

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	4
1.1 Supported Web Browsers	4
1.2 Setting Up Your Network	4
1.3 UI Username/Password.....	4
1.4 Logging in to the application	4
FEDERATION MANAGER UI.....	5
2 INVESTIGATOR VIEW.....	6
2.1.1 Selectable Nodes	7
2.1.2 Custom (KQL) Search.....	7
2.1.3 CUSTOM (BPF) Search.....	9
2.1.4 Create Active Trigger	11
2.1.5 Expand IPv6 Address	12
2.2 Visualizations and Dashboards	13
2.2.1 Viewing an existing dashboard	13
2.2.2 Overview dashboard.....	13
2.2.3 Drilldown example	14
2.2.4 Dashboard structure.....	14
2.2.5 Creating a new dashboard	16
2.2.6 Creating a new visualization	17
2.2.7 Adding a visualization to a dashboard.....	22
2.2.8 Deleting a dashboard or visualization	24
2.2.9 Backup and restore custom dashboards.....	24
2.2.10 Discover.....	26
2.2.11 Pin a field to a column.....	26
2.2.12 Searches.....	27
3 ADMINISTRATOR VIEW	30
3.1 Configuration	30
3.1.1 Home	30
3.1.2 Selectable Nodes	31
3.1.3 Precapture Filter	31
3.1.4 Active Triggers.....	33
3.1.5 File Carving	34
3.1.6 Licensing	40
3.1.7 System Health.....	41
3.1.8 Software Updates	42
3.1.9 System Alerts	43
3.2 Search Management.....	44
3.2.1 Completed Searches	44
3.2.2 Pending Searches.....	45
3.2.3 Search Filter Library	46

3.3	AAA Management	46
3.3.1	Authorization.....	46
3.3.2	Authentication	47
3.3.3	Auditlog Preferences	50
3.3.4	Auditlog Receiver Settings.....	50
3.4	IDS Ruleset Management	51
3.4.1	Activated Rulesets	51
3.4.2	Deactivated Rulesets	53
3.4.3	SigDetect Ruleset	54
3.5	Augmentation.....	55
3.5.1	Suspicious Signatures	55
3.5.2	Suspicious IPs.....	57
3.5.3	Suspicious Domains	59
3.5.4	Suspicious MD5sums	60
3.5.5	Defended Assets	60
3.5.6	Defended Services	62
APPENDIX A – BPF FILTER.....		63
APPENDIX B - EXTENDING BPF SEARCH FILTERS		68
APPENDIX C - DECRYPTING PCAP WITH SSL SESSION KEYS		71
APPENDIX D – SPLUNK UNIVERSAL FORWARDER INSTALLATION		73
APPENDIX E - GET PCAP FROM INVESTIGATOR.....		74

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.

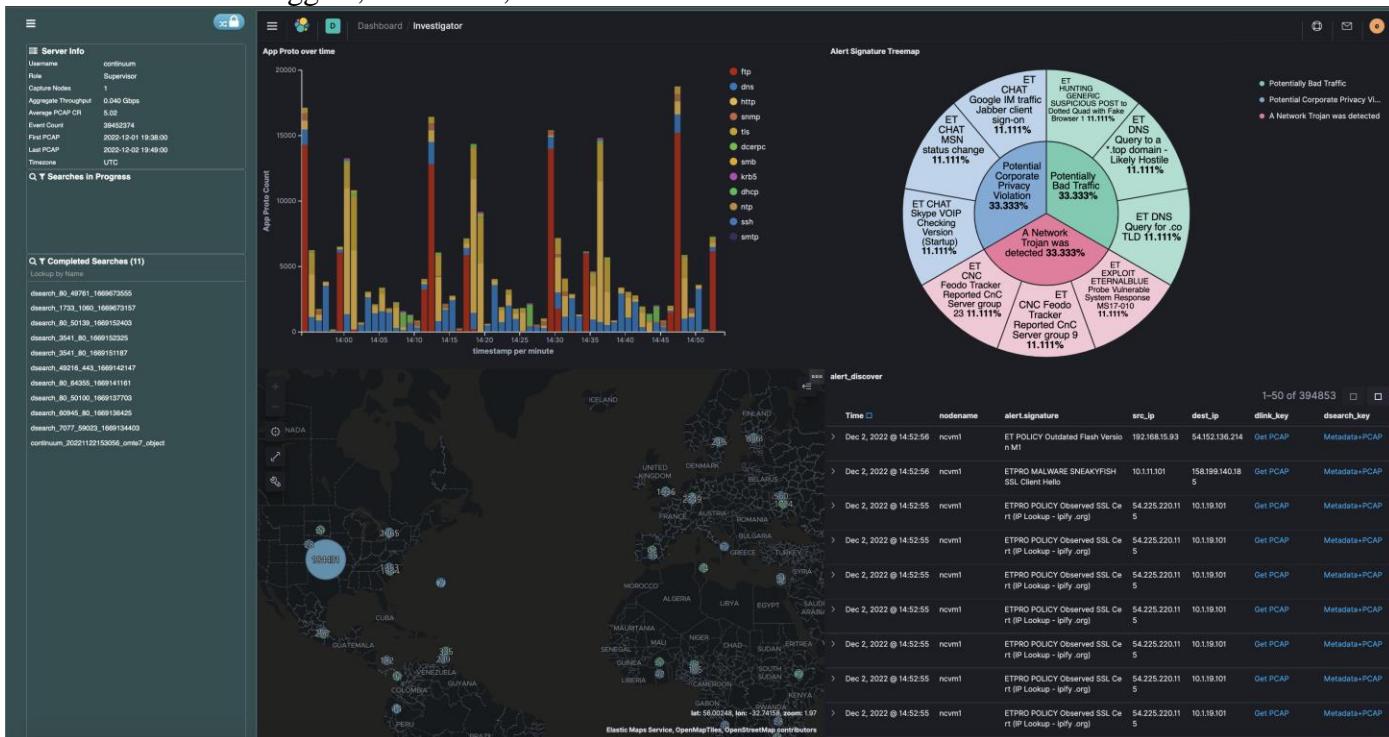
1.4 LOGGING IN TO THE APPLICATION

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.

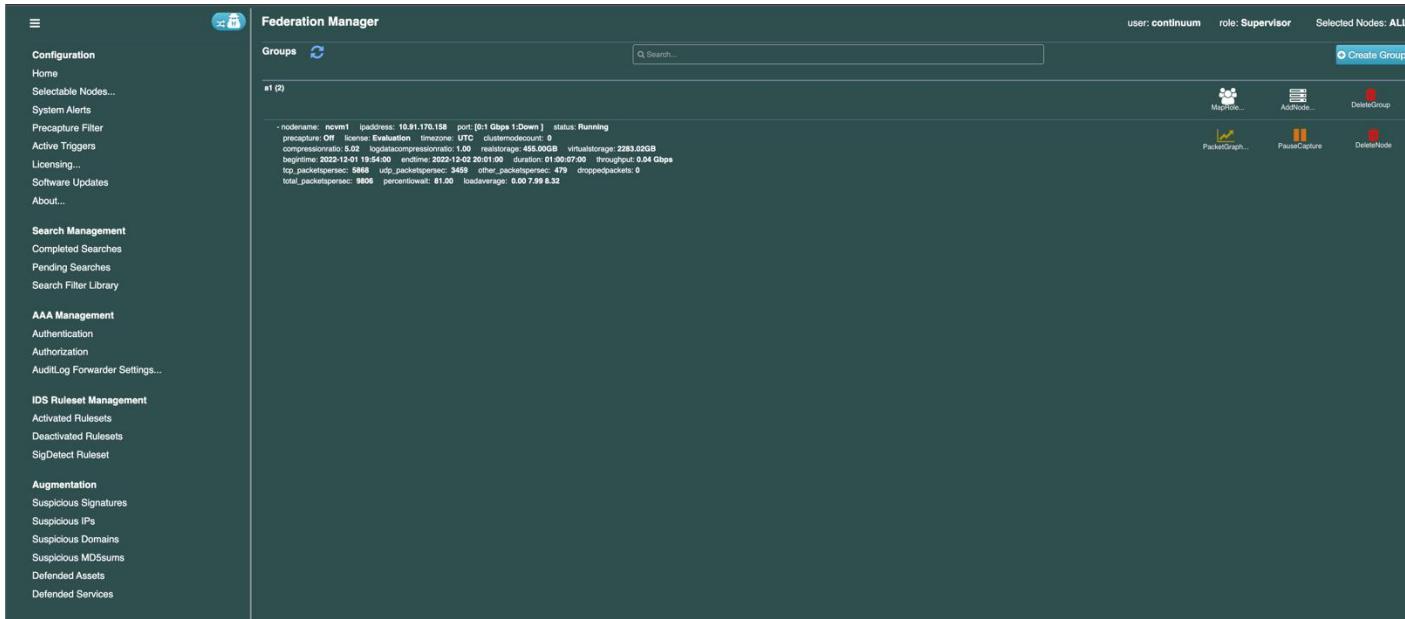
FEDERATION MANAGER UI

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.



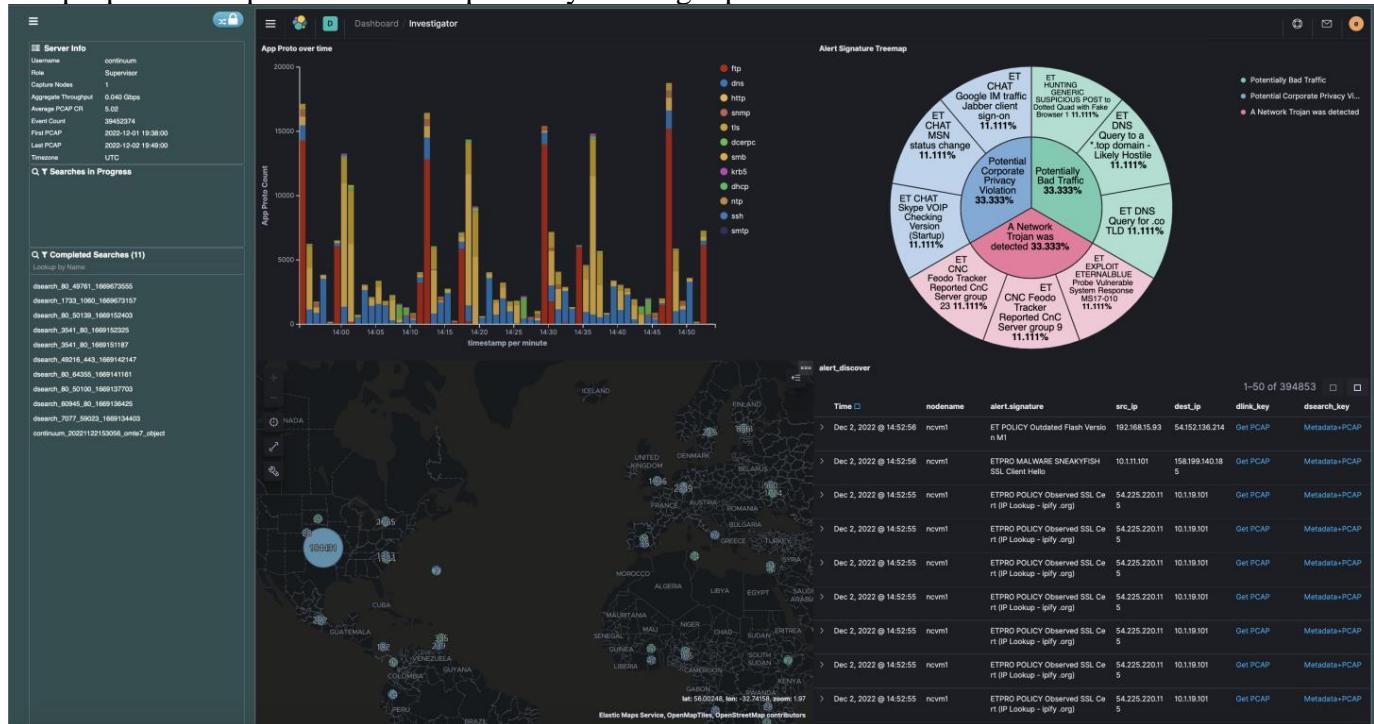
2. Administrator View - primarily used by UI administrators to setup, upload, or generally manage federation nodes.



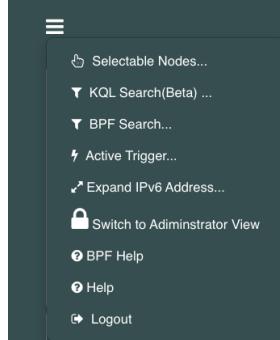
2 INVESTIGATOR VIEW

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.

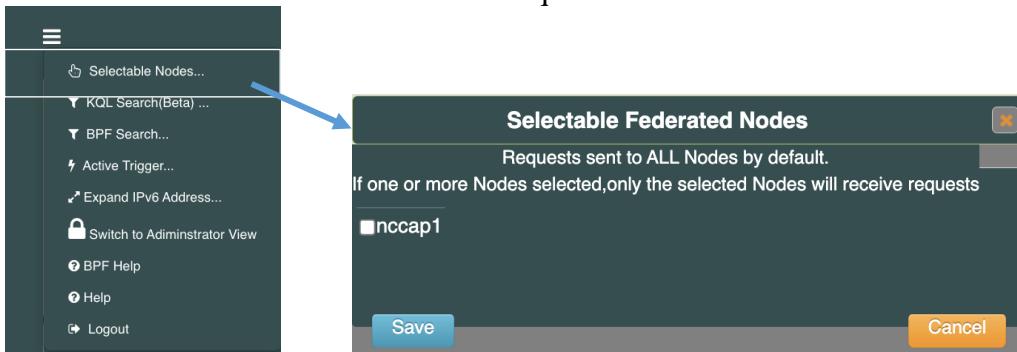


The Investigator drop down menu (≡) to the left the product logo is shown below:



2.1.1 Selectable Nodes

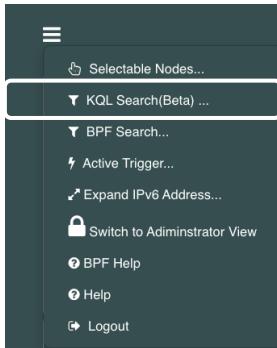
Each FM UI request goes to all connected federation nodes by default. This menu option allows users to restrict which federation nodes receive requests.



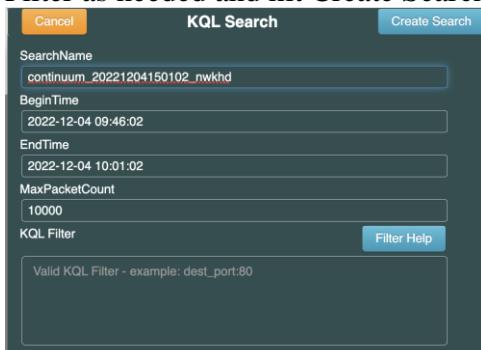
Users with Supervisor role are shown names of all the federated nodes. Other users are shown only the federated nodes from the groups they are allowed to view. The selected node list is effective until a new selection is made.

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

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_tz=2g
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 #8
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 top 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 host 2.3.4.5	
Create Search Search Library Cancel Request	

View Packets (continuum_20221122153056_omte7_object)

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 å 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 å 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 å 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 å 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 å 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 å 51914 [ACK] Seq=1411 Ack=1 Win=115 Len=1410
2022-11-22 10:15:56.002	10.1.1.52:51912	31.13.69.245:80	TCP	1464	80 å 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 å 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 å 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 å 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 å 80 [ACK] Seq=1 Ack=421 Win=258 Len=0
2022-11-22 10:15:56.003	31.13.69.245:80	10.1.1.52:51914	TCP	1464	80 å 51914 [ACK] Seq=421 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 å 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 å 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 å 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 å 51914 [ACK] Seq=7051 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 å 80 [ACK] Seq=1 Ack=8461 Win=258 Len=0
2022-11-22 10:15:56.003	31.13.69.245:80	10.1.1.52:51914	TCP	1464	80 å 51914 [ACK] Seq=8461 Ack=1 Win=115 Len=1410

View Objects (continuum_20221122153056_omte7_object)

55d1c6c0-97d7-4...

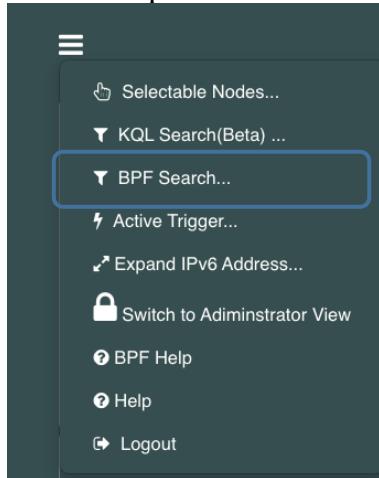
1 / 1 - 120% + Find Text Download Print ...



FileName	Size	MD5
17662087_1865520113686672_8841619392077758464-n.jpg	21e7f5f5ccf3ed464a96...	Download View
17818238_806507009501886_2717383150564016128-n.jpg	ace7c06d18d0a2dd50...	Download View

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:

Create Custom(BPF) Search

SearchName	continuum2_20221204150852_zarj
BeginTime	2022-12-04 09:53:52
EndTime	2022-12-04 10:08:52
MaxPacketCount	10000
BPF Filter	tcp or udp
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 host 2.3.4.5
<input type="button" value="Create Search"/> <input type="button" value="Search Library"/> <input type="button" value="Cancel Request"/>	

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.

Create Custom(BPF) Search

SearchName
continuum2_20221204150852_zarxj

BeginTime
2022-12-04 09:53:52

EndTime
2022-12-04 10:08:52

MaxPacketCount
10000

BPF Filter
tcp or udp

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
tcp
host 1.2.3.4
host 1.2.3.4
host 1.2.3.4
host 1.2.3.4
src host 192.168.5.56 and src port 53805 and dst host 169.55.165.141 and dst port 80
port 80
src host 192.168.5.7 and src port 7077 and dst host 91.121.30.149 and dst port 59023
src host 10.5.26.4 and src port 445 and dst host 10.5.26.132 and dst port 49221
src host 64.94.43.110 and src port 80 and dst

Search Filter Library

src host 192.168.5.56 and src port 53805 and dst host 169.55.165.141 and dst port 80
port 80
src host 192.168.5.7 and src port 7077 and dst host 91.121.30.149 and dst port 59023
src host 10.5.26.4 and src port 445 and dst host 10.5.26.132 and dst port 49221
src host 64.94.43.110 and src port 80 and dst

Create Search

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.

Create ActiveTrigger

Trigger Name
continuum2_20221204153107

Seconds Before
30

Seconds After
30

SearchFilter (https://biot.com/capstats/bpf.html)
valid BPF Filter eg.,tcp or udp

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.

Expand IPv6 Address

IPv6 to be Expanded

↔

Expanded IPv6:4

Expanded IPv6:2

Enter IPv6 address to be expanded:

↔

Expanded IPv6:4

Expanded IPv6:2

Press Expand button:

Expand IPv6 Address

IPv6 to be Expanded

↔

Expanded IPv6:4

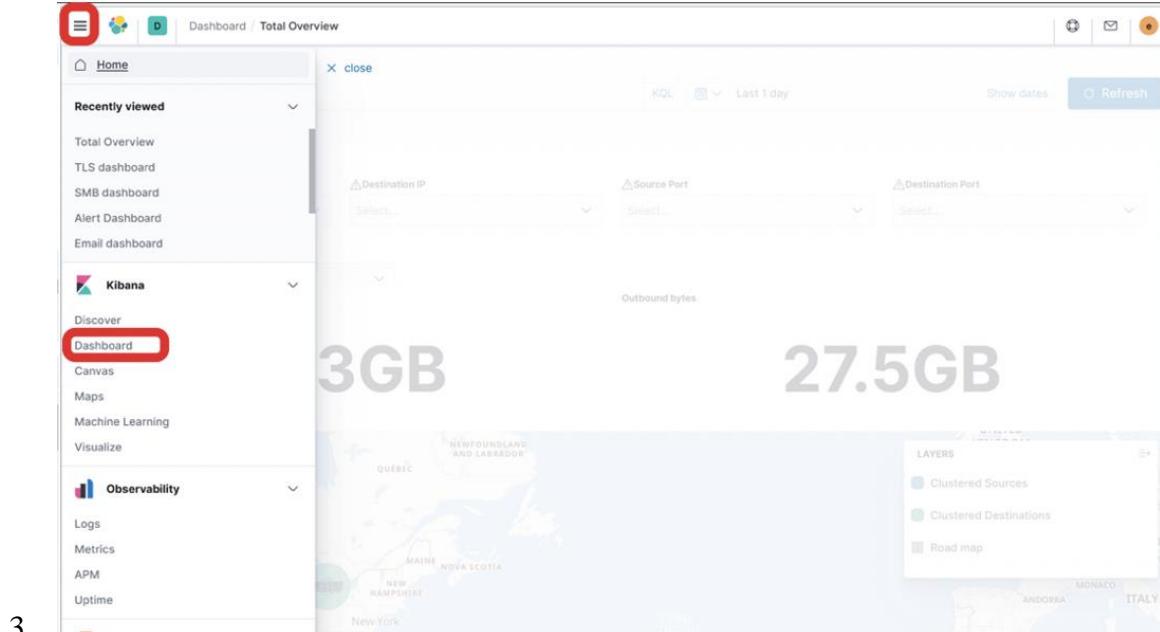
Expanded IPv6:2

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

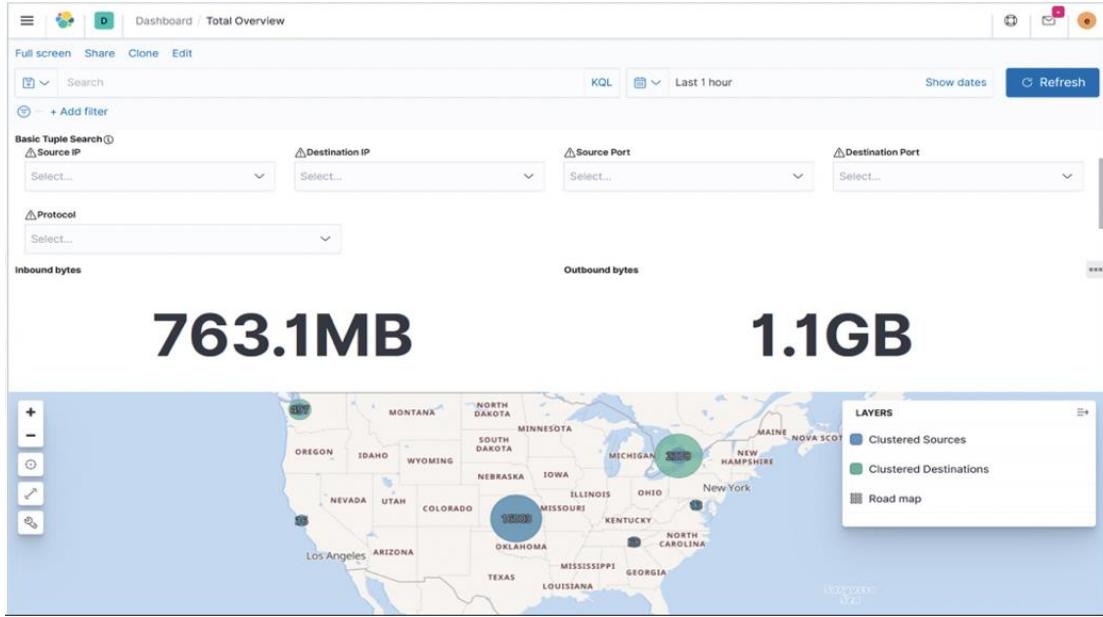
1. To view an existing dashboard object in Kibana, click on the 3 bars at the top left of the screen to open the drop-down menu
2. Click on dashboard



- 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

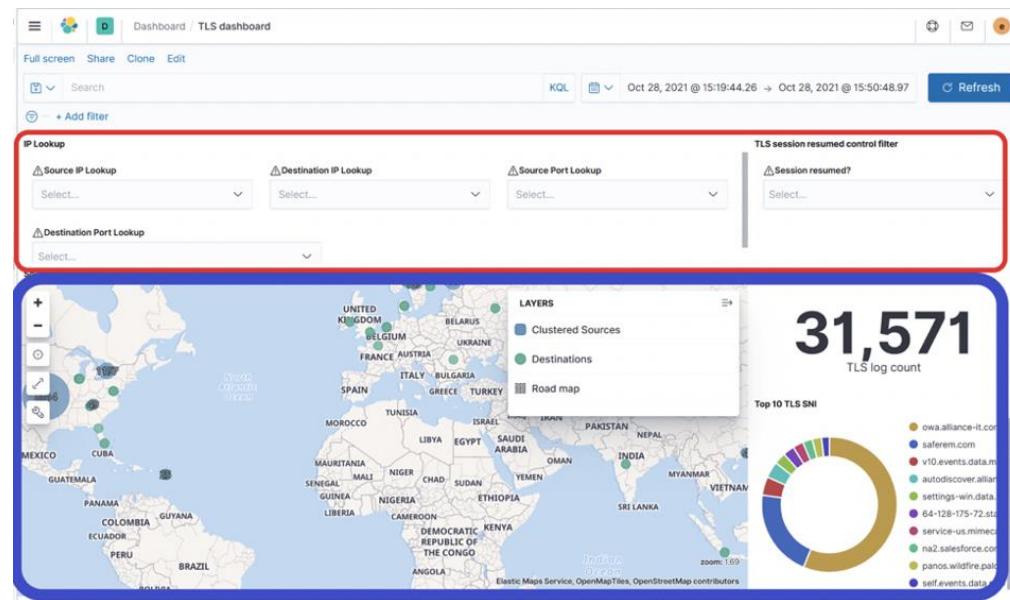
At the bottom of the overview are breakouts of different logs by protocol. By clicking and dragging over sections in the chart, the option to filter by the time span and the option to drill down deeper into the dedicated protocol dashboard will appear. Some protocols have multiple drill down dashboards 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.



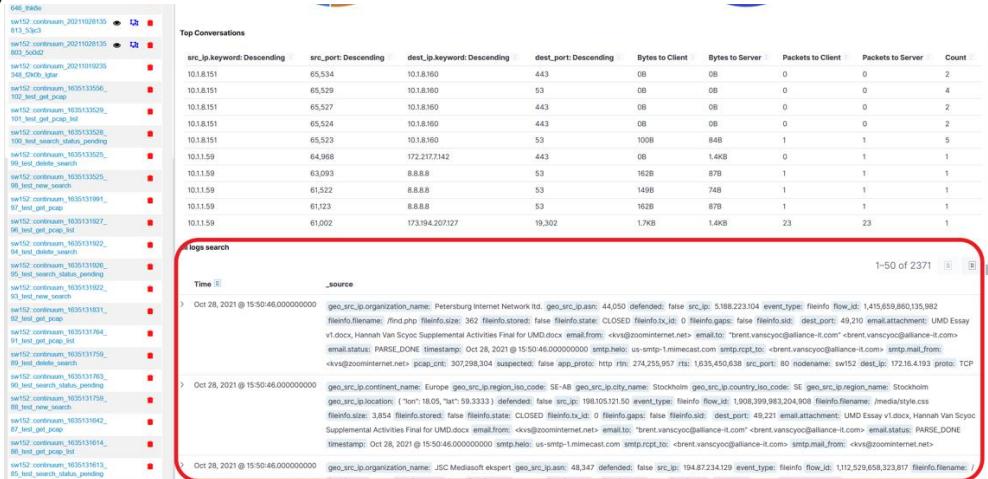
2.2.4 Dashboard structure

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

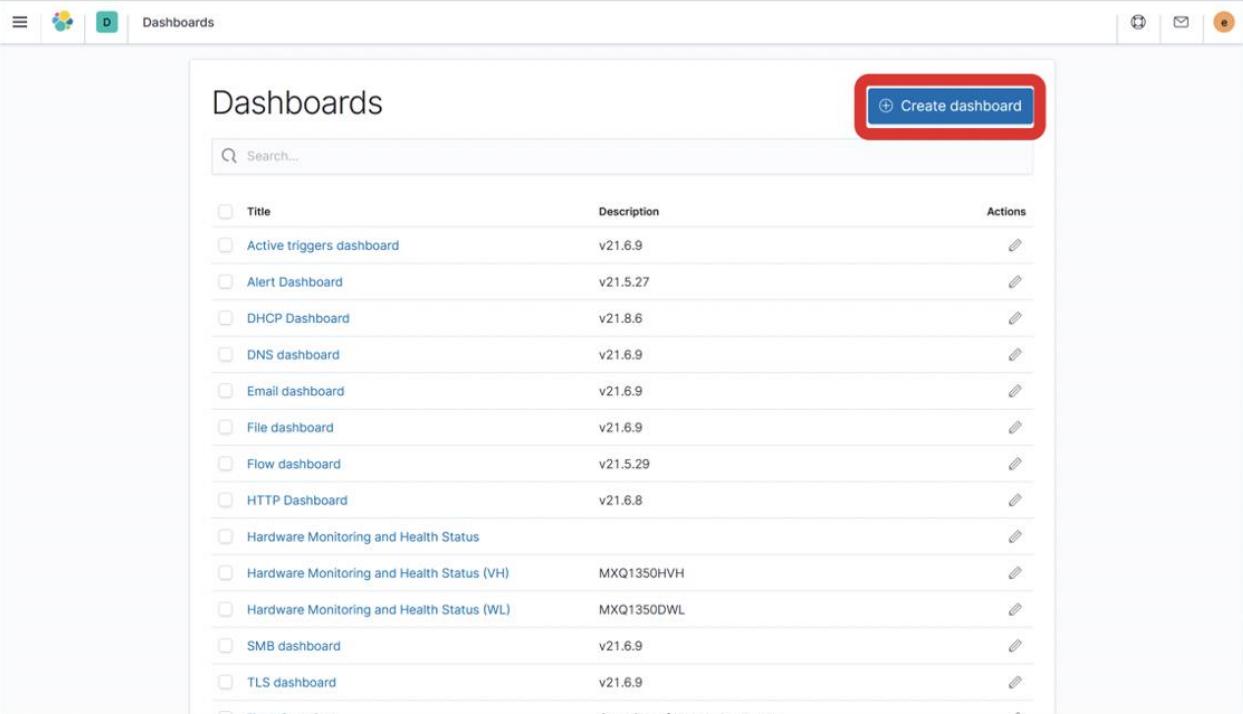


- "All log" viewer at the bottom includes more than the filtered protocols that the dashboard is named after so you can see associated traffic



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



The screenshot shows the SentryWire interface for managing dashboards. At the top, there's a navigation bar with icons for Home, Analytics, and Dashboards. The 'Dashboards' tab is selected. Below the navigation is a search bar labeled 'Search...'. The main area is titled 'Dashboards' and contains a table with the following data:

Title	Description	Actions
Active triggers dashboard	v21.6.9	
Alert Dashboard	v21.5.27	
DHCP Dashboard	v21.8.6	
DNS dashboard	v21.6.9	
Email dashboard	v21.6.9	
File dashboard	v21.6.9	
Flow dashboard	v21.5.29	
HTTP Dashboard	v21.6.8	
Hardware Monitoring and Health Status		
Hardware Monitoring and Health Status (VH)	MXQ1350HVH	
Hardware Monitoring and Health Status (WL)	MXQ1350DWL	
SMB dashboard	v21.6.9	
TLS dashboard	v21.6.9	
Total Overview	Overview of the whole system	

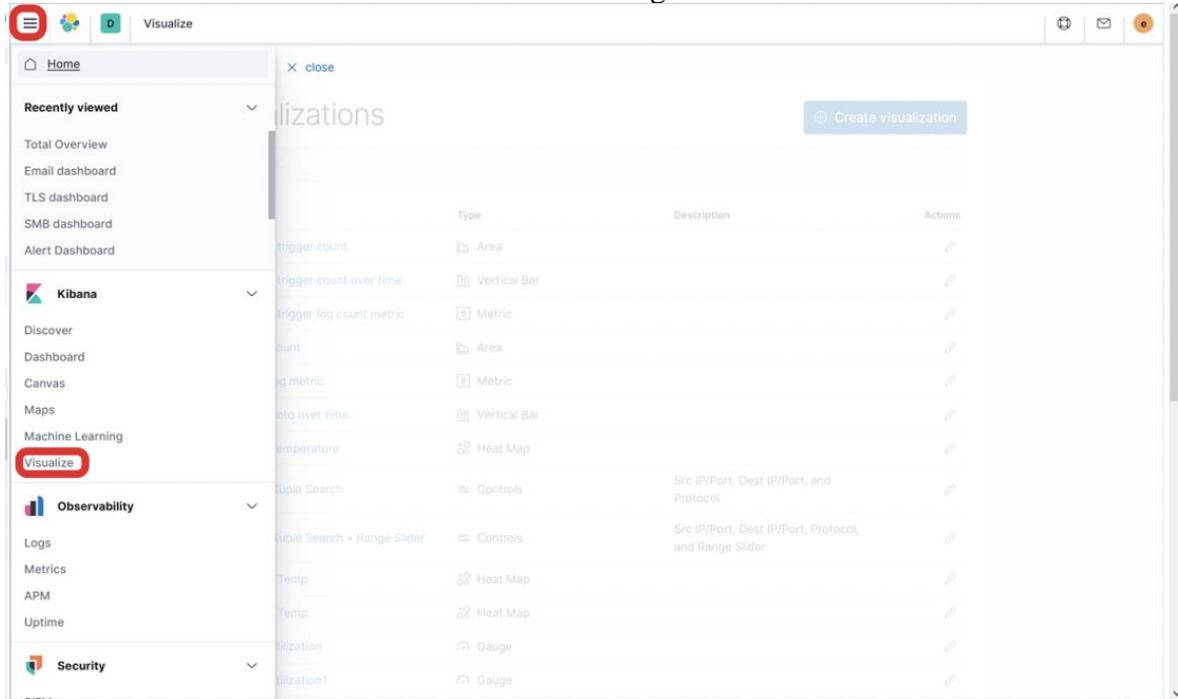
In the top right corner of the dashboard list, there is a blue button with a white plus sign and the text 'Create dashboard', which is highlighted with a red rectangular box.

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



	Type	Description	Actions
trigger count	Area		
trigger count over time	Vertical Bar		
trigger log count metric	Metric		
Log count	Area		
Log metric	Metric		
Log over time	Vertical Bar		
Temperature	Heat Map		
Tuple Search	Controls	Src IP/Port, Dest IP/Port, and Protocol	
Tuple Search + Range Slider	Controls	Src IP/Port, Dest IP/Port, Protocol, and Range Slider	
Temp	Heat Map		
Temp	Heat Map		
Utilization	Gauge		
Utilization1	Gauge		

Visualizations

[Create visualization](#)

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

New Visualization

Filter



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](#)

X

New Pie / Choose a source

Sort ▾

Types 2 ▾

- all logs search
- all_log_investigator_dynamic
- Email attachment search
- File
- ilo*
- investigate_*
- netflow_smb_event_search
- SMB Commands

< 1 2 >

● Count investigate_*

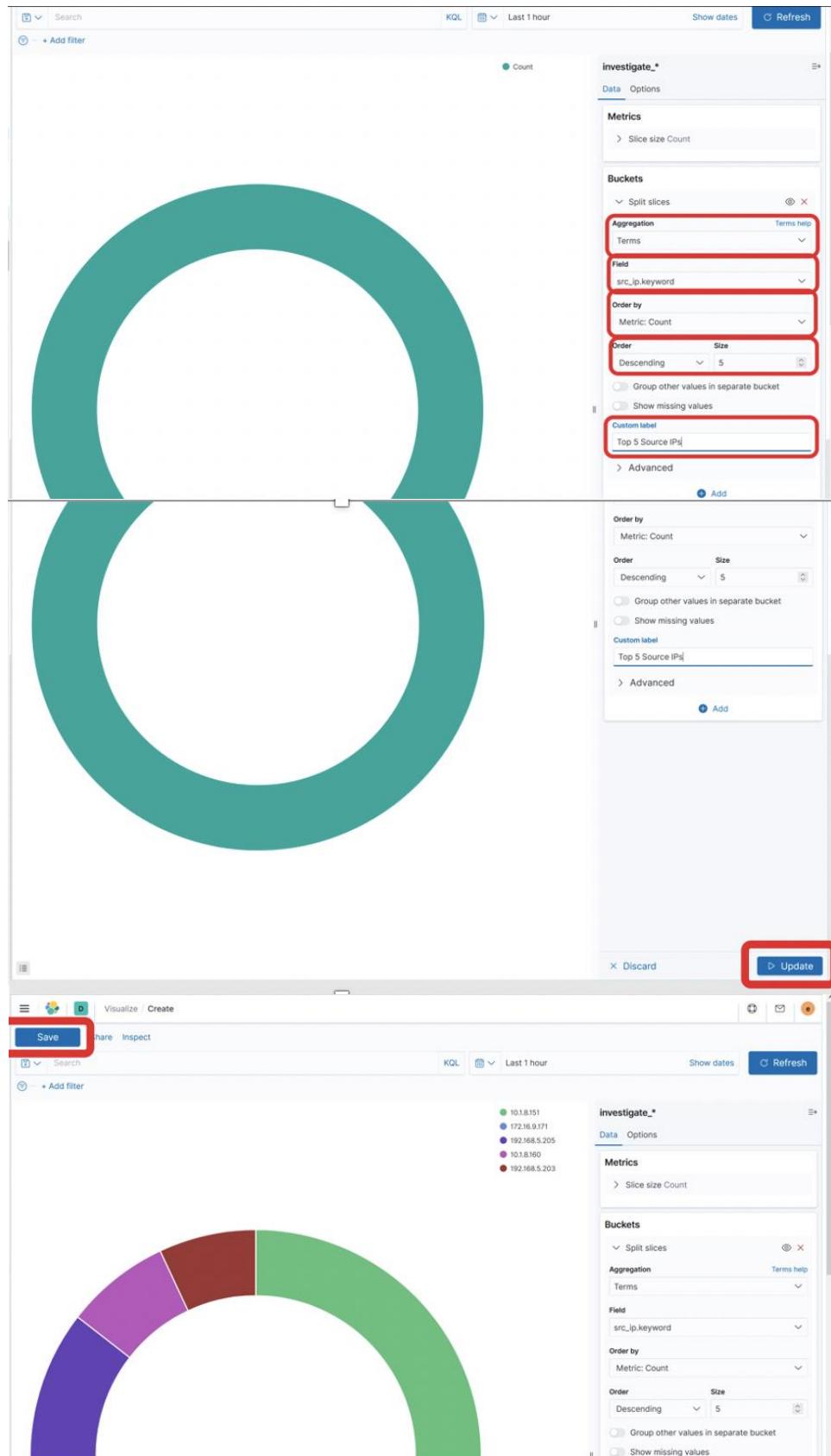
Data Options

Metrics > Slice size Count

Buckets Add

● Add ADD BUCKET

Split slices Split chart



X

Save visualization

Title

Top 5 Source IPs

Description

(Empty text area)

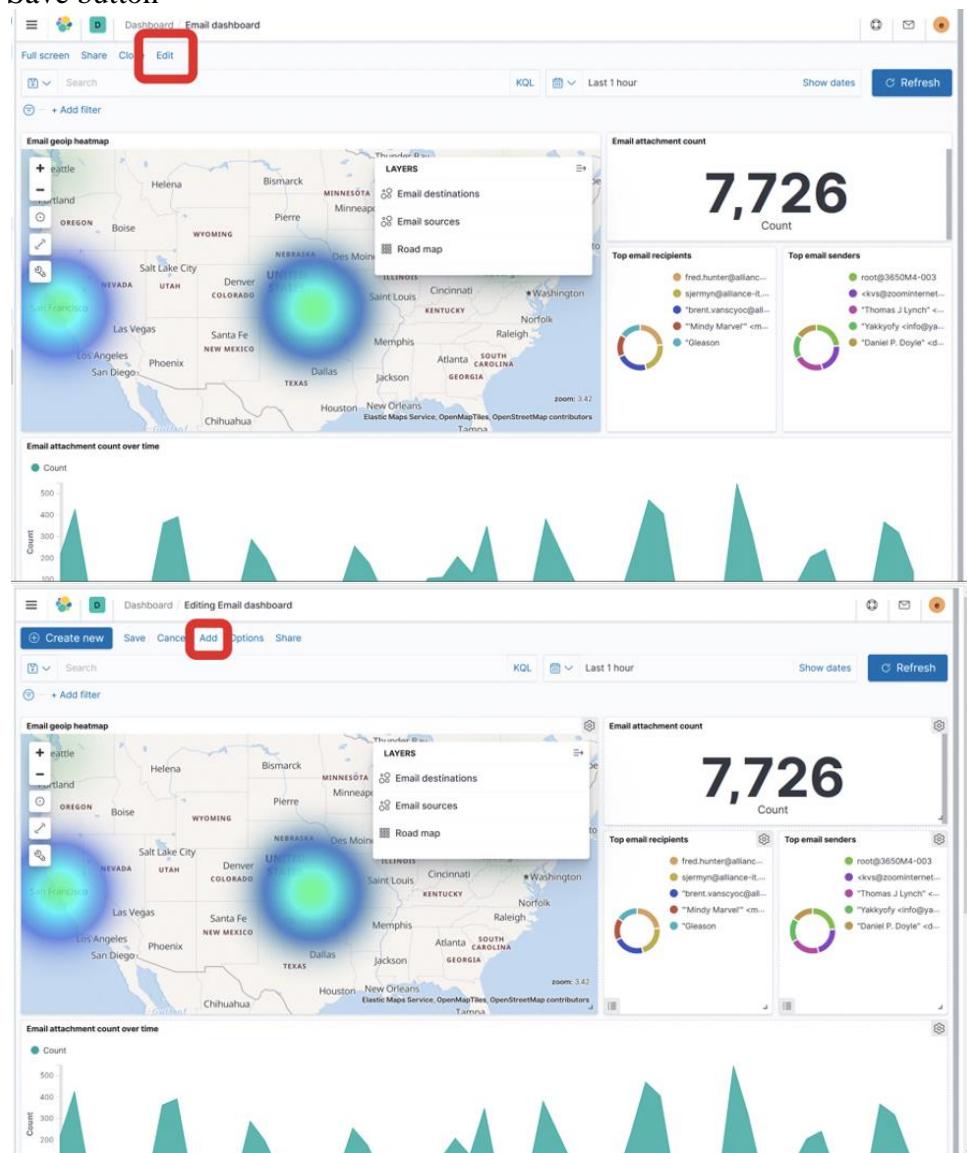
Cancel

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



Editing Email dashboard

Add panels

Top 5 (highlighted)

Top 5 Source IPs

Email geoplot heatmap

Email attachment count over time

Log entries

Top 5 Source IPs

Save (highlighted)

Dashboard **Editing Email dashboard (unsaved)**

Email geoplot heatmap

Email attachment count

7,696 Count

Top email recipients

Top email senders

X

Save dashboard

 Save as new dashboard

Title

Email dashboard

Description

v21.6.9

 Store time with dashboard

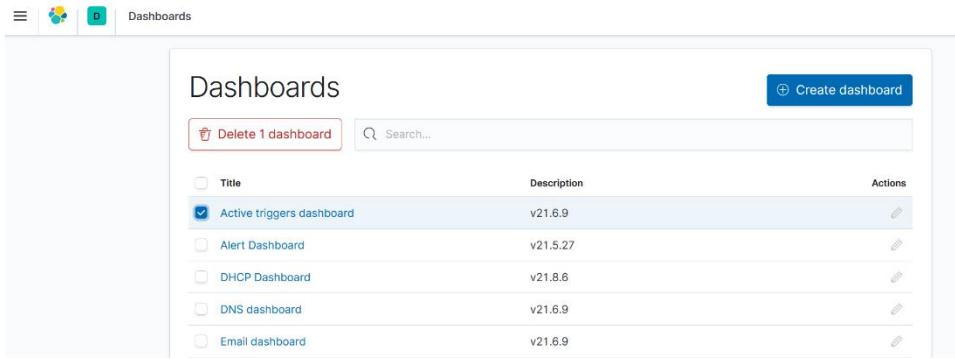
This changes the time filter to the currently selected time each time this dashboard is loaded.

Cancel

Save

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



Dashboards			
<input type="button" value="Delete 1 dashboard"/> <input type="text" value="Search..."/>		<input type="button" value="Create dashboard"/>	
	Title	Description	Actions
<input checked="" type="checkbox"/>	Active triggers dashboard	v21.6.9	<input type="button" value="Edit"/>
<input type="checkbox"/>	Alert Dashboard	v21.5.27	<input type="button" value="Edit"/>
<input type="checkbox"/>	DHCP Dashboard	v21.8.6	<input type="button" value="Edit"/>
<input type="checkbox"/>	DNS dashboard	v21.6.9	<input type="button" value="Edit"/>
<input type="checkbox"/>	Email dashboard	v21.6.9	<input type="button" value="Edit"/>

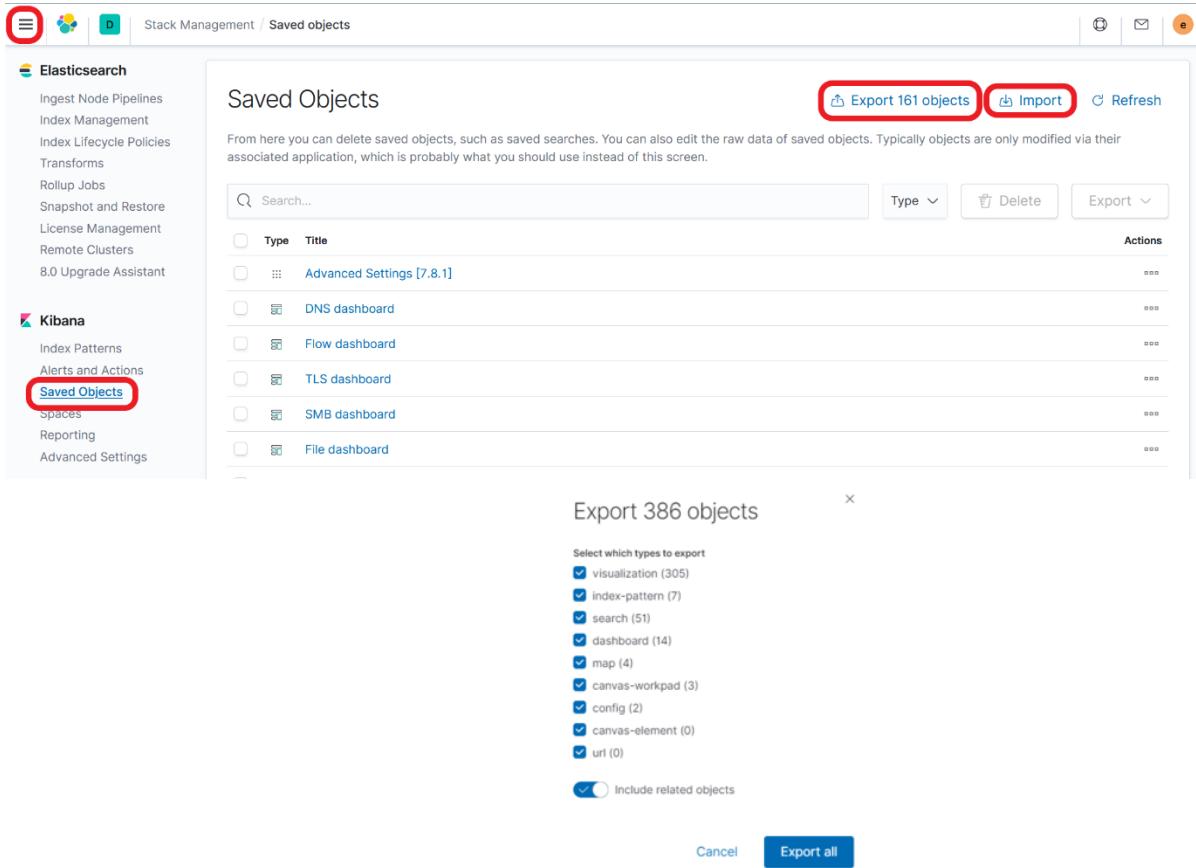
2.2.9 Backup and restore custom dashboards

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



Stack Management / Saved objects

Elasticsearch

- Ingest Node Pipelines
- Index Management
- Index Lifecycle Policies
- Transforms
- Rollup Jobs
- Snapshot and Restore
- License Management
- Remote Clusters
- 8.0 Upgrade Assistant

Kibana

- Index Patterns
- Alerts and Actions
- Saved Objects**
- Spaces
- Reporting
- Advanced Settings

Saved Objects

From here you can delete saved objects, such as saved searches. You can also edit the raw data of saved objects. Typically objects are only modified via their associated application, which is probably what you should use instead of this screen.

Search... Type Title Actions

Type	Title	Actions
Advanced Settings [7.8.1]		...
DNS dashboard		...
Flow dashboard		...
TLS dashboard		...
SMB dashboard		...
File dashboard		...

Export 386 objects

Select which types to export

visualization (305)
 index-pattern (7)
 search (51)
 dashboard (14)
 map (4)
 canvas-workpad (3)
 config (2)
 canvas-element (0)
 url (0)

Include related objects

Cancel Export all

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.

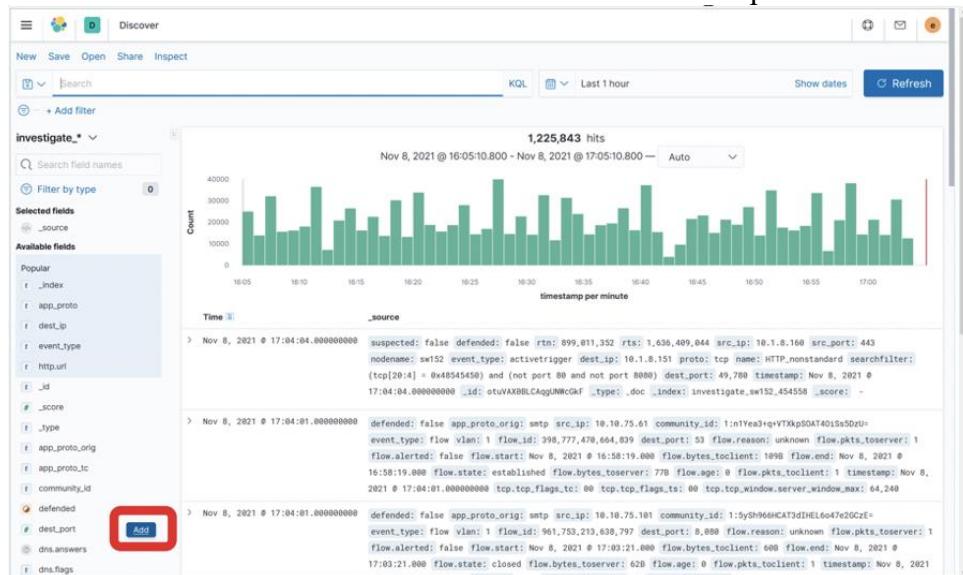


The screenshot shows the SentryWire Discover interface. On the left, there is a sidebar titled "investigate_*" with a search bar and a "Filter by type" section. Below this are sections for "Selected fields" (which includes "_source") and "Available fields". The "Available fields" section lists various metadata fields such as _index, _id, _score, _type, _id, alert.action, alert.gid, alert.metadata.affect..., alert.metadata.attac..., alert.metadata.creat..., alert.metadata.depl..., alert.metadata.form..., and alert.metadata.mobi... . To the right of the sidebar is a histogram titled "25,988 hits" showing the count of events per minute from Oct 28, 2021, at 16:33 to 17:33. Below the histogram is a table of log entries. The first entry is:

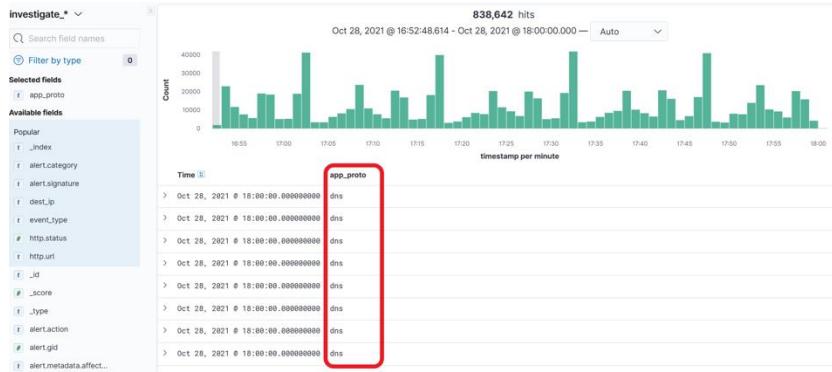
```
geo_src_ip.organization_name: Cogeco Peer 1 geo_src_ip.ip:asn: 13,768 pcp_cnt: 218,733,768 suspected: false
defended: false app_proto: http rts: 1,655,641,284 ts: 1,655,456,310 src_ip: 209.15.36.33 src_port: 80
node_name: swt32 event_type: fileinfo flow_id: 1,261,881,074,881,861 dest_ip: 10.1.1.32 proto: TCP
fileinfo.magic: HTML document, ASCII text fileinfo.filename: /1http://request_uri/notseen fileinfo.size: 110
fileinfo.stored: false fileinfo.state: CLOSED fileinfo.tx_id: 6 fileinfo.gps: false fileinfo.sid:
```

Subsequent entries show similar log details with different timestamps and flow IDs.

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



This screenshot shows the same Discover interface as the previous one, but with a red box highlighting the "Add" button located at the bottom of the "Available fields" sidebar. The sidebar and histogram are identical to the previous screenshot. The log table below also contains the same entries as the previous screenshot.



2.2.12 Searches

Kibana uses KQL, which is further defined in the [documentation](#), but below are the basics.

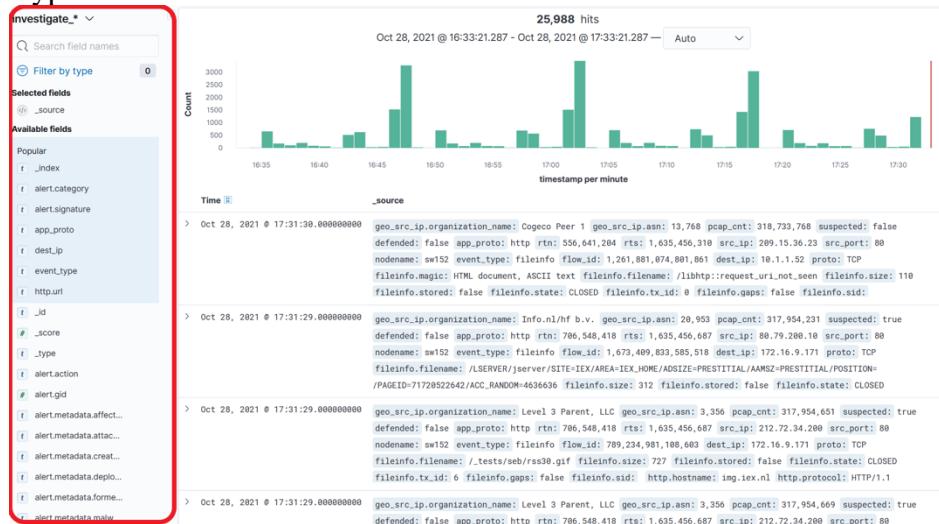
Accessing fields

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

Example:

ttt.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:

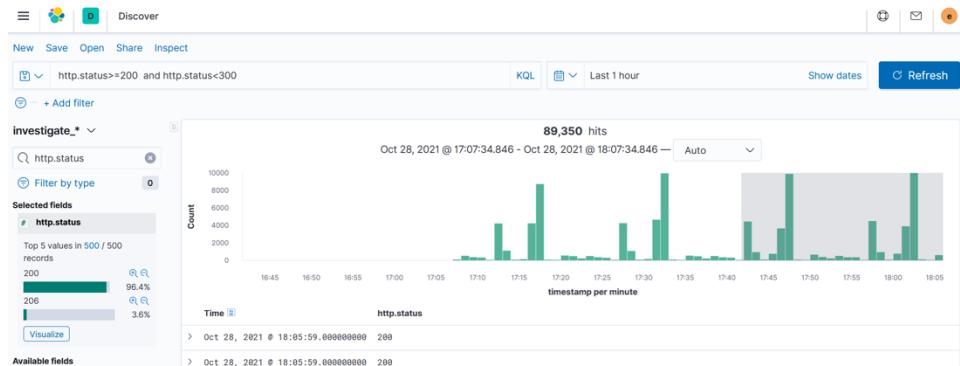
not dest_port : 80

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.

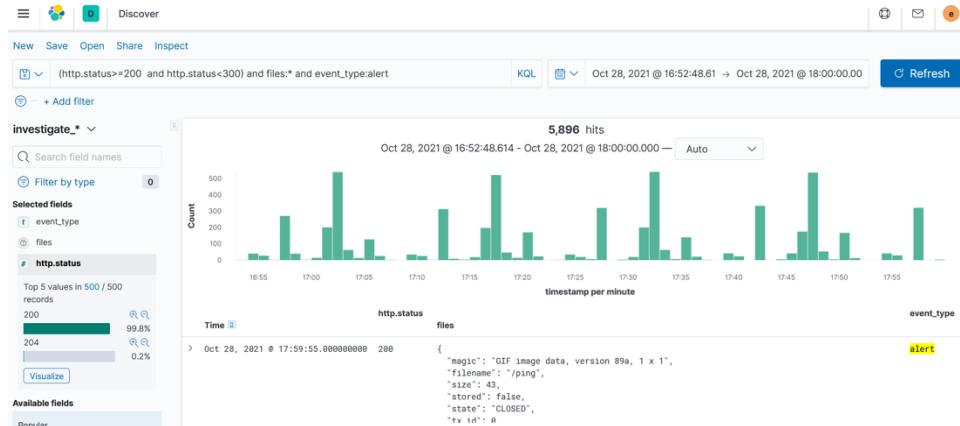
Example query to return all DNS logs for a specific source:

```
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

KQL 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

SYNTAX OPTIONS

1,134,592 hits

/ 17, 2021 @ 11:38:23.897 — Auto

Count

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: 88.87.281.221 src_port: 7,088 nodename: sw152 event_type: activetrigger dest_ip: 18.9.38.101 proto: tcp name: HTTP_nonstandard searchfilter: (tcp[20:4] = 0x48545450) and (not port 80 and not port 8080) ioc: Emotet4, 88.87.281.221 dest_port: 64,314 timestamp: Nov 17, 2021 @ 11:37:43.000000000 _id: OybDLn8BLCAqgUNWSSV9 _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: 59,924 timestamp: Nov 17, 2021 @ 11:37:10.000000000 _id: CibDLn8BLCAqgUNWSSV9 _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: OSbDLn8BLCAqgUNWSSV9 _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

event_type : smtp

Lucene

1,680 hits

/ Nov 17, 2021 @ 10:41:07.437 — Nov 17, 2021 @ 11:41:07.437 — Auto

Count

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 @ 11:38:43.000000000 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

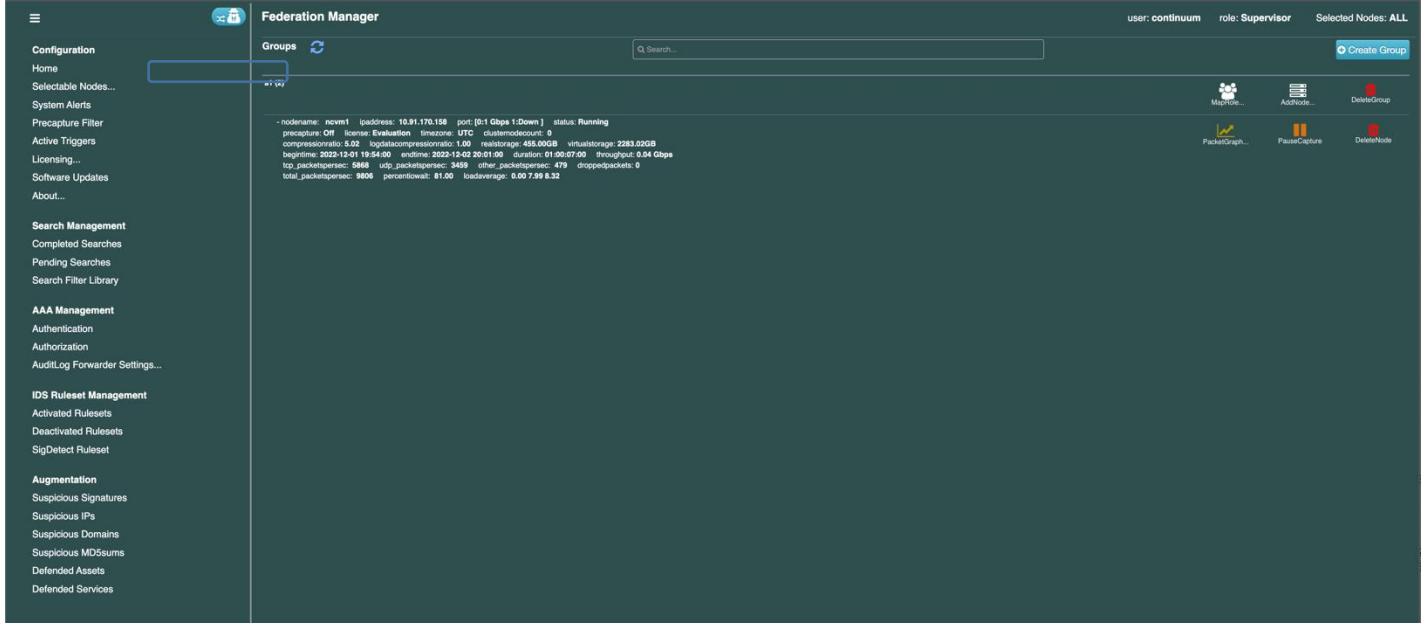
The Home button shows the Groups and Nodes of the Federation Manager. Top of the Admin UI page shows the currently logged in user's name, user's role, authentication mode and product version. The following sections describe each of the options available on the left panel and the actions/views based on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

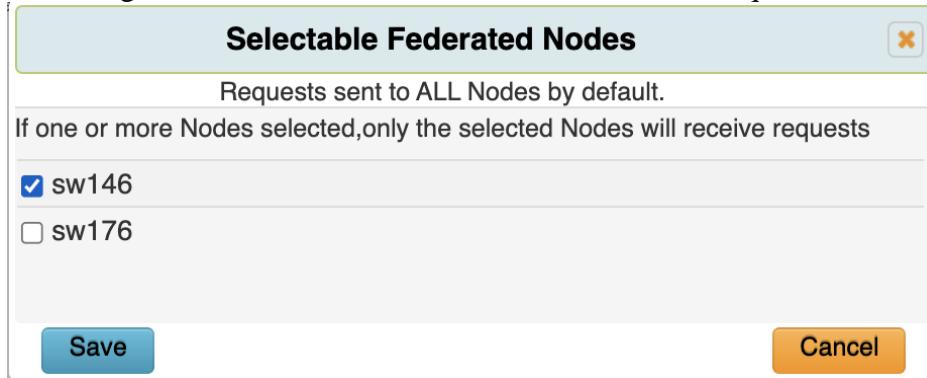
- The advertised throughput includes system resource calculations for packet processing. As such, the throughput is measured as it reaches the interface, not after internal processing. This allows us to ensure we do not drop packets, while still giving accurate metrics.
- Delete Node: A node can be deleted 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.



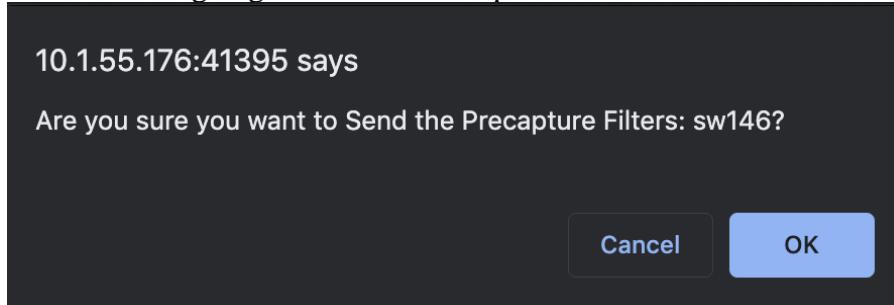
The screenshot shows the SentryWire Federation Manager interface. On the left, there's a sidebar with various management sections: Configuration (Selectable Nodes...), Search Management (Completed Searches, Pending Searches, Search Filter Library), AAA Management (Authentication, Authorization, Audit Log Forwarder Settings...), IDS Ruleset Management (Activated Rulesets, Deactivated Rulesets, SigDetect Ruleset), Augmentation (Suspicious Signatures, Suspicious IPs, Suspicious Domains, Suspicious MD5sums, Defended Assets, Defended Services). The main area is titled 'Federation Manager' and contains a 'Groups' section with a 'Create Group' button. Below it is a table with detailed statistics about a node named 'sw146'. At the bottom right are icons for 'Monitor...', 'Address...', 'DeleteGroup', 'PacketGraph...', 'PauseCapture', and 'DeleteNode'.

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.



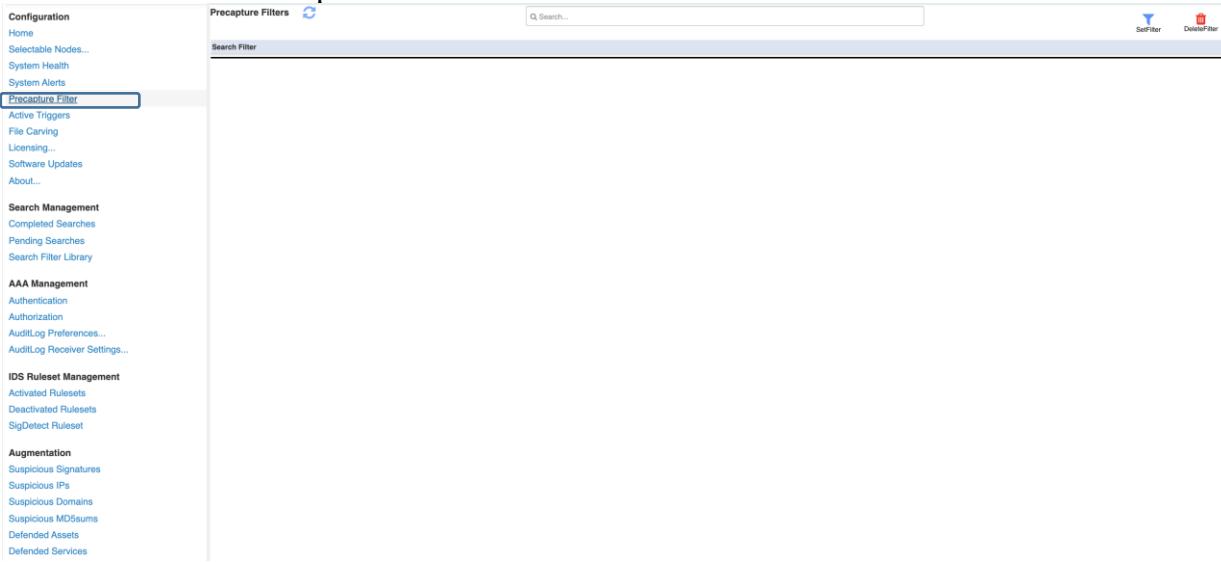
From this point on, when a request such as SetPrecapture is initiated, the user is presented with the list of nodes that are going to receive this request:



3.1.3 Precapture Filter

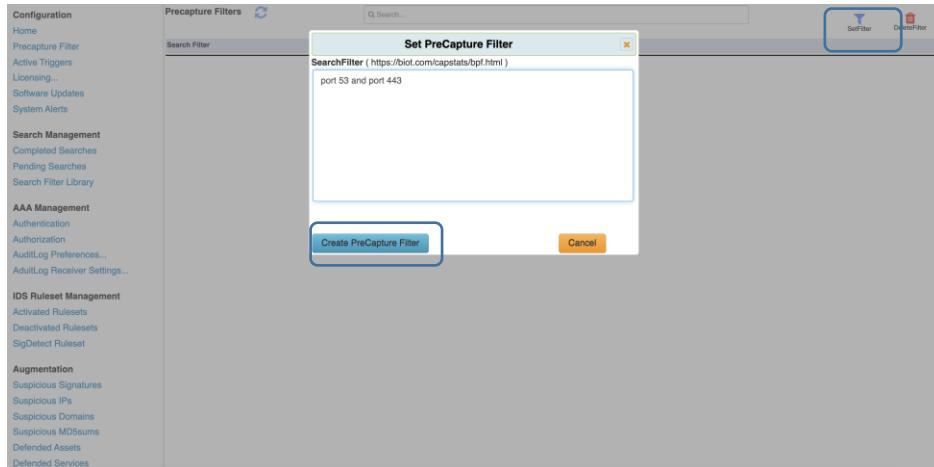
By default, all the received traffic is captured and stored. A precapture filter can be applied to receive only the

traffic that needs to be captured.

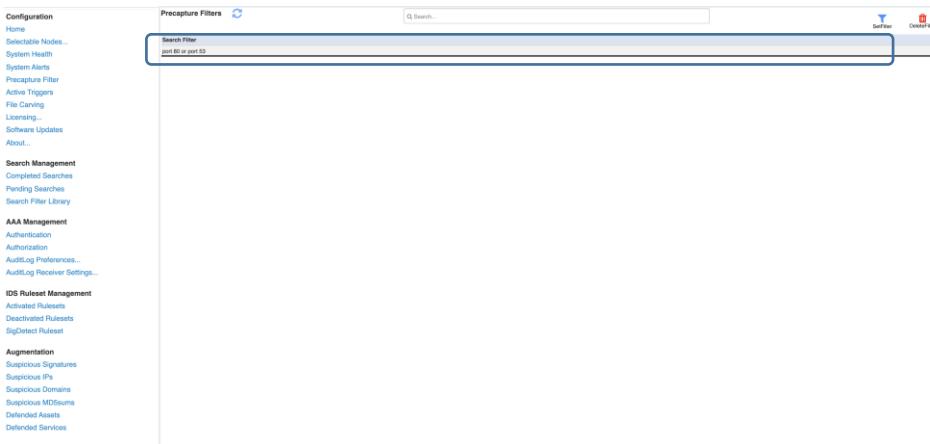


The screenshot shows the SentryWire interface with the "PreCapture Filter" option selected in the configuration sidebar. The main area displays a search bar and a "Search Filter" input field.

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.



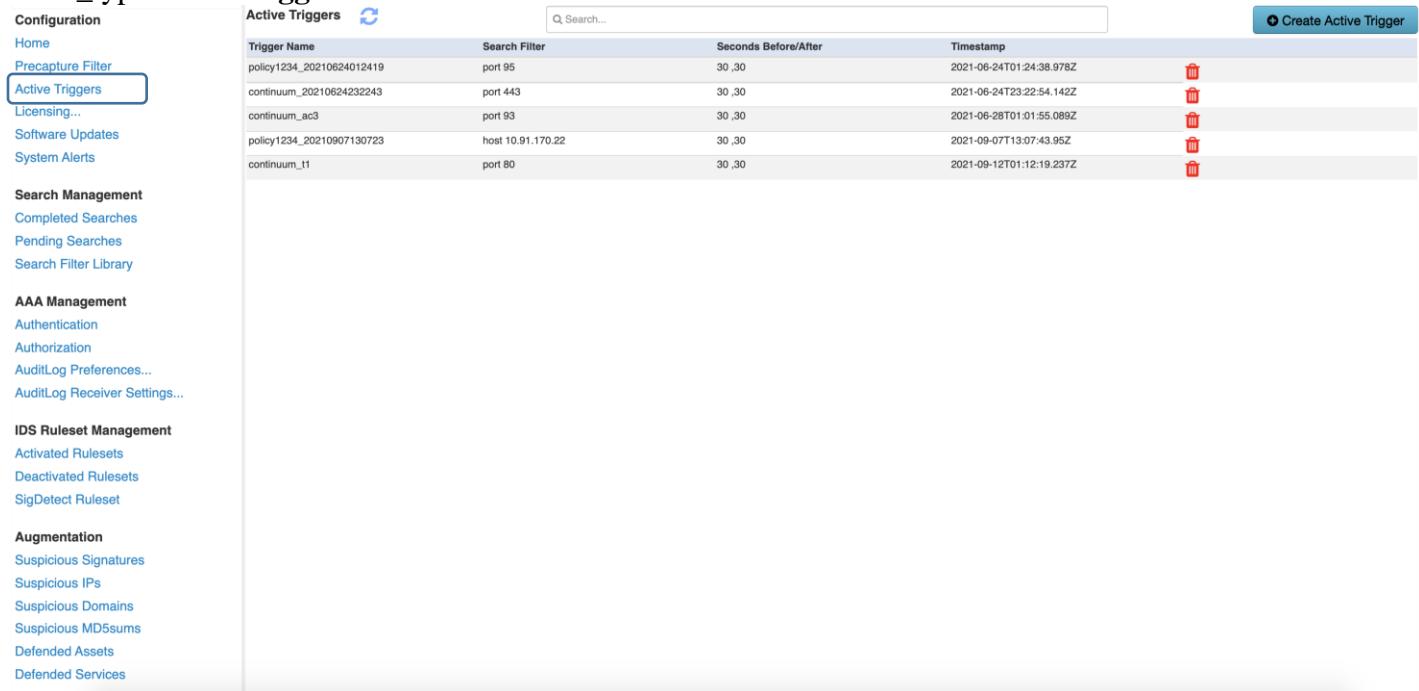
The screenshot shows the "Set PreCapture Filter" dialog box. The filter rule entered is "port 53 or port 443". The "Create PreCapture Filter" button is highlighted with a blue border.



The screenshot shows the SentryWire interface with the search bar containing the filter "port 80 or port 53". The filter is highlighted with a blue border.

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**



Trigger Name	Search Filter	Seconds Before/After	Timestamp	Action
policy1234_20210624012419	port 95	30,30	2021-06-24T01:24:38.978Z	
continuum_20210624232243	port 443	30,30	2021-06-24T23:22:54.142Z	
continuum_ac3	port 93	30,30	2021-06-28T01:01:55.089Z	
policy1234_20210907130723	host 10.91.170.22	30,30	2021-09-07T13:07:43.95Z	
continuum_t1	port 80	30,30	2021-09-12T01:12:19.237Z	

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.

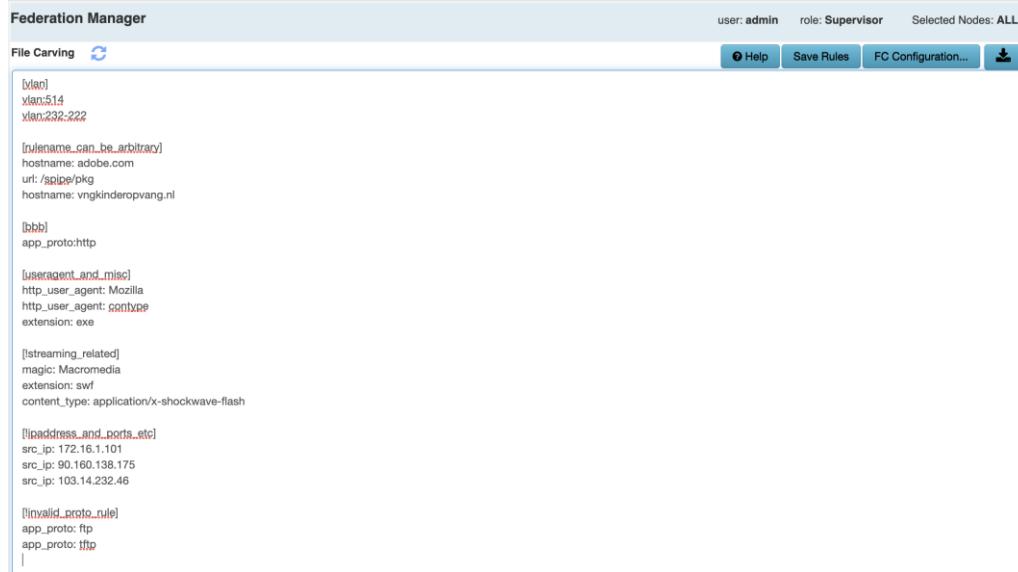
Active trigger name can only have alphanumeric characters and underscore (_). Duplicate names are not allowed.

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.

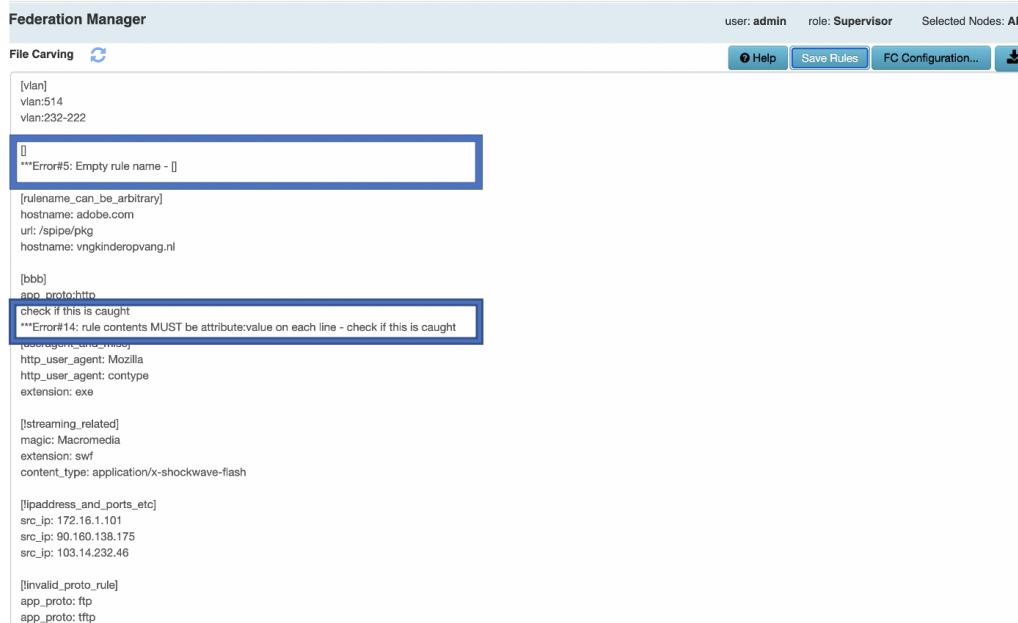
File Carving page allows authorized users to specify file carving rules and save them to the server. If the rules are valid, they are forwarded to each federated node.



This screenshot shows the 'File Carving' section of the SentryWire interface. At the top, there are tabs for 'File Carving' and 'FC Configuration...', along with buttons for 'Help', 'Save Rules', and 'FC Configuration...'. The main area displays a list of file carving rules:

- [vlan]
 - vlan:514
 - vlan:232-222
- [rulename_can_be_arbitrary]
 - hostname: adobe.com
 - url: /spipe/pkg
 - hostname: vngkinderopvang.nl
- [bbb]
 - app_proto:http
- [useragent_and_misc]
 - http_user_agent: Mozilla
 - http_user_agent: contype
 - extension: exe
- [!streaming_related]
 - magic: Macromedia
 - extension: swf
 - content_type: application/x-shockwave-flash
- [!ipaddress_and_ports_etc]
 - src_ip: 172.16.1.101
 - src_ip: 90.160.138.175
 - src_ip: 103.14.232.46
- [!invalid_proto_rule]
 - app_proto: ftp
 - app_proto: tftp

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.



This screenshot shows the same 'File Carving' section as above, but with validation errors highlighted by red boxes:

- A red box surrounds the first rule entry, containing the message: "Error#5: Empty rule name - []".
- A red box surrounds the second rule entry, containing the message: "Error#14: rule contents MUST be attribute:value on each line - check if this is caught".

The rest of the rule list is identical to the one in the first screenshot.

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:
 $rule1 \text{ OR } rule2 \text{ OR } rule3$
- When a rule contains multiple attributes:
 - o 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
 - o 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**:

Three screenshots illustrating the integration of File Carving into the SentryWire Investigator View:

- Dashboard View:** Shows a list of available dashboards, including "FileCarving" which is highlighted with a blue border.
- File Carving Status Code Bar Chart:** A bar chart showing the count of file carving status codes over time. The x-axis represents the timestamp per minute from 19:00 to 19:55. The y-axis represents the count from 0 to 400. A legend indicates two categories: 200 (blue bars) and 503 (red bars). Most bars are blue, with one red bar at approximately 19:45.
- File Carving Log Table:** A detailed log of file carving events. Each row contains a timestamp, session ID, and the file path or identifier being carved. The log shows numerous entries for Nov 14, 2021, with file paths like "10.1.8.160_80_10.1.8.151_2628_328e94df4f351ae79e327c4e5e1c2a54b7c6ddb13bea70ba18f52ec8e37c7ad". The last few rows show entries for Nov 15, 2021, with file paths like "10.1.8.160_80_10.1.8.151_2595_8a6999b4ce2c63330c19ef94bf35adb99b6b9a640034dcdbafa79b3b2391ff".

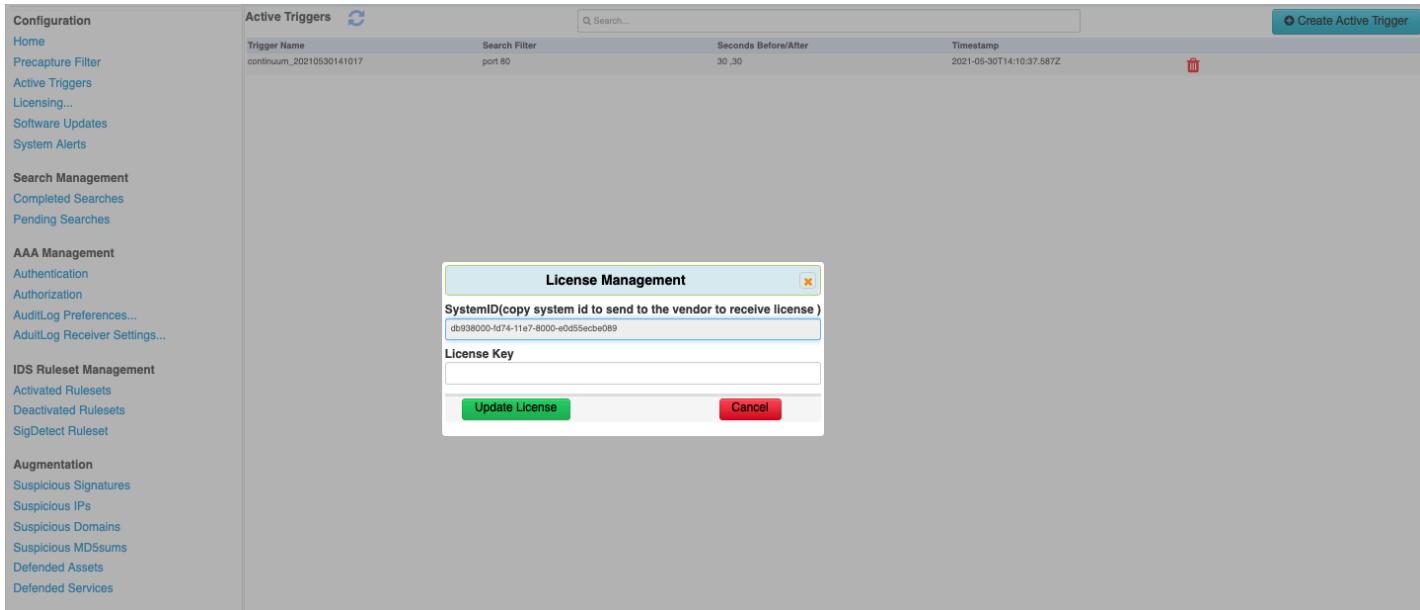
3.1.6 Licensing

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.



The screenshot shows the SentryWire web interface with the following details:

- Left Sidebar (Configuration):**
 - Home
 - Precapture Filter
 - Active Triggers** (selected)
 - Licensing...
 - Software Updates
 - System Alerts
 - Search Management
 - Completed Searches
 - Pending Searches
 - AAA Management
 - Authentication
 - Authorization
 - AuditLog Preferences...
 - AdultLog Receiver Settings...
 - IDS Ruleset Management
 - Activated Rulesets
 - Deactivated Rulesets
 - SigDetect Ruleset
 - Augmentation
 - Suspicious Signatures
 - Suspicious IPs
 - Suspicious Domains
 - Suspicious MD5sums
 - Defended Assets
 - Defended Services
- Active Triggers Tab:**

Trigger Name	Search Filter	Seconds Before/After	Timestamp
continuum_20210530141017	port 80	30 .30	2021-05-30T14:10:37.587Z
- License Management Dialog Box:**

SystemID(copy system id to send to the vendor to receive license)
db938000-1d74-11e7-8000-e0d55ecbe089

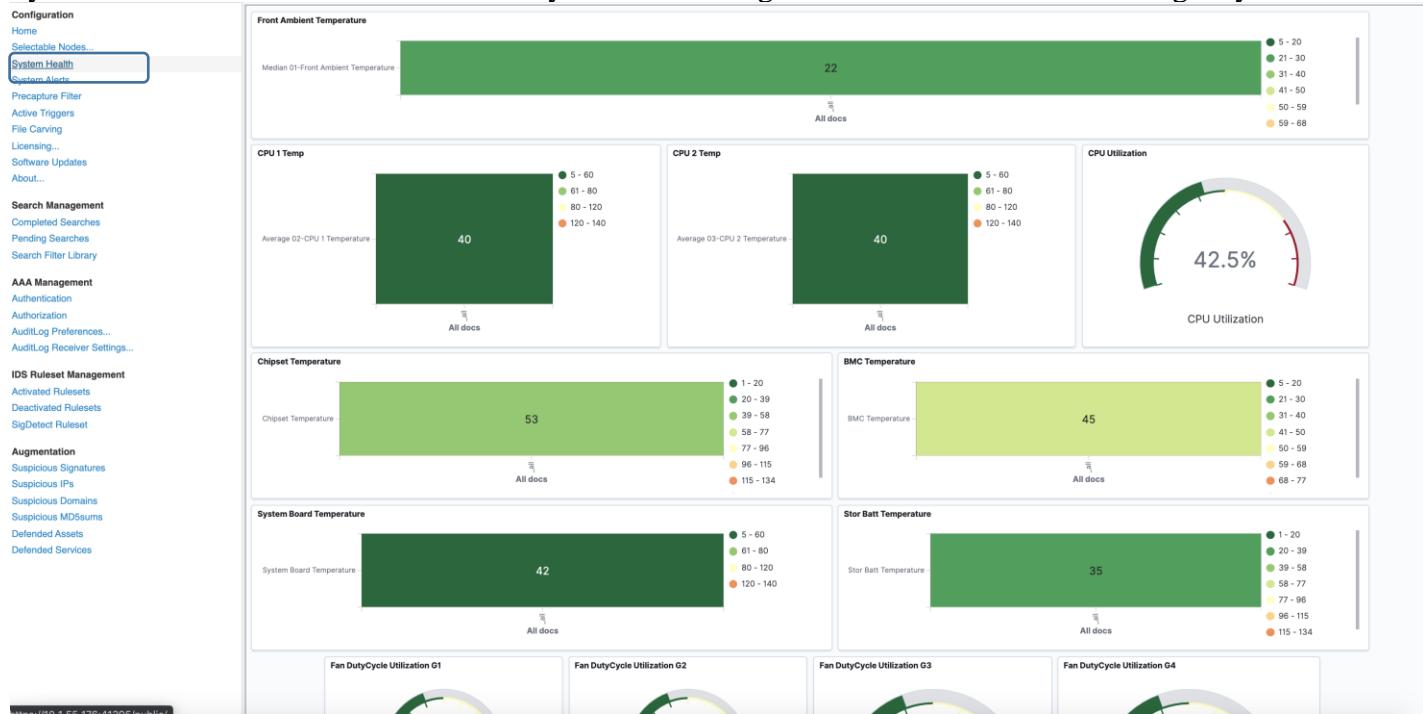
License Key

Buttons: Update License (green), Cancel (red)

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.

Configuration	Software Updates		
	Date	NodeName	Message
Home	2021-11-05T19:03:01	sw146	Received softwareupdate_20211105185455_jpmctest.zip
Selectable Nodes...	2021-11-05T19:03:01	sw146	Updated using softwareupdate_20211105185455_jpmctest.zip
System Health	2021-11-05T19:02:59	sw176	Sending jpmctest.zip to sw146
System Alerts	2021-11-05T18:59:22	sw176	Received softwareupdate_20211105185455_jpmctest.zip
Precapture Filter	2021-11-05T18:59:22	sw176	Updated using softwareupdate_20211105185455_jpmctest.zip
Active Triggers	2021-11-05T18:59:21	sw146	Received softwareupdate_20211105185455_jpmctest.zip
File Carving	2021-11-05T18:59:21	sw146	Updated using softwareupdate_20211105185455_jpmctest.zip
Licensing	2021-11-05T18:59:19	sw176	Sending jpmctest.zip to sw146
Software Updates	2021-11-05T18:59:19	sw176	Sending jpmctest.zip to sw176
About...	2021-11-05T18:46:37	sw176	Received softwareupdate_20211105184607_sw2_adadd_124.zip
Search Management	2021-11-05T18:46:37	sw176	Updated using softwareupdate_20211105184607_sw2_adadd_124.zip
Completed Searches	2021-11-05T18:46:36	sw146	Received softwareupdate_20211105184607_sw2_adadd_124.zip
Pending Searches	2021-11-05T18:46:35	sw146	Updated using softwareupdate_20211105184607_sw2_adadd_124.zip
Search Filter Library	2021-11-05T18:46:35	sw176	Sending sw2_adadd_124.zip to sw146
AAA Management	2021-11-05T18:19:27	sw176	Sending sw2_adadd_124.zip to sw176
Authentication	2021-11-05T18:19:26	sw176	Received softwareupdate_20211105181908_pj2_abc_123.zip
Authorization	2021-11-05T18:19:24	sw146	Updated using softwareupdate_20211105181908_pj2_abc_123.zip
AuditLog Preferences...	2021-11-05T18:19:24	sw176	Sending pj2_abc_123.zip to sw146
AuditLog Receiver Settings...	2021-11-05T18:19:24	sw176	Sending pj2_abc_123.zip to sw176
IDS Ruleset Management	2021-11-05T18:19:24	sw176	Sending pj2_abc_123.zip to sw146
Activated Rulesets	2021-11-05T18:09:22	sw176	Received softwareupdate_20211105180922_pj2_abc_123.zip
Deactivated Rulesets	2021-11-05T18:09:22	sw176	Updated using softwareupdate_20211105180922_pj2_abc_123.zip
SigDetect Ruleset	2021-11-05T18:09:20	sw176	Sending pj2_abc_123.zip to sw146
Augmentation			
Suspicious Signatures			
Suspicious IPs			
Suspicious Domains			
Suspicious MD5sums			
Defended Assets			
Defended Services			

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.

Federation Manager					
System Alerts				Selected Nodes: ALL	
Category	Date	NodeName	Message	Severity	Category
TrafficAlert(4008)	2021-11-18T01:40:36	nc179	searchname: continuum_20211118013503_kv4vv_9tic_eemue, searchfilter:tcp or udp, beginTime:1637198403, endTime:1637199323, result:Pkt<0,Seconds>0	2:Warning	Search
Admin(1)	2021-11-18T01:40:30	nc179	searchname: continuum_20211118013503_kv4vv_9tic_eemue, searchfilter:tcp or udp, beginTime:1637198403, endTime:1637199323	2:Warning	Search
Group(2)	2021-11-18T01:40:26	nc179	searchname: continuum_20211118013523_d4mcf_bmsww, searchfilter:tcp or udp, beginTime:1637198423, endTime:1637199343, result:Pkt<0,Seconds>0	2:Warning	Search
Node(7)	2021-11-18T01:40:25	nc179	searchname: continuum_20211118013503_kv4vv_9tic_lukng, searchfilter:tcp or udp, beginTime:1637198403, endTime:1637199323, result:Pkt<0,Seconds>0	2:Warning	Search
Precapture(1)	2021-11-18T01:40:21	nc179	searchname: continuum_20211118013523_d4mcf_bmsww, searchfilter:tcp or udp, beginTime:1637198423, endTime:1637199343	2:Warning	Search
Activetrigger(2)	2021-11-18T01:40:20	nc179	searchname: continuum_20211118013503_kv4vv_9tic_lukng, searchfilter:tcp or udp, beginTime:1637198403, endTime:1637199323	2:Warning	Search
SoftwareUpdate(59)	2021-11-18T01:39:35	svr146	searchname: continuum_20211118013523_d4mcf_bmsww, searchfilter:tcp or udp, beginTime:1637198403, endTime:1637199323, result:Pkt<0,Seconds>0	2:Warning	Search
Search(249)	2021-11-18T01:39:30	svr146	searchname: continuum_20211118013503_kv4vv_9tic_eemue, searchfilter:tcp or udp, beginTime:1637198403, endTime:1637199323	2:Warning	Search
Authentication(217)	2021-11-18T01:39:30	svr146	searchname: continuum_20211118013523_d4mcf_bmsww, searchfilter:tcp or udp, beginTime:1637198423, endTime:1637199343, result:Pkt<0,Seconds>0	2:Warning	Search
Authorization(0)	2021-11-18T01:39:29	svr146	searchname: continuum_20211118013503_kv4vv_9tic_lukng, searchfilter:tcp or udp, beginTime:1637198403, endTime:1637199323, result:Pkt<0,Seconds>0	2:Warning	Search
IDSRuleset(0)	2021-11-18T01:39:25	svr146	searchname: continuum_20211118013523_d4mcf_bmsww, searchfilter:tcp or udp, beginTime:1637198423, endTime:1637199343	2:Warning	Search
Augmentation(6)	2021-11-18T01:39:24	svr146	searchname: continuum_20211118013503_kv4vv_9tic_lukng, searchfilter:tcp or udp, beginTime:1637198403, endTime:1637199323	2:Warning	Search
	2021-11-18T01:35:55	nc179	searchname: continuum_20211118013503_kv4vv_9tic_eemue, searchfilter:tcp or udp, beginTime:1637198403, endTime:1637199323, result:Pkt<0,Seconds>0	2:Warning	Search
	2021-11-18T01:35:49	nc179	searchname: continuum_20211118013503_kv4vv_9tic_lukng, searchfilter:tcp or udp, beginTime:1637198403, endTime:1637199323	2:Warning	Search
	2021-11-18T01:35:40	nc179	searchname: continuum_20211118013523_d4mcf, searchfilter:tcp or udp, beginTime:1637198423, endTime:1637199343, result:Pkt<0,Seconds>0	2:Warning	Search
	2021-11-18T01:35:34	nc179	searchname: continuum_20211118013523_d4mcf, searchfilter:tcp or udp, beginTime:1637198423, endTime:1637199343	2:Warning	Search
	2021-11-18T01:35:25	nc179	searchname: continuum_20211118013503_kv4vv_9tic_lukng, searchfilter:tcp or udp, beginTime:1637198403, endTime:1637199323, result:Pkt<0,Seconds>0	2:Warning	Search
	2021-11-18T01:35:20	nc179	searchname: continuum_20211118013503_kv4vv_9tic_lukng, searchfilter:tcp or udp, beginTime:1637198403, endTime:1637199323	2:Warning	Search
	2021-11-18T01:34:59	svr146	searchname: continuum_20211118013503_kv4vv_9tic_eemue, searchfilter:tcp or udp, beginTime:1637198403, endTime:1637199323, result:Pkt<0,Seconds>0	2:Warning	Search
	2021-11-18T01:34:54	svr146	searchname: continuum_20211118013503_kv4vv_9tic_eemue, searchfilter:tcp or udp, beginTime:1637198403, endTime:1637199323	2:Warning	Search
	2021-11-18T01:34:44	svr146	searchname: continuum_20211118013523_d4mcf, searchfilter:tcp or udp, beginTime:1637198423, endTime:1637199343, result:Pkt<0,Seconds>0	2:Warning	Search
	2021-11-18T01:34:40	nc179	searchname: continuum_20211118013423_520n, searchfilter:tcp or udp, beginTime:1637198363, endTime:1637199283, result:Pkt<0,Seconds>0	2:Warning	Search
	2021-11-18T01:34:39	svr146	searchname: continuum_20211118013523_d4mcf, searchfilter:tcp or udp, beginTime:1637198423, endTime:1637199343	2:Warning	Search

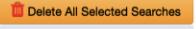
The search bar allows narrowing down alerts by date, nodename, severity, category, and terms inside the message. Any authorized user can download System Alerts. These cannot be deleted.

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

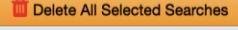
Completed searches from all the Federated Nodes are displayed on this page. Search name contains name of the user who created the search. Each node's search returns different set of packets; therefore, they are represented as a separate line.

Configuration	Completed Searches							
	NodeName	SearchName	Begin Time	End Time	SearchFilter	MaxPkts	SearchResult	
Home	nc179	continuum_1631381920_1_rest2	2021-09-11 10:00:00	2021-09-11 12:00:00	tcp	1000		
Precapture Filter	sw146	continuum_1631381920_1_rest2	2021-09-11 10:00:00	2021-09-11 12:00:00	tcp	1000	Pkts=1151 Seconds=5 TotalSize=591KB	
Active Triggers	sw146	continuum_1631377579_1_rest2	2021-09-11 10:00:00	2021-09-11 12:00:00	PcapData.tcp	1000	Pkts=1151 Seconds=6 TotalSize=591KB	
Licensing...	nc179	continuum_1631377579_1_rest2	2021-09-11 10:00:00	2021-09-11 12:00:00	PcapData.tcp	1000		
Software Updates	nc179	continuum_1631351542_1_rest1	2021-09-10 13:30	2021-09-10 14:00	PcapData.tcp	10000		
System Alerts	sw146	continuum_1631351542_1_rest1	2021-09-10 13:30	2021-09-10 14:00	PcapData.tcp	10000		
Search Management	sw146	continuum_20210910010817_clix2	2021-09-09 00:53:17	2021-09-10 01:08:17	port 80	1000000	Pkts=11501 Seconds=4 TotalSize=1MB	
Completed Searches	nc179	continuum_1631091788_3_RESTPooja1	2021-09-04 12:00:00	2021-09-04 12:00:00	PcapData.tcp	1000	Pkts=25 Seconds=6 TotalSize=3KB	
Pending Searches	nc179	continuum_1630731446_2_RESTPooja_jmryhm	2021-09-04 12:00:00	2021-09-04 12:00:00	PcapData.tcp	1000	Pkts=25 Seconds=6 TotalSize=3KB	
Search Filter Library	nc179	continuum_1630731446_2_RESTPooja	2021-09-04 12:00:00	2021-09-04 12:00:00	PcapData.tcp	1000		
AAA Management	nc179	continuum_20210902195732_5fdp9_r2awo_zb2r_d4r35_0ktq_ej	2021-09-02 23:42:32	2021-09-02 23:42:32	udp[0:2] = 0x0223	1000		
Authentication	nc179	continuum_20210902195732_5fdp9_qa5dd_xqvgs	2021-09-02 19:42:32	2021-09-02 19:57:32	udp[0:2] = 0x0223	1000		
Authorization	nc179	continuum_20210902195732_5fdp9_r2awo_zb2r_d4r35_0ktq	2021-09-02 19:42:32	2021-09-02 19:57:32	ip6[39:2] = 0x0223	1000	NoPcapData	
AuditLog Preferences...	nc179	continuum_20210902195732_5fdp9_74kyj	2021-09-02 19:42:32	2021-09-02 19:57:32	udp[0:2] = 0x0223	1000	NoPcapData	
AuditLog Receiver Settings...	nc179	continuum_20210902195732_5fdp9_qa5dd	2021-09-02 19:42:32	2021-09-02 19:57:32	udp[0:2] = 0x0003	1000	NoPcapData	
IDS Ruleset Management	nc179	continuum_20210902195732_5fdp9_r2awo_zb2r_d4r35	2021-09-02 19:42:32	2021-09-02 19:57:32	ip6[0:2] = 0x6000	1000	Pkts=140 Seconds=6 TotalSize=18KB	
Activated Rulesets	nc179	continuum_20210902195732_5fdp9_r2awo_zb2r	2021-09-02 19:42:32	2021-09-02 19:57:32	ip6 [0:2] = 0x86d0	1000	NoPcapData	
Deactivated Rulesets	nc179	continuum_20210902195732_5fdp9_r2awo	2021-09-02 19:42:32	2021-09-02 19:57:32	udp	1000	Pkts=245 Seconds=5 TotalSize=76KB	
SigDetect Ruleset	nc179	continuum_20210902195732_5fdp9	2021-09-02 19:42:32	2021-09-02 19:57:32	udp[0:2] = 0x0222	10000	NoPcapData	
Augmentation	nc179	continuum_20210902195448_v8a2g	2021-09-02 23:39:48	2021-09-02 23:54:40	tcp[20:4] = 0x48545450 and (not port 80)	10000		
Suspicious Signatures	nc179	continuum_20210902195213_ftfl	2021-09-02 19:37:13	2021-09-02 19:52:13	udp[20:4] = 0x63350103	10000	Pkts=49 Seconds=5 TotalSize=23KB	
Suspicious IPs	nc179	continuum_1630595608_1_REST3	2021-09-01 10:00:00	2021-09-01 10:20:00	tcp	1000	Pkts=1151 Seconds=5 TotalSize=55KB	
Suspicious Domains	nc179	continuum_20210902112233_i27g_yikd_dgrw_w_1pl5c_x3yia_fff	2021-09-02 11:21:55	2021-09-02 13:00:50	ip6[0:2] & 0x0222 = 1	1000	NoPcapData	
Suspicious MD5sums	nc179	continuum_20210902112233_i27g_yikd_dgrw_w_1pl5c_x3yia_fff	2021-09-02 11:21:55	2021-09-02 13:00:50	ip6 and udp[0:2] == 0x0222	1000	NoPcapData	
Defended Assets	nc179	continuum_20210902112233_i27g_yikd_dgrw_w_1pl5c_x3yia_fff	2021-09-02 11:21:55	2021-09-02 13:00:50	udp[0:2] == 0x0222	1000	NoPcapData	
Defended Services	nc179	continuum_20210902112233_i27g_yikd_dgrw_w_1pl5c_x3yia_fff	2021-09-02 11:21:55	2021-09-02 13:00:50	udp[0:2] == 0x0222	1000	NoPcapData	

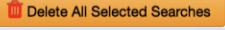
The Search bar is critical in narrowing down the results to view and delete searches.

Few examples of the search bar usage:

Show only cancelled searches:

Completed Searches							
NodeName	SearchName	Begin Time	End Time	SearchFilter	MaxPkts	SearchResult	
nc186	continuum_20210608115824_oh2oi	2021-06-08 11:43:24	2021-06-08 11:56:24	tcp or udp		Cancelled	

Show searches that were done on a particular day:

Completed Searches							
NodeName	SearchName	Begin Time	End Time	SearchFilter	MaxPkts	SearchResult	
nc186	continuum_20210607210332_mifmw	2021-06-07 20:44:32	2021-06-07 21:03:32	port 80	100000	Pkts=176376 Seconds=12 TotalSize=120MB	
nc186	continuum_20210607205905_sgz4d	2021-06-07 20:44:05	2021-06-07 20:51:05	tcp or udp	10000	Pkts=11501 Seconds=10 TotalSize=5MB	
nc186	continuum_20210607200448_y9bef	2021-06-07 19:49:48	2021-06-07 20:04:48	tcp or udp	10000	Pkts=11501 Seconds=16 TotalSize=5MB	

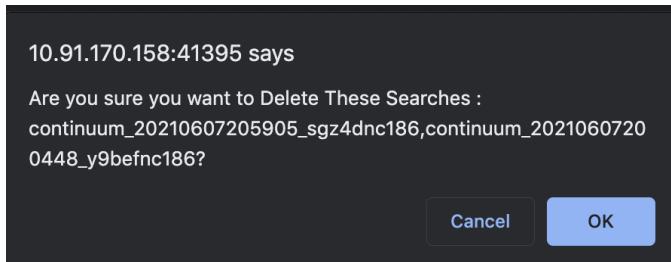
Show searches of a particular user:

Completed Searches		Search Bar						Delete All Selected Searches
NodeName	SearchName		Begin Time	End Time	SearchFilter	MaxPkts	SearchResult	
<input type="checkbox"/> nc186	poluser1_20210608114552_p512e	poluser1	2021-06-08 11:30:52	2021-06-08 11:45:52	tcp or udp	10000	Pkts=11501 Seconds=13 TotalSize=6MB	

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:

Federation Manager							user: continuum	role: Admin	authenticationmode: local	version: 408.14r2.1
Completed Searches		Search Bar						Delete All Selected Searches		
NodeName	SearchName		Begin Time	End Time	SearchFilter	MaxPkts	SearchResult			
<input type="checkbox"/> nc186	continuum_20210607210332_mifmw		2021-06-07 20:44:32	2021-06-07 21:05:32	port 80	100000	Pkts=176376 Seconds=12 TotalSize=120MB			
<input checked="" type="checkbox"/> nc186	continuum_20210607205905_sgz24d		2021-06-07 20:44:05	2021-06-07 20:51:05	tcp or udp	10000	Pkts=11501 Seconds=10 TotalSize=5MB			
<input checked="" type="checkbox"/> nc186	continuum_20210607200448_y9bef		2021-06-07 19:49:48	2021-06-07 20:04:48	tcp or udp	10000	Pkts=11501 Seconds=16 TotalSize=5MB			

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



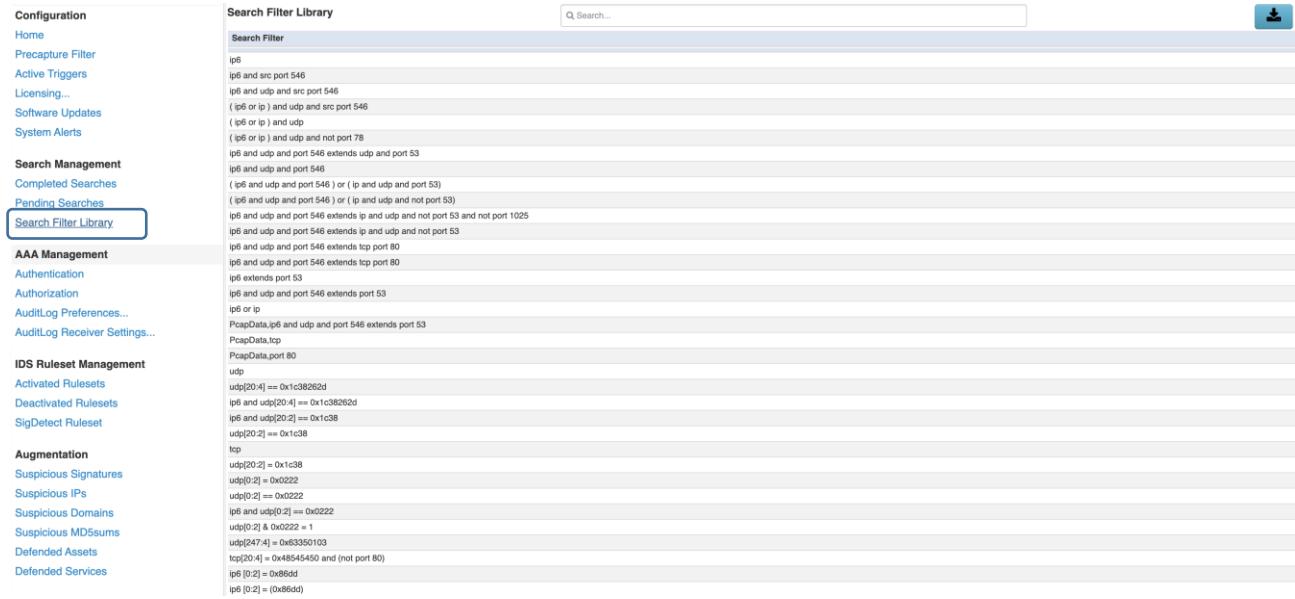
3.2.2 Pending Searches

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.

Federation Manager						user: continuum	role: Admin	authenticationmode: local	version: 408.14r2.1
Pending Searches		Search Bar						Delete	
Node Name	Search Name		Begin Time	End Time	Search Filter	Search Status			
nc186	continuum_20210608121958_ldnxq		2021-06-08 12:04:58	2021-06-08 12:19:58	PcapData, port 80	Pending			

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.



The screenshot shows a list of search filters in a table format. The columns include RoleName, Groups, Policy, Licensing, Authentication, Authorization, Auditing, and Search. A 'Create Role' button is located at the top right of the table area. The filters listed are:

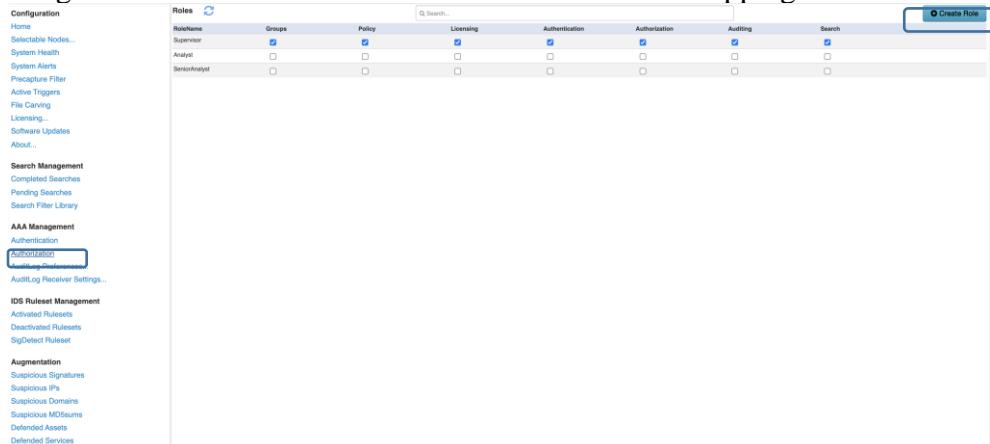
RoleName	Groups	Policy	Licensing	Authentication	Authorization	Auditing	Search
Supervisor	<input checked="" type="checkbox"/>						
Analyst	<input type="checkbox"/>						
SeniorAnalyst	<input type="checkbox"/>						

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.



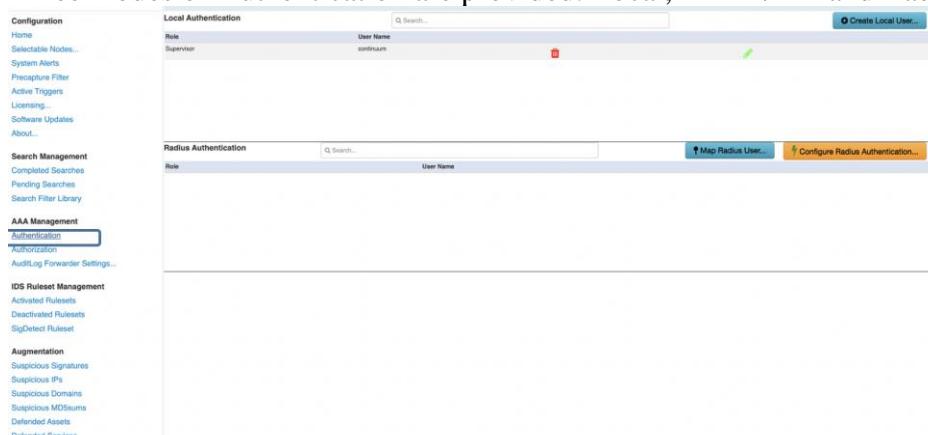
The screenshot shows a table of roles with checkboxes for various permissions. A 'Create Role' button is located at the top right of the table area. The roles listed are:

RoleName	Groups	Policy	Licensing	Authentication	Authorization	Auditing	Search
Supervisor	<input checked="" type="checkbox"/>						
Analyst	<input type="checkbox"/>						
SeniorAnalyst	<input type="checkbox"/>						

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

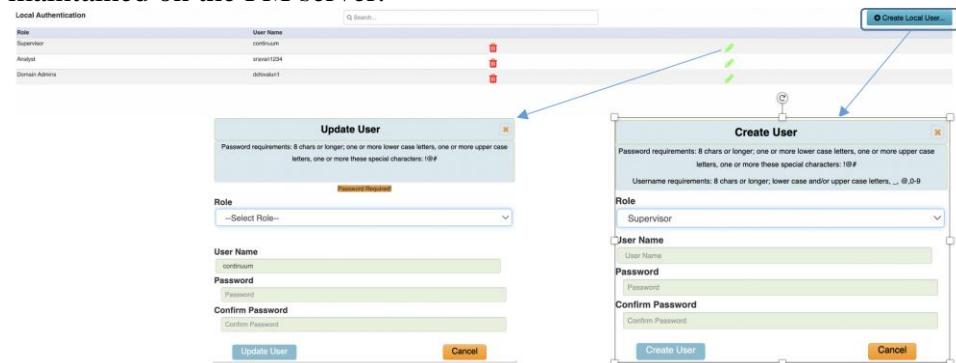
Three modes of Authentication are provided: Local, LDAP/AD and Radius authentication



The screenshot shows the SentryWire configuration interface. On the left, there's a sidebar with various management sections like Configuration, Search Management, AAA Management, IDS Ruleset Management, and Augmentation. The AAA Management section has 'Authentication' selected. The main area has two tabs: 'Local Authentication' and 'Radius Authentication'. In the Local Authentication tab, there's a table with columns 'Role' (Supervisor) and 'User Name' (continuum). In the Radius Authentication tab, there's a table with columns 'Role' (Supervisor) and 'User Name' (continuum). Buttons for 'Create Local User...' and 'Map Radius User...' are visible.

Local Authentication

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



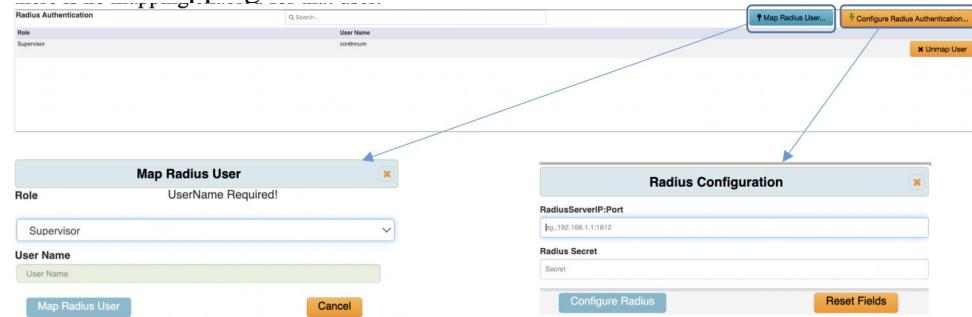
This screenshot shows the Local Authentication interface. It includes a 'Create User' dialog and an 'Update User' dialog. Both dialogs require a 'User Name' (continuum), 'Password', and 'Confirm Password'. The 'Create User' dialog also has a 'Role' dropdown set to 'Supervisor'. Arrows point from the 'Create User' and 'Update User' dialogs back to the main Local Authentication table.

LDAP/AD Authentication

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

Radius Authentication

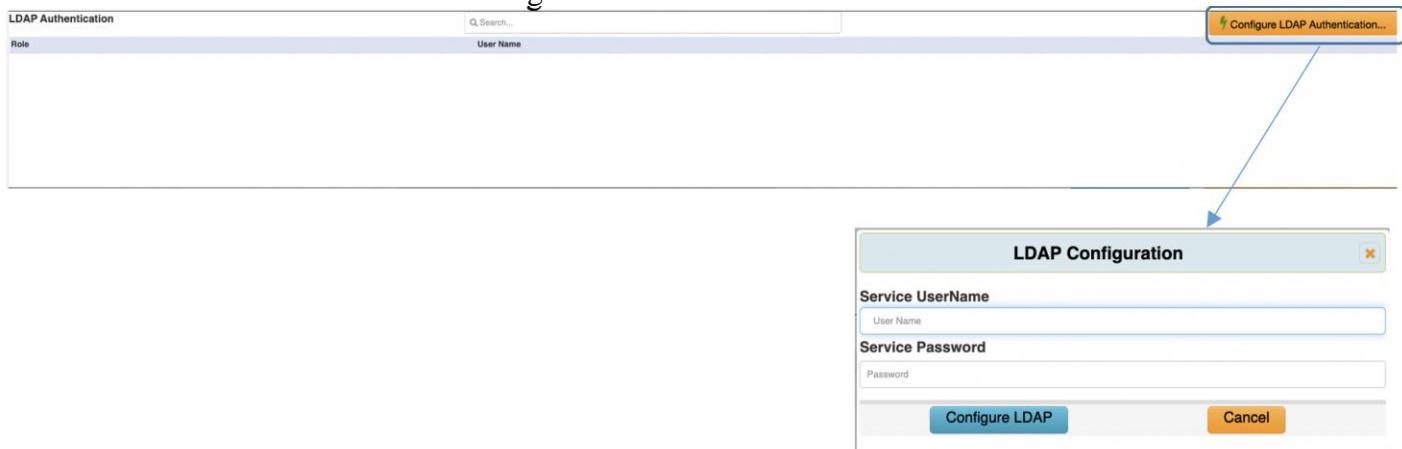
Radius authentication requires IP:Port of the radius server and the Radius secret string to be configured. FM server uses this information to authenticate Radius users at login time. MapUser allows a Radius user to be mapped to a FM role. The image shows one Radius mapped user named continuum mapped 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.



This screenshot shows the Radius Authentication interface. It includes a 'Map Radius User' dialog and a 'Radius Configuration' dialog. The 'Map Radius User' dialog has a 'Role' dropdown set to 'Supervisor' and a 'User Name' input field. The 'Radius Configuration' dialog has fields for 'RadiusServerIP:Port' (192.168.1.1:1812) and 'Radius Secret' (Secret). Arrows point from the 'Map Radius User' and 'Radius Configuration' dialogs back to the main Radius Authentication table.

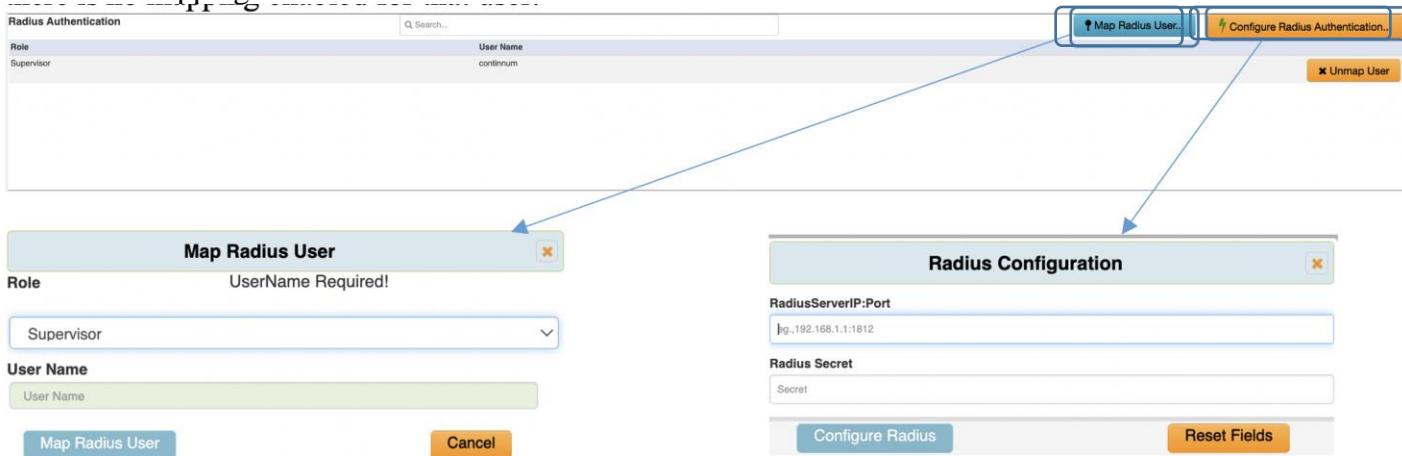
LDAP Authentication

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.



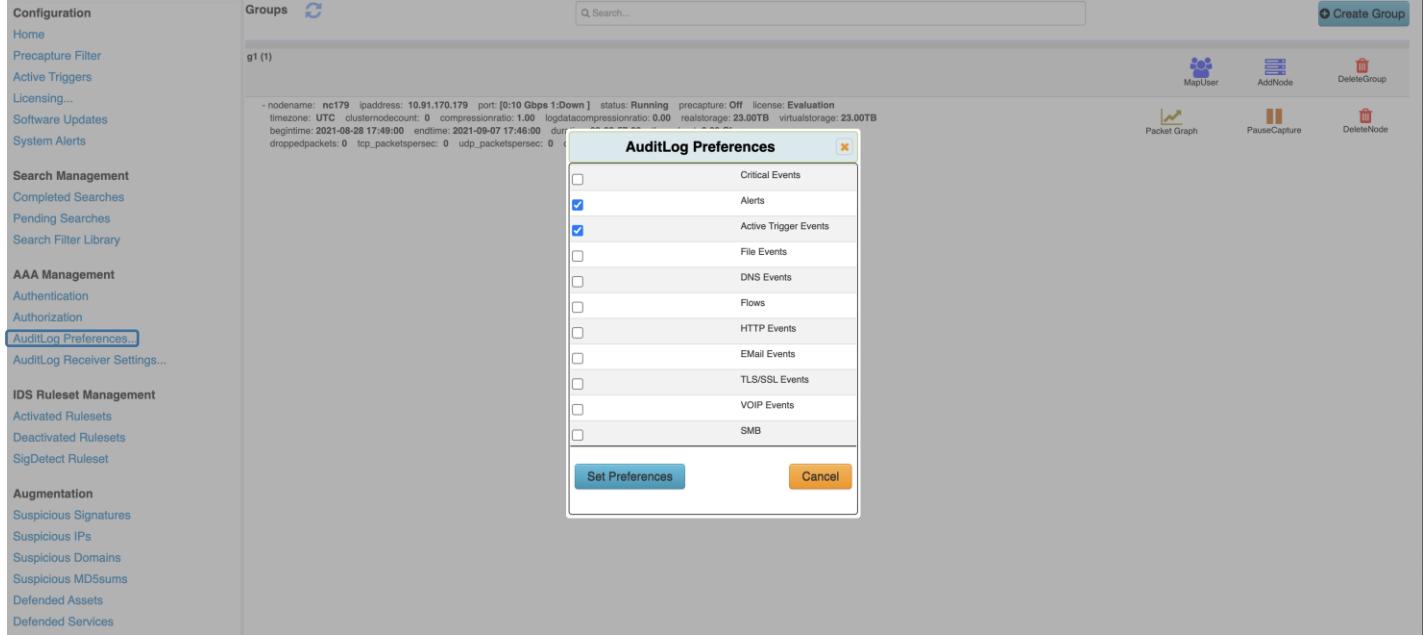
Radius Authentication

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

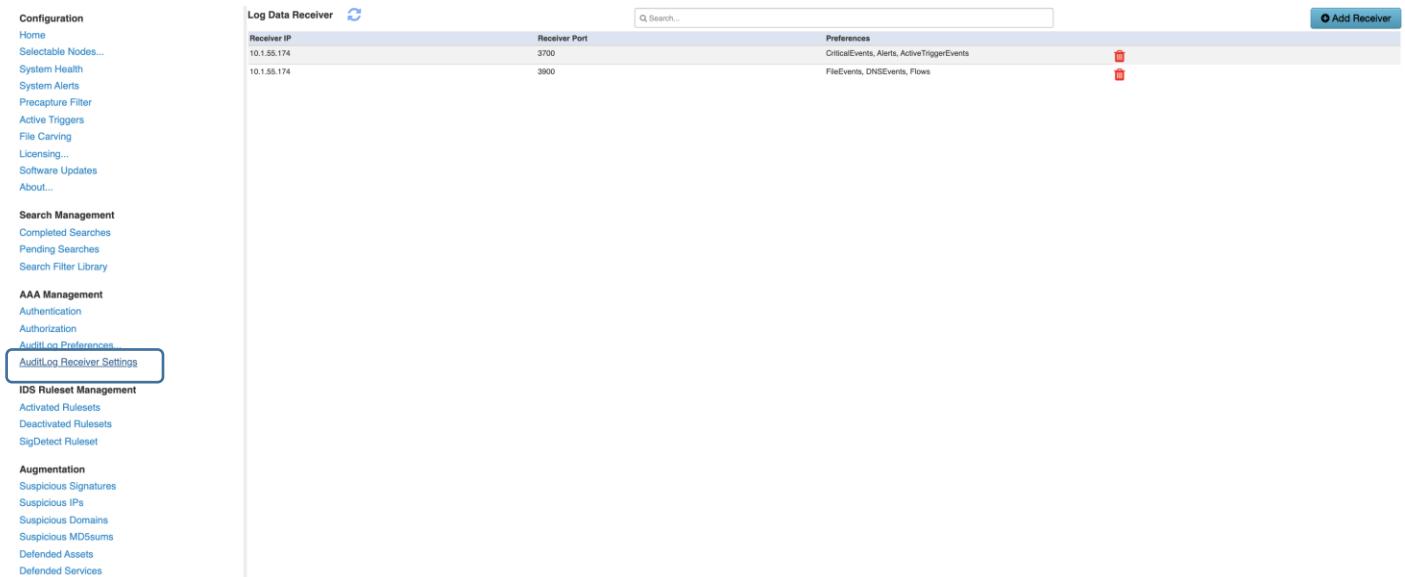
Logs of various event types are generated by the capture and analytics servers. Auditlog Preferences dialog box allows users to indicate which of the logs must be made available to the external applications such as Splunk.



The screenshot shows the SentryWire interface with the 'AuditLog Preferences' dialog box open. The left sidebar contains navigation links for Configuration, Home, Precapture Filter, Active Triggers, Licensing, Software Updates, System Alerts, Search Management, AAA Management, IDS Ruleset Management, Augmentation, and AuditLog Receiver Settings. The 'AuditLog Preferences' link is highlighted with a blue border. The main area displays a group named 'g1 (1)' with detailed node information and a list of audit log preferences. The 'AuditLog Preferences' dialog box lists various event types: Critical Events, Alerts, Active Trigger Events, File Events, DNS Events, Flows, HTTP Events, EMail Events, TLS/SSL Events, VOIP Events, and SMB. Each item has a checkbox next to it, with 'Alerts', 'Active Trigger Events', and 'File Events' checked. At the bottom of the dialog are 'Set Preferences' and 'Cancel' buttons.

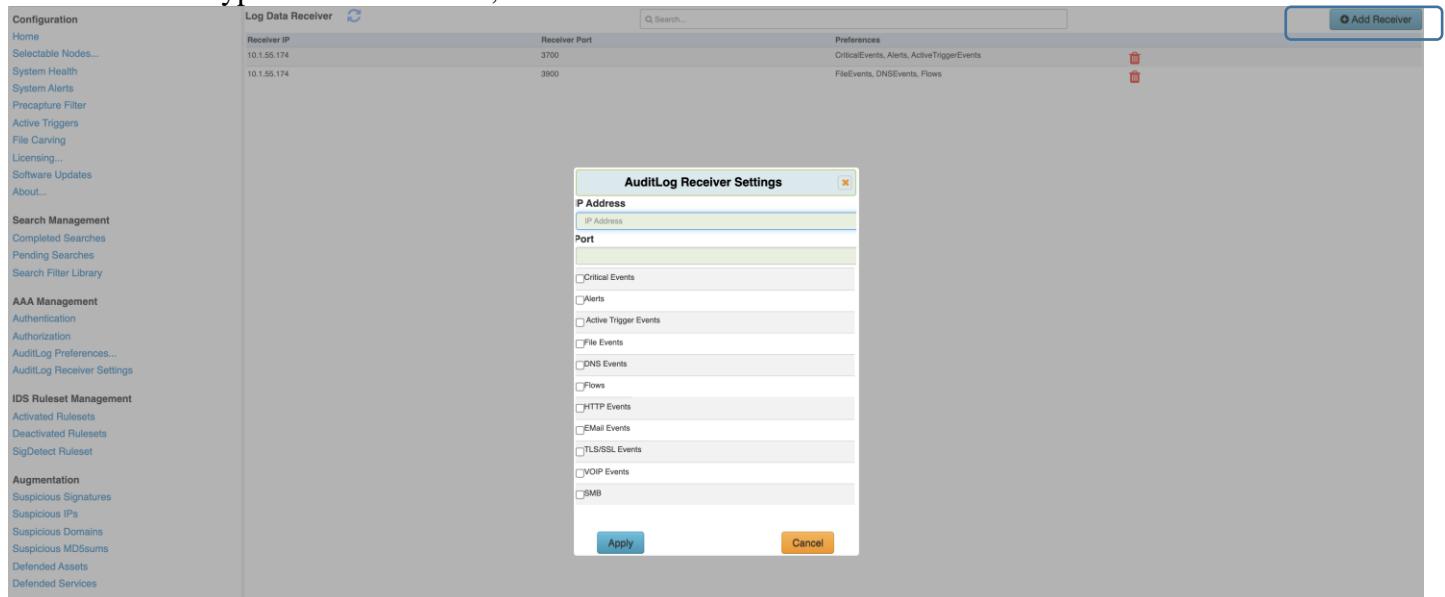
3.3.4 Auditlog Receiver Settings

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.



The screenshot shows the SentryWire interface with the 'Log Data Receiver' dialog box open. The left sidebar contains navigation links for Configuration, Home, Selectable Nodes..., System Health, System Alerts, Precapture Filter, Active Triggers, File Carving, Licensing..., Software Updates, About..., Search Management, AAA Management, and AuditLog Receiver Settings. The 'AuditLog Receiver Settings' link is highlighted with a blue border. The main area displays a table of log data receivers with columns for Receiver IP, Receiver Port, and Preferences. Two entries are listed: one for 10.1.55.174 port 3700 with preferences 'CriticalEvents, Alerts, ActiveTriggerEvents' and another for 10.1.55.174 port 3900 with preferences 'FileEvents, DNSEvents, Flows'. At the top right of the dialog is an 'Add Receiver' button.

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.



The screenshot shows the SentryWire interface with the 'Log Data Receiver' configuration page. On the left, there is a sidebar with various menu items such as Home, Selectable Nodes, System Health, System Alerts, PreCapture Filter, Active Triggers, File Carving, Licensing, Software Updates, About, Search Management, AAA Management, IDS Ruleset Management, Augmentation, and more. The main area displays two rows of receiver configurations: one with Receiver IP 10.1.55.174 and Port 3700, and another with Receiver IP 10.1.55.174 and Port 3900. A search bar is at the top right. A blue 'Add Receiver' button is located in the top right corner of the main area. A modal window titled 'AuditLog Receiver Settings' is open in the center, containing fields for 'IP Address' (10.1.55.174) and 'Port' (3700). Below these are several checkboxes for selecting event types: Critical Events, Alerts, Active Trigger Events, File Events, DNS Events, Flows, HTTP Events, eMail Events, TLS/SSL Events, VOIP Events, and SMB. At the bottom of the modal are 'Apply' and 'Cancel' buttons.

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.

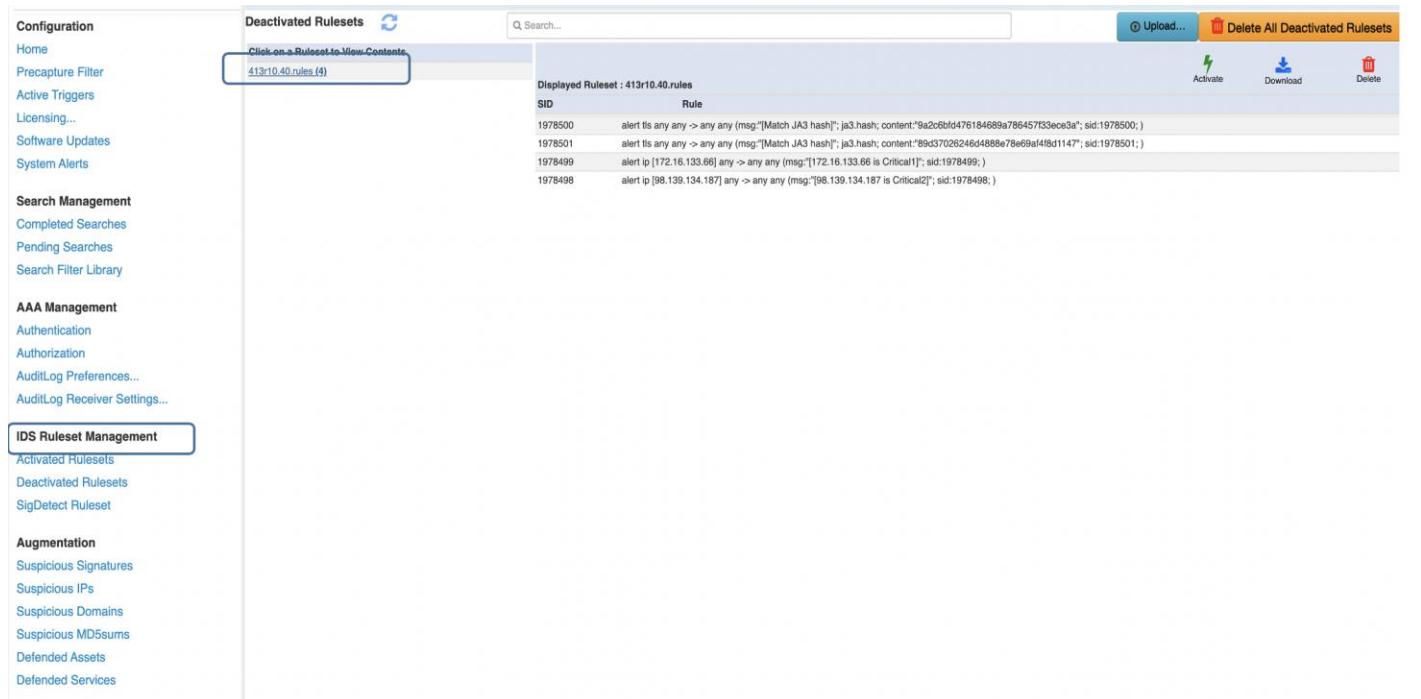
- Click on a activated ruleset to see its contents. The following image shows contents of a ruleset named activebunk2.rules file.
- Select a ruleset and click on Deactivate button. This ruleset will move to Deactivated Rulesets page. Each node removes the new ruleset from Suricata alert generation.
- 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	Activated Rulesets 	Activated Rulesets 	
		Displayed Ruleset : activex.rules	
Home	Click on a Ruleset to View Contents	Q Search...	
Precapture Filter	3coresec.rules (20)		
Active Triggers	activex.rules (732)		
Licensing...	adware_pup.rules (237)		
Software Updates	attack_response.rules (299)		
System Alerts	botcc.portgrouped.rules (0)		
Search Management	botcc.rules (24)		
Completed Searches	chat.rules (104)		
Pending Searches	ciamry.rules (100)		
Search Filter Library	coiminer.rules (4464)		
AAA Management	compromised.rules (93)		
Authentication	current_events.rules (190)		
Authorization	dns.rules (59)		
AuditLog Preferences...	dos.rules (214)		
AuditLog Receiver Settings...	drop.rules (41)		
IDS Ruleset Management	dshield.rules (1)		
Activated Rulesets	exploit_kit.rules (1643)		
Deactivated Rulesets	exploit.rules (2449)		
SigDetect Ruleset	ftp.rules (121)		
Augmentation	games.rules (96)		
Suspicious Signatures	hunting.rules (773)		
Suspicious IPs	icmp_info.rules (66)		
Suspicious Domains	icmp.rules (39)		
Suspicious MD5sums	imap.rules (41)		
Defended Assets	inappropriate.rules (25)		
Defended Services	info.rules (847)		
ja3.rules (139)	ja3.rules (139)		
malware.rules (26853)	malware.rules (26853)		
misc.rules (63)	misc.rules (63)		
mobile_malware.rules (4770)	mobile_malware.rules (4770)		
netbios.rules (732)	netbios.rules (732)		
p2p.rules (122)	netbios.rules (732)		
phishing.rules (9630)	phishing.rules (9630)		
policy.rules (2024)	policy.rules (2024)		
pop3.rules (26)	pop3.rules (26)		
rpc.rules (126)	rpc.rules (126)		

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 413r10.40.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.

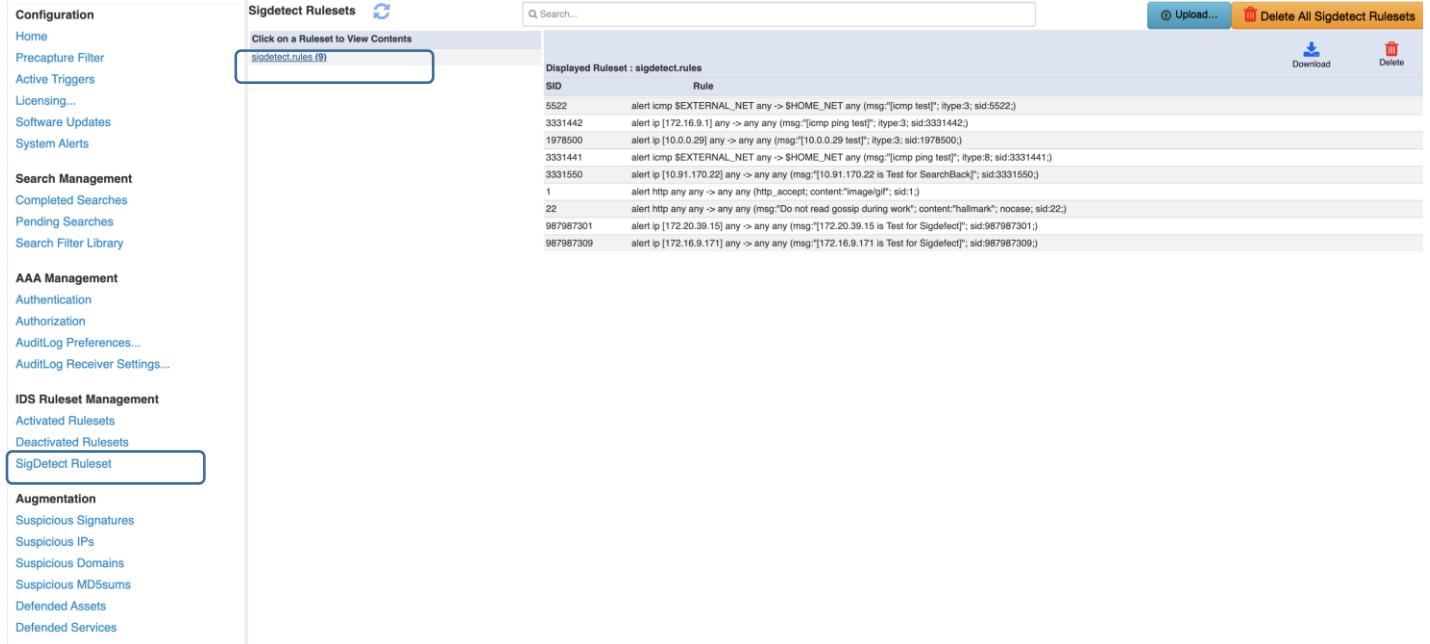


SID	Rule
1978500	alert ts any any -> any any (msg:"[Match JA3 hash]"; ja3.hash; content:"9a2c6bfd476184689a786457f33ece3a"; sid:1978500;)
1978501	alert ts any any -> any any (msg:"[Match JA3 hash]"; ja3.hash; content:"89d37026246d4888e78e69a4f8d1147"; sid:1978501;)
1978499	alert ip [172.16.133.66] any -> any any (msg:[172.16.133.66 is Critical1]; sid:1978499;)
1978498	alert ip [98.139.134.187] any -> any any (msg:[98.139.134.187 is Critical2]; sid:1978498;)

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 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.



SID	Rule
5522	alert icmp \$EXTERNAL_NET any -> \$HOME_NET any (msg:"[icmp test]"; itype:3; sid:5522;)
3331442	alert ip [172.16.9.1] any -> any any (msg:"[icmp ping test]"; itype:3; sid:3331442;)
1978500	alert ip [10.0.0.29] any -> any any (msg:"[10.0.0.29 test]"; itype:3; sid:1978500;)
3331441	alert icmp \$EXTERNAL_NET any -> \$HOME_NET any (msg:"[icmp ping test]"; itype:8; sid:3331441;)
3331550	alert ip [10.91.170.22] any -> any any (msg:"[10.91.170.22 is Test for SearchBack]"; sid:3331550;)
1	alert http any any -> any any (http.accept; content:"image/gif"; sid:1;)
22	alert http any any -> any any (msg:"Do not read gossip during work"; content:"hallmark"; nocase; sid:22;)
987987301	alert ip [172.20.39.15] any -> any any (msg:"[172.20.39.15 is Test for Sigdetect]"; sid:987987301;)
987987309	alert ip [172.16.9.171] any -> any any (msg:"[172.16.9.171 is Test for Sigdetect]"; sid:987987309;)

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.

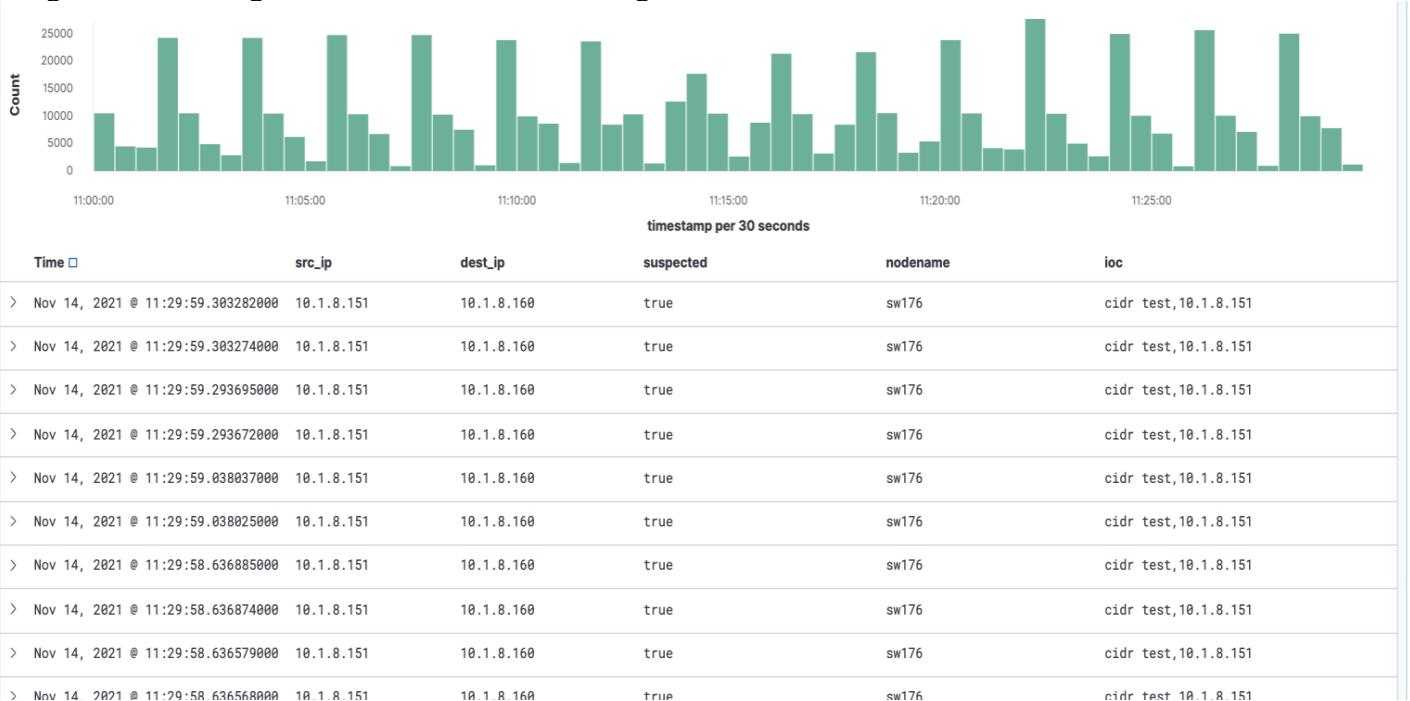
- Suspicious Signatures
- Suspicious Ips
- Suspicious Domains
- Suspicious MD5sums
- Defended Assets
- Defended Services

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:



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**.

Configuration	SuspiciousSignatures 	Description	  
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			

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,deedeeefb|zero
```

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**.

Configuration	Suspicious IPs	Description
Home	SuspIP	
Precapture Filter	1.1.11.201	AI_202108.50.Malware Distribution
Active Triggers	1.2.67.208	babu2345
Licensing...	1.1.73.235	babu2346
Software Updates	1.2.102.135	babu2346
System Alerts	1.1.85.118	babu2346
	1.1.86.166	babu2346
	10.1.2.3	asdad
Search Management	192.168.1.1	susp ip1
Completed Searches	10.1.8.160	babu2222
Pending Searches	163.176.1.100	babu2222
Search Filter Library	224.0.0.252	babu2222
AAA Management	1.1.111.201	babu2345
Authentication	1.2.67.208	babu2346
Authorization	1.1.73.235	babu2346
AuditLog Preferences...	1.2.102.135	babu2346
AuditLog Receiver Settings...	1.1.85.118	babu2346
	172.16.139.250	babu2346
	172.16.133.132	dc1223
	207.171.163.14	dc1223
IDS Ruleset Management		
Activated Rulesets		
Deactivated Rulesets		
SigDetect Ruleset		
Augmentation		
Suspicious Signatures		
Suspicious IPs		
Suspicious Domains		
Suspicious MD5sums		
Defended Assets		
Defended Services		

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

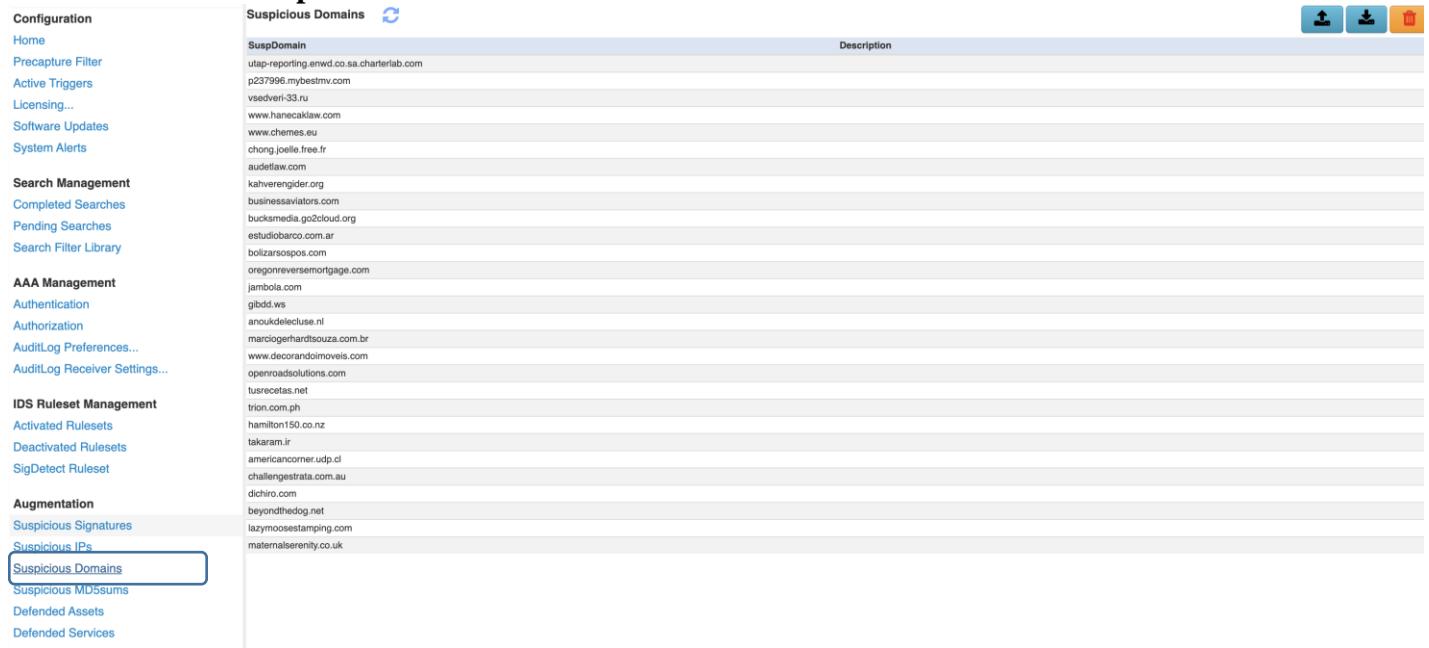
Currently available suspicious IP Addresses can be downloaded () by any authorized user.

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:



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**



SuspDomain	Description
utap-reporting.enwd.co.sa.charterlab.com	
p237996.mybestmv.com	
vsedveri-33.ru	
www.hanecaklaw.com	
www.chemes.eu	
chong.joelle.free.fr	
audetlaw.com	
kahverengider.org	
businessaviators.com	
bucksmedia.go2cloud.org	
estudiobarco.com.ar	
bolizarsospo.com	
oregonversemortgage.com	
jambola.com	
gibdd.ws	
anoudeldeuse.nl	
marcogerhardtouza.com.br	
www.decorandomovels.com	
openroadsolutions.com	
tusrecetas.net	
trion.com.ph	
hamilton150.co.nz	
takaram.ir	
americancorner_udp.cl	
challengestrata.com.au	
dichiro.com	
beyondthedog.net	
lazymousestamping.com	
maternalserenity.co.uk	

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.

Configuration	Suspicious MD5sums	Description
Home		
Precapture Filter	bff56ce49dd485d195fdfa0a02342568	white
Active Triggers	9f01c5a28b93d36a11cb84e9761dc535	robo
Licensing...	907cf1b6d6b7e2a6ad0ed46348f400b9	aspx
Software Updates	21e7f5f5ccf3ed464a964a228dc94d65	
System Alerts	868977d0e4fc052edcb4dedcbc8e9c51b	
	0b6039f65b5a0015e3b3e37b0cbbc6	
	ace7c06d18d0a2ad5d0d9b2d36922825d	
Search Management	5aa907731a03af160a45ec3050cf40a2	Heodo
Completed Searches	973eb0b20c62c0ebb87e56ff0c141a1	Heodo
Pending Searches	7197c3b9b14a4a192d627d27b5eb000a	Heodo
	a02507baefec1929a3e43e2d409158	Heodo
AAA Management	a49dd325a6c686a8325319f19bf8b0ae0	Heodo
Authentication	a51cb71eb049e3797a40b573b421fa	Heodo
Authorization	a0a96bbb99dd5a46cd338b3f5330e5b3	Heodo
AuditLog Preferences...	54bae4a4ef4e461f8a77199485ede11e	Heodo
AuditLog Receiver Settings...	675f13cf69de4400be60c51407b0fc1	Heodo
IDS Ruleset Management	d330a103fb36b659f17d5448efa5dd0	Heodo
Activated Rulesets	654d88b56278f3219bf7713ad6a16	Heodo
Deactivated Rulesets	c14a5526ae569b0cc30641c46d941bf3	Heodo
SigDetect Ruleset	7d11e9755e8009d81cb286149c025eb	Heodo
	a1b429cd806b599421df7ea59a200cb	Heodo
Augmentation	a4b6fffeef9c278daac263606c5449	Heodo
Suspicious Signatures	a067b1377e07ba5c79661677b0707df	Heodo
Suspicious IPs	a4920c6089a0919a036c7b7b0e1728ec	Heodo
Suspicious Domains	8e9efeb4ca9b8b8eebafaf4b6153f4757	Heodo
Suspicious MD5sums	a6185c38b4bd1046052e027e10391e68	Heodo
	a0ad0bf71b23db867da0652dec3341e2	Heodo
	e3334ee90005903cee5378c4117cf64	Heodo
	90880db5abc8746c39c42260a48660b7	Heodo
Defended Assets		
Defended Services		

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**.

- Configuration**
- [Home](#)
- [Precapture Filter](#)
- [Active Triggers](#)
- [Licensing...](#)
- [Software Updates](#)
- [System Alerts](#)

- Search Management**
- [Completed Searches](#)
- [Pending Searches](#)

- 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		↻
DefendedIP		Description
179.32.32.62		port 443
186.117.155.48		port 443
186.117.155.48		port 443

Upload
Download

Defended Assets

Defended Services

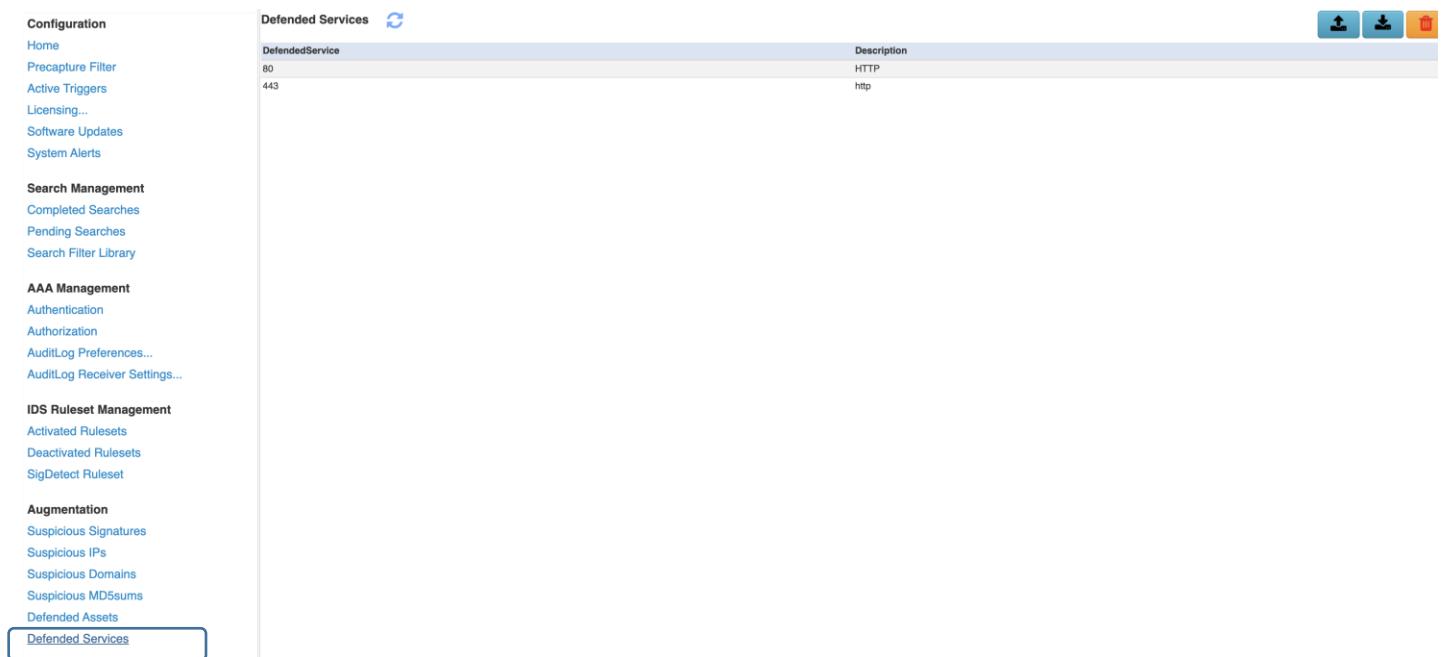
Authorized users can upload () new defended asset list as a csv file with each line containing an ip address of a defended asset, a comma, and an optional description. Each line of the csv file must have a valid ip address. Description is optional. If Description is provided, defended asset and Description 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**.



DefendedService	Description
80	HTTP
443	http

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. <ul style="list-style-type: none"> • 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

<p>[src dst] net <network></p> <p>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</p>	<p>Matches packets to or from source/destination or either, residing in a network.</p> <p>An IPv4 network number can be specified as:</p> <ul style="list-style-type: none"> • 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)
<p>[src dst] net <network> mask <netmask> or</p> <p>[src dst] net <network>/<len></p> <p>E.g., dst net 192.168.1.0 mask 255.255.255.255 or</p> <p>dst net 192.168.1.0/24 src net 192.168.1 mask 255.255.255.0</p> <p>or</p> <p>src net 192.168.1/24 dst net 172.16 mask 255.255.0.0 src net 10 mask 255.0.0.0</p>	<p>Matches packets with specific netmask. /len can also be specified to capture traffic from range of IP addresses.</p> <ul style="list-style-type: none"> • 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
<p>[src dst] port <port> or</p> <p>[tcp udp] [src dst] port <port></p> <p>E.g., src port 443 dst port 20 port 80</p>	<p>Matches packets sent to/from port</p> <ul style="list-style-type: none"> • Protocols (e.g., tcp/udp/ip etc.) can be applied to a port to get specific results
<p>[src dst] portrange <p1>-<p2> or</p> <p>[tcp udp] [src dst] portrange <p1>-<p2></p> <p>E.g., src portrange 80-88 tcp portrange 1501-1549</p>	<p>Matches packets to/from a port in the given range</p> <ul style="list-style-type: none"> • Protocols can be applied to port range to filter specific packets within the range
<p>less <length></p> <p>E.g., less 300 (or len <300)</p>	<p>Matches packets less than or equal to length</p>
<p>greater <length></p> <p>E.g., greater 301 (or len >300)</p>	<p>Matches packets greater than or equal to length</p>
<p>(ether ip ip6) proto <protocol></p>	<p>Matches an Ethernet, IPv4, or IPv6 protocol</p>

E.g., ether proto 0x888e ip proto 50	<ul style="list-style-type: none"> 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>] <ul style="list-style-type: none"> 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>] <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> 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] & 0xffffffff0f > 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

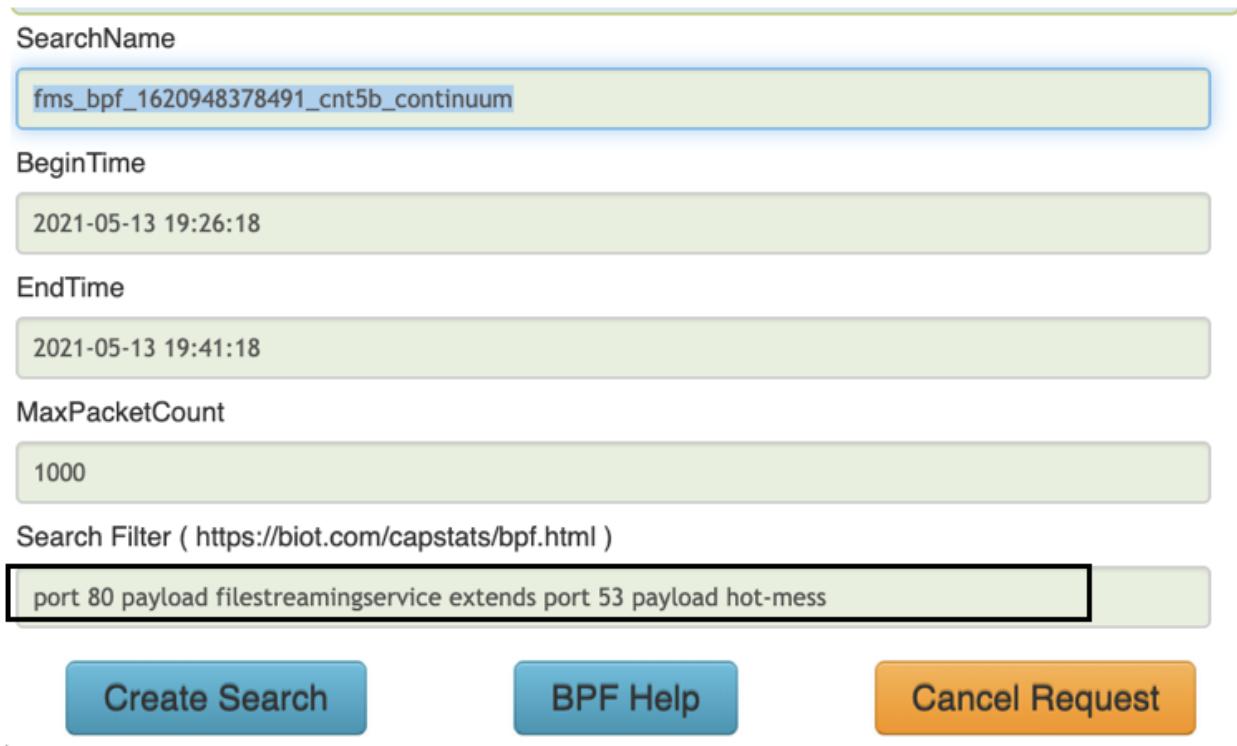
APPENDIX B - EXTENDING BPF SEARCH FILTERS

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



The screenshot shows a search configuration window with the following fields:

- SearchName: fms_bpf_1620948378491_cnt5b_continuum
- BeginTime: 2021-05-13 19:26:18
- EndTime: 2021-05-13 19:41:18
- MaxPacketCount: 1000
- Search Filter (https://biot.com/capstats/bpf.html):
 port 80 payload filestreamingservice extends port 53 payload hot-mess
- Buttons at the bottom: Create Search (blue), BPF Help (blue), Cancel Request (orange)

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

Search Details

SearchName	fms_bpf_1620948378491_cnt5b_continuum
Begintime	2021-05-13 23:26:18
Endtime	2021-05-13 23:41:18
SearchFilter	PcapData port 80 payload filestreamingservice extends port 53 payload hot-mess@PcapData
MaxPacketCount	1000
SearchResult	Pkts=1163 Seconds=6 TotalSize=284KB NoMerge SnapLen=All

1
⬇️ PcapData (MaxPcaps: 1)
⬇️ LogData
⬇️ Objects
Clone Search

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.

View Packets (fms_bpf_1620948378491_cnt5b_continuum)

Time	Source IP	Destination IP	Protocol	Port	Description
2021-05-13 19:39:16.009 -0400	172.17.8.8:53	172.17.8.174:61613	DNS	184	Standard query response 0x1336 SRV _gc._tcp.Default-First-Site-N
2021-05-13 19:39:16.015 -0400	172.17.8.174:58512	172.17.8.8:53	DNS	92	Standard query 0x8bc4 SOA DESKTOP-TZMKHKC.one-hot-mess.com
2021-05-13 19:39:16.015 -0400	172.17.8.8:53	172.17.8.174:58512	DNS	171	Standard query response 0x8bc4 SOA DESKTOP-TZMKHKC.one-hot-mess.
2021-05-13 19:39:16.015 -0400	172.17.8.174:62976	172.17.8.8:53	DNS	160	Dynamic update 0xb6e7 SOA one-hot-mess.com CNAME AAAA A A 172.17.
2021-05-13 19:39:16.015 -0400	172.17.8.8:53	172.17.8.174:62976	DNS	160	Dynamic update response 0xb6e7 SOA one-hot-mess.com CNAME AAAA A
2021-05-13 19:39:16.041 -0400	172.17.8.174:49779	13.107.4.50:80	HTTP	367	GET /filestreamingservice/files/001eb2ac-b2c2-4a55-a78d-85def1f0
2021-05-13 19:39:16.041 -0400	172.17.8.174:49785	205.185.216.10:80	HTTP	473	GET /filestreamingservice/files/0092fb1c-d27f-429c-acdd-29b392ed
2021-05-13 19:39:16.041 -0400	172.17.8.174:49784	205.185.216.42:80	HTTP	473	GET /filestreamingservice/files/0092fb1c-d27f-429c-acdd-29b392ed
2021-05-13 19:39:16.042 -0400	172.17.8.174:49789	205.185.216.42:80	HTTP	472	GET /filestreamingservice/files/001eb2ac-b2c2-4a55-a78d-85def1f0
2021-05-13 19:39:16.042 -0400	172.17.8.174:49790	205.185.216.10:80	HTTP	472	GET /filestreamingservice/files/001eb2ac-b2c2-4a55-a78d-85def1f0
2021-05-13 19:39:16.042 -0400	172.17.8.174:49790	205.185.216.10:80	HTTP	484	GET /filestreamingservice/files/001eb2ac-b2c2-4a55-a78d-85def1f0
2021-05-13 19:39:16.042 -0400	172.17.8.174:49787	205.185.216.42:80	HTTP	489	GET /filestreamingservice/files/0092fb1c-d27f-429c-acdd-29b392ed
2021-05-13 19:39:16.056 -0400	172.17.8.174:49797	205.185.216.10:80	HTTP	472	GET /filestreamingservice/files/9ed29ecb-8df0-4d34-83a5-a3fd5d6a
2021-05-13 19:39:16.057 -0400	172.17.8.174:49798	205.185.216.42:80	HTTP	486	GET /filestreamingservice/files/9ed29ecb-8df0-4d34-83a5-a3fd5d6a
2021-05-13 19:39:16.065 -0400	172.17.8.174:49801	205.185.216.42:80	HTTP	472	GET /filestreamingservice/files/9ed29ecb-8df0-4d34-83a5-a3fd5d6a
2021-05-13 19:39:16.065 -0400	172.17.8.174:49802	205.185.216.10:80	HTTP	472	GET /filestreamingservice/files/9ed29ecb-8df0-4d34-83a5-a3fd5d6a
2021-05-13 19:39:16.065 -0400	172.17.8.174:49803	205.185.216.10:80	HTTP	473	GET /filestreamingservice/files/669bf2c3-676c-4886-abcb-369234eb
2021-05-13 19:39:16.065 -0400	172.17.8.174:49804	205.185.216.42:80	HTTP	473	GET /filestreamingservice/files/669bf2c3-676c-4886-abcb-369234eb
2021-05-13 19:39:16.071 -0400	172.17.8.174:64898	172.17.8.8:53	DNS	97	Standard query 0xb2d1 SRV _ldap._tcp.dc._msdcs.one-hot-mess.com
2021-05-13 19:39:16.071 -0400	172.17.8.8:53	172.17.8.174:64898	DNS	165	Standard query response 0xb2d1 SRV _ldap._tcp.dc._msdcs.one-hot-
2021-05-13 19:39:16.071 -0400	172.17.8.174:62494	172.17.8.8:53	DNS	92	Standard query 0xb5d3 A One-Hot-Mess-DC.one-hot-mess.com
2021-05-13 19:39:16.071 -0400	172.17.8.8:53	172.17.8.174:62494	DNS	108	Standard query response 0xb5d3 A One-Hot-Mess-DC.one-hot-mess.co
2021-05-13 19:39:16.071 -0400	172.17.8.174:63374	172.17.8.8:53	DNS	109	Standard query 0x7610 SRV _ldap._tcp.dc._msdcs.localdomain.one-h
2021-05-13 19:39:16.071 -0400	172.17.8.8:53	172.17.8.174:63374	DNS	188	Standard query response 0x7610 No such name SRV _ldap._tcp.dc._m
2021-05-13 19:39:16.071 -0400	172.17.8.8:53	172.17.8.174:58724	DNS	160	Standard query response 0xe4c9 No such name A wpad.one-hot-mess.
2021-05-13 19:39:16.071 -0400	172.17.8.174:58724	172.17.8.8:53	DNS	81	Standard query 0xe4c9 A wpad.one-hot-mess.com

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-
23	2021-05-13 23:39:16.015914587	172.17.8.174	172.17.8.8	DNS	92	Standard query 0x8bc4 SOA DESKTOP-TZMKHHC.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-TZMKHHC.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-a3ffd56a2aa?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-a3ffd56a2aa?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-a3ffd56a2aa?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-a3ffd56a2aa?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.
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
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._msdcs.localdomain.one-

> 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

Hex	Dec	Source	Dest	Protocol	Length	Info
0000	a4 1f 72 c2 09 6a 00 11	75 8c fd 47 08 00 45 00	···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 ····			

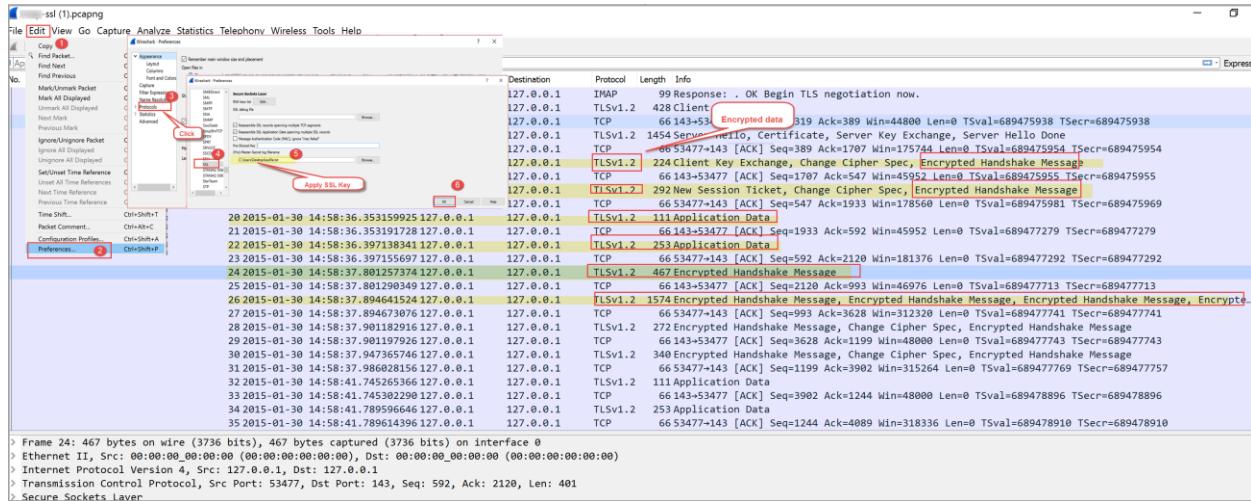
APPENDIX C - DECRYPTING PCAP WITH SSL SESSION KEYS

This workflow presumes the user has:

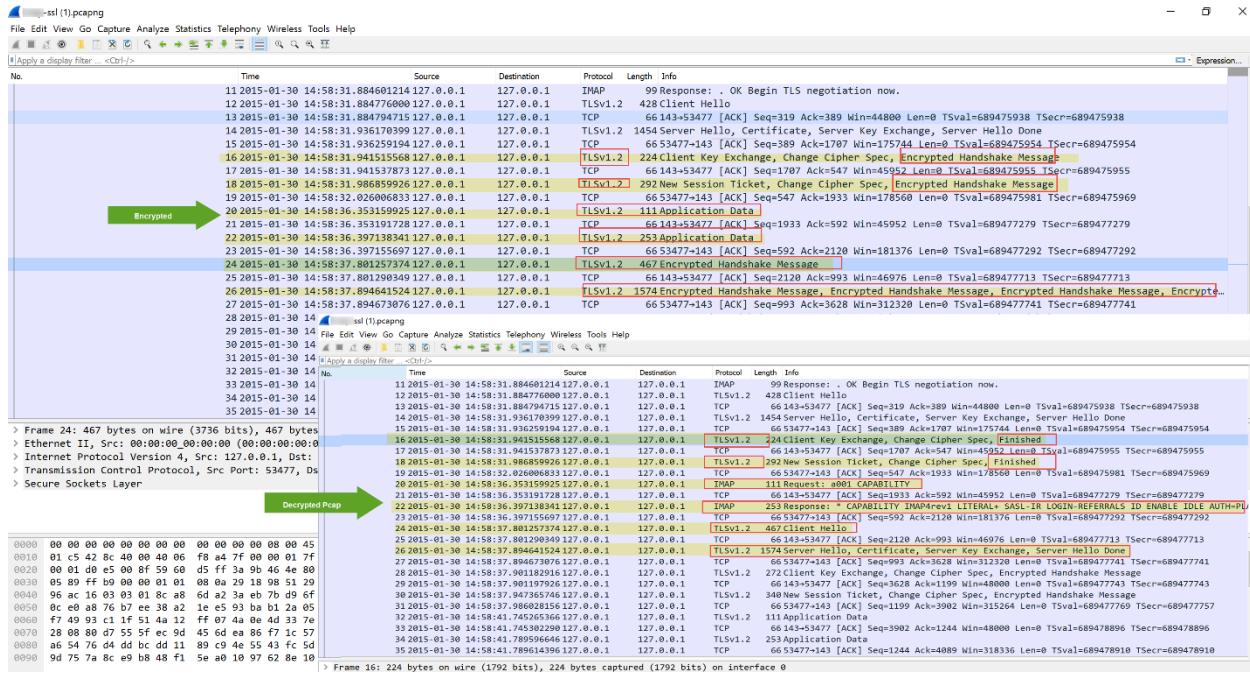
- A set of SSL Session keys for decrypting pcap data
- Downloaded one or more (encrypted) pcaps from a completed pcap search

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

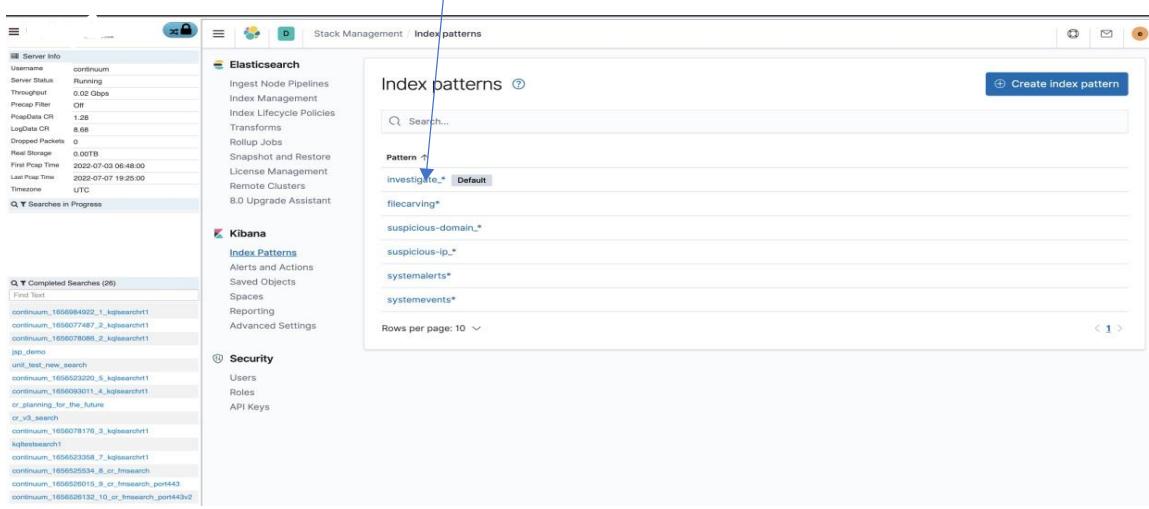
This process will require back-end console access of the FM Server. Run the following commands to set up the forwarder. In the following steps, 192.168.1.175 represents the Splunk forward server ip address.

- 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_*



The screenshot shows the SentryWire interface under 'Stack Management / Index patterns'. A blue arrow points from the 'investigate_*' entry in the list to the 'investigate_*' link in the breadcrumb navigation bar above the main content area.

Elasticsearch

- Ingest Node Pipelines
- Index Management
- Index Lifecycle Policies
- Transforms
- Rollup Jobs
- Snapshot and Restore
- License Management
- Remote Clusters
- 8.0 Upgrade Assistant

Kibana

- Index Patterns
- Alerts and Actions
- Saved Objects
- Spaces
- Reporting
- Advanced Settings

Security

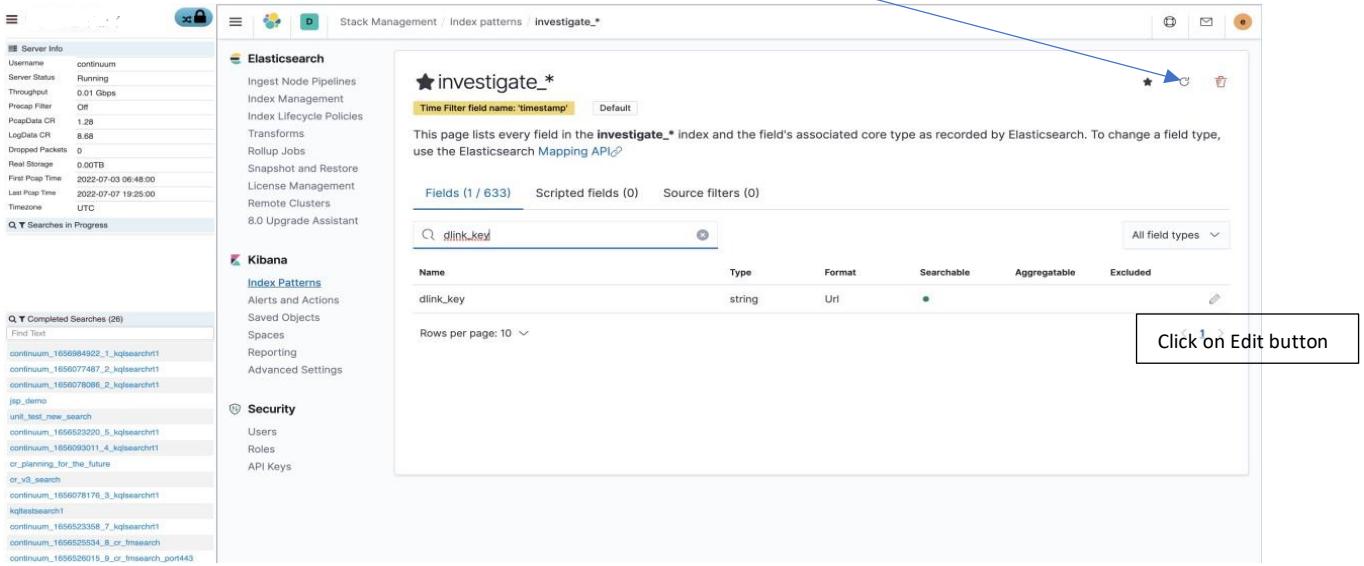
- Users
- Roles
- API Keys

Completed Searches (26)

Search Bar: Search...

Buttons: Create index pattern, Refresh, Help, Logout

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



The screenshot shows the 'investigate_*' index pattern details page. A blue arrow points from the 'dlink_key' entry in the 'Fields' table to the 'Edit' button in the 'Actions' column of the same row.

Fields (1 / 633)

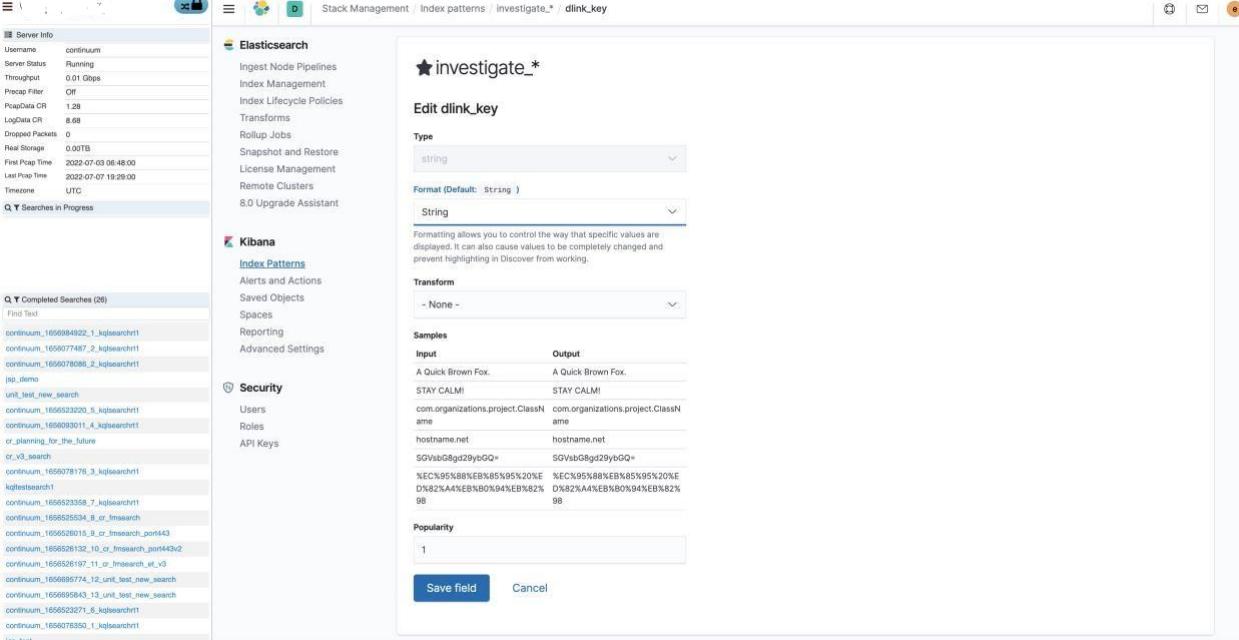
Name	Type	Format	Searchable	Aggregatable	Excluded
dlink_key	string	Url	●		

Actions:

- Edit (highlighted)
- Delete
- Copy
- Share

Buttons: All field types, Refresh, Help, Logout

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



Server Info

- Username: continuum
- Server Status: Running
- Throughput: 0.00 Gbps
- Precap Filter: Off
- PopData CR: 1.28
- LogData CR: 8.68
- Dropped Packets: 0
- Real Storage: 0.00TB
- First Pop Time: 2022-07-03 06:48:00
- Last Pop Time: 2022-07-07 19:29:00
- Timezone: UTC

Completed Searches (26)

Elasticsearch

Kibana

Security

Investigate_*

Edit dlink_key

Type: string

Format (Default: String): String

Transform: - None -

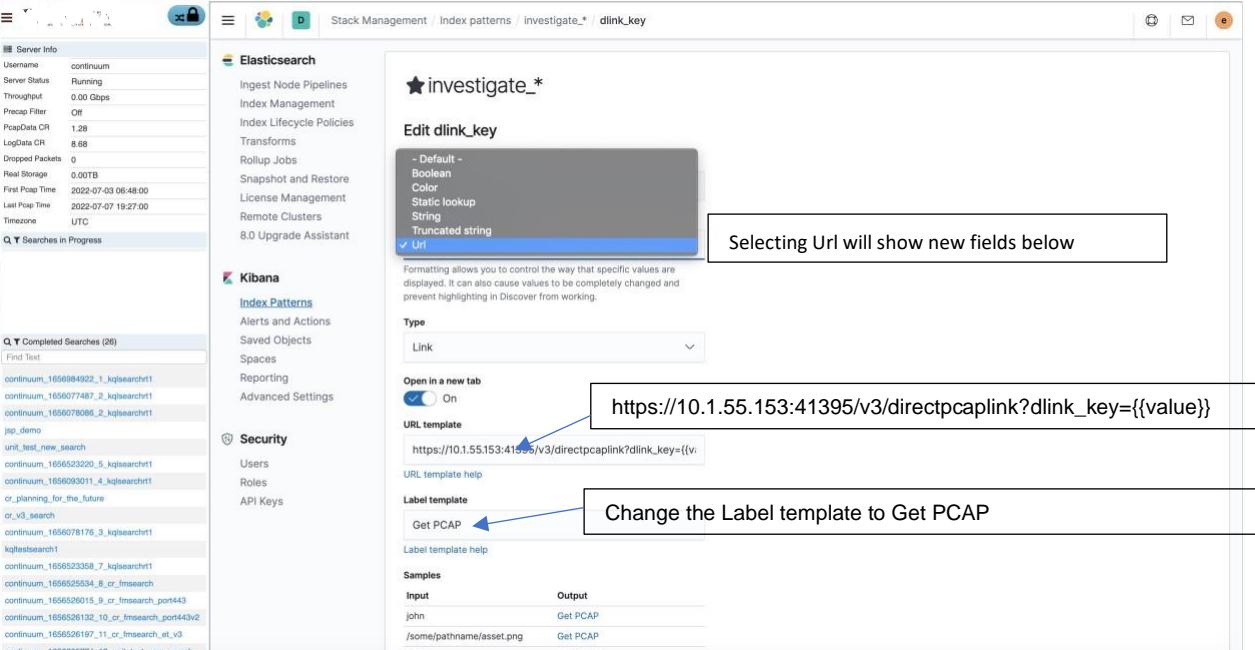
Samples

Input	Output
A Quick Brown Fox.	A Quick Brown Fox.

Popularity: 1

Save field Cancel

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



Server Info

- Username: continuum
- Server Status: Running
- Throughput: 0.00 Gbps
- Precap Filter: Off
- PopData CR: 1.28
- LogData CR: 8.68
- Dropped Packets: 0
- Real Storage: 0.00TB
- First Pop Time: 2022-07-03 06:48:00
- Last Pop Time: 2022-07-07 19:27:00
- Timezone: UTC

Completed Searches (26)

Elasticsearch

Kibana

Security

Investigate_*

Edit dlink_key

Type: Url

- Default -
Boolean
Color
Static lookup
String
Truncated string

Selecting Url will show new fields below

Open in a new tab: On

URL template: https://10.1.55.153:41395/v3/directpcaplink?dlink_key={{value}}

URI template help

Label template: Get PCAP

Change the Label template to Get PCAP

Label template help

Samples

Input	Output
john	Get PCAP
/some pathname/asset.png	Get PCAP
1234	Get PCAP

Label template help

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

★investigate_*

Edit dlink_key

Type

Format (Default: String)

Formatting allows you to control the way that specific values are displayed. It can also cause values to be completely changed and prevent highlighting in Discover from working.

Type

Open in a new tab
 On

URL template

URL template help

Label template

Label template help

Samples

Input	Output
john	Get PCAP
/some pathname/asset.png	Get PCAP
1234	Get PCAP

Popularity

Save field **Cancel**

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

Server Info

Username	continuum
Server Status	Running
Throughput	0.03 Gbps
Precap Filter	Off
PostData CR	1.28
LogData CR	1.00
Dropped Packets	0
Real Storage	0.00TB
First Pcap Time	2022-07-30 06:19:00
Last Pcap Time	2022-08-04 21:55:00
Timezone	UTC

Discover

New Save Open Share Inspect

tcp.rst:true

+ Add filter

25,706 hits

Aug 4, 2022 @ 16:57:21.832 - Aug 4, 2022 @ 17:57:21.832 — Auto

Count timestamp per minute

Time _source

Completed Searches (98)

Find Test

continuum_20220804203249_ap18| chris_rofe_20220804202351_gpv6 continuum_20220804175718_bm84 test1_1bw7 test1_fbw continuum_20220804012810_0_s3cwi test1 continuum_20220803123609_x463c_Test1_vptbd_c7sq continuum_20220803123609_x463c_Test1_vptbd continuum_20220803150319_tcpub_zxwei continuum_20220803150319_tcpub continuum_20220803151152_ue89m_Core continuum_20220803150309_x3zxa continuum_20220803134619_z11th continuum_20220803133446_0ibba continuum_20220803131033_xutel_T2 continuum_20220803123609_x463c_Test1 continuum_20220803121313_x3sg continuum_1658847146_5_Phantom3 continuum_1658847124_4_Phantom3 continuum_1658796056_3_phantom_test

Another view:

Server Info

Username	continuum
Server Status	Running
Throughput	0.03 Gbps
Precap Filter	Off
PostData CR	1.28
LogData CR	1.00
Dropped Packets	0
Real Storage	0.00TB
First Pcap Time	2022-07-30 06:19:00
Last Pcap Time	2022-08-04 21:57:00
Timezone	UTC

Discover

New Save Open Share Inspect

tcp.rst:true

+ Add filter

investigate_*

Search field names

Filter by type 0

Selected fields

- dest_ip
- dest_port
- dlink_key
- src_ip
- src_port

Available fields

- _id
- _index
- _score
- _type
- app.proto
- app.proto_orig
- app.proto_tc
- community_id
- communityID
- defended
- ether.dest_macs
- ether.src_macs
- event_type
- flow_id
- flow.age
- flow.alerted

Launchpad

25,706 hits

Aug 4, 2022 @ 16:57:21.832 - Aug 4, 2022 @ 17:57:21.832 — Auto

Count timestamp per minute

Time src_ip src_port dest_ip dest_port dlink_key

Selected fields

Available fields

Launchpad