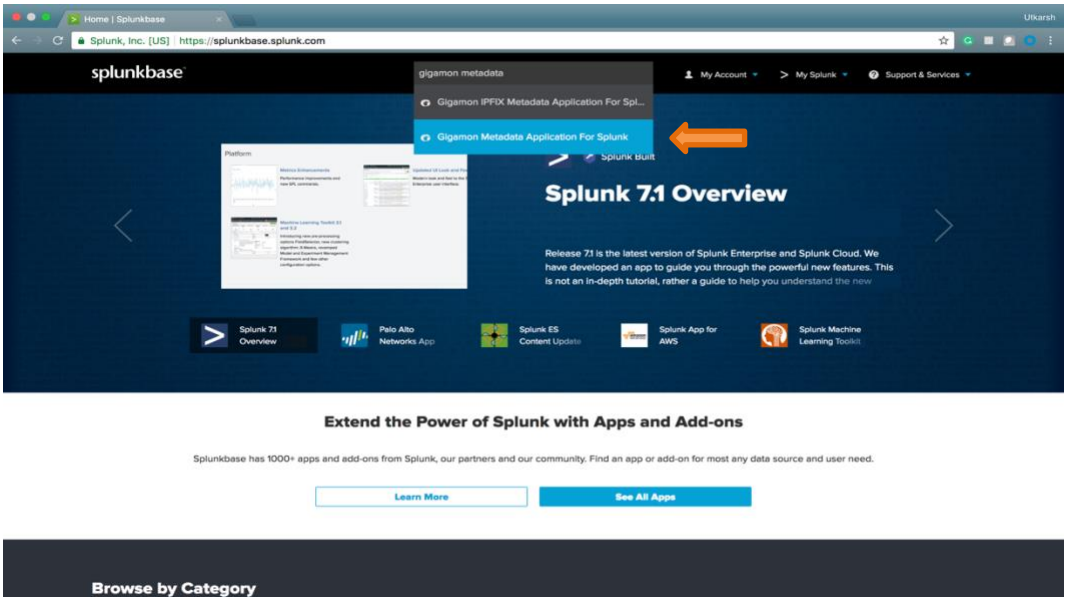
When you set up Splunk for the first time, it takes you over the license agreement, hit yes and create a password.

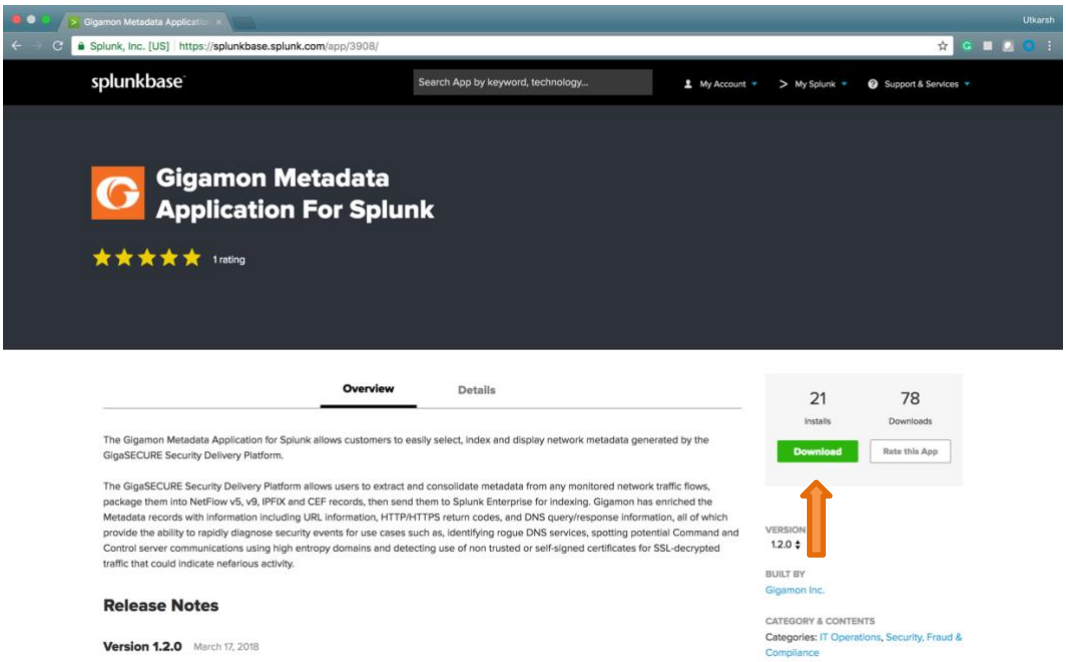


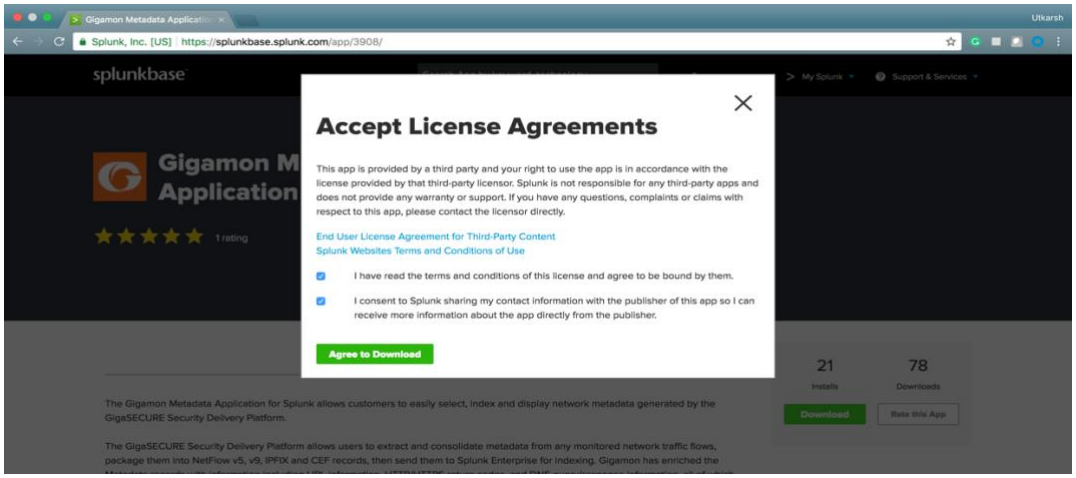
Now you can access Splunk by opening the browser and hitting 127.0.0.1:8000 or the machine's IP.

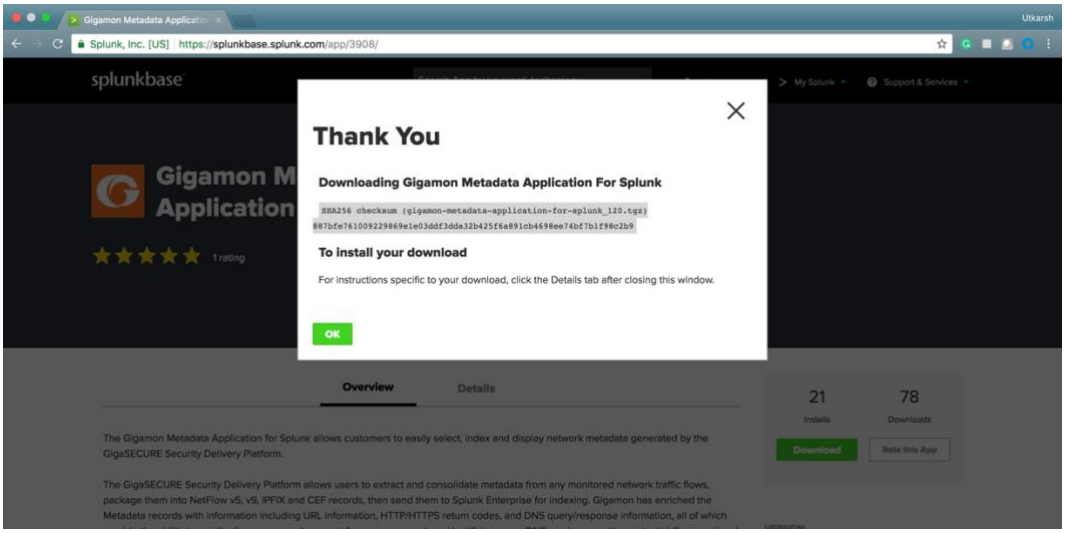


Downloading and installing the Gigamon Metadata Application for Splunk



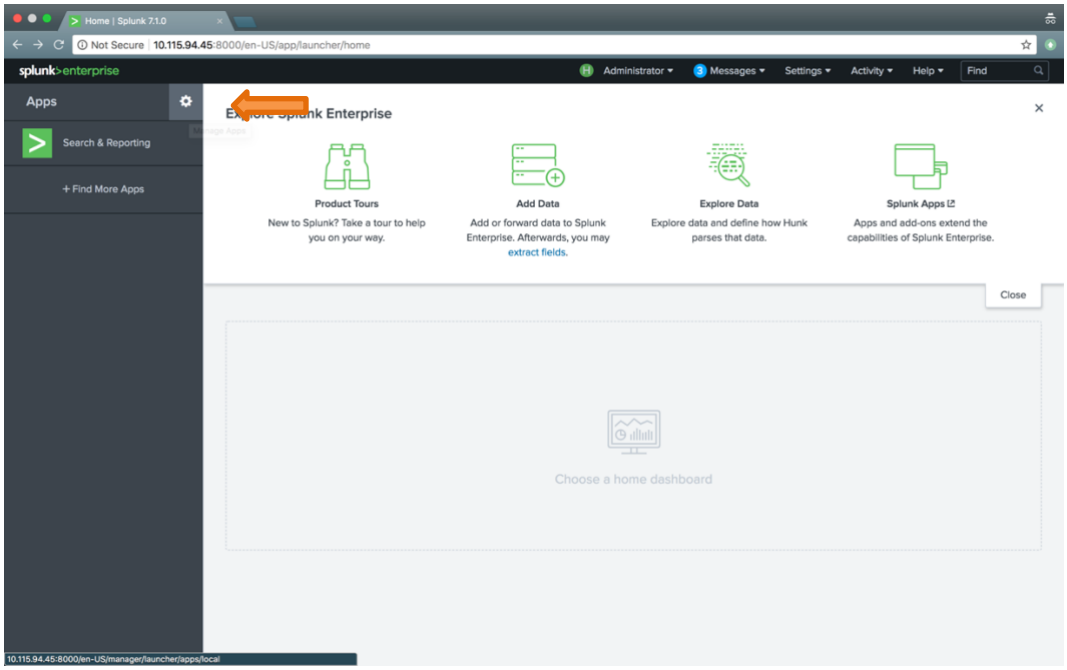




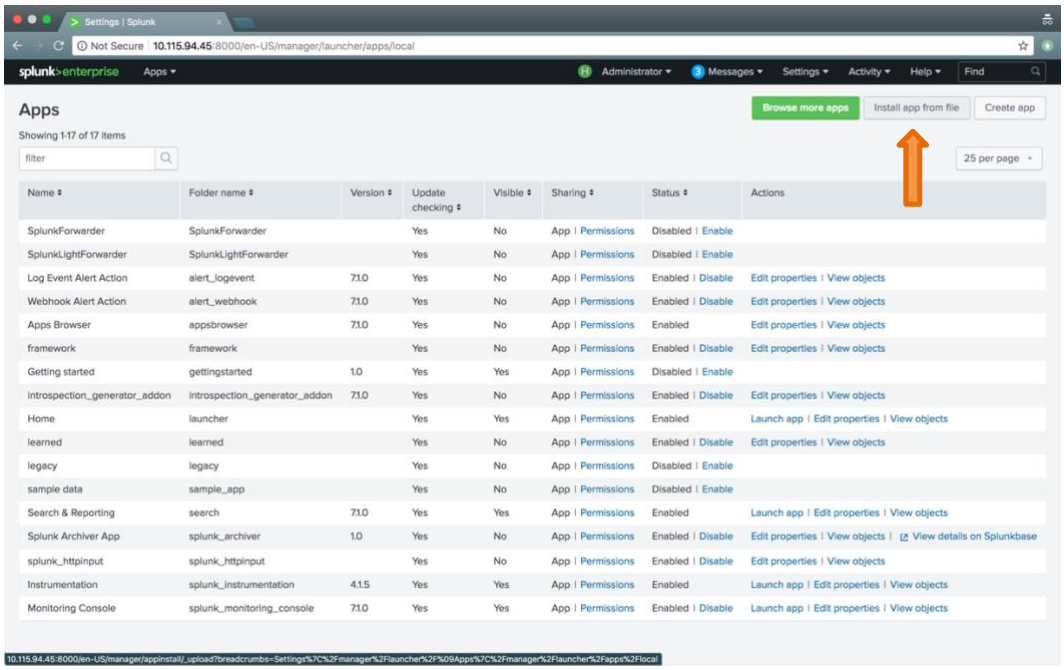


Similarly download “Splunk Stream” and “URL Toolbox” apps. *Splunk Stream is only required for IPFIX. If you just want CEF, you can skip installing Splunk Stream

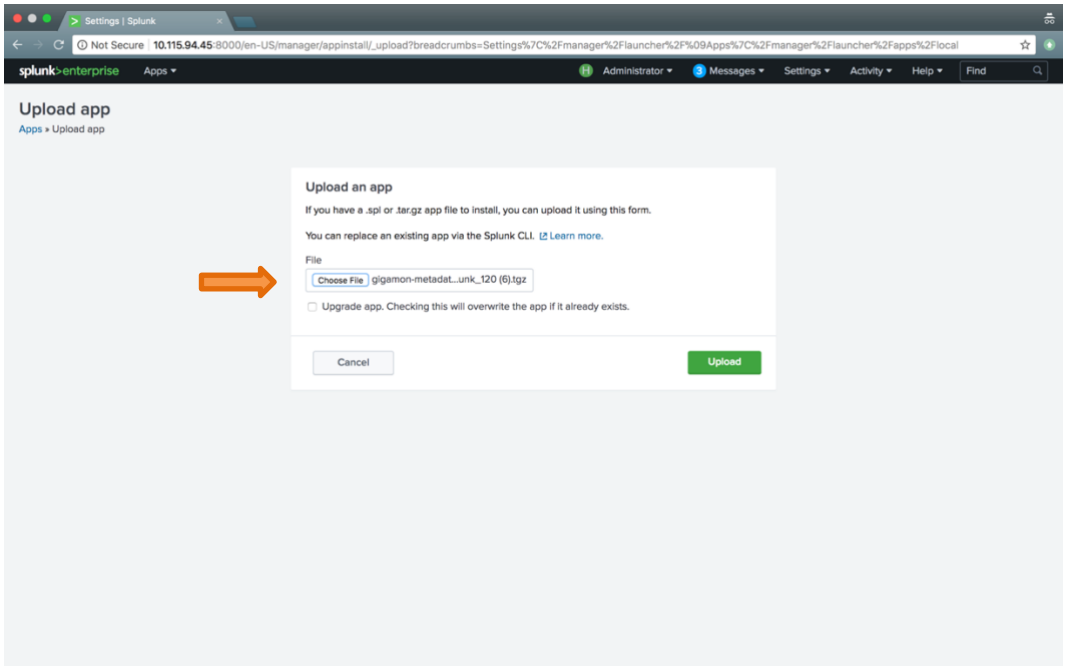
Now in Splunk, follow the steps to install these apps:
Click the wheel button near Apps.



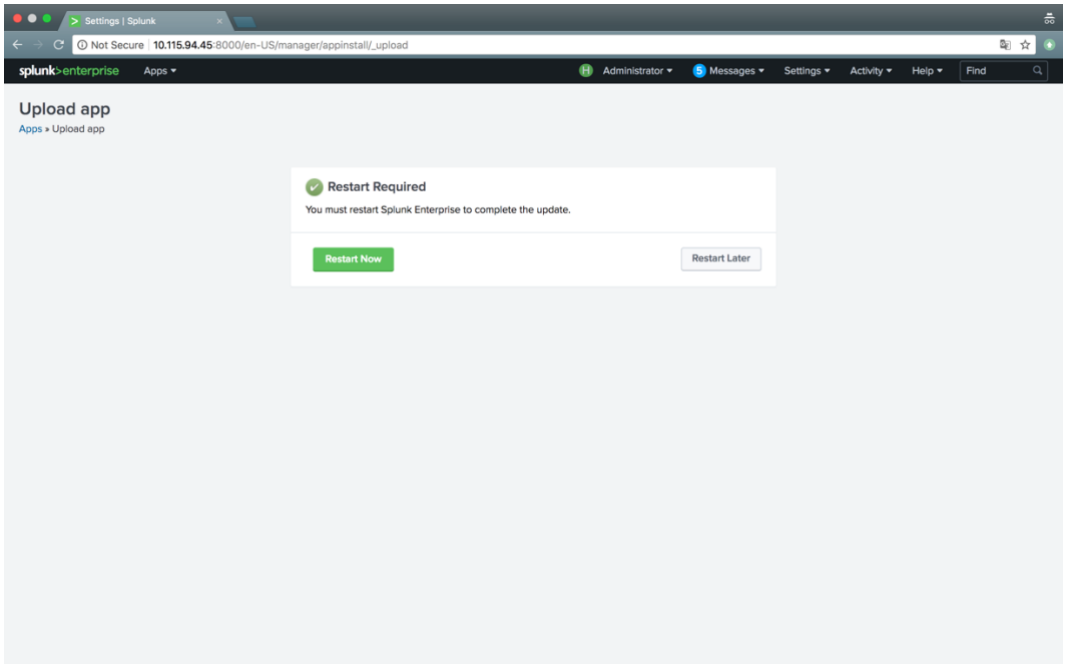
Click “install from file”



Choose the downloaded file to be installed



Restart Splunk to complete installation



Similarly, install the “Splunk Stream” and “URL Toolbox” apps. *Splunk Stream is only required for IPFIX. If you just want CEF, you can skip installing Splunk Stream

Configuring IPFIX Generation on GigaVUE node

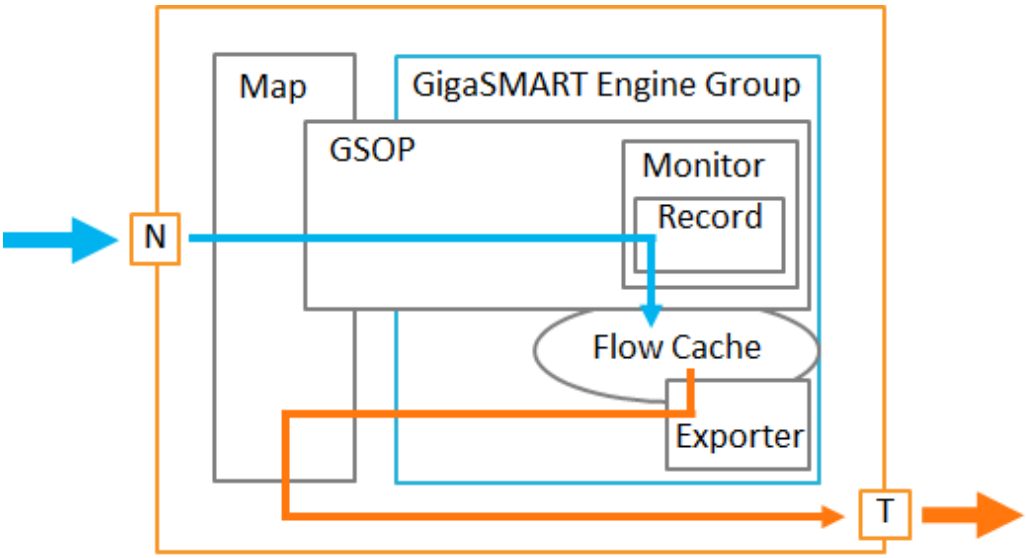
This section details the configuration required for IPFIX solution to work with Splunk. Configuration presented in this document are for representational purposes to get the deployment working. It can be completely customized as per your requirement. Detailed information about each individual element and how to configure NetFlow generation can be found in the GigaVUE-OS CLI User's Guide. Refer to the GigaVUE-OS CLI User's Guide on the Gigamon Customer Portal.

Configuration of IPFIX generation on a GigaVUE node is a simple and straight forward process involving three major steps.

Step 1: Setup the Tunnel Tool port that would be used to export the IPFIX records to the collector
Step 2: Define the NetFlow components – Records, Monitor and Exporter
Step 3: Setup the GigaSMART operation for NetFlow

For NetFlow/IPFIX generation on GigaVUE nodes, it should be noted that all the elements mentioned above should be bound to the same GigaSMART Engine Group.

The below picture illustrates the packet flow across various components inside GigaVUE node for IPFIX record generation.



This guide uses GigaVUE FM Workflow to configure IPFIX generation on GigaVUE node. Steps detailed in this guide can also be performed using the H-VUE web interface, as well as outside Workflows within Fabric Manager by selecting GigaSMART® from the left menu on the web interface. CLI configuration has also been presented in the Annexure for reference purposes.

Configuration to generate IPFIX

Summary of below config:

- Input traffic feed is connected to port 1/1/x1
- Tunnel is created on port 1/1/g1 which is connected to the machine(or VM) running Splunk and has the interface ip configured to 10.2.0.41
- Here, we use the destination IP 10.2.0.41 netmask 255.255.255.0 and destination port 2055

Tips for below config:

- SSH into the H series device to use the below config

  ssh <UserName>@<IP> i.e. ssh admin@10.115.90.1
- Use the commands: “enable” and “config terminal” before you start using the below config
- Do not copy paste the entire config at once. This might cause the device to be unresponsive. Copy paste the commands in one paragraph together.

```
port 1/1/x1 params admin enable
port 1/1/x2 type network
port 1/1/g1 type tool
port 1/1/g1 params admin enable


apps netflow exporter alias metadata_exporter
 destination ip4addr 10.2.0.41
 dscp 10
 format netflow version ipfix
 transport udp 2055
 template-refresh-interval 50
 ttl 64
 exit

## Gsgroup configurations
apps netflow record alias dns-1
 netflow-version ipfix
 export-blank-pen no
 sampling set 1 in 1
 collect add private pen gigamon dns additional-class
 collect add private pen gigamon dns authority-type-text
 collect add private pen gigamon dns bits
 collect add private pen gigamon dns additional-class-text
 collect add private pen gigamon dns identifier
 collect add ipv4 protocol
 collect add ipv4 source address
 collect add ipv4 destination address
 collect add transport tcp source-port
 collect add transport tcp destination-port
 collect add transport udp source-port
 collect add private pen gigamon dns ar-count
 collect add transport udp destination-port
 collect add private pen gigamon dns additional-name
 collect add private pen gigamon dns additional-rd-length
 collect add private pen gigamon dns additional-rdata
 collect add private pen gigamon dns additional-ttl
 collect add private pen gigamon dns additional-type
 collect add private pen gigamon dns additional-type-text
 collect add private pen gigamon dns an-count
 collect add private pen gigamon dns authority-class
 collect add private pen gigamon dns authority-class-text
 collect add private pen gigamon dns authority-name
 collect add private pen gigamon dns authority-rd-length
 collect add private pen gigamon dns authority-rdata
 collect add private pen gigamon dns authority-ttl
 collect add private pen gigamon dns authority-type
 match add ipv4 source address
 match add ipv4 destination address
 match add transport source-port
 match add transport destination-port
 match add ipv4 protocol
 exit
```

```
apps netflow record alias dns-2
 netflow-version ipfix
 export-blank-pen no
 sampling set 1 in 1
 collect add private pen gigamon dns ns-count
 collect add private pen gigamon dns response-rdata
 collect add private pen gigamon dns response-ttl
 collect add private pen gigamon dns op-code
 collect add private pen gigamon dns response-type
 collect add private pen gigamon dns response-type-text
 collect add ipv4 source address
 collect add ipv4 destination address
 collect add transport tcp source-port
 collect add transport tcp destination-port
 collect add transport udp source-port
 collect add private pen gigamon dns response-class-text
 collect add transport udp destination-port
 collect add ipv4 protocol
 collect add private pen gigamon dns qd-count
 collect add private pen gigamon dns query-class
 collect add private pen gigamon dns query-class-text
 collect add private pen gigamon dns query-name
 collect add private pen gigamon dns query-type
 collect add private pen gigamon dns query-type-text
 collect add private pen gigamon dns response-class
 collect add private pen gigamon dns response-code
 collect add private pen gigamon dns response-ipv4-addr
 collect add private pen gigamon dns response-ipv4-addr-text
 collect add private pen gigamon dns response-ipv6-addr
 collect add private pen gigamon dns response-ipv6-addr-text
 collect add private pen gigamon dns response-name
 collect add private pen gigamon dns response-rd-length
 match add ipv4 source address
 match add ipv4 destination address
 match add transport source-port
 match add transport destination-port
 match add ipv4 protocol
 exit

apps netflow record alias http
 netflow-version ipfix
 export-blank-pen no
 sampling set 1 in 1
 collect add private pen gigamon http response-code
 collect add private pen gigamon http url width 249
 collect add private pen gigamon http user-agent width 240
 collect add transport tcp destination-port
 collect add transport tcp source-port
 collect add ipv4 destination address
 collect add ipv4 source address
 match add ipv4 source address
 match add ipv4 destination address
 match add transport source-port
```

```
 match add transport destination-port
 match add ipv4 protocol
 exit

apps netflow record alias ssl
 netflow-version ipfix
 export-blank-pen no
 sampling set 1 in 1
 collect add private pen gigamon ssl certificate issuer
 collect add private pen gigamon ssl server cipher-text
 collect add private pen gigamon ssl server compressionMethod
 collect add private pen gigamon ssl certificate issuerCommonName
 collect add private pen gigamon ssl server nameIndication
 collect add private pen gigamon ssl server sessionId
 collect add private pen gigamon ssl server version
 collect add private pen gigamon ssl server version-text
 collect add ipv4 destination address
 collect add ipv4 source address
 collect add transport tcp source-port
 collect add private pen gigamon ssl certificate subjectAltName
 collect add transport tcp destination-port
 collect add private pen gigamon ssl certificate serialNumber
 collect add private pen gigamon ssl certificate serialNumber-text
 collect add private pen gigamon ssl certificate signatureAlgorithm
 collect add private pen gigamon ssl certificate signatureAlgorithm-text
 collect add private pen gigamon ssl certificate subject
 collect add private pen gigamon ssl certificate subjectAlgorithm
 collect add private pen gigamon ssl certificate subjectAlgorithm-text
 collect add private pen gigamon ssl certificate subjectCommonName
 collect add private pen gigamon ssl certificate subjectKeySize
 collect add private pen gigamon ssl certificate validNotAfter
 collect add private pen gigamon ssl certificate validNotAfter-text
 collect add private pen gigamon ssl certificate validNotBefore
 collect add private pen gigamon ssl certificate validNotBefore-text
 collect add private pen gigamon ssl server cipher
 match add ipv4 source address
 match add ipv4 destination address
 match add transport source-port
 match add transport destination-port
 match add ipv4 protocol
 exit


gsgroup alias gsgrp_netflow port-list 1/1/e1

##
## Tunnel configurations
##
apps netflow monitor alias metadata_monitor
 cache timeout active 60
 cache timeout inactive 15
 cache timeout event transaction-end
 sampling set no-sampling
 port-list all
```

```
 record add dns-1
 record add dns-2
 record add ssl
 record add http
 exit

tunneled-port 1/1/g1 ip 10.2.0.40 255.255.255.0 gateway 10.2.0.41 mtu 1500 port-list gsgrp_netflow

## Tunnel netflow exporter configurations

tunneled-port 1/1/g1 netflow-exporter add metadata_exporter


## Gs params configurations
gsparams gsgroup gsgrp_netflow
 cpu utilization type total rising 80
 dedup-action drop
 dedup-ip-tclass include
 dedup-ip-tos include
 dedup-tcp-seq include
 dedup-timer 50000
 dedup-vlan ignore
 eng-watchdog-timer 60
 erspan3-timestamp format none
 flow-mask disable
 flow-sampling-rate 5
 flow-sampling-timeout 1
 flow-sampling-type device-ip
 generic-session-timeout 5
 gtp-control-sample enable
 gtp-flow timeout 48
 gtp-persistence disable
 gtp-persistence file-age-timeout 30
 gtp-persistence interval 10
 gtp-persistence restart-age-time 30
 ip-frag forward enable
 ip-frag frag-timeout 10
 ip-frag head-session-timeout 30
 lb failover disable
 lb failover-thres lt-bw 80
 lb failover-thres lt-pkt-rate 1000
 lb replicate-gtp-c disable
 lb use-link-spd-wt disable
 netflow-monitor add metadata_monitor
 resource buffer-asf disable
 resource cpu overload-threshold 90
 resource hsm-ssl buffer disable
 resource hsm-ssl packet-buffer 1000
 resource hsm-ssl session-count 1
 sip-media timeout 30
 sip-session timeout 30
 sip-tcp-idle-timeout 20
 ssl-decrypt decrypt-fail-action drop
 ssl-decrypt enable
```

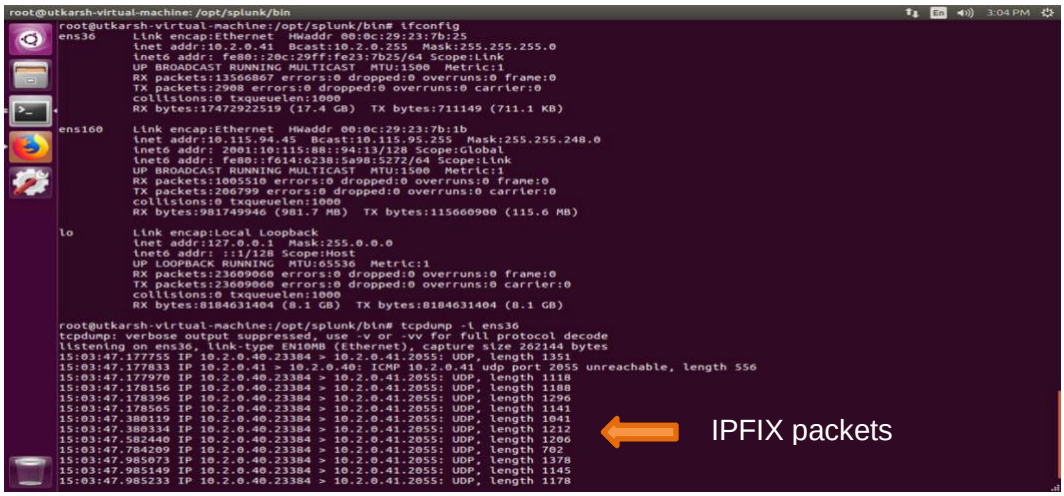
```
 ssl-decrypt hsm-pkcs11 dynamic-object enable
 ssl-decrypt hsm-pkcs11 load-sharing enable
 ssl-decrypt hsm-timeout 1000
 ssl-decrypt key-cache-timeout 10800
 ssl-decrypt non-ssl-traffic drop
 ssl-decrypt pending-session-timeout 60
 ssl-decrypt session-timeout 300
 ssl-decrypt tcp-syn-timeout 20
 ssl-decrypt ticket-cache-timeout 10800
 tunnel-arp-timeout 600
 tunnel-health-check action pass
 tunnel-health-check disable
 tunnel-health-check dstport 54321
 tunnel-health-check interval 600
 tunnel-health-check protocol icmp
 tunnel-health-check rcvport 54321
 tunnel-health-check retries 5
 tunnel-health-check roundtriptime 1
 tunnel-health-check srcport 54321
 tunnel-ndp-timeout 600
 exit

##
## Gsop configurations
##
gsop alias gsop_netflow flow-ops netflow port-list gsgrp_netflow

##
## Traffic map connection configurations
##
map alias Ipfix_Metadata_to_Splunk
 type regular byRule
 roles replace admin to owner_roles
 comment "export DNS,SSL,URL,HTTP metadata to SIEM tools like SPLUNK for analysis"
 use gsop gsop_netflow
 rule add pass ipver 4
 to 1/1/g1
 from 1/1/x1
 exit
```

Verifying the configuration

On Gigamon Device:

```
Utk-HC1 (config) # show tunneled-port
=============================================================================================================================
Port      mac address          ip address                    mask              gw                mtu   gsgroup   gw status          aging time
-----------------------------------------------------------------------------------------------------------------------------
1/1/g1    00:1D:AC:2F:27:AF    10.2.0.40                     255.255.255.0     10.2.0.41         1500  gsgrp_netflow Arp Resolved      05:55
Exporter[1]:metadata_exporter
Utk-HC1 (config) # show tunnel-po
% Unrecognized command "tunnel-po".
Type "show ?" for help.
Utk-HC1 (config) # show tunneled-port
brief  ipv4   ipv6   port   stats
Utk-HC1 (config) # show tunneled-port stats

=============================================================
Tunnel port: 1/1/g1   Type : ipv4
=============================================================
        rx_packets                  : 501
        rx_octets                   : 278065
        tx_packets                  : 754869
        tx_octets                   : 990265998
        pkts_drop                   : 0
        pkts_drop_no_arp            : 0
        pkts_drop_wrong_addr        : 0
  ARP
        pkts_arp_in                 : 28
        pkts_arp_req_in             : 15
        pkts_arp_rep_in             : 13
        pkts_arp_req_out            : 5360
        pkts_arp_rep_out            : 15
        pkts_arp_drop               : 0
  ICMP
        pkts_icmp_in                : 473
        pkts_ping_req_in            : 0
        pkts_ping_resp_out          : 0
        pkts_icmp_drop              : 0
  health-check
        pkt_health_chk_req_in       : 0
        pkt_health_chk_req_out      : 0
        pkt_health_chk_rep_in       : 473
        pkt_health_chk_rep_out      : 0
```

On the Machine(or VM) which has a Splunk instance:

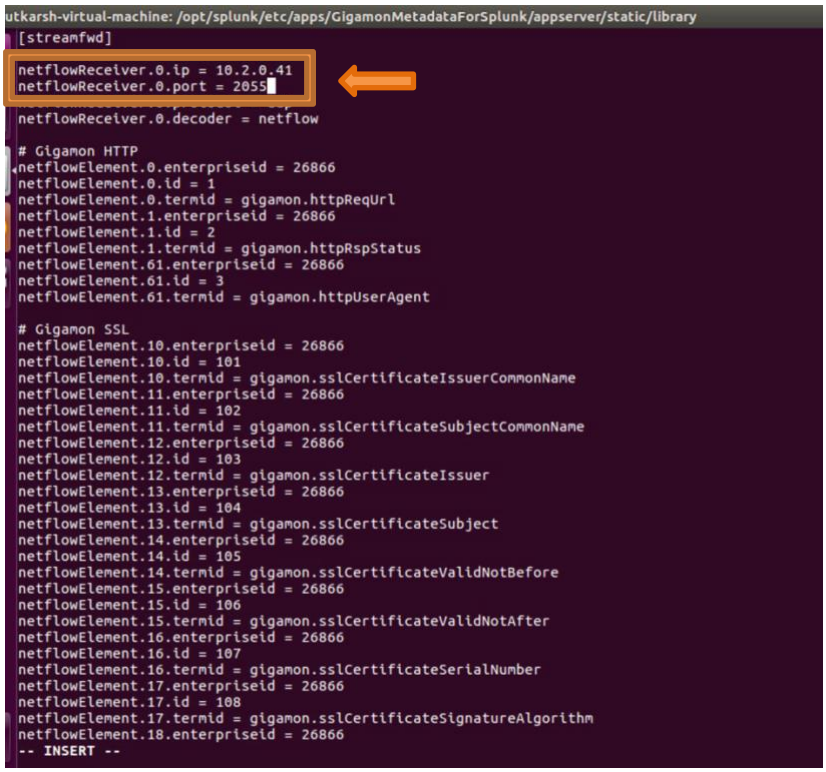


NOTE: the interface receiving IPFIX traffic should not be in promiscuous mode

Setting up Splunk to ingest IPFIX – Part 1 (file level changes)

The base location of the Gigamon-specific configuration is SPLUNK_HOME/etc/apps/GigamonMetadaForSplunk/appserver/static/library

When in the base directory, edit gigamon_streamfwd.conf to change the reciever IP and Port to your local settings (replace @@IP and @@PORT).



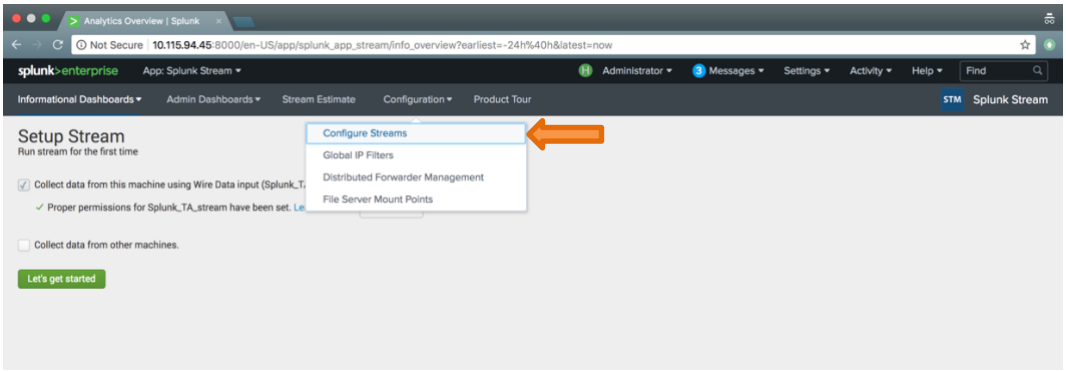
Now the simplest approach is to just use the below commands to copy the files from base directory to Splunk's internal directories: (just copy paste the below commands on terminal when in base directory, no need to modify any file manually thereafter) *these commands work only for ubuntu, for windows use appropriate commands to copy paste

```
cp gigamon_streamfwd.conf /opt/splunk/etc/apps/splunk_app_stream/local/streamfwd.conf
cp gigamon_streamfwd.conf /opt/splunk/etc/apps/Splunk_TA_stream/local/streamfwd.conf
cp gigamon_vocabulary_7.1.1.xml /opt/splunk/etc/apps/splunk_app_stream/default/vocabularies/gigamon.xml
cp gigamon_vocabulary_7.1.1.xml /opt/splunk/etc/apps/Splunk_TA_stream/default/vocabularies/gigamon.xml
cp gigamon_stream.json /opt/splunk/etc/apps/splunk_app_stream/default/streams/netflow
```

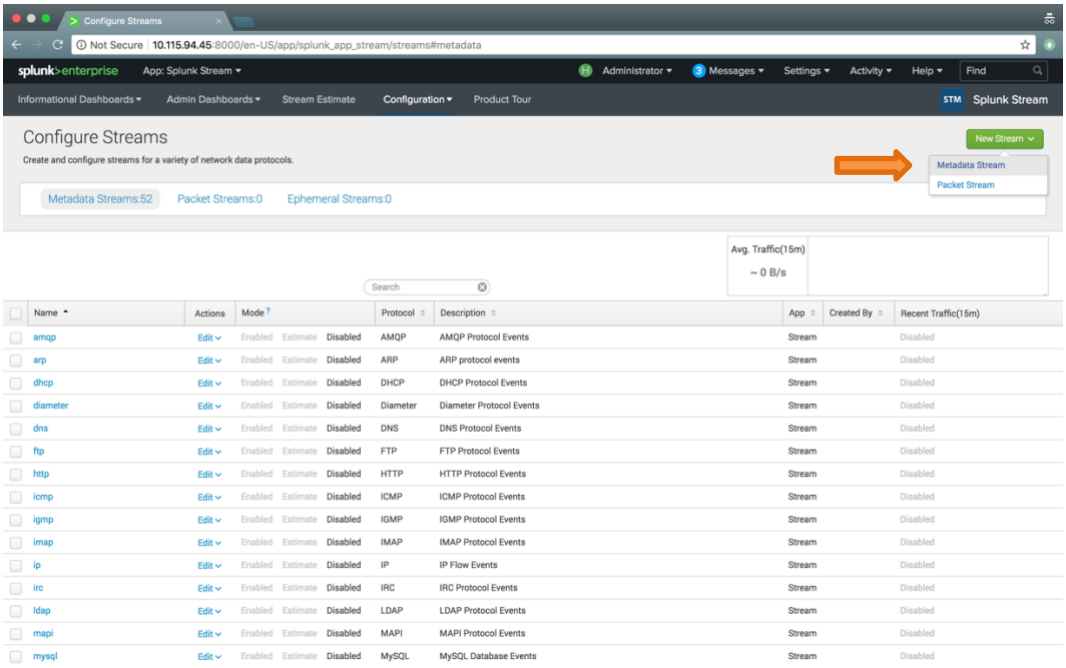
Setting up Splunk to ingest IPFIX- Part 2(within Splunk)

Now we need to Configure Stream via the steps at Stream Configuration

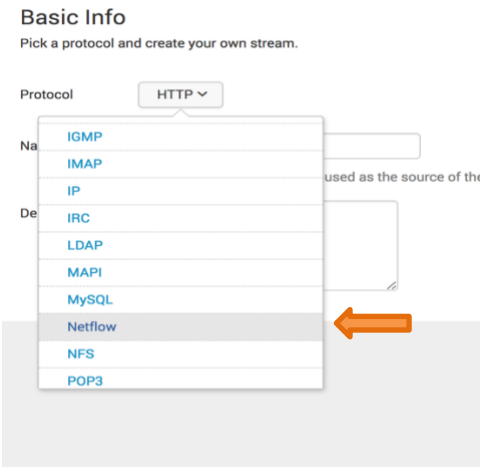
1. On the Splunk Home page, click on the app “Splunk Stream”
2. Use the navigation bar: **Configuration** -> **Configure Streams**

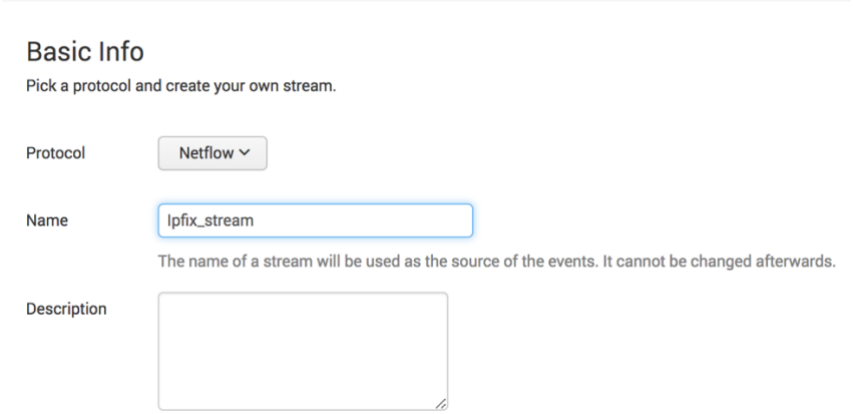


3. In the top right of the dashboard, click **New Stream** -> **Metadata Stream**
    1. (Full Documentation here)



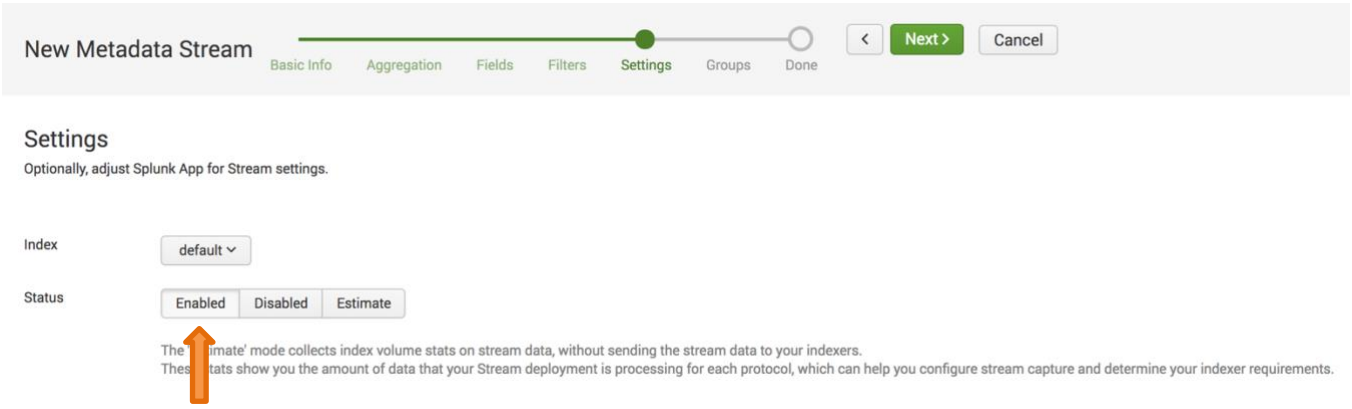
4. Basic Info
    1. **Protocol**: *Netflow*
    2. **Name**: *your source name*
3. Click **Next**





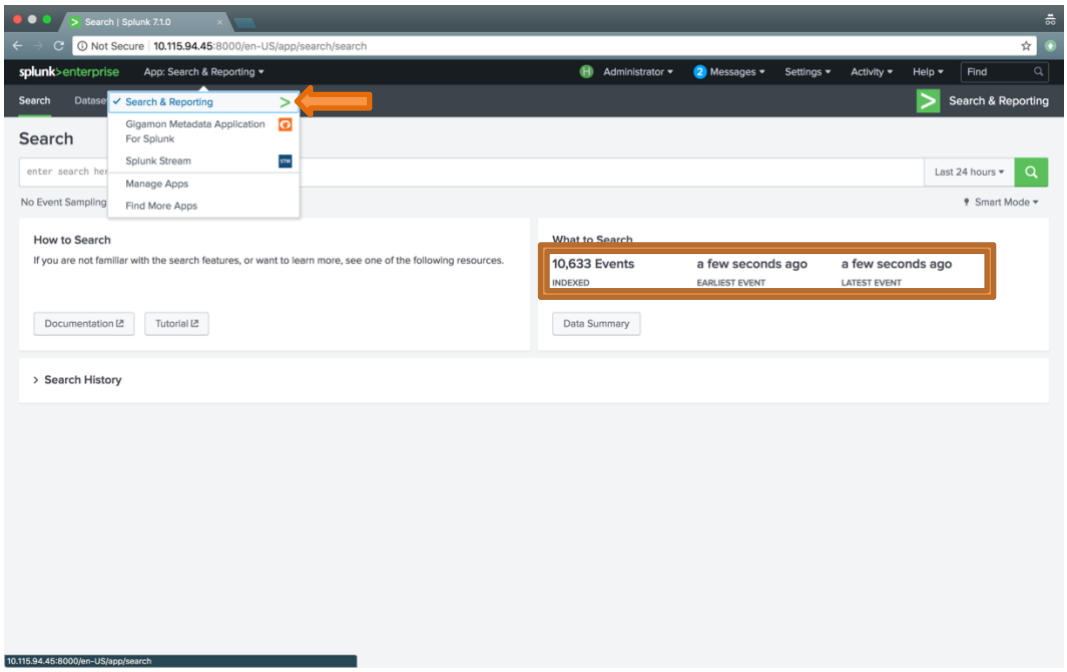
5. Aggregation (Full documentation here)
    1. Click **Next** to accept the default of No
6. Fields (Full documentation here)
    1. Deselect the fields that you do not want to collect
    2. Click **Next**
7. Filters (Full documentation here)
    1. Create a filter to limit the data that is collected
    2. Click **Next**

8. Settings
    1. Select an index to collect data to
    2. Select the status
    3. Click **Next**



9. Groups
    1. Select a forwarder group (if applicable)
    2. Click **Create Stream**
10. Done
    1. Click **Done**

Verifying the Setup



Configuring CEF Generation on GigaVUE node

Summary of below config:

- input traffic feed is connected to port 1/1/x1
- tunnel is created on port 1/1/g1 which is connected to the machine(or VM) running Splunk and has the interface IP configured to 10.2.0.41
- Here, we use the destination IP 10.2.0.41 netmask 255.255.255.0 and destination port 2055

Tips for below config:

- SSH into the H series device to use the below config

  ssh <UserName>@<IP> i.e. ssh admin@10.115.90.1
- Use the commands: “enable” and “config terminal” before you start using the below config
- Do not copy paste the entire config at once. This might cause the device to be unresponsive. Best practice is to copy paste the commands in one paragraph together.

Configuration to generate

```
port 1/1/x1 params admin enable
port 1/1/x2 type network
port 1/1/g1 type tool
port 1/1/g1 params admin enable


apps netflow exporter alias metadata_exporter
 destination ip4addr 10.2.0.41
 dscp 0
 format cef version 23
 transport udp 514
 template-refresh-interval 1800
 ttl 64
 exit

## Gsgroup configurations
apps netflow record alias dns-1
 netflow-version ipfix
 export-blank-pen no
 sampling set 1 in 1
 collect add private pen gigamon dns additional-class
 collect add private pen gigamon dns authority-type-text
 collect add private pen gigamon dns bits
 collect add private pen gigamon dns additional-class-text
 collect add private pen gigamon dns identifier
 collect add ipv4 protocol
 collect add ipv4 source address
 collect add ipv4 destination address
 collect add transport tcp source-port
 collect add transport tcp destination-port
 collect add transport udp source-port
 collect add private pen gigamon dns ar-count
 collect add transport udp destination-port
 collect add private pen gigamon dns additional-name
 collect add private pen gigamon dns additional-rd-length
 collect add private pen gigamon dns additional-rdata
 collect add private pen gigamon dns additional-ttl
 collect add private pen gigamon dns additional-type
 collect add private pen gigamon dns additional-type-text
 collect add private pen gigamon dns an-count
 collect add private pen gigamon dns authority-class
 collect add private pen gigamon dns authority-class-text
 collect add private pen gigamon dns authority-name
 collect add private pen gigamon dns authority-rd-length
 collect add private pen gigamon dns authority-rdata
 collect add private pen gigamon dns authority-ttl
 collect add private pen gigamon dns authority-type
 match add ipv4 source address
 match add ipv4 destination address
 match add transport source-port
 match add transport destination-port
```

```
  match add ipv4 protocol
  exit

apps netflow record alias dns-2
  netflow-version ipfix
  export-blank-pen no
  sampling set 1 in 1
  collect add private pen gigamon dns ns-count
  collect add private pen gigamon dns response-rdata
  collect add private pen gigamon dns response-ttl
  collect add private pen gigamon dns op-code
  collect add private pen gigamon dns response-type
  collect add private pen gigamon dns response-type-text
  collect add ipv4 source address
  collect add ipv4 destination address
  collect add transport tcp source-port
  collect add transport tcp destination-port
  collect add transport udp source-port
  collect add private pen gigamon dns response-class-text
  collect add transport udp destination-port
  collect add ipv4 protocol
  collect add private pen gigamon dns qd-count
  collect add private pen gigamon dns query-class
  collect add private pen gigamon dns query-class-text
  collect add private pen gigamon dns query-name
  collect add private pen gigamon dns query-type
  collect add private pen gigamon dns query-type-text
  collect add private pen gigamon dns response-class
  collect add private pen gigamon dns response-code
  collect add private pen gigamon dns response-ipv4-addr
  collect add private pen gigamon dns response-ipv4-addr-text
  collect add private pen gigamon dns response-ipv6-addr
  collect add private pen gigamon dns response-ipv6-addr-text
  collect add private pen gigamon dns response-name
  collect add private pen gigamon dns response-rd-length
  match add ipv4 source address
  match add ipv4 destination address
  match add transport source-port
  match add transport destination-port
  match add ipv4 protocol
  exit

apps netflow record alias http
  netflow-version ipfix
  export-blank-pen no
  sampling set 1 in 1
  collect add private pen gigamon http response-code
  collect add private pen gigamon http url width 249
  collect add private pen gigamon http user-agent width 240
  collect add transport tcp destination-port
  collect add transport tcp source-port
  collect add ipv4 destination address
  collect add ipv4 source address
  match add ipv4 source address
```

```
 match add ipv4 destination address
 match add transport source-port
 match add transport destination-port
 match add ipv4 protocol
 exit

apps netflow record alias ssl
 netflow-version ipfix
 export-blank-pen no
 sampling set 1 in 1
 collect add private pen gigamon ssl certificate issuer
 collect add private pen gigamon ssl server cipher-text
 collect add private pen gigamon ssl server compressionMethod
 collect add private pen gigamon ssl certificate issuerCommonName
 collect add private pen gigamon ssl server nameIndication
 collect add private pen gigamon ssl server sessionId
 collect add private pen gigamon ssl server version
 collect add private pen gigamon ssl server version-text
 collect add ipv4 destination address
 collect add ipv4 source address
 collect add transport tcp source-port
 collect add private pen gigamon ssl certificate subjectAltName
 collect add transport tcp destination-port
 collect add private pen gigamon ssl certificate serialNumber
 collect add private pen gigamon ssl certificate serialNumber-text
 collect add private pen gigamon ssl certificate signatureAlgorithm
 collect add private pen gigamon ssl certificate signatureAlgorithm-text
 collect add private pen gigamon ssl certificate subject
 collect add private pen gigamon ssl certificate subjectAlgorithm
 collect add private pen gigamon ssl certificate subjectAlgorithm-text
 collect add private pen gigamon ssl certificate subjectCommonName
 collect add private pen gigamon ssl certificate subjectKeySize
 collect add private pen gigamon ssl certificate validNotAfter
 collect add private pen gigamon ssl certificate validNotAfter-text
 collect add private pen gigamon ssl certificate validNotBefore
 collect add private pen gigamon ssl certificate validNotBefore-text
 collect add private pen gigamon ssl server cipher
 match add ipv4 source address
 match add ipv4 destination address
 match add transport source-port
 match add transport destination-port
 match add ipv4 protocol
 exit


gsgroup alias gsgrp_netflow port-list 1/1/e1

##
## Tunnel configurations
##
apps netflow monitor alias metadata_monitor
 cache timeout active 60
 cache timeout inactive 15
 cache timeout event transaction-end
```

```
 sampling set no-sampling
 port-list all
 record add dns-1
 record add dns-2
 record add ssl
 record add http
 exit

tunneled-port 1/1/g1 ip 10.2.0.40 255.255.255.0 gateway 10.2.0.41 mtu 1500 port-list gsgrp_netflow

## Tunnel netflow exporter configurations

tunneled-port 1/1/g1 netflow-exporter add metadata_exporter


## Gs params configurations
gsparams gsgroup gsgrp_netflow
 cpu utilization type total rising 80
 dedup-action drop
 dedup-ip-tclass include
 dedup-ip-tos include
 dedup-tcp-seq include
 dedup-timer 50000
 dedup-vlan ignore
 eng-watchdog-timer 60
 erspan3-timestamp format none
 flow-mask disable
 flow-sampling-rate 5
 flow-sampling-timeout 1
 flow-sampling-type device-ip
 generic-session-timeout 5
 gtp-control-sample enable
 gtp-flow timeout 48
 gtp-persistence disable
 gtp-persistence file-age-timeout 30
 gtp-persistence interval 10
 gtp-persistence restart-age-time 30
 ip-frag forward enable
 ip-frag frag-timeout 10
 ip-frag head-session-timeout 30
 lb failover disable
 lb failover-thres lt-bw 80
 lb failover-thres lt-pkt-rate 1000
 lb replicate-gtp-c disable
 lb use-link-spd-wt disable
 netflow-monitor add metadata_monitor
 resource buffer-asf disable
 resource cpu overload-threshold 90
 resource hsm-ssl buffer disable
 resource hsm-ssl packet-buffer 1000
 resource hsm-ssl session-count 1
 sip-media timeout 30
 sip-session timeout 30
 sip-tcp-idle-timeout 20
```

```
 ssl-decrypt decrypt-fail-action drop
 ssl-decrypt enable
 ssl-decrypt hsm-pkcs11 dynamic-object enable
 ssl-decrypt hsm-pkcs11 load-sharing enable
 ssl-decrypt hsm-timeout 1000
 ssl-decrypt key-cache-timeout 10800
 ssl-decrypt non-ssl-traffic drop
 ssl-decrypt pending-session-timeout 60
 ssl-decrypt session-timeout 300
 ssl-decrypt tcp-syn-timeout 20
 ssl-decrypt ticket-cache-timeout 10800
 tunnel-arp-timeout 600
 tunnel-health-check action pass
 tunnel-health-check disable
 tunnel-health-check dstport 54321
 tunnel-health-check interval 600
 tunnel-health-check protocol icmp
 tunnel-health-check rcvport 54321
 tunnel-health-check retries 5
 tunnel-health-check roundtriptime 1
 tunnel-health-check srcport 54321
 tunnel-ndp-timeout 600
 exit

##
## Gsop configurations
##
gsop alias gsop_netflow flow-ops netflow port-list gsgrp_netflow

##
## Traffic map connection configurations
##
map alias cef_Metadata_to_Splunk
 type regular byRule
 roles replace admin to owner_roles
 comment "export DNS,SSL,URL,HTTP metadata to SIEM tools like SPLUNK for analysis"
 use gsop gsop_netflow
 rule add pass ipver 4
 to 1/1/g1
 from 1/1/x1
 exit
```

Verifying the configuration

On Gigamon Device:

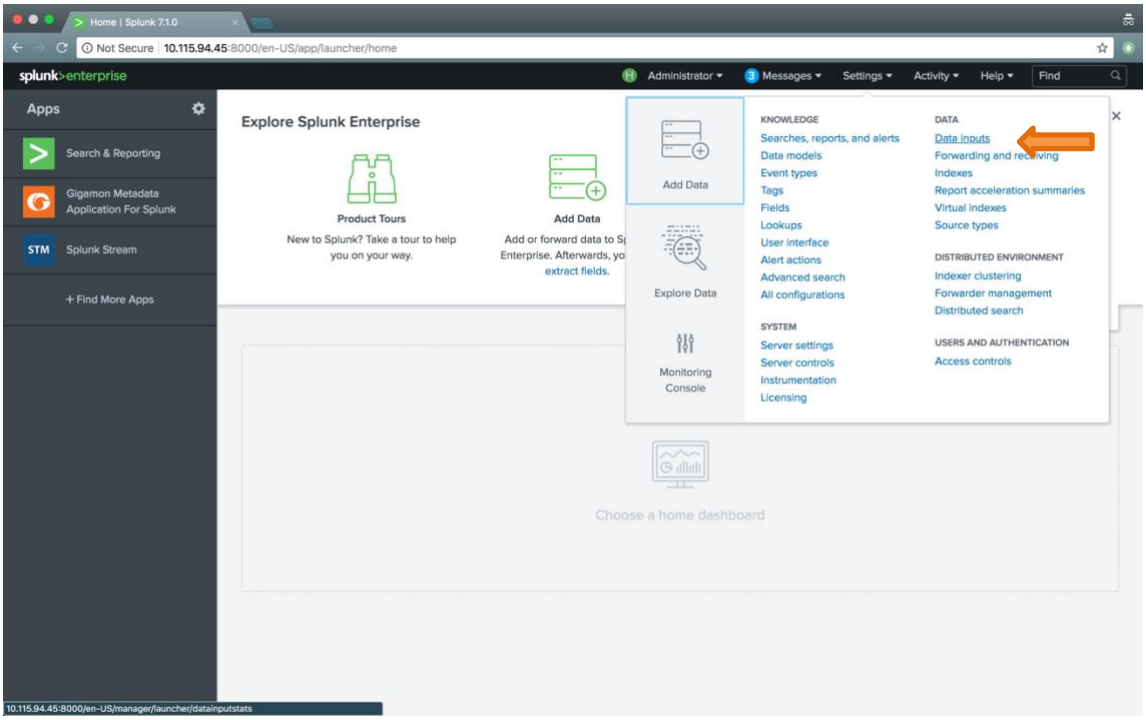
```
Utk-HC1 (config) # show tunneled-port
=============================================================================================================================
Port      mac address          ip address                    mask              gw                    mtu   gsgroup   gw status          aging time
-----------------------------------------------------------------------------------------------------------------------------
1/1/g1    00:1D:AC:2F:27:AF    10.2.0.40                     255.255.255.0     10.2.0.41             1500  gsgrp_netflow Arp Resolved      05:55
Exporter[1]:metadata_exporter
Utk-HC1 (config) # show tunnel-po
% Unrecognized command "tunnel-po".
Type "show ?" for help.
Utk-HC1 (config) # show tunneled-port
brief  ipv4   ipv6   port   stats
Utk-HC1 (config) # show tunneled-port stats

============================================================
Tunnel port: 1/1/g1   Type : ipv4
============================================================
        rx_packets                  : 501
        rx_octets                   : 278065
        tx_packets                  : 754869
        tx_octets                   : 990265998
        pkts_drop                   : 0
        pkts_drop_no_arp            : 0
        pkts_drop_wrong_addr        : 0
  ARP
        pkts_arp_in                 : 28
        pkts_arp_req_in             : 15
        pkts_arp_rep_in             : 13
        pkts_arp_req_out            : 5360
        pkts_arp_rep_out            : 15
        pkts_arp_drop               : 0
  ICMP
        pkts_icmp_in                : 473
        pkts_ping_req_in            : 0
        pkts_ping_resp_out          : 0
        pkts_icmp_drop              : 0
  health-check
        pkt_health_chk_req_in       : 0
        pkt_health_chk_req_out      : 0
        pkt_health_chk_rep_in       : 473
        pkt_health_chk_rep_out      : 0
```

On the Machine(or VM) which has a Splunk instance:

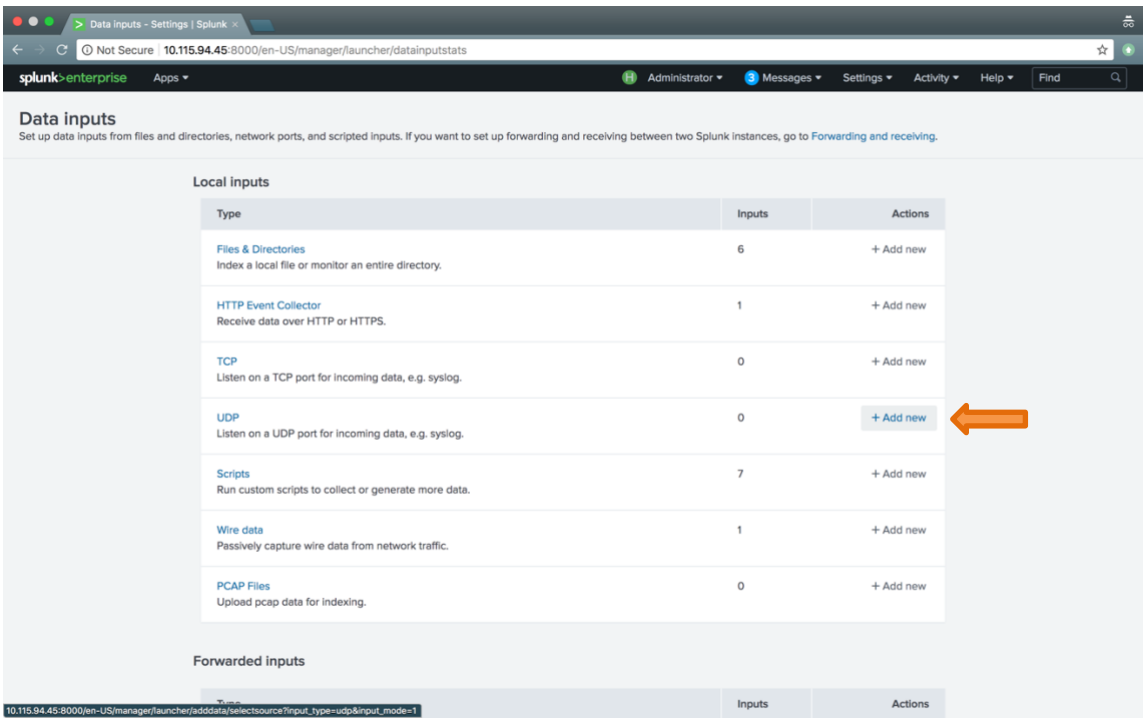
```
root@shiv-cef3:/home/shiv# ifconfig
ens36     Link encap:Ethernet  HWaddr 00:0c:29:2b:70:4b
          inet addr:10.0.0.41  Bcast:10.0.0.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe2b:704b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:16049615 errors:0 dropped:0 overruns:0 frame:0
          TX packets:30214 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:14405902132 (14.4 GB)  TX bytes:15628270 (15.6 MB)

ens160    Link encap:Ethernet  HWaddr 00:0c:29:2b:70:41
          inet addr:10.115.94.59  Bcast:10.115.95.255  Mask:255.255.248.0
          inet6 addr: fe80::3ace:44e6:7ff8:5dc6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1786535 errors:0 dropped:0 overruns:0 frame:0
          TX packets:262444 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:597581041 (597.5 MB)  TX bytes:253907416 (253.9 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:46184129 errors:0 dropped:0 overruns:0 frame:0
          TX packets:46184129 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:14451670084 (14.4 GB)  TX bytes:14451670084 (14.4 GB)

root@shiv-cef3:/home/shiv# tcpdump -i ens36
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens36, link-type EN10MB (Ethernet), capture size 262144 bytes
18:12:28.566445 IP 10.0.0.40.23384 > 10.0.0.41.10514: UDP, length 255
18:12:28.566611 IP 10.0.0.40.23384 > 10.0.0.41.10514: UDP, length 862
18:12:28.566853 IP 10.0.0.40.23384 > 10.0.0.41.10514: UDP, length 846
18:12:28.566974 IP 10.0.0.40.23384 > 10.0.0.41.10514: UDP, length 856
18:12:28.567103 IP 10.0.0.40.23384 > 10.0.0.41.10514: UDP, length 861
18:12:28.567447 IP 10.0.0.40.23384 > 10.0.0.41.10514: UDP, bad length 1526 > 1472
18:12:28.567452 IP 10.0.0.40 > 10.0.0.41: udp
```

Setting up Splunk to ingest CEF

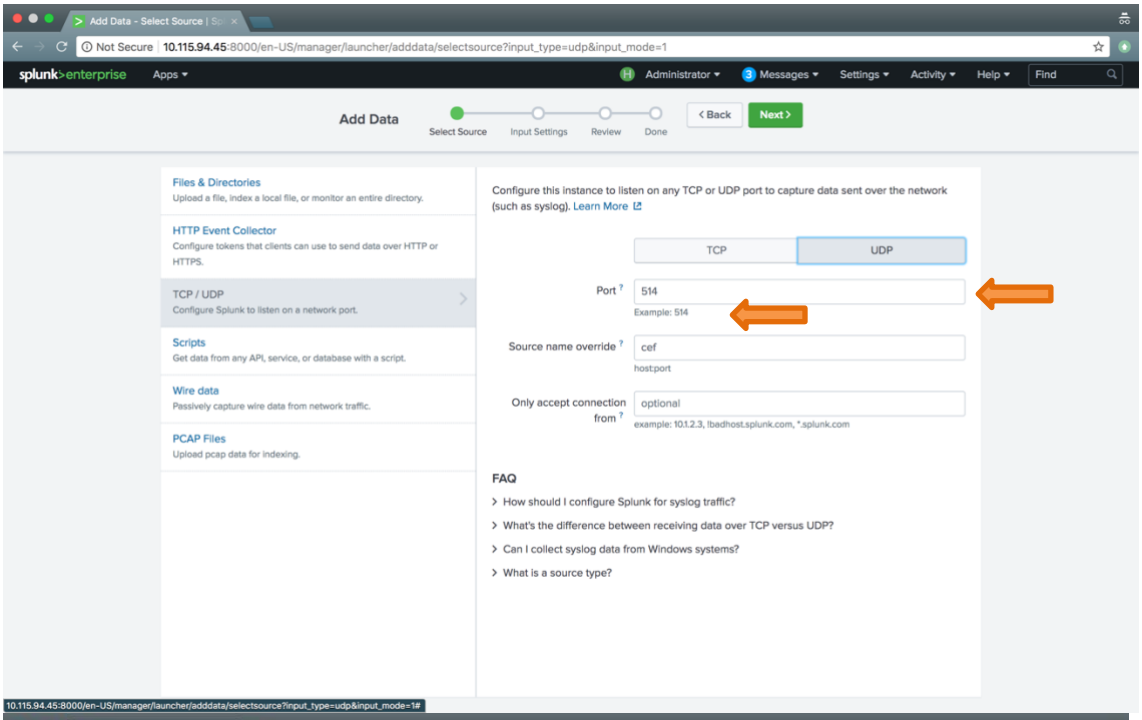
On Splunk web interface, click on the settings button:
Under “Data” find the option “Data inputs” and select it

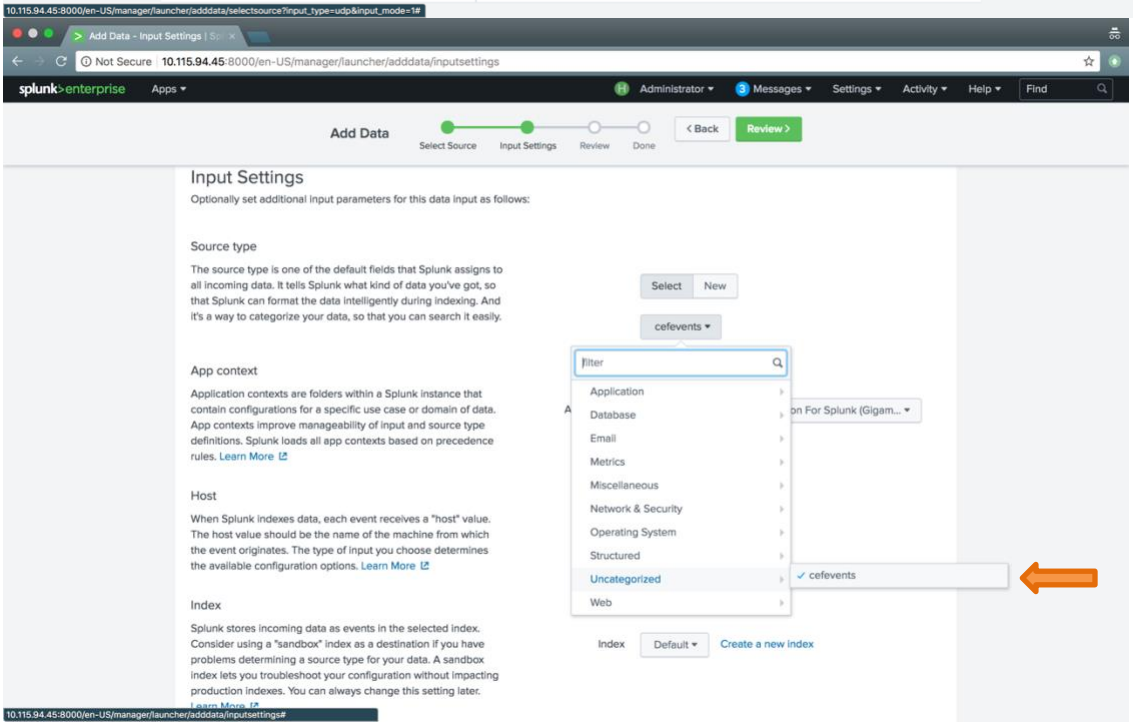


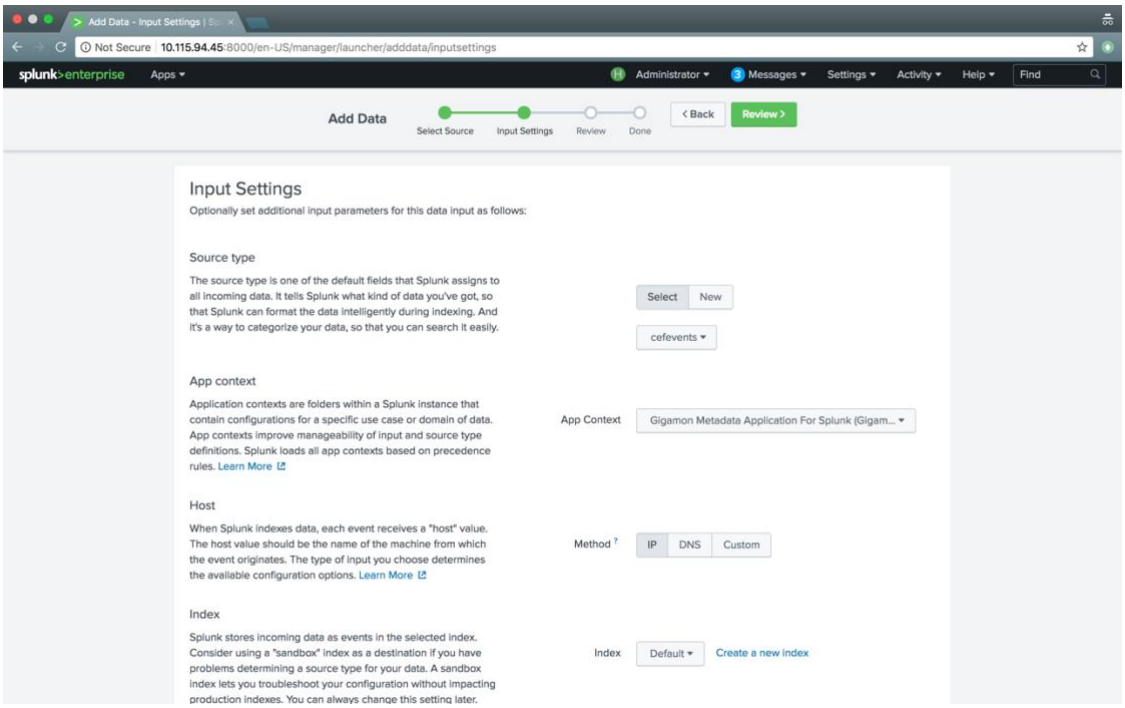
Add a new UDP input under Local inputs

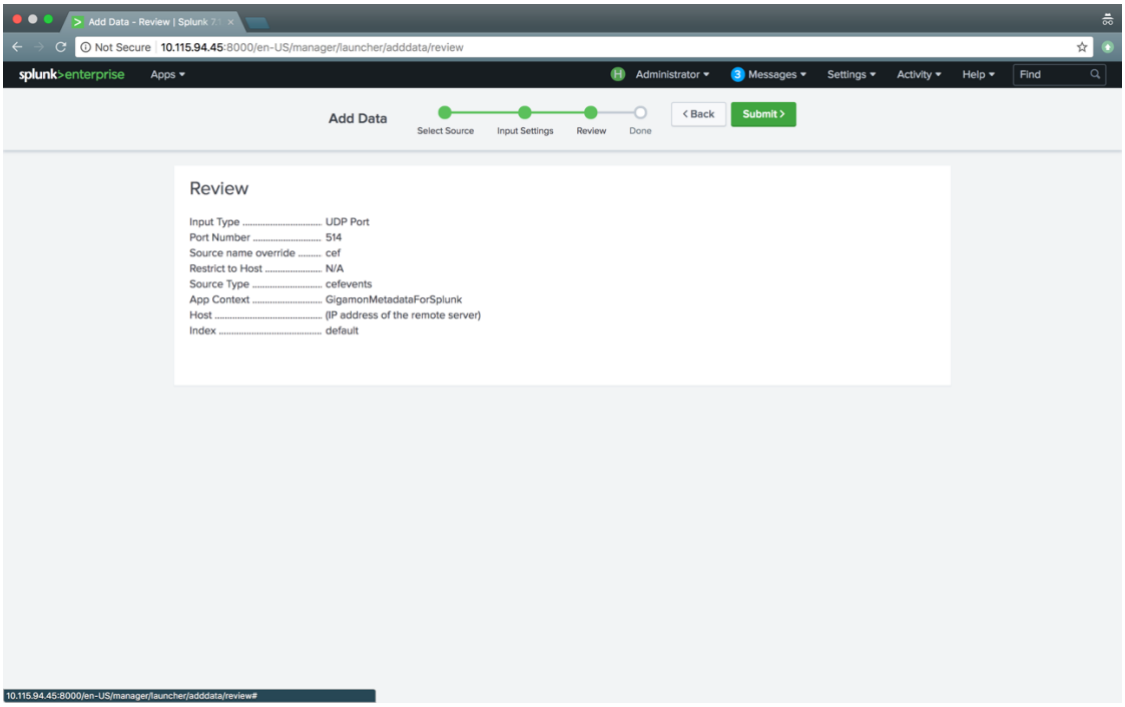


514 is the port number used. Change it to whatever the port number desired. Make sure that it matches with port number configuration on GigaSMART device.

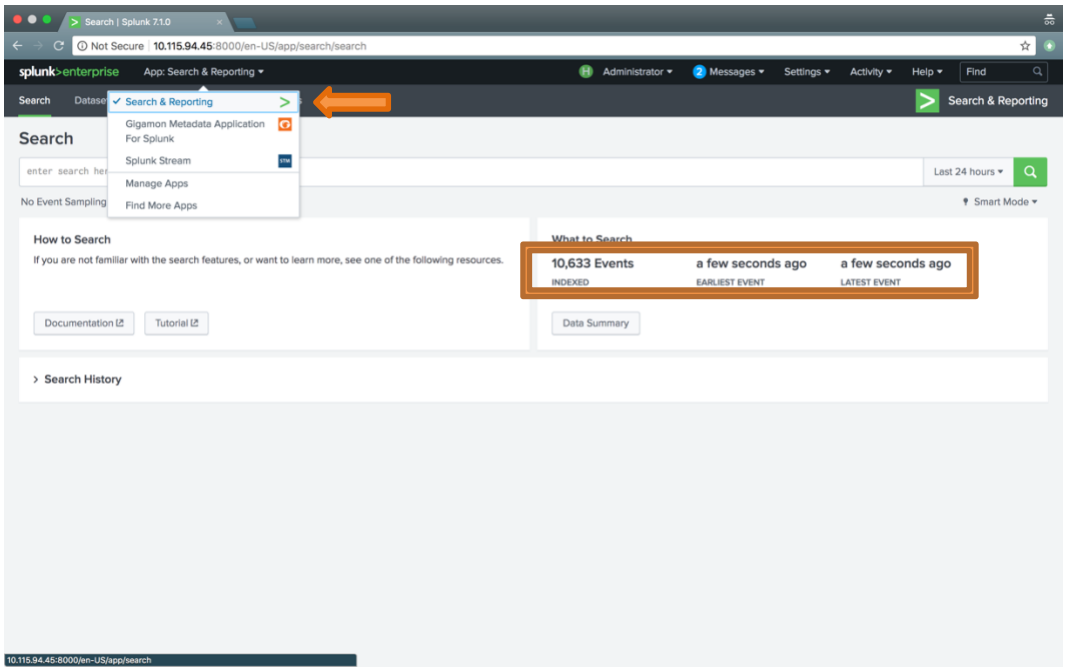





Add Data - Input Settings
Not Secure 10.115.94.45:8000/en-US/manager/launcher/adddata/inputsettings
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Add Data
Select Source
Input Settings
Review
Done
< Back
Review >
Input Settings
Optionally set additional input parameters for this data input as follows:
Source type
The source type is one of the default fields that Splunk assigns to all incoming data. It tells Splunk what kind of data you've got, so that Splunk can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.
Select
New
cefevents
App context
Application contexts are folders within a Splunk instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source type definitions. Splunk loads all app contexts based on precedence rules. Learn More
App Context
Gigamon Metadata Application For Splunk (Gigam...
Host
When Splunk indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. Learn More
Method
IP
DNS
Custom
Index
Splunk stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later.
Index
Default
Create a new index


Add Data - Review | Splunk
Not Secure 10.115.94.45:8000/en-US/manager/launcher/adddata/review
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Add Data
Select Source
Input Settings
Review
Done
< Back
Submit >
Review
Input Type ..... UDP Port
Port Number 514
Source name override ..... cef
Restrict to Host ..... N/A
Source Type ..... cefevents
App Context ..... GigamonMetadataForSplunk
Host ..... (IP address of the remote server)
Index ..... default
10.115.94.45:8000/en-US/manager/launcher/adddata/review#

Verifying the Setup



Summary

This document described the integration between Splunk SIEM and Gigamon's GigaSECURE Security Delivery Platform. By leveraging metadata, Splunk users can benefit by gaining increased non-intrusive visibility into their infrastructure while minimizing the amount of data that has to be searched through which, in turn, reduces the time to detect suspicious threats and anomalous behavior.

Appendix

Use cases available with Gigamon's custom metadata elements

SSL Widgets		
Widget	**What You See**	**What You Infer**
SSL Versions Seen	Shows different SSL versions seen in the network and their percentage. Current valid versions are TLSv1, TLSv1.1, TLSv1.2 & SSLv3.	• Percentage of connections (if any) running obsolete SSL versions (SSLv2, SSLv3). • Security compliance posture of the organization. • List of servers hosted on non-compliant version.
SSL Domains Accessed on Non-Standard Ports	Default port for SSL transaction is 443 but SSL transaction is seen on ports other than configured/allowed port list.	• Server misconfiguration. • Non-compliance. • Server/resources are compromised.
Top SSL Certificate Issuers	Shows the top Certificate issuers for a given time range.	• Are those certificates known & trusted • Drill down to see source IPs using unknown certificates.
Top SSL Cipher	Shows the top Ciphers seen in the network for a given time range.	• Only configured Ciphers should be seen. • Drill down to see source IPs using non-complaint ciphers.
SSL Self Signed Certificates	Lists all the self-signed certificates seen in the network.	• Determine whether the self-signed certificates are expected or not.
SSL Certificate Distribution	Shows the heat map of SSL certificates geographic location.	• Geographic location of SSL certificate origin.

DNS Widgets		
Widget	**What You See**	**What You Infer**
List of DNS Servers Seen	List of DNS servers seen in the network.	• List of DNS servers matches with expected configured list. • Unknown DNS servers could be due to misconfiguration or Rouge DNS server.
Top DNS Error Responses	Lists the top DNS error responses seen and their percentage.	• Status code seen are expected or not. • Timeline of the status code.
Top 10 DNS Queries	Lists top DNS Queries seen in the network for a given time period.	• Lists shows DNS query name, source and destination IP addresses, whether the query was successful or not and average TTL values.
DNS Traffic on Non-Standard Ports	DNS Query traffic seen on non-standard port. Standard port for DNS Query is 53.	• DNS service ran on non-standard ports. • Some other service (ex. LDAP) ran on DNS port.
Non-DNS Traffic on DNS Port (53)	This widget should be empty.	• One should not see non-DNS traffic on the standard DNS port 53. • There should not be any entries in this widget. If you see any entries in this widget then there is misconfiguration.
DNS Query Name Entropy	List of DNS domain names with Shannon Entropy values sorted from higher to lower value.	• The higher the entropy value, the higher the chance that the domain name is not valid. By using the entropy values, admins can determine whether a botnet or some kind of command-and-control is making random domain name queries.
Number of DNS Requests Over the Time	Line graph of DNS requests over a period of time.	• One can determine whether requests are sent to primary or secondary DNS server and time when the switchover has happened from primary to secondary or vice-versa.

URL Widgets		
Widget	**What You See**	**What You Infer**
Top HTTP Error Responses	HTTP/HTTPS status codes for the whole network and their percentage.	• Status code seen are expected. • Timeline of the status code.
TOP URL Domains Visited	Pie chart top URL domains seen for a given time range.	• Top URL domains are valid and expected.
Top URL Domains Visited by Client IP	Lists top URL domains visited by client IP addresses.	• Top URL domains are valid and expected • Drill down to see src & destination IP addresses.
URL Domain Entropy (Shannon Entropy)	List of URL domain names with Shannon Entropy values sorted from higher to lower value.	• The higher the entropy value, the higher the chance that the URL domain name is not valid. By using the entropy values, admins can determine whether a botnet or some kind of command-and-control is making random domain name queries.
Top Domains Visited on Non-Standard Ports	Lists URL domains visited using ports other than port 80 (for GTTP) and 443 (for HTTPS).	• HTTP and HTTPS servers running on non-standard ports. • How many HTTP/HTTPS servers running on same servers using different port numbers. • Compliance of the servers.
Count of URLs Accessed using Domain Name vs IP Address	Lists count of URLs accessed using Domain name vs using direct IP addresses.	• Lists count of URLs accessed using Domain name vs using direct IP addresses.