SentryWire
PACKET CAPTURE PLATFORM

FEDERATION MANAGER UI

USER GUIDE

Software Version: 7.3.0.309-408.14

Document version 1.13
12/01/2022

Document Revision History

Ver 1.0	Initial Release (#408.14)	05/31/2021
Ver 1.1	Added LDAP Map User details	06/05/2021
Ver 1.2	Merged Investigator View Guide with Administrator View Guide	06/19/2021
Ver 1.3	Removed static network access setup description.	07/17/2021
Ver 1.4	Updates to Expand IPv6, Map User, Search Library, BPF Help	09/10/2021
Ver 1.5	File Carving, System Health	10/20/2021
Ver 1.6	Support for multiple log receivers	11/10/2021
Ver 1.7	Minor updates/corrections	12/01/2021
Ver 1.8	File Carving Rules	02/24/2022
Ver 1.9	Appendix D – Splunk Forwarder	03/01/2022
Ver 1.10	Added KQL Search and GetPCAP, Removed JSON Search	08/03/2022
Ver 1.11	IDP for LDAP/AD Authentication/Authorization	09/30/2022
Ver 1.12	Changes due to embedded LDAP/AD Authentication	10/29/2022
Ver 1.13	Updated Investigator View	12/01/2022

Contents

INTRODUCTION

Federation Manager (FM) allows seamless access to services from one domain to another irrespective to the physical location of the capture server. The Federation Manager (FM) allows the user to manage several groups having multiple Federated Nodes (also referred to in this guide as FNs or nodes), and actively monitor and perform packet analysis on each one of them, from a central interface. Each Federated Node is a capture and analytics server responsible for capturing, storing and indexing of all received traffic and analytics data. The FN software captures all data/traffic traversing the network full duplex via Test Access Port (TAP) or SPAN ports and operates in passive mode. FN Software does concurrently capture inbound and outbound PCAP in standard libcap format for all traffic traversing the Internet Access Point (IAP), to include IPv6.Since each group in FM can have multiple Federated Nodes, any actions performed on a selected group applies to all nodes that are configured within the group.
Along with a central management, the administrators can actively monitor, execute, and view searches and track packet capture statistics across all connected Federated Nodes within the selected group. This provides increased scalability and allows the administrators to also detect and prioritize security threats, pinpoint performance issues and manage incident responses – all from a single control center.
The FM further allows the administrator to drill down into event details, perform root cause analysis and troubleshooting for all controlled federated nodes.
Before using this application, some basic initial configuration is required. Please refer to the Quick Start Guide for details.

1.1 SUPPORTED WEB BROWSERS

- Google Chrome 44.0.2403.157 or above. (Preferred browser)
- Mozilla Firefox version 45.0.1 - 47.0.1

1.2 SETTING UP YOUR NETWORK

To ensure this application is accessible via web, an IP address must be assigned to one of the Ethernet ports before installing this application. The install process will confirm if the Management IP address is accurate. Please refer to RHEL 7/CentOS 7 network setup process to ensure the IP Address is set correctly.
SSH Access: After setting up an IP address locally, you can perform future operating system administrative functions by remote login via an SSH client. Configure your SSH client to connect using port 22.

1.3 UI USERNAME/PASSWORD

- Username must be minimum of 8 characters and maximum of 32 characters.
- Password has the following restrictions:
  - Must be minimum of 8 characters and maximum of 32 characters.
  - Must have at least 1 uppercase character, 1 lowercase character, 1 special character
    - Allowed special characters for password:
      !@#&*$
  - Spaces, % ,^, Backslash "\" or Forward slash "/"is not allowed.
  - $ is not allowed in the beginning.

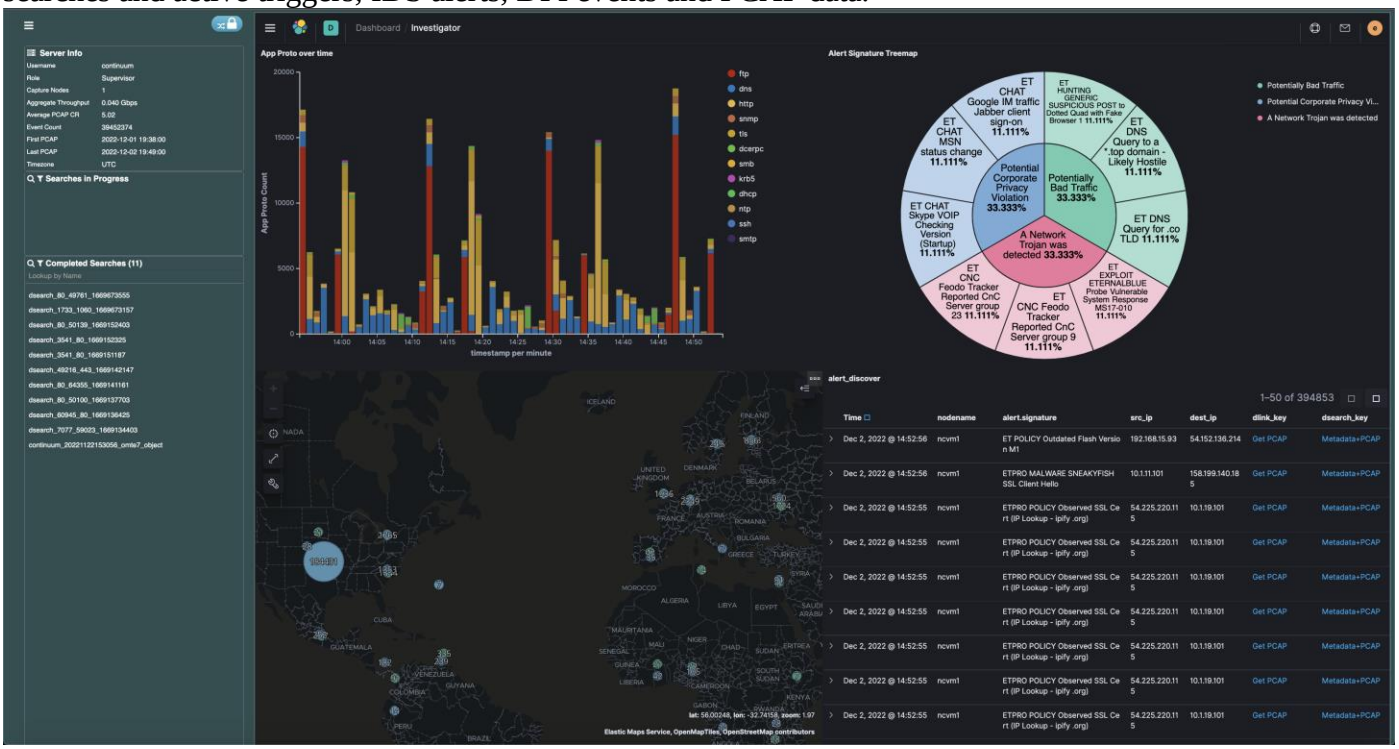
1.4 LOGGING IN TO THE APPLICATION

On any remote system connected to the network, open a supported web browser, and enter the IP address (not FM server's hostname) and port number 41395 over https. For Example: https://<IP Address>:41395
Login username and password will be provided directly to the customer.

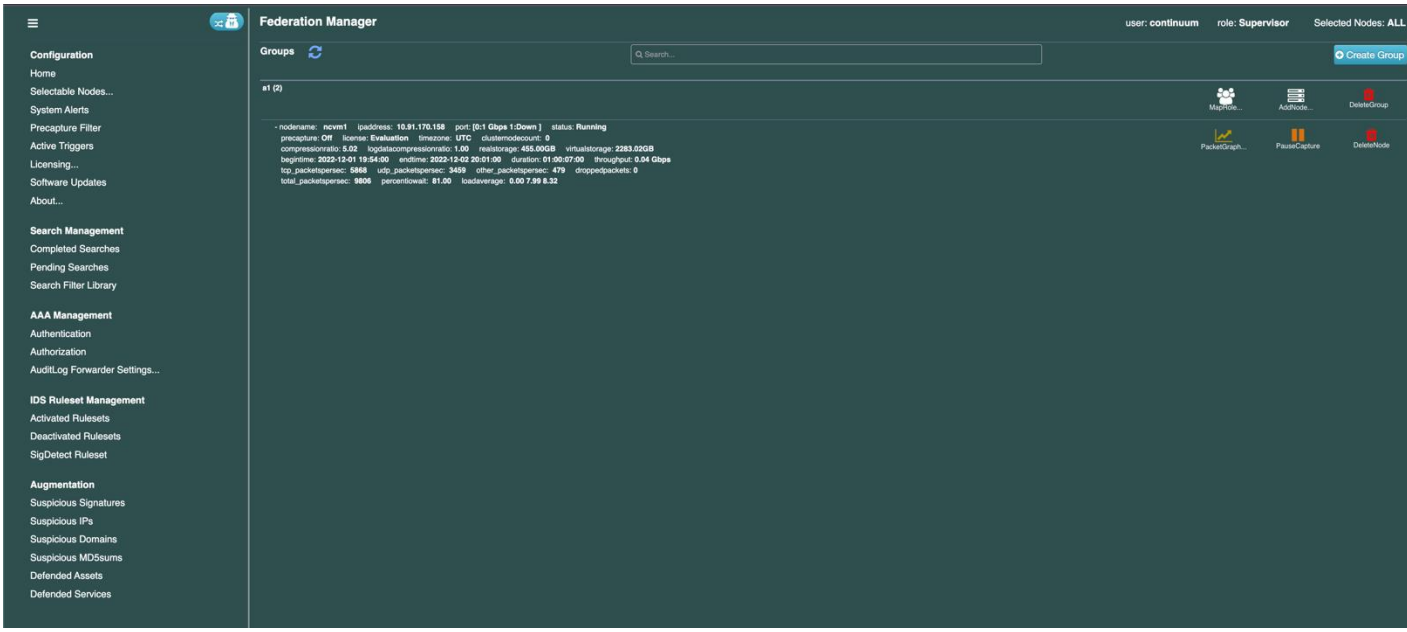
FEDERATION MANAGER UI

Federation Manager UI has two views – Users can switch between these two views by clicking on the button to the right of the company Logo:

1. Investigator View – primarily used by Analysts to view and analyze data via Kibana/Elastic, create searches and active triggers, IDS alerts, DPI events and PCAP data.



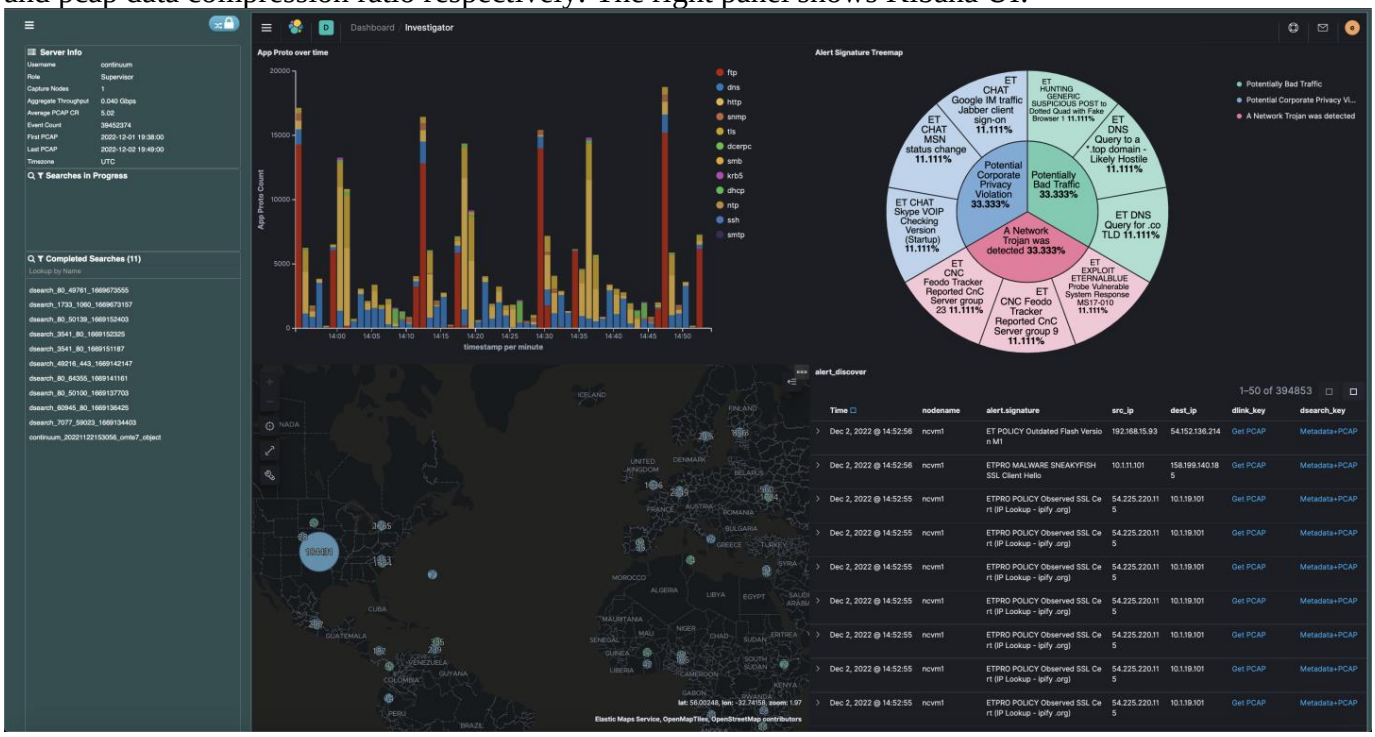
2. Administrator View - primarily used by UI administrators to setup, upload, or generally manage federation nodes.



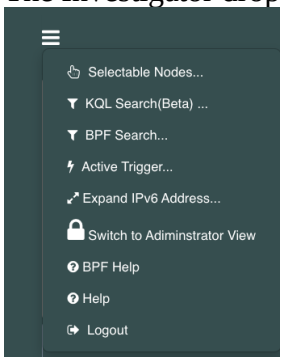
2 INVESTIGATOR VIEW

The capture and analytics platform has multiple ways for users to sync L7 metadata with its L4-L7 metadata, flexibility is at the core of the platform's capabilities. Additionally, the capture platform produces metadata in JSON format for L4 and L7 network flows with Community ID Flow Hashing allowing external monitoring systems to link L7 flow records with metadata more easily. Users are able to pivot with L7 metadata from other systems to FM and execute searches on the system using L4 or L7 metadata attributes on the local unit or via Federation Manager. **rsync** can be leveraged to pull data in from external systems and allow this metadata to be indexed via the capture software and searched against, the original timestamps are maintained during this process. REST API provides the ability to use an external tool's L7 data with timestamps to search against L4 metadata and packet attributes stored on the capture server.

The left panel shows drop-down menu to the left of the logo, and three different sections: Server Info, Searches in Progress, and Completed Searches. LogData CR, PcapData CR show logdata compression ratio and pcap data compression ratio respectively. The right panel shows Kibana UI.

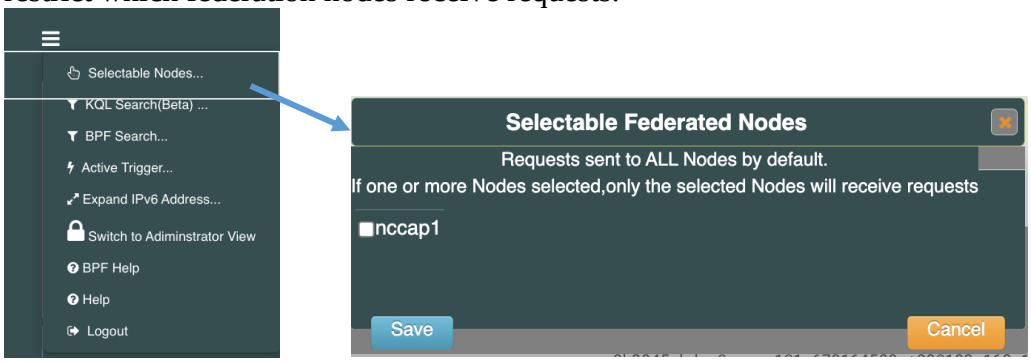


The Investigator drop down menu (☰) to the left the product logo is shown below:



2.1.1 Selectable Nodes

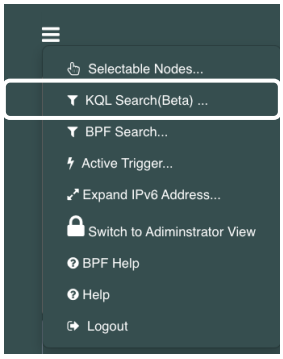
Each FM UI request goes to all connected federation nodes by default. This menu option allows users to restrict which federation nodes receive requests.



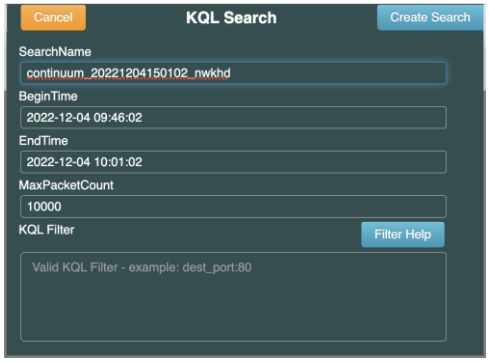
Users with Supervisor role are shown names of all the federated nodes. Other users are shown only the federated nodes from the groups they are allowed to view. The selected node list is effective until a new selection is made.

2.1.2 Custom (KQL) Search

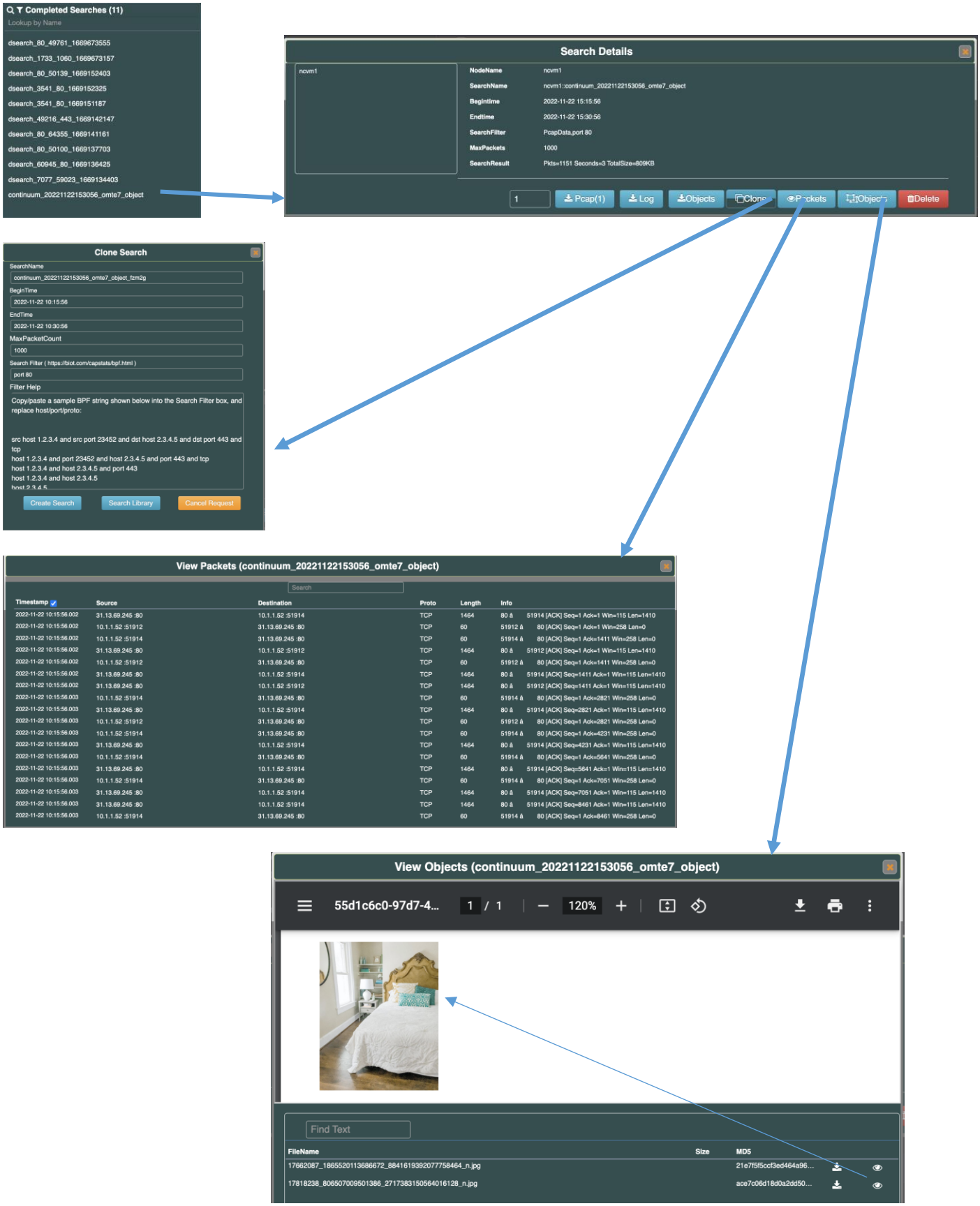
This method allows users to create searches using Kibana Query Language (KQL) Syntax.



This pops up a KQL Search Window. Edit SearchName, BeginTime, EndTime, MaxPacketCount and KQL Filter as needed and hit Create Search button.

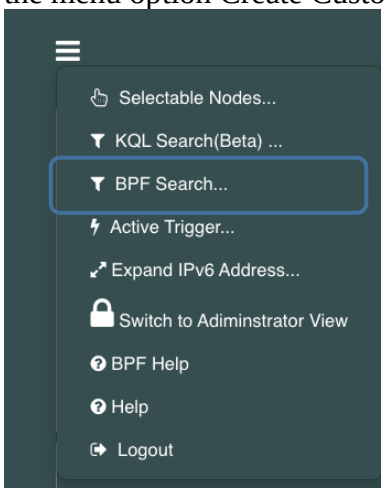


Once the search is completed, an entry for it is displayed in Completed Searches section. Click on a completed search to see a dialog box that allows downloading of the search artifacts.If the Federation has more than one Federation node, there will be one entry for each node that receives the search request.


Completed Searches (11)
Lookup by Name
dsearch_80_49761_1669673555
dsearch_1733_1060_1669673157
dsearch_80_50139_1669152403
dsearch_3541_80_1669152325
dsearch_3541_80_1669151187
dsearch_49216_443_1669142147
dsearch_80_64355_1669141161
dsearch_80_50100_1669137703
dsearch_60945_80_1669136425
dsearch_7077_59023_1669134403
continuum_20221122153056_omte7_object
Search Details
ncvm1
NodeName ncvm1
SearchName ncvm1::continuum_20221122153056_omte7_object
Begintime 2022-11-22 15:15:56
Endtime 2022-11-22 15:30:56
SearchFilter PcapData,port 80
MaxPackets 1000
SearchResult Pkts=1151 Seconds=3 TotalSize=809KB
1
Pcap(1)
Log
Objects
Clone
Packets
Objects
Delete
Clone Search
SearchName
continuum_20221122153056_omte7_object_fzm2g
BeginTime
2022-11-22 10:15:56
EndTime
2022-11-22 10:30:56
MaxPacketCount
1000
Search Filter (https://biot.com/capstats/bpf.html)
port 80
Filter Help
Copy/paste a sample BPF string shown below into the Search Filter box, and replace host/port/proto:
src host 1.2.3.4 and src port 23452 and dst host 2.3.4.5 and dst port 443 and tcp
host 1.2.3.4 and port 23452 and host 2.3.4.5 and port 443 and tcp
host 1.2.3.4 and host 2.3.4.5 and port 443
host 1.2.3.4 and host 2.3.4.5
Create Search
Search Library
Cancel Request
View Packets (continuum_20221122153056_omte7_object)
Search
Timestamp
Source
Destination
Proto
Length
Info
2022-11-22 10:15:56.002 31.13.69.245 :80 10.1.1.52 :51914 TCP 1464 80 â 51914 [ACK] Seq=1 Ack=1 Win=115 Len=1410
2022-11-22 10:15:56.002 10.1.1.52 :51912 31.13.69.245 :80 TCP 60 51912 â 80 [ACK] Seq=1 Ack=1 Win=258 Len=0
2022-11-22 10:15:56.002 10.1.1.52 :51914 31.13.69.245 :80 TCP 60 51914 â 80 [ACK] Seq=1 Ack=1411 Win=258 Len=0
2022-11-22 10:15:56.002 31.13.69.245 :80 10.1.1.52 :51912 TCP 1464 80 â 51912 [ACK] Seq=1 Ack=1 Win=115 Len=1410
2022-11-22 10:15:56.002 10.1.1.52 :51912 31.13.69.245 :80 TCP 60 51912 â 80 [ACK] Seq=1 Ack=1411 Win=258 Len=0
2022-11-22 10:15:56.002 31.13.69.245 :80 10.1.1.52 :51914 TCP 1464 80 â 51914 [ACK] Seq=1411 Ack=1 Win=115 Len=1410
2022-11-22 10:15:56.002 31.13.69.245 :80 10.1.1.52 :51912 TCP 1464 80 â 51912 [ACK] Seq=1411 Ack=1 Win=115 Len=1410
2022-11-22 10:15:56.003 10.1.1.52 :51914 31.13.69.245 :80 TCP 60 51914 â 80 [ACK] Seq=1 Ack=2821 Win=258 Len=0
2022-11-22 10:15:56.003 31.13.69.245 :80 10.1.1.52 :51914 TCP 1464 80 â 51914 [ACK] Seq=2821 Ack=1 Win=115 Len=1410
2022-11-22 10:15:56.003 10.1.1.52 :51912 31.13.69.245 :80 TCP 60 51912 â 80 [ACK] Seq=1 Ack=2821 Win=258 Len=0
2022-11-22 10:15:56.003 10.1.1.52 :51914 31.13.69.245 :80 TCP 60 51914 â 80 [ACK] Seq=1 Ack=4231 Win=258 Len=0
2022-11-22 10:15:56.003 31.13.69.245 :80 10.1.1.52 :51914 TCP 1464 80 â 51914 [ACK] Seq=4231 Ack=1 Win=115 Len=1410
2022-11-22 10:15:56.003 10.1.1.52 :51914 31.13.69.245 :80 TCP 60 51914 â 80 [ACK] Seq=1 Ack=5641 Win=258 Len=0
2022-11-22 10:15:56.003 31.13.69.245 :80 10.1.1.52 :51914 TCP 1464 80 â 51914 [ACK] Seq=5641 Ack=1 Win=115 Len=1410
2022-11-22 10:15:56.003 10.1.1.52 :51914 31.13.69.245 :80 TCP 60 51914 â 80 [ACK] Seq=1 Ack=7051 Win=258 Len=0
2022-11-22 10:15:56.003 31.13.69.245 :80 10.1.1.52 :51914 TCP 1464 80 â 51914 [ACK] Seq=7051 Ack=1 Win=115 Len=1410
2022-11-22 10:15:56.003 31.13.69.245 :80 10.1.1.52 :51914 TCP 1464 80 â 51914 [ACK] Seq=8461 Ack=1 Win=115 Len=1410
2022-11-22 10:15:56.003 10.1.1.52 :51914 31.13.69.245 :80 TCP 60 51914 â 80 [ACK] Seq=1 Ack=8461 Win=258 Len=0
View Objects (continuum_20221122153056_omte7_object)
55d1c6c0-97d7-4...
1 / 1
120%
Find Text
FileName
Size
MD5
17662087_1865520113686672_8841619392077758464_n.jpg
21e7f5f5ccf3ed464a96...
17818238_806507009501386_2717383150564016128_n.jpg
ace7c06d18d0a2dd50...

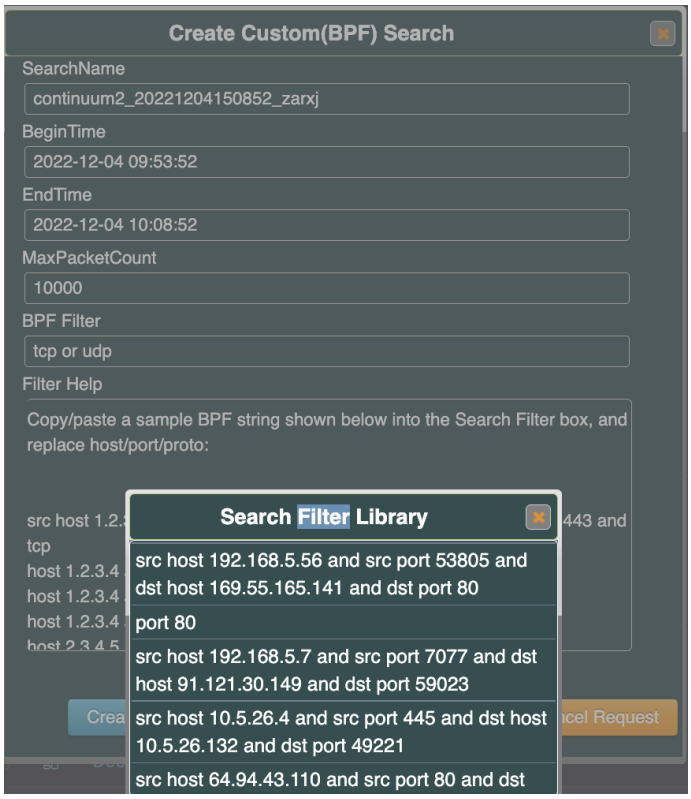
2.1.3 CUSTOM (BPF) Search

Berkeley Packet Filter (BPF) allows searching for pcaps based on various attributes of network traffic. Use the menu option Create Custom (BPF) Search for this purpose.



Dialog box appears:

Search Library collects BPF Filters that were used previously used. Click on the Search Library button to see past search filters (if any). Copy/Paste one of these filters or enter your own.

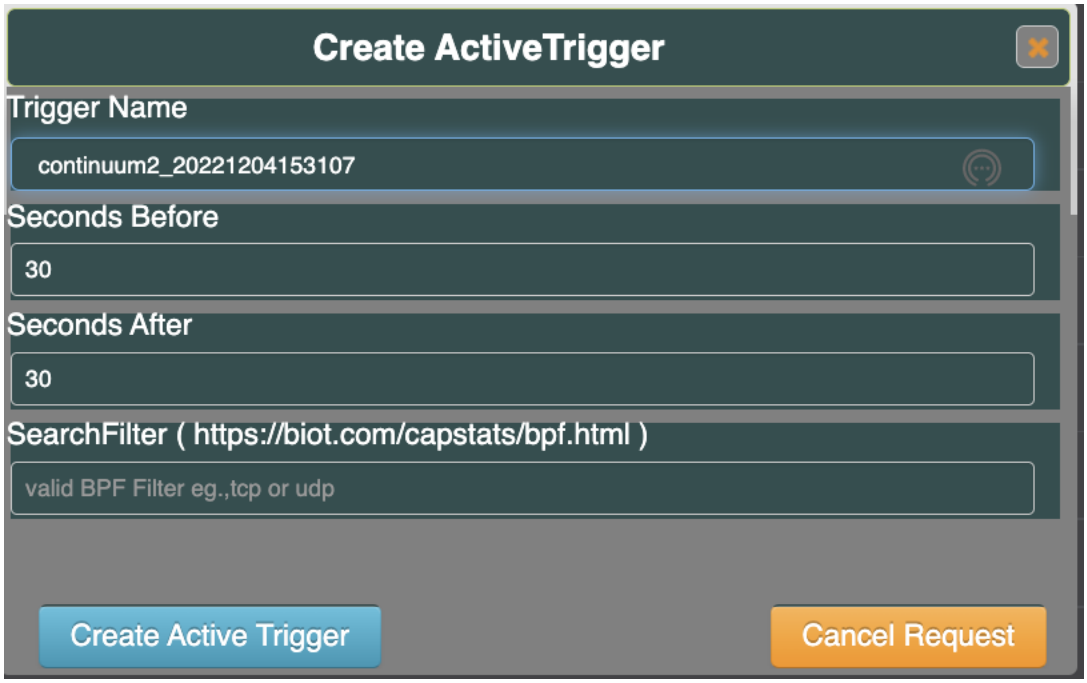


Modify the Search Name, Begin/End time, BPF Search filter and Max Packet Count as needed, and press Create Search button. The new search appears in Searches In Progress panel. Once the search is complete, it appears in Completed Searches panel. Selecting one of the completed searches pops up a dialog box which allows downloading of pcap data, metadata, objects, view packets and clone the search.

2.1.4 Create Active Trigger

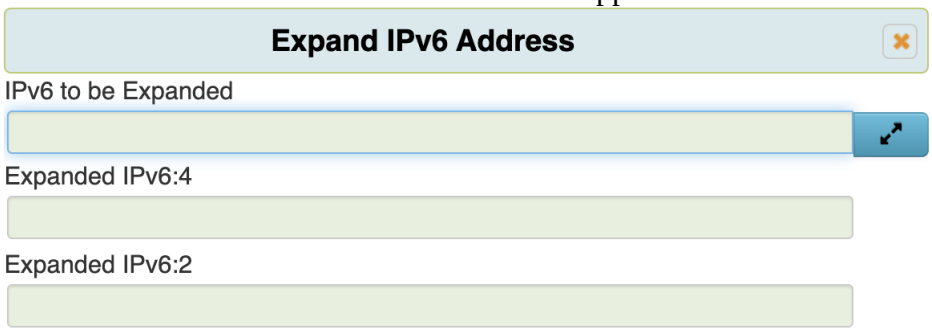
Active triggers allow users to get alerts when specified BPF filter matches payload of a packet. For example, you can specify an IP address as the search filter, and you will see an alert when traffic containing the IP address is captured.

- To generate a trigger, specify the trigger name and time frame (Seconds Before and Seconds After) and a valid BPF filter.
- Seconds Before/After allows users to avoid generating too many alerts. An alert for the same trigger is generated only after this time is passed. Values of 30/30 indicate that minimum time between trigger generation is 1 min.
- The Add button allows the FM user to create a global active trigger (100 per node) for each configured node.

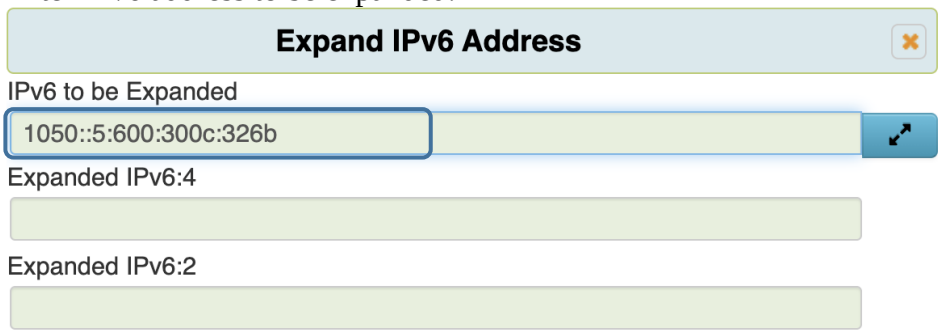


2.1.5 Expand IPv6 Address

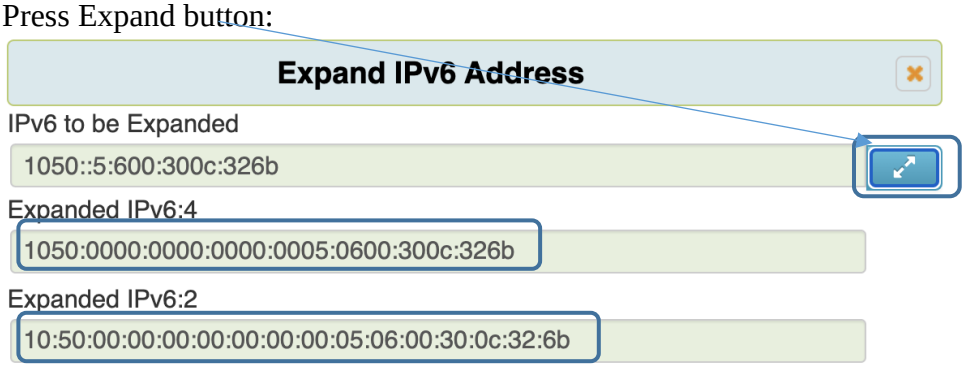
This menu option will pop up a resizable Dialog box that allows users to expand ipv6 addresses. More information about this feature is available in Appendix B.



Enter IPv6 address to be expanded:



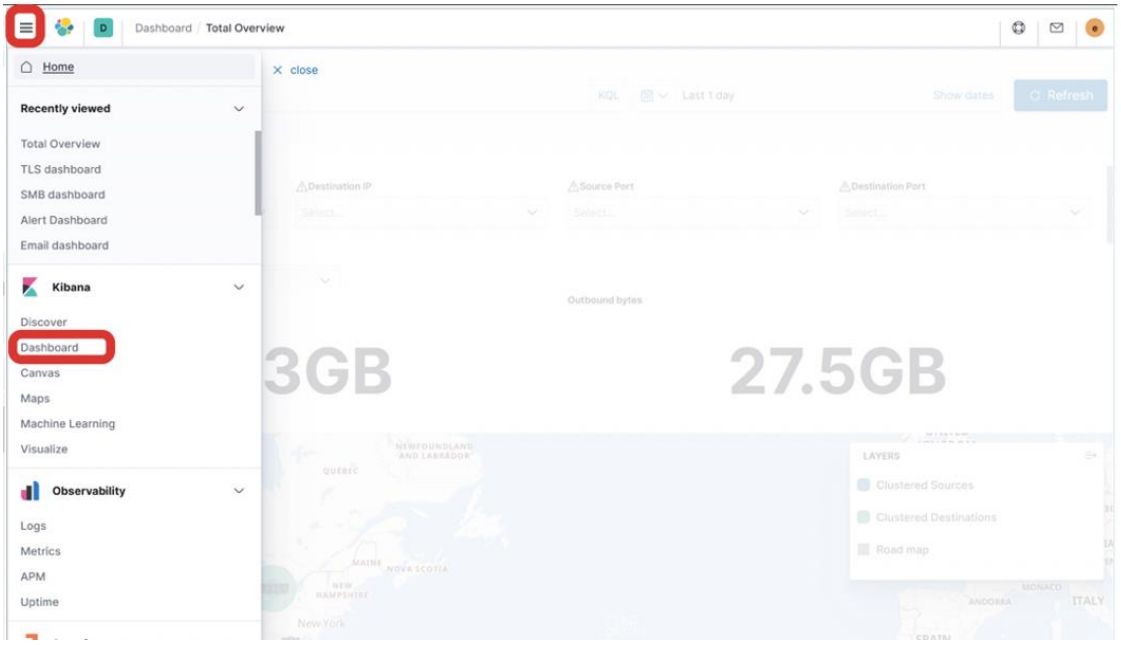
Press Expand button:



2.2 VISUALIZATIONS AND DASHBOARDS

The following are basic functionality operations for using Elastic Kibana within the FM UI. Kibana allows users to easily and quickly visualize, explore, and search metadata logs generated by the server and execute packet searches using the corresponding log files. This is not an all-encompassing guide to using Elastic Kibana but instead covers the most important features for use with the Packet Capture appliance.

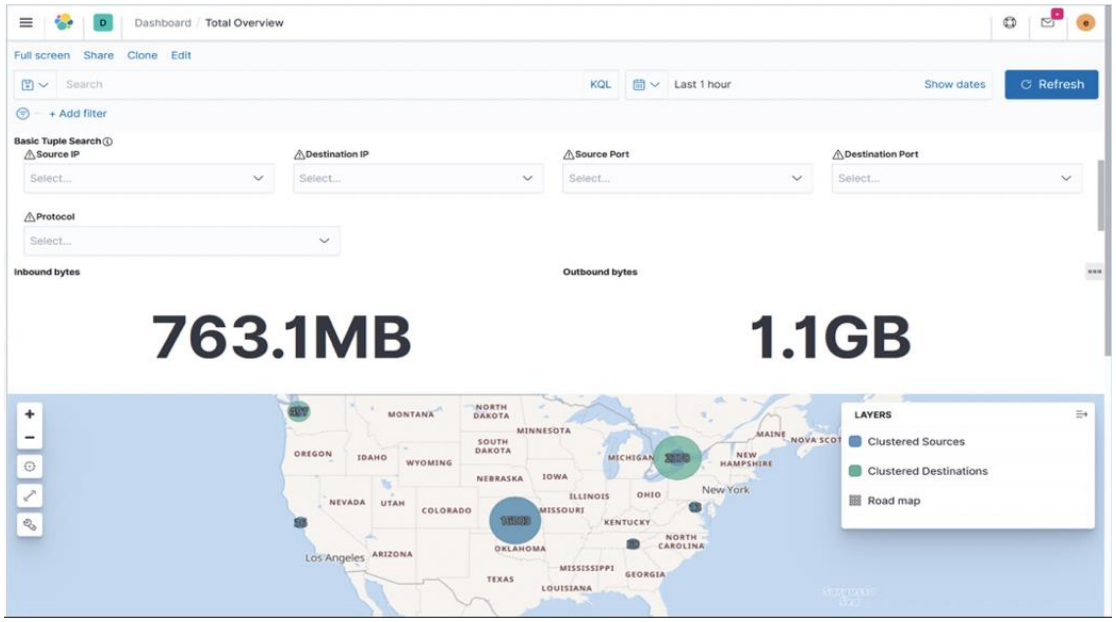
2.2.1 Viewing an existing dashboard

1. To view an existing dashboard object in Kibana, click on the 3 bars at the top left of the screen to open the drop-down menu
2. Click on dashboard
3. 

4. Find the desired dashboard and click on it
    a. This will redirect the user to the appropriate dashboard for exploration, drill-down, and pivot

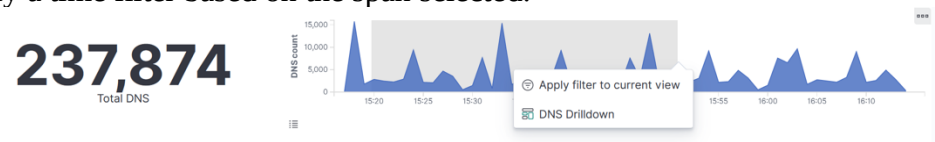
2.2.2 Overview dashboard

When visiting the platform, the “Total Overview” dashboard will be the landing page. On this page, it will show the sources, destinations, and flow rate of traffic over time. Scroll down the page to get a bird’s eye view of the traffic broken down by the most common fields.



2.2.3 Drilldown example

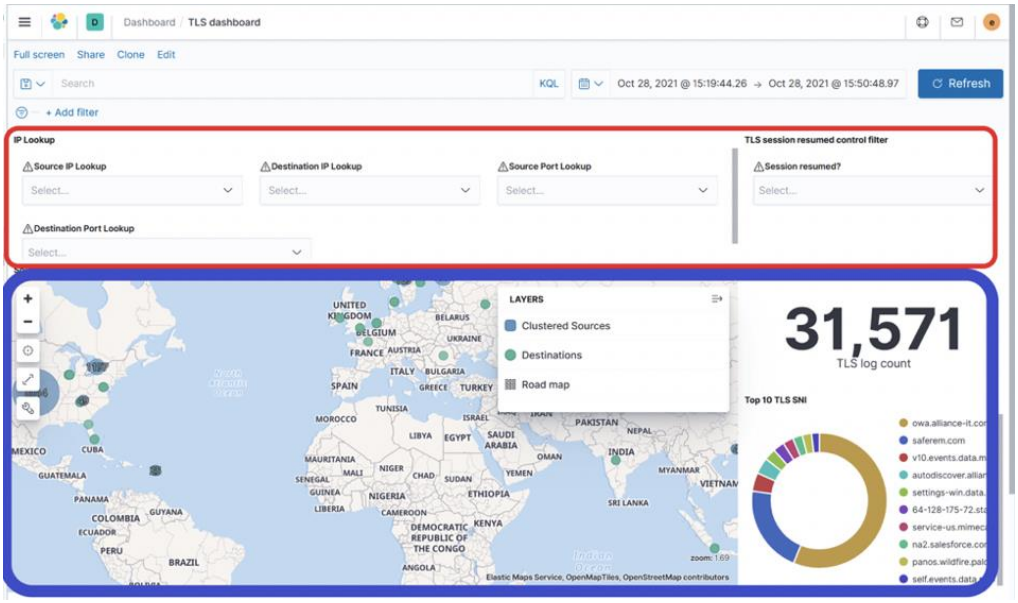
At the bottom of the overview are breakouts of different logs by protocol. By clicking and dragging over sections in the chart, the option to filter by the time span and the option to drill down deeper into the dedicated protocol dashboard will appear. Some protocols have multiple drill down dashboards associated. By clicking the “DNS Drilldown” option in the screenshot below, the system would navigate to the DNS dashboard, and apply a time filter based on the span selected.



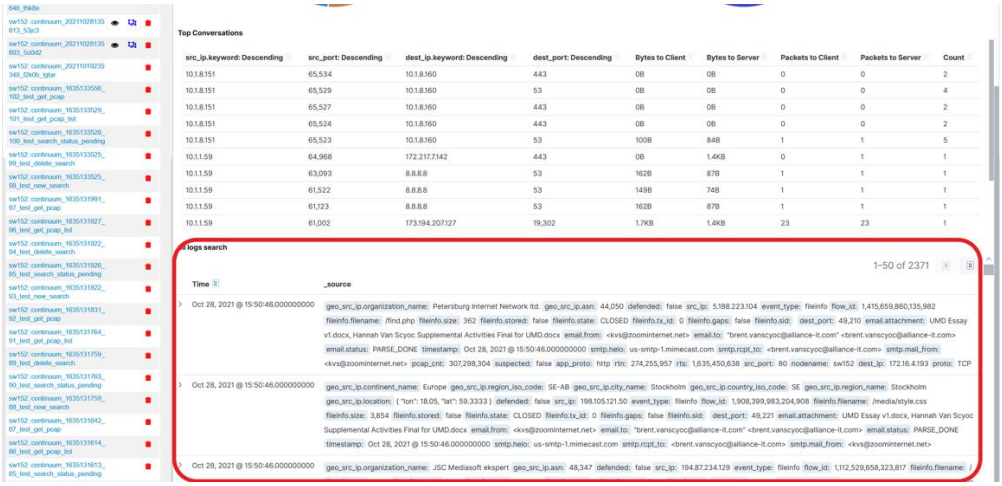
2.2.4 Dashboard structure

Pre-made dashboards follow a structure to ensure a consistent experience across the entire platform.

- Interactive packet filter at the top in case you do not want to type out a filter in the search bar
- Map, timeline, total log count, or other high level information next

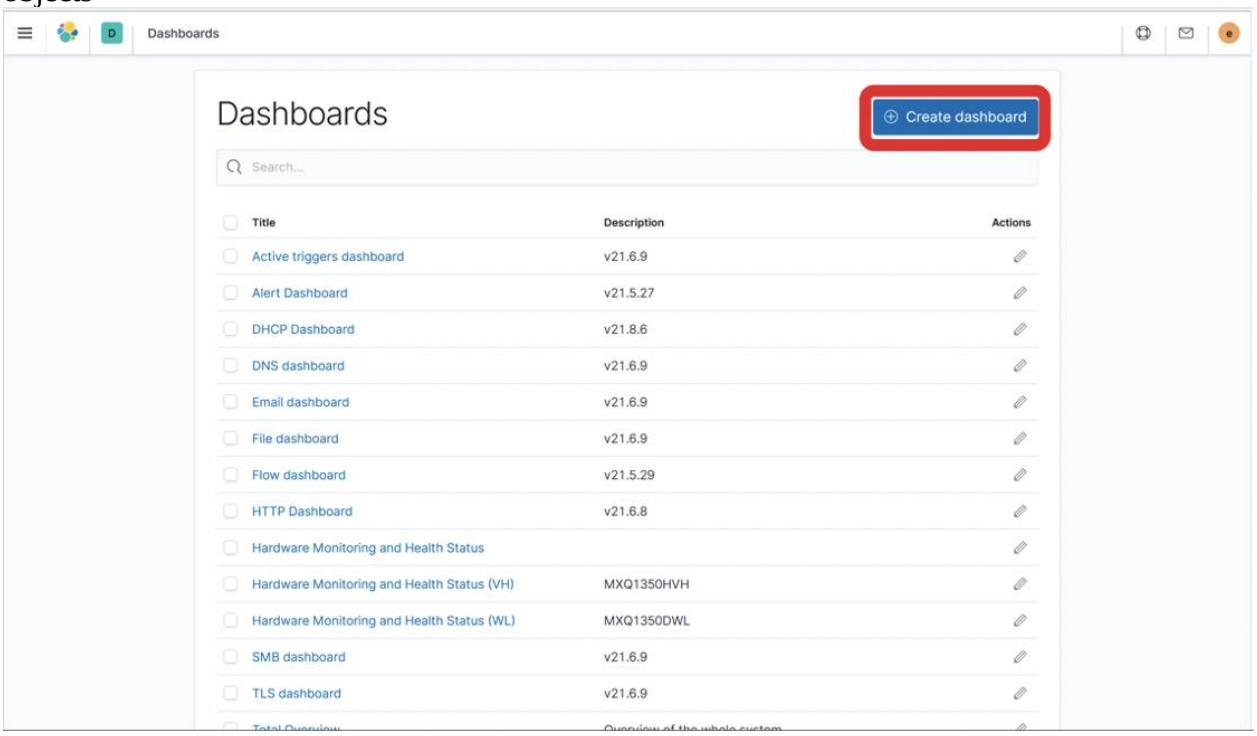


- "All log" viewer at the bottom includes more than the filtered protocols that the dashboard is named after so you can see associated traffic



2.2.5 Creating a new dashboard

1. Click on the 3 bars at the top left of the screen to open the drop-down menu
2. Click on “dashboard”
3. Click on the Create dashboard button
4. By default, the new dashboard will be blank and can be filled with existing or new visualization objects

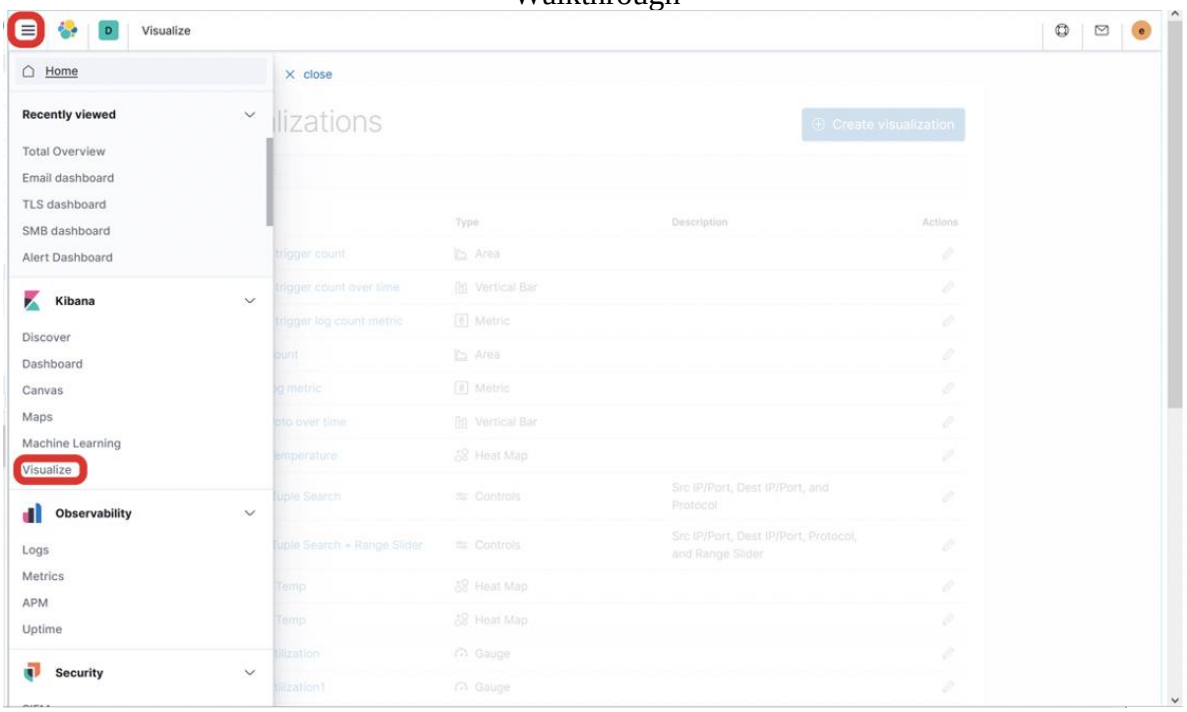


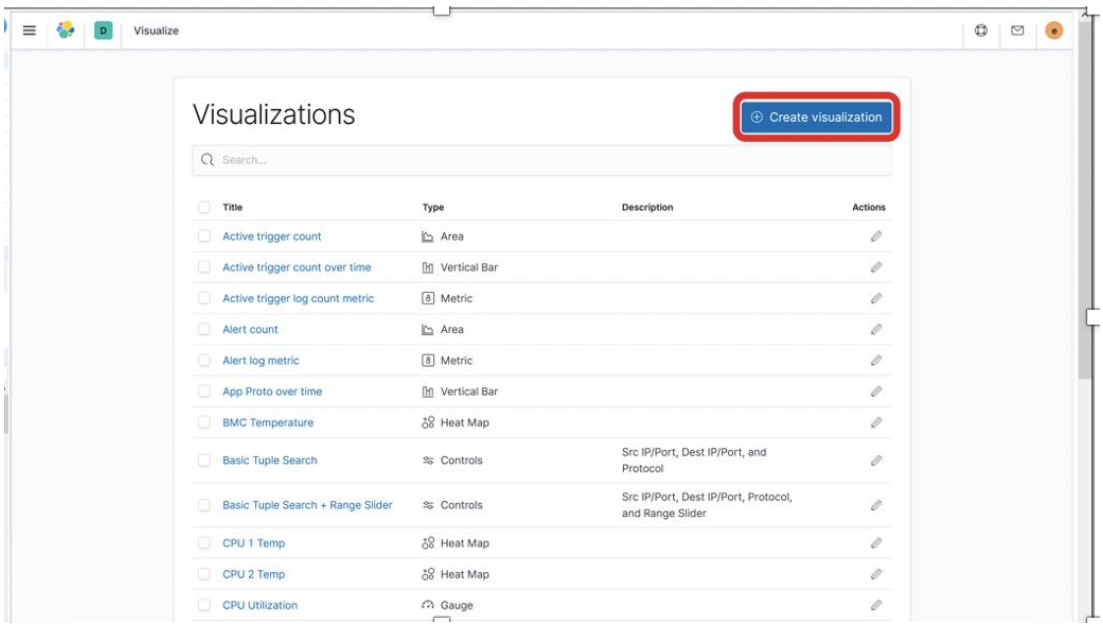
2.2.6 Creating a new visualization

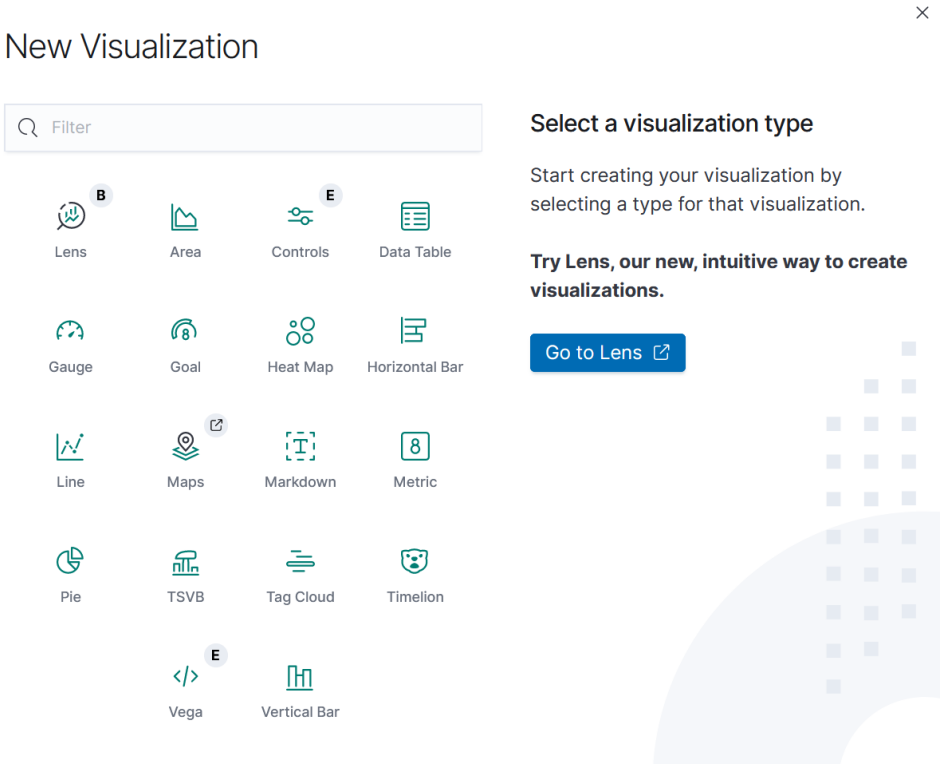
Visualization objects serve as the widgets that make up the various dashboard objects.

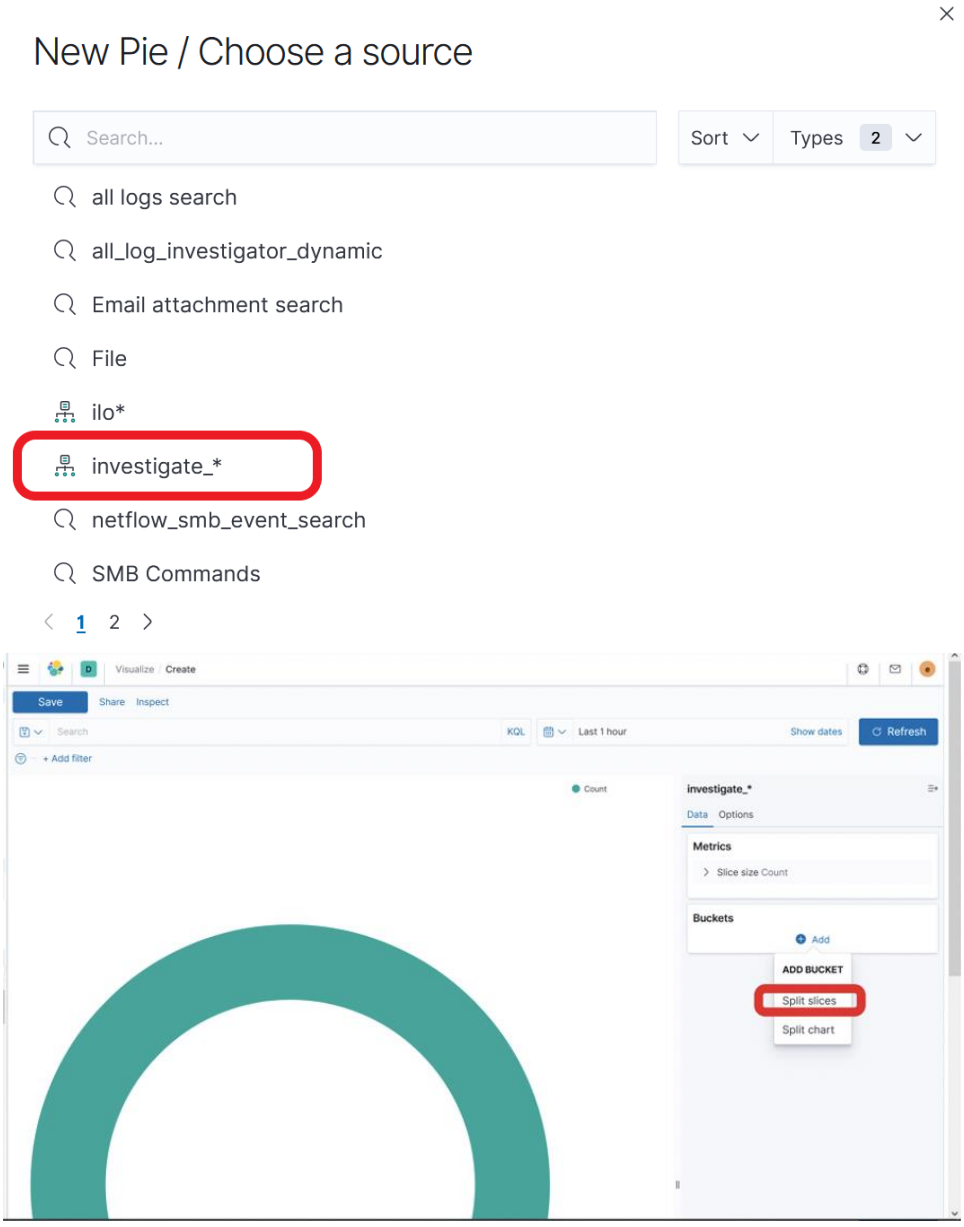
1. Click on the 3 bars at the top left of the screen to open the drop-down menu
2. Click on Visualize
3. Click on the Create visualization button
4. On the pop-up menu, select the desired style of visualization. This tutorial will use “Pie”.
5. Choose a saved index to use as the data set for the visualization
    a. The index will be “investigate-*” for almost all visualizations
6. Fine tune the visualization to display the desired information
7. Scroll to the bottom and press “update”
8. Scroll back up and click the Save button
9. Name your visualization and save it. This visualization will be available to be added to any dashboards

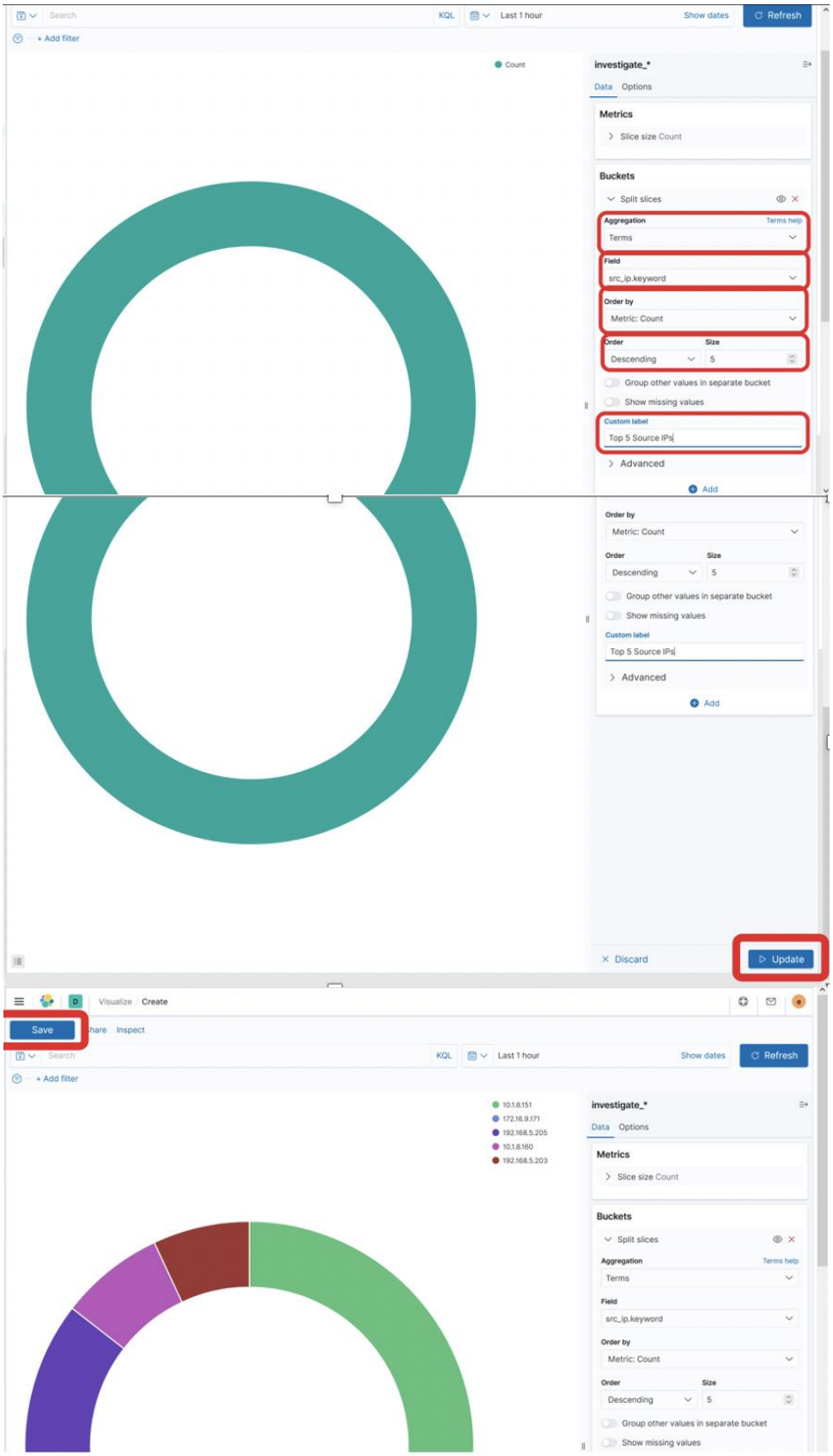
Walkthrough

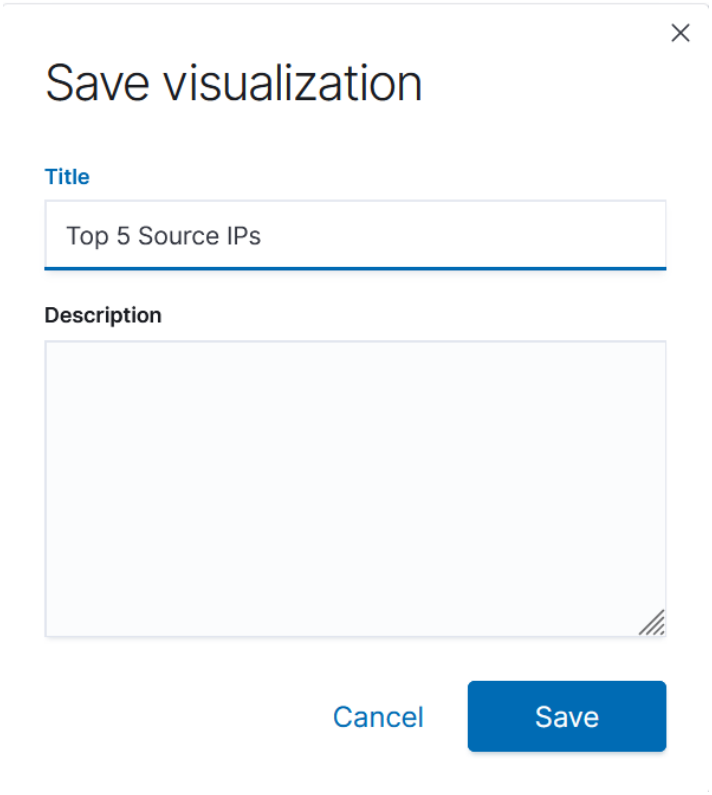



Visualize
Visualizations
Create visualization
Search...
Title
Type
Description
Actions
Active trigger count
Area
Active trigger count over time
Vertical Bar
Active trigger log count metric
Metric
Alert count
Area
Alert log metric
Metric
App Proto over time
Vertical Bar
BMC Temperature
Heat Map
Basic Tuple Search
Controls
Src IP/Port, Dest IP/Port, and Protocol
Basic Tuple Search + Range Slider
Controls
Src IP/Port, Dest IP/Port, Protocol, and Range Slider
CPU 1 Temp
Heat Map
CPU 2 Temp
Heat Map
CPU Utilization
Gauge


New Visualization
Filter
Lens
Area
Controls
Data Table
Gauge
Goal
Heat Map
Horizontal Bar
Line
Maps
Markdown
Metric
Pie
TSVB
Tag Cloud
Timelion
Vega
Vertical Bar
Select a visualization type
Start creating your visualization by selecting a type for that visualization.
Try Lens, our new, intuitive way to create visualizations.
Go to Lens


New Pie / Choose a source
Search...
Sort
Types 2
all logs search
all_log_investigator_dynamic
Email attachment search
File
ilo*
investigate_*
netflow_smb_event_search
SMB Commands
1 2
Visualize Create
Save Share Inspect
Search KQL Last 1 hour Show dates Refresh
+ Add filter
Count
investigate_*
Data Options
Metrics
Slice size Count
Buckets
Add
ADD BUCKET
Split slices
Split chart

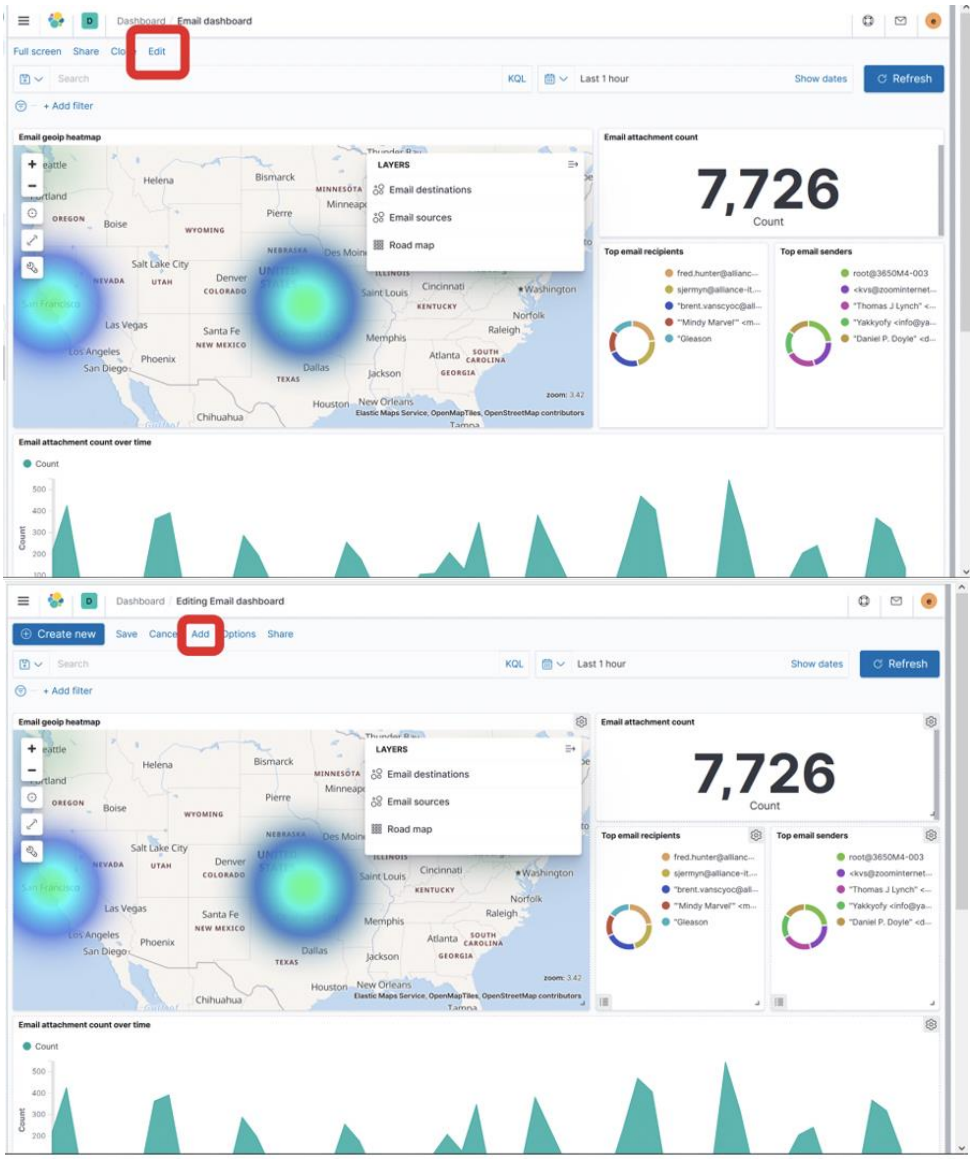

Search
KQL
Last 1 hour
Show dates
Refresh
+ Add filter
Count
investigate_*
Data
Options
Metrics
Slice size Count
Buckets
Split slices
Aggregation
Terms help
Terms
Field
src_ip.keyword
Order by
Metric: Count
Order
Size
Descending
5
Group other values in separate bucket
Show missing values
Custom label
Top 5 Source IPs
Advanced
Add
Discard
Update
Visualize / Create
Save
Share
Inspect
10.1.8.151
172.16.9.171
192.168.5.205
10.1.8.160
192.168.5.203

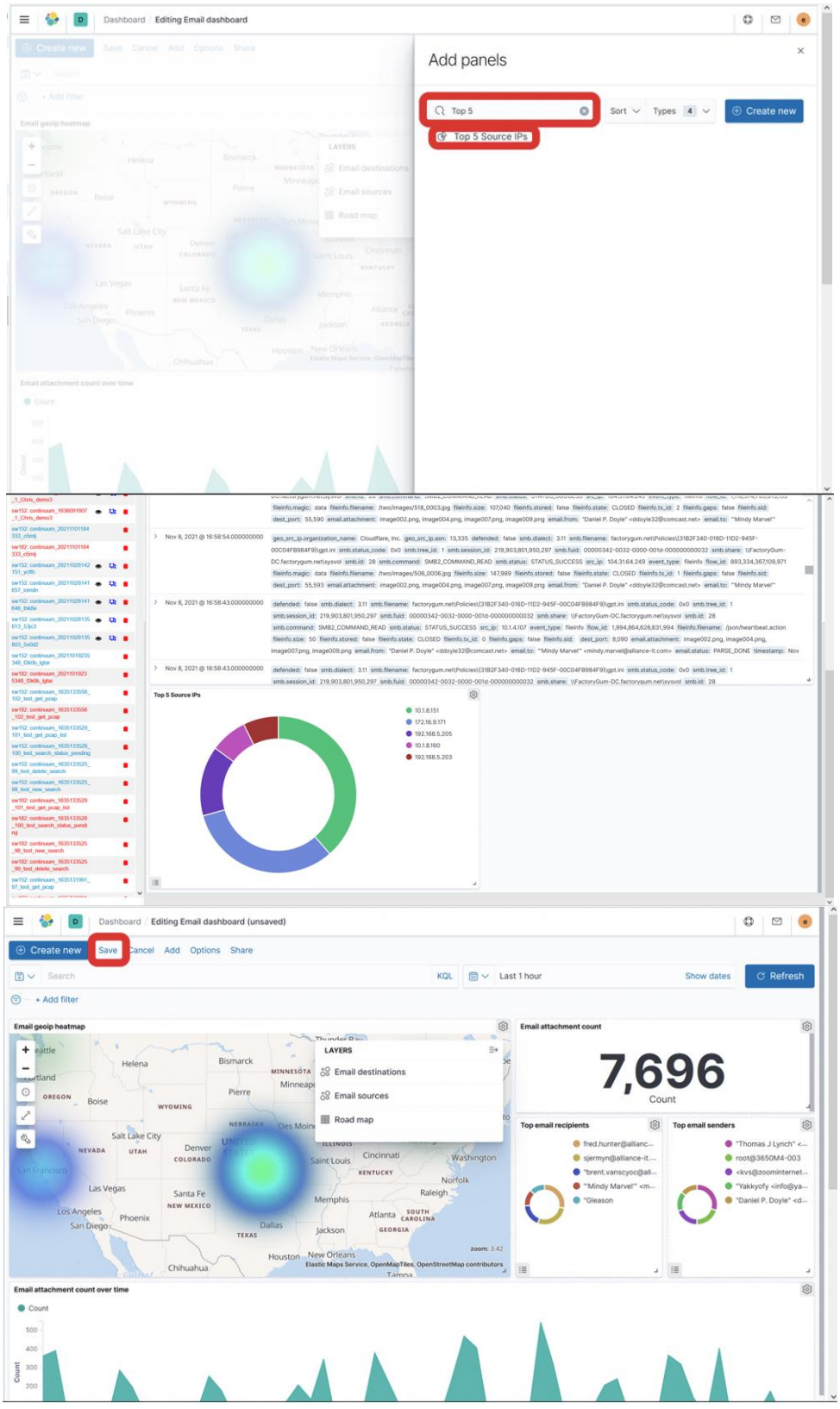

Save visualization
Title
Top 5 Source IPs
Description
Cancel
Save

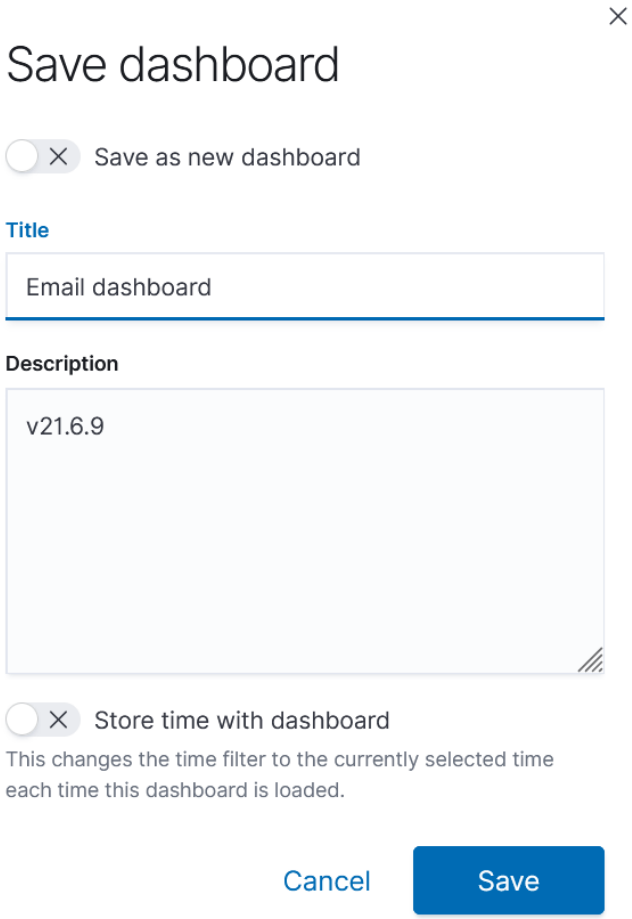
2.2.7 Adding a visualization to a dashboard

To add an existing visualization to a dashboard, click on the 3 bars at the top left of the screen to open the drop-down menu.

1. Visit any dashboard
2. Click “Edit”
3. Click the “Add” to add an existing visualization
    a. You can also select “Create new” to make a new visualization and automatically have it added to this dashboard.
4. Find the desired visualization by name and click on it to add it to the dashboard
5. Once the visualization is added, it will appear at the bottom of the entire dashboard. It can be freely moved and resized within the dashboard.
6. Click the Save button at the top of the page to save as an existing or new dashboard
7. “Save as new dashboard” will save as a copy
8. “Store time with dashboard” ensures that every time you visit it, the time selection is consistent
9. Click the Save button

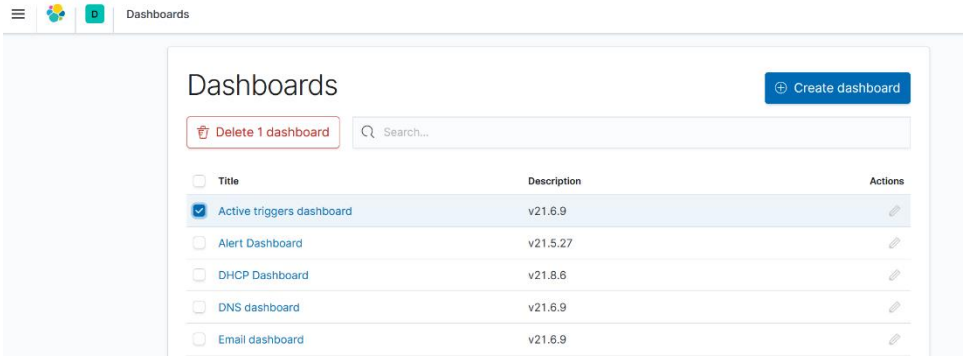



Dashboard / Editing Email dashboard
Add panels
Top 5
Sort
Types
Create new
Top 5 Source IPs
Top 5 Source IPs
Dashboard / Editing Email dashboard (unsaved)
Create new
Save
Cancel
Add
Options
Share
Search
KQL
Last 1 hour
Show dates
Refresh
+ Add filter
Email geoip heatmap
LAYERS
Email destinations
Email sources
Road map
Email attachment count
7,696
Count
Top email recipients
Top email senders
Email attachment count over time
Count



2.2.8 Deleting a dashboard or visualization

1. Navigate to “Dashboards” or “Visualizations” section.
2. Add check marks to the items you wish to delete
3. Click the red “Delete N dashboard(s)” button

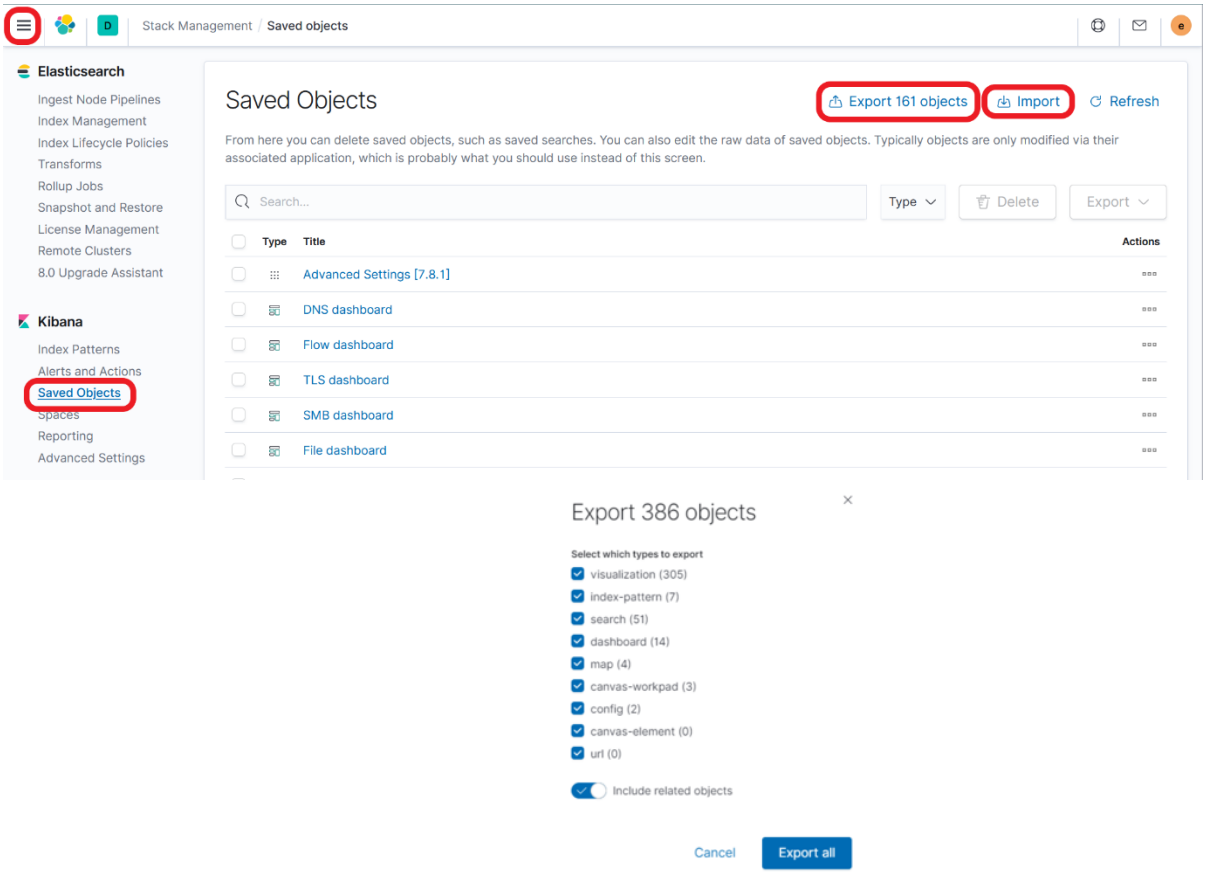


2.2.9 Backup and restore custom dashboards

1. To import existing visualization and dashboard objects, click on the 3 bars at the top left of the screen to open the drop-down menu
2. Click on Stack Management (found at the bottom of the drop-down menu)
3. Click on the Saved Objects button within the Kibana category of options
4. Backing up objects

a. Select the checkboxes by items you wish to backup. Then click “Export N Objects” at the top of the page. Clicking the export button without selecting any will export everything.
b. Ensure that you select “include related objects”
c. Dashboard and visualization objects are saved in .ndjson format

5. Restoring a backup
   a. Click the import button
   b. Choose the file to import
   c. Once the files are imported, any new dashboards and visualizations will automatically populate the lists of dashboards and visualizations and will be viewable and editable



2.2.10 Discover

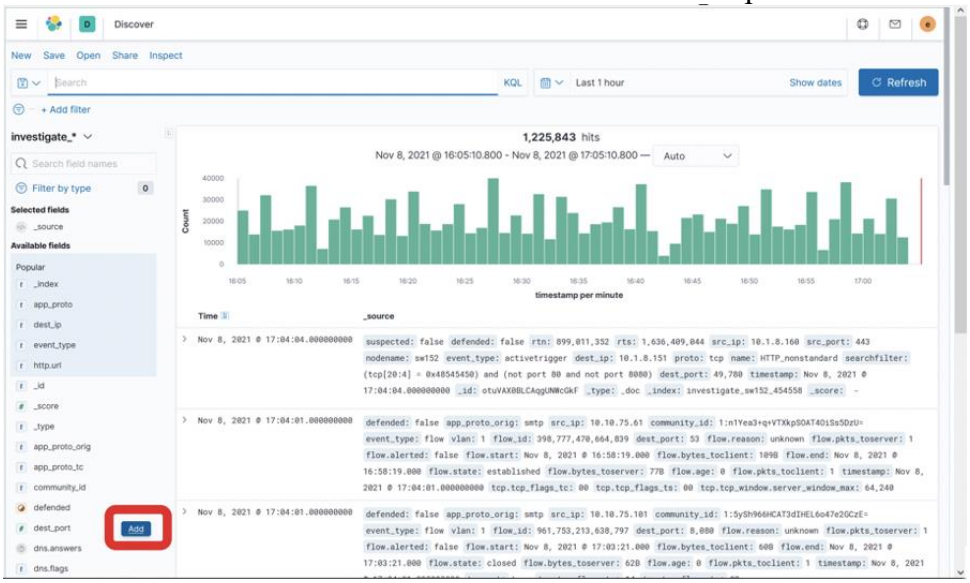
The Discover panel allows for full exploration, search, and drill-down of all metadata logs within Elastic.

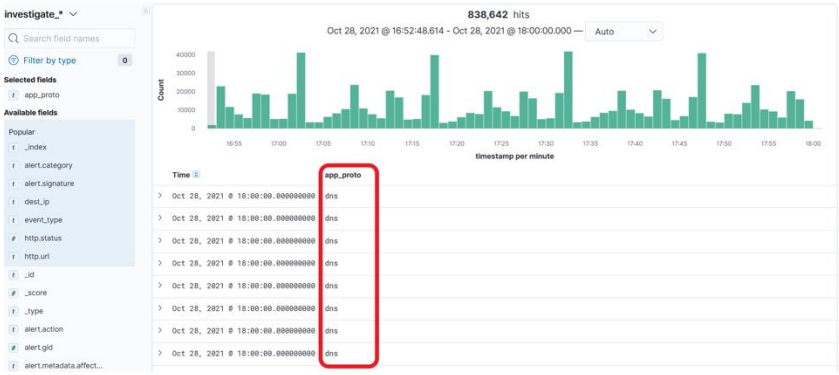
1. Click on the 3 bars at the top left of the screen to open the drop-down menu.
2. Click on Discover
3. From here, custom KQL searches and filters as well as custom time ranges can be applied to navigate through the metadata and find the desired logs
4. These logs can then be used to execute a packet search directly within the FM UI or to confirm events or alerts seen on other appliances

2.2.11 Pin a field to a column

To make a field appear as a column in searches, add the field from the panel on the left.

Hover over the desired field and click “Add” to add a column in the results panel focused on that field.





2.2.12 Searches

Kibana uses KQL, which is further defined in the documentation, but below are the basics.

Accessing fields

Fields are accessed by name, where sub-fields are appended with a period after the parent, and before the child.

Example:

ttp.status

A full list of available fields is shown on the left of the results. This shows the full name of the field, and an icon displaying the type of field it is.

Checking for existence

Wildcards can be placed anywhere in the search bar e.g. wild cards in fields or values.

A colon denotes that you are referencing the value of a specific field.

Example query to return results that contain an http status code:

http.status : *

Negating a clause

If you want to exclude specific results, prepend “not” before the term to exclude.

Example query to show all destination ports that are not port 80:

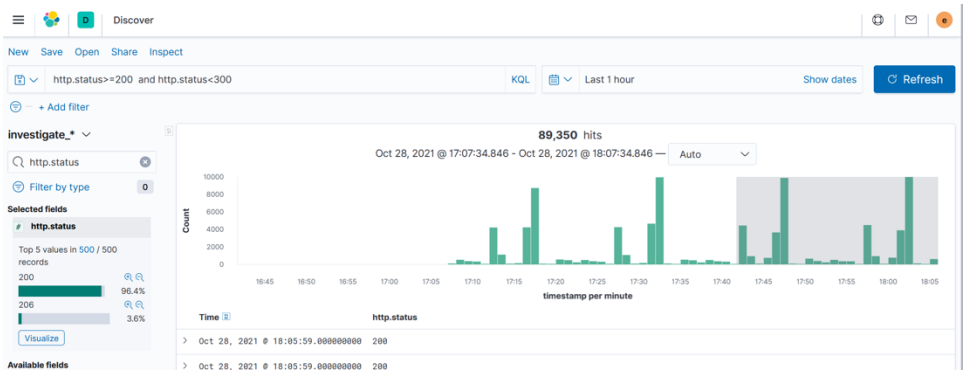
not dest_port : 80

Numerical values

Comparisons can be made to immediate values on the fly.

Example query that returns results where a http status is between 200 and 299 inclusive:

http.status>=200 and http.status<300



Boolean queries

"and" and "or" can join search terms. This can create much more complex searches than would otherwise be possible.

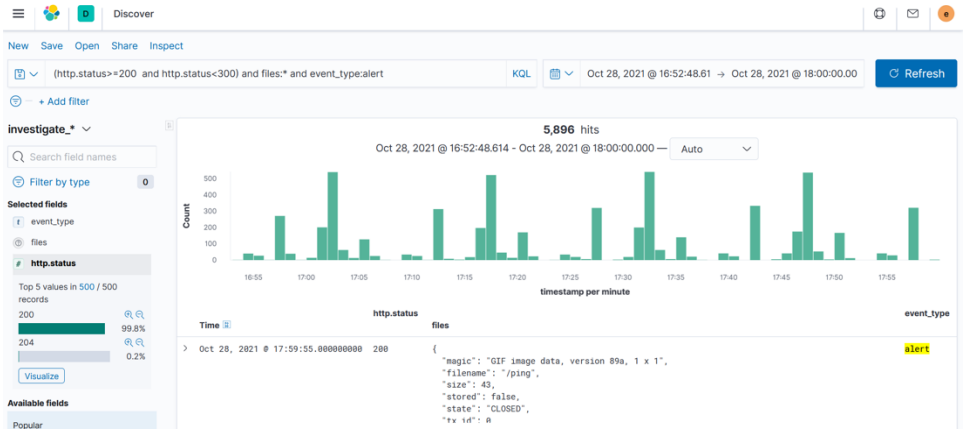
Example query to return all DNS logs for a specific source:

src_ip:192.168.5.205 and event_type:dns

Combining these techniques

By combining these techniques, we can create queries to show results like the following:

(http.status>=200 and http.status<300) and files:* and not dest_port:(80 or 443)

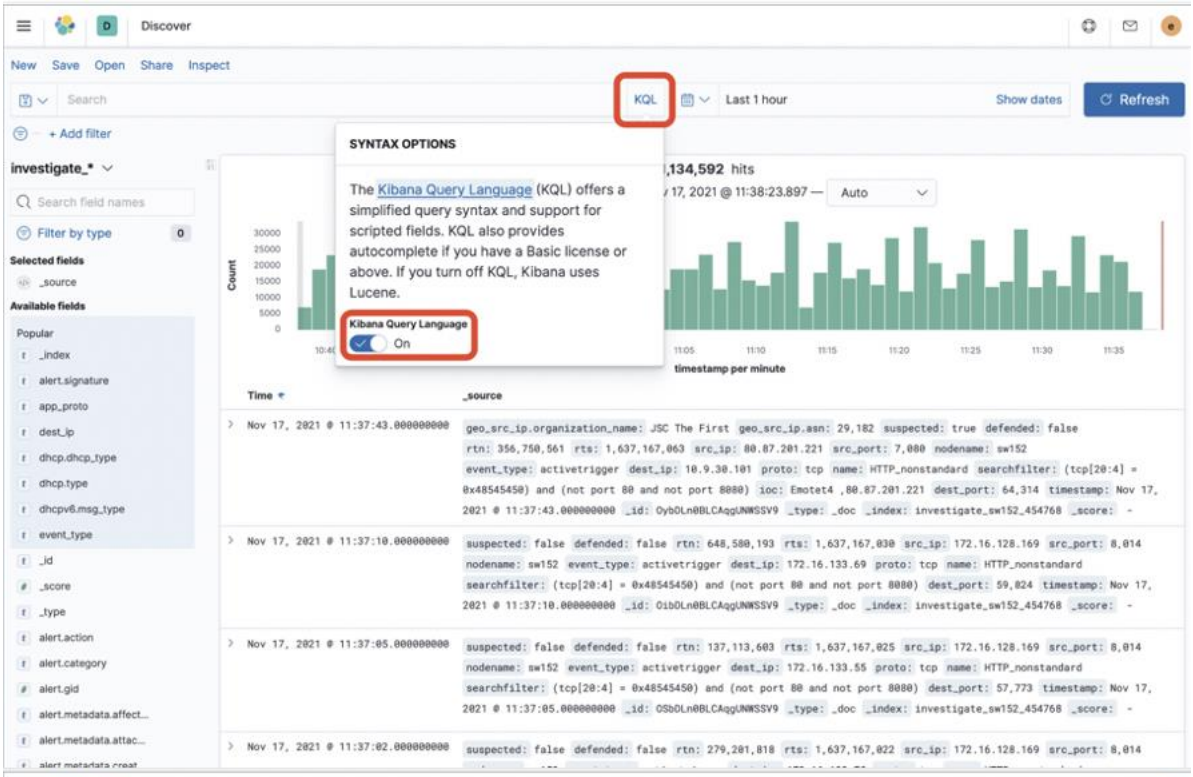


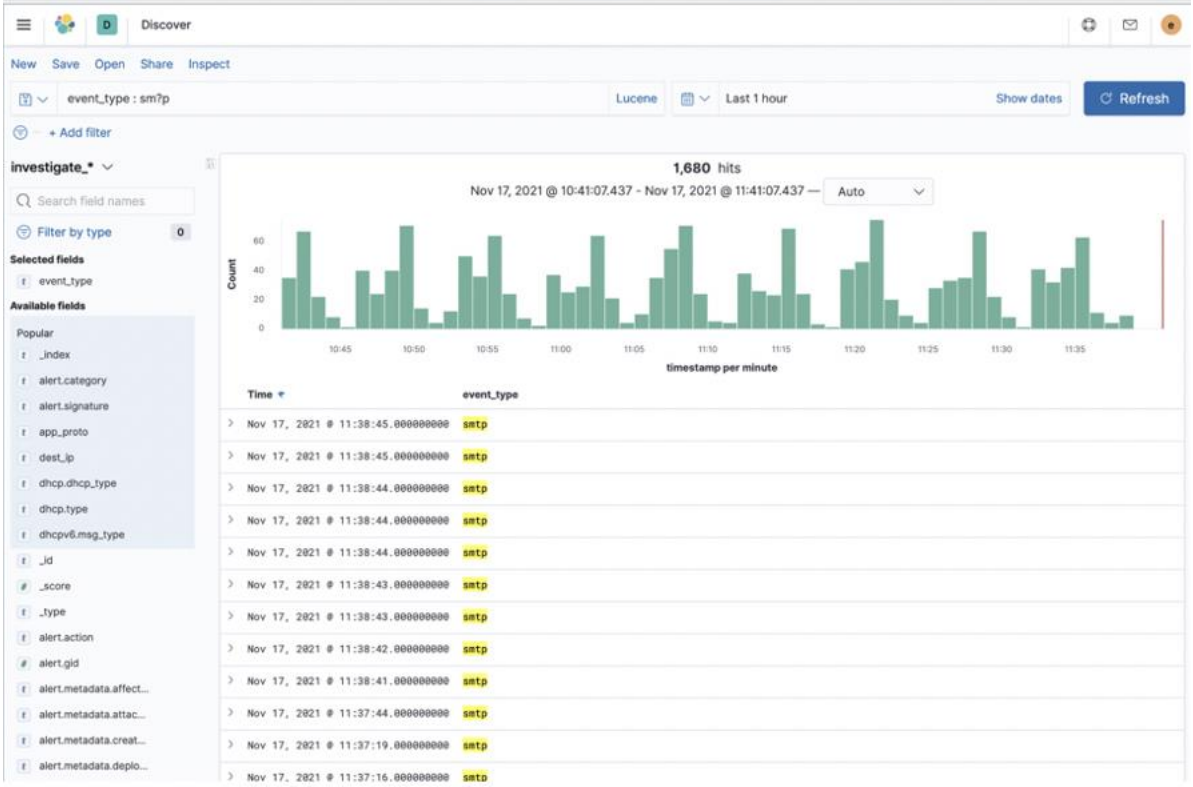
This query displays results that do not use destination port 80 or 443 but contain successful http status codes where at least one file was seen.

Single character wildcard

Single character wildcard works when there are no spaces in the value, as spaces would separate the terms in the search, and enclosing the value in quotes will not parse the "?" as a wildcard character.

1. Turn off Kibana Query Language to switch to Lucene query syntax.
2. Use a "?" character to denote the wildcard character in your search


Discover
New Save Open Share Inspect
Search
KQL
Last 1 hour
Show dates
Refresh
+ Add filter
SYNTAX OPTIONS
The Kibana Query Language (KQL) offers a simplified query syntax and support for scripted fields. KQL also provides autocomplete if you have a Basic license or above. If you turn off KQL, Kibana uses Lucene.
Kibana Query Language
On
investigate_*
Search field names
Filter by type
Selected fields
_source
Available fields
Popular
_index
alert.signature
app_proto
dest_ip
dhcp.dhcp_type
dhcp.type
dhcpv6.msg_type
event_type
_id
_score
_type
alert.action
alert.category
alert.gid
alert.metadata.affect...
alert.metadata.attac...
,134,592 hits
17, 2021 @ 11:38:23.897 —
Auto
Count
timestamp per minute
Time
_source
Nov 17, 2021 @ 11:37:43.000000000
geo_src_ip.organization_name: JSC The First geo_src_ip.asn: 29,182 suspected: true defended: false rtn: 356,750,561 rts: 1,637,167,063 src_ip: 80.87.201.221 src_port: 7,080 nodename: sw152 event_type: activetrigger dest_ip: 10.9.30.101 proto: tcp name: HTTP_nonstandard searchfilter: (tcp[20:4] = 0x48545450) and (not port 80 and not port 8080) ioc: Emotet4 ,80.87.201.221 dest_port: 64,314 timestamp: Nov 17, 2021 @ 11:37:43.000000000 _id: OybOLn0BLCAqgUNWSSV9 _type: _doc _index: investigate_sw152_454768 _score: -
Nov 17, 2021 @ 11:37:10.000000000
suspected: false defended: false rtn: 648,580,193 rts: 1,637,167,030 src_ip: 172.16.128.169 src_port: 8,014 nodename: sw152 event_type: activetrigger dest_ip: 172.16.133.69 proto: tcp name: HTTP_nonstandard searchfilter: (tcp[20:4] = 0x48545450) and (not port 80 and not port 8080) dest_port: 59,824 timestamp: Nov 17, 2021 @ 11:37:10.000000000 _id: OibOLn0BLCAqgUNWSSV9 _type: _doc _index: investigate_sw152_454768 _score: -
Nov 17, 2021 @ 11:37:05.000000000
suspected: false defended: false rtn: 137,113,603 rts: 1,637,167,025 src_ip: 172.16.128.169 src_port: 8,014 nodename: sw152 event_type: activetrigger dest_ip: 172.16.133.55 proto: tcp name: HTTP_nonstandard searchfilter: (tcp[20:4] = 0x48545450) and (not port 80 and not port 8080) dest_port: 57,773 timestamp: Nov 17, 2021 @ 11:37:05.000000000 _id: OSbOLn0BLCAqgUNWSSV9 _type: _doc _index: investigate_sw152_454768 _score: -
Nov 17, 2021 @ 11:37:02.000000000
suspected: false defended: false rtn: 279,281,818 rts: 1,637,167,022 src_ip: 172.16.128.169 src_port: 8,014


Discover
New Save Open Share Inspect
event_type : sm?p
Lucene
Last 1 hour
Show dates
Refresh
+ Add filter
investigate_*
Search field names
Filter by type
Selected fields
event_type
Available fields
Popular
_index
alert.category
alert.signature
app_proto
dest_ip
dhcp.dhcp_type
dhcp.type
dhcpv6.msg_type
_id
_score
_type
alert.action
alert.gid
alert.metadata.affect...
alert.metadata.attac...
alert.metadata.creat...
alert.metadata.deplo...
1,680 hits
Nov 17, 2021 @ 10:41:07.437 - Nov 17, 2021 @ 11:41:07.437 —
Auto
Count
timestamp per minute
Time
event_type
Nov 17, 2021 @ 11:38:45.000000000 smtp
Nov 17, 2021 @ 11:38:45.000000000 smtp
Nov 17, 2021 @ 11:38:44.000000000 smtp
Nov 17, 2021 @ 11:38:44.000000000 smtp
Nov 17, 2021 @ 11:38:44.000000000 smtp
Nov 17, 2021 @ 11:38:43.000000000 smtp
Nov 17, 2021 @ 11:38:43.000000000 smtp
Nov 17, 2021 @ 11:38:42.000000000 smtp
Nov 17, 2021 @ 11:38:41.000000000 smtp
Nov 17, 2021 @ 11:37:44.000000000 smtp
Nov 17, 2021 @ 11:37:19.000000000 smtp
Nov 17, 2021 @ 11:37:16.000000000 smtp

3 ADMINISTRATOR VIEW

This group of menu options allow authorized users to configure federation groups/nodes, set precapture filter and manage active triggers.

3.1 CONFIGURATION

3.1.1 Home

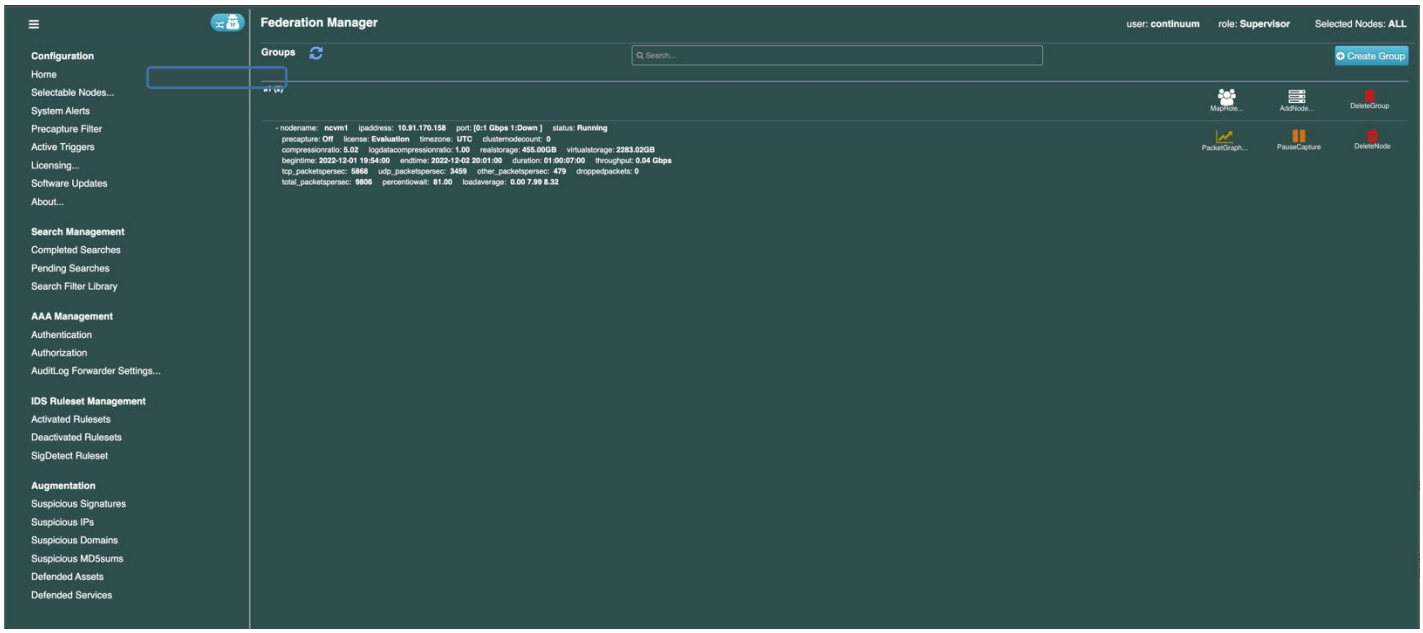
The Home button shows the Groups and Nodes of the Federation Manager. Top of the Admin UI page shows the currently logged in user's name, user's role, authentication mode and product version. The following sections describe each of the options available on the left panel and the actions/views based on the selected option.

The following actions are available on this page. Each of these actions on this page are permitted only to the users with *Groups* permission.

- Groups:
  - Create Group – Authorized users can create groups using **Create Group** button. A group can consist of zero or more nodes. Each group has an Add Node and a Delete Group button.
  - Add Node – Add one or more Federation Nodes to a group using button. Enter IP address of the node.
  - Delete Group – A group can only be deleted when it is empty. Delete all nodes from a group before deleting a group.
  - Map User – This allows which users are allowed to view/manage the nodes of the group.
- Nodes:
  - Each Federation Node can be added to a single group at a time. A node can be added to a group by clicking on the group's **Add Node** button. A dialog box appears with the name of the group shown in the top box. Enter the IP Address of the node to be added and click on **Add Node**.

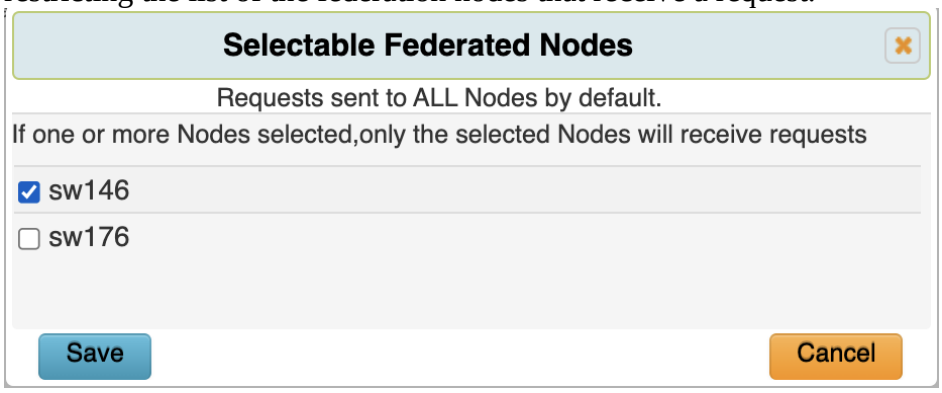
Once a node is added, its details (including the nodename) are displayed. Federated Nodes (appliances) support MTU size of up to 1600. Each node supports packet decoding of these protocols: IPv4, IPv6, TCP, UDP, SCTP, ICMPv4, ICMPv6, GRE, Ethernet, VLAN, ERSPAN, VXLAN, VNTAG, HTTP, HTTP/2, SSL, TLS, SMB, DCERPC, SMTP, FTP, SSH, DNS, NTP, DHCP, TFTP, KRB5, IKEv2, SIP, SNMP

  - The advertised throughput includes system resource calculations for packet processing. As such, the throughput is measured as it reaches the interface, not after internal processing. This allows us to ensure we do not drop packets, while still giving accurate metrics.
  - Delete Node: A node can be deleted by selecting **Delete Node** button. This does not cause any change in the capture state of the node. This node can now be added to the same group or to a different group.
  - Pause/Resume Capture: A node's capture can be paused and resumed if necessary, using the button **Pause Capture** that toggles to **Resume Capture** on being Paused and vice versa.

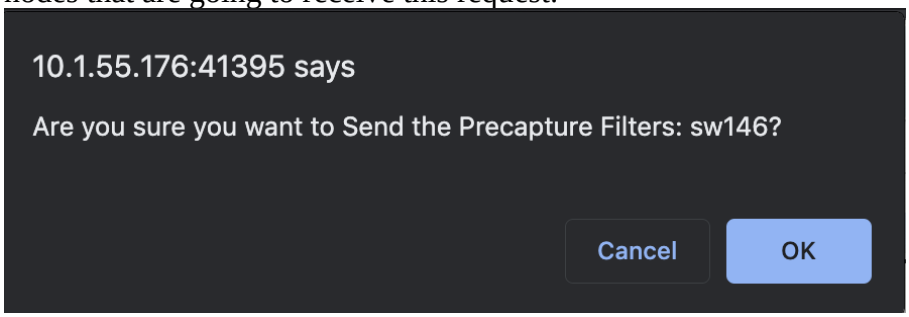


3.1.2 Selectable Nodes

By default, every request to the FM server is sent to all connected federation nodes. This menu option allows restricting the list of the federation nodes that receive a request.



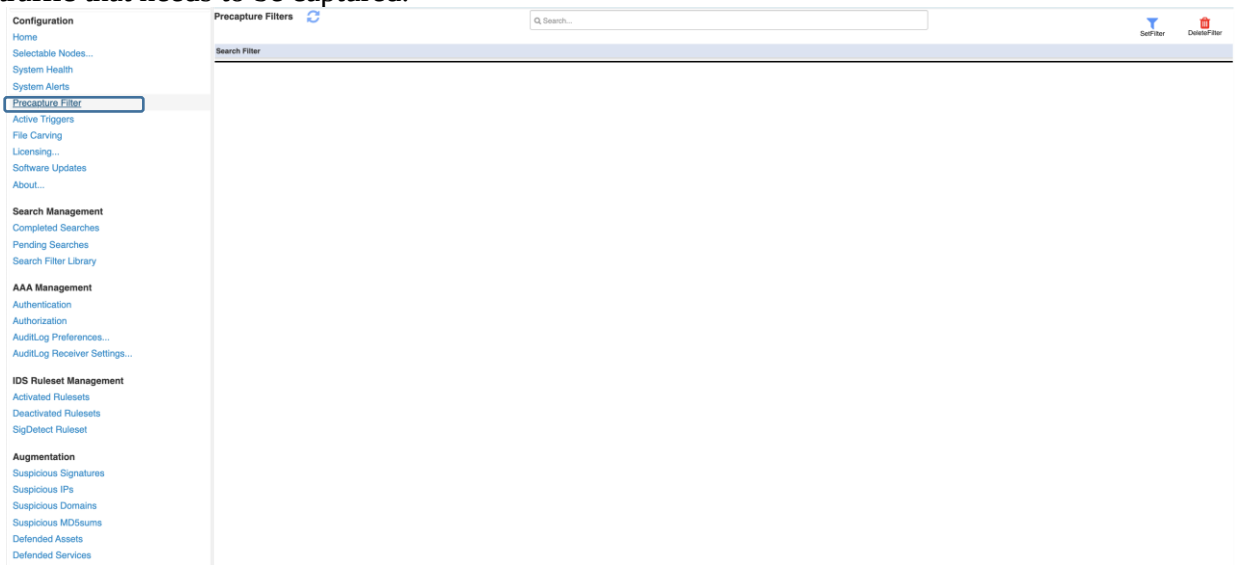
From this point on, when a request such as SetPrecapture is initiated, the user is presented with the list of nodes that are going to receive this request:



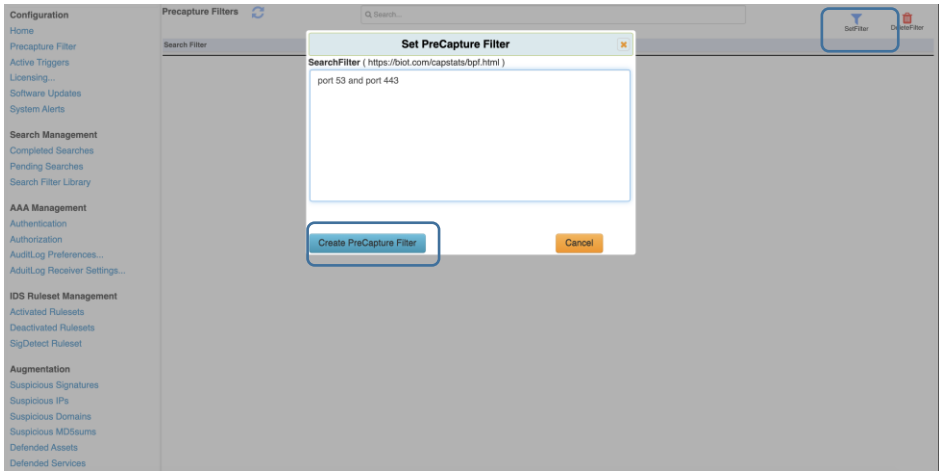
3.1.3 Precapture Filter

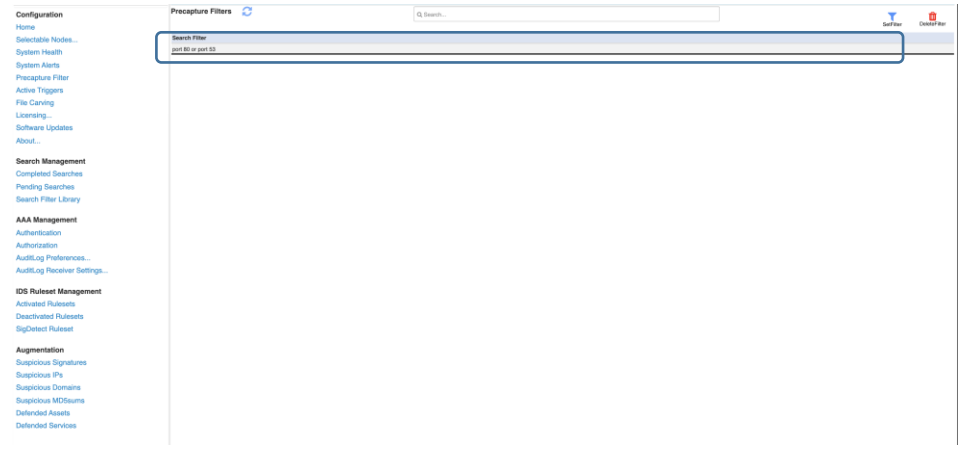
By default, all the received traffic is captured and stored. A precapture filter can be applied to receive only the

traffic that needs to be captured.



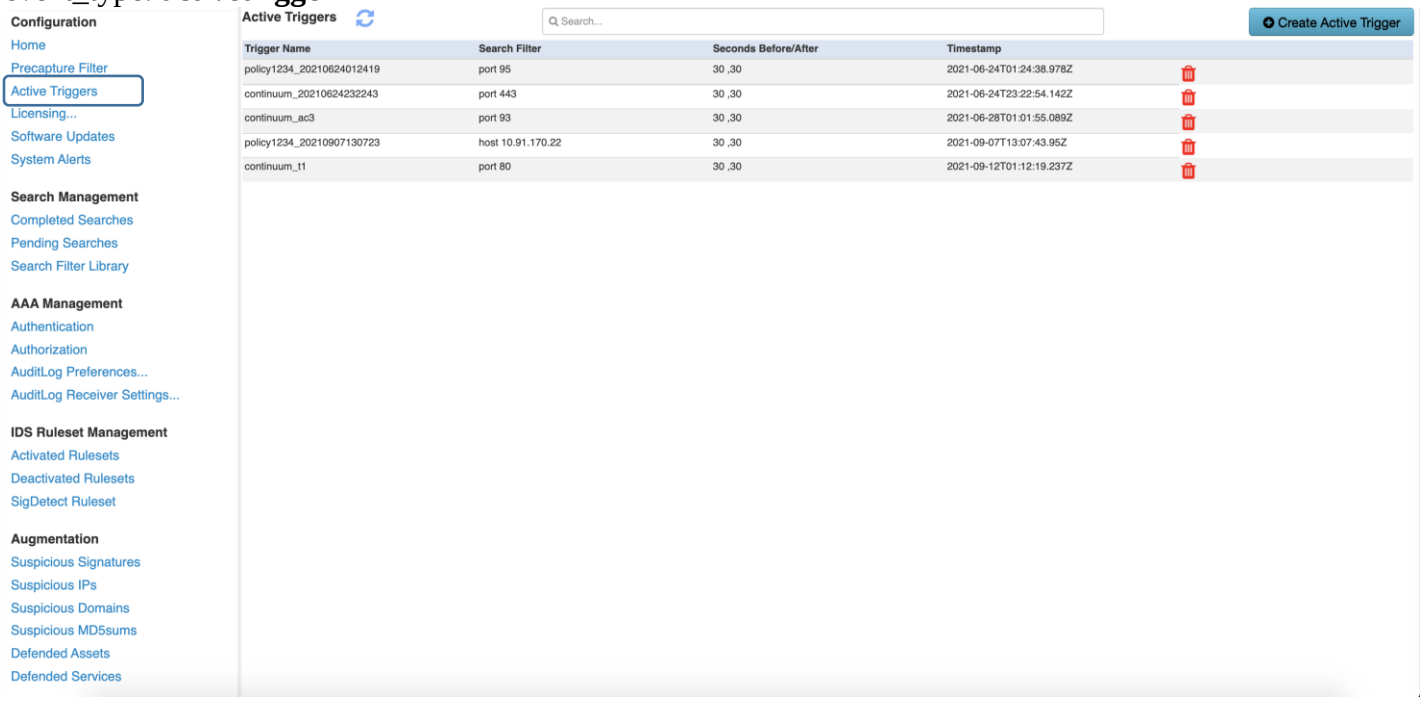
Click on SetFilter button to set a precapture filter. The following filter will result in is capturing traffic that has port 53 or port 80 as either source or destination port.





3.1.4 Active Triggers

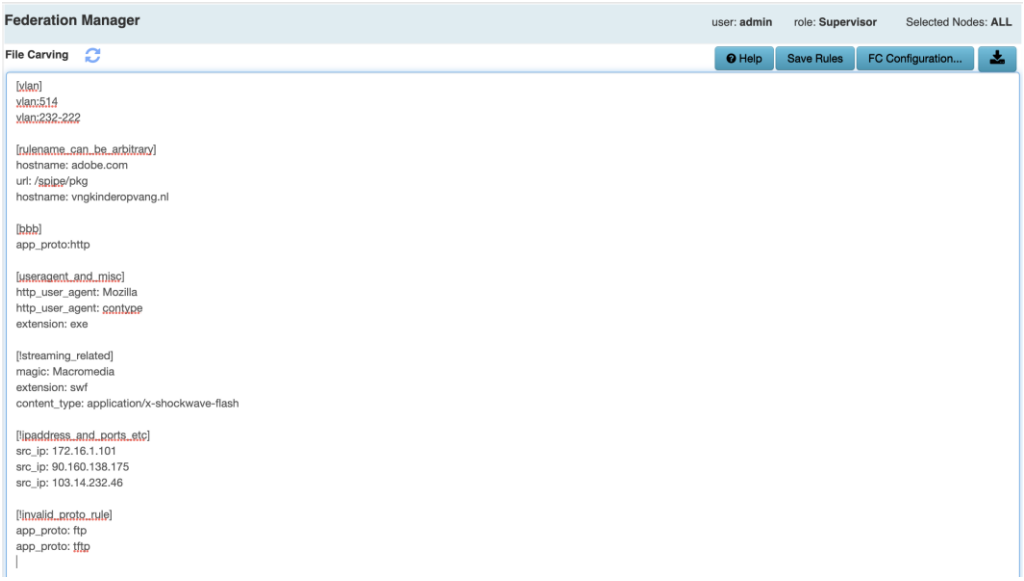
Active Triggers offer a simple mechanism to generate alerts based on Berkeley Packet Filter (BPF). Authorized users can create, view, and delete active triggers. The alerts generated by these triggers have the event_type: **activetrigger**



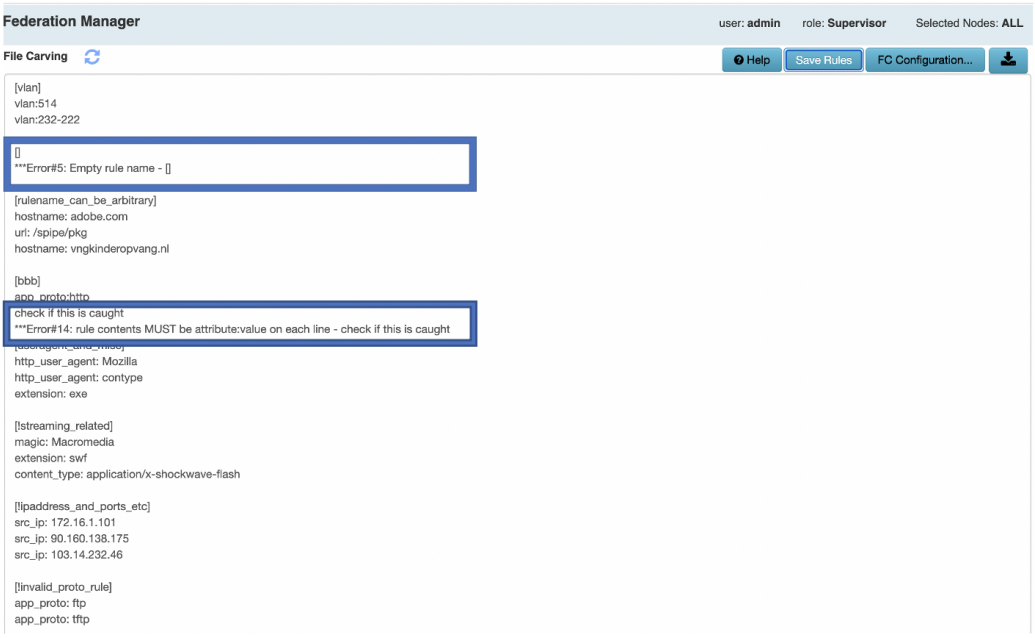
A user must have a role with Policy permission enabled to be able to create and delete active triggers. Other users can view created triggers.
Active trigger name can only have alphanumeric characters and underscore (_). Duplicate names are not allowed.
Active trigger filter must be a valid BPF filter. It cannot be ip, tcp, udp, tcp or udp as these are trivial filters.
Seconds before and Seconds after fields help avoid active trigger storms if the matches are occurring too frequently.

3.1.5 File Carving

The Capture Server extracts files from captured traffic stream and stores them to the disk, based on various configuration parameters. File Carving (**FC**) does not impact capture, indexing, or search performance.
File Carving page allows authorized users to specify file carving rules and save them to the server. If the rules are valid, they are forwarded to each federated node.



The rule page is editable. Add/Modify/Delete rules as necessary and press **Save Rules** button. If there are errors, the errors are displayed below the line where the error occurred.



Fix the errors and press **Save Rules** button again. When (and only when) there are no errors, this file is saved and sent to each Federated Node.

3.1.5.1 FC Attributes

Each rule contains one or more attributes. The following are valid attributes that are recognized by the file carving processor. Attribute names and their values are case sensitive. Attributes url, http_user_agent, http_content_type are wildcard matches. All other attributes are exact matches.

Attribute	Description	Example(s)	Notes
vlan	1-4094	vlan:1 vlan:200-300	Exact match
src_ip	Source Host IP	src_ip:10.1.5.4	Exact match
dest_ip	Destination Host IP	dest_ip:5.6.7.8	Exact match
host	Source or Destination IP		Exact match
proto	Protocol string	proto:tcp	Exact match
app_proto	Application Protocol	app_proto:http app_proto:tls app_proto:dns	Exact match
http_method	POST,GET,PUT,DELETE	http_method:POST	Exact match POST matches xPOSTy does not match
extension	File extension specified	extension:pdf extension:docx	Exact match Abc1.pdf matches Abc1.abpdf does not match
status	http status code	status:200 status:401	Exact match
filename	Name of the extracted file	filename:abc_logo.png	Exact match
url	Substring of url value Taken as *<value>*	url:spipe	**Wildcard match**

http_user_agent	User Agent	http_user_agent:Mozilla	**Wildcard match**
http_content_type	Content type	http_content_type:json	**Wildcard match**
magic	File Magic information independent of the file extension	magic:Windows	**Wildcard match**

3.1.5.2 FC Rules

File Carving rules allow controlled forwarding of files to an external system(/application) for further processing. Multiple rules can be specified simultaneously. Each rule contains one or more attributes that map to DPI file event metadata attributes (listed in FC Attributes table shown above).

- When there are multiple rules, they are evaluated as part of an **OR** expression by default:
  rule1 OR rule2 OR rule3
- When a rule contains multiple attributes:
  - If the rulename is preceded by '&', its attributes are evaluated as part of an AND expression.
    - If an attribute name is preceded by '!', it is evaluated as AND NOT
  - If the rulename is NOT preceded by '&', its attributes are evaluated as part of an OR expression

- A positive rule passes when specified attribute values **match** the corresponding attribute values of file event metadata. Format of each positive rule is as follows:
  [rulename1]
  attribute1:value1
  attribute2:value2

- Example1 of positive rule – Any file event with vlan 234 or vlan between 3000 through 3005 are considered a match:
  [samplerule1]
  vlan:234
  vlan:3000-3005

- Example2 of positive rule – Any file event with src_ip 10.1.44.22 or file magic string that contains the word Windows is considered a match:
  [samplerule2]
  src_ip:10.1.44.22
  magic:Windows

- Example3 of positive rule with '&' – Any file event with src_ip 10.1.44.22 **and** file magic string that contains the word Windows is considered a match:
  [&samplerule3]
  src_ip:10.1.44.22
  magic:Windows

- Example4 of positive rule with '&' and '!' – Any file event with src_ip 10.1.44.22 **and** file magic string that **does not contain** the word Windows is considered a match:
  [&samplerule4]
  src_ip:10.1.44.22
  !magic:Windows
-

- A negative rule passes when specified attribute values **do not match** the corresponding attribute values of file event metadata. Prepend a rule name with exclamation character **!** to make it a negative rule. Format of each negative rule is as follows:
  [!rulename2]
  attribute3:value3
  attribute4:value4

- Example of a negative rule – Any file event with *app_proto* value **not equal** to *ftp* is considered a match.
  [!samplerule8]
  app_proto:ftp

3.1.5.3 An example workflow:

- When multiple rules are specified, a single rule match results in the corresponding Consider the following set of rules:

  [e1rule]
  app_proto:smb

  [e2rule]
  vlan:514

  This rule set allows any file event with app_proto: smb OR vlan:514. Just one rule match is enough to forward the file specified by the file event.
  If a file event has app_proto:http and vlan:305, none of the rules matches. The file specified by this file event is dropped.

- Add one more rule to the set:

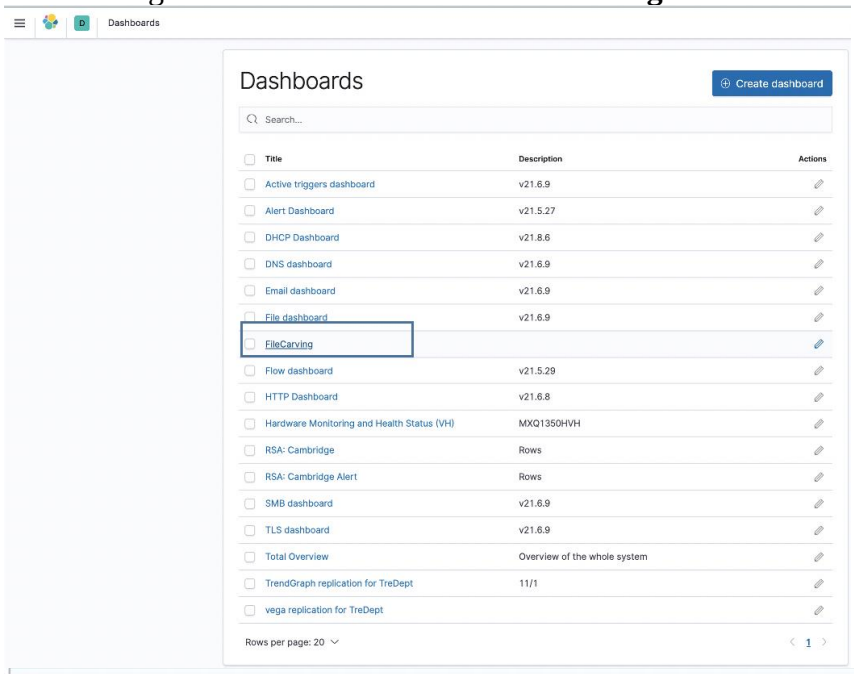
  [e1rule]
  app_proto:smb

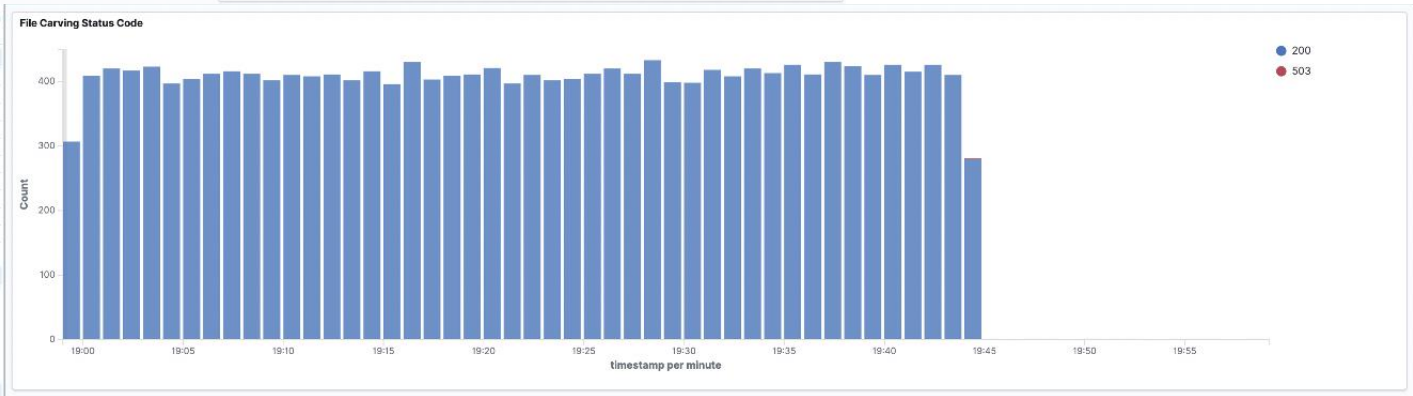
  [e2rule]
  vlan:514

  [!e5vlanx]
  vlan:300

  Addition of the negative rule e5vlanx results in any event with a vlan not equal to 300 being forwarded to the file processing server.

File Carving is available as a dashboard in **Investigator View:**





File Carving Log

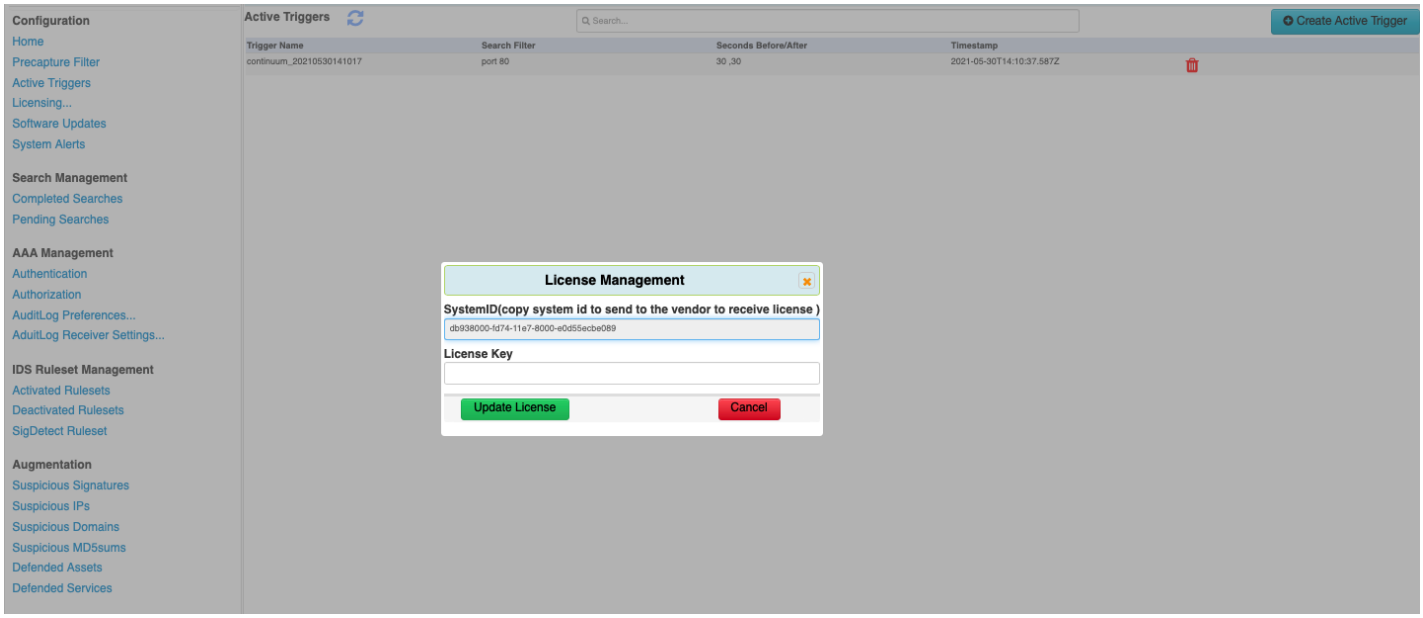
Nov 14, 2021 @ 19:44:38.000	sw176	10.1.8.160_80_10.1.8.151_2628_328e94df4f351ae79e327c4e5e1c2ca54b7c6ddb13bea70ba18f52ec8e37c7ad	503
Nov 14, 2021 @ 19:44:37.000	sw176	10.1.8.160_80_10.1.8.151_2580_0ec82929160dcdf2e2b9e9f1ed89720f0b237f98f0ea3a67027ff3239c03c556	200
Nov 14, 2021 @ 19:44:37.000	sw176	10.1.8.160_80_10.1.8.151_2581_dc9ba824f5f4caf778f7b8162a67d106fe9c4c23ef3503dd974c47af82bf3db2	200
Nov 14, 2021 @ 19:44:37.000	sw176	10.1.8.160_80_10.1.8.151_2588_0c7b569a0ad39513a7a238117912f85945af36d8aaccbbfbe81907b1f3dbd754	200
Nov 14, 2021 @ 19:44:37.000	sw176	10.1.8.160_80_10.1.8.151_2588_aae002664c9eeeb7468fca80a83806311f13d17bf0b33277638a22b4cc19cf5d	200
Nov 14, 2021 @ 19:44:37.000	sw176	10.1.8.160_80_10.1.8.151_2593_35d995b5322134fc1f645a3a32d919f698d184b7b3705424ecac7fa7340b3fb6	200
Nov 14, 2021 @ 19:44:37.000	sw176	10.1.8.160_80_10.1.8.151_2593_64b8fd9cd36b6cc77a0271b919b5171feac634155d3d77f8620595cb1cfa5e9a	200
Nov 14, 2021 @ 19:44:37.000	sw176	10.1.8.160_80_10.1.8.151_2593_c8d042a80c16123dbfbb7ab0c1e7a99d2c5aa48e2425581fa9ac8544c4f951e6	200
Nov 14, 2021 @ 19:44:37.000	sw176	10.1.8.160_80_10.1.8.151_2595_8a6999b4ce2c63330c19ef94bfe35adb99b6b9a640034dcdbafa79b3b23911ff	200
Nov 14, 2021 @ 19:44:37.000	sw176	10.1.8.160_80_10.1.8.151_2597_c2da186542bc6a89434152936a46c2e11bb6193e71ebd1137c7595d9d568e5a8	200
Nov 14, 2021 @ 19:44:36.000	sw176	10.1.8.160_80_10.1.8.151_2546_ba44b2bf68b180e9c963f3fed5c14149c2f2ce6d9bf3305ab157d324496b227c	200
Nov 14, 2021 @ 19:44:36.000	sw176	10.1.8.160_80_10.1.8.151_2547_26e9036331a8b5b38eb341fc9685b298aa1e2b17aa83c17350d0703cc7c49f78	200
Nov 14, 2021 @ 19:44:36.000	sw176	10.1.8.160_80_10.1.8.151_2555_b4ca8693879ae00682ef51df38254cefa3ab5c225f517e465447b3855d6dcce5	200

3.1.6 Licensing

1. Contact your Security representative to obtain a license key for the Federation Manager.

   Note:

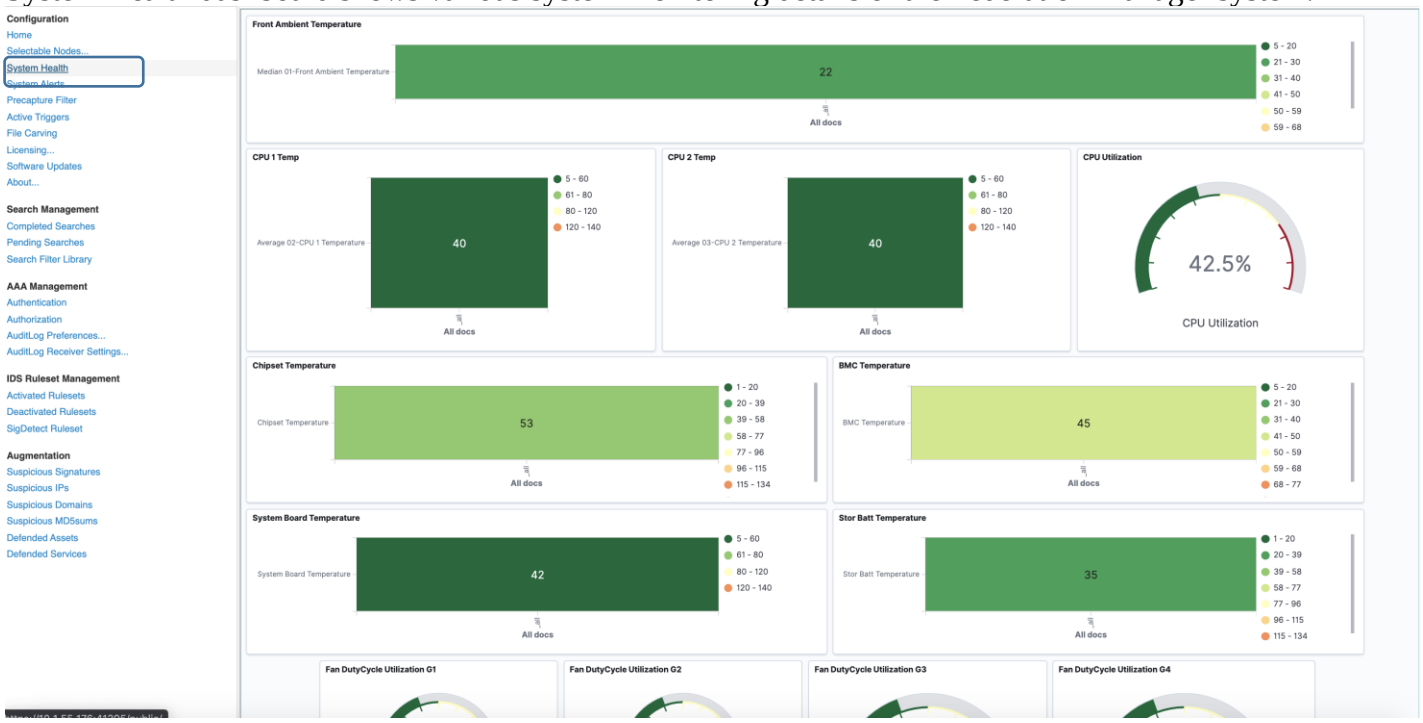
   - System Id is required to obtain a valid license key.
   - Only Admin or authorized users, can apply the license key.
2. Once a license key has been forwarded, copy and paste the provided string into the License Key text box in the web user interface.
3. Click “Update License” button to apply the new license.



Note: A user must have a role with licensing permission enabled to be able update software license.

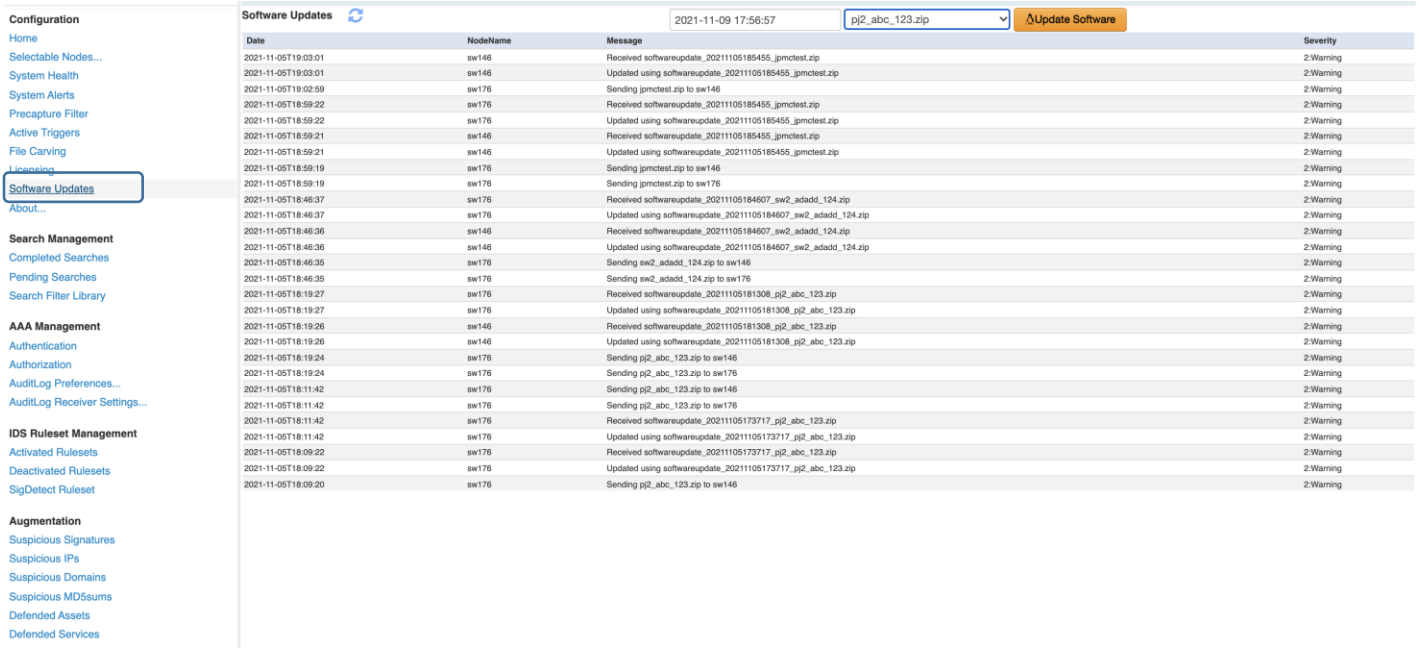
3.1.7 System Health

System Health dashboard shows various system monitoring details of the Federation Manager system.



3.1.8 Software Updates

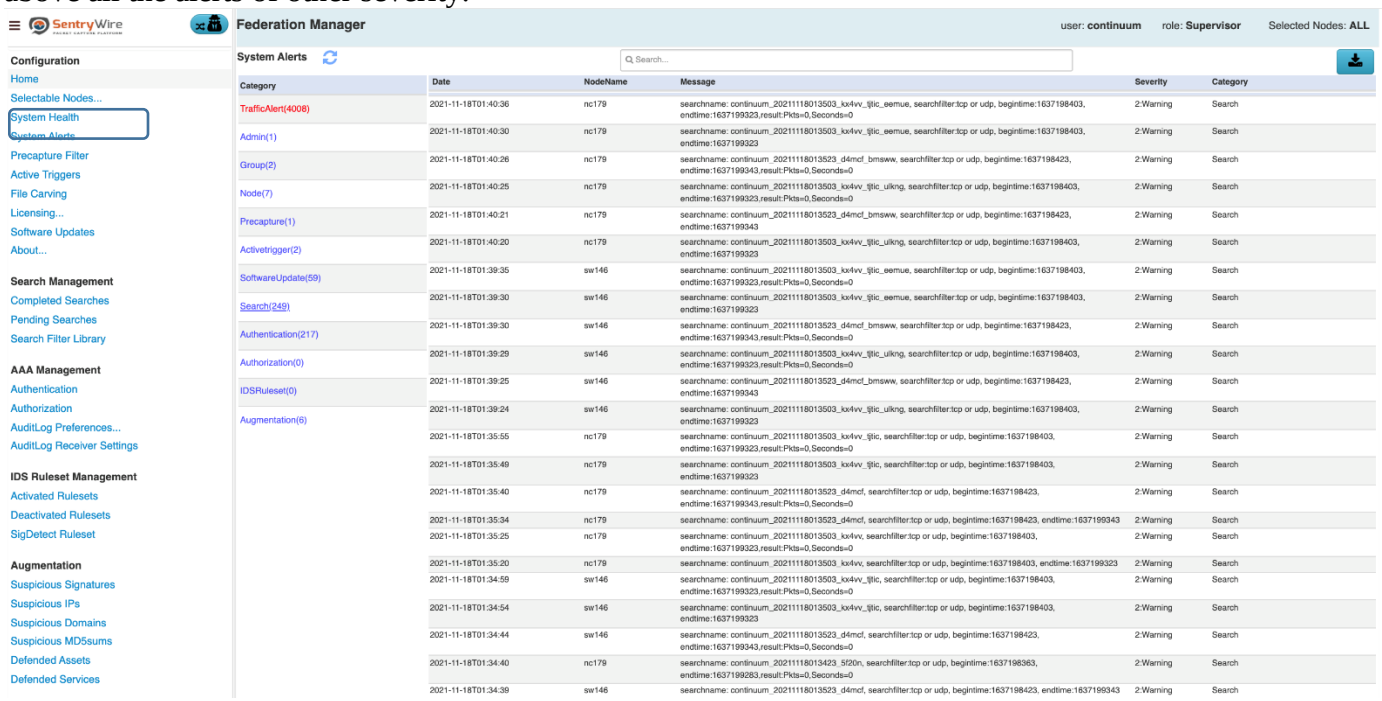
This page allows the user to perform FM license update, software updates and reboot/shutdown Federated Nodes. The software updates are specific to the Federation Manager and its nodes. Each software update must be made available in a specific folder accessible to the Federation Manager server. Authorized users can select the date and time of the software to be installed.



A user must have a role with Policy permission enabled to be able update software. Each package is a zip file that contains an installer script, a version.txt file, and a tgz file with all the files necessary files for completing the software update. Software update alerts are shown on this page when the update is scheduled to run, when it is running and the result of the update on each node.

3.1.9 System Alerts

This page shows system alerts from all the Federated Nodes. Severe alerts are displayed in descending order above all the alerts of other severity.



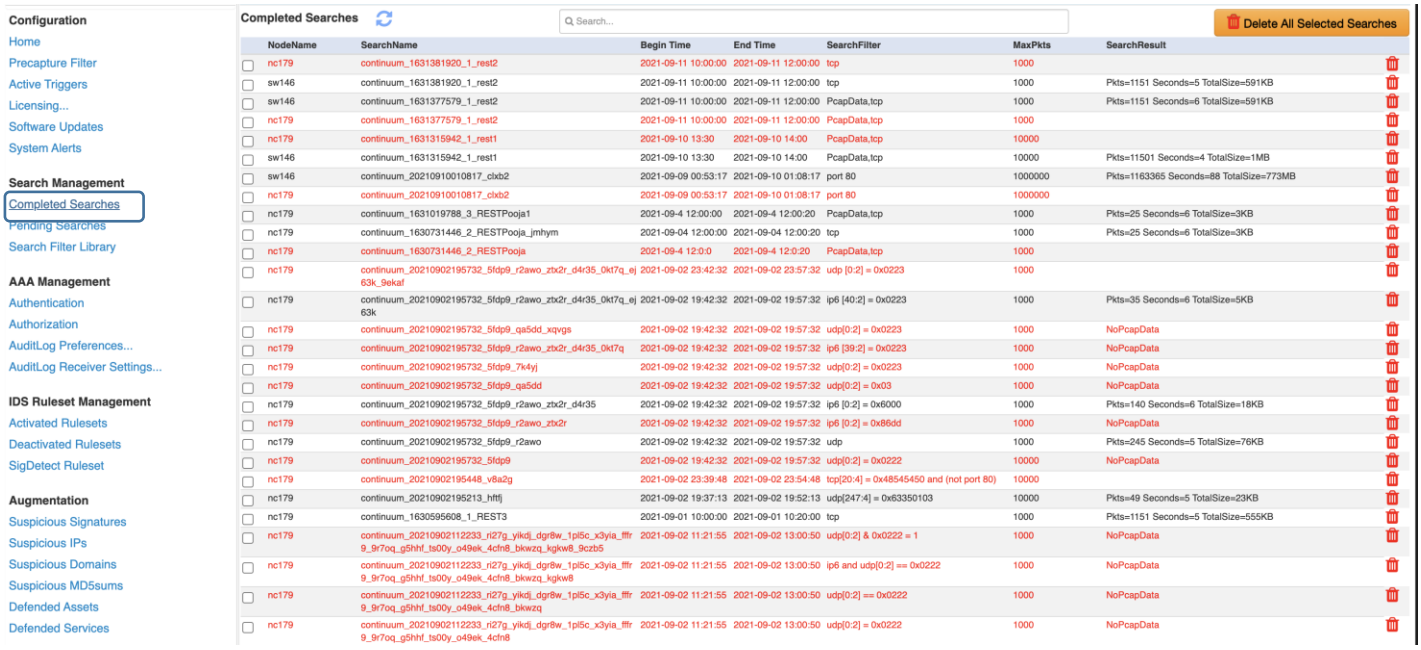
The search bar allows narrowing down alerts by date, nodename, severity, category, and terms inside the message. Any authorized user can download System Alerts. These cannot be deleted.

3.2 SEARCH MANAGEMENT

Investigator UI allows users to create a search, view packets, download data and clone a search.
FM Admin UI allows authorized users to delete multiple searches at a time.

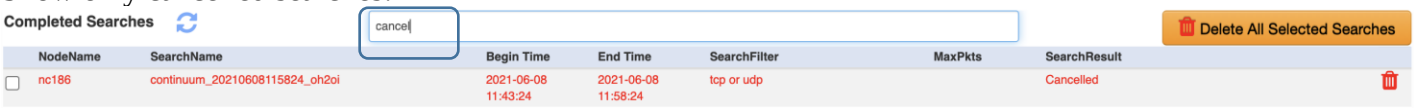
3.2.1 Completed Searches

Completed searches from all the Federated Nodes are displayed on this page. Search name contains name of the user who created the search. Each node's search returns different set of packets; therefore, they are represented as a separate line.

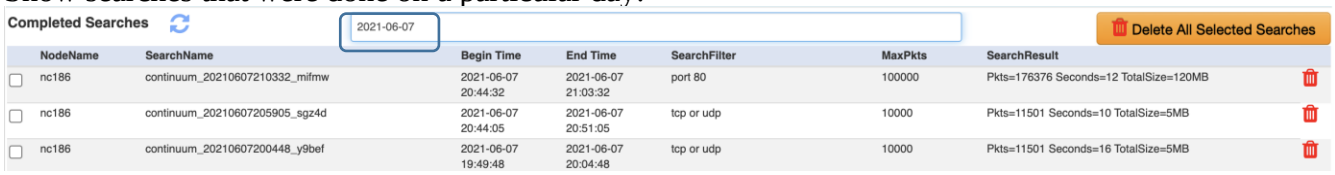


The Search bar is critical in narrowing down the results to view and delete searches.
Few examples of the search bar usage:

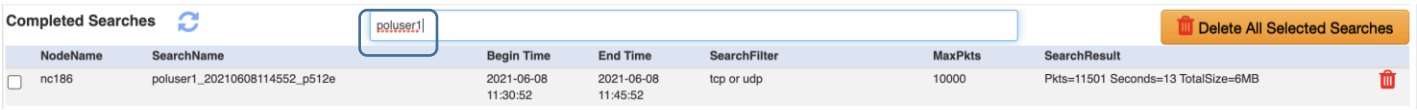
Show only cancelled searches:



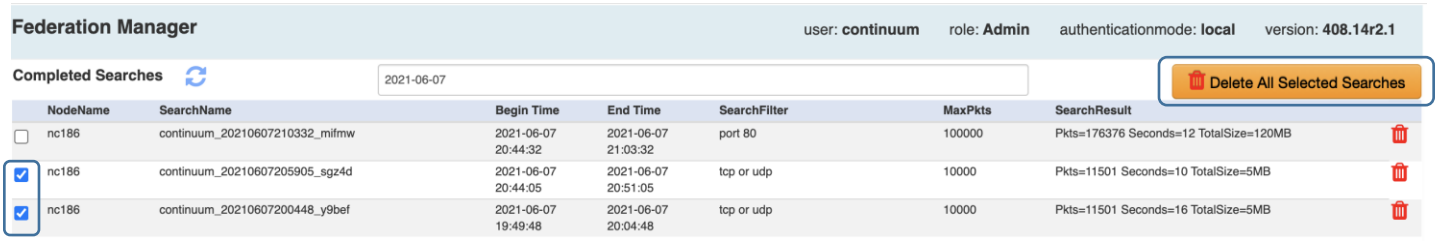
Show searches that were done on a particular day:



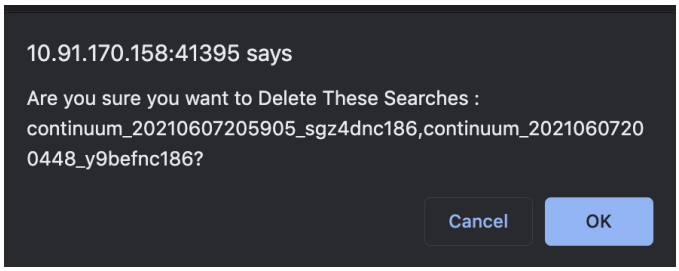
Show searches of a particular user:



Once searches are narrowed down as shown above, user can select one or more of the searches and click on Delete All Selected Searches button to delete them:

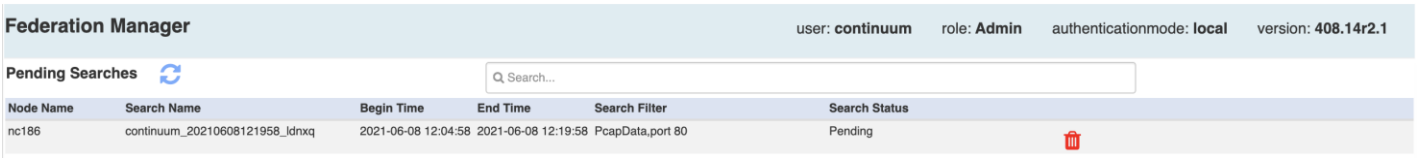


User is asked to confirm the selected list of searches to be deleted:



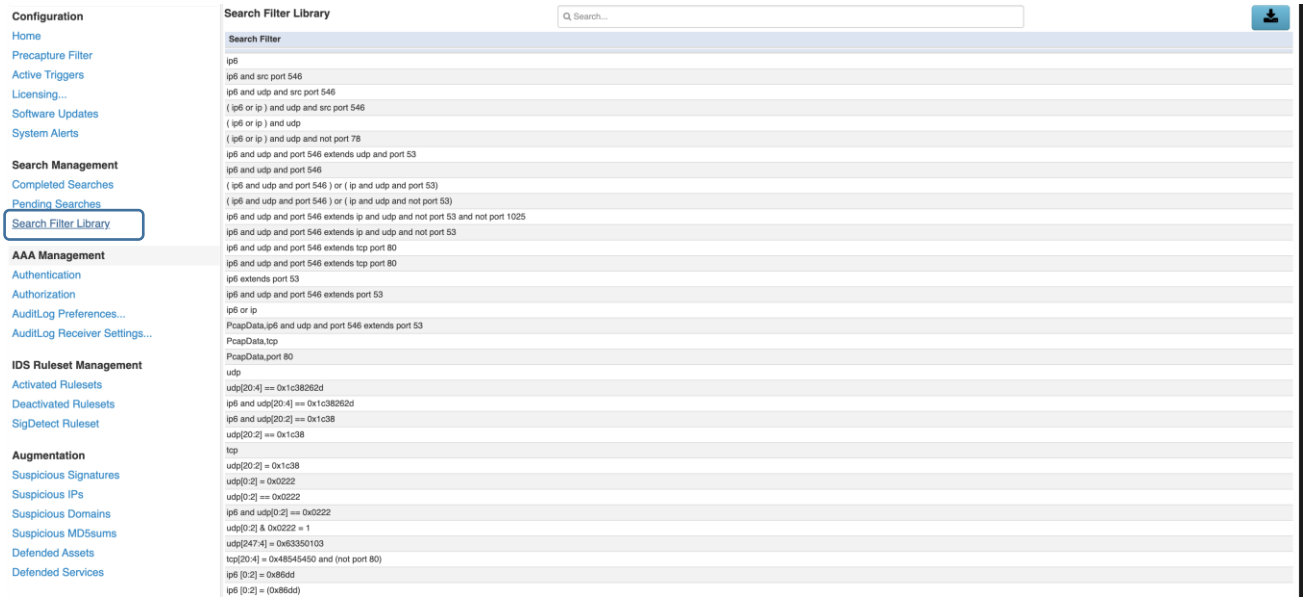
3.2.2 Pending Searches

This page shows all the searches that are currently queued or in progress. A search on this page can be cancelled. A cancelled search moves to Completed Searches page from which it can be removed. The search bar allows users to narrow down the pending searches. Pending searches can be cancelled one at a time.



3.2.3 Search Filter Library

This page shows the list of unique search filters from previous searches. These can be downloaded but not be deleted.

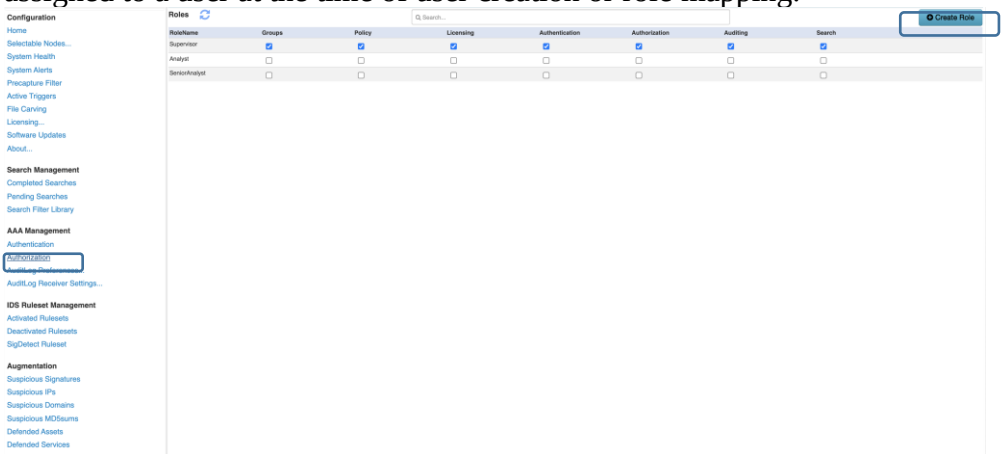


3.3 AAA MANAGEMENT

This group of menu items allows users to handle Authentication, Authorization and Auditing

3.3.1 Authorization

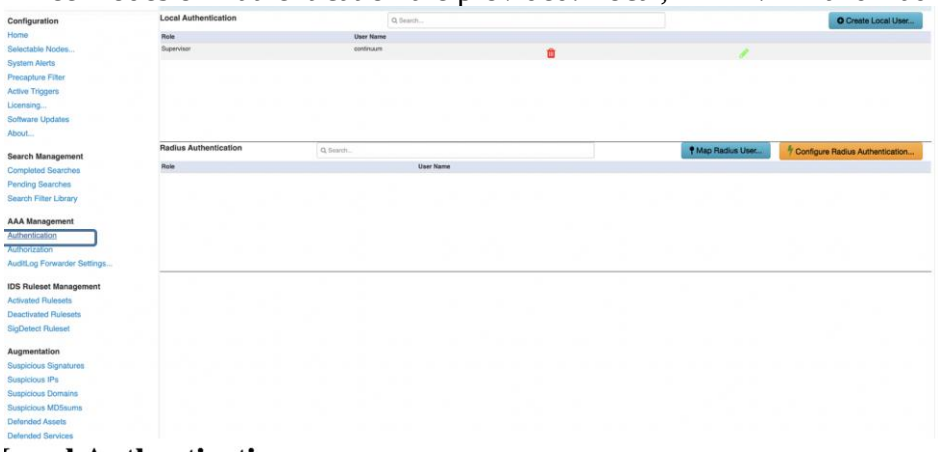
Authorization page allows creating new roles and setting permissions for each role. When a user is assigned a role, the FM UI actions are enabled/disabled based on the permissions of the role. Once created, these roles are provided as a dropdown list for each of the authentication modes under the Authentication tab and can be assigned to a user at the time of user creation or role mapping.



To add a role, click on the “Create Role” button at the top right of the panel. The above picture shows several roles created each with a specific permission. Each role can have multiple permissions.

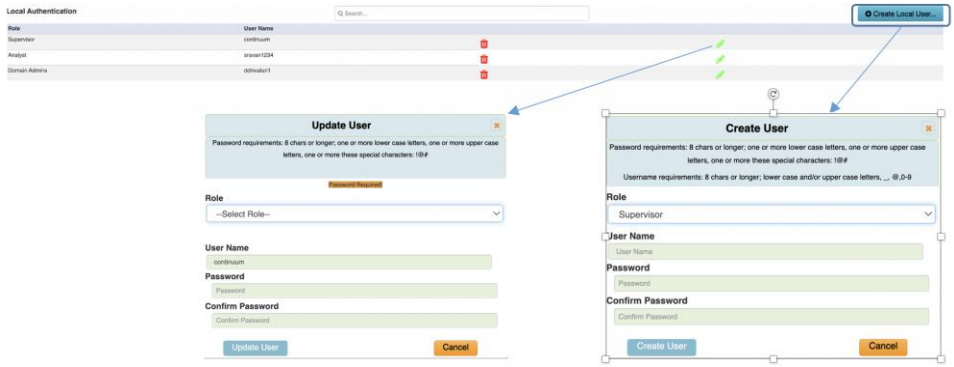
3.3.2 Authentication

Three modes of Authentication are provided: Local, LDAP/AD and Radius authentication



Local Authentication

Local Authentication allows administrators to create/delete/modify users with a role and a password maintained on the FM server.

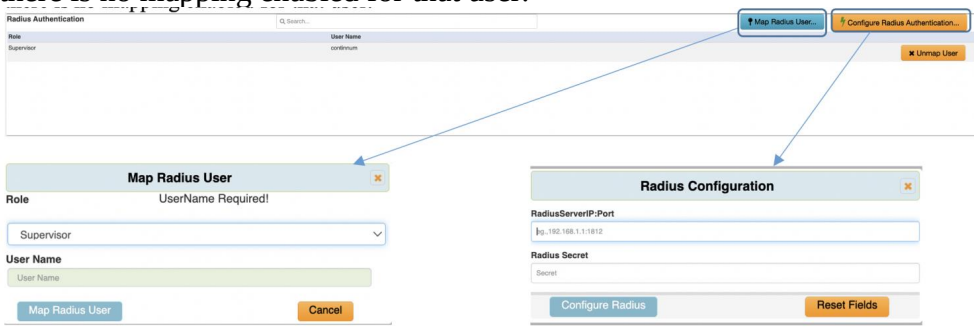


LDAP/AD Authentication

There is no UI Admin step necessary as LDAP/AD Authentication server is embedded.

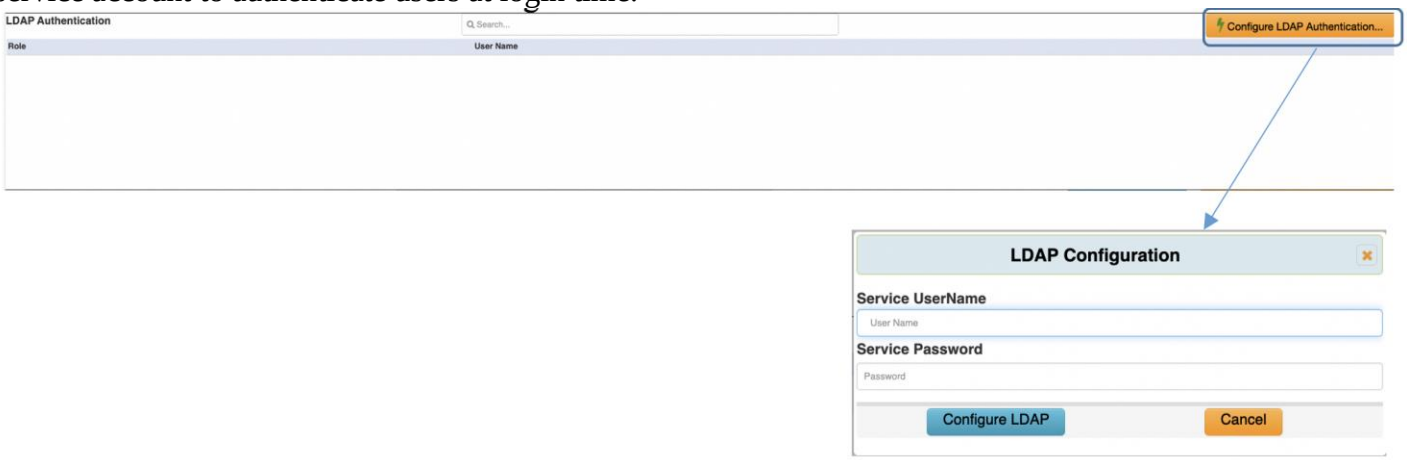
Radius Authentication

Radius authentication requires IP:Port of the radius server and the Radius secret string to be configured. FM server uses this information to authenticate Radius users at login time. MapUser allows a Radius user to be mapped to a FM role. The image shows one Radius mapped user named continuum mapped to Supervisor role. Each mapped user is assigned their mapped role on logging in. A Radius user is not allowed to login if there is no mapping enabled for that user.



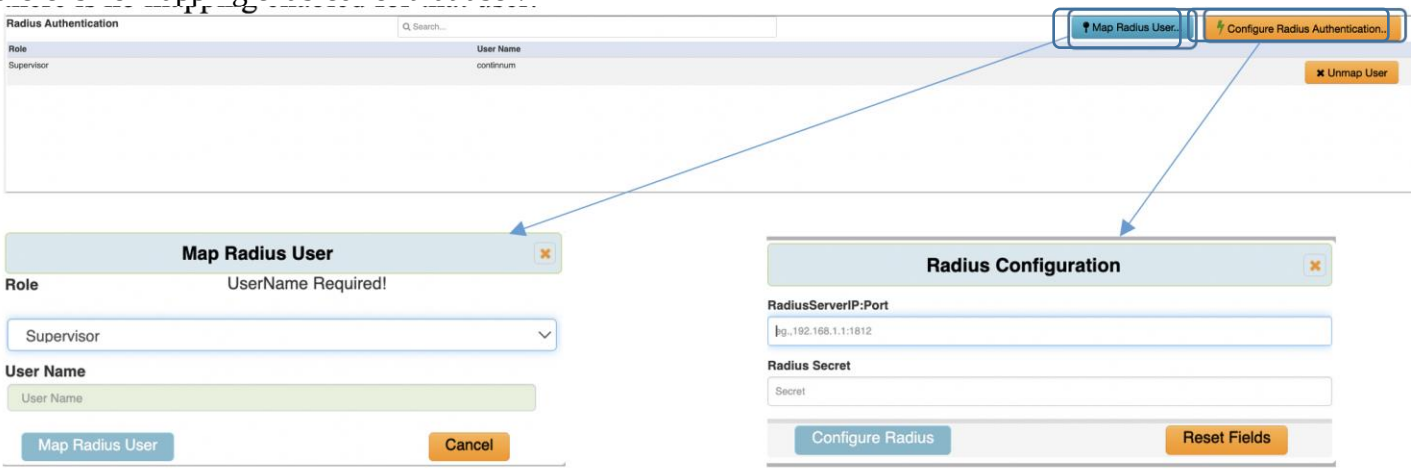
LDAP Authentication

Before any AD/LDAP user can login, a service username/password must be provided. FM server uses this service account to authenticate users at login time.



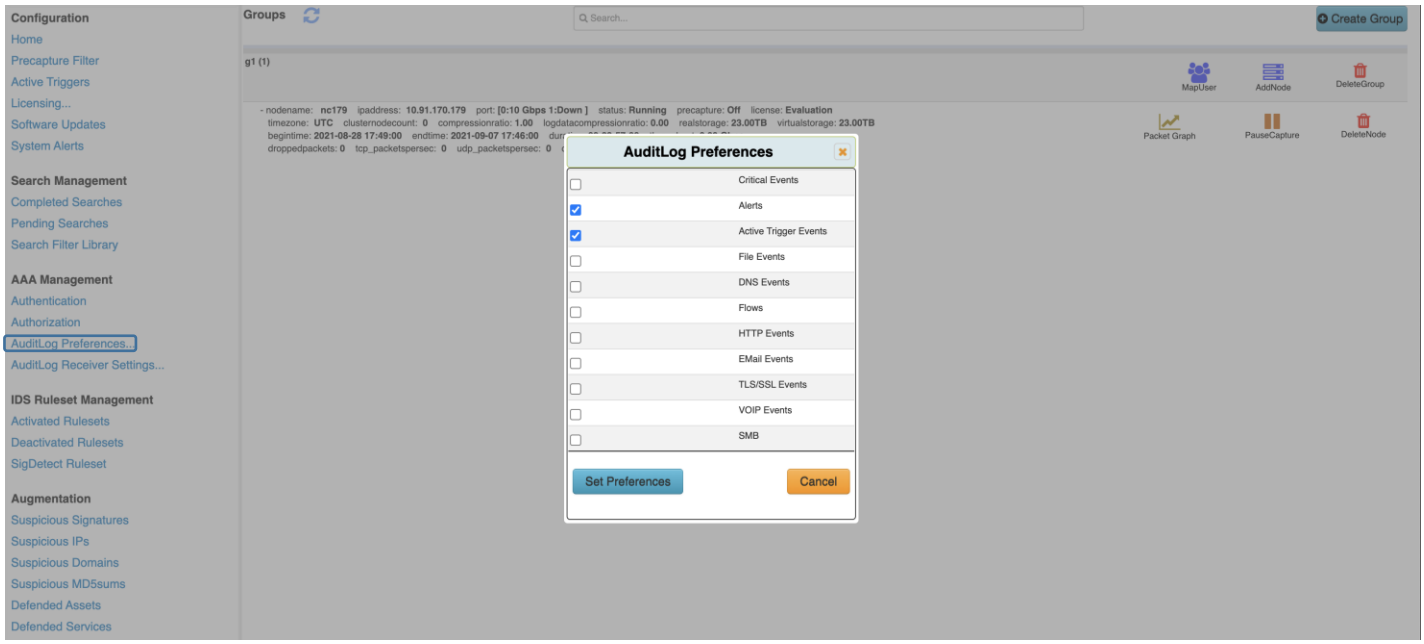
Radius Authentication

Radius authentication requires IP:Port of the radius server and the Radius secret string to be configured. FM server uses this information to authenticate Radius users at login time. MapUser allows a Radius user to be mapped to a FM role. The image shows one Radius mapped user named continuum mapped to Supervisor role. Each mapped user is assigned their mapped role on logging in. A Radius user is not allowed to login if there is no mapping enabled for that user.



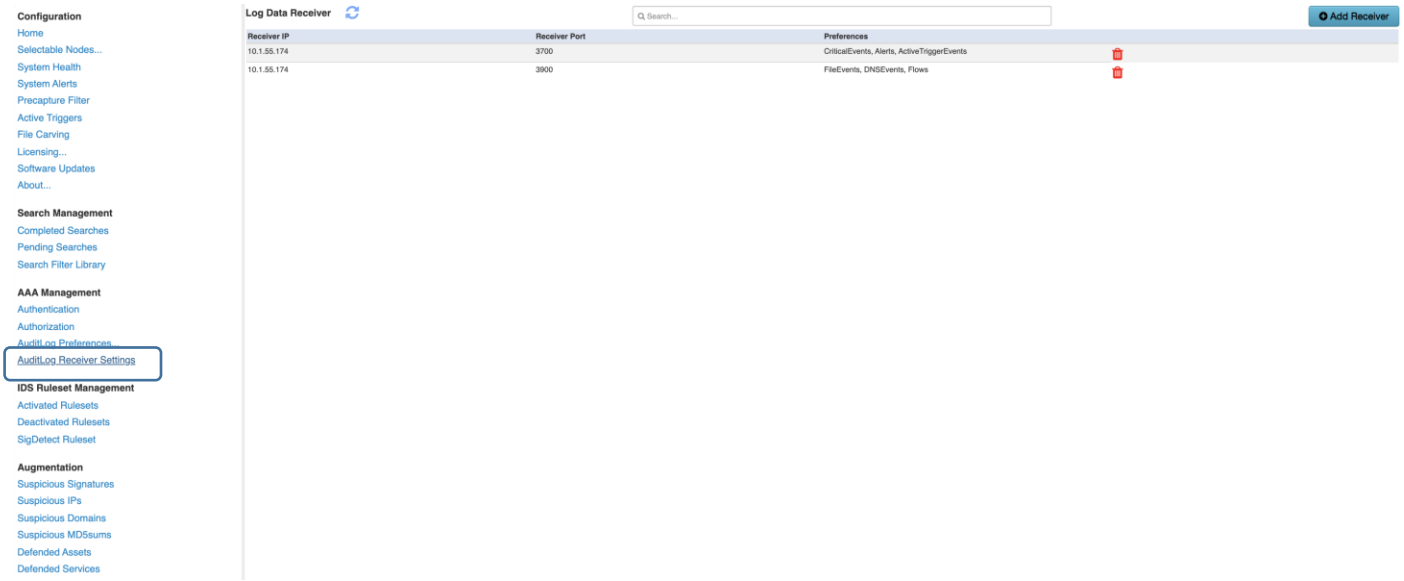
3.3.3 Auditlog Preferences

Logs of various event types are generated by the capture and analytics servers. Auditlog Preferences dialog box allows users to indicate which of the logs must be made available to the external applications such as Splunk.

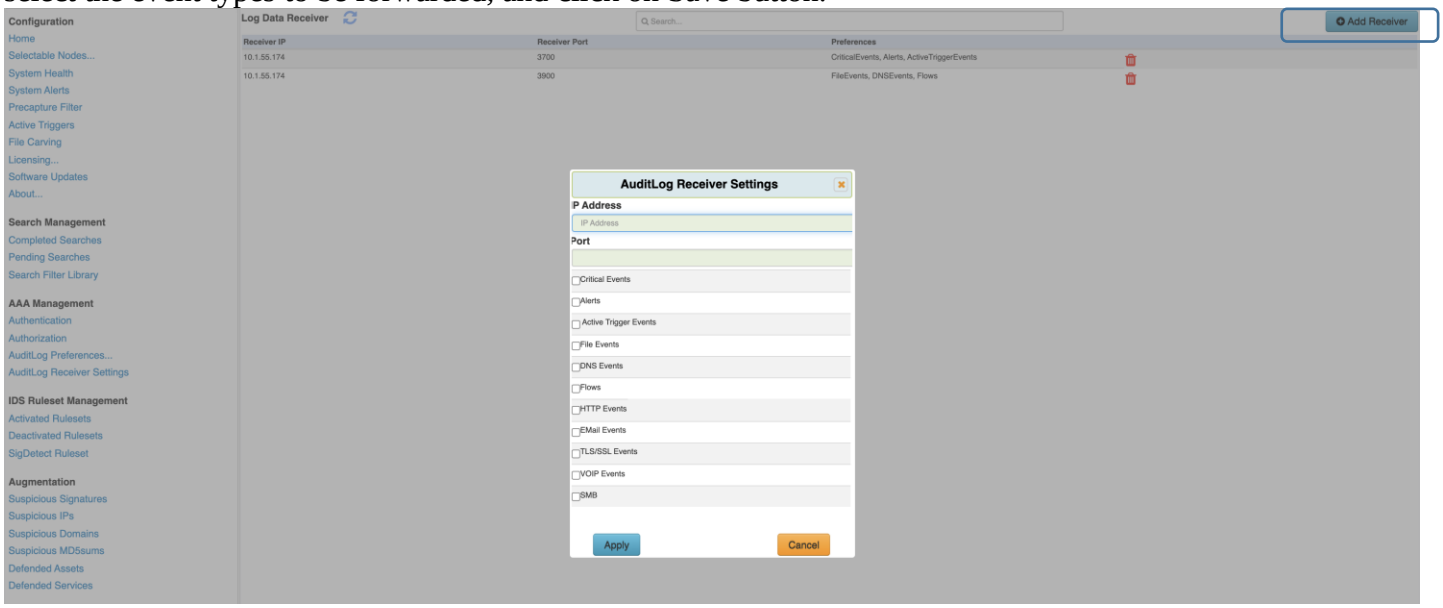


3.3.4 Auditlog Receiver Settings

These settings will allow the server to forward logs to be pushed to an external server running at the IPAddress:Port. The frequency of forwarding is once every 5 minutes by default. The receiver must be able to receive .zip files.



Multiple AuditLog Receivers can be active simultaneously. Each receiver can receive logs of different types. To add a new AuditLog Receiver, click on Add Receiver button, enter new receiver's IP Address and Port, select the event types to be forwarded, and click on Save button.



3.4 IDS RULESET MANAGEMENT

IDS Rulesets are list of extensive rules (signatures). The user also has the privilege to upload user defined rulesets based on their specific needs. The format of these rulesets can be found at https://suricata.readthedocs.io/en/suricata-6.0.0/rules/intro.html

This group has the menu options to upload, activate, deactivate and delete IDS Rulesets and SigDetect Rulesets.

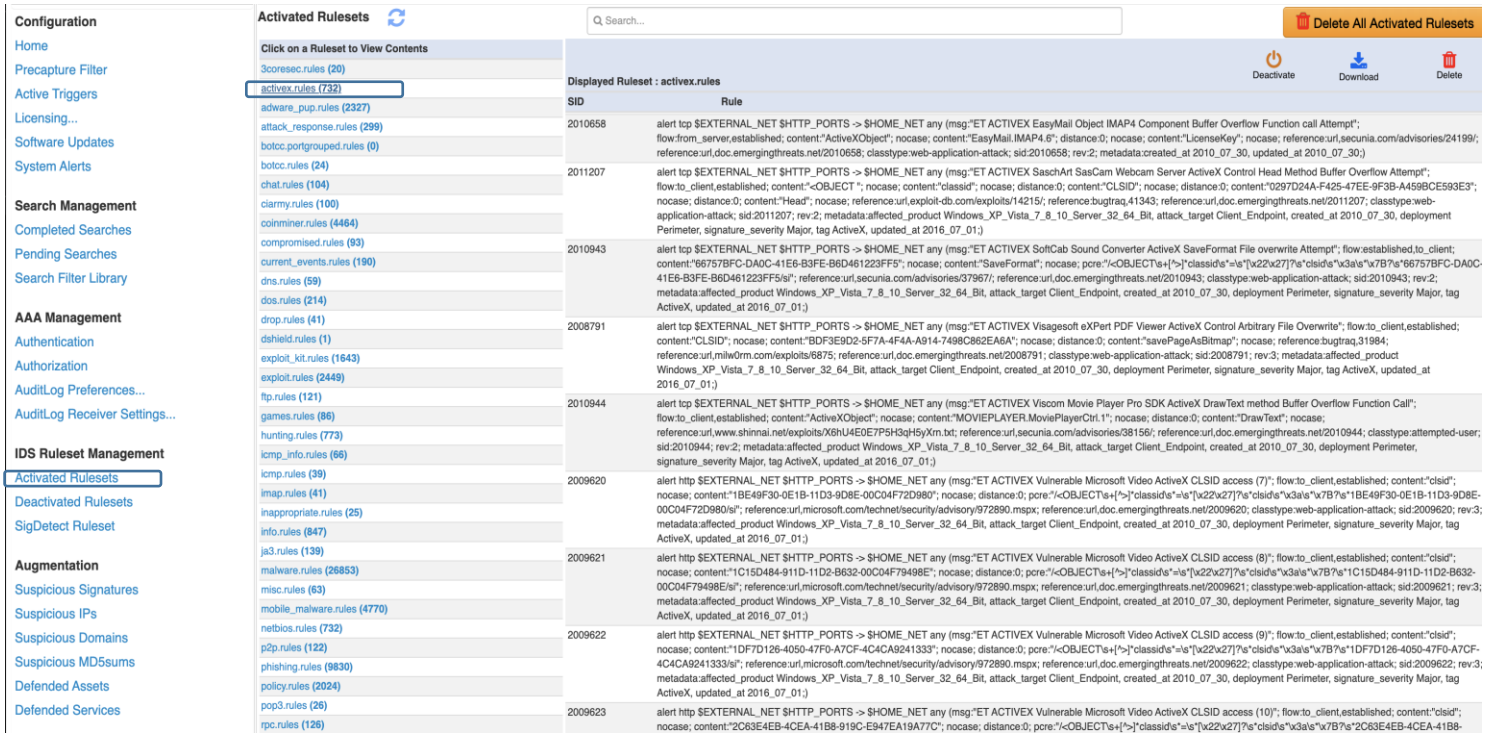
- Activated Rulesets
- Deactivated Rulesets
- SigDetect Rulesets

When an IDS ruleset is uploaded, it is part of the Deactivated Rulesets. The newly uploaded ruleset must be activated before its rules are made available to the server. If the uploaded ruleset has the same name as a ruleset that has already been uploaded, the new ruleset replaces the old ruleset.

3.4.1 Activated Rulesets

This page allows authorized users to view activated IDS Rulesets, deactivate rulesets to stop alerts from being generated.

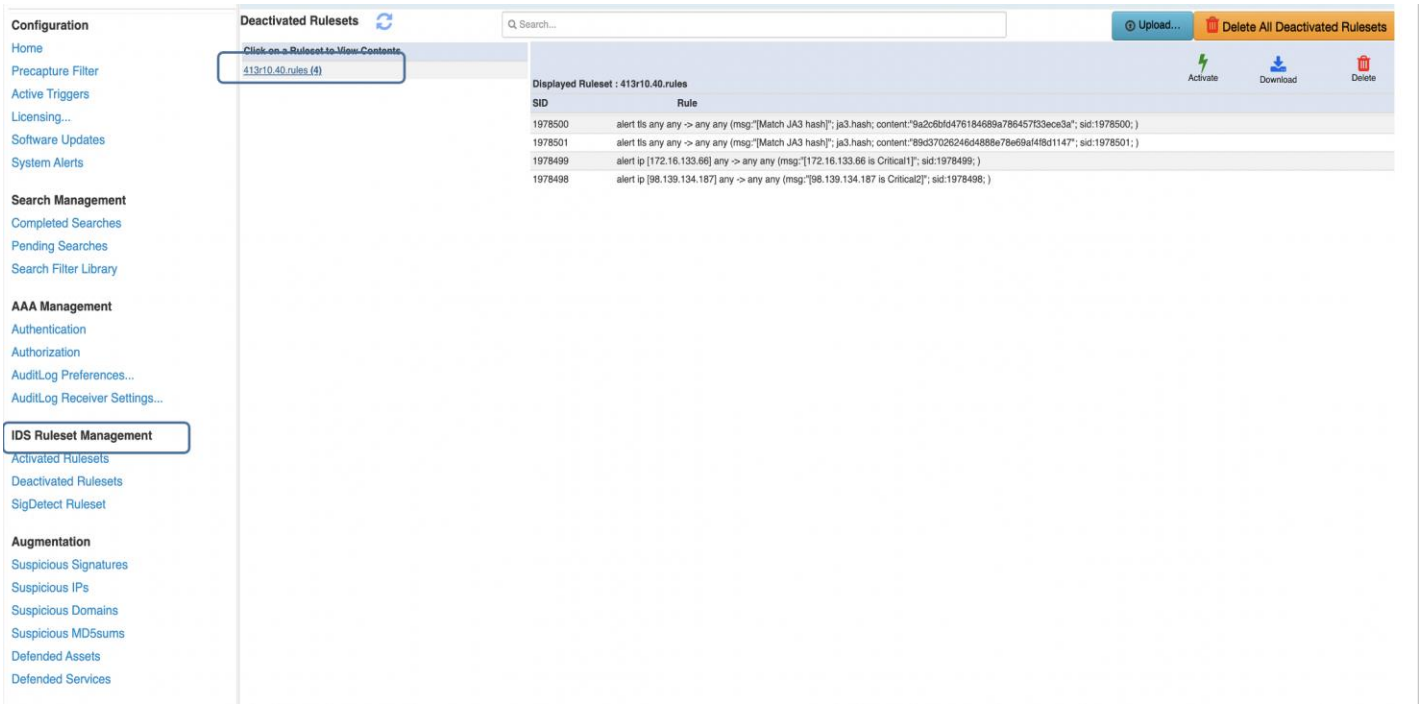
- Click on a activated ruleset to see its contents. The following image shows contents of a ruleset named activebunk2.rules file.
- Select a ruleset and click on Deactivate button. This ruleset will move to Deactivated Rulesets page. Each node removes the new ruleset from Suricata alert generation.
- Select a ruleset and click on Download button to download the selected ruleset.
- Select a ruleset and click on Delete button to delete the ruleset.


Configuration
Home
Precapture Filter
Active Triggers
Licensing...
Software Updates
System Alerts
Search Management
Completed Searches
Pending Searches
Search Filter Library
AAA Management
Authentication
Authorization
AuditLog Preferences...
AuditLog Receiver Settings...
IDS Ruleset Management
Activated Rulesets
Deactivated Rulesets
SigDetect Ruleset
Augmentation
Suspicious Signatures
Suspicious IPs
Suspicious Domains
Suspicious MD5sums
Defended Assets
Defended Services
Activated Rulesets
Search...
Delete All Activated Rulesets
Click on a Ruleset to View Contents
3coresec.rules (20)
activex.rules (732)
adware_pup.rules (2327)
attack_response.rules (299)
botcc.portgrouped.rules (0)
botcc.rules (24)
chat.rules (104)
ciarmy.rules (100)
coinminer.rules (4464)
compromised.rules (93)
current_events.rules (190)
dns.rules (59)
dos.rules (214)
drop.rules (41)
dshield.rules (1)
exploit_kit.rules (1643)
exploit.rules (2449)
ftp.rules (121)
games.rules (86)
hunting.rules (773)
icmp_info.rules (66)
icmp.rules (39)
imap.rules (41)
inappropriate.rules (25)
info.rules (847)
ja3.rules (139)
malware.rules (26853)
misc.rules (63)
mobile_malware.rules (4770)
netbios.rules (732)
p2p.rules (122)
phishing.rules (9830)
policy.rules (2024)
pop3.rules (26)
rpc.rules (126)
Displayed Ruleset : activex.rules
Deactivate
Download
Delete
SID
Rule
2010658
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX EasyMail Object IMAP4 Component Buffer Overflow Function call Attempt"; flow:from_server,established; content:"ActiveXObject"; nocase; content:"EasyMail.IMAP4.6"; distance:0; nocase; content:"LicenseKey"; nocase; reference:url,secunia.com/advisories/24199/; reference:url,doc.emergingthreats.net/2010658; classtype:web-application-attack; sid:2010658; rev:2; metadata:created_at 2010_07_30, updated_at 2010_07_30;)
2011207
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX SaschArt SasCam Webcam Server ActiveX Control Head Method Buffer Overflow Attempt"; flow:to_client,established; content:"<OBJECT "; nocase; content:"classid"; nocase; distance:0; content:"CLSID"; nocase; distance:0; content:"0297D24A-F425-47EE-9F3B-A459BCE593E3"; nocase; distance:0; content:"Head"; nocase; reference:url,exploit-db.com/exploits/14215/; reference:bugtraq,41343; reference:url,doc.emergingthreats.net/2011207; classtype:web-application-attack; sid:2011207; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag ActiveX, updated_at 2016_07_01;)
2010943
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX SoftCab Sound Converter ActiveX SaveFormat File overwrite Attempt"; flow:established,to_client; content:"66757BFC-DA0C-41E6-B3FE-B6D461223FF5"; nocase; content:"SaveFormat"; nocase; pcre:"/<OBJECT\s+[^>]*classid\s*=\s*[\x22\x27]?\s*clsid\s*\x3a\s*\x7B?\s*66757BFC-DA0C-41E6-B3FE-B6D461223FF5/si"; reference:url,secunia.com/advisories/37967/; reference:url,doc.emergingthreats.net/2010943; classtype:web-application-attack; sid:2010943; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag ActiveX, updated_at 2016_07_01;)
2008791
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Visagesoft eXPert PDF Viewer ActiveX Control Arbitrary File Overwrite"; flow:to_client,established; content:"CLSID"; nocase; content:"BDF3E9D2-5F7A-4F4A-A914-7498C862EA6A"; nocase; distance:0; content:"savePageAsBitmap"; nocase; reference:bugtraq,31984; reference:url,milw0rm.com/exploits/6875; reference:url,doc.emergingthreats.net/2008791; classtype:web-application-attack; sid:2008791; rev:3; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag ActiveX, updated_at 2016_07_01;)
2010944
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Viscom Movie Player Pro SDK ActiveX DrawText method Buffer Overflow Function Call"; flow:to_client,established; content:"ActiveXObject"; nocase; content:"MOVIEPLAYER.MoviePlayerCtrl.1"; nocase; distance:0; content:"DrawText"; nocase; reference:url,www.shinnai.net/exploits/X6hU4E0E7P5H3qH5yXrn.txt; reference:url,secunia.com/advisories/38156/; reference:url,doc.emergingthreats.net/2010944; classtype:attempted-user; sid:2010944; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag ActiveX, updated_at 2016_07_01;)
2009620
alert http $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Vulnerable Microsoft Video ActiveX CLSID access (7)"; flow:to_client,established; content:"clsid"; nocase; content:"1BE49F30-0E1B-11D3-9D8E-00C04F72D980"; nocase; distance:0; pcre:"/<OBJECT\s+[^>]*classid\s*=\s*[\x22\x27]?\s*clsid\s*\x3a\s*\x7B?\s*1BE49F30-0E1B-11D3-9D8E-00C04F72D980/si"; reference:url,microsoft.com/technet/security/advisory/972890.mspx; reference:url,doc.emergingthreats.net/2009620; classtype:web-application-attack; sid:2009620; rev:3; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag ActiveX, updated_at 2016_07_01;)
2009621
alert http $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Vulnerable Microsoft Video ActiveX CLSID access (8)"; flow:to_client,established; content:"clsid"; nocase; content:"1C15D484-911D-11D2-B632-00C04F79498E"; nocase; distance:0; pcre:"/<OBJECT\s+[^>]*classid\s*=\s*[\x22\x27]?\s*clsid\s*\x3a\s*\x7B?\s*1C15D484-911D-11D2-B632-00C04F79498E/si"; reference:url,microsoft.com/technet/security/advisory/972890.mspx; reference:url,doc.emergingthreats.net/2009621; classtype:web-application-attack; sid:2009621; rev:3; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag ActiveX, updated_at 2016_07_01;)
2009622
alert http $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Vulnerable Microsoft Video ActiveX CLSID access (9)"; flow:to_client,established; content:"clsid"; nocase; content:"1DF7D126-4050-47F0-A7CF-4C4CA9241333"; nocase; distance:0; pcre:"/<OBJECT\s+[^>]*classid\s*=\s*[\x22\x27]?\s*clsid\s*\x3a\s*\x7B?\s*1DF7D126-4050-47F0-A7CF-4C4CA9241333/si"; reference:url,microsoft.com/technet/security/advisory/972890.mspx; reference:url,doc.emergingthreats.net/2009622; classtype:web-application-attack; sid:2009622; rev:3; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2010_07_30, deployment Perimeter, signature_severity Major, tag ActiveX, updated_at 2016_07_01;)
2009623
alert http $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Vulnerable Microsoft Video ActiveX CLSID access (10)"; flow:to_client,established; content:"clsid"; nocase; content:"2C63E4EB-4CEA-41B8-919C-E947EA19A77C"; nocase; distance:0; pcre:"/<OBJECT\s+[^>]*classid\s*=\s*[\x22\x27]?\s*clsid\s*\x3a\s*\x7B?\s*2C63E4EB-4CEA-41B8-

3.4.2 Deactivated Rulesets

This page allows authorized users to upload new IDS rulesets. The following image shows one such uploaded rulesets.

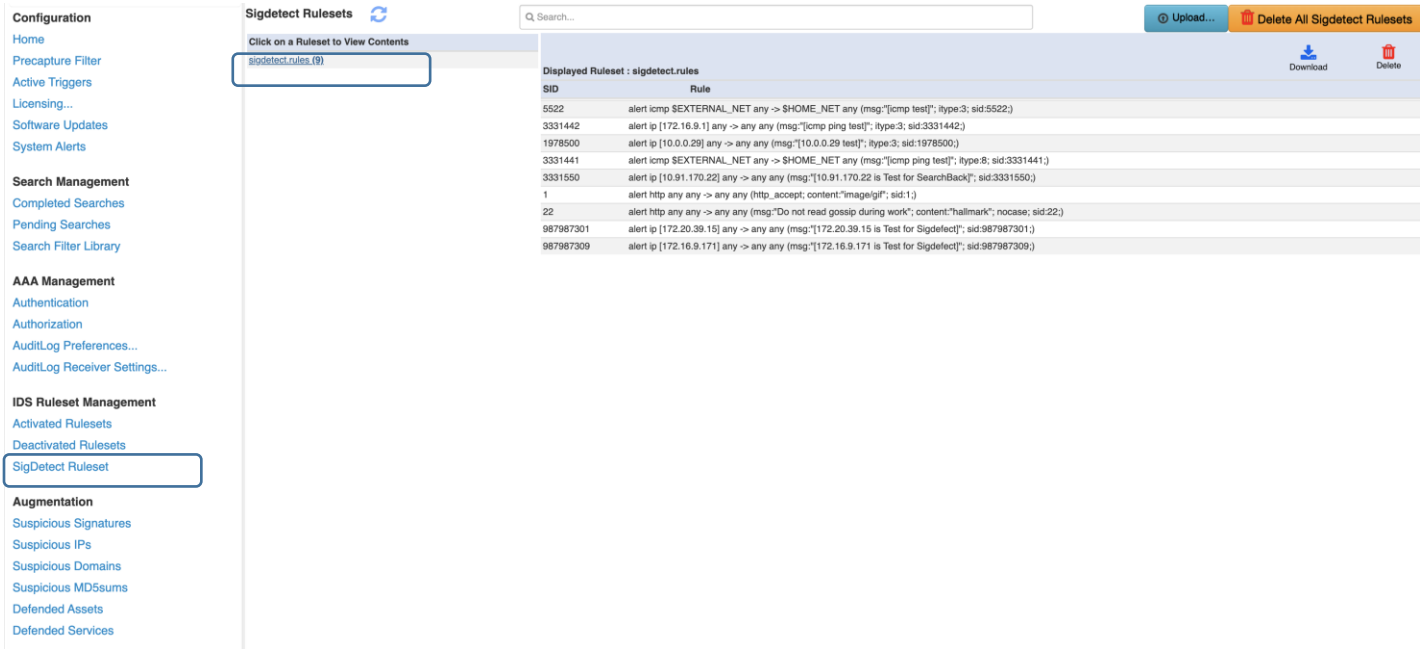
- Click on a deactivated ruleset to see its contents. The following image shows contents of a ruleset named 413.10.40.rules
- Select a ruleset and click on Activate button. This ruleset will move to Activated Rulesets page. Each node adds the new ruleset for Suricata alert generation.
- Select a ruleset and click on Download button to download the selected ruleset.
- Select a ruleset and click on Delete button to delete the ruleset.



3.4.3 SigDetect Ruleset

SigDetect Rulesets are used to generate alerts on pcap data of search. Once a search is complete, the server makes the all the uploaded SigDetect rules at the time of the search completion to Suricata for alert generation. This allows checking for alerts for signatures that were not available when the traffic was originally captured.

- Click on a SigDetect ruleset to see its contents. The following image shows contents of a ruleset named sigdetect.rules
- Select a ruleset and click on Download button to download the selected ruleset.
- Select a ruleset and click on Delete button to delete the ruleset. These rules will not be part of any future searches.



Once a search is completed, any Suricata alerts found for the search's pcap data are stored in sigdetect.json file.

3.5 AUGMENTATION

Augmentation allows users to upload additional data that can be used to enhance the value of stored data and allow data correlation. Augmentation has 6 menu items. The workflow and the interaction of each of the options in this section are like one another.

- Suspicious Signatures
- Suspicious Ips
- Suspicious Domains
- Suspicious MD5sums
- Defended Assets
- Defended Services

Only those users that have a role with Policy permission can upload augmentation data. Any authorized user can download augmentation data.

Authorized users can upload () a csv file for each of the augmentation types mentioned above. Each line contains a valid entry of the item being uploaded, a comma, and an optional description of this line's item. An example csv file for Suspicious IP Addresses is shown below:

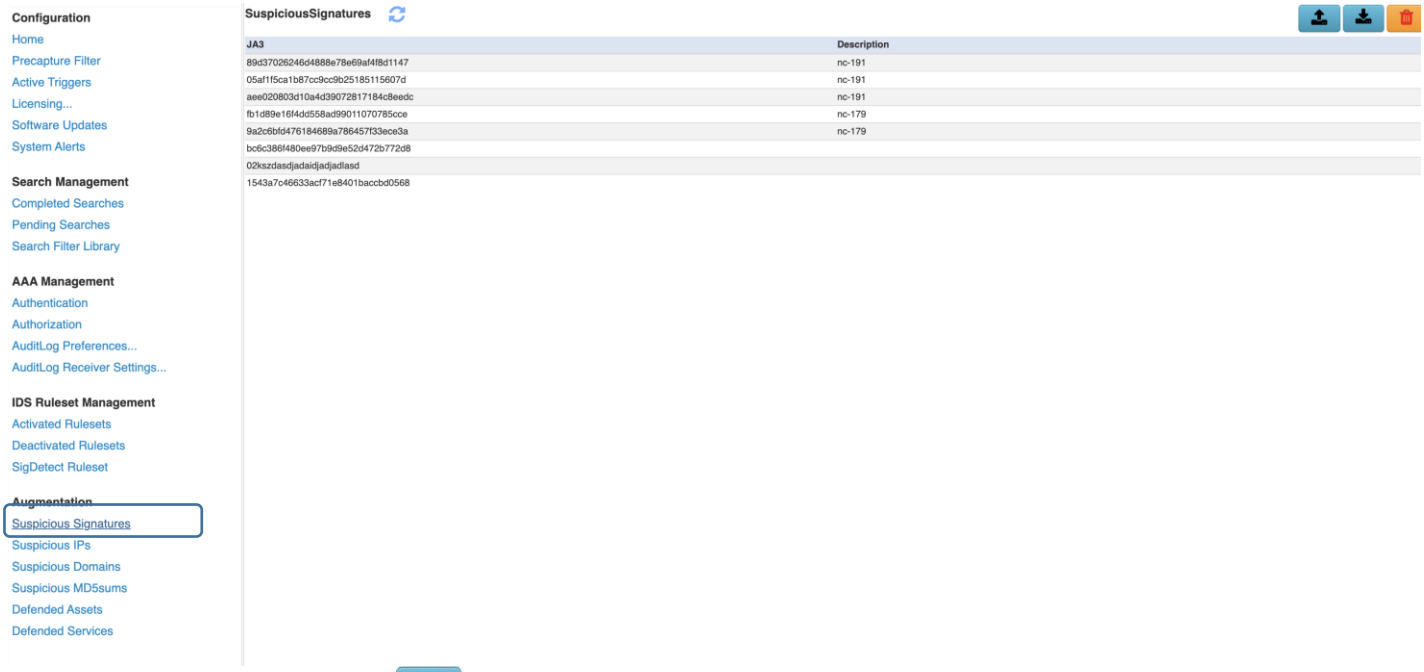
110.22.34.24,suspip3424
10.1.8.0/24,cidr test

When an event's source/destination IP Address either matches a suspicious IP Address or part of a suspicious CIDR block, the event's ioc field is augmented with the custom data uploaded. For example, the following image shows the augmented ioc value on matching an IP Address from 10.1.8.0/24 CIDR Block:

Time	src_ip	dest_ip	suspected	nodename	ioc
Nov 14, 2021 @ 11:29:59.303282000	10.1.8.151	10.1.8.160	true	sw176	cidr test,10.1.8.151
Nov 14, 2021 @ 11:29:59.303274000	10.1.8.151	10.1.8.160	true	sw176	cidr test,10.1.8.151
Nov 14, 2021 @ 11:29:59.293695000	10.1.8.151	10.1.8.160	true	sw176	cidr test,10.1.8.151
Nov 14, 2021 @ 11:29:59.293672000	10.1.8.151	10.1.8.160	true	sw176	cidr test,10.1.8.151
Nov 14, 2021 @ 11:29:59.038037000	10.1.8.151	10.1.8.160	true	sw176	cidr test,10.1.8.151
Nov 14, 2021 @ 11:29:59.038025000	10.1.8.151	10.1.8.160	true	sw176	cidr test,10.1.8.151
Nov 14, 2021 @ 11:29:58.636885000	10.1.8.151	10.1.8.160	true	sw176	cidr test,10.1.8.151
Nov 14, 2021 @ 11:29:58.636874000	10.1.8.151	10.1.8.160	true	sw176	cidr test,10.1.8.151
Nov 14, 2021 @ 11:29:58.636579000	10.1.8.151	10.1.8.160	true	sw176	cidr test,10.1.8.151
Nov 14, 2021 @ 11:29:58.636568000	10.1.8.151	10.1.8.160	true	sw176	cidr test,10.1.8.151

3.5.1 Suspicious Signatures

This shows the list of currently uploaded suspicious JA3 signatures. When a TLS event matches one of these signatures, that event is marked as **suspected**.



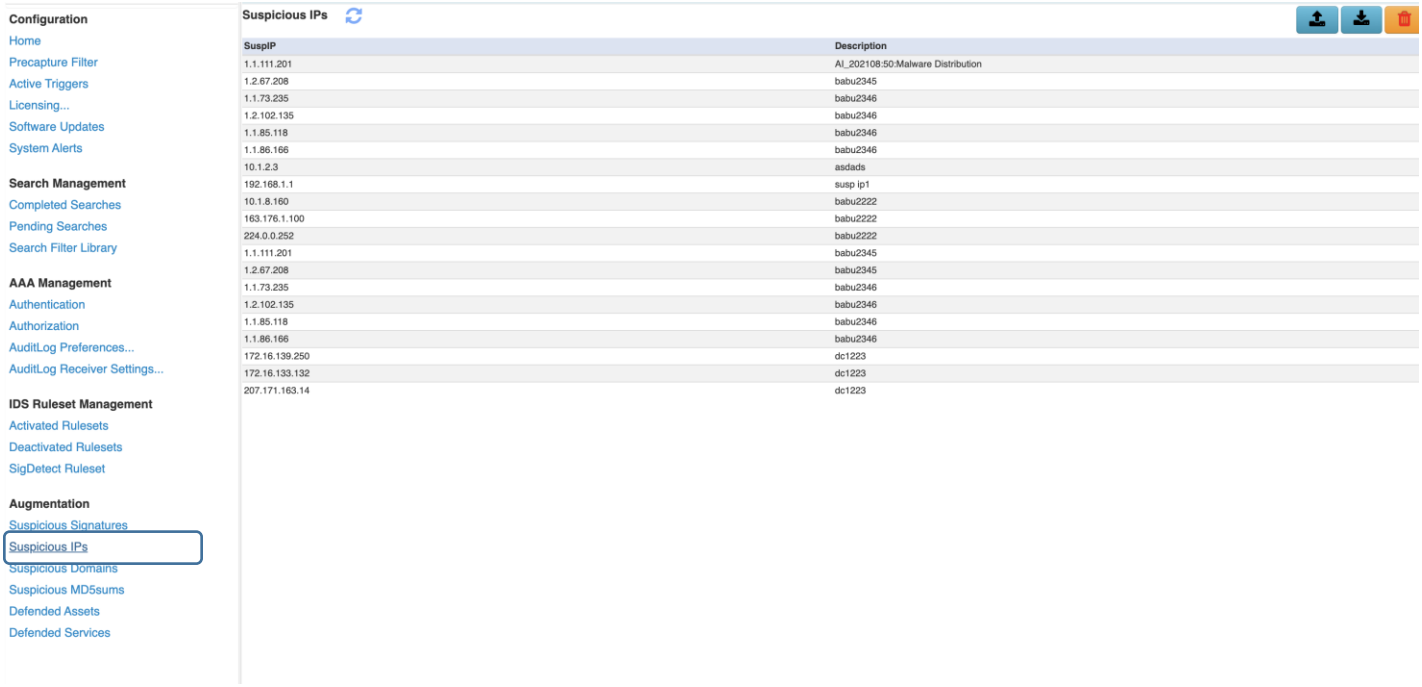
Authorized users can upload ( ) new suspected signatures as a csv file with each line containing a ja3 signature, a comma, and an optional description of the signature. Each line of the csv file must have a JA3. Description of the JA3 is optional. If Description is provided, JA3 and Description values must be separated by comma. A sample csv file is shown below:

```
4192c0a946c5bd9b544b4656d9f624a4,db4
Acb741bcdffb787c5a52654c78645bdf
e1691a31bfe345d2692da75636ddfb00,deedeefbzero
```

Currently available signatures can be downloaded ( ) by any authorized user.

3.5.2 Suspicious IPs

These are class of IP addresses that are considered as unsafe and unreliable within a network traffic. When an IDS alert's source ip or dest ip matches one of the uploaded IP addresses, the alert is marked as **suspected**.



Authorized users can upload () new suspected IP Address as a csv file with each line containing an ip address, a comma, and an optional description of the ip address. Each line of the csv file must have a valid ip address. Description is optional. If Description is provided, IP Address and Description values must be separated by a comma. A sample csv file is shown below:

```
46.29.161.246, description1
149.154.159.226
46.29.161.249,twofournine
```

The uploaded file can include CIDR block too.
10.1.8.0/24, cidr test

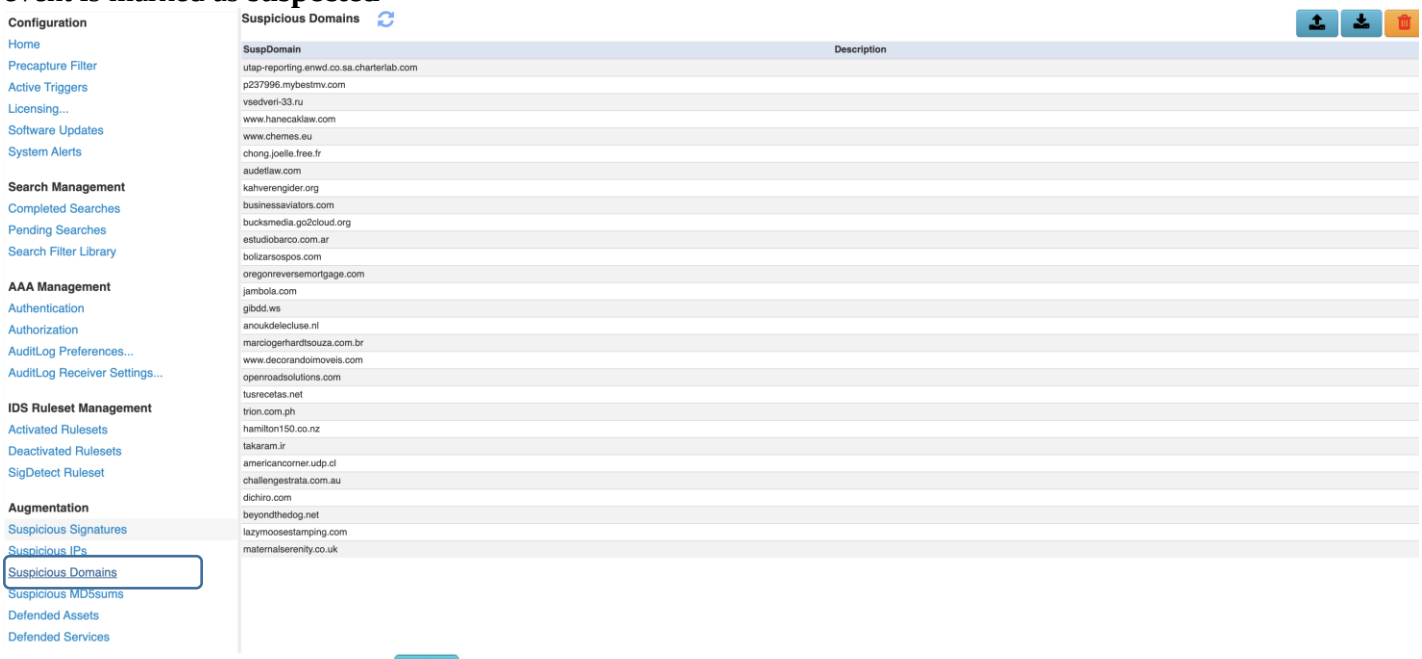
Currently available suspicious IP Addresses can be downloaded () by any authorized user.

When an event's source/destination IP Address either matches a suspicious IP Address or part of a suspicious CIDR block, the event's ioc field is augmented with the custom data uploaded. For example, the following image shows the augmented ioc value on matching an IP Address from 10.1.8.0/24 CIDR Block:

Time	src_ip	dest_ip	suspected	nodename	ioc
Nov 14, 2021 @ 11:29:59.303282000	10.1.8.151	10.1.8.160	true	sw176	cidr test,10.1.8.151
Nov 14, 2021 @ 11:29:59.303274000	10.1.8.151	10.1.8.160	true	sw176	cidr test,10.1.8.151
Nov 14, 2021 @ 11:29:59.293695000	10.1.8.151	10.1.8.160	true	sw176	cidr test,10.1.8.151
Nov 14, 2021 @ 11:29:59.293672000	10.1.8.151	10.1.8.160	true	sw176	cidr test,10.1.8.151
Nov 14, 2021 @ 11:29:59.038037000	10.1.8.151	10.1.8.160	true	sw176	cidr test,10.1.8.151
Nov 14, 2021 @ 11:29:59.038025000	10.1.8.151	10.1.8.160	true	sw176	cidr test,10.1.8.151
Nov 14, 2021 @ 11:29:58.636885000	10.1.8.151	10.1.8.160	true	sw176	cidr test,10.1.8.151
Nov 14, 2021 @ 11:29:58.636874000	10.1.8.151	10.1.8.160	true	sw176	cidr test,10.1.8.151
Nov 14, 2021 @ 11:29:58.636579000	10.1.8.151	10.1.8.160	true	sw176	cidr test,10.1.8.151
Nov 14, 2021 @ 11:29:58.636568000	10.1.8.151	10.1.8.160	true	sw176	cidr test,10.1.8.151

3.5.3 Suspicious Domains

Domain names are an important avenue to investigate security incidents or to prevent some malicious activity to occur on your network. When a DNS event's domain name matches one of the uploaded domains, the DNS event is marked as **suspected**



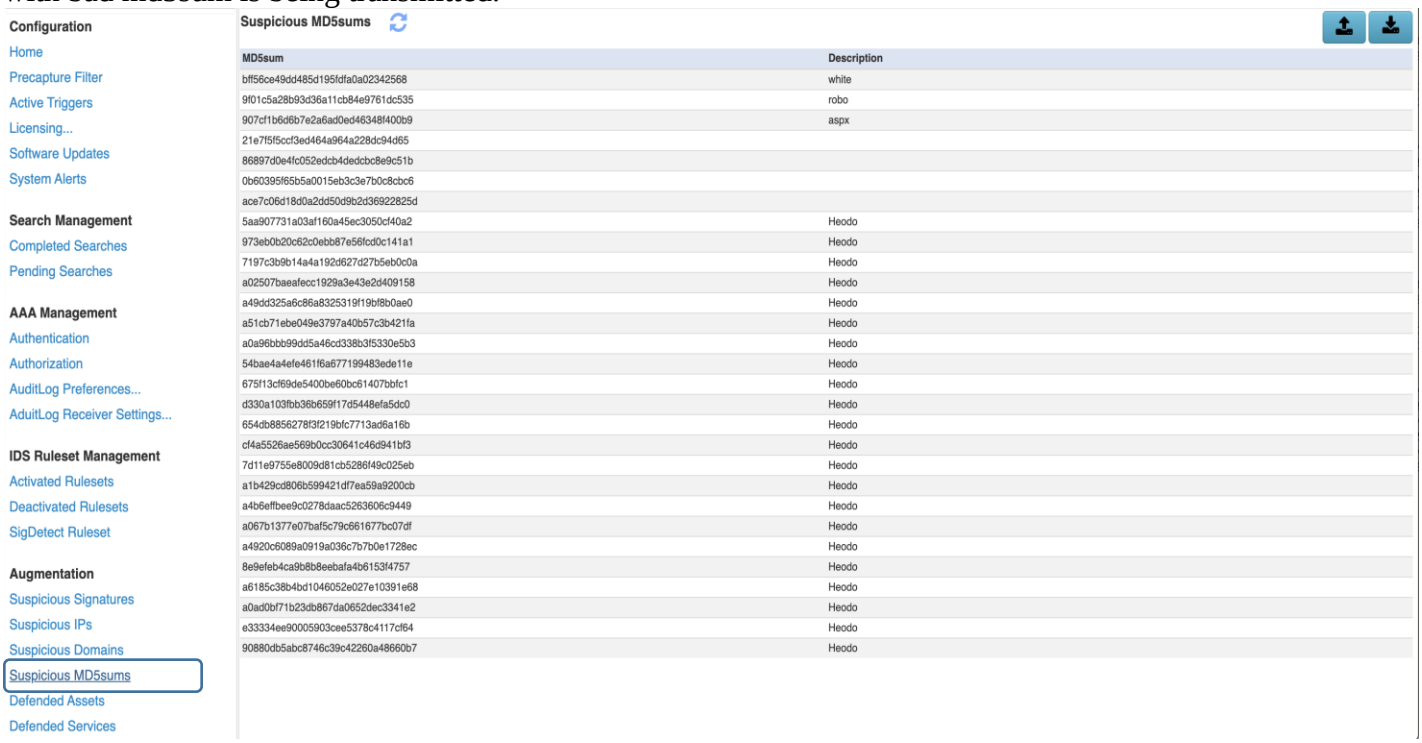
Authorized users can upload () new suspected domain names as a csv file with each line containing a domain name, a comma, and an optional description of the domain. Each line of the csv file must have a valid domain name. Description is optional. If Description is provided, IP Address and Description values must be separated by a comma. A sample csv file is shown below:

```
p237996.mybestmv.com
vsedveri-33.ru
www.hanecaklaw.com
www.chemes.eu
chong.joelle.free.fr
audetlaw.com
kahverengider.org
```

Currently available suspicious domain names can be downloaded () by any authorized user

3.5.4 Suspicious MD5sums

This page allows users to upload known bad md5sums for allowing the software to identify/alert when a file with bad md5sum is being transmitted.



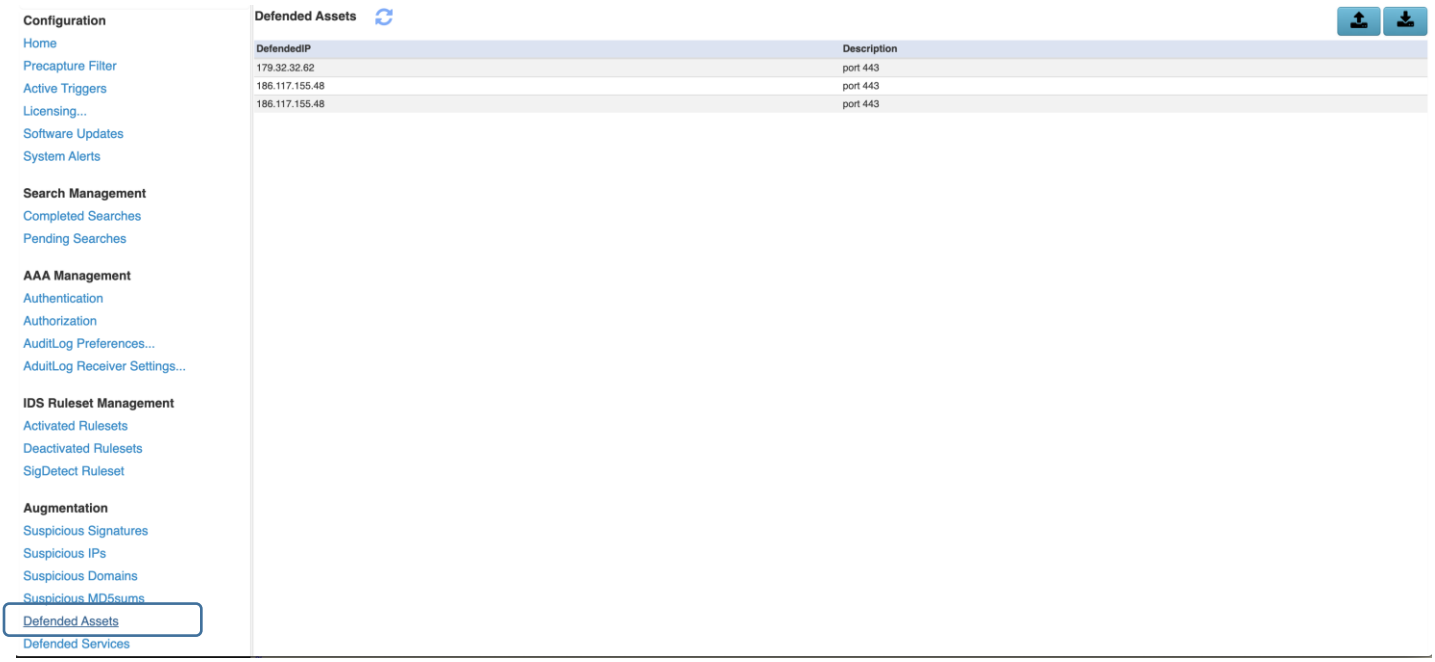
Authorized users can upload () new suspected md5sums as a csv file with each line containing a md5sum, a comma, and an optional description. Each line of the csv file must have a valid md5sum. Description is optional. If Description is provided, md5sum and Description values must be separated by a comma. A sample csv file is shown below:

```
bff56ce49dd485d195fdfa0a02342568,white
9f01c5a28b93d36a11cb84e9761dc535,robo
907cf1b6d6b7e2a6ad0ed46348f400b9,aspx
21e7f5f5ccf3ed464a964a228dc94d65,
```

Currently available md5sums can be downloaded () by any authorized user.

3.5.5 Defended Assets

Defended Asset lists are IP addresses of the systems that are approved, recognized and considered to be safe and may even be critical to the organization. If an alert's source ip or dest ip matches an ip address of a defended asset, this alert is marked as **defended**. It is quite possible for an alert to be marked both **defended** and **suspected**.



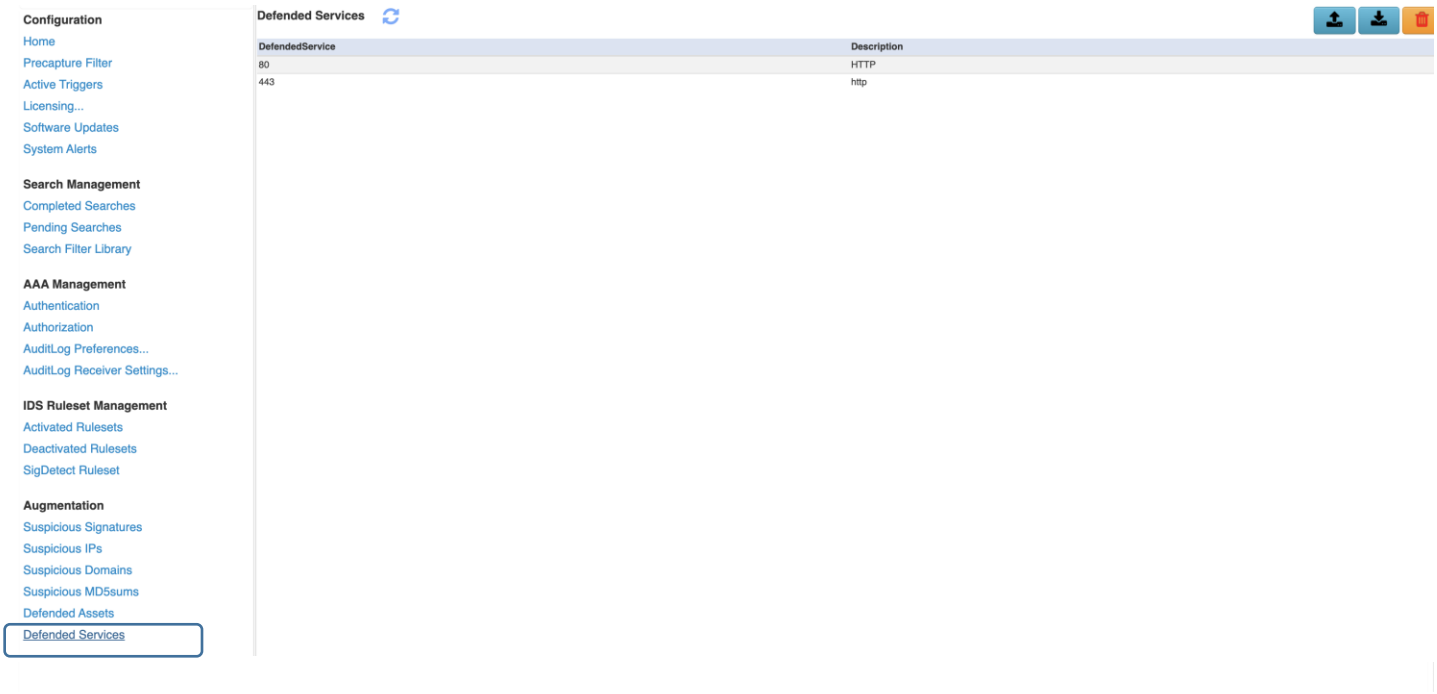
Authorized users can upload () new defended asset list as a csv file with each line containing an ip address of a defended asset, a comma, and an optional description. Each line of the csv file must have a valid ip address. Description is optional. If Description is provided, defended asset and Description values must be separated by a comma. A sample csv file is shown below:

```
176.32.32.62,system62
185.117.155.48,payroll
176.32.33.203
```

Currently available defended assets can be downloaded () by any authorized user.

3.5.6 Defended Services

Defended Service lists are port numbers of the applications that are approved, recognized and considered to be safe and may even be critical to the organization. If an alert's source port or dest port matches a port of a defended service, this alert is marked as **defended**. It is quite possible for an alert to be marked both **defended** and **suspected**.



Authorized users can upload () new defended service list as a csv file with each line containing port address of a defended service, a comma, and an optional description. Each line of the csv file must have a valid port number. Description is optional. If Description is provided, defended service and Description values must be separated by a comma. A sample csv file is shown below:

```
443,missioncritical
3306,essential
```

Currently available defended services can be downloaded () by any authorized user.

APPENDIX A – BPF FILTER

Berkeley Packet Filter (BPFs) are a raw interface to data link layers in a protocol independent fashion. They are a powerful tool for intrusion detection analysis. Using them will allow the user to quickly drill down specific packets to see and reduce large packet captures down to the essentials.

The BPF syntax consists of one or more primitives. Primitives usually consist of an *id(*name or number) preceded by one or more qualifiers. There are three different kinds of qualifier:

type
qualifiers say what kind of thing the id name or number refers to. E.g., **host**, **net**, **port**, **portrange.** If there is no qualifier**, host** is assumed.

dir
qualifiers specify a particular transfer direction to and/or from *id.* Possible directions are src,dst,src or dst. E.g., dst net 128.3

proto
qualifiers restrict the match to the particular protocol. Possible protocols are: **ether**, **fddi**, **tr**, **wlan**, **ip**, **ip6**, **arp**, **rarp**, **decnet**, **tcp** and **udp.**

1.1 Primitive Filters

Allowable primitives are given below for reference:

Primitive Filters	Description
[src|dst] host <host> E.g., src host <*host*> dst host <*host*> host <*host*> ip host <*host*>	Matches a host as the IP source, destination, or either. • These host expressions can be used in conjunction with other protocols like ip, arp, rarp or ip6
ether [src|dst] host <ehost> E.g., ether host <MAC> ether src host <MAC> ether dst host <MAC>	Matches a host as the Ethernet source, destination, or either

[src|dst] net <network> E.g., dst net 192.168.1.0 src net 192.168.1 dst net 172.16 src net 10 net 192.168.1.0 net 192.168.1.0/24 src net 192.168.1/24	Matches packets to or from source/destination or either, residing in a network. An IPv4 network number can be specified as: • Dotted quad (e.g., 192.168.1.0) • Dotted triple (e.g., 192.168.1) • Dotted pair (e.g., 172.16) • Or single number (e.g., 10)
[src|dst] net <network> mask <netmask> **or** [src|dst] net <network>/<len> E.g., dst net 192.168.1.0 mas 255.255.255.255 **or** dst net 192.168.1.0/24 src net 192.168.1 mask 255.255.255.0 **or** src net 192.168.1/24 dst net 172.16 mask 255.255.0.0 src net 10 mask 255.0.0.0	Matches packets with specific netmask. /len can also be specified to capture traffic from range of IP addresses. • Netmask for dotted quad (e.g., 192.168.1.0) is 255.255.255.255 • Netmask for dotted triple (e.g., 192.168.1) is 255.255.255.0 • Netmask for dotted pair (e.g.,172.16) is 255.255.0.0 • Or single number (e.g.,10) is 255.0.0.0
[src|dst] port <port> **or** [tcp|udp] [src|dst] port <port> E.g., src port 443 dst port 20 port 80	Matches packets sent to/from port • Protocols (e.g., tcp/udp/ip etc.) can be applied to a port to get specific results
[src|dst] portrange <p1>-<p2> **or** [tcp|udp] [src|dst] portrange <p1>-<p2> E.g., src portrange 80-88 tcp portrange 1501-1549	Matches packets to/from a port in the given range • Protocols can be applied to port range to filter specific packets within the range
less <length> E.g., less 300 (or len <300)	Matches packets less than or equal to length
greater <length> E.g., greater 301(or len >300)	Matches packets greater than or equal to length
(ether|ip|ip6) proto <protocol>	Matches an Ethernet, IPv4, or IPv6 protocol

E.g., ether proto 0x888e ip proto 50	• Protocol can be a number or name. (Except for named protocols that bpf is aware of such as icmp, tcp, udp, dns, etc)
(ip|ip6) protochain <protocol> E.g., ip6 protochain 6	Matches IPv4, or IPv6 packets with a protocol header in the protocol header chain
(ether|ip) broadcast	Matches Ethernet or IPv4 broadcasts
(ether|ip|ip6) multicast E.g., ether[0] & 1 != 0	Matches Ethernet, IPv4, or IPv6 multicasts
vlan [<vlan>] ○ E.g., vlan 100 && vlan 200 (filters on vlan 200 encapsulated within vlan 100) ○ vlan && vlan 300 && ip (filters IPv4 protocols encapsulated in vlan 300 encapsulated within any higher order vlan)	Matches 802.1Q frames optionally with a VLAN ID of vlan
mpls [<label>] ○ E.g., mpls 100000 && mpls 1024 (filters packets with outer label 100000 and inner Label 1024) ○ mpls && mpls 1024 && host 192.9.200.1(filters packets to and from 192.9.200.1 with an inner label of 1024 and any outer label)	Matches MPLS packets, optionally with a label of label • mpls expression may be used more than once, to filter on MPLS hierarchies.

1.2 Protocols

- Various protocols can be combined with primitive BPF filters using modifiers and operators. Types of valid Protocols are given below:

arp	ip6	udp	fddi	link	slip	rarp
ether	ip	wlan	icmp	tcp	radio	ppp

1.3 Modifiers

Types of valid modifiers/operators:

Parentheses	( )
Negation	!=
Concatenation	'&&' or 'and'
Alteration	'||' or 'or'

1.4 Examples of some filters using operators and modifiers:

udp dst port not 53	UDP not bound for port 53
host 10.0.0.1 && host 10.0.0.2	Traffic between these hosts
Tcp dst port 80 or 8080	Packets to either tcp ports
ether[0:4] & 0xffffff0f > 25	Range based mask applied to bytes greater than 25
ip[1] != 0	Captures packets for which Types of Service(TOS) field in the ip header is not equal to 0
ether host 11:22:33:44:55:66	Matches a specific host with that Mac address
ether[0] & 1 = 0 and ip[16] >= 224	Captures ip broadcast or multicast broadcast that were not sent via Ethernet broadcast/multicast
icmp[icmptype] != icmp-echo	Captures all icmp packets that are not echo requests
ip[0] & 0xf !=5	Catches all IP packets with options
ip[6:2] & 0x1fff = 0	Catches only unfragmented IPv4 datagrams and frag zero of fragmented ipv4 datagrams
tcp[13] & 16 != 0	Captures tcp-ack packets
tcp[13] & 32 !=0	Captures tcp-urg packets
tcp[13] & 8!=0	Captures tcp-psh packets
tcp[13] & 4!=0	Captures tcp-rst packets
tcp[13] & 2!=0	Captures tcp-syn packets
tcp[13] & 1!=0	Captures tcp-fin packets
tcp[tcpflags] & (tcp-syn|tcp-fin) != 0	Captures start and end packets (the SYN and FIN packets) of each TCP conversation

not host 1.2.3.4	any ip not matching 1.2.3.4
not host 1.2.3.4.and not host 2.3.4.5	Any ip not equal to 1.2.3.4 and not equal to 2.3.4.5
vlan and not host 1.2.3.4 and not host 2.3.4.5	Same as above with 1 vlan id

APPENDIX B - EXTENDING BPF SEARCH FILTERS

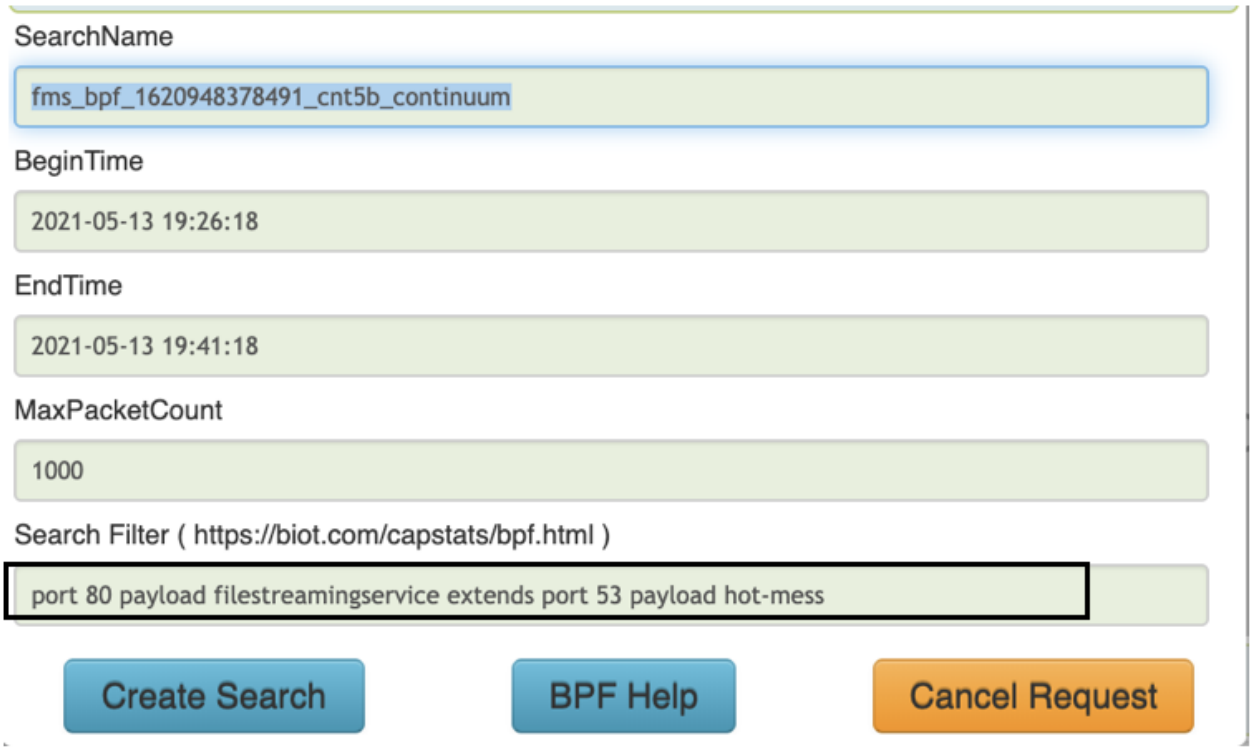
Multiple BPF search filters can be combined with the word **extends.** This feature allows each bpf filter to be independent of other filters in the same search. This is primarily useful when each filter has its own payload or some filters have payload and some do not.

Without extends, the user will be required to create multiple searches, merge the resulting pcaps - a multi-step process that is slow and inconvenient. Some examples shown below:

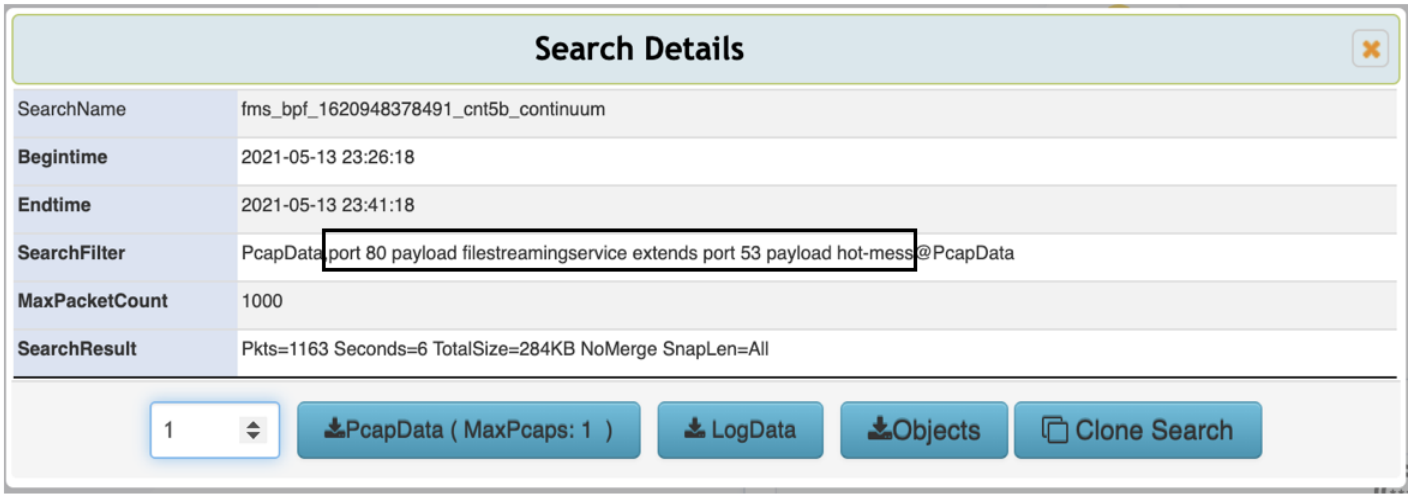
1. To get packets with destination or host ip 1.2.3.4 and payload HTTP or packets with port number 53
   host 1.2.3.4 payload HTTP extends port 53

2. To get packets with source or destination port 80 and packets with port 53 with payload microsoft.com
   port 80 extends port 53 payload microsoft.com

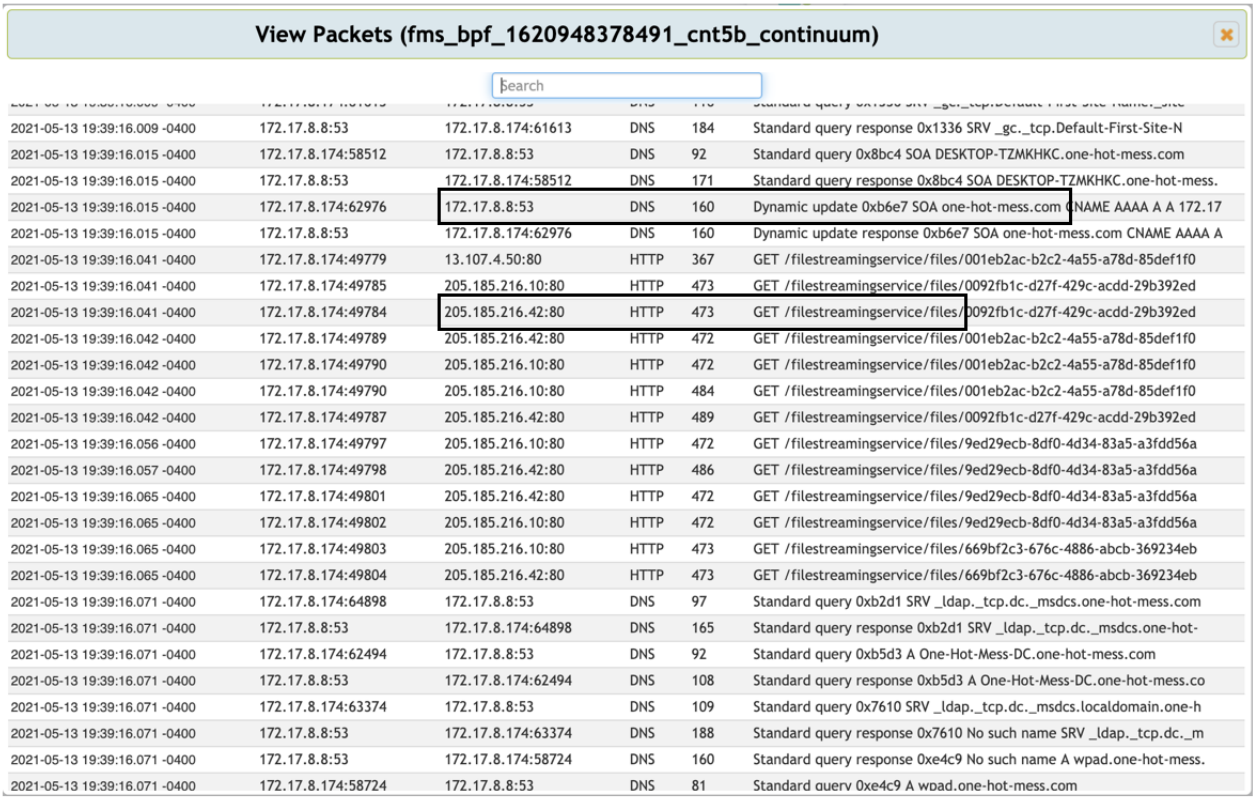
Step 1) User creates a compound search with zero or more extends



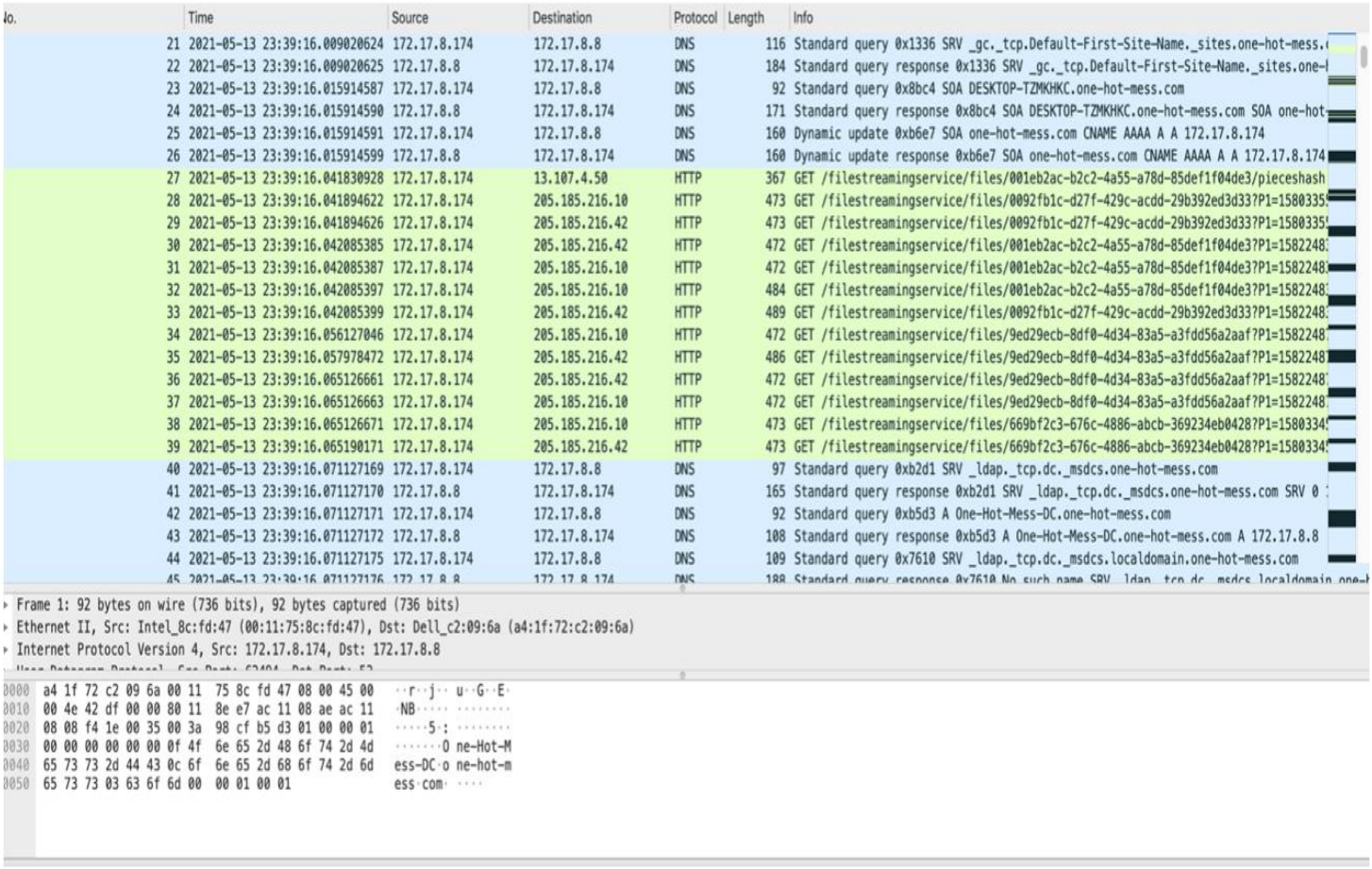
Step 2) Packets for both bpf strings are saved into the search pcap.



Step 3) These packets can be viewed without downloading to the local system. Each packet with only the matching payload and port is retrieved to be part of the resulting pcap.



Step 4) The pcap can be downloaded and viewed with any application that reads pcap files (eg., Wireshark, Tshark)



No.	Time	Source	Destination	Protocol	Length	Info
21	2021-05-13 23:39:16.009020624	172.17.8.174	172.17.8.8	DNS	116	Standard query 0x1336 SRV _gc._tcp.Default-First-Site-Name._sites.one-hot-mess.
22	2021-05-13 23:39:16.009020625	172.17.8.8	172.17.8.174	DNS	184	Standard query response 0x1336 SRV _gc._tcp.Default-First-Site-Name._sites.one-h
23	2021-05-13 23:39:16.015914587	172.17.8.174	172.17.8.8	DNS	92	Standard query 0x8bc4 SOA DESKTOP-TZMKHKC.one-hot-mess.com
24	2021-05-13 23:39:16.015914590	172.17.8.8	172.17.8.174	DNS	171	Standard query response 0x8bc4 SOA DESKTOP-TZMKHKC.one-hot-mess.com SOA one-hot-
25	2021-05-13 23:39:16.015914591	172.17.8.174	172.17.8.8	DNS	160	Dynamic update 0xb6e7 SOA one-hot-mess.com CNAME AAAA A A 172.17.8.174
26	2021-05-13 23:39:16.015914599	172.17.8.8	172.17.8.174	DNS	160	Dynamic update response 0xb6e7 SOA one-hot-mess.com CNAME AAAA A A 172.17.8.174
27	2021-05-13 23:39:16.041830928	172.17.8.174	13.107.4.50	HTTP	367	GET /filestreamingservice/files/001eb2ac-b2c2-4a55-a78d-85def1f04de3/pieceshash
28	2021-05-13 23:39:16.041894622	172.17.8.174	205.185.216.10	HTTP	473	GET /filestreamingservice/files/0092fb1c-d27f-429c-acdd-29b392ed3d33?P1=1580335
29	2021-05-13 23:39:16.041894626	172.17.8.174	205.185.216.42	HTTP	473	GET /filestreamingservice/files/0092fb1c-d27f-429c-acdd-29b392ed3d33?P1=1580335
30	2021-05-13 23:39:16.042085385	172.17.8.174	205.185.216.42	HTTP	472	GET /filestreamingservice/files/001eb2ac-b2c2-4a55-a78d-85def1f04de3?P1=1582248
31	2021-05-13 23:39:16.042085387	172.17.8.174	205.185.216.10	HTTP	472	GET /filestreamingservice/files/001eb2ac-b2c2-4a55-a78d-85def1f04de3?P1=1582248
32	2021-05-13 23:39:16.042085397	172.17.8.174	205.185.216.10	HTTP	484	GET /filestreamingservice/files/001eb2ac-b2c2-4a55-a78d-85def1f04de3?P1=1582248
33	2021-05-13 23:39:16.042085399	172.17.8.174	205.185.216.42	HTTP	489	GET /filestreamingservice/files/0092fb1c-d27f-429c-acdd-29b392ed3d33?P1=1582248
34	2021-05-13 23:39:16.056127046	172.17.8.174	205.185.216.10	HTTP	472	GET /filestreamingservice/files/9ed29ecb-8df0-4d34-83a5-a3fdd56a2aaf?P1=1582248
35	2021-05-13 23:39:16.057978472	172.17.8.174	205.185.216.42	HTTP	486	GET /filestreamingservice/files/9ed29ecb-8df0-4d34-83a5-a3fdd56a2aaf?P1=1582248
36	2021-05-13 23:39:16.065126661	172.17.8.174	205.185.216.42	HTTP	472	GET /filestreamingservice/files/9ed29ecb-8df0-4d34-83a5-a3fdd56a2aaf?P1=1582248
37	2021-05-13 23:39:16.065126663	172.17.8.174	205.185.216.10	HTTP	472	GET /filestreamingservice/files/9ed29ecb-8df0-4d34-83a5-a3fdd56a2aaf?P1=1582248
38	2021-05-13 23:39:16.065126671	172.17.8.174	205.185.216.10	HTTP	473	GET /filestreamingservice/files/669bf2c3-676c-4886-abcb-369234eb0428?P1=1580334
39	2021-05-13 23:39:16.065190171	172.17.8.174	205.185.216.42	HTTP	473	GET /filestreamingservice/files/669bf2c3-676c-4886-abcb-369234eb0428?P1=1580334
40	2021-05-13 23:39:16.071127169	172.17.8.174	172.17.8.8	DNS	97	Standard query 0xb2d1 SRV _ldap._tcp.dc._msdcs.one-hot-mess.com
41	2021-05-13 23:39:16.071127170	172.17.8.8	172.17.8.174	DNS	165	Standard query response 0xb2d1 SRV _ldap._tcp.dc._msdcs.one-hot-mess.com SRV 0 1
42	2021-05-13 23:39:16.071127171	172.17.8.174	172.17.8.8	DNS	92	Standard query 0xb5d3 A One-Hot-Mess-DC.one-hot-mess.com
43	2021-05-13 23:39:16.071127172	172.17.8.8	172.17.8.174	DNS	108	Standard query response 0xb5d3 A One-Hot-Mess-DC.one-hot-mess.com A 172.17.8.8
44	2021-05-13 23:39:16.071127175	172.17.8.174	172.17.8.8	DNS	109	Standard query 0x7610 SRV _ldap._tcp.dc._msdcs.localdomain.one-hot-mess.com
45	2021-05-13 23:39:16.071127176	172.17.8.8	172.17.8.174	DNS	188	Standard query response 0x7610 No such name SRV _ldap._tcp.dc._msdcs.localdomain.one-h

```
▸ Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)
▸ Ethernet II, Src: Intel_8c:fd:47 (00:11:75:8c:fd:47), Dst: Dell_c2:09:6a (a4:1f:72:c2:09:6a)
▸ Internet Protocol Version 4, Src: 172.17.8.174, Dst: 172.17.8.8
```

```
0000  a4 1f 72 c2 09 6a 00 11  75 8c fd 47 08 00 45 00   ··r··j·· u··G··E·
0010  00 4e 42 df 00 00 80 11  8e e7 ac 11 08 ae ac 11   ·NB····· ········
0020  08 08 f4 1e 00 35 00 3a  98 cf b5 d3 01 00 00 01   ·····5·: ········
0030  00 00 00 00 00 00 0f 4f  6e 65 2d 48 6f 74 2d 4d   ·······O ne-Hot-M
0040  65 73 73 2d 44 43 0c 6f  6e 65 2d 68 6f 74 2d 6d   ess-DC·o ne-hot-m
0050  65 73 73 03 63 6f 6d 00  00 01 00 01              ess·com· ····
```

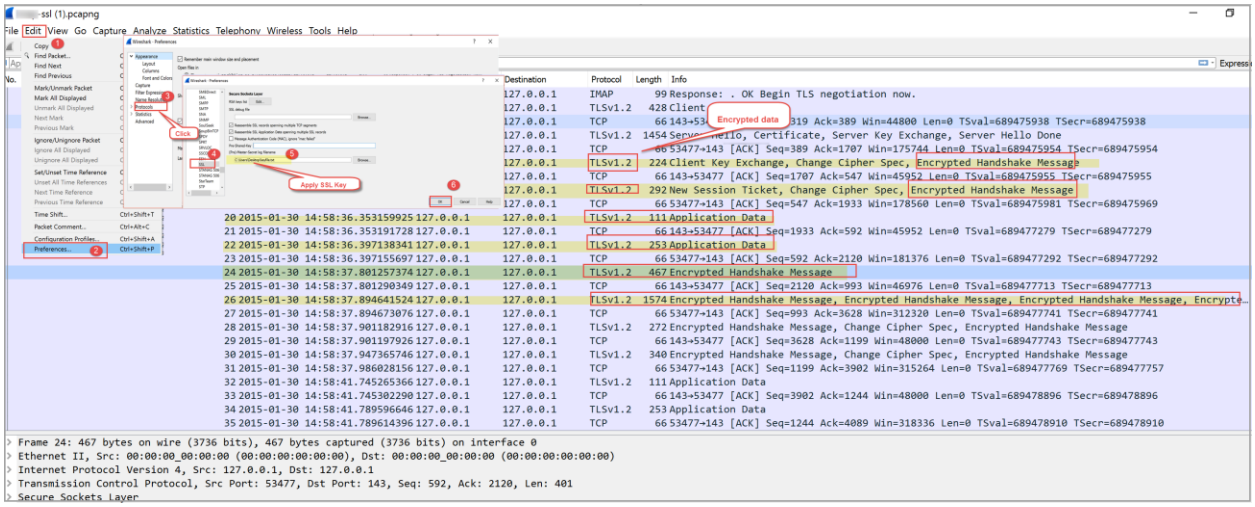
APPENDIX C - DECRYPTING PCAP WITH SSL SESSION KEYS

This workflow presumes the user has:

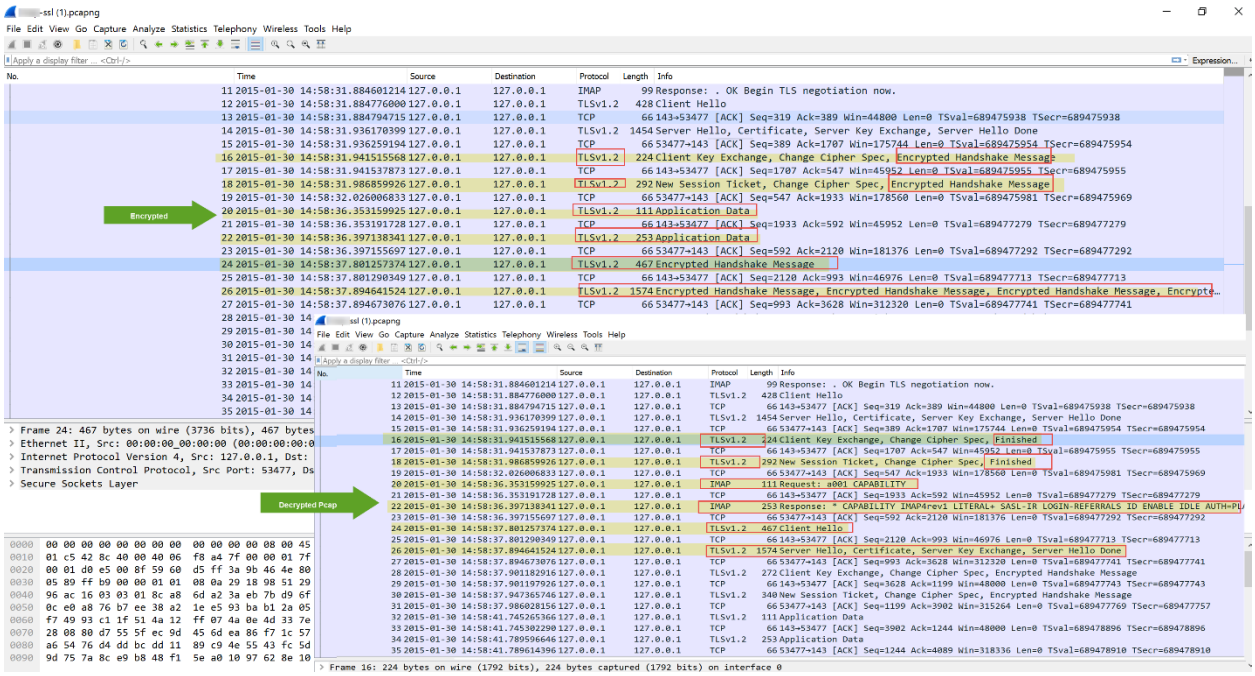
- A set of SSL Session keys for decrypting pcap data
- Downloaded one or more (encrypted) pcaps from a completed pcap search

Workflow

1. Open Wireshark application
2. Load the encrypted pcap file
3. Select **Edit->Preferences…**
4. Select and expand **Protocols**, scroll down and select SSL (or type ssl)



5. Click Browse button under (Pre)-Master-Secret log filename.
6. Select the Session Key filename to be loaded.
7. [Optional] To produce a debug file, click Browse button under SSL debug file and provide a location/filename for a debug file. **Note:** Wireshark will write to this file.
8. Click OK
9. If the Session Key is correct/matching, the loaded pcap file will be decrypted.



Notes

- Wireshark automatically tries to decrypt any other pcaps using the SSL Session Key loaded currently. To remove this file or replace with a new file, repeat the steps 3 through 8.
- Wireshark can only decrypt SSL/TLS packet data if RSA keys are used to encrypt the data.
- Wireshark can only decrypt SSL/TLS packet data if the capture includes the initial SSL/TLS session establishment. Re-used sessions cannot be decrypted; you can identify these as the server will not send a certificate or alternatively, the Wireshark SSL debug file will display a ssl_restore_session can't find stored session error message.
- Duplicate packets may cause issues and prevent all relevant packets being decrypted.

APPENDIX D – SPLUNK UNIVERSAL FORWARDER INSTALLATION

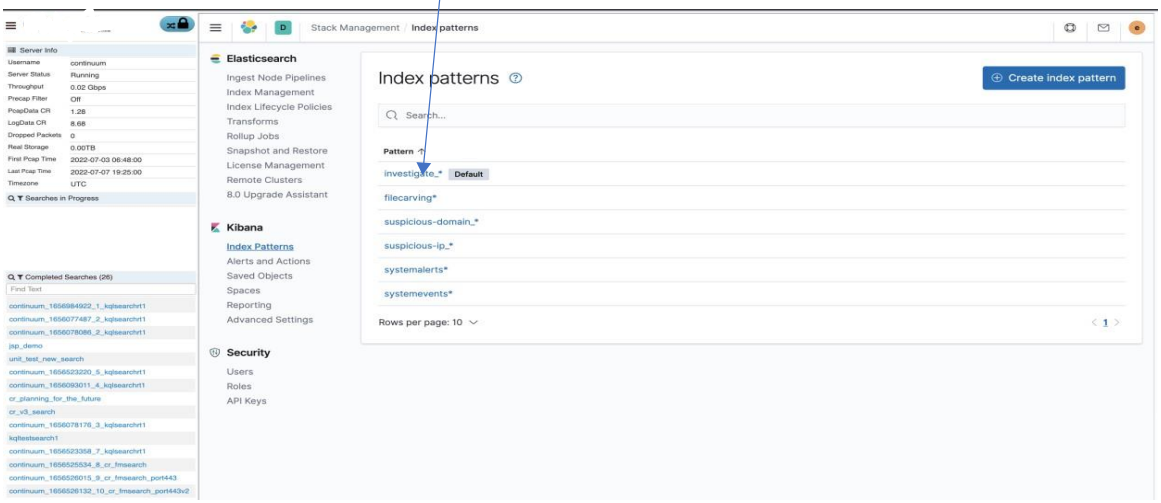
This process will require back-end console access of the FM Server. Run the following commands to set up the forwarder. In the following steps, 192.168.1.175 represents the Splunk forward server ip address.

- Get the package https://www.splunk.com/en_us/download/universal-forwarder/thank-you-universalforwarder.html
- rpm -i splunkforwarder-*.rpm
- cd /opt/splunkforwarder/bin
- ./splunk start
- mkdir /opt/splunkforwarder/to175
- ./splunk add monitor /opt/splunkforwarder/to175
- ./splunk add forward-server 192.168.1.175:9997
- ./splunk restart
- sudo firewall-cmd --zone=public --permanent --add-port=9997/udp
- sudo firewall-cmd --zone=public --permanent --add-port=9997/tcp
- systemctl restart firewalld
- ./splunk start
- cd /opt/splunkforwarder/bin
- ./splunk add monitor /storage0/logforwarder
- ./splunk add forward-server 192.168.1.175:9997
- ./splunk restart

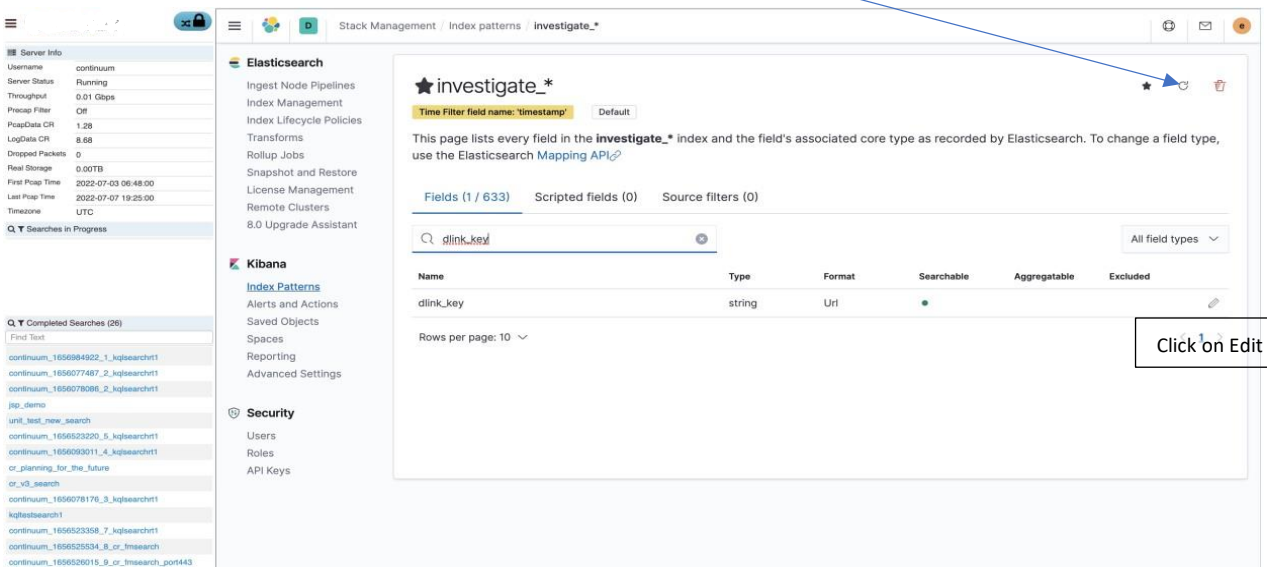
APPENDIX E - GET PCAP FROM INVESTIGATOR

This feature allows packets of a flow to be retrieved with a single click once the field dlink_key is mapped as shown below.

1) Stack Management->Index patterns-> Select Index Patterns, click on investigate_*

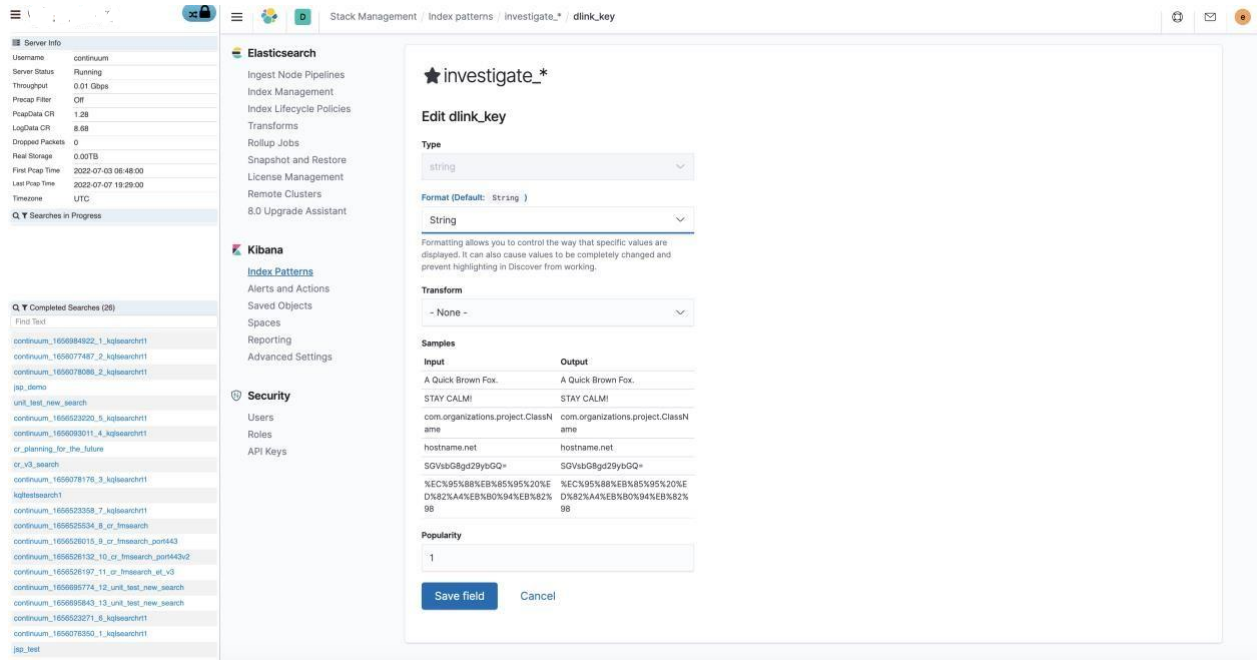


2) Search for dlink_key, if It does not show up, Hit refresh and try again..

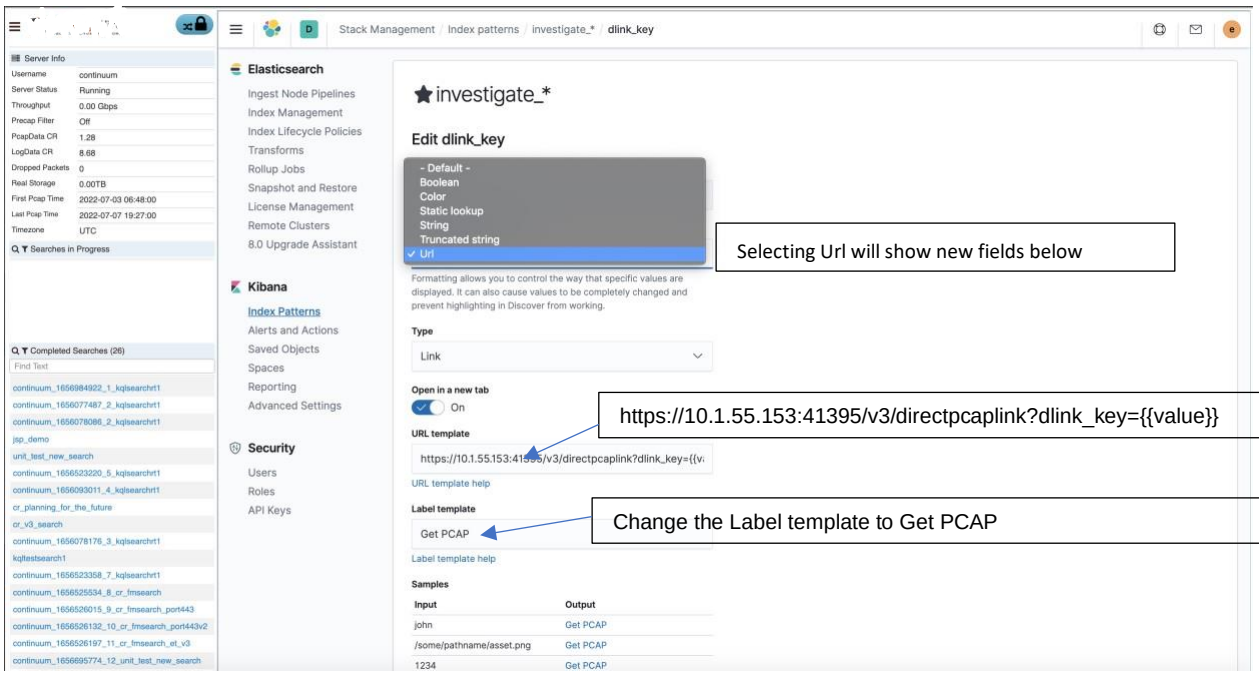


Click on Edit button

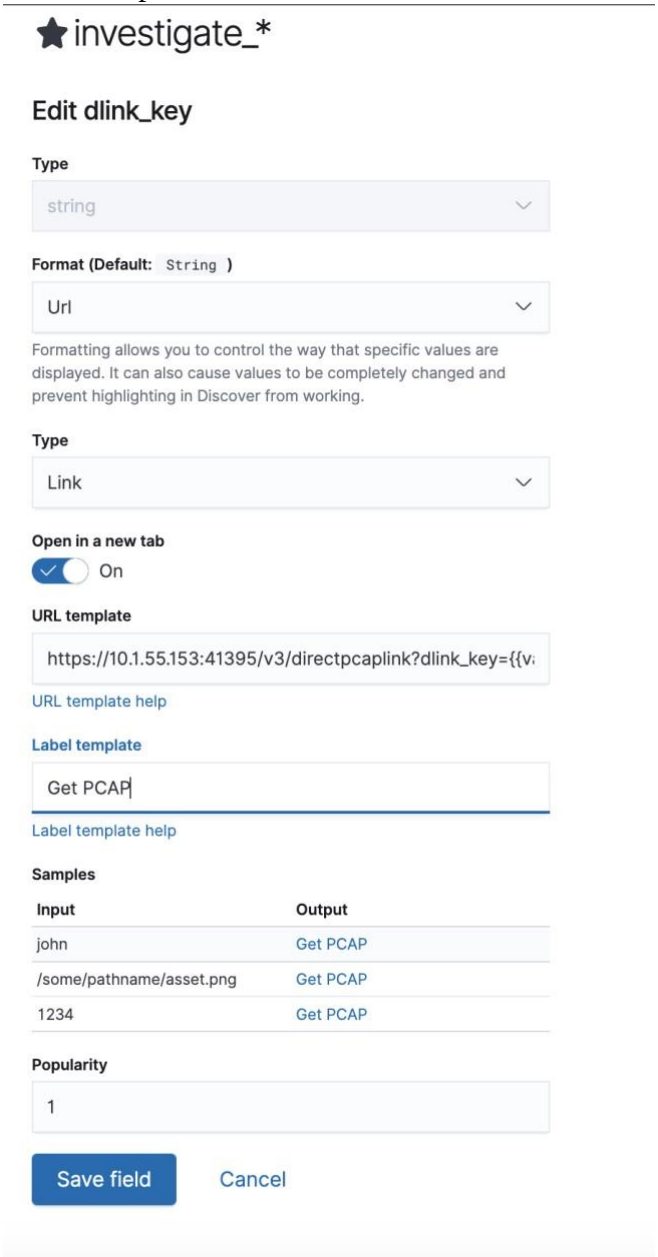
3) Change String to Url Default String – needs change to Url



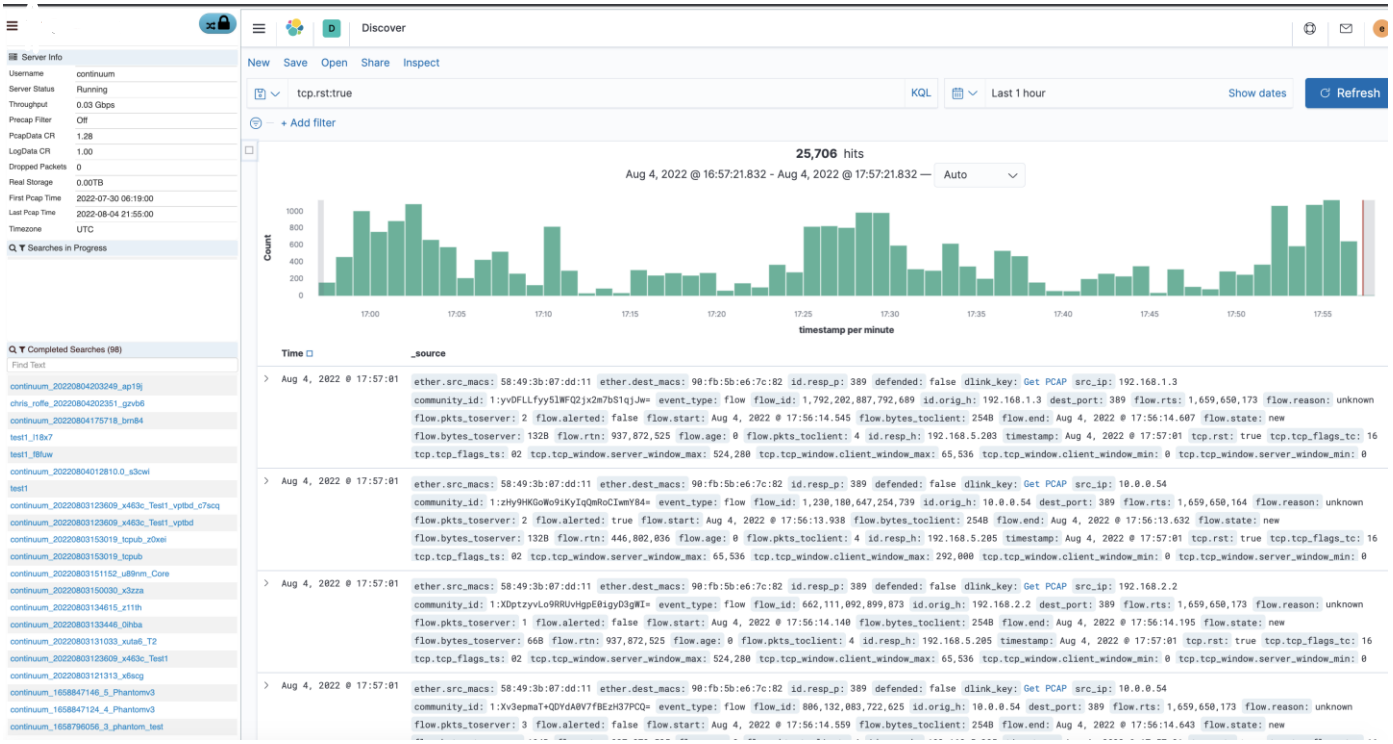
4) Add Url template https://<fmip>:41395/v3/directpcaplink?dlink_key={{value}}



5) Click on Save field – the screen must return to the Index data display to show that the Url setting has been accepted.



6) Refresh the page to see dlink_key show as GetPCAP hyperlinked to the flow being displayed.



Another view: