

FEDERATION MANAGER UI

USER GUIDE

Software Version: 7.3.0.309-408.14

Document version 1.7

12/10/2021

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	Added Appendix E, F, & G	12/10/2021

Contents

INTRODUCTION.....	5
1.1 Supported Web Browsers.....	5
1.2 Setting Up Your Network	5
1.3 UI Username/Password.....	5
1.4 Logging in to the application	6
FEDERATION MANAGER UI	6
2 INVESTIGATOR VIEW	7
2.1.1 Selectable Nodes.....	8
2.1.2 ASSISTED (JSON) Search.....	10
2.1.3 CUSTOM (BPF) Search	14
2.1.4 Create Active Trigger	17
2.1.5 Expand IPv6 Address	19
2.2 Visualizations and Dashboards	20
2.2.1 Viewing an existing dashboard.....	20
2.2.2 Overview dashboard	20
2.2.3 Drilldown example	21
2.2.4 Dashboard structure	21
2.2.5 Creating a new dashboard.....	23
2.2.6 Creating a new visualization.....	24
2.2.7 Adding a visualization to a dashboard.....	28
2.2.8 Deleting a dashboard or visualization.....	30
2.2.9 Backup and restore custom dashboards	30
2.2.10 Discover.....	32
2.2.11 Pin a field to a column	32
2.2.12 Searches	33
3 ADMINISTRATOR VIEW.....	35
3.1 Configuration	36

3.1.1	Home	36
3.1.2	Selectable Nodes.....	37
3.1.3	Precapture Filter.....	38
3.1.4	Active Triggers	40
3.1.5	File Carving	41
3.1.6	Licensing	45
3.1.7	System Health.....	46
3.1.8	Software Updates.....	47
3.1.9	System Alerts.....	48
3.2	Search Management.....	49
3.2.1	Completed Searches.....	49
3.2.2	Pending Searches	50
3.2.3	Search Filter Library.....	52
3.3	AAA Management	52
3.3.1	Authorization	52
3.3.2	Authentication.....	53
3.3.3	Auditlog Preferences	56
3.3.4	Auditlog Receiver Settings	56
3.4	IDS Ruleset Management	57
3.4.1	Activated Rulesets	58
3.4.2	Deactivated Rulesets.....	59
3.4.3	SigDetect Ruleset.....	60
3.5	Augmentation.....	61
3.5.1	Suspicious Signatures	62
3.5.2	Suspicious IPs.....	64
3.5.3	Suspicious Domains.....	66
3.5.4	Suspicious MD5sums	67
3.5.5	Defended Assets	68

3.5.6 Defended Services	69
APPENDIX A – BPF FILTER	70
APPENDIX B - EXTENDING BPF SEARCH FILTERS	76
APPENDIX C - DECRYPTING PCAP WITH SSL SESSION KEYS.....	80
APPENDIX D - SENTRYWIRE SPLUNK ADVANCED SYNTAX	82
APPENDIX E - SENTRYWIRE SPLUNK APP DOCUMENTATION.....	85
APPENDIX F – TROUBLESHOOTING RECOMMENDATIONS.....	94
APPENDIX G – SYSTEM CONFIGURATION (NTP AND DNS)	99

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 (Refer to Firefox Certificate Exception in **Appendix E**)

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

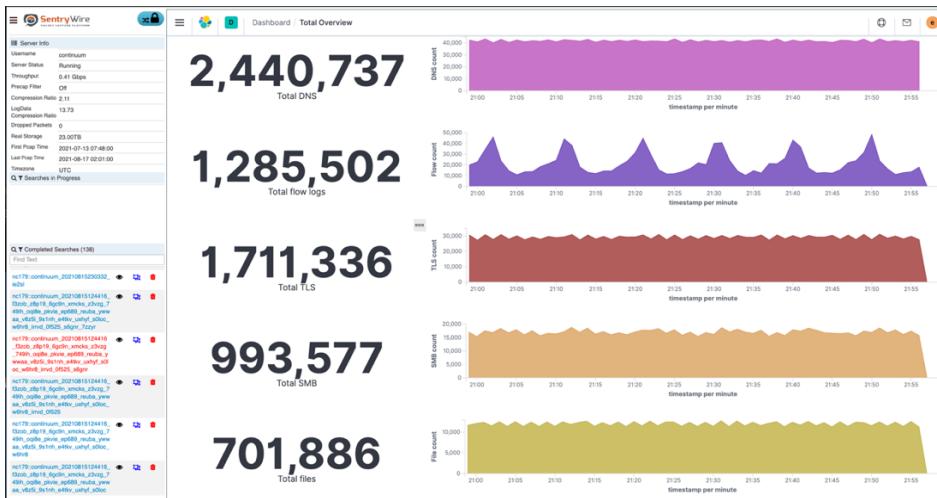
On any remote system connected to the network, open a supported web browser, and enter the IP address (not FM server's hostname) and port number 41395 over https. For Example: <https://<IP Address>:41395>

Login username and password will be provided directly to the customer.

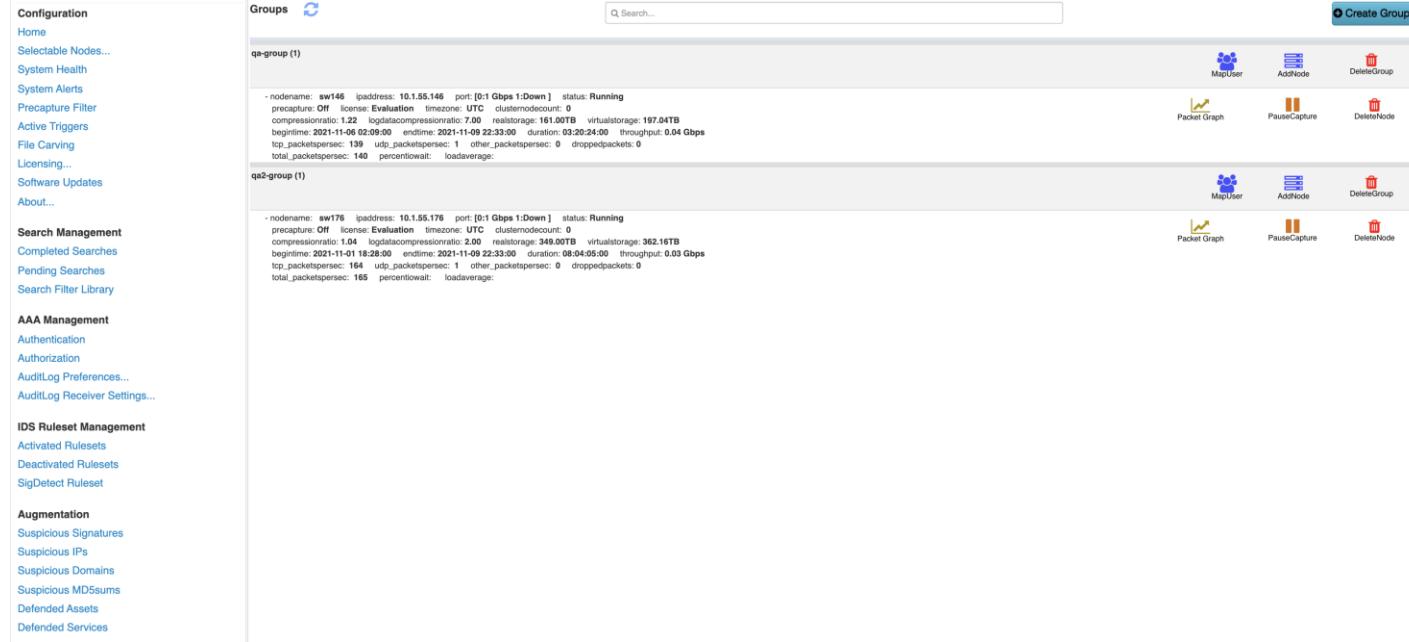
FEDERATION MANAGER UI

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.



The screenshot shows the SentryWire Platform interface. On the left, a 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, 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, and Defended Services.

The main area is divided into three sections:

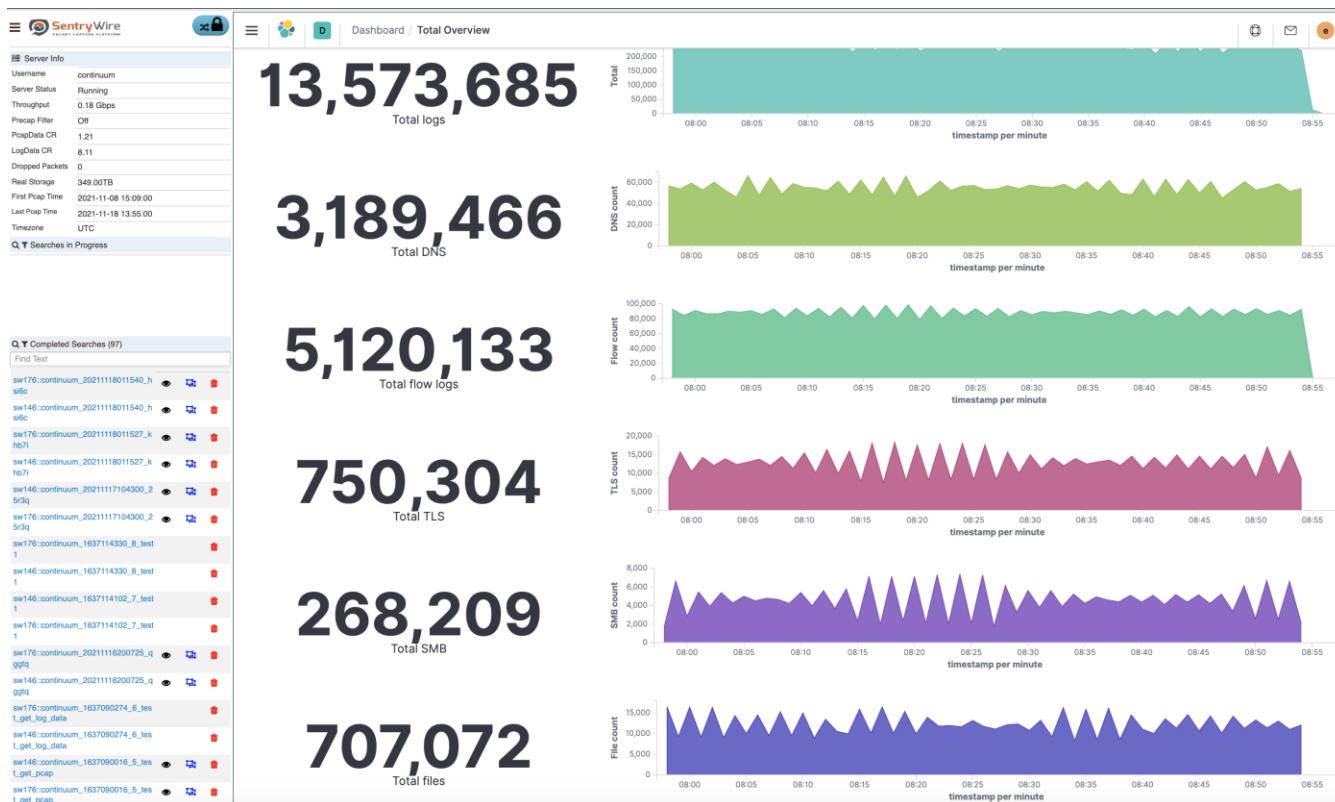
- Groups:** Shows two groups: qa-group (1) and qa2-group (1). Each group has a detailed configuration table and actions (MapUser, AddNode, DeleteGroup, Packet Graph, PauseCapture, DeleteNode).
- LogData CR:** Displays logdata compression ratio statistics for two nodes: sw145 and sw176. The table includes columns for nodename, loadaddress, port, precapture, license, evaluation, timezone, clustermodecount, compressionratio, logdatacompressionratio, realstorage, virtualstorage, beginime, endime, duration, throughput, total_packetspersec, and percentiowait.
- Kibana UI:** Shows the Kibana search interface with a search bar and results table.

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.

Appendix D provides brief overview of the relevant portions of Kibana usage process.

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:

 [Selectable Nodes...](#)

 [Create Assisted\(JSON\) Search...](#)

 [Create Custom\(BPF\) Search...](#)

 [Create Active Trigger...](#)

 [Expand IPv6 Address...](#)

 [Switch to Administrator View](#)

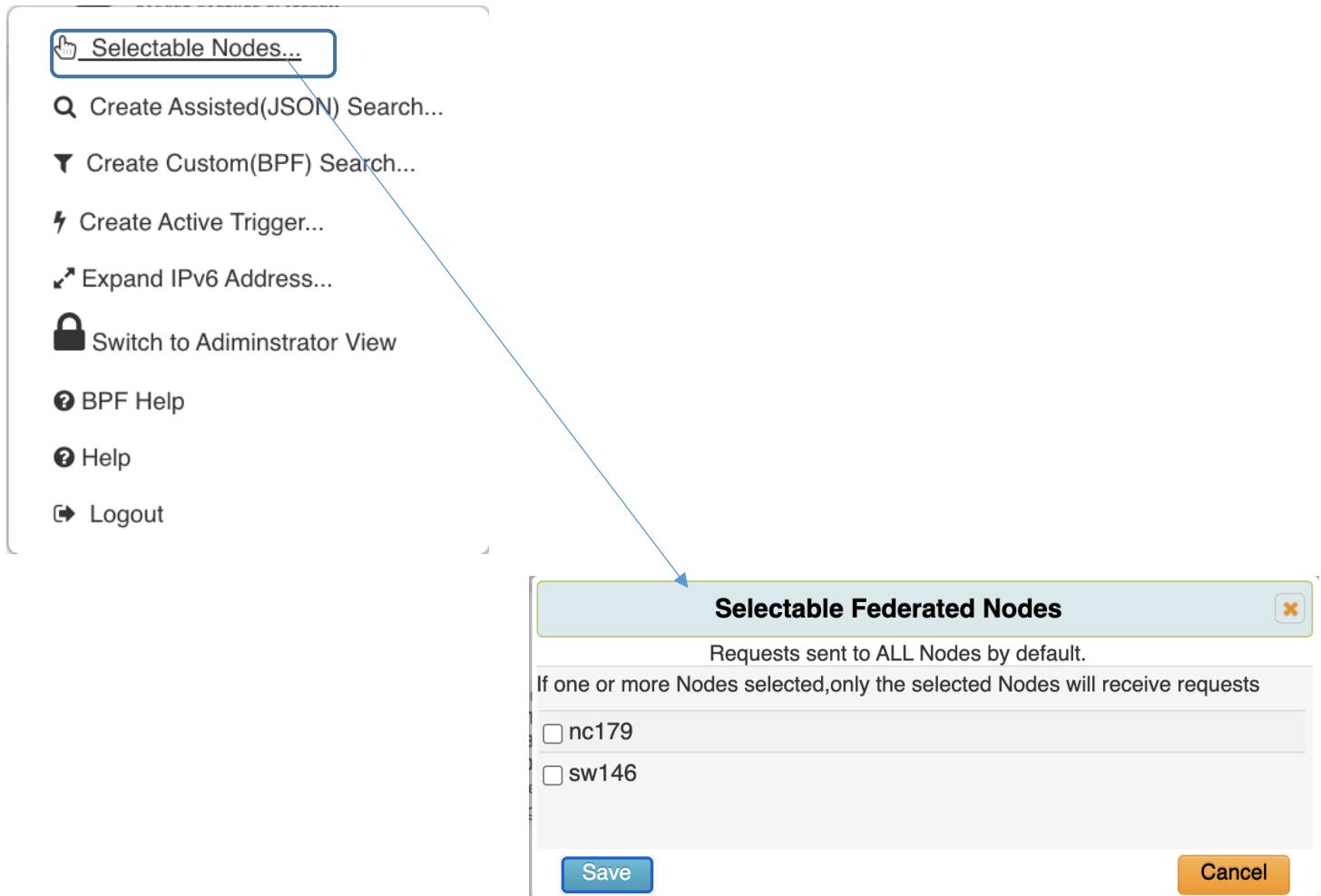
 [BPF Help](#)

 [Help](#)

 [Logout](#)

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.



The screenshot shows a context menu with the following items:

- Selectable Nodes...
- Create Assisted(JSON) Search...
- Create Custom(BPF) Search...
- Create Active Trigger...
- Expand IPv6 Address...
- Switch to Administrator View
- BPF Help
- Help
- Logout

A blue arrow points from the "Selectable Nodes..." menu item to a modal window titled "Selectable Federated Nodes".

Selectable Federated Nodes

Requests sent to ALL Nodes by default.
If one or more Nodes selected, only the selected Nodes will receive requests

nc179
 sw146

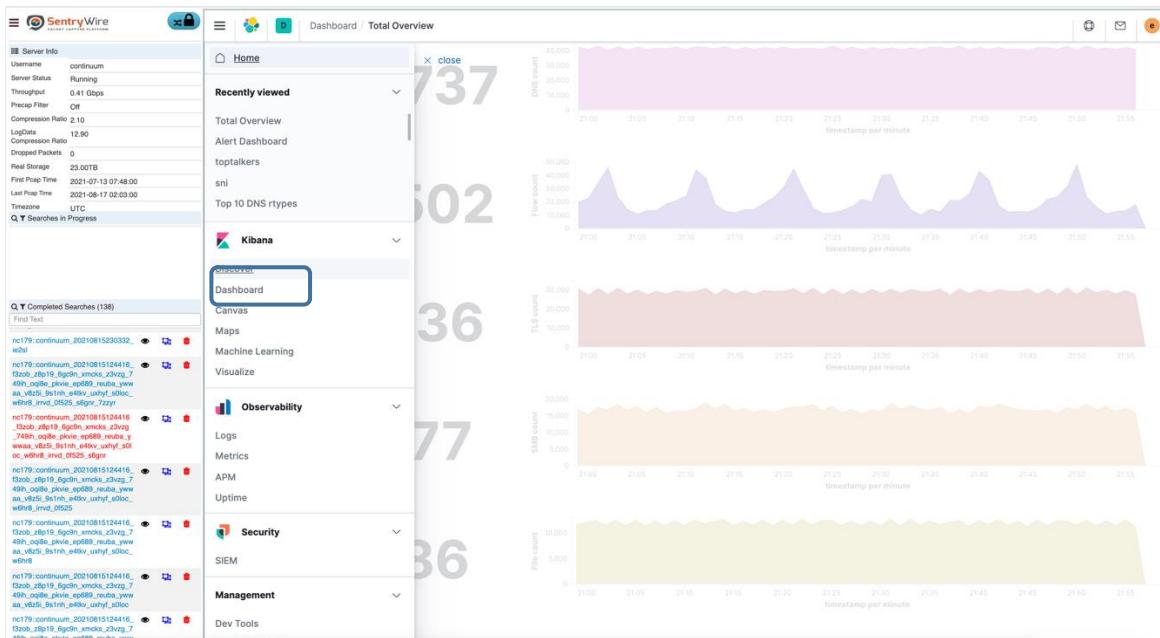
Save **Cancel**

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 ASSISTED (JSON) Search

Following sections describe how to create a search, an active trigger.

This method allows users to create searches without any prior knowledge of BPF syntax. Switch from the Dashboard view to Discover view by selecting Discover menu option as shown below:



Once in Discover mode, navigate to a metadata event that you would like to use as the basis for the JSON-assisted search, and expand it.

SentryWire

Discover

Server Info

- Username: continuum
- Server Status: Running
- Throughput: 0.40 Gbps
- Precap Filter: Off
- Compression Ratio: 2.10
- LogData: 12.90
- Compression Ratio: 2.10
- Dropped Packets: 0
- Real Storage: 23.00TB
- First Pop Time: 2021-07-13 07:48:00
- Last Pop Time: 2021-08-17 02:03:00
- Timezone: UTC
- Q. T Searches in Progress

Completed Searches (138)

Find Text

nc179_continuum_20210815230332_le2sl

nc179_continuum_20210815124416_f32ob_zp19_8gdn_xmcks_z3vzg_749n_oq8e_pkiv_e089_reuba_yww_aa_vbz5_9s1nh_e4kv_uvhyl_s0loc_w6n8_irvd_0f525_s6gnr_s6gnr

nc179_continuum_20210815124416_f32ob_zp19_8gdn_xmcks_z3vzg_749n_oq8e_pkiv_e089_reuba_yww_aa_vbz5_9s1nh_e4kv_uvhyl_s0loc_w6n8_irvd_0f525

nc179_continuum_20210815124416_f32ob_zp19_8gdn_xmcks_z3vzg_749n_oq8e_pkiv_e089_reuba_yww_aa_vbz5_9s1nh_e4kv_uvhyl_s0loc_w6n8_irvd_0f525

nc179_continuum_20210815124416_f32ob_zp19_8gdn_xmcks_z3vzg_749n_oq8e_pkiv_e089_reuba_yww_aa_vbz5_9s1nh_e4kv_uvhyl_s0loc_w6n8_irvd_0f525

nc179_continuum_20210815124416_f32ob_zp19_8gdn_xmcks_z3vzg_749n_oq8e_pkiv_e089_reuba_yww_aa_vbz5_9s1nh_e4kv_uvhyl_s0loc_w6n8_irvd_0f525

nc179_continuum_20210815124416_f32ob_zp19_8gdn_xmcks_z3vzg_749n_oq8e_pkiv_e089_reuba_yww_aa_vbz5_9s1nh_e4kv_uvhyl

View surrounding documents View single document

Expanded document

Table JSON

```

{
    "_id": "sRhbUXsBS6dyifb3EPjP",
    "_index": "investigate_nc179_452546",
    "_score": "-",
    "_type": ".doc",
    "app_proto": "tls",
    "app_proto_orig": "smtp",
    "app_proto_tc": "failed",
    "community_id": "1:hkY6Z4X0u8Lyfx6515aHVLU+e6I=",
    "defended": "false",
    "dest_ip": "10.1.8.168",
    "dest_port": "443",
    "event_type": "flow",
    "flow.age": "8",
    "flow.alerted": "false",
    "flow.bytes_toclient": "832B",
    "flow.bytes_toserver": "1.3KB",
    "flow.end": "Aug 16, 2021 @ 22:03:48.000000000",
    "flow.pkts_toclient": "9",
    "flow.pkts_toserver": "12",
    "flow.reason": "unknown"
}

```

Select JSON option and click on the copy button to the right of the page:

SentryWire

Discover

Server Info

- Username: continuum
- Server Status: Running
- Throughput: 0.41 Gbps
- Precap Filter: Off
- Compression Ratio: 2.10
- LogData: 12.45
- Compression Ratio: 2.10
- Dropped Packets: 0
- Real Storage: 23.00TB
- First Pop Time: 2021-07-13 07:48:00
- Last Pop Time: 2021-08-17 02:05:00
- Timezone: UTC
- Q. T Searches in Progress

Completed Searches (138)

Find Text

nc179_continuum_20210815230332_le2sl

nc179_continuum_20210815124416_f32ob_zp19_8gdn_xmcks_z3vzg_749n_oq8e_pkiv_e089_reuba_yww_aa_vbz5_9s1nh_e4kv_uvhyl_s0loc_w6n8_irvd_0f525_s6gnr_s6gnr

nc179_continuum_20210815124416_f32ob_zp19_8gdn_xmcks_z3vzg_749n_oq8e_pkiv_e089_reuba_yww_aa_vbz5_9s1nh_e4kv_uvhyl_s0loc_w6n8_irvd_0f525

nc179_continuum_20210815124416_f32ob_zp19_8gdn_xmcks_z3vzg_749n_oq8e_pkiv_e089_reuba_yww_aa_vbz5_9s1nh_e4kv_uvhyl_s0loc_w6n8_irvd_0f525

nc179_continuum_20210815124416_f32ob_zp19_8gdn_xmcks_z3vzg_749n_oq8e_pkiv_e089_reuba_yww_aa_vbz5_9s1nh_e4kv_uvhyl_s0loc_w6n8_irvd_0f525

nc179_continuum_20210815124416_f32ob_zp19_8gdn_xmcks_z3vzg_749n_oq8e_pkiv_e089_reuba_yww_aa_vbz5_9s1nh_e4kv_uvhyl_s0loc_w6n8_irvd_0f525

nc179_continuum_20210815124416_f32ob_zp19_8gdn_xmcks_z3vzg_749n_oq8e_pkiv_e089_reuba_yww_aa_vbz5_9s1nh_e4kv_uvhyl_s0loc_w6n8_irvd_0f525

nc179_continuum_20210815124416_f32ob_zp19_8gdn_xmcks_z3vzg_749n_oq8e_pkiv_e089_reuba_yww_aa_vbz5_9s1nh_e4kv_uvhyl

View surrounding documents View single document

Expanded document

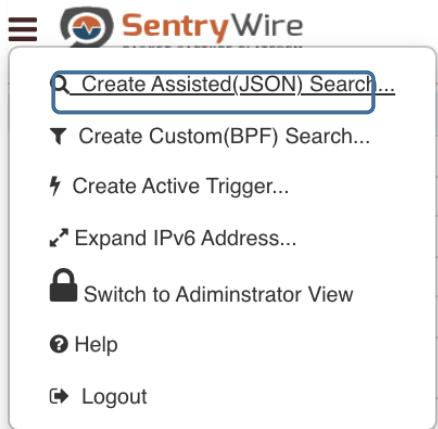
Table JSON

```

{
    "_index": "investigate_nc179_452546",
    "_type": ".doc",
    "_id": "sRhbUXsBS6dyifb3EPjP",
    "_version": "1",
    "_score": "null",
    "source": {
        "icmp_type": 8,
        "metadata": {
            "flowbits": [
                "ET_dcerpc_mslass"
            ]
        },
        "defend": "false",
        "app_proto_orig": "smtp",
        "src_ip": "10.1.8.151",
        "community_id": "1:hkY6Z4X0u8Lyfx6515aHVLU+e6I=",
        "event_type": "flow",
        "flow_id": "1:630,438,134,843,998",
        "icmp_code": 0,
        "dest_port": 443,
        "flow": {
            "reason": "unknown",
            "pkts_toserver": 12,
            "alerted": "false",
            "start": "2021-08-17T02:03:48",
            "bytes_toclient": 832,
            "end": "2021-08-17T02:03:48",
            "state": "closed",
            "bytes_toserver": 1333,
            "age": 8,
            "pkts_toclient": 9
        },
        "timestamp": "2021-08-17T02:04:01",
        "tcp": {
            "rst": true,
            "tcp_flags_tc": "1b",
            "tcp_flags_ts": "1f",
            "tcp_window": 1
        }
    }
}

```

Select the Menu option:



Dialog box appears:

Create Search

Search Name	continuum_20210626233712_o3la6
Event JSON	<pre>1)From DiscoverView of a Federated Node,Copy/Paste JSON data of a document. 2)Edit attributes such as Begintime,Endtime,MacPacketCount as needed. 3)Press Create Search</pre>
Payload Search Filter	Comma seperated list of search terms.For example:HTTP,fe:0a:97,10.2.12.
Cancel Request	

Paste the search details into the Event JSON, the other field data is extracted from the JSON data:

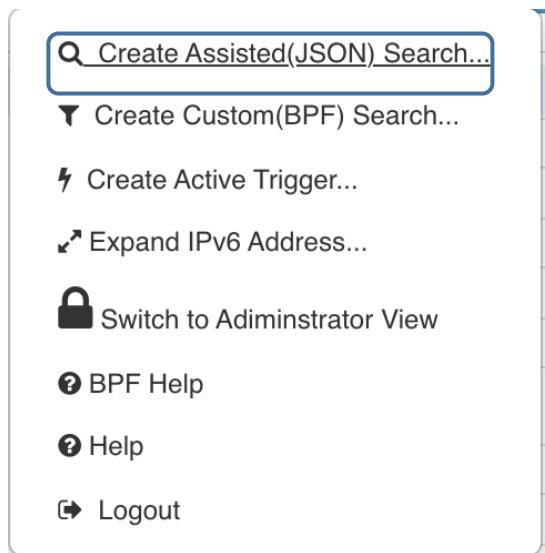
Create Search

Search Name	continuum_20210626234604_vuco6
Event JSON	<pre>"sort": [1624750679000000000]</pre>
Begintime	2021-06-26 23:21:40
Endtime	2021-06-26 23:47:40
MaxPacketCount	10000
dest_ip	64.215.255.95
dest_port	80
proto	TCP
src_ip	172.16.133.163
src_port	3665
Payload Search Filter	Comma seperated list of search terms.For example:HTTP,fe:0a:97,10.2.12.
Create Search	
Cancel Request	

Click on the **Create Search** button to create the search named *continuum_20210626234604_yuc06*. This search will appear in Searches in Progress Panel. Once the search is complete, it will appear in Completed Searches panel.

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 X

SearchName
continuum_2021062623529_9286q

BeginTime
2021-09-10 15:27:02

EndTime
2021-09-10 15:42:02

Search Filter (<https://biot.com/capstats/bpf.html>)
tcp or udp

MaxPacketCount
10000

Create Search
|
Search Library
|
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	continuum_2021062623529_9286q
BeginTime	2021-09-10 15:27:02
EndTime	2021-09-10 15:27:02
Search Filter (BPF)	BPF Search Filter Library <ul style="list-style-type: none"> ip6 ip6 and src port 546 ip6 and udp and src port 546 (ip6 or ip) and udp and src port 546 (ip6 or ip) and udp (ip6 or ip) and udp and not port 78 ip6 and udp and port 546 extends udp and port 53
MaxPacketCount	10000
<input style="background-color: #007bff; color: white; padding: 5px; width: 100%;" type="button" value="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:

Searches in Progress

nc179::continuum_20210626235319_q286q	X
---------------------------------------	---

Once the search is complete, it appears in Completed Searches panel:

Completed Searches (73)

Find Text			
nc179::continuum_20210626235319_q286q	Eye icon	Copy icon	Trash icon
nc179::continuum_20210626234821_nyr1o	Eye icon	Copy icon	Trash icon
nc179::continuum_20210626234604_vuco6	Eye icon	Copy icon	Trash icon
nc179::continuum_20210626233712_osla6	Eye icon	Copy icon	Trash icon
nc179::continuum_20210624231257_m036r	Eye icon	Copy icon	Trash icon
nc179::continuum_20210624214013_4x4y9_yvxeq	Eye icon	Copy icon	Trash icon
nc179::continuum_20210624231257_pgwjr	Eye icon	Copy icon	Trash icon
nc179::continuum_20210624214506_7manu	Eye icon	Copy icon	Trash icon
nc179::continuum_20210624214013_4x4y9	Eye icon	Copy icon	Trash icon
nc179::continuum_20210624210746_bt4r_xlkh6	Eye icon	Copy icon	Trash icon
nc179::continuum_20210624210746_bt4r_xlkh6	Eye icon	Copy icon	Trash icon

Click on the Search Name hyperlink to see Search Info:

Search Details	
SearchName	fms_2021_02_22_09_09_16_846
BeginTime	2021-02-22 13:34:40
EndTime	2021-02-22 14:0:40
SearchFilter	PcapData,host 172.20.134.10 and port 63718 and host 172.20.34.10 and port 53@PcapData
MaxPacketCount	10000
SearchResult	Pkts=1794 Seconds=92 TotalSize=183KB MergeAllPCAPs SnapLen=All

1

PcapData(1)

LogData

Download Objects

Clone Search

Delete Search

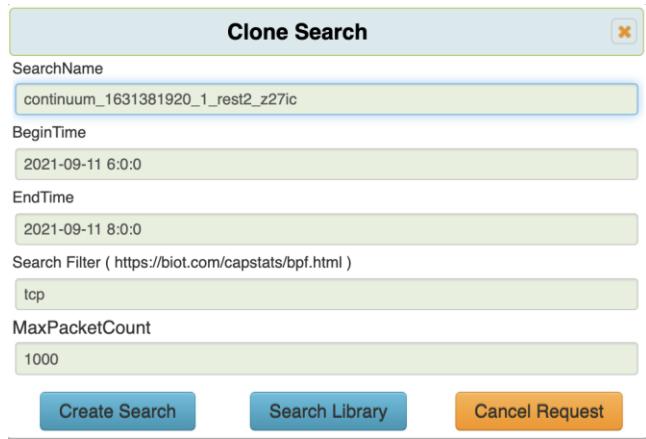
View Packets of the Search by clicking on :

View Packets (fms_2021_02_22_09_09_16_846)					
<input type="text" value="Search"/>					
Timestamp <input checked="" type="checkbox"/>	Source	Destination	Proto	Length	Info
2021-02-22 08:34:41.124 -0500	172.20.134.10	172.20.34.10	DNS	85	Standard query 0xaf96 PTR 55.64.20.172.in-addr.arpa
2021-02-22 08:34:41.127 -0500	172.20.34.10	172.20.134.10	DNS	96	Standard query response 0xaf96 Server failure PTR 55.64.20.172.i
2021-02-22 08:34:41.665 -0500	172.20.134.10	172.20.34.10	DNS	85	Standard query 0x791 PTR 59.64.20.172.in-addr.arpa
2021-02-22 08:34:41.678 -0500	172.20.34.10	172.20.134.10	DNS	85	Standard query response 0x791 Server failure PTR 59.64.20.172.i
2021-02-22 08:34:42.129 -0500	172.20.134.10	172.20.34.10	DNS	85	Standard query 0x0f53 PTR 49.100.10.10.in-addr.arpa
2021-02-22 08:34:42.149 -0500	172.20.34.10	172.20.134.10	DNS	96	Standard query response 0x0f53 Server failure PTR 49.100.10.10.i
2021-02-22 08:34:46.287 -0500	172.20.134.10	172.20.34.10	DNS	85	Standard query 0xaf96 PTR 55.64.20.172.in-addr.arpa
2021-02-22 08:34:46.289 -0500	172.20.34.10	172.20.134.10	DNS	96	Standard query response 0xaf96 Server failure PTR 55.64.20.172.i
2021-02-22 08:34:46.830 -0500	172.20.134.10	172.20.34.10	DNS	85	Standard query 0x791 PTR 59.64.20.172.in-addr.arpa
2021-02-22 08:34:46.843 -0500	172.20.34.10	172.20.134.10	DNS	85	Standard query response 0x791 Server failure PTR 59.64.20.172.i
2021-02-22 08:34:47.297 -0500	172.20.134.10	172.20.34.10	DNS	85	Standard query 0x0f53 PTR 49.100.10.10.in-addr.arpa
2021-02-22 08:34:47.319 -0500	172.20.34.10	172.20.134.10	DNS	96	Standard query response 0x0f53 Server failure PTR 49.100.10.10.i
2021-02-22 08:34:51.452 -0500	172.20.134.10	172.20.34.10	DNS	85	Standard query 0xaf96 PTR 55.64.20.172.in-addr.arpa
2021-02-22 08:34:51.454 -0500	172.20.34.10	172.20.134.10	DNS	96	Standard query response 0xaf96 Server failure PTR 55.64.20.172.i
2021-02-22 08:34:51.992 -0500	172.20.134.10	172.20.34.10	DNS	85	Standard query 0x791 PTR 59.64.20.172.in-addr.arpa
2021-02-22 08:34:52.005 -0500	172.20.34.10	172.20.134.10	DNS	85	Standard query response 0x791 Server failure PTR 59.64.20.172.i
2021-02-22 08:34:52.459 -0500	172.20.134.10	172.20.34.10	DNS	85	Standard query 0x0f53 PTR 49.100.10.10.in-addr.arpa
2021-02-22 08:34:52.481 -0500	172.20.34.10	172.20.134.10	DNS	96	Standard query response 0x0f53 Server failure PTR 49.100.10.10.i
2021-02-22 08:34:56.619 -0500	172.20.134.10	172.20.34.10	DNS	85	Standard query 0xaf96 PTR 55.64.20.172.in-addr.arpa
2021-02-22 08:34:56.622 -0500	172.20.34.10	172.20.134.10	DNS	96	Standard query response 0xaf96 Server failure PTR 55.64.20.172.i
2021-02-22 08:34:57.157 -0500	172.20.134.10	172.20.34.10	DNS	85	Standard query 0x791 PTR 59.64.20.172.in-addr.arpa
2021-02-22 08:34:57.177 -0500	172.20.34.10	172.20.134.10	DNS	85	Standard query response 0x791 Server failure PTR 59.64.20.172.i
2021-02-22 08:34:57.622 -0500	172.20.134.10	172.20.34.10	DNS	85	Standard query 0x0f53 PTR 49.100.10.10.in-addr.arpa
2021-02-22 08:34:57.642 -0500	172.20.34.10	172.20.134.10	DNS	96	Standard query response 0x0f53 Server failure PTR 49.100.10.10.i
2021-02-22 08:35:01.780 -0500	172.20.134.10	172.20.34.10	DNS	85	Standard query 0xaf96 PTR 55.64.20.172.in-addr.arpa

Click on Download icon () to download the search pcap for further analysis using Wireshark or any other tools that accept standard pcap files, and Delete icon () to delete this search.

Click on Clone icon () to Clone this search. Any of the fields can be modified:

Note the URL next to the Search Filter that can be used to understand Berkeley Packet Filter (BPF) syntax. Click on **BPF Help** button to understand BPF syntax:



The dialog box is titled "Clone Search". It contains the following fields:

- SearchName: continuum_1631381920_1_rest2_z27ic
- BeginTime: 2021-09-11 6:0:0
- EndTime: 2021-09-11 8:0:0
- Search Filter (URL: https://biot.com/capstats/bpf.html): tcp
- MaxPacketCount: 1000

At the bottom are three buttons: "Create Search" (blue), "Search Library" (blue), and "Cancel Request" (orange).

Click on **Create Search** button to create a new 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 allow 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

continuum_20210910195334 

Seconds Before

30

Seconds After

30

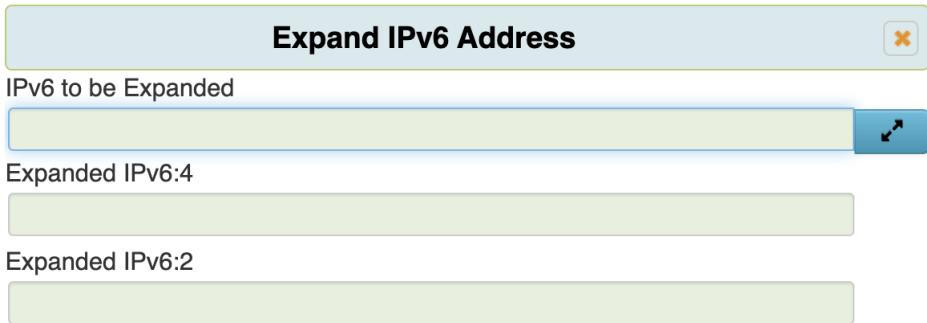
SearchFilter (https://biot.com/capstats/bpf.html)

host 10.91.170.111 and port 80

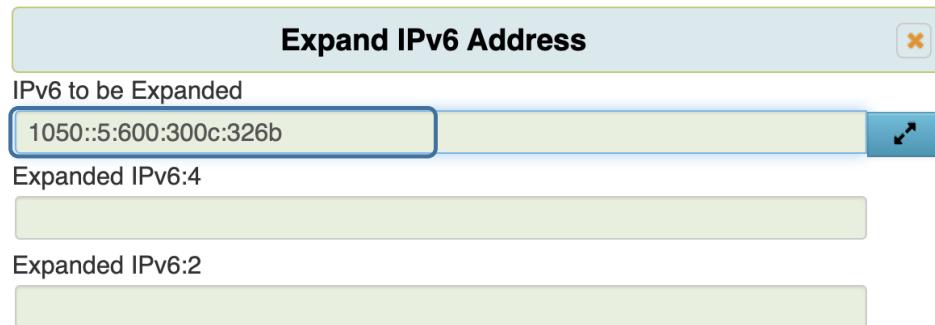
Create Active Trigger **Cancel Request**

2.1.5 Expand IPv6 Address

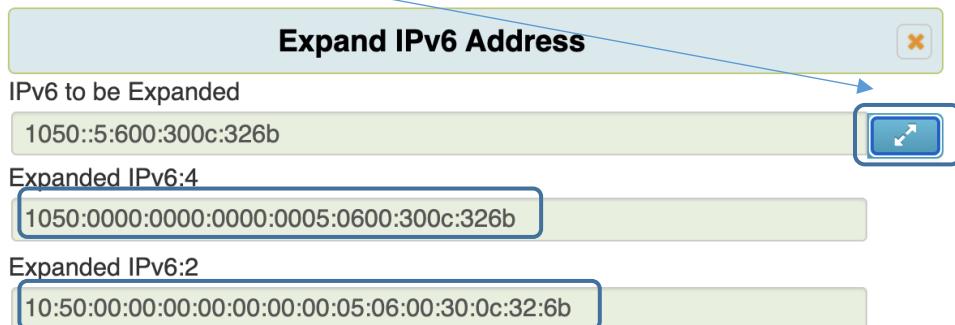
This menu option will pop up a resizable Dialog box that allows users to expand ipv6 addresses. More information about this feature is available in Appendix B.



Enter IPv6 address to be expanded:



Press Expand button:

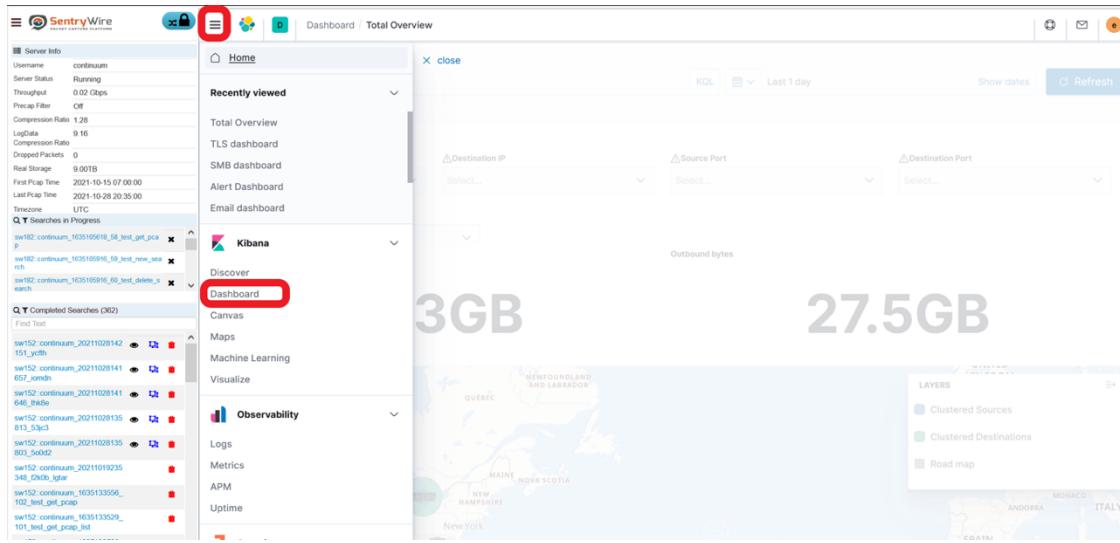


2.2 VISUALIZATIONS AND DASHBOARDS

The following are basic functionality operations for using Elastic Kibana within the SentryWire UI. Kibana allows users to easily and quickly visualize, explore, and search metadata logs generated by SentryWire 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 SentryWire 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

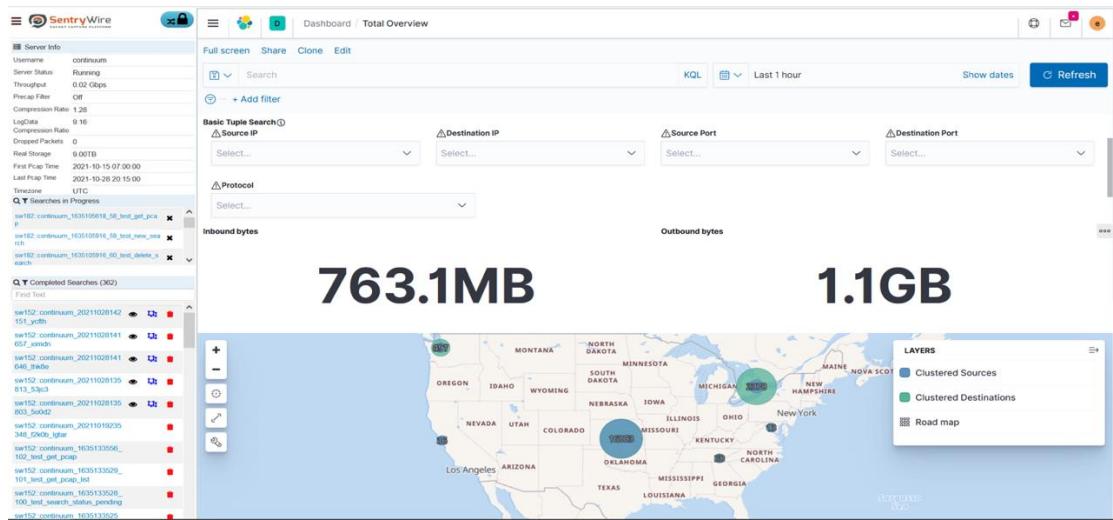


The screenshot shows the SentryWire UI interface. On the left, there is a sidebar with various metrics and search results. In the center, there is a main dashboard area with a map and some statistics. At the top left, there is a navigation menu with three horizontal bars. A red circle highlights this icon. Below it, the menu items include "Home", "Recently viewed", "Discover", "Dashboard" (which is highlighted with a red box), "Canvas", "Maps", "Machine Learning", and "Visualize".

3. 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

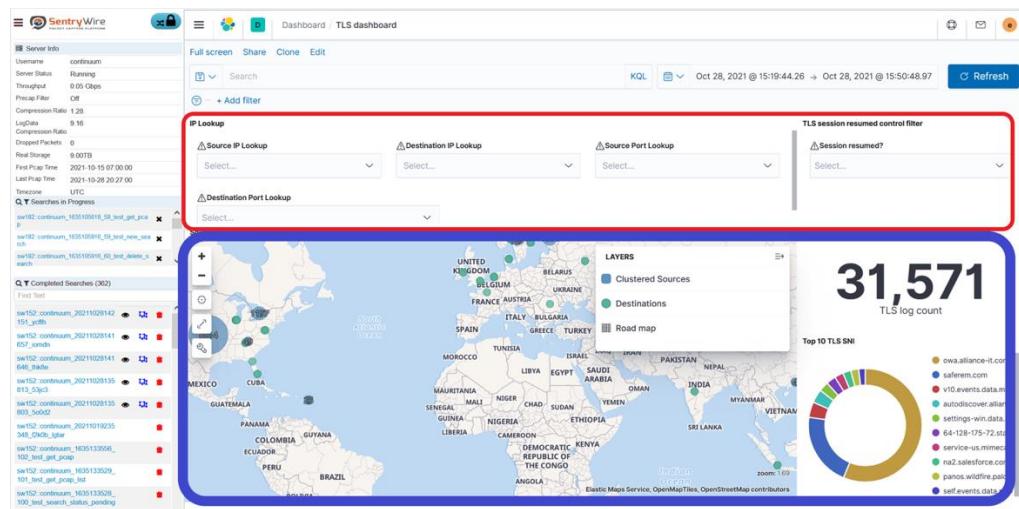
At the bottom of the overview are breakouts of different logs by protocol. By clicking and dragging over sections in the chart, the option to filter by the time span and the option to drill down deeper into the dedicated protocol dashboard will appear. Some protocols have multiple drill down dashboards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

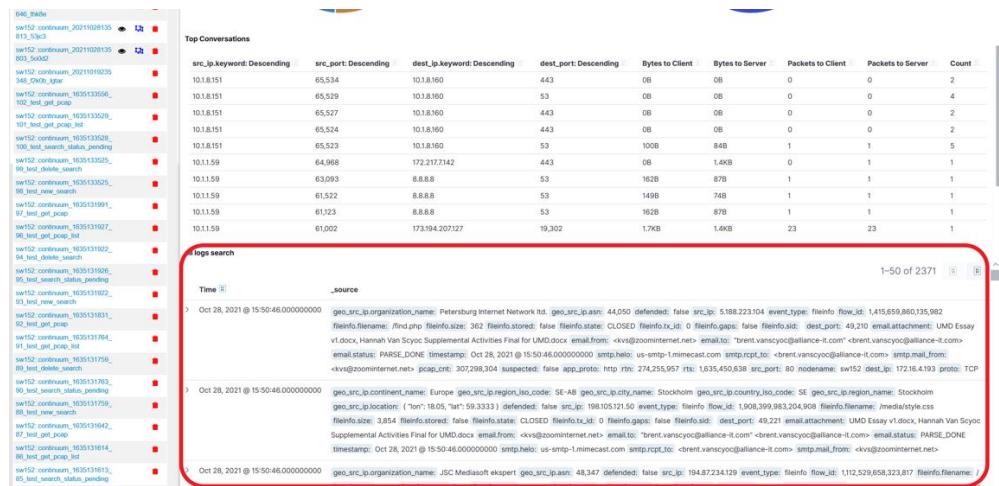


The screenshot shows the SentryWire TLS dashboard. At the top, there's a header with 'SentryWire' logo, 'Dashboard', and 'TLS dashboard'. Below the header are sections for 'Server Info' (including Username: continuum, Server IP: 10.1.1.1, Throughput: 0.05 Gbps, Prefix Filter: Off, Compression Rate: 1.29, LogData: 9.16, Compression Ratio: 1.29, File Storage: 0.00TB, First Pack Time: 2021-10-15 07:00:00, Last Pack Time: 2021-10-29 20:27:00, Timezone: UTC) and 'TLS session resumed control filter' (with a dropdown menu for 'Session resumed?').

The main area features a world map titled 'TLS log count' with a value of 31,571. It includes legends for 'Clustered Sources' (blue dots), 'Destinations' (green dots), and 'Road map' (grey lines). A 'Top 10 TLS SNI' donut chart is also present.

On the left, there's a sidebar titled 'Completed Searches (362)' containing a list of search entries, and a 'Searches in Progress' section with several items listed.

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



The screenshot shows the SentryWire log search viewer. At the top, there's a search bar with placeholder text 'Time [] _source []'. Below the search bar, there are two log entries:

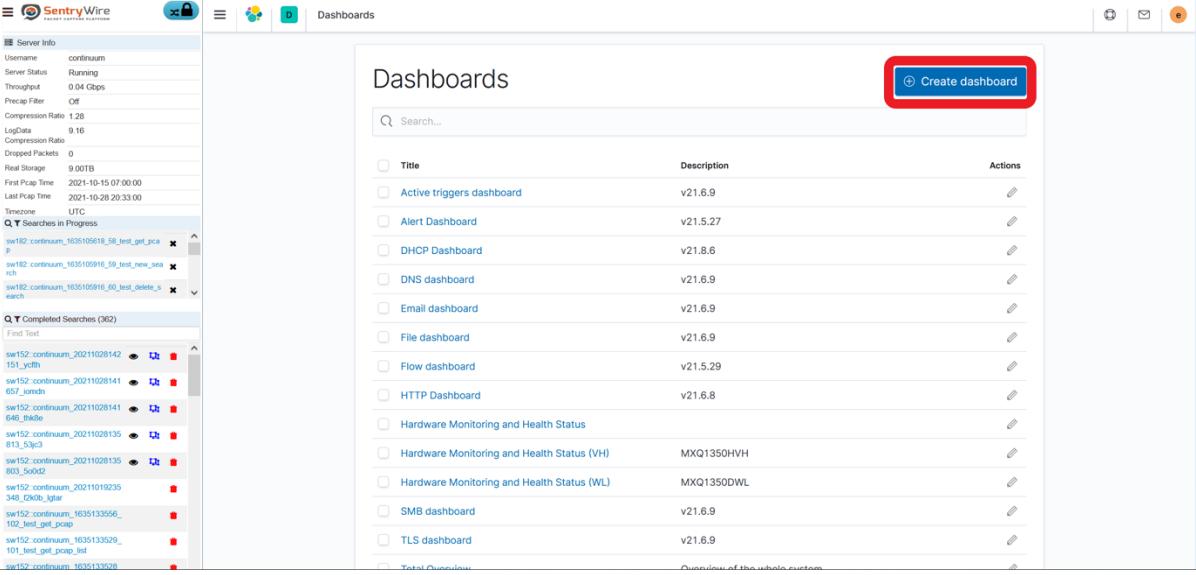
```

Time [Oct 28, 2021 @ 15:50:46.000000000] _source [geo_src_ip_organization_name: Petersburg Internet Network ltd. geo_src_ip_port: 44,050 definded: false geo_ip: 5.188.223.104 event_type: fileinfo flow_id: 1,415,659,860,135,982 fileinfo.filename: /tmp/pd_ fileinfo.size: 362 fileinfo.state: CLOSED fileinfo.id: 0 fileinfo.gaps: false fileinfo.sid: dest_port: 49,210 email.attachment: UMD Essay v1.docx, Hannah Van Scyoc Supplementary Activities Final for UND.docx email.from: <v@zoominternet.net> email.to: <brent.vansycogalliance-it.com> email.status: PARSE_DONE timestamp: Oct 28, 2021 @ 15:50:46.000000000 smtp.helo: us-smtp-1.micemcast.com smtp.rpt_to: direct.vansycogalliance-it.com smtp.mail_from: <v@zoominternet.net> smtp.port: 307,298,304 suspected: false app.protocol: http:// ip: 274,255,957 rts: 16,35,450,638 arc.port: 80 modename: sw12 dest_ip: 172.16.4.193 proto: TCP
Time [Oct 28, 2021 @ 15:50:46.000000000] _source [geo_src_ip_continent_name: Europe geo_src_ip_region_id: 48 geo_src_ip_name: Stockholm geo_src_ip_country_id: SE geo_src_ip_region_name: Stockholm geo_src_ip_location: ('101', '180', '50', '33,331') definded: false geo_ip: 199,105,121,50 event_type: fileinfo flow_id: 1,006,393,93,2,04,908 fileinfo.filename: media/style.css fileinfo.size: 3,054 fileinfo.state: CLOSED fileinfo.id: 0 fileinfo.gaps: false fileinfo.sid: dest_port: 49,221 email.attachment: UMD Essay v1.docx, Hannah Van Scyoc Supplementary Activities Final for UND.docx email.from: <v@zoominternet.net> email.to: <brent.vansycogalliance-it.com> email.status: PARSE_DONE timestamp: Oct 28, 2021 @ 15:50:46.000000000 smtp.helo: us-smtp-1.micemcast.com smtp.rpt_to: direct.vansycogalliance-it.com> smtp.mail_from: <v@zoominternet.net>
    
```

At the bottom, there's a table titled 'Top Conversations' with columns: src_ip.keyword: Descending, src_port: Descending, dest_ip.keyword: Descending, dest_port: Descending, Bytes to Client, Bytes to Server, Packets to Client, Packets to Server, Count. The table lists several conversations between different IP addresses and ports.

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 with the 'Dashboards' section open. On the left, there is a sidebar with 'Server Info' and 'Completed Searches'. The main area displays a list of dashboards with columns for Title, Description, and Actions. A red box highlights the 'Create dashboard' button in the top right corner of the list area.

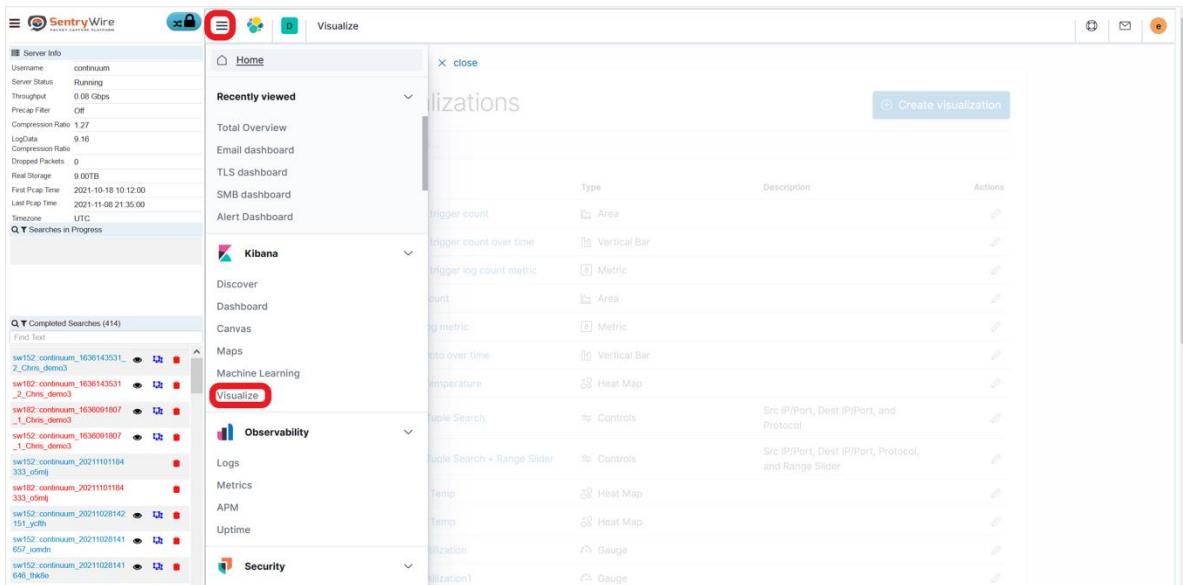
Title	Description	Actions
Active triggers dashboard	v21.6.9	
Alert Dashboard	v21.5.27	
DHCP Dashboard	v21.8.6	
DNS dashboard	v21.6.9	
Email dashboard	v21.6.9	
File dashboard	v21.6.9	
Flow dashboard	v21.5.29	
HTTP Dashboard	v21.6.8	
Hardware Monitoring and Health Status		
Hardware Monitoring and Health 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	

2.2.6 Creating a new visualization

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

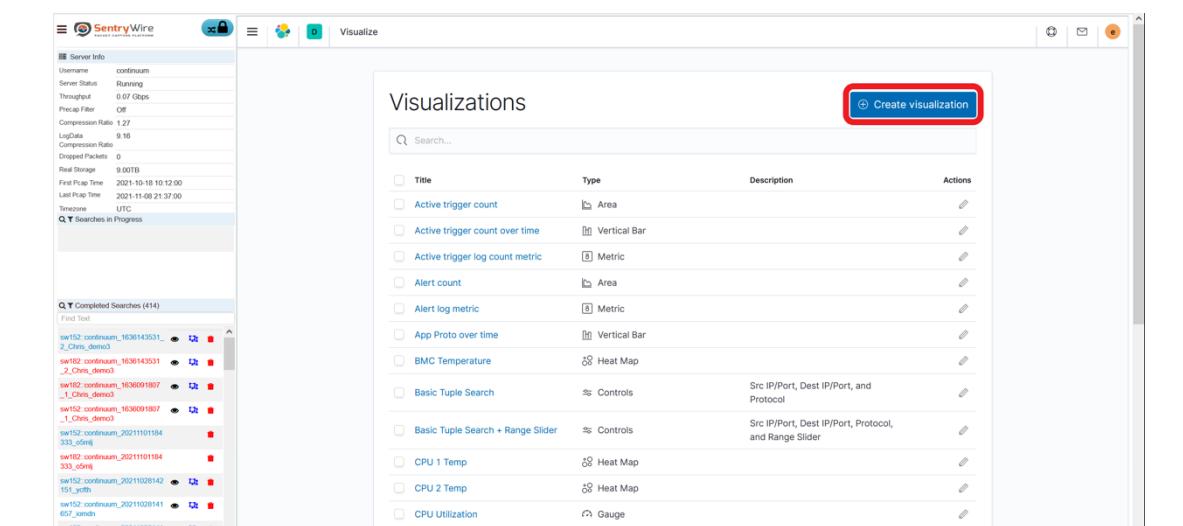
1. Click on the 3 bars at the top left of the screen to open the drop-down menu
2. Click on Visualize
3. Click on the Create visualization button
4. On the pop-up menu, select the desired style of visualization. This tutorial will use “Pie”.
5. Choose a saved index to use as the data set for the visualization
 - a. The index will be “investigate-*” for almost all SentryWire 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



The screenshot shows the SentryWire interface with the 'Visualize' section open. The 'Create visualization' button is highlighted with a red box.

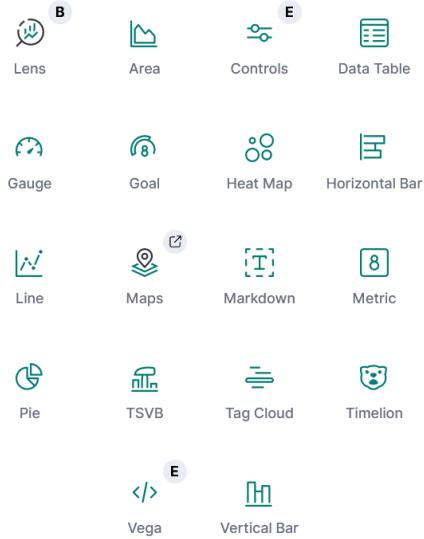
Title	Type	Description	Actions
Active trigger count	Area		
Active trigger count over time	Vertical Bar		
Active trigger log count metric	Metric		
Alert count	Area		
Alert log metric	Metric		
App Proto over time	Vertical Bar		
BMC Temperature	Heat Map		
Basic Tuple Search	Controls	Src IP/Port, Dest IP/Port,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



The screenshot shows the SentryWire interface with the 'Visualize' section open. The 'Create visualization' button is no longer visible in the top right corner of the 'Visualizations' panel.

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

New Visualization

 Filter

Select a visualization type

Start creating your visualization by selecting a type for that visualization.

Try **Lens**, our new, intuitive way to create visualizations.

[Go to Lens](#)

New Pie / Choose a source

 Search...Sort Types 2

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

< [1](#) [2](#) >

The screenshot shows three vertically stacked SentryWire interface windows, each displaying a search results table and a large teal circular progress bar.

Top Window:

- Left Panel (Server Info):**
 - Server Status: Running
 - Throughput: 0.0 Gbps
 - Preproc Filter: Off
 - Compression Rate: 1.27
 - LogData: 9.16
 - Dropped Packets: 0
 - Real Storage: 0.00TB
 - First Prep Time: 2021-10-18 10:23:00
 - Last Prep Time: 2021-10-08 21:41:00
 - Timezone: UTC
- Middle Panel (Completed Searches):** Shows 414 completed searches. A specific entry is highlighted: `sw152_continuum_1636143531_1_Chris_demo3`.
- Right Panel (Metrics & Buckets):**
 - Metrics:** Slice size Count
 - Buckets:** ADD BUCKET, Split slices (highlighted)

Middle Window:

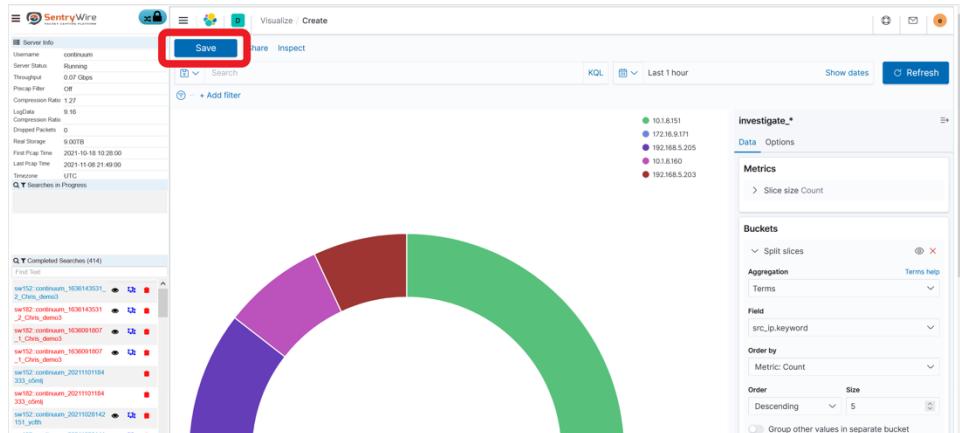
- Left Panel (Server Info):** Same configuration as the top window.
- Middle Panel (Completed Searches):** Shows 414 completed searches. A specific entry is highlighted: `sw152_continuum_1636143531_1_Chris_demo3`.
- Right Panel (Metrics & Buckets):**
 - Aggregation:** Terms (highlighted)
 - Field:** src_ip.keyword
 - Order by:** Metric: Count
 - Order:** Descending, Size (highlighted)
 - Custom label:** Top 5 Source IPs (highlighted)

Bottom Window:

- Left Panel (Server Info):** Same configuration as the top window.
- Middle Panel (Completed Searches):** Shows 414 completed searches. A specific entry is highlighted: `sw152_continuum_1636143531_1_Chris_demo3`.
- Right Panel (Metrics & Buckets):**
 - Order by:** Metric: Count
 - Order:** Descending, Size (highlighted)
 - Custom label:** Top 5 Source IPs

Action Buttons:

- Top Window:** Split slices (highlighted)
- Middle Window:** Update (highlighted)



Save visualization

Title

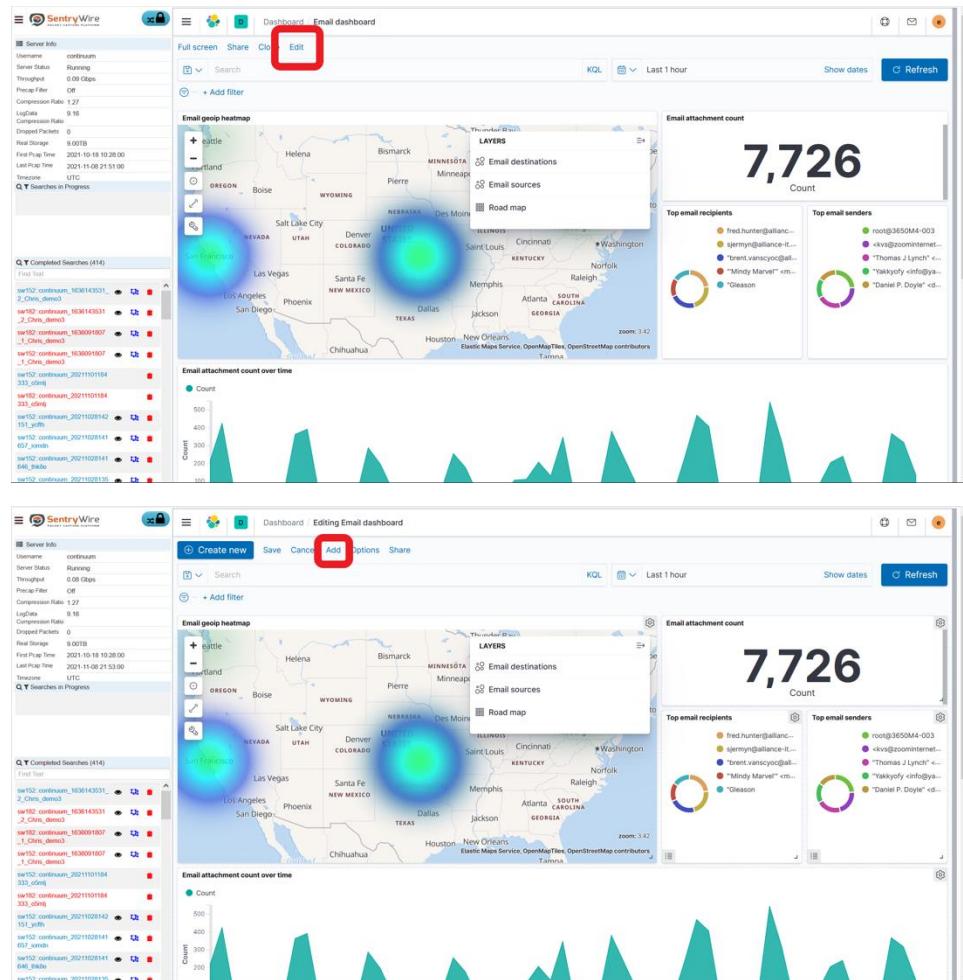
Description

Cancel
Save

2.2.7 Adding a visualization to a dashboard

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

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



The image consists of two vertically stacked screenshots of the SentryWire dashboard. Both screenshots show a similar layout with a sidebar on the left containing 'Server Info' and 'Completed Searches' lists, and a main area with several visualizations. In the top screenshot, the top navigation bar has 'Edit' highlighted with a red box. In the bottom screenshot, the top navigation bar has 'Create new' highlighted with a red box. The visualizations include an 'Email geoip heatmap' showing activity across the US and abroad, an 'Email attachment count' chart with a large value of 7,726, and a list of 'Top email recipients' and 'Top email senders'.

The dashboard displays various metrics and visualizations:

- Server Info:** Shows current status (Running), throughput (0.08 Gbps), and compression ratios.
- Completed Searches (414):** A list of completed searches with timestamps and file names.
- Email attachment count over time:** A line chart showing the count of attachments over time.
- Email geoip heatmap:** A map of the United States showing email attachment counts by location.
- Add panels:** A modal for adding new panels to the dashboard, with a search bar for "Top 5" and a red box highlighting the "Create new" button.
- Logs:** A detailed log entry for Nov 8, 2021, at 16:58:54, showing SMB commands like `SMB2_COMMAND_READ` and `SMB2_COMMAND_WRITE` with their respective parameters and session details.
- Top 5 Source IPs:** A donut chart showing the distribution of top 5 source IPs.
- Dashboard (unsaved):** A second version of the dashboard with similar components but different data.

X

Save dashboard

 Save as new dashboard

Title

Email dashboard

Description

v21.6.9

 Store time with dashboard

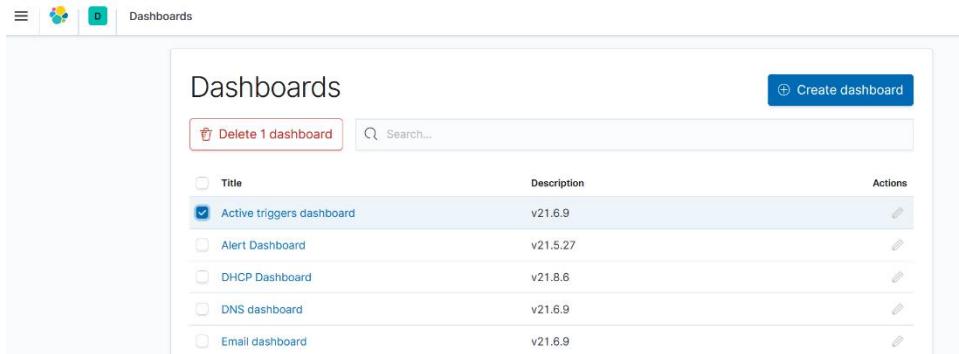
This changes the time filter to the currently selected time each time this dashboard is loaded.

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



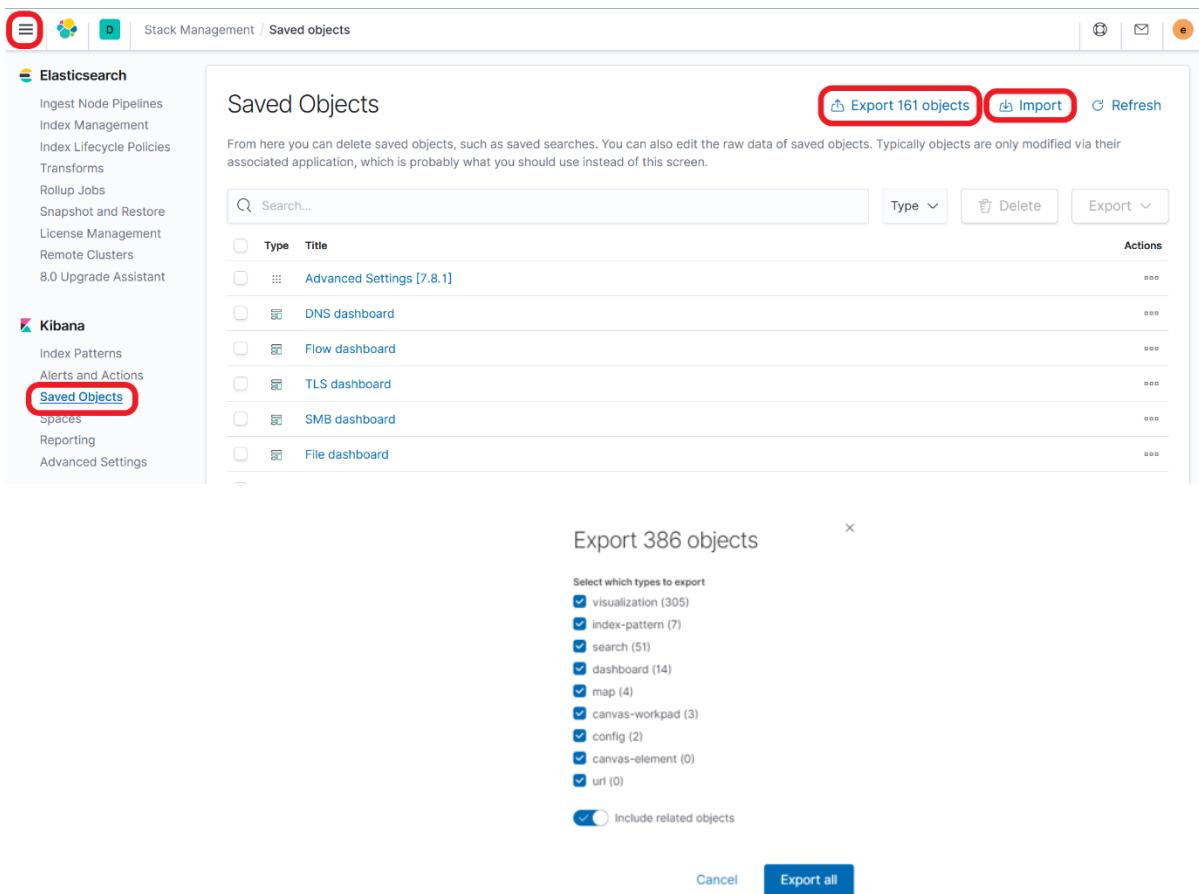
The screenshot shows the SentryWire interface with the "Dashboards" section open. At the top, there is a red button labeled "Delete 1 dashboard". Below it is a search bar with the placeholder "Search...". A table lists five dashboards:

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	

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.

Export 161 objects Import Refresh

Type	Title	Actions
<input type="checkbox"/>	Advanced Settings [7.8.1]	...
<input type="checkbox"/>	DNS dashboard	...
<input type="checkbox"/>	Flow dashboard	...
<input type="checkbox"/>	TLS dashboard	...
<input type="checkbox"/>	SMB dashboard	...
<input type="checkbox"/>	File dashboard	...

Search... Type Title Actions

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

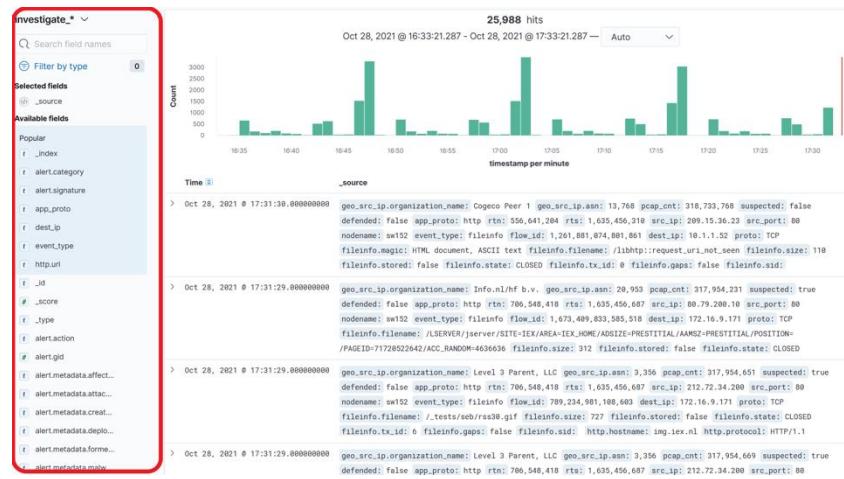
2.2.10 Discover

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 SentryWire UI or to confirm events or alerts seen on other appliances

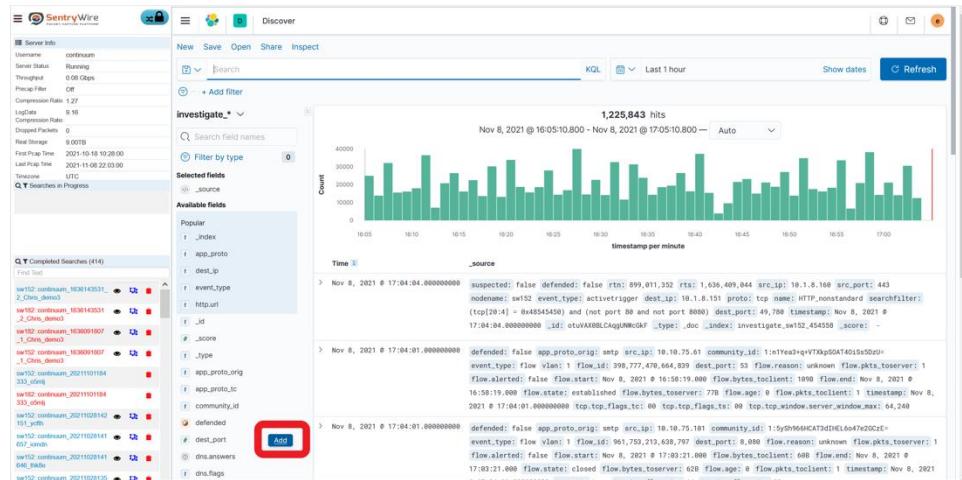
2.2.11 Pin a field to a column

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

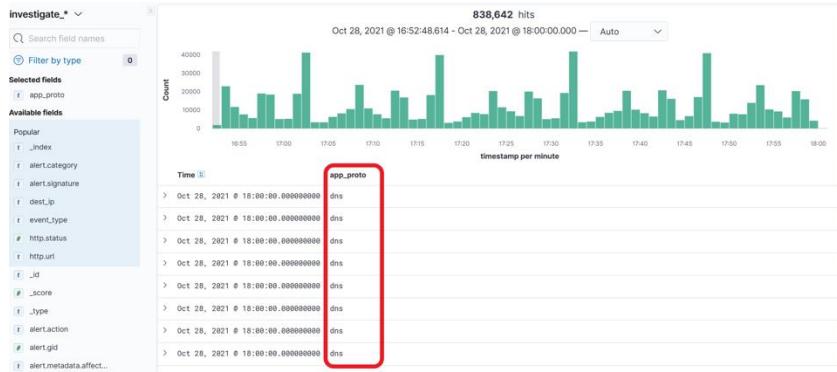


The screenshot shows the SentryWire Discover interface. On the left, there's a sidebar titled 'investigate_*' with a search bar and a 'Filter by type' button. Below it, under 'Selected fields', is a list of fields: '_index', '_score', '_type', 'alert.action', 'alert.gid', 'alert.metadata.affect...', 'alert.metadata.attac...', 'alert.metadata.creat...', 'alert.metadata.depl...', 'alert.metadata.form...', and 'alert.metadata.mobi...'. To the right is a histogram titled '25,988 hits' showing the count of hits per minute from 10:35 to 17:30. Below the histogram is a list of log entries for October 28, 2021, each with a timestamp, source, and detailed log information.

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



This screenshot shows the SentryWire Discover interface with a different set of logs. The sidebar on the left shows 'Completed Searches (414)' and a list of search names. The main area has a histogram titled '1,225,843 hits' and a list of log entries for November 8, 2021. A red box highlights the 'Selected fields' section in the sidebar, and another red box highlights the 'Add' button at the bottom of the sidebar.



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:

```
ntp.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:

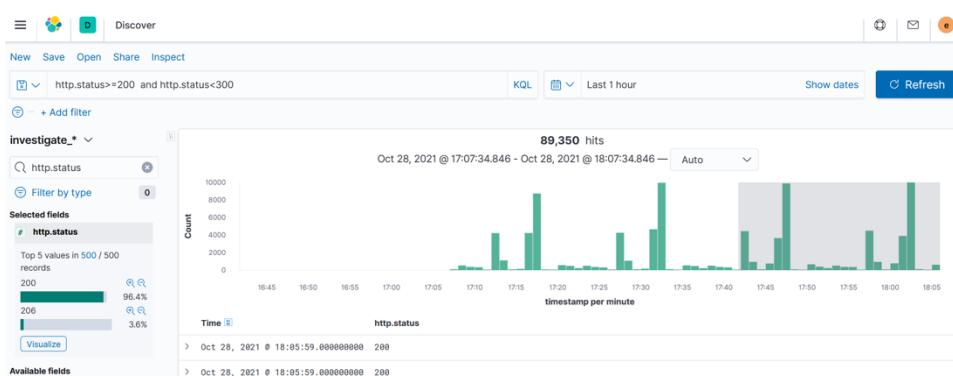
```
not dest_port : 80
```

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.

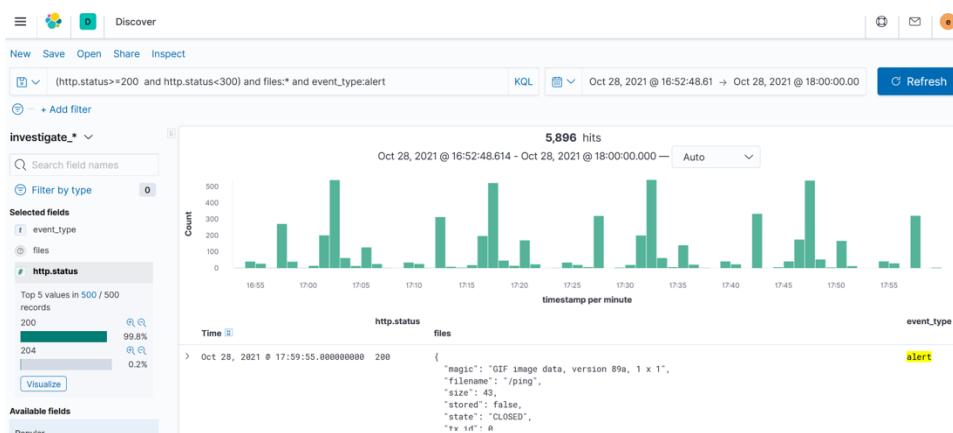
Example query to return all DNS logs for a specific source:

```
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)
```

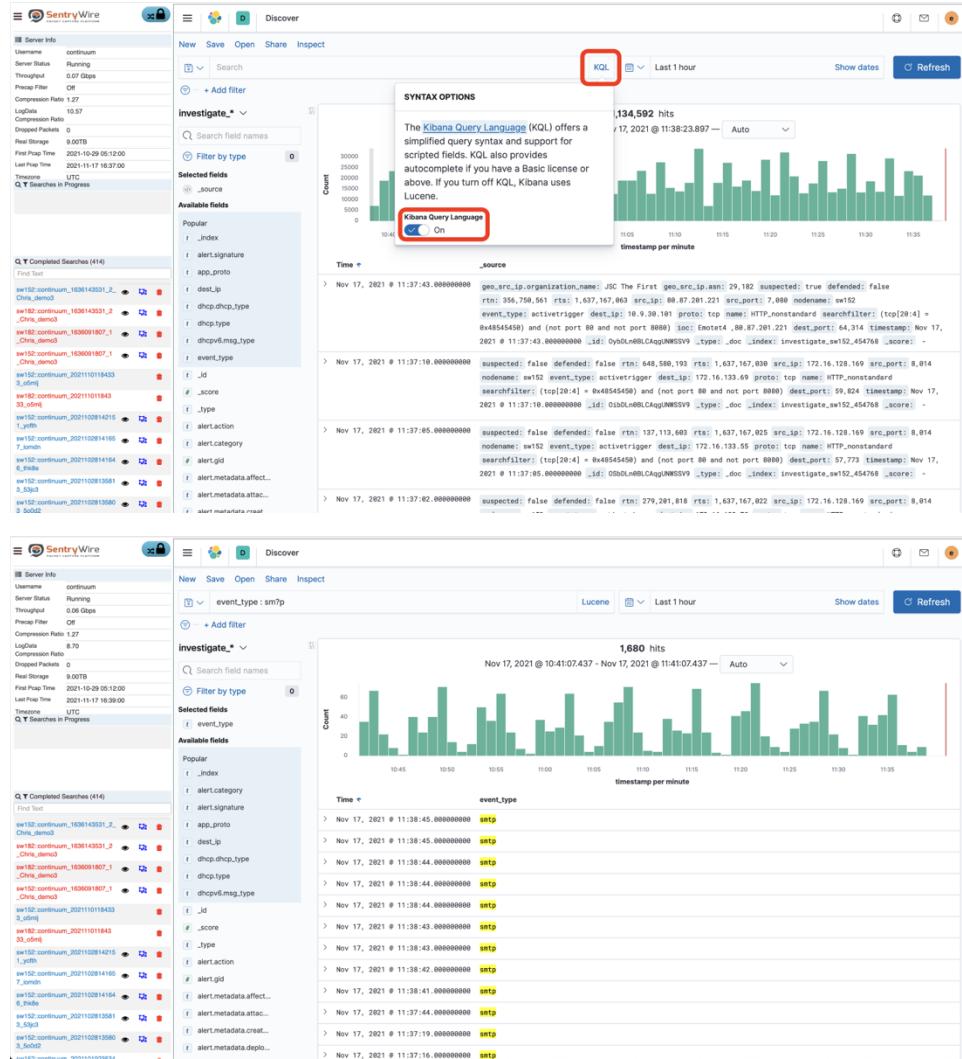


This query displays results that do not use destination port 80 or 443 but contain successful http status codes where at least one file was seen.

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



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

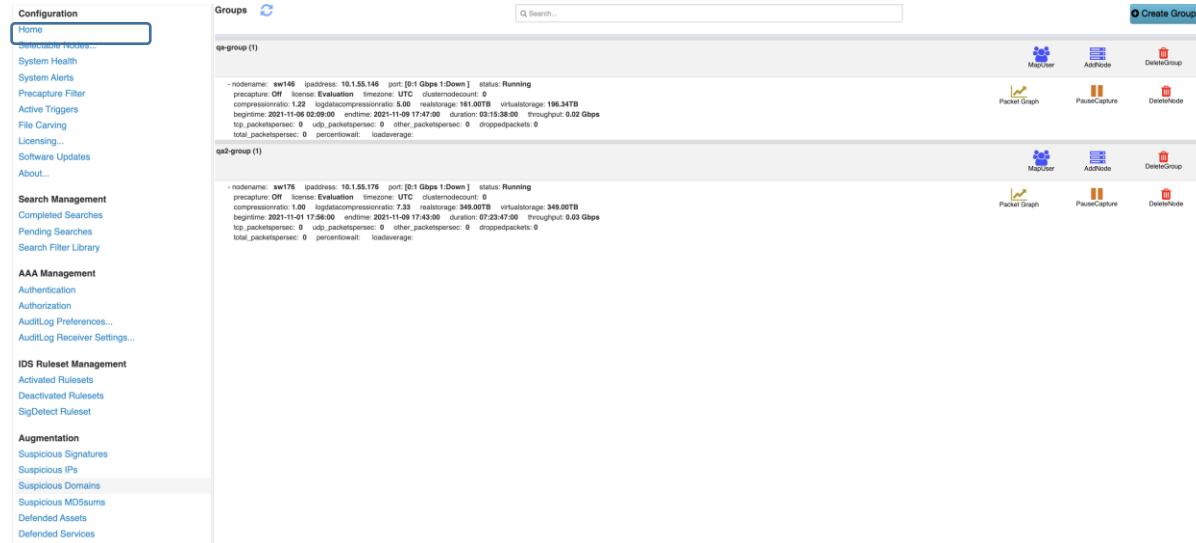
The Home button shows the Groups and Nodes of the Federation Manager. Top of the Admin UI page shows the currently logged in user's name, user's role, authentication mode and product version. The following sections describe each of the options available on the left panel and the actions/views based on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

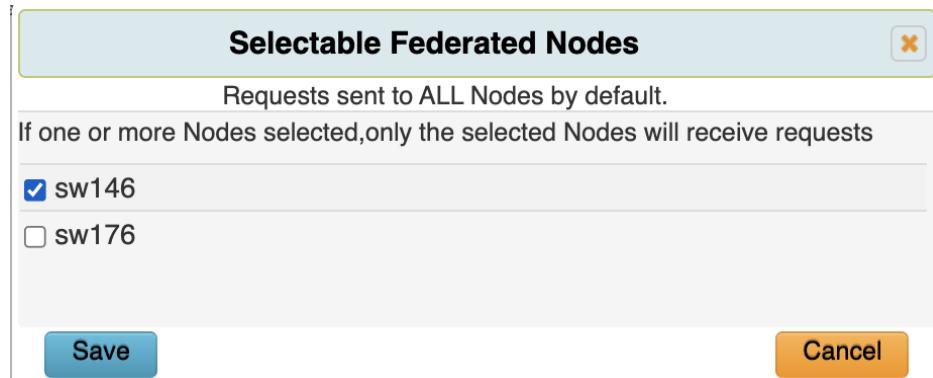
- The advertised throughput includes system resource calculations for packet processing. As such, the throughput is measured as it reaches the interface, not after internal processing. This allows us to ensure we do not drop packets, while still giving accurate metrics.
- Delete Node: A node can be deleted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



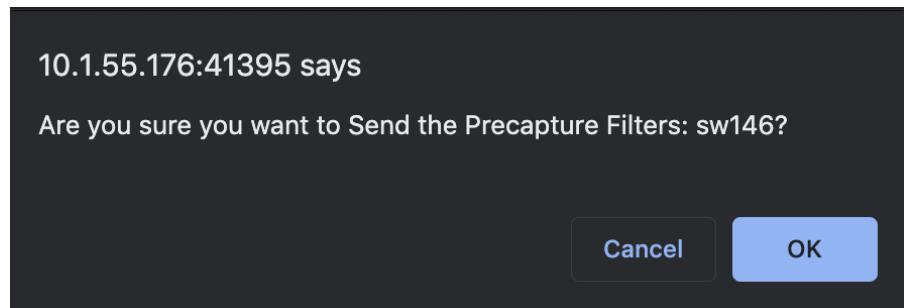
The screenshot shows the SentryWire Configuration interface. On the left, there's a sidebar with various management sections like Configuration, Search Management, AAA Management, and IDS Ruleset Management. The main area displays two groups: 'qa-group (1)' and 'qa2-group (1)'. Each group has detailed node information, including node name, IP address, port, status, and log statistics. To the right of each group are three buttons: 'Map User' (blue), 'Add Node' (green), and 'Delete Group' (red). Below the groups are three more buttons: 'Packet Graph' (blue), 'Pause Capture' (green), and 'Delete Node' (red).

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.

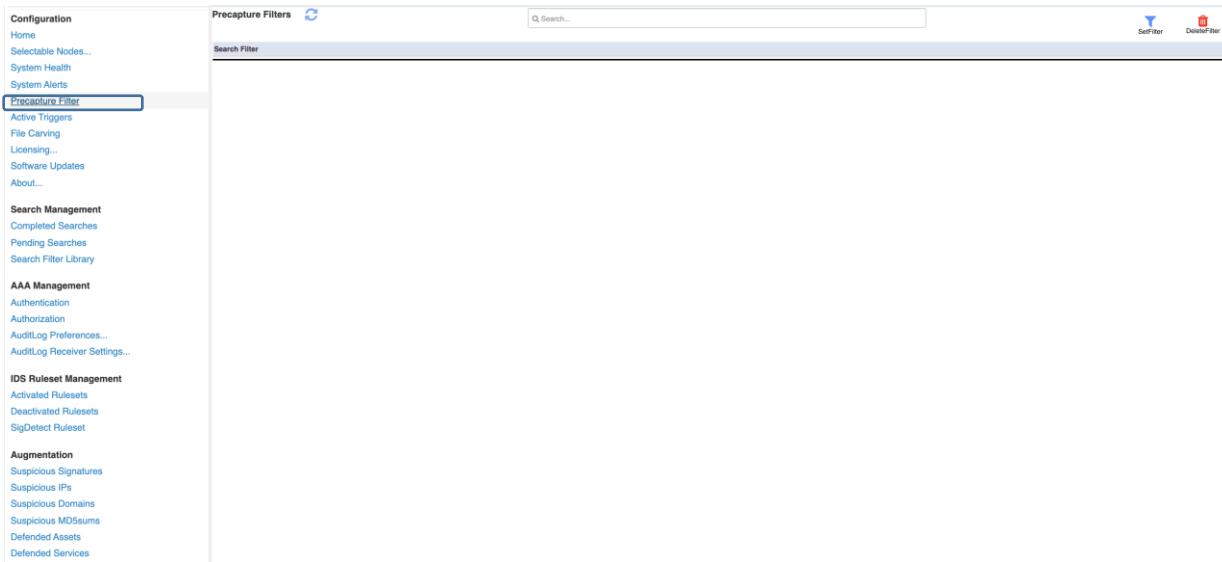


From this point on, when a request such as SetPrecapture is initiated, the user is presented with the list of nodes that are going to receive this request:



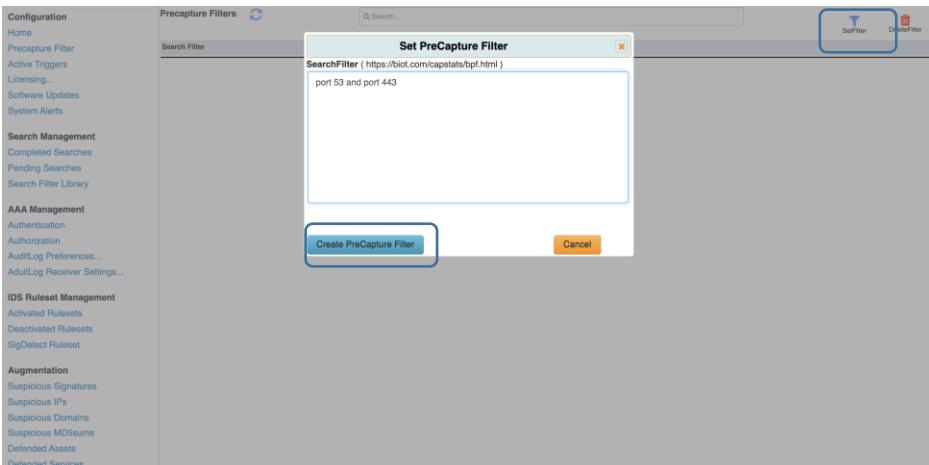
3.1.3 Precapture Filter

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.

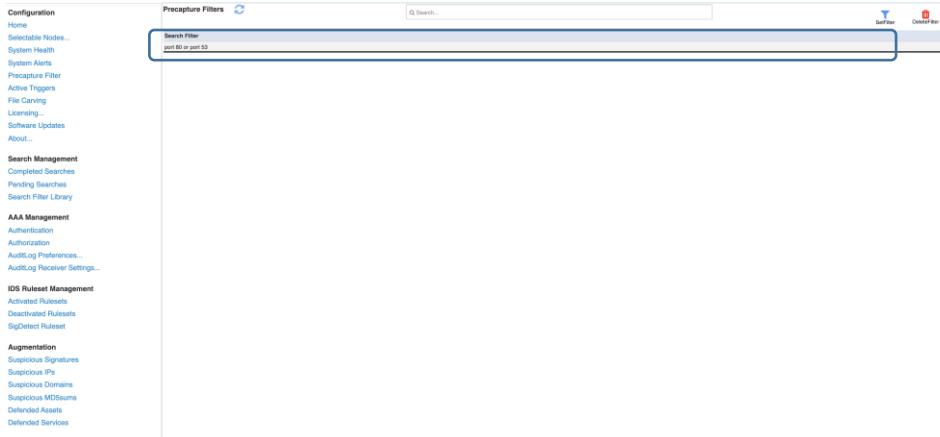


The screenshot shows the SentryWire Configuration interface. The left sidebar contains several sections: Home, Selectable Nodes..., System Health, System Alerts, **Procedure Filter** (which is highlighted with a blue border), Active Triggers, File Carving, Licensing..., Software Updates, About..., Search 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, and Defended Services.

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



The screenshot shows a 'Set PreCapture Filter' dialog box. The search bar contains 'SearchFilter (https://biot.com/capstats/bpf.html)'. The text area below contains the filter rule: 'port 53 and port 443'. At the bottom are two buttons: 'Create PreCapture Filter' (highlighted with a blue border) and 'Cancel'.



The screenshot shows the SentryWire interface with a sidebar on the left containing various management and monitoring links. The main area features a search bar at the top and a large, empty workspace below it.

- Configuration**
 - Nodes...
 - Selectable Nodes...
 - System Health
 - System Alerts
 - Precapture Filter
 - Active Triggers
 - File Carving
 - Licensing...
 - Software Updates
 - About...
- 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
 - SigDeter RuleSet
- Augmentation**
 - Suspicious Signatures
 - Suspicious IPs
 - Suspicious Domains
 - Suspicious MD5sums
 - Defended Assets
 - Defended Services

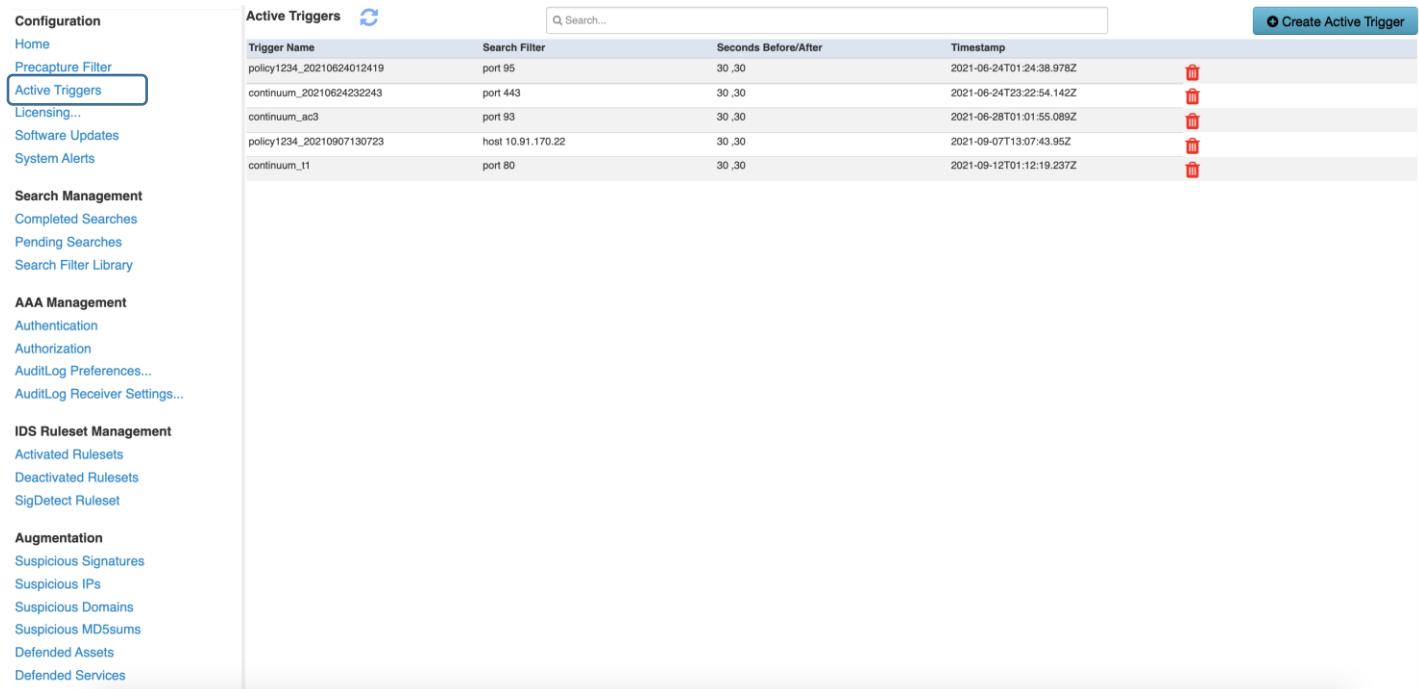
Precapture Filters   

Search Filter  port 80 or port 133

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
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 SentryWire 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.

There are three types of FC Workflows:

- Streaming FC Workflow
Files extracted from traffic stream, de-duplicated and sent to a file handler
- On-demand FC UI Workflow
- On-demand FC REST Workflow

Configuration	File Carving			Q Search...	FC Configuration...	FC On Demand...	FC Help...	
	Date	NodeName	Status(Code)		File Name			
Home	2021-11-01T17:33:09Z	sw143	forwarded(200)	68.71.216.175_80_172.16.133.98_53395_4ceac07973d82d46928d76ec6ce0e0575409ce408708072087268c94615c598				
System Health	2021-11-01T17:33:09Z	sw143	forwarded(200)	69.147.86.184_80_172.16.133.98_53594_952f9ad5b919e69a0c7863738103208d1led6a56b7889b13f16e0c5c45				
System Alerts	2021-11-01T17:33:09Z	sw143	forwarded(200)	74.208.215.199_80_192.168.1.96_49212_256f26c04ccbdde6536615def0bb1136c86f6afe5dc22da7c6c1c93f1fbfa5				
Select Destination Nodes...	2021-11-01T17:33:09Z	sw143	forwarded(200)	80.93.82.33_80_192.168.1.96_49255_02fe78cc01e2004744f4fc5822759e9b943820bfef7fe0a79585062e2e8ca				
Precapture Filter	2021-11-01T17:33:09Z	sw143	forwarded(200)	84.53.136.152_80_172.16.9.171_2782_b611df63f0fc0a0f8c1089fffa50aae5d5dd9c29ad5d631a6893b7e431d				
Active Triggers	2021-11-01T17:33:09Z	sw143	forwarded(200)	94.126.17.113_80_192.168.1.96_50057_4b673d13a5783029ca344a3bfffcc9381ee9c0998e7ec0cafb1b100f41467396				
File Carving	2021-11-01T17:33:08Z	sw143	forwarded(200)	50.97.85.91_80_192.168.1.96_49264_8261d79352f7ca9681e19c91266cb538869a07d46939e7c782d41fce00239				
Licensing...	2021-11-01T17:33:08Z	sw143	forwarded(200)	52.204.154.173_80_192.168.1.96_49883_9ef5dd4a4818d802d807fe7ff7790318ed2f7b692a0728143558ded2b8d1				
Software Updates	2021-11-01T17:33:08Z	sw143	forwarded(200)	59.106.13.181_80_192.168.1.96_50005_04025fd9c9e3deda41a6cae0301b01a697514a59f60c05794d88c5c4e				
Search Management	2021-11-01T17:33:08Z	sw143	forwarded(200)	62.69.184.129_80_172.16.9.171_2611_ca26c0314c52b5a511582d69e6326c4d00d7b64fa366c7f6713a239d8a9c79				
Completed Searches	2021-11-01T17:33:08Z	sw143	forwarded(200)	62.75.251.116_80_192.168.1.96_49544_0782d6c937a24eefabcf0febe178ab31a2c533319055605a0d1e28320488				
Pending Searches	2021-11-01T17:33:08Z	sw143	forwarded(200)	64.17.236.31_80_172.16.133.153_35048_7269a79fe25c8747ce644254884663b4b7540e78fc9fffb68086508e9b				
Search Filter Library	2021-11-01T17:33:08Z	sw143	forwarded(200)	64.215.253.17_80_172.16.133.40_50109_5b80b156219a03321014127ebaa3f73a18f5000751d2179a2416fead39				
AAA Management	2021-11-01T17:33:08Z	sw143	forwarded(200)	65.254.227.240_80_10.3.1.218_49791_dfcffca3491a2af9d52d5c68625259fb1b1284c24586bd1571d195c207b2050				
Authentication	2021-11-01T17:33:07Z	sw143	forwarded(200)	65.254.227.240_80_10.3.1.218_49792_def548b8025b8434d81dc3b4259432343b34d51f7bc7029b78bbff14b545				
Authorization	2021-11-01T17:33:07Z	sw143	forwarded(200)	65.254.227.240_80_10.3.1.218_49793_cfbd76425f0323c0cb13b05a099fa40c01b0bd3b652f3933d4b318126				
Audit Log Preferences...	2021-11-01T17:33:07Z	sw143	forwarded(200)	65.254.227.240_80_10.3.1.218_49794_02054e93b0c7551d5f6874829ff1b2885d5d9ae922d148cb785b6a0f022a65				
Audit Log Receiver Settings...	2021-11-01T17:33:07Z	sw143	forwarded(200)	213.186.33.16_80_192.168.1.96_49644_34fc40eb9483412e02d03aa7232190639a39edfe0e1b872cd0ff86ba929				
IDS Ruleset Management	2021-11-01T17:33:07Z	sw143	forwarded(200)	213.186.33.17_80_192.168.1.96_49268_66c6c2b9494713afad7547ff0f4737a4b3a4e371a734d9754e13f9le992082596b				
Activated Rulesets	2021-11-01T17:33:07Z	sw143	forwarded(200)	216.151.187.105_80_172.16.133.48_60330_884bf48acd9e7f989cd6498c921c13328a02805077ca705ad105071e0f95				
Deactivated Rulesets	2021-11-01T17:33:07Z	sw143	forwarded(200)	216.38.163.167_80_172.16.133.163_3668_4704394e823a6c21a8881da7899418535330b5946293236a3d995265292				
SigDetect Ruleset	2021-11-01T17:33:07Z	sw143	forwarded(200)	216.52.121.204_80_172.16.133.41_52639_90845a966c5153052ff9d028627c7923ad6f83865c002f2a65d8f71470				
Augmentation	2021-11-01T17:33:07Z	sw143	forwarded(200)	219.94.128.87_80_192.168.1.96_49781_01b7d25434e0fb743d96e809bca821c9d92dcfc8e83754c51d3f9le992082596b				
Suspicious Signatures	2021-11-01T17:33:06Z	sw143	forwarded(200)	219.94.128.87_80_192.168.1.96_49816_70abf02c181fb44a956d7c873959f7ceee5b754e51d3f9le992082596b				
Suspicious IPs	2021-11-01T17:33:06Z	sw143	forwarded(200)	219.94.128.87_80_192.168.1.96_49817_47ffab22d73a3d0b9a140e006c929ff0e15d5055ffef1e3d54f48e6100e0301ec				
Suspicious Domains	2021-11-01T17:33:06Z	sw143	forwarded(200)	219.94.128.87_80_192.168.1.96_49818_192.213.122.34_80_86_860bb0de0a0b92abde7ecaf54fb4e4451ad7153d35480eccb820187733d953				
Suspicious MD5sums	2021-11-01T17:33:06Z	sw143	forwarded(200)	219.94.128.87_80_192.168.1.96_49819_198.1.96.50061_194.213.122.34_80_86_860bb0de0a0b92abde7ecaf54fb4e4451ad7153d35480eccb820187733d953				
Defended Assets	2021-11-01T17:33:06Z	sw143	forwarded(200)	219.94.128.87_80_192.168.1.96_49820_a0d493f88e4f4a03f082e6b03d6c5b88845193921b1a65682721789137				
Defended Services	2021-11-01T17:33:06Z	sw143	forwarded(200)	219.94.128.87_80_192.168.1.96_49821_g92148e4921ac5cd5b87c3f88a				
	2021-11-01T17:33:06Z	sw143	forwarded(200)	202.93.17.181_80_192.168.1.96_49352_093f120319f23cae05faae92e65d38ba9087c34c6448cae3707411cb73209				

The File Carving configuration for streaming workflow can be updated by clicking on FC Configuration button:

Configuration	File Carving	FC Configuration...	FC On Demand...	FC Help...																																																																																																																																																	
Selectable Nodes...																																																																																																																																																					
System Health																																																																																																																																																					
System Alerts																																																																																																																																																					
Precapture Filter																																																																																																																																																					
Active Triggers																																																																																																																																																					
File Carving	<table border="1"> <thead> <tr> <th>Date</th> <th>NodeName</th> <th>Status(Code)</th> <th>File Name</th> </tr> </thead> <tbody> <tr><td>2021-11-09T18:09:03Z</td><td>sw176</td><td>forwarded(200)</td><td>23.60.139.27,_80_10.5.14.102,_49734,_4289353b88d7e7fa967461305f1ebc2f0410008b8b2aadf4ce0770279dd140</td></tr> <tr><td>2021-11-09T18:09:03Z</td><td>sw176</td><td>forwarded(200)</td><td>23.60.139.27,_80_10.5.14.102,_49735,_4972eadfb8ed253ffbc9158fc029025634499302aef0a281bd3b67113443d</td></tr> <tr><td>2021-11-09T18:09:03Z</td><td>sw176</td><td>forwarded(200)</td><td>23.60.139.27,_80_10.5.14.102,_49736,_2d20a05fbdb6f67765a481344af5d1f257446d3e9d928984c2036090903</td></tr> <tr><td>2021-11-09T18:09:03Z</td><td>sw176</td><td>forwarded(200)</td><td>23.60.139.27,_80_10.5.14.102,_49737,_5be85a367a5f52004c2a9df986a3fb9e01cd37f7859975c5820c6035ea909d</td></tr> <tr><td>2021-11-09T18:09:03Z</td><td>sw176</td><td>forwarded(200)</td><td>23.60.139.27,_80_10.5.14.102,_49738,_aeafad9e950eae755bae03d183834c78d07b058debe3e977aee0506</td></tr> <tr><td>2021-11-09T18:09:03Z</td><td>sw176</td><td>forwarded(200)</td><td>0.14.102,_49737,_2acab1228e9353c5fd50f75b8a19698fc0b780c08f7993c9cf799af7a96e4e</td></tr> <tr><td>2021-11-09T18:09:03Z</td><td>sw176</td><td>forwarded(200)</td><td>5.14.102,_49737,_beb2e653c3485d1c2e53b8e2429183e0dd987de71652371700aa89337128</td></tr> <tr><td>2021-11-09T18:09:03Z</td><td>sw176</td><td>forwarded(200)</td><td>172.16.133.194,_48311,_49886e62c4463c3178573dc31533cb2b67a797c2034646c9567c2698fd5</td></tr> <tr><td>2021-11-09T18:09:02Z</td><td>sw176</td><td>forwarded(200)</td><td>2.16.133.54,_46410,_a05369e03232547a2a969e34311ea114237cc2e1837eb459e3f67a67bf</td></tr> <tr><td>2021-11-09T18:09:02Z</td><td>sw176</td><td>forwarded(200)</td><td>5.14.102,_49733,_31299f5e001383cbfb8aaffa0384186795a25aadd50f9e23d217c0404aa0a2</td></tr> <tr><td>2021-11-09T18:09:02Z</td><td>sw176</td><td>forwarded(200)</td><td>8.151,_51910,_bd3ecf5abbd04092a0fa6a70704289c991273cd3d1f9798e6b0a719b390a87</td></tr> <tr><td>2021-11-09T18:09:02Z</td><td>sw176</td><td>forwarded(200)</td><td>8.151,_51911,_c5091_40325a80c0c19587b17808d1010aee5fa965959efef54a8d185ec038738</td></tr> <tr><td>2021-11-09T18:09:02Z</td><td>sw176</td><td>forwarded(200)</td><td>172.16.133.194,_48312,_49886e62c4463c3178573dc31533cb2b67a797c2034646c9567c2698fd5</td></tr> <tr><td>2021-11-09T18:09:02Z</td><td>sw176</td><td>forwarded(200)</td><td>2.16.133.54,_46411,_2d9e28ccb8301d404e6e88a8b202015457725588035ac56864e52098363</td></tr> <tr><td>2021-11-09T18:04:53Z</td><td>sw176</td><td>forwarded(200)</td><td>16.151,_51913,_e1882330c102883674474dfe44e4ac0b50e0de789597513480e0e2be7525d</td></tr> <tr><td>2021-11-09T18:04:53Z</td><td>sw176</td><td>forwarded(200)</td><td>16.133.54,_43406,_8d2c1e440725c278bb8df7b477baa3b35a10731311f1a1b1faa187d5</td></tr> <tr><td>2021-11-09T18:04:53Z</td><td>sw176</td><td>forwarded(200)</td><td>16.133.54,_43407,_e46370afaf669a72567a53c3290015b69f778e2890232556de5ee5659386</td></tr> <tr><td>2021-11-09T18:04:53Z</td><td>sw176</td><td>forwarded(200)</td><td>16.133.54,_43408,_1620e5c527a987147641c0c7220a4edc447d707cdca4637072c0393373a8f</td></tr> <tr><td>2021-11-09T18:04:53Z</td><td>sw176</td><td>forwarded(200)</td><td>16.133.54,_43409,_ce4e4f9a933aae106d23aa96c6d20a466466dd0a7a4677cd7a945ad586440</td></tr> <tr><td>2021-11-09T18:04:53Z</td><td>sw176</td><td>forwarded(200)</td><td>2.16.133.54,_46411,_2d9e28ccb8301d404e6e88a8b202015457725588035ac56864e52098363</td></tr> <tr><td>2021-11-09T18:04:53Z</td><td>sw176</td><td>forwarded(200)</td><td>172.16.133.54,_64382,_e444e1e4a588350917474dfe44e4ac0b50e0de789597513480e0e2be7525d</td></tr> <tr><td>2021-11-09T18:04:53Z</td><td>sw176</td><td>forwarded(200)</td><td>172.16.133.54,_64383,_e845d430a7e7a2e95f9590e01bd1d1ca9838eae29438e9e14879001c028</td></tr> <tr><td>2021-11-09T18:04:53Z</td><td>sw176</td><td>forwarded(200)</td><td>72.16.133.54,_84544,_a2ee2293111468a3c338a8303d4e5d305e5e9e86c0537033a01f8a</td></tr> <tr><td>2021-11-09T18:04:53Z</td><td>sw176</td><td>forwarded(200)</td><td>72.16.133.54,_84544,_3010e603195327d83507272ad0b6b683a3f2a3e5f5870b9696216022cb</td></tr> <tr><td>2021-11-09T18:04:53Z</td><td>sw176</td><td>forwarded(200)</td><td>72.16.133.54,_84544,_34fdff5c270e480aaaf3733cb2b948b850a1340d7f98409709933526</td></tr> <tr><td>2021-11-09T18:04:53Z</td><td>sw176</td><td>forwarded(200)</td><td>72.16.133.54,_84544,_69c5596c2b4edee3a4953229b9d7222a723a1bba157081bc8b0da8a953</td></tr> <tr><td>2021-11-09T18:04:53Z</td><td>sw176</td><td>forwarded(200)</td><td>72.16.133.54,_84544,_794e91539c59aae7c9fbaf375497744dec4dd9e399a014c35c397998114</td></tr> <tr><td>2021-11-09T18:04:53Z</td><td>sw176</td><td>forwarded(200)</td><td>72.16.133.54,_84544,_80dd4972287829691026599825210c1edca7269130c1862a229f631b</td></tr> <tr><td>2021-11-09T18:04:53Z</td><td>sw176</td><td>forwarded(200)</td><td>2.16.133.55,_57642,_dc1c54abed8c007f137927504f222d1c839f1076b08ebeecfd4d4e08249f</td></tr> <tr><td>2021-11-09T18:04:53Z</td><td>sw176</td><td>forwarded(200)</td><td>16.133.54,_84545,_80ee46009d608d477a198e0a25949380a281f4af2d197c7001b5</td></tr> <tr><td>2021-11-09T18:04:53Z</td><td>sw176</td><td>forwarded(200)</td><td>16.133.54,_84546,_8969ee02020314794cfcfaea530103150050e9ed00ff1ea033fb949411a7</td></tr> <tr><td>2021-11-09T18:04:53Z</td><td>sw176</td><td>forwarded(200)</td><td>74.125.226.218,_80_172.16.133.54,_64382,_e2027a98eae232c0b8af4c40a4d1f0d77568f383932899142195c12b4</td></tr> <tr><td>2021-11-09T18:04:53Z</td><td>sw176</td><td>forwarded(200)</td><td>74.125.226.218,_80_172.16.133.54,_64382,_e9745f4d7a77271e9484bc6207b30191291fc07bwee00f7216ba2</td></tr> <tr><td>2021-11-09T18:04:53Z</td><td>sw176</td><td>forwarded(200)</td><td>74.125.226.218,_80_172.16.133.54,_64567,_a5fb23a2640c1106c12152597eacfa3f71178ba3d02b9005477e75897</td></tr> <tr><td>2021-11-09T18:04:53Z</td><td>sw176</td><td>forwarded(200)</td><td>74.125.226.1,_80_172.16.133.54,_64579,_867900eaa33910c5d73473817a3892a5556b5b030aacc5126076038920d</td></tr> <tr><td>2021-11-09T18:04:53Z</td><td>sw176</td><td>forwarded(200)</td><td>74.125.226.1,_80_172.16.133.54,_64580,_7db11ef4d1349962455d91c482d94e499584b4ea912ceew2460853188a7r23</td></tr> </tbody> </table>	Date	NodeName	Status(Code)	File Name	2021-11-09T18:09:03Z	sw176	forwarded(200)	23.60.139.27,_80_10.5.14.102,_49734,_4289353b88d7e7fa967461305f1ebc2f0410008b8b2aadf4ce0770279dd140	2021-11-09T18:09:03Z	sw176	forwarded(200)	23.60.139.27,_80_10.5.14.102,_49735,_4972eadfb8ed253ffbc9158fc029025634499302aef0a281bd3b67113443d	2021-11-09T18:09:03Z	sw176	forwarded(200)	23.60.139.27,_80_10.5.14.102,_49736,_2d20a05fbdb6f67765a481344af5d1f257446d3e9d928984c2036090903	2021-11-09T18:09:03Z	sw176	forwarded(200)	23.60.139.27,_80_10.5.14.102,_49737,_5be85a367a5f52004c2a9df986a3fb9e01cd37f7859975c5820c6035ea909d	2021-11-09T18:09:03Z	sw176	forwarded(200)	23.60.139.27,_80_10.5.14.102,_49738,_aeafad9e950eae755bae03d183834c78d07b058debe3e977aee0506	2021-11-09T18:09:03Z	sw176	forwarded(200)	0.14.102,_49737,_2acab1228e9353c5fd50f75b8a19698fc0b780c08f7993c9cf799af7a96e4e	2021-11-09T18:09:03Z	sw176	forwarded(200)	5.14.102,_49737,_beb2e653c3485d1c2e53b8e2429183e0dd987de71652371700aa89337128	2021-11-09T18:09:03Z	sw176	forwarded(200)	172.16.133.194,_48311,_49886e62c4463c3178573dc31533cb2b67a797c2034646c9567c2698fd5	2021-11-09T18:09:02Z	sw176	forwarded(200)	2.16.133.54,_46410,_a05369e03232547a2a969e34311ea114237cc2e1837eb459e3f67a67bf	2021-11-09T18:09:02Z	sw176	forwarded(200)	5.14.102,_49733,_31299f5e001383cbfb8aaffa0384186795a25aadd50f9e23d217c0404aa0a2	2021-11-09T18:09:02Z	sw176	forwarded(200)	8.151,_51910,_bd3ecf5abbd04092a0fa6a70704289c991273cd3d1f9798e6b0a719b390a87	2021-11-09T18:09:02Z	sw176	forwarded(200)	8.151,_51911,_c5091_40325a80c0c19587b17808d1010aee5fa965959efef54a8d185ec038738	2021-11-09T18:09:02Z	sw176	forwarded(200)	172.16.133.194,_48312,_49886e62c4463c3178573dc31533cb2b67a797c2034646c9567c2698fd5	2021-11-09T18:09:02Z	sw176	forwarded(200)	2.16.133.54,_46411,_2d9e28ccb8301d404e6e88a8b202015457725588035ac56864e52098363	2021-11-09T18:04:53Z	sw176	forwarded(200)	16.151,_51913,_e1882330c102883674474dfe44e4ac0b50e0de789597513480e0e2be7525d	2021-11-09T18:04:53Z	sw176	forwarded(200)	16.133.54,_43406,_8d2c1e440725c278bb8df7b477baa3b35a10731311f1a1b1faa187d5	2021-11-09T18:04:53Z	sw176	forwarded(200)	16.133.54,_43407,_e46370afaf669a72567a53c3290015b69f778e2890232556de5ee5659386	2021-11-09T18:04:53Z	sw176	forwarded(200)	16.133.54,_43408,_1620e5c527a987147641c0c7220a4edc447d707cdca4637072c0393373a8f	2021-11-09T18:04:53Z	sw176	forwarded(200)	16.133.54,_43409,_ce4e4f9a933aae106d23aa96c6d20a466466dd0a7a4677cd7a945ad586440	2021-11-09T18:04:53Z	sw176	forwarded(200)	2.16.133.54,_46411,_2d9e28ccb8301d404e6e88a8b202015457725588035ac56864e52098363	2021-11-09T18:04:53Z	sw176	forwarded(200)	172.16.133.54,_64382,_e444e1e4a588350917474dfe44e4ac0b50e0de789597513480e0e2be7525d	2021-11-09T18:04:53Z	sw176	forwarded(200)	172.16.133.54,_64383,_e845d430a7e7a2e95f9590e01bd1d1ca9838eae29438e9e14879001c028	2021-11-09T18:04:53Z	sw176	forwarded(200)	72.16.133.54,_84544,_a2ee2293111468a3c338a8303d4e5d305e5e9e86c0537033a01f8a	2021-11-09T18:04:53Z	sw176	forwarded(200)	72.16.133.54,_84544,_3010e603195327d83507272ad0b6b683a3f2a3e5f5870b9696216022cb	2021-11-09T18:04:53Z	sw176	forwarded(200)	72.16.133.54,_84544,_34fdff5c270e480aaaf3733cb2b948b850a1340d7f98409709933526	2021-11-09T18:04:53Z	sw176	forwarded(200)	72.16.133.54,_84544,_69c5596c2b4edee3a4953229b9d7222a723a1bba157081bc8b0da8a953	2021-11-09T18:04:53Z	sw176	forwarded(200)	72.16.133.54,_84544,_794e91539c59aae7c9fbaf375497744dec4dd9e399a014c35c397998114	2021-11-09T18:04:53Z	sw176	forwarded(200)	72.16.133.54,_84544,_80dd4972287829691026599825210c1edca7269130c1862a229f631b	2021-11-09T18:04:53Z	sw176	forwarded(200)	2.16.133.55,_57642,_dc1c54abed8c007f137927504f222d1c839f1076b08ebeecfd4d4e08249f	2021-11-09T18:04:53Z	sw176	forwarded(200)	16.133.54,_84545,_80ee46009d608d477a198e0a25949380a281f4af2d197c7001b5	2021-11-09T18:04:53Z	sw176	forwarded(200)	16.133.54,_84546,_8969ee02020314794cfcfaea530103150050e9ed00ff1ea033fb949411a7	2021-11-09T18:04:53Z	sw176	forwarded(200)	74.125.226.218,_80_172.16.133.54,_64382,_e2027a98eae232c0b8af4c40a4d1f0d77568f383932899142195c12b4	2021-11-09T18:04:53Z	sw176	forwarded(200)	74.125.226.218,_80_172.16.133.54,_64382,_e9745f4d7a77271e9484bc6207b30191291fc07bwee00f7216ba2	2021-11-09T18:04:53Z	sw176	forwarded(200)	74.125.226.218,_80_172.16.133.54,_64567,_a5fb23a2640c1106c12152597eacfa3f71178ba3d02b9005477e75897	2021-11-09T18:04:53Z	sw176	forwarded(200)	74.125.226.1,_80_172.16.133.54,_64579,_867900eaa33910c5d73473817a3892a5556b5b030aacc5126076038920d	2021-11-09T18:04:53Z	sw176	forwarded(200)	74.125.226.1,_80_172.16.133.54,_64580,_7db11ef4d1349962455d91c482d94e499584b4ea912ceew2460853188a7r23
Date	NodeName	Status(Code)	File Name																																																																																																																																																		
2021-11-09T18:09:03Z	sw176	forwarded(200)	23.60.139.27,_80_10.5.14.102,_49734,_4289353b88d7e7fa967461305f1ebc2f0410008b8b2aadf4ce0770279dd140																																																																																																																																																		
2021-11-09T18:09:03Z	sw176	forwarded(200)	23.60.139.27,_80_10.5.14.102,_49735,_4972eadfb8ed253ffbc9158fc029025634499302aef0a281bd3b67113443d																																																																																																																																																		
2021-11-09T18:09:03Z	sw176	forwarded(200)	23.60.139.27,_80_10.5.14.102,_49736,_2d20a05fbdb6f67765a481344af5d1f257446d3e9d928984c2036090903																																																																																																																																																		
2021-11-09T18:09:03Z	sw176	forwarded(200)	23.60.139.27,_80_10.5.14.102,_49737,_5be85a367a5f52004c2a9df986a3fb9e01cd37f7859975c5820c6035ea909d																																																																																																																																																		
2021-11-09T18:09:03Z	sw176	forwarded(200)	23.60.139.27,_80_10.5.14.102,_49738,_aeafad9e950eae755bae03d183834c78d07b058debe3e977aee0506																																																																																																																																																		
2021-11-09T18:09:03Z	sw176	forwarded(200)	0.14.102,_49737,_2acab1228e9353c5fd50f75b8a19698fc0b780c08f7993c9cf799af7a96e4e																																																																																																																																																		
2021-11-09T18:09:03Z	sw176	forwarded(200)	5.14.102,_49737,_beb2e653c3485d1c2e53b8e2429183e0dd987de71652371700aa89337128																																																																																																																																																		
2021-11-09T18:09:03Z	sw176	forwarded(200)	172.16.133.194,_48311,_49886e62c4463c3178573dc31533cb2b67a797c2034646c9567c2698fd5																																																																																																																																																		
2021-11-09T18:09:02Z	sw176	forwarded(200)	2.16.133.54,_46410,_a05369e03232547a2a969e34311ea114237cc2e1837eb459e3f67a67bf																																																																																																																																																		
2021-11-09T18:09:02Z	sw176	forwarded(200)	5.14.102,_49733,_31299f5e001383cbfb8aaffa0384186795a25aadd50f9e23d217c0404aa0a2																																																																																																																																																		
2021-11-09T18:09:02Z	sw176	forwarded(200)	8.151,_51910,_bd3ecf5abbd04092a0fa6a70704289c991273cd3d1f9798e6b0a719b390a87																																																																																																																																																		
2021-11-09T18:09:02Z	sw176	forwarded(200)	8.151,_51911,_c5091_40325a80c0c19587b17808d1010aee5fa965959efef54a8d185ec038738																																																																																																																																																		
2021-11-09T18:09:02Z	sw176	forwarded(200)	172.16.133.194,_48312,_49886e62c4463c3178573dc31533cb2b67a797c2034646c9567c2698fd5																																																																																																																																																		
2021-11-09T18:09:02Z	sw176	forwarded(200)	2.16.133.54,_46411,_2d9e28ccb8301d404e6e88a8b202015457725588035ac56864e52098363																																																																																																																																																		
2021-11-09T18:04:53Z	sw176	forwarded(200)	16.151,_51913,_e1882330c102883674474dfe44e4ac0b50e0de789597513480e0e2be7525d																																																																																																																																																		
2021-11-09T18:04:53Z	sw176	forwarded(200)	16.133.54,_43406,_8d2c1e440725c278bb8df7b477baa3b35a10731311f1a1b1faa187d5																																																																																																																																																		
2021-11-09T18:04:53Z	sw176	forwarded(200)	16.133.54,_43407,_e46370afaf669a72567a53c3290015b69f778e2890232556de5ee5659386																																																																																																																																																		
2021-11-09T18:04:53Z	sw176	forwarded(200)	16.133.54,_43408,_1620e5c527a987147641c0c7220a4edc447d707cdca4637072c0393373a8f																																																																																																																																																		
2021-11-09T18:04:53Z	sw176	forwarded(200)	16.133.54,_43409,_ce4e4f9a933aae106d23aa96c6d20a466466dd0a7a4677cd7a945ad586440																																																																																																																																																		
2021-11-09T18:04:53Z	sw176	forwarded(200)	2.16.133.54,_46411,_2d9e28ccb8301d404e6e88a8b202015457725588035ac56864e52098363																																																																																																																																																		
2021-11-09T18:04:53Z	sw176	forwarded(200)	172.16.133.54,_64382,_e444e1e4a588350917474dfe44e4ac0b50e0de789597513480e0e2be7525d																																																																																																																																																		
2021-11-09T18:04:53Z	sw176	forwarded(200)	172.16.133.54,_64383,_e845d430a7e7a2e95f9590e01bd1d1ca9838eae29438e9e14879001c028																																																																																																																																																		
2021-11-09T18:04:53Z	sw176	forwarded(200)	72.16.133.54,_84544,_a2ee2293111468a3c338a8303d4e5d305e5e9e86c0537033a01f8a																																																																																																																																																		
2021-11-09T18:04:53Z	sw176	forwarded(200)	72.16.133.54,_84544,_3010e603195327d83507272ad0b6b683a3f2a3e5f5870b9696216022cb																																																																																																																																																		
2021-11-09T18:04:53Z	sw176	forwarded(200)	72.16.133.54,_84544,_34fdff5c270e480aaaf3733cb2b948b850a1340d7f98409709933526																																																																																																																																																		
2021-11-09T18:04:53Z	sw176	forwarded(200)	72.16.133.54,_84544,_69c5596c2b4edee3a4953229b9d7222a723a1bba157081bc8b0da8a953																																																																																																																																																		
2021-11-09T18:04:53Z	sw176	forwarded(200)	72.16.133.54,_84544,_794e91539c59aae7c9fbaf375497744dec4dd9e399a014c35c397998114																																																																																																																																																		
2021-11-09T18:04:53Z	sw176	forwarded(200)	72.16.133.54,_84544,_80dd4972287829691026599825210c1edca7269130c1862a229f631b																																																																																																																																																		
2021-11-09T18:04:53Z	sw176	forwarded(200)	2.16.133.55,_57642,_dc1c54abed8c007f137927504f222d1c839f1076b08ebeecfd4d4e08249f																																																																																																																																																		
2021-11-09T18:04:53Z	sw176	forwarded(200)	16.133.54,_84545,_80ee46009d608d477a198e0a25949380a281f4af2d197c7001b5																																																																																																																																																		
2021-11-09T18:04:53Z	sw176	forwarded(200)	16.133.54,_84546,_8969ee02020314794cfcfaea530103150050e9ed00ff1ea033fb949411a7																																																																																																																																																		
2021-11-09T18:04:53Z	sw176	forwarded(200)	74.125.226.218,_80_172.16.133.54,_64382,_e2027a98eae232c0b8af4c40a4d1f0d77568f383932899142195c12b4																																																																																																																																																		
2021-11-09T18:04:53Z	sw176	forwarded(200)	74.125.226.218,_80_172.16.133.54,_64382,_e9745f4d7a77271e9484bc6207b30191291fc07bwee00f7216ba2																																																																																																																																																		
2021-11-09T18:04:53Z	sw176	forwarded(200)	74.125.226.218,_80_172.16.133.54,_64567,_a5fb23a2640c1106c12152597eacfa3f71178ba3d02b9005477e75897																																																																																																																																																		
2021-11-09T18:04:53Z	sw176	forwarded(200)	74.125.226.1,_80_172.16.133.54,_64579,_867900eaa33910c5d73473817a3892a5556b5b030aacc5126076038920d																																																																																																																																																		
2021-11-09T18:04:53Z	sw176	forwarded(200)	74.125.226.1,_80_172.16.133.54,_64580,_7db11ef4d1349962455d91c482d94e499584b4ea912ceew2460853188a7r23																																																																																																																																																		

- VLAN list is comma separated. Accepts individual vlans, or ranges.
Example: 1,17-22,30
- IP Address list is comma separated. Accepts individual addresses, and CIDR
Example: 10.1.2.3,10.1.1.0/24,11.2.4.100

File Carving on Demand allows users to request files from a specific time period to be sent to an external server.

Federation Manager

File Carving			
			<input type="text" value="Search..."/> File Configuration... FC On Demand... FC Help...
Date	NodeName	Status(Code)	File Name
2021-11-09T18:09:03Z	sw176	forwarded(200)	23.60.139.27.80_10.5.14.102.49734_426f3953b8d7ebfa9a86748163051ebec2f041008bb8b2xaaf4ce0770279dd140
2021-11-09T18:09:03Z	sw176	forwarded(200)	23.60.139.27.80_10.5.14.102.49735_4972ebed8ed25fbfb81596e2092534e4893902a9a28d15b5d3e7119443d
2021-11-09T18:09:03Z	sw176	forwarded(200)	23.60.139.27.80_10.5.14.102.49736_2d20b05dbbd65770a56a461344415bf1267a5463e5d0c295840c26609093
2021-11-09T18:09:03Z	sw176	forwarded(200)	23.60.139.27.80_10.5.14.102.49736_4972ebed8ed25fbfb81596e2092534e4893902a9a28d15b5d3e7119443d
2021-11-09T18:09:03Z	sw176	forwarded(200)	23.60.139.27.80_10.5.14.102.49736_aefad59e950ea755bae9a316383a4c7f65e970d5556e83e6e97a70ee5050
2021-11-09T18:09:03Z	sw176	forwarded(200)	23.60.139.27.80_10.5.14.102.49737_2cab1228e8935d5dfdd1756ba196986cd8786c2097893ca97993a7d7a0664e
2021-11-09T18:09:03Z	sw176	forwarded(200)	23.60.139.27.80_10.5.14.102.49737_bebe853a348512fe3c18921893e0d9ff7de716527717008993738
2021-11-09T18:09:02Z	sw176	forwarded(200)	199.102.234.31.80_172.16.133.41.s3091_44035ab0c19580717800101aaee5fa09595e65f548d6195e038738
2021-11-09T18:09:02Z	sw176	forwarded(200)	21.16.133.54.64610.e0536a0079238474da93411aa112370a281837a486e7167fb7c26916d0e55e636b
2021-11-09T18:09:02Z	sw176	forwarded(200)	5.14.102.49733_310955d8013830cb08a8a8341867952a5aaad559e9e23e218c7904080e02
2021-11-09T18:09:01Z	sw176	forwarded(200)	8.151.51911.b03e65ab04092406a9a7042b9c9173d19978a6b29173d93b0a7
2021-11-09T18:09:01Z	sw176	forwarded(200)	8.151.51912.c936985273e15e4cb5d5a0e592f16ea8fa0f22d7559213e033d305bb7b8a
2021-11-09T18:09:01Z	sw176	forwarded(200)	8.151.51913.e186230310c2853674474df844e0c09de799-59715480e24b7524df
2021-11-09T18:09:53Z	sw176	forwarded(200)	16.133.54.64390.8d216e4457252785697fb2d77tda3b3e365c410731311a1be16a4187d5
2021-11-09T18:09:53Z	sw176	forwarded(200)	16.133.54.64394.a46370a4d69e63d3016060195327d8c350723aade06b68a83563a2e35870e6669216023d6
AAA Management	sw176	forwarded(200)	16.133.54.64464.1820e52c7a987147e41a0e272304edc7d76a4c670722d3e93933a8f
Authentication	sw176	forwarded(200)	16.133.54.64468.ce44e09383d8e002d2ea9e6a03204468466ddc97a467793414d56640
Authorization	sw176	forwarded(200)	2.16.133.54.64411.2d9e286cb83019404e6a88ab2021546772568033ac55864a5206803
Audit Log Preferences...	sw176	forwarded(200)	172.16.133.54.64382.e044ae4ca5583505747575ded370feee07102bf2960b708529918cSeacc
Audit Log Receiver Settings...	sw176	forwarded(200)	172.16.133.54.64450.e4d4a30272d7a9d939d1c1bd1f21ccaa8938a2943dc9e4887c001c2028
IDS Ruleset Management	sw176	forwarded(200)	2.16.133.54.64544.2a2ee22b7711146a93308803034c65d568e6e60c86137703e133401401b
Activated Rulesets	sw176	forwarded(200)	2.16.133.54.64544.344d05c270a480a8a0d37d3d6b9c9d88b080134a0f0984979943526
Deactivated Rulesets	sw176	forwarded(200)	72.16.133.54.64544.6955c595fb4e6e24953229e9ff722a73a1bb81570818cfc80da8e93
SigDetect Ruleset	sw176	forwarded(200)	2.16.133.54.64544.70e6e1539c5caaa79fbaf7549574474edc4d939e99901a013c35c3970998114
Augmentation	sw176	forwarded(200)	72.16.133.54.64544.8b0dd97c2287929910258998bc01c1edca872e99130c1682a222f9e51b
Suspicious Signatures	sw176	forwarded(200)	2.16.133.55.57942.dcf1d545ab46e8c0c070137927504e4222c83951076b0cbeefc9a408249f
Suspicious IPs	sw176	forwarded(200)	75.98.93.51.3801776.16.133.54.64360.80e46008620890477a1f980a252940388b2011fe54d21987d7001b5
Suspicious Domains	sw176	forwarded(200)	75.98.93.51.80_172.16.133.54.64360.89e69203147942fc2d3d1031505e6f68bd7fed033fb6e41fa7
Suspicious DDSums	sw176	forwarded(200)	74.125.226.210.80_172.16.133.54.64362.92079a862a32c08a40a4d8f1ad77569f3103928296
Defended Assets	sw176	forwarded(200)	74.125.226.210.80_74.125.226.210.80_74.125.226.210.80_74.125.226.210.80_74.125.226.210.80
Defended Services	sw176	forwarded(200)	74.125.226.210.80_74.125.226.210.80_74.125.226.210.80_74.125.226.210.80_74.125.226.210.80
2021-11-09T18:09:51Z	sw176	forwarded(200)	72.16.133.54.64544.2a2ee22b7711146a93308803034c65d568e6e60c86137703e133401401b
2021-11-09T18:09:51Z	sw176	forwarded(200)	72.16.133.54.64544.344d05c270a480a8a0d37d3d6b9c9d88b080134a0f0984979943526
2021-11-09T18:09:51Z	sw176	forwarded(200)	72.16.133.54.64544.6955c595fb4e6e24953229e9ff722a73a1bb81570818cfc80da8e93
2021-11-09T18:09:51Z	sw176	forwarded(200)	2.16.133.54.64544.70e6e1539c5caaa79fbaf7549574474edc4d939e99901a013c35c3970998114
2021-11-09T18:09:51Z	sw176	forwarded(200)	72.16.133.54.64544.8b0dd97c2287929910258998bc01c1edca872e99130c1682a222f9e51b
2021-11-09T18:09:51Z	sw176	forwarded(200)	2.16.133.55.57942.dcf1d545ab46e8c0c070137927504e4222c83951076b0cbeefc9a408249f
File Carving On Demand			
Request Name			x
continuum_20211109183110.xlsb			
Begin Time			
2021-11-09 12:56:10			
End Time			
2021-11-09 13:11:10			
VLAN			
Vlan			
File Extension			
File Extension			
IP Address			
IP Address			
Domain Name			
Domains			
Request File Carving			
Close			

File Carving is available as a dashboard in Investigator View:

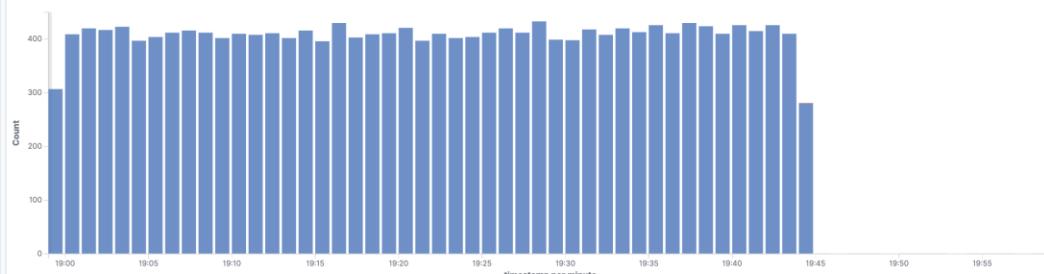
SentryWire

Dashboards

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	
FileCarving		
Flow dashboard	v21.5.29	
HTTP Dashboard	v21.6.8	
Hardware Monitoring and Health Status (VH)	MXQ1350HVH	
RSA: Cambridge	Rows	
RSA: Cambridge Alert	Rows	
SMB dashboard	v21.6.9	
TLS dashboard	v21.6.9	
Total Overview	Overview of the whole system	
TrendGraph replication for TreDept	11/1	
vega replication for TreDept		

Rows per page: 20 < 1 >

File Carving Status Code



File Carving Log

Date	Time	File	Content Hash	Status
Nov 14, 2021	@ 19:44:38.000	sw176	10.1.160.80.10.1.8.151_2628_328e94df4351ae79e327c4e5e1c2ca54b7c6ddbd13bea70ba18f52ec8e37c7ad	503
Nov 14, 2021	@ 19:44:37.000	sw176	10.1.160.80.10.1.8.151_2580_0e82929160cd2e2b9e9fe89209b2379890ea3a6702773239c03c556	200
Nov 14, 2021	@ 19:44:37.000	sw176	10.1.160.80.10.1.8.151_2581_dc0ba824f514caf778f7b8162a67d1069e94c23ef3503d974c47af82bf3db2	200
Nov 14, 2021	@ 19:44:37.000	sw176	10.1.160.80.10.1.8.151_2588_oc7b569a0ad39513a7a238117912f85945af36d8aacccbfbe81907bf13dbd754	200
Nov 14, 2021	@ 19:44:37.000	sw176	10.1.160.80.10.1.8.151_2588_ae002864c9eeeb7488fcfa8083806311f3d17fb0f33277638a22d4cc19fc5fd	200
Nov 14, 2021	@ 19:44:37.000	sw176	10.1.160.80.10.1.8.151_2593_35d95b5322134fc1f645a3a32d919f698d184b7b3705424ecac7fa7340b3fb6	200
Nov 14, 2021	@ 19:44:37.000	sw176	10.1.160.80.10.1.8.151_2593_b4b8fd9cd36b6cc77a02710919b517feac83415d3d778620595cb1cfaf5e9a	200
Nov 14, 2021	@ 19:44:37.000	sw176	10.1.160.80.10.1.8.151_2593_c8d042a80c0f6123dfbf7a0c0ce79992c25aa48e242551f9a9e8544c4f9516	200
Nov 14, 2021	@ 19:44:37.000	sw176	10.1.160.80.10.1.8.151_2595_8a6999b4ce2c6330c19ef94bfe35adb99b6b9a640034dcdbfa79b5b2391ff	200
Nov 14, 2021	@ 19:44:37.000	sw176	10.1.160.80.10.1.8.151_2597_c2a188542b6889434152936946c2e1bb6193e71ebd1137c7595d9d568e5a8	200
Nov 14, 2021	@ 19:44:36.000	sw176	10.1.160.80.10.1.8.151_2546_ba44b2bf68b180e9c963f3fed5c14149c2f2ce6d9bf3305ab157d324496b227c	200
Nov 14, 2021	@ 19:44:36.000	sw176	10.1.160.80.10.1.8.151_2547_26e9036331a8b5b38eb341fc9685b298afe2b17aa83c17350d0703c7c49f78	200
Nov 14, 2021	@ 19:44:36.000	sw176	10.1.160.80.10.1.8.151_2555_hdca8992879aa00992a5f1f39154-aed3a3a5c-254f517a65447h385546d-c-e-a5	200

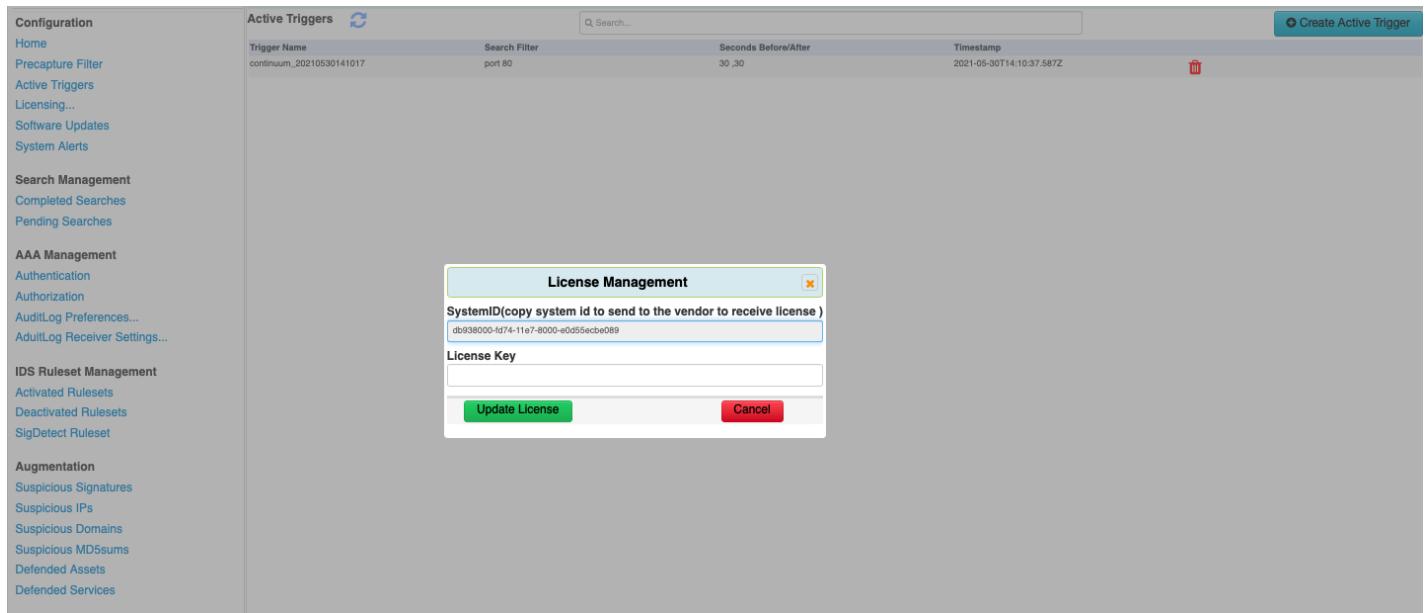
3.1.6 Licensing

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

Note:

- System Id is required to obtain a valid license key.
- Only Admin or authorized users, can apply the license key.

2. Once a license key has been forwarded, copy and paste the provided string into the License Key text box in the web user interface.
3. Click “Update License” button to apply the new license.

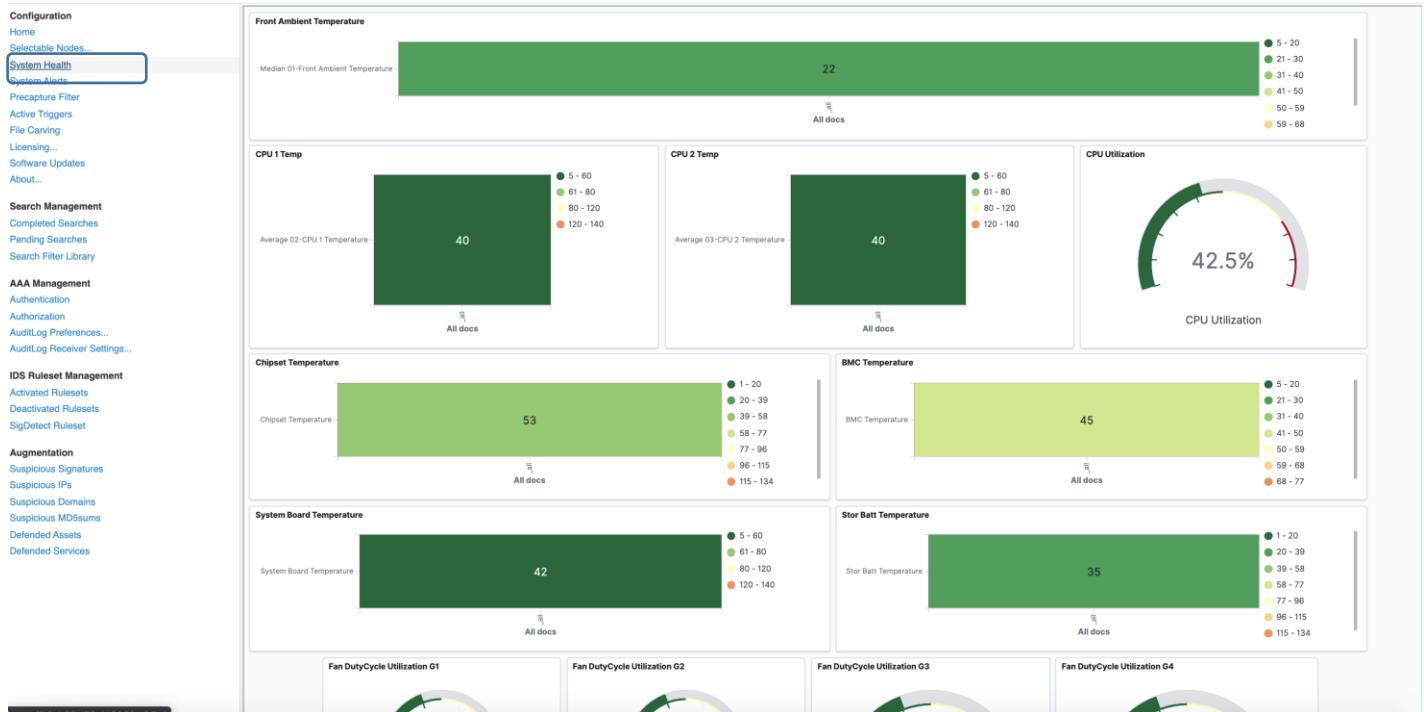


The screenshot shows the SentryWire configuration interface. On the left, there's a sidebar with various management sections like Configuration, Home, Precapture Filter, Active Triggers, Licensing..., Software Updates, System Alerts, Search Management, AAA Management, IDS Ruleset Management, and Augmentation. The 'Licensing...' section is highlighted. In the main area, there's a table titled 'Active Triggers' with one entry: 'continuum_20210530141017' with a timestamp of '2021-05-30T14:10:37.587Z'. Below this is a 'License Management' dialog box. It contains a text input field labeled 'SystemID(copy system id to send to the vendor to receive license)' with the value 'db938000-1d74-11e7-8000-e0d55ecbe089'. There's also a 'License Key' input field, a 'Update License' button, and a 'Cancel' button.

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.

Software Updates			
Date	NodeName	Message	Severity
2021-11-05T19:03:01	sw146	Received softwareupdate_20211105185455_jpmctest.zip	2:Warning
2021-11-05T19:03:01	sw146	Updated using softwareupdate_20211105185455_jpmctest.zip	2:Warning
2021-11-05T19:02:59	sw176	Sending jpmctest.zip to sw146	2:Warning
2021-11-05T18:59:22	sw176	Received softwareupdate_20211105185455_jpmctest.zip	2:Warning
2021-11-05T18:59:22	sw176	Updated using softwareupdate_20211105185455_jpmctest.zip	2:Warning
2021-11-05T18:59:21	sw146	Received softwareupdate_20211105185455_jpmctest.zip	2:Warning
2021-11-05T18:59:21	sw146	Updated using softwareupdate_20211105185455_jpmctest.zip	2:Warning
2021-11-05T18:59:19	sw176	Sending jpmctest.zip to sw146	2:Warning
2021-11-05T18:59:19	sw176	Received softwareupdate_20211105184607_sw2_adadd_124.zip	2:Warning
2021-11-05T18:46:37	sw176	Updated using softwareupdate_20211105184607_sw2_adadd_124.zip	2:Warning
2021-11-05T18:46:37	sw146	Received softwareupdate_20211105184607_sw2_adadd_124.zip	2:Warning
2021-11-05T18:46:36	sw146	Updated using softwareupdate_20211105184607_sw2_adadd_124.zip	2:Warning
2021-11-05T18:46:36	sw146	Sending sw2_adadd_124.zip to sw146	2:Warning
2021-11-05T18:46:35	sw176	Sending sw2_adadd_124.zip to sw176	2:Warning
2021-11-05T18:46:35	sw176	Received softwareupdate_20211105181308_pj2_abc_123.zip	2:Warning
2021-11-05T18:19:27	sw176	Updated using softwareupdate_20211105181308_pj2_abc_123.zip	2:Warning
2021-11-05T18:19:27	sw146	Received softwareupdate_20211105181308_pj2_abc_123.zip	2:Warning
2021-11-05T18:19:26	sw146	Updated using softwareupdate_20211105181308_pj2_abc_123.zip	2:Warning
2021-11-05T18:19:24	sw176	Sending pj2_abc_123.zip to sw146	2:Warning
2021-11-05T18:19:24	sw176	Sending pj2_abc_123.zip to sw176	2:Warning
2021-11-05T18:11:42	sw176	Sending pj2_abc_123.zip to sw176	2:Warning
2021-11-05T18:11:42	sw176	Received softwareupdate_20211105173717_pj2_abc_123.zip	2:Warning
2021-11-05T18:11:42	sw176	Updated using softwareupdate_20211105173717_pj2_abc_123.zip	2:Warning
2021-11-05T18:09:22	sw176	Received softwareupdate_20211105173717_pj2_abc_123.zip	2:Warning
2021-11-05T18:09:22	sw176	Updated using softwareupdate_20211105173717_pj2_abc_123.zip	2:Warning
2021-11-05T18:09:20	sw176	Sending pj2_abc_123.zip to sw146	2:Warning

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
user: continuum role: Supervisor Selected Nodes: ALL

System Alerts

Category	Date	NodeName	Message	Severity	Category
TrafficAlert(4008)	2021-11-18T01:40:36	nc178	searchname: continuum_20211118013503_kxlvv_glic_eemue, searchfilter:tcp or udp, beginTime:1637198403, endTime:1637199323, result:Pkts=0,Seconds=0	2:Warning	Search
Admin(1)	2021-11-18T01:40:30	nc178	searchname: continuum_20211118013503_kxlvv_glic_eemue, searchfilter:tcp or udp, beginTime:1637198403, endTime:1637199323	2:Warning	Search
Group(2)	2021-11-18T01:40:26	nc178	searchname: continuum_20211118013523_d4mcf_bmsww, searchfilter:tcp or udp, beginTime:1637198423, endTime:1637199343, result:Pkts=0,Seconds=0	2:Warning	Search
Node(7)	2021-11-18T01:40:25	nc178	searchname: continuum_20211118013503_kxlvv_glic_lukng, searchfilter:tcp or udp, beginTime:1637198403, endTime:1637199323, result:Pkts=0,Seconds=0	2:Warning	Search
Precapture(1)	2021-11-18T01:40:21	nc178	searchname: continuum_20211118013523_d4mcf_bmsww, searchfilter:tcp or udp, beginTime:1637198423, endTime:1637199343	2:Warning	Search
Activetrigger(2)	2021-11-18T01:40:20	nc178	searchname: continuum_20211118013503_kxlvv_glic_lukng, searchfilter:tcp or udp, beginTime:1637198403, endTime:1637199323	2:Warning	Search
SoftwareUpdate(59)	2021-11-18T01:39:35	sw146	searchname: continuum_20211118013503_kxlvv_glic_eemue, searchfilter:tcp or udp, beginTime:1637198403, endTime:1637199323, result:Pkts=0,Seconds=0	2:Warning	Search
Search(249)	2021-11-18T01:39:30	sw146	searchname: continuum_20211118013503_kxlvv_glic_eemue, searchfilter:tcp or udp, beginTime:1637198403, endTime:1637199323	2:Warning	Search
Authentication(217)	2021-11-18T01:39:30	sw146	searchname: continuum_20211118013523_d4mcf_bmsww, searchfilter:tcp or udp, beginTime:1637198423, endTime:1637199343, result:Pkts=0,Seconds=0	2:Warning	Search
Authorization(0)	2021-11-18T01:39:29	sw146	searchname: continuum_20211118013503_kxlvv_glic_lukng, searchfilter:tcp or udp, beginTime:1637198403, endTime:1637199323, result:Pkts=0,Seconds=0	2:Warning	Search
IDSRuleset(0)	2021-11-18T01:39:25	sw146	searchname: continuum_20211118013523_d4mcf_bmsww, searchfilter:tcp or udp, beginTime:1637198423, endTime:1637199343	2:Warning	Search
Augmentation(6)	2021-11-18T01:39:24	sw146	searchname: continuum_20211118013503_kxlvv_glic_lukng, searchfilter:tcp or udp, beginTime:1637198403, endTime:1637199323	2:Warning	Search
2021-11-18T01:35:55	nc179	searchname: continuum_20211118013503_kxlvv_glic_searchfilter:tcp or udp, beginTime:1637198403, endTime:1637199323, result:Pkts=0,Seconds=0	2:Warning	Search	
2021-11-18T01:35:49	nc179	searchname: continuum_20211118013503_kxlvv_glic_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:Pkts=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_kxlvv_glic_searchfilter:tcp or udp, beginTime:1637198403, endTime:1637199323, result:Pkts=0,Seconds=0	2:Warning	Search	
2021-11-18T01:35:20	nc179	searchname: continuum_20211118013503_kxlvv_glic_searchfilter:tcp or udp, beginTime:1637198403, endTime:1637199323	2:Warning	Search	
2021-11-18T01:34:59	sw146	searchname: continuum_20211118013503_kxlvv_glic_searchfilter:tcp or udp, beginTime:1637198403, endTime:1637199323, result:Pkts=0,Seconds=0	2:Warning	Search	
2021-11-18T01:34:54	sw146	searchname: continuum_20211118013503_kxlvv_glic_searchfilter:tcp or udp, beginTime:1637198403, endTime:1637199323	2:Warning	Search	
2021-11-18T01:34:44	sw146	searchname: continuum_20211118013523_d4mcf, searchfilter:tcp or udp, beginTime:1637198423, endTime:1637199343, result:Pkts=0,Seconds=0	2:Warning	Search	
2021-11-18T01:34:40	nc179	searchname: continuum_20211118013423_S2In, searchfilter:tcp or udp, beginTime:1637198583, endTime:1637199283, result:Pkts=0,Seconds=0	2:Warning	Search	
2021-11-18T01:34:39	sw146	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			Delete All Selected 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,tcpcap	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,tcpcap	1000		
Software Updates	nc179	continuum_1631315942_1_rest1	2021-09-10 13:30	2021-09-10 14:00	PcapData,tcpcap	10000		
System Alerts	sw146	continuum_1631315942_1_rest1	2021-09-10 13:30	2021-09-10 14:00	PcapData,tcpcap	10000	Pkts=11501 Seconds=4 TotalSize=1MB	
Search Management	sw146	continuum_20210910010817_cbt2	2021-09-09 00:53:17	2021-09-10 01:08:17	port 80	1000000	Pkts=1163365 Seconds=88 TotalSize=773MB	
Completed Searches	nc179	continuum_20210910010817_cbt2	2021-09-09 00:53:17	2021-09-10 01:08:17	port 80	1000000		
Pending Searches	nc179	continuum_1631019788_3_RESTPooja1	2021-09-4 12:00:00	2021-09-4 12:00:20	PcapData,tcpcap	1000	Pkts=25 Seconds=6 TotalSize=3KB	
Search Filter Library	nc179	continuum_1630731446_2_RESTPooja_imhytm	2021-09-04 12:00:00	2021-09-04 12:00:20	tcp	1000	Pkts=25 Seconds=6 TotalSize=3KB	
AAA Management	nc179	continuum_1630731446_2_RESTPooja_imhytm	2021-09-04 12:00:00	2021-09-04 12:00:20	PcapData,tcpcap	1000		
Authentication	nc179	continuum_20210902195732_5fd9_g2awo_zb2r_d4r35_0kt7q_ej	2021-09-02 23:42:32	2021-09-02 23:57:32	udp [0:2] = 0x0223 63k_9ekaf	1000		
Authorization	nc179	continuum_20210902195732_5fd9_g2awo_zb2r_d4r35_0kt7q_ej	2021-09-02 19:42:32	2021-09-02 19:57:32	ip6 [40:2] = 0x0223 63k_9ekaf	1000	Pkts=35 Seconds=6 TotalSize=5KB	
AuditLog Preferences...	nc179	continuum_20210902195732_5fd9_g2awo_zb2r_d4r35_0kt7q_ej	2021-09-02 19:42:32	2021-09-02 19:57:32	ip6 [39:2] = 0x0223	1000	NoPcapData	
AuditLog Receiver Settings...	nc179	continuum_20210902195732_5fd9_g2awo_zb2r_d4r35_0kt7q_ej	2021-09-02 19:42:32	2021-09-02 19:57:32	ip6 [39:2] = 0x0223	1000	NoPcapData	
IDS Ruleset Management	nc179	continuum_20210902195732_5fd9_g2awo_zb2r_d4r35_0kt7q_ej	2021-09-02 19:42:32	2021-09-02 19:57:32	ip6 [40:2] = 0x0223 63k_9ekaf	1000	NoPcapData	
Activated Rulesets	nc179	continuum_20210902195732_5fd9_g2awo_zb2r_d4r35_0kt7q_ej	2021-09-02 19:42:32	2021-09-02 19:57:32	ip6 [40:2] = 0x0223 63k_9ekaf	1000	NoPcapData	
Deactivated Rulesets	nc179	continuum_20210902195732_5fd9_g2awo_zb2r_d4r35_0kt7q_ej	2021-09-02 19:42:32	2021-09-02 19:57:32	ip6 [40:2] = 0x0223 63k_9ekaf	1000	NoPcapData	
SigDetect Ruleset	nc179	continuum_20210902195732_5fd9_g2awo_zb2r_d4r35_0kt7q_ej	2021-09-02 19:42:32	2021-09-02 19:57:32	ip6 [40:2] = 0x0223 63k_9ekaf	100000	NoPcapData	
Augmentation	nc179	continuum_20210902195448_vba2g	2021-09-02 23:39:48	2021-09-02 23:54:48	tcp[20:4] = 0x48545450 and (not port 80)	10000		
Suspicious Signatures	nc179	continuum_20210902195213_httl	2021-09-02 19:37:13	2021-09-02 19:52:13	tcp[247:4] = 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=555KB	
Suspicious Domains	nc179	continuum_20210902112233_n27g_yikd_dgrw_w_1plsc_x3yia_fff_9_9r7oq_g5hml_100y_049ek_4cfn8_bkwzq_kgw8_S9zb5	2021-09-02 11:21:55	2021-09-02 13:00:50	ip6[0:2] & 0x0222 = 1	1000	NoPcapData	
Suspicious MD5sums	nc179	continuum_20210902112233_n27g_yikd_dgrw_w_1plsc_x3yia_fff_9_9r7oq_g5hml_100y_049ek_4cfn8_bkwzq_kgw8_S9zb5	2021-09-02 11:21:55	2021-09-02 13:00:50	ip6 and ip6[0:2] == 0x0222	1000	NoPcapData	
Defended Assets	nc179	continuum_20210902112233_n27g_yikd_dgrw_w_1plsc_x3yia_fff_9_9r7oq_g5hml_100y_049ek_4cfn8_bkwzq_kgw8_S9zb5	2021-09-02 11:21:55	2021-09-02 13:00:50	ip6[0:2] == 0x0222	1000	NoPcapData	
Defended Services	nc179	continuum_20210902112233_n27g_yikd_dgrw_w_1plsc_x3yia_fff_9_9r7oq_g5hml_100y_049ek_4cfn8_bkwzq_kgw8_S9zb5	2021-09-02 11:21:55	2021-09-02 13:00:50	ip6[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			cancel	Delete All Selected Searches		
NodeName	SearchName	Begin Time	End Time	SearchFilter	MaxPkts	SearchResult
nc186	continuum_20210608115824_oh2oi	2021-06-08 11:43:24	2021-06-08 11:58:24	tcp or udp		Cancelled

Show searches that were done on a particular day:

Completed Searches		2021-06-07						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 21:03:32	port 80	100000	Pkts=176376 Seconds=12 TotalSize=120MB	
<input type="checkbox"/> 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	
<input 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	

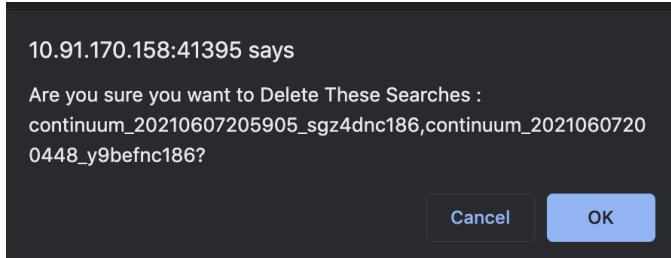
Show searches of a particular user:

Completed Searches		poluser1						Delete All Selected Searches
NodeName	SearchName		Begin Time	End Time	SearchFilter	MaxPkts	SearchResult	
<input type="checkbox"/> nc186	poluser1_20210608114552_p512e		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		2021-06-07						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 21:03:32	port 80	100000	Pkts=176376 Seconds=12 TotalSize=120MB				
<input checked="" type="checkbox"/> 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				
<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

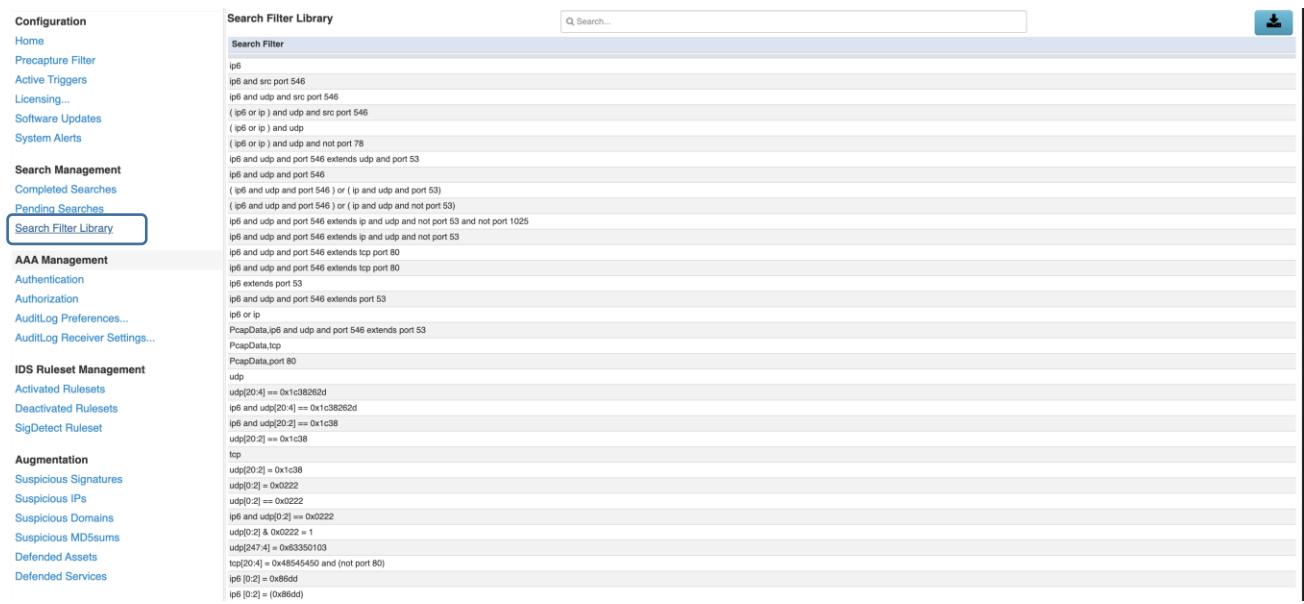
user: continuum role: Admin authenticationmode: local version: 408.14r2.1

Pending Searches  Search...

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.



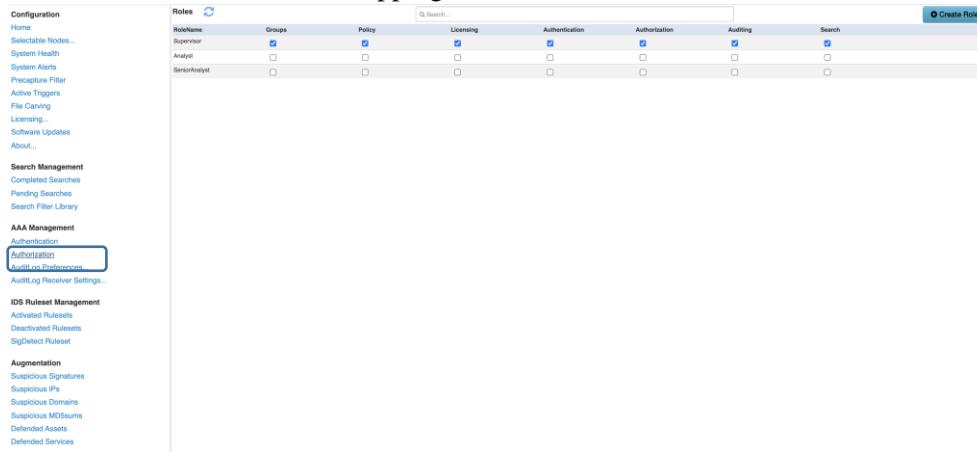
Search Filter
ip6
ip6 and src port 546
ip6 and udp and src port 546
(ip6 or ip) and udp and src port 546
(ip6 or ip) and udp
(ip6 or ip) and udp and not port 78
ip6 and udp and port 546 extends udp and port 53
ip6 and udp and port 546
(ip6 and udp and port 546) or (ip and udp and port 53)
(ip6 and udp and port 546) or (ip and udp and not port 53)
ip6 and udp and port 546 extends ip and udp and not port 53 and not port 1025
ip6 and udp and port 546 extends ip and udp and not port 53
ip6 and udp and port 546 extends tcp port 80
ip6 and udp and port 546 extends tcp port 80
ip6 extends port 53
ip6 and udp and port 546 extends port 53
ip6 or ip
PcapData.ip6 and udp and port 546 extends port 53
PcapData.tcp
PcapData.port 80
udp
udp[20:4] == 0x1c38262d
ip6 and udp[20:4] == 0x1c38262d
ip6 and udp[20:2] == 0xc1c38
udp[20:2] == 0xc1c38
tcp
udp[20:2] = 0xc1c38
udp[0:2] = 0x2222
udp[0:2] == 0x2222
ip6 and udp[0:2] == 0x2222
ip6 and udp[0:2] == 0x2222
udp[0:2] & 0x2222 = 1
udp[247:4] = 0x63350103
tcp[20:4] = 0x48545450 and (not port 80)
ip6 [0:2] = 0xb8dd
ip6 [0:2] = (0xb8dd)

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.

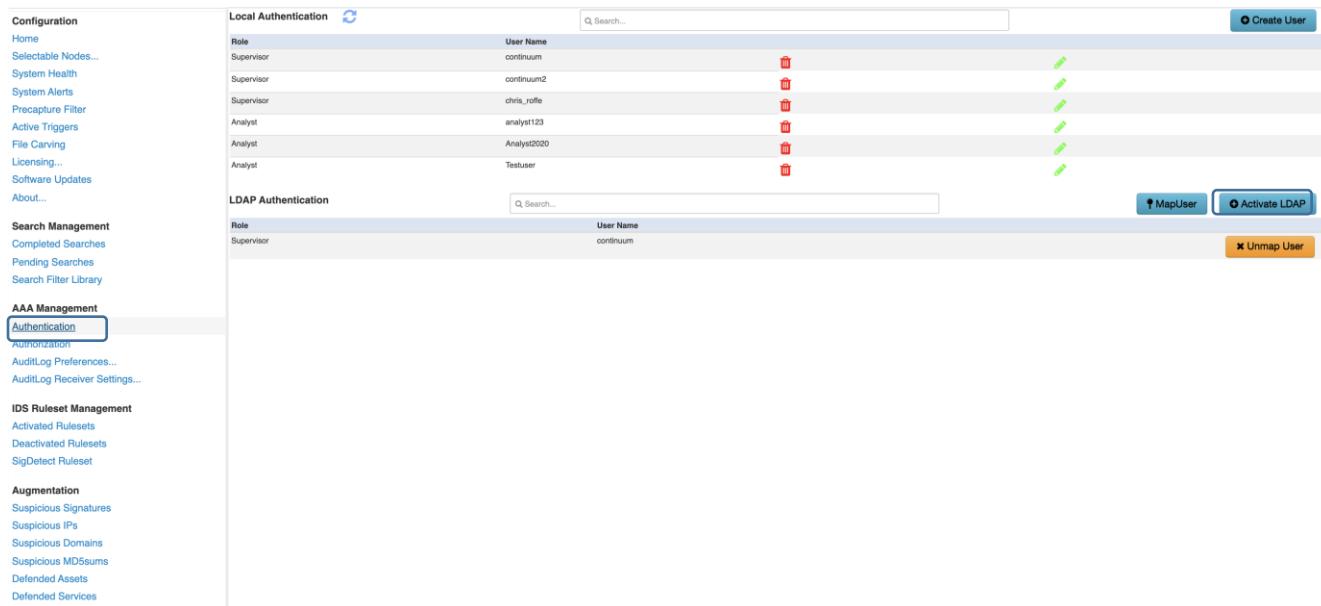


RoleName	Groups	Policy	Licensing	Authentication	Authorization	Auditing	Search
Supervisor	<input checked="" type="checkbox"/>						
Analyst	<input type="checkbox"/>						
SeniorAnalyst	<input type="checkbox"/>						

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

This page allows users to create, delete or update local users, map LDAP users to available roles.



The screenshot shows the SentryWire web interface under the 'AAA Management' section, specifically the 'Authentication' tab. The left sidebar contains navigation links for Home, Selectable Nodes, System Health, System Alerts, Precapture Filter, Active Triggers, File Carving, Licensing, Software Updates, About, Search Management, Completed Searches, Pending Searches, Search Filter Library, AAA Management (with sub-links for Authorization, AuditLog Preferences, and AuditLog Receiver Settings), IDS Ruleset Management (with sub-links for Activated Rulesets, Deactivated Rulesets, and SigDetect Ruleset), and Augmentation (with sub-links for Suspicious Signatures, Suspicious IPs, Suspicious Domains, Suspicious MD5sums, Defended Assets, and Defended Services).

The main content area has two tabs: 'Local Authentication' and 'LDAP Authentication'. The 'Local Authentication' tab displays a table of users with their roles and permissions. The table includes columns for Role, User Name, and various permission icons (red and green). A search bar and buttons for 'Create User', 'MapUser', and 'Activate LDAP' are visible. The 'LDAP Authentication' tab shows a single user entry for 'continuum' mapped to the 'Supervisor' role, with buttons for 'MapUser' and 'Unmap User'.

Local Authentication:

By default, FM and its nodes are in Local Authentication Mode. In this mode, users can login with a valid username and password maintained on the FM server.

LDAP Authentication:

The image also shows LDAP Authentication section. One or more LDAP users must be mapped to FM Roles before activating LDAP authentication mode.

MapUser allows an LDAP user to be mapped to a FM role. The above image shows one LDAP user mapped user named continuum mapped to Supervisor role. Each mapped user is assigned their mapped role on logging in. An LDAP user is not allowed to login if there is no mapping enabled for that user. Click on the MapUser button to map a new LDAP user to a FM role. Select a role from the drop down, enter user name, click on Map LDAP User button.

Map LDAP User

Role	<input type="text" value="Analyst"/>
User Name	<input type="text" value="analyst232@example.com"/>
<input type="button" value="Map LDAP User"/> <input type="button" value="Cancel"/>	

LDAP authentication mode must be activated before being able to login using one of the mapped LDAP users. Click on Activate LDAP button to see LDAP Configuration dialog box.

Configuration <ul style="list-style-type: none"> Home Selectable Nodes... System Health System Alerts Precapture Filter Active Triggers File Carving Licensing... Software Updates About... Search Management <ul style="list-style-type: none"> Completed Searches Pending Searches Search Filter Library AAA Management <ul style="list-style-type: none"> Authentication Authorizations AuditLog Preferences... AuditLog Receiver Settings... IDS Ruleset Management <ul style="list-style-type: none"> Activated Rulesets Deactivated Rulesets SigDetect Ruleset Augmentation <ul style="list-style-type: none"> Suspicious Signatures Suspicious IPs Suspicious Domains Suspicious MD5sums Defended Assets Defended Services 	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th colspan="2" style="text-align: left; padding: 2px;">Local Authentication</th> <th style="text-align: right; padding: 2px;">Q Search...</th> <th style="text-align: right; padding: 2px;"></th> </tr> </thead> <tbody> <tr> <td style="width: 15%;">Role</td> <td style="width: 40%;">User Name</td> <td style="width: 15%;"></td> <td style="width: 30%;"></td> </tr> <tr> <td>Supervisor</td> <td>continuum</td> <td></td> <td></td> </tr> <tr> <td>Supervisor</td> <td>continuum2</td> <td></td> <td></td> </tr> <tr> <td>Supervisor</td> <td>chris_roffe</td> <td></td> <td></td> </tr> <tr> <td>Analyst</td> <td>analyst123</td> <td></td> <td></td> </tr> <tr> <td>Analyst</td> <td>Analyst2020</td> <td></td> <td></td> </tr> <tr> <td>Analyst</td> <td>Testuser</td> <td></td> <td></td> </tr> </tbody> </table> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th colspan="2" style="text-align: left; padding: 2px;">LDAP Authentication</th> <th style="text-align: right; padding: 2px;">Q Search...</th> <th style="text-align: right; padding: 2px;"></th> <th style="text-align: right; padding: 2px;"></th> </tr> </thead> <tbody> <tr> <td style="width: 15%;">Role</td> <td style="width: 40%;">User Name</td> <td style="width: 15%;"></td> <td style="width: 30%;"></td> </tr> <tr> <td>Supervisor</td> <td>continuum</td> <td></td> <td></td> <td></td> </tr> </tbody> </table>	Local Authentication		Q Search...		Role	User Name			Supervisor	continuum			Supervisor	continuum2			Supervisor	chris_roffe			Analyst	analyst123			Analyst	Analyst2020			Analyst	Testuser			LDAP Authentication		Q Search...			Role	User Name			Supervisor	continuum			
Local Authentication		Q Search...																																													
Role	User Name																																														
Supervisor	continuum																																														
Supervisor	continuum2																																														
Supervisor	chris_roffe																																														
Analyst	analyst123																																														
Analyst	Analyst2020																																														
Analyst	Testuser																																														
LDAP Authentication		Q Search...																																													
Role	User Name																																														
Supervisor	continuum																																														

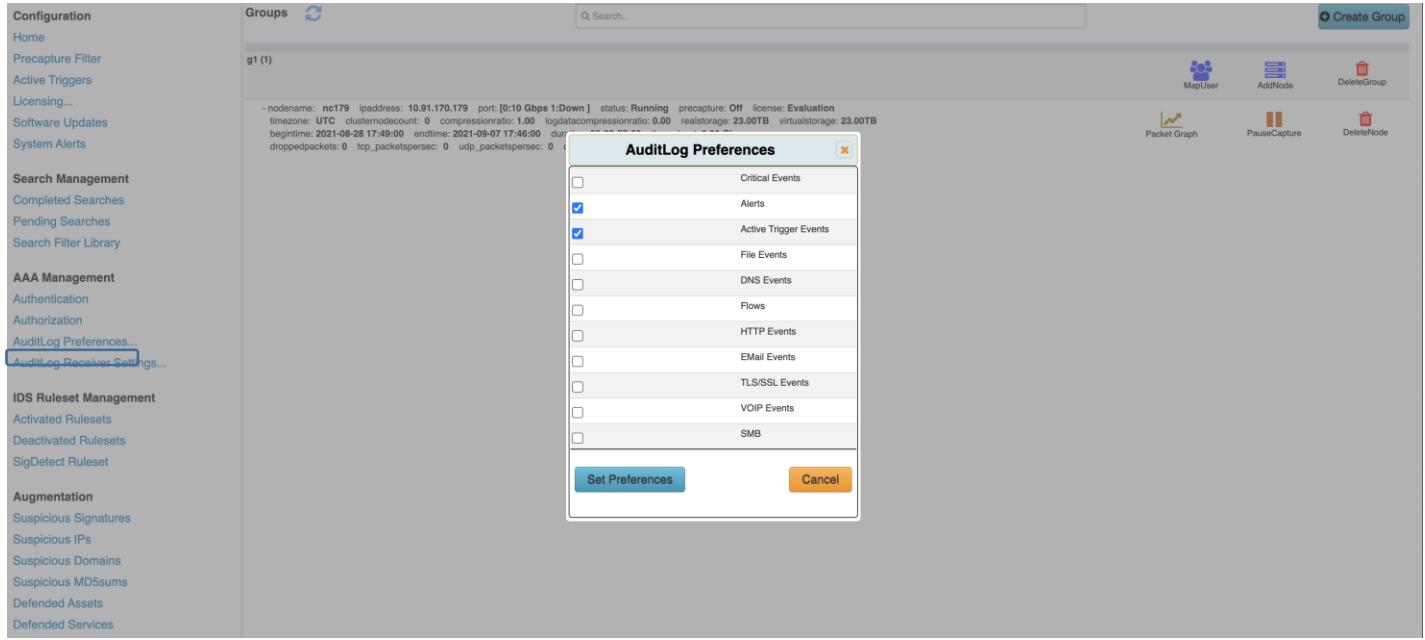
LDAP Configuration

Server IP	<input type="text" value="10.1.55.147"/>
UserName	<input type="text" value="continuum"/>
Password	<input type="text" value="Password"/>
BindString	<input type="text" value="continuum@sentrywire.test"/>
<input type="button" value="Activate ldap"/> <input type="button" value="Cancel"/>	

Once LDAP mode is activated successfully, the user must logout and log back in with valid LDAP credentials.

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, and Augmentation. The 'AuditLog Preferences...' link is highlighted with a blue box. The main area shows a group named 'g1 (1)' with a list of log types: Critical Events, Alerts, Active Trigger Events, File Events, DNS Events, Flows, HTTP Events, EMail Events, TLS/SSL Events, VOIP Events, and SMB. The 'Alerts' and 'Active Trigger Events' checkboxes are 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.

Configuration

- Home
- Selectable Nodes...
- System Health
- System Alerts
- Precapture Filter
- Active Triggers
- File Carving
- Licensing...
- Software Updates
- About...

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

Log Data Receiver			<input type="text"/> Search...	
Receiver IP	Receiver Port		Preferences	
10.1.55.174	3700		CriticalEvents, Alerts, ActiveTriggerEvents	
10.1.55.174	3900		FileEvents, DNSEvents, Flows	

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.

Configuration

- Home
- Selectable Nodes...
- System Health
- System Alerts
- Precapture Filter
- Active Triggers
- File Carving
- Licensing...
- Software Updates
- About...

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

Log Data Receiver			<input type="text"/> Search...	
Receiver IP	Receiver Port		Preferences	
10.1.55.174	3700		CriticalEvents, Alerts, ActiveTriggerEvents	
10.1.55.174	3900		FileEvents, DNSEvents, Flows	

AuditLog Receiver Settings

<input type="checkbox"/> IP Address
<input type="checkbox"/> Port
<input type="checkbox"/> Critical Events
<input type="checkbox"/> Alerts
<input type="checkbox"/> Active Trigger Events
<input type="checkbox"/> File Events
<input type="checkbox"/> DNS Events
<input type="checkbox"/> Flows
<input type="checkbox"/> HTTP Events
<input type="checkbox"/> EMail Events
<input type="checkbox"/> TLS/SSL Events
<input type="checkbox"/> VOIP Events
<input type="checkbox"/> SMB

Apply
Cancel

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.

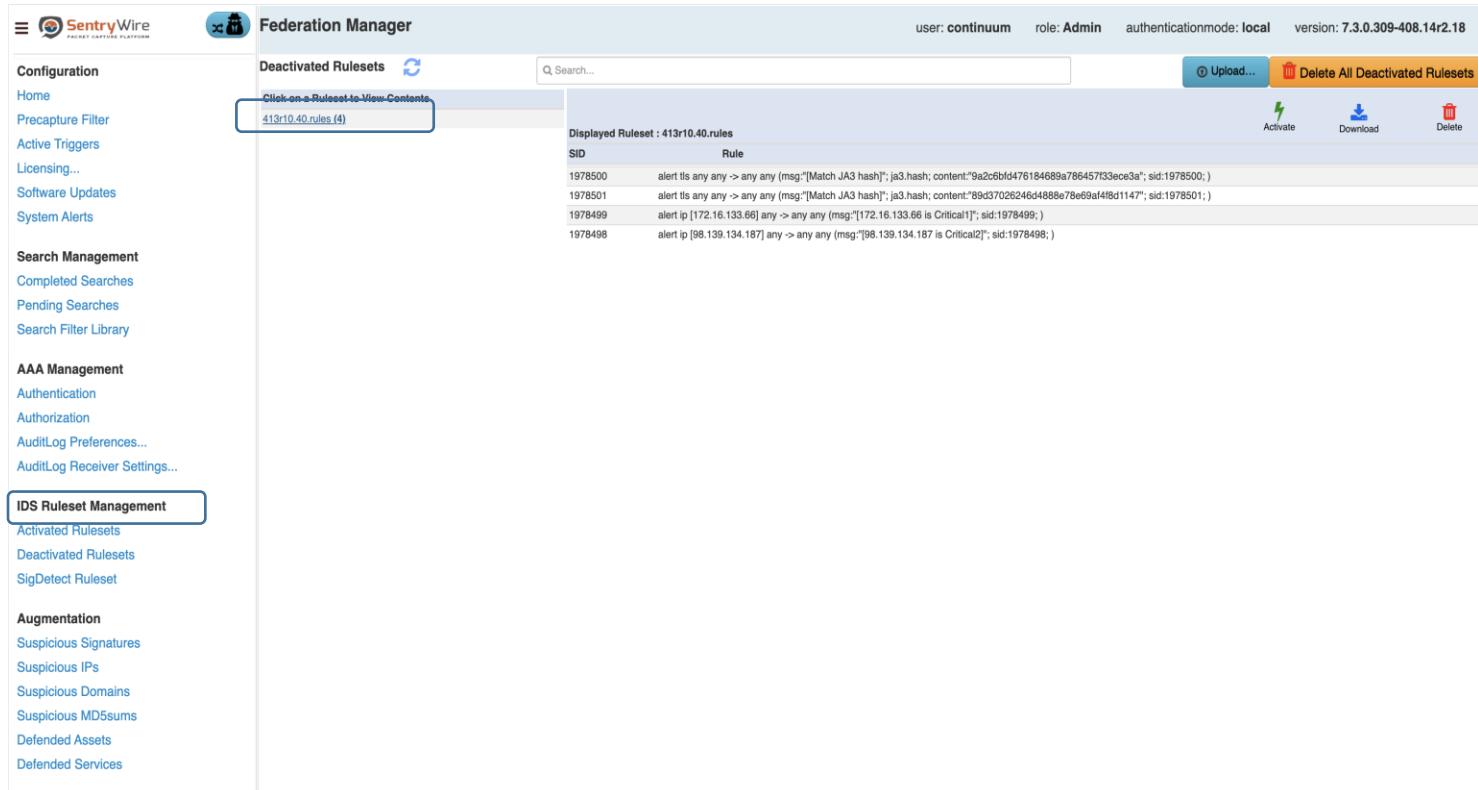
- Click on a activated ruleset to see its contents. The following image shows contents of a ruleset named activebunk2.rules file.
- Select a ruleset and click on Deactivate button. This ruleset will move to Deactivated Rulesets page. Each node removes the new ruleset from Suricata alert generation.
- 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	Displayed Ruleset : activex.rules
Home		 Search...
Precapture Filter		
Active Triggers		 Deactivate  Download  Delete
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	 Click on a Ruleset to View Contents 3coresec.rules (20) activex.rules (732)	
Deactivated Rulesets		
SigDetect Ruleset		
Augmentation		
Suspicious Signatures		
Suspicious IPs		
Suspicious Domains		
Suspicious MD5sums		
Defended Assets		
Defended Services		

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.

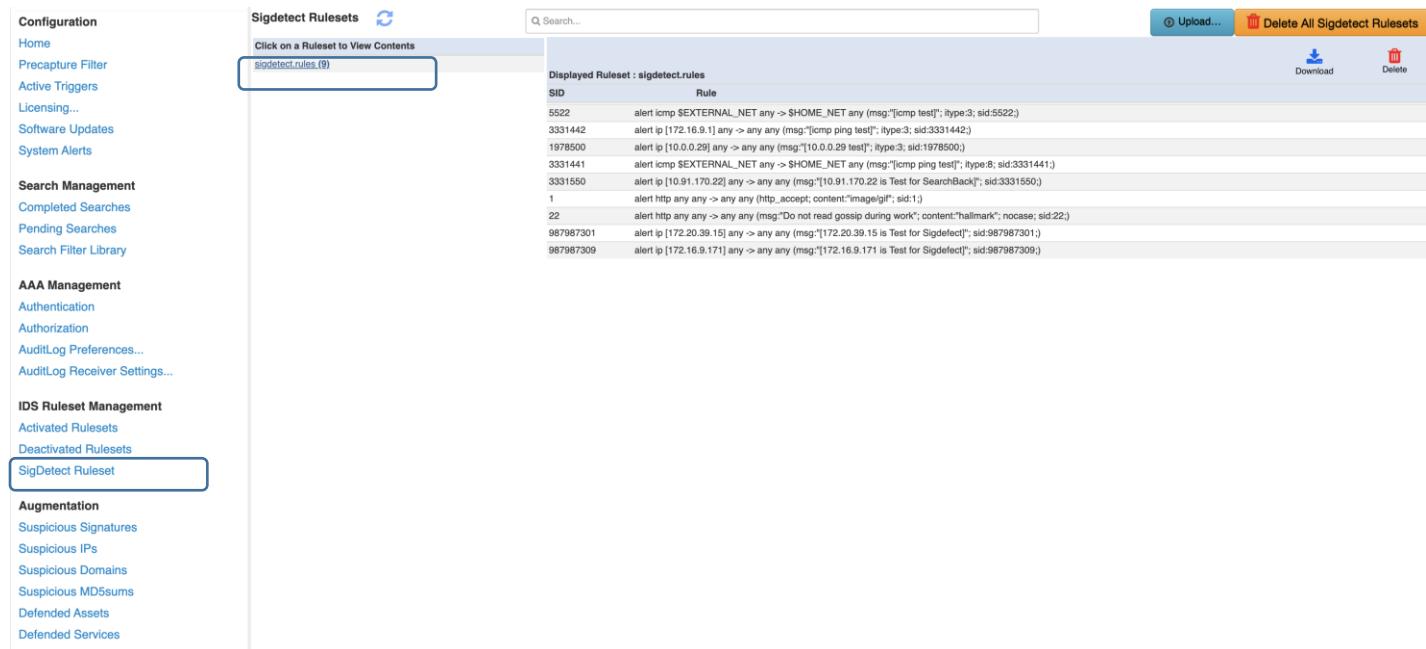


Displayed Ruleset : 413r10.40.rules	
SID	Rule
1978500	alert ts any any -> any any (msg:"[Match JA3 hash]"; ja3.hash; content:"9a2c6bfd476184689a78645733ece3a"; sid:1978500;)
1978501	alert ts any any -> any any (msg:"[Match JA3 hash]"; ja3.hash; content:"89d37026246d4888e78e69af4bd1147"; sid:1978501;)
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 the all the uploaded SigDetect rules at the time of the search completion to Suricata for alert generation. This allows checking for alerts for signatures that were not available when the traffic was originally captured.

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



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 Sigdefect]"; sid:987987301;)
987987309	alert ip [172.16.9.171] any -> any any (msg:"[172.16.9.171 is Test for Sigdefect]"; 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	Actions
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 Rulesets		
Augmentation		
Suspicious Signatures		
Suspicious IPs		
Suspicious Domains		
Suspicious MD5sums		
Defended Assets		
Defended Services		

SuspiciousSignatures

JA3	Description
89d37026246d488e78e69af4fb1d147	nc-191
05af115ca1b87cc9cc9b25185115607d	nc-191
ae0f20803d10a4d39072817184b8eedc	nc-191
fb1d89ef164dd558ad99011070785cce	nc-179
9a2c6bbfd476184689a786457f33e0e3a	nc-179
bc6c3861480ee97b9d9e52d472b772d8	02kszdadsjdajdsjdajdsjd
02kszdadsjdajdsjdajdsjd	1543a7c46633acf71e8401bacbcd0568

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 	  
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 Rulesets		
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**

Configuration	Suspicious Domains	Description	Actions
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 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 	
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		
Defended Services		

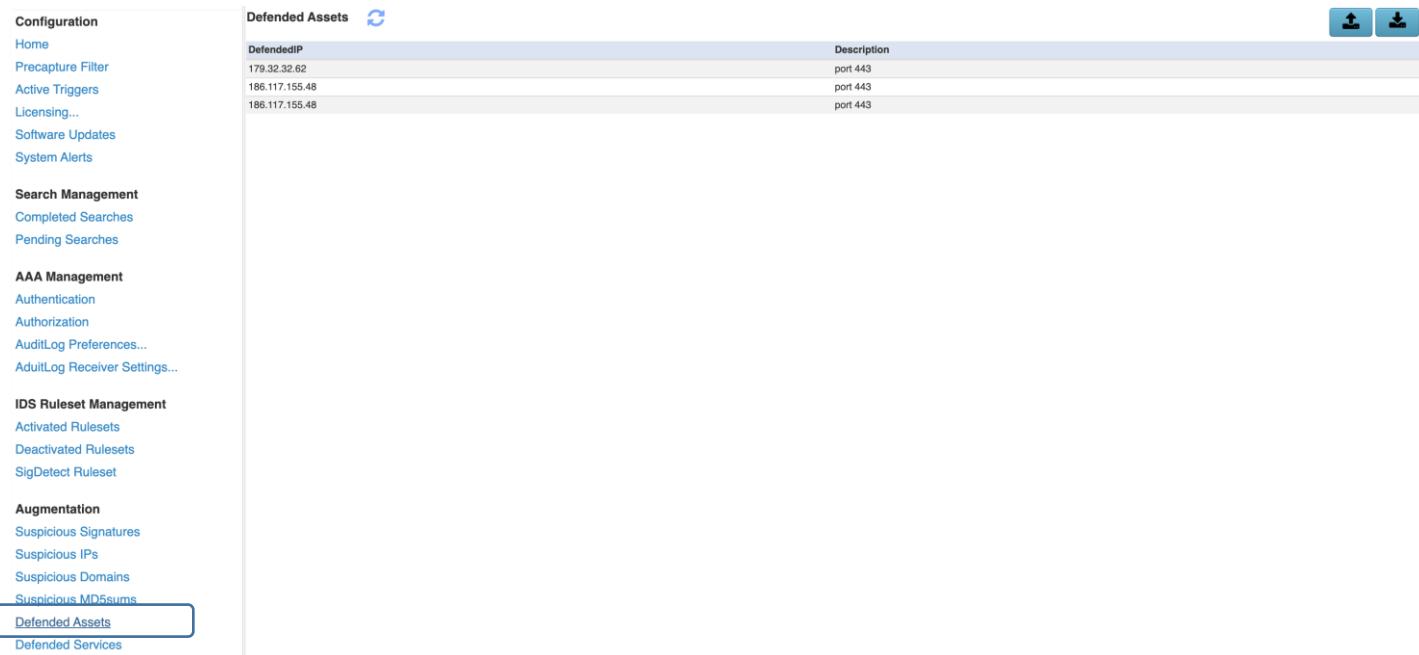
Authorized users can upload () new suspected md5sums as a csv file with each line containing a md5sum, a comma, and an optional description. Each line of the csv file must have a valid md5sum. Description is optional. If Description is provided, md5sum and Description values must be separated by a comma.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

```
bf56ce49dd485d195fd8a02342568,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**.



DefendedIP	Description
179.32.32.62	port 443
186.117.155.48	port 443
186.117.155.48	port 443

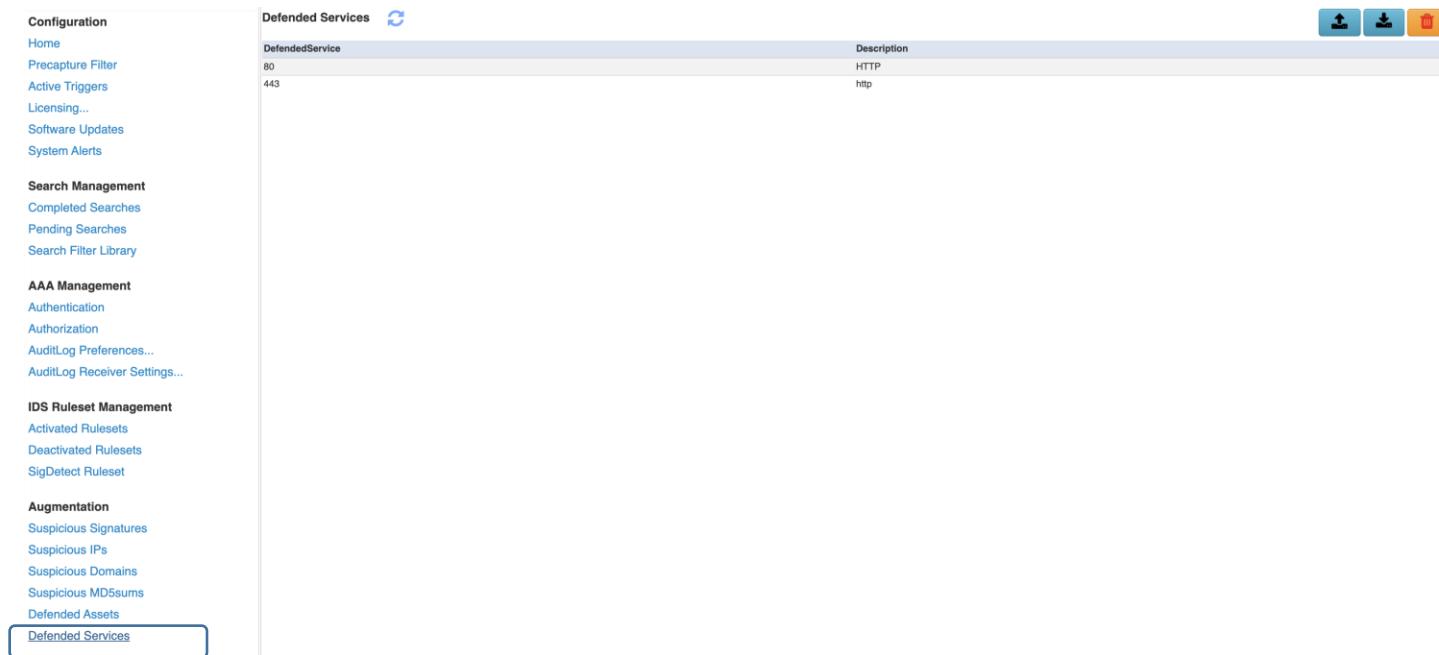
Authorized users can upload () new defended asset list as a csv file with each line containing an ip address of a defended asset, a comma, and an optional description. Each line of the csv file must have a valid ip address. Description is optional. If Description is provided, defended asset and Description 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**, **fdmi**, **tr**, **wlan**, **ip**, **ip6**, **arp**, **rarp**, **decnet**, **tcp** and **udp**.

1.1 Primitive Filters

Allowable primitives are given below for reference:

Primitive Filters	Description
<p>[src dst] host <host></p> <p>E.g., src host <host></p> <p>dst host <host></p> <p>host <host></p> <p>ip host <host></p>	<p>Matches a host as the IP source, destination, or either.</p> <ul style="list-style-type: none"> • These host expressions can be used in conjunction with other protocols like ip, arp, rarp or ip6
<p>ether [src dst] host <ehost></p> <p>E.g., ether host <MAC></p> <p>ether src host <MAC></p> <p>ether dst host <MAC></p>	<p>Matches a host as the Ethernet source, destination, or either</p>
<p>[src dst] net <network></p> <p>E.g., dst net 192.168.1.0</p> <p>src net 192.168.1</p> <p>dst net 172.16</p> <p>src net 10</p> <p>net 192.168.1.0</p> <p>net 192.168.1.0/24</p> <p>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</p> <p>src net 192.168.1 mask 255.255.255.0 or</p> <p>src net 192.168.1/24</p> <p>dst net 172.16 mask 255.255.0.0</p> <p>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>Matches packets sent to/from port</p>

E.g., src port 443 dst port 20 port 80	<ul style="list-style-type: none"> Protocols (e.g., tcp/udp/ip etc.) can be applied to a port to get specific results
[src dst] portrange <p1>-<p2> or [tcp udp] [src dst] portrange <p1>-<p2> E.g., src portrange 80-88 tcp portrange 1501-1549	<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
less <length> E.g., less 300 (or len <300)	Matches packets less than or equal to length
greater <length> E.g., greater 301(or len >300)	Matches packets greater than or equal to length
(ether ip ip6) proto <protocol> E.g., ether proto 0x888e ip proto 50	<p>Matches an Ethernet, IPv4, or IPv6 protocol</p> <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>] o E.g., vlan 100 && vlan 200 (filters on vlan 200 encapsulated within vlan 100)	Matches 802.1Q frames optionally with a VLAN ID of vlan

<ul style="list-style-type: none"> ○ vlan && vlan 300 && ip (filters IPv4 protocols encapsulated in vlan 300 encapsulated within any higher order vlan) 	
<ul style="list-style-type: none"> 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) 	<p>Matches MPLS packets, optionally with a label of label</p> <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] & 0xfffff0f > 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

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

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 <input type="button" value="▼"/> <input type="button" value="PcapData (MaxPcaps: 1)"/> <input type="button" value="LogData"/> <input type="button" value="Objects"/> <input type="button" value="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)					
			Search		
2021-05-13 19:39:16.009 -0400	172.17.8.8:53	172.17.8.174:61613	DNS	184	Standard query 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 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-a3ffd56a
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-a3ffd56a
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-a3ffd56a
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-a3ffd56a
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-a3fd56a2aa?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-a3fd56a2aa?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-a3fd56a2aa?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-a3fd56a2aa?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 ····			

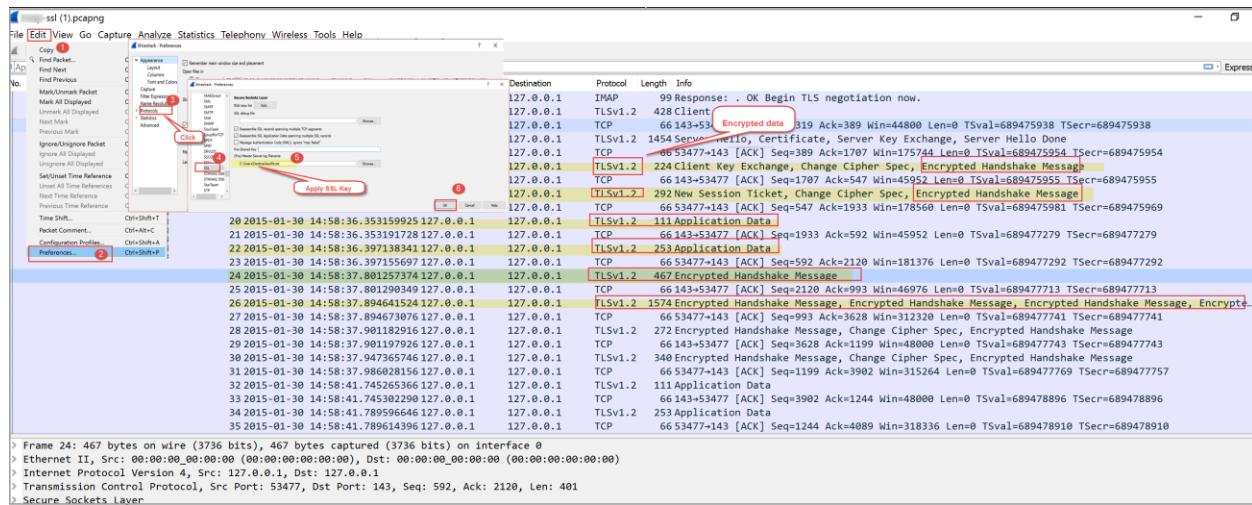
APPENDIX C - DECRYPTING PCAP WITH SSL SESSION KEYS

This workflow presumes the user has:

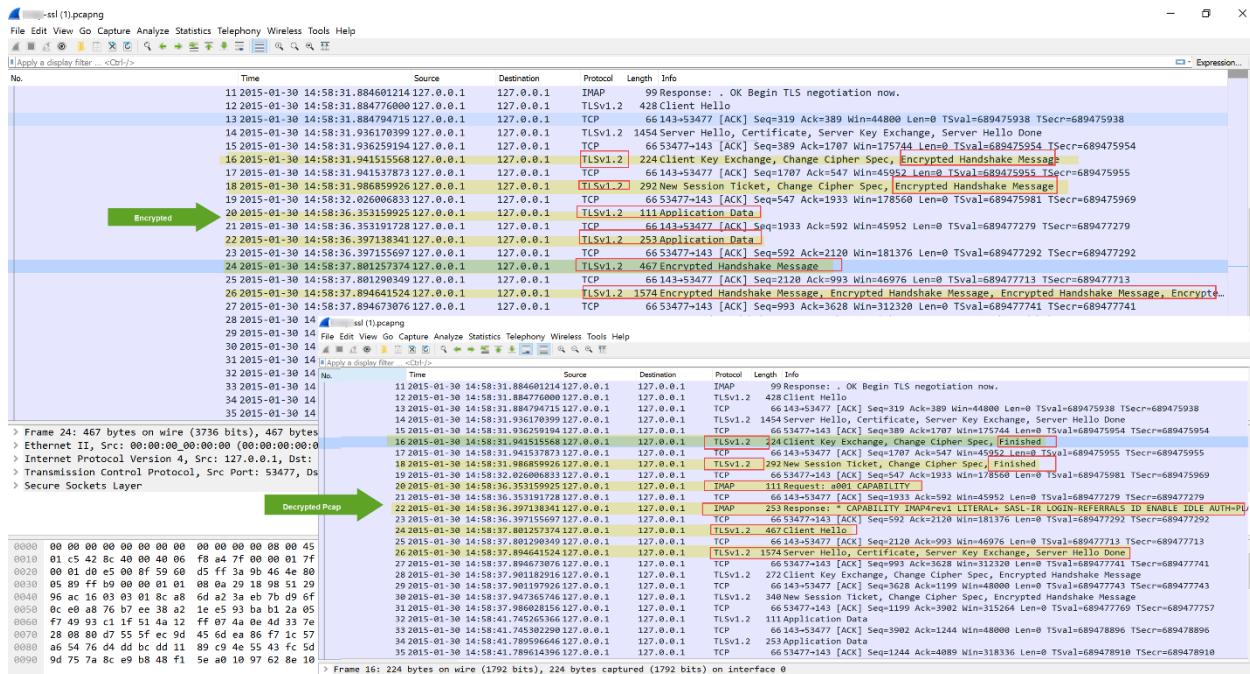
- A set of SSL Session keys for decrypting pcap data
- Downloaded one or more (encrypted) pcaps from a completed pcap search

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 - SENTRYWIRE SPLUNK ADVANCED SYNTAX

Lucene Query Syntax

Lucene query syntax is available to Kibana users who opt out of the [Kibana Query Language](#). Full documentation for this syntax is available as part of Elasticsearch [query string syntax](#).

The main reason to use the Lucene query syntax in Kibana is for advanced Lucene features, such as regular expressions or fuzzy term matching. However, Lucene syntax is not able to search nested objects or scripted fields.

Kibana Query Language

The Kibana Query Language (KQL) is a simple syntax for filtering Elasticsearch data using free text search or field-based search. KQL is only used for filtering data, and has no role in sorting or aggregating the data.

KQL is able to suggest field names, values, and operators as you type. The performance of the suggestions is controlled by [Kibana settings](#).

KQL has a different set of features than the [Lucene query syntax](#). KQL is able to query nested fields and [scripted fields](#). KQL does not support regular expressions or searching with fuzzy terms. To use the legacy Lucene syntax, click **KQL** next to the **Search** field, and then turn off KQL.

Switching Between KQL and Lucene in Kibana

You can switch between Kibana Query Language and Lucene Syntax by clicking on the square on the right end of the search bar in Kibana. It will either read KQL or Lucene depending on which is activated. Once clicked, you can toggle the Kibana Query Language button either on or off.

We recommend that you start with KQL and use Lucene for more complex searches

Finding Values

Find data where **any field matches any of the words/terms** listed. The term must appear as it is in the data, e.g. this query won't match data containing the word "darker".

KQL

orange and (dark or light)

i Use quotes to search for the word "and"/"or"

"and" "or" xor

Lucene

AND/OR must be written uppercase

orange AND (dark OR light)

Use **and/or and parentheses** to define that multiple terms need to appear. This query would find all data that have the term "orange" and either "dark" or "light" (or both) in it.

KQL

orange and (dark or light)

i Use quotes to search for the word "and"/"or"

"and" "or" xor

Lucene

AND/OR must be written uppercase

orange AND (dark OR light)

To **find values only in specific fields** you can put the field name before the value e.g. this query will only find "orange" in the color field.

KQL

color : orange title : our planet or title : dark

Lucene

color:orange

↳ Spaces need to be escaped
title:our\ planet OR title:dark

Putting quotes around values makes sure they are found in that specific order (“**match a phrase**”) e.g. if you want to make sure to only find data containing “our planet” and not “planet our” you’d need the following query:

KQL

"our planet" title : "our planet"

Lucene

"our planet"

i No escaping of spaces in phrases

title:"our planet"

You can use the **wildcard** * to match just parts of a term/word, e.g. this query will find anything beginning with “dark” like “darker”, “darkest”, “darkness”, etc.

KQL

dark*

Lucene

dark*

Wildcards can be used anywhere in a term/word.

↳ Using a wildcard in front of a word can be rather slow and resource intensive for your Elasticsearch — use with care.

KQL

d*k *les

Lucene

d*k *les

You can use the * wildcard also for searching over multiple fields in KQL e.g. this query will search “fakestreet” in all fields beginning with “user.address.”.

KQL

user.address.* : fakestreet

Lucene

Not supported

Comparing values

Compare numbers or dates. Those operators also work on text/keyword fields, but might behave [not very intuitive](#) and thus I’d recommend avoiding usage with text/keyword fields.

KQL

vlan >= 42 and vlan < 100
time >= "2020-04-10"

Lucene

vlan:>=42 AND vlan:<100

↳ No quotes around the date in Lucene
time:>=2020-04-10

Lucene supports a special **range operator** to search for a range (besides using comparator operators shown above).
KQL is not supported.

Lucene

vlan:[511 TO 514]

i Excluding sides of the range using curly braces

vlan:[511 TO 514}

vlan:{511 TO 514}

i Use a wildcard for having an open sided interval

vlan:[10 TO *]

vlan:[* TO 514]

Special queries

Find data in which a specific field **exists** (i.e. that does have a non null value for that field).

KQL

destination : *

Lucene

exists:destination

Querying **nested fields** is only supported in KQL. The syntax is a bit more complex given the complexity of nested queries. Thus I'd recommend reading the [official documentation](#).

KQL

products:{ name:pencil and price > 10 }

Lucene

Not supported

Lucene has the ability to search for [regular expressions](#). *This can be rather slow and resource intensive for your Elasticsearch — use with care.*

KQL

Not (yet) supported (see [#46855](#))

Lucene

mail:/mailbox\.org\$/

Fuzzy search allows searching for strings, that are very similar to the given query.

KQL

Not (yet) supported (see [#54343](#))

Lucene

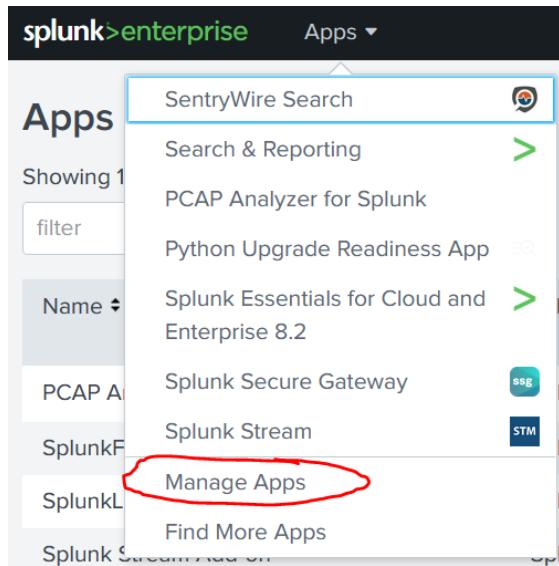
user:maria~

APPENDIX E - SENTRYWIRE SPLUNK APP DOCUMENTATION

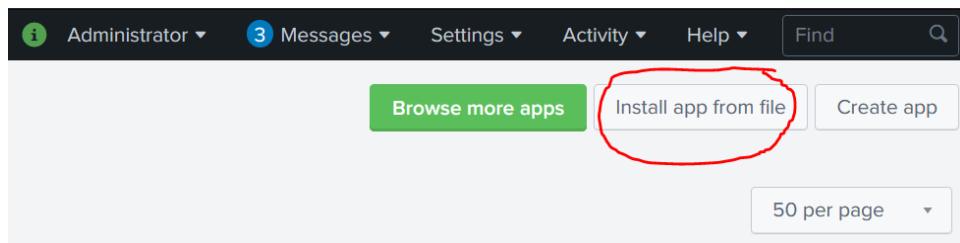
Installation

The SentryWire Splunk app currently comes as an SPL file that must be manually installed on the system.

Navigate to the “Manage Apps” page



Click “Install app from file” near the top right



Browse to the .spl file provided by the SentryWire team.

Install App From File

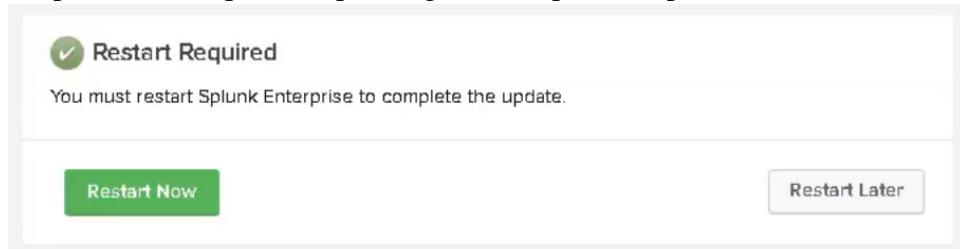
If you have a .spl or .tar.gz app file to install, you can upload it using this form.

You can replace an existing app via the Splunk CLI. [Learn more.](#)

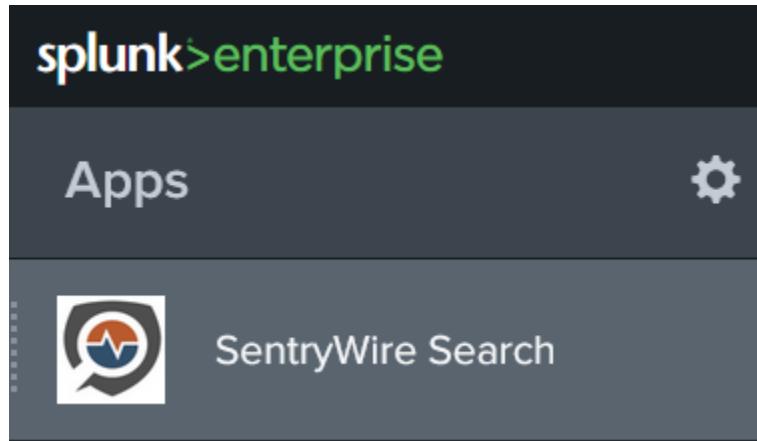
File
 No file selected.

Upgrade app. Checking this will overwrite the app if it already exists.

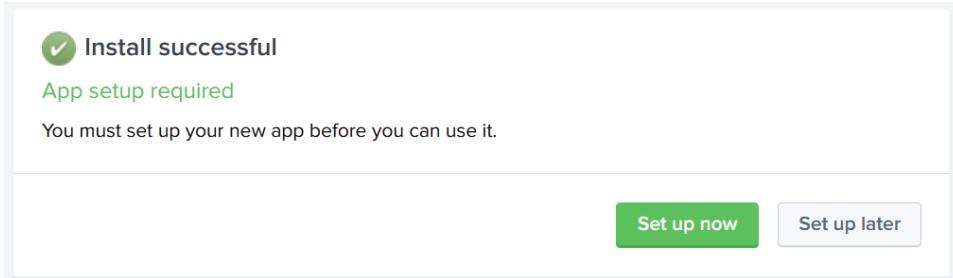
There may be a prompt to restart Splunk depending on the Splunk implementation.



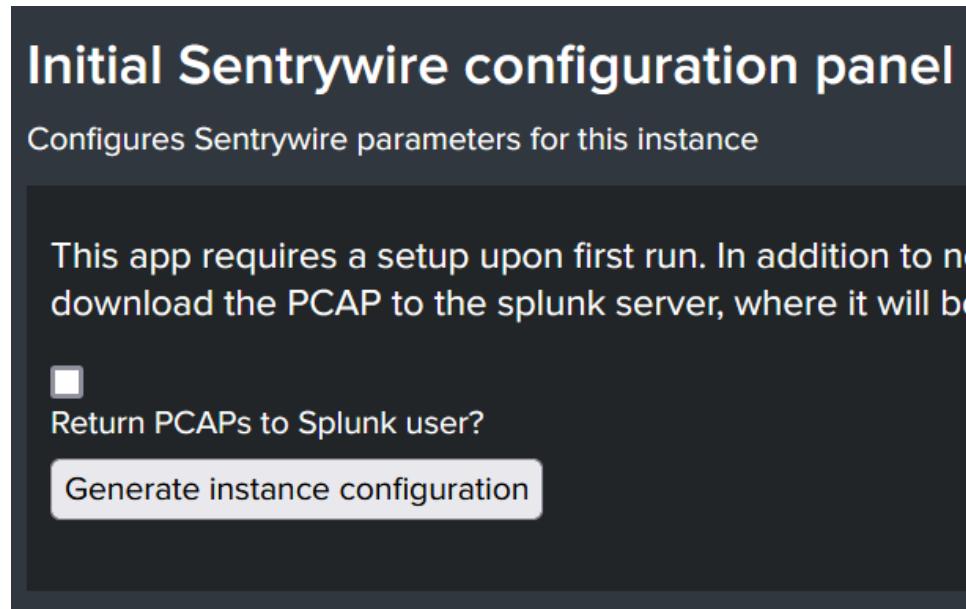
The app should now appear in the list of installed apps.



The first time the app is opened, the system will display a notification page explaining that the app requires additional information to configure the instance. Click the green button to continue.



The system will transition to the “Initial SentryWire configuration panel”. Leave the checkbox unmarked if the system should not download PCAPs to the Splunk host for the Splunk user to retrieve. If left unmarked, users will need to retrieve the search results from the SentryWire cluster. Click “Generate instance configuration” after the selection is made.



The system will automatically transition to the SentryWire authentication tab. Enter the information for the SentryWire unit and click submit.

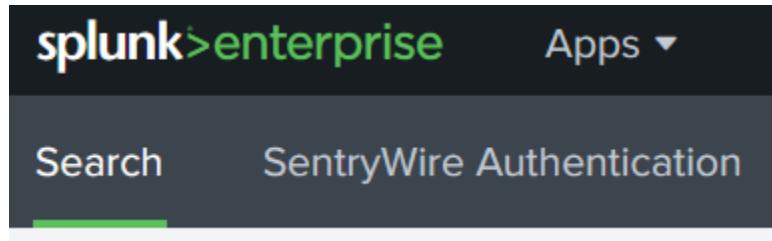
It is necessary to do this as every Splunk user that plans to use this app.

SentryWire Unit IP Address	SentryWire Username	SentryWire Password
10.1.55.152	continuum	██████████████
i	Time	Event
>	10/12/21 10:44:43.751 PM	Username "continuum" accepted.

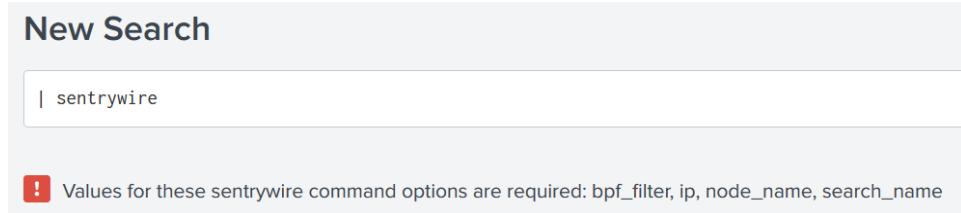
Setup is complete.

Running a search

Navigate to the search bar



We will craft a search using the SentryWire command. Place a vertical bar at the start of the search bar, and type SentryWire. This will run the SentryWire command with no input, as any events sent to the command are currently ignored.



New Search

| sentrywire

! Values for these sentrywire command options are required: bpf_filter, ip, node_name, search_name

There are several required inputs, defined in any order. Variables use this format: <*variable*>="<*value*>"

Field	Description
search_name="Splunk_search"	This is the name of the search. Data will be added to it to create the search token as it appears in the SentryWire UI.
bpf_filter="port 67"	The BPF language filter to match packets that are desirable.
ip="192.168.1.55"	IP address of the SentryWire unit to query.
node_name="east_coast"	Node name of the unit to search.
Date range	Use the native Splunk input specified in the right of the search bar.

Example search

```
| sentrywire search_name="Splunk_search" bpf_filter="port 67" ip="172.155.0.22"
```

New Search

| sentrywire search_name="Splunk_search" bpf_filter="port 67" ip="10.1.55.152" node_name="sw152"

✓ 2 events (10/11/21 11:00:00.000 PM to 10/12/21 11:23:50.000 PM) No Event Sampling ▾

Events (2) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect

	Time	Event
>	10/12/21 11:23:52.465 PM	Sentrywire search created with identifier: continuum_1634095432_37_Splunk_search
>	10/12/21 11:23:52.474 PM	Time elapsed: 0.04 seconds

There may or may not have a link in the response, depending on how the system is configured.

If so, the link will contain a zipped copy of the first PCAP in the search. In searches that require the search to complete, the search will display “No results yet found” until the results are gathered and downloaded.

New Search

| sentrywire search_name="Chris_demo" bpf_filter="port 67" ip="10.1.55.152" node_name="sw152" max_packets=10

0 of 0 events matched No Event Sampling ▾

Events (0) Patterns Statistics Visualization

No results yet found

Right click to open link in new tab to download the link.

New Search

| sentrywire search_name="Splunk_search" bpf_filter="port 67" ip="10.1.55.152" node_name="sw152" max_packets=10

✓ 2 events (10/11/21 11:00:00.000 PM to 10/12/21 11:42:07.000 PM) No Event Sampling ▾

Events (2) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect

	Time	Event
>	10/12/21 11:42:34.596 PM	Sentrywire PCAP location: http://10.1.55.173:8000/static/app/sentrywire/pcaps/continuum_1634096529_39_Splunk_search.zip
>	10/12/21 11:42:34.613 PM	Time elapsed: 25.41 seconds

Available fields

There is no order to the fields. Those appearing in red are required for each search. If optional fields such as username + password, or start + end time are defined in the search, the variables presented in the search will take priority over alternatives.

Field	Description
search_name	Name of the search.
bpf_filter	BPF filter to apply to time span.
ip	Location of SentryWire unit.
node_name	Name of the SentryWire node
max_packets	The maximum number of packets to include in the results. May return slightly more or less depending on session data.
username	SentryWire username. Bind credentials to current user via login page. If manually specified, must use both username and password.
password	SentryWire password. Can bind credentials to current user via login page. If manually specified, must use both username and password.
start_time	Use the native Splunk input specified in the right of the search bar. Can be manually specified in ISO 8601 format <ul style="list-style-type: none"> • 2021-09-24T12:17:41 • YYYY-MM-DDTHH:mm:ss If manually specified, must use both start and end.
end_time	Use the native Splunk input specified in the right of the search bar. Can be manually specified in ISO 8601 format <ul style="list-style-type: none"> • 2021-09-24T12:17:41 • YYYY-MM-DDTHH:mm:ss If manually specified, must use both start and end.

Updating SentryWire credentials

To update the credentials associated with a Splunk account, resubmit valid credentials in the SentryWire authentication page.

SentryWire Unit IP Address	SentryWire Username	SentryWire Password						
10.1.55.152	continuum	██████████████						
<table><thead><tr><th>i</th><th>Time</th><th>Event</th></tr></thead><tbody><tr><td>></td><td>10/12/21 10:44:43.751 PM</td><td>Username "continuum" accepted.</td></tr></tbody></table>			i	Time	Event	>	10/12/21 10:44:43.751 PM	Username "continuum" accepted.
i	Time	Event						
>	10/12/21 10:44:43.751 PM	Username "continuum" accepted.						
<input type="button" value="Submit"/>								

Error reporting

These things happen. Errors will appear in a dialog prompt under the search bar. In the case of a failed search, it is possible that the SentryWire unit started the search, but did not complete it in time. In this case, the successful search is still available on the SentryWire unit.

New Search

```
| sentrywire username="JoeAdmin" password="Password" search_name="Splunk_search_demo" bpf_filter="port
```

! The following error(s) occurred while the search ran. Therefore, search results might be incomplete. [Show errors.](#)

Show the error to gain insight into the issue.

New Search

```
| sentrywire username="JoeAdmin" password="Password" search_name="Splunk_search_demo" bpf_filter="port
```

! The following error(s) occurred while the search ran. Therefore, search results might be incomplete. [Hide errors.](#)

- Login failure: 401 Invalid username and/or password Message: Invalid Username and/or Password
- External search command 'sentrywire' returned error code 1..

Universal forwarder installation

This process will require back end console access. Run the following commands to set up the forwarder.

- 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 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/
- ./splunk add monitor /storage0/logforwarder
- ./splunk add forward-server 192.168.1.175:9997
- ./splunk restart

Underlying system description

It is unnecessary for an average user to understand the remainder of the document.

Commands

There are two SentryWire commands that constitute the app.

SentryWire

This is the search function. Most users will be familiar with this.

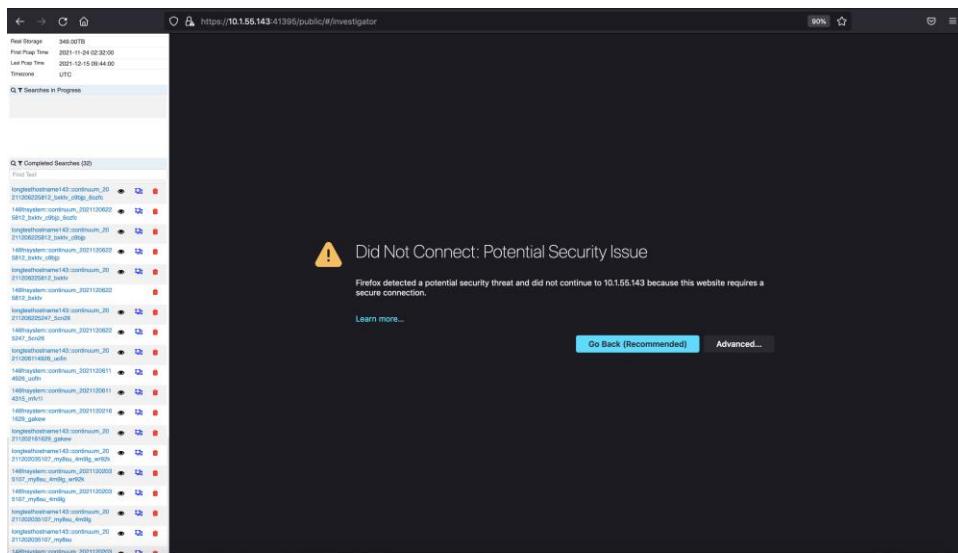
SentryWire-login

This command is run when the user presses submit on the SentryWire authentication page. It takes username, password, and ip as variables. It is recommended to use the UI as it does not show plaintext passwords on screen.

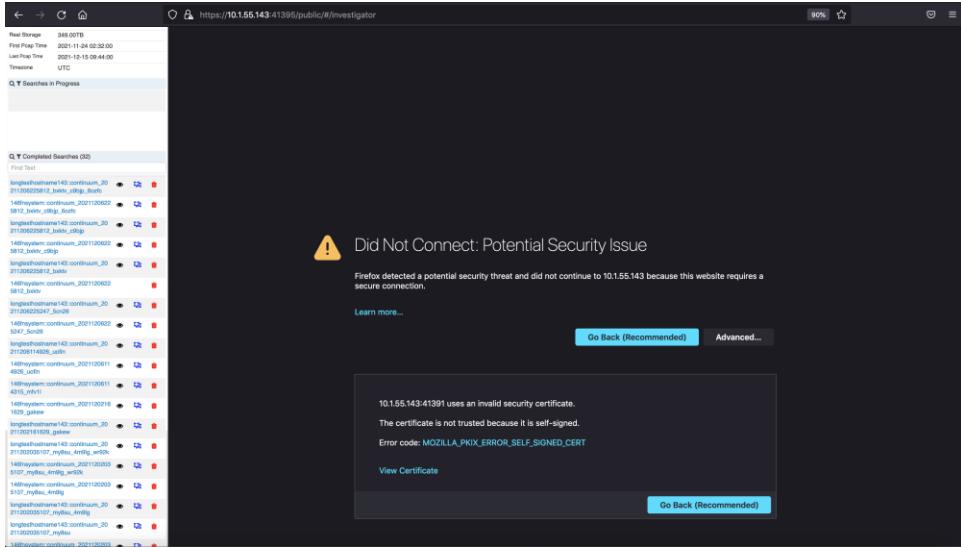
APPENDIX F – TROUBLESHOOTING RECOMMENDATIONS

Firefox Certificate Exception

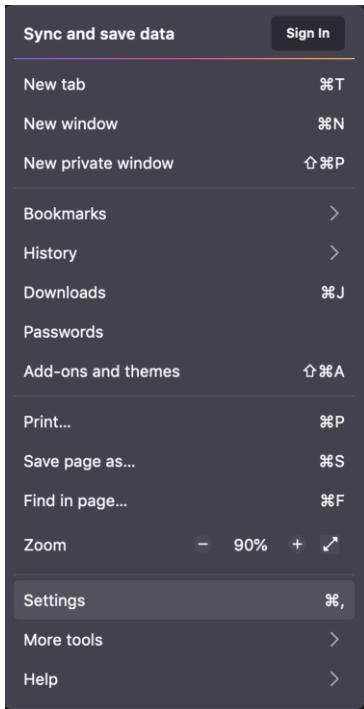
If Firefox browser shows Certificate error as shown below, follow the steps shown in this section. FM <serverip> Address is 10.1.55.143 for this example.



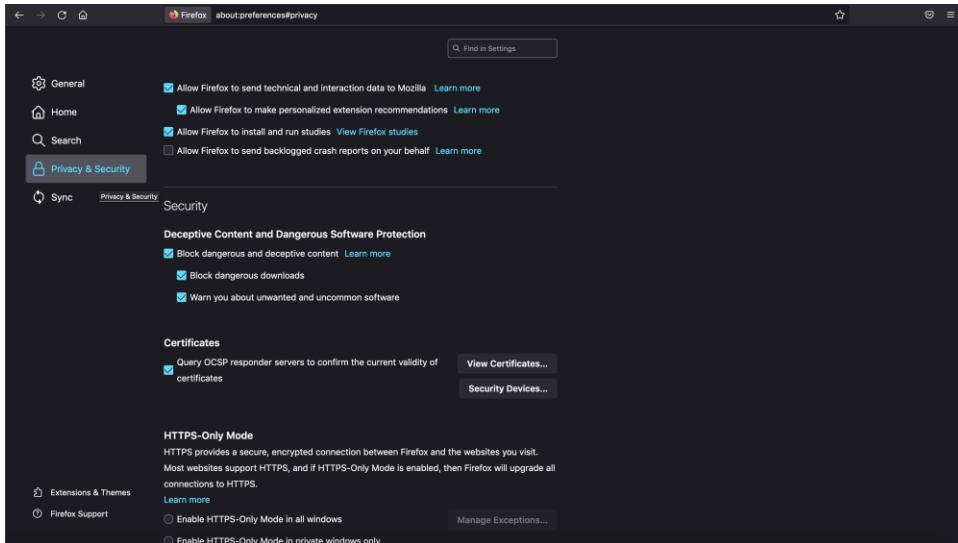
Click on Advanced... does not show Accept Risk and Continue option:



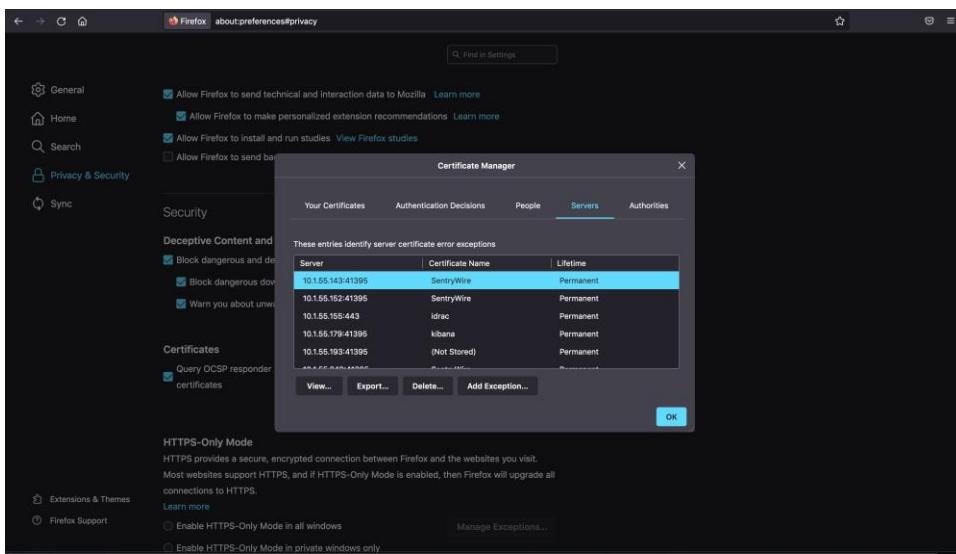
Select Browser Settings:



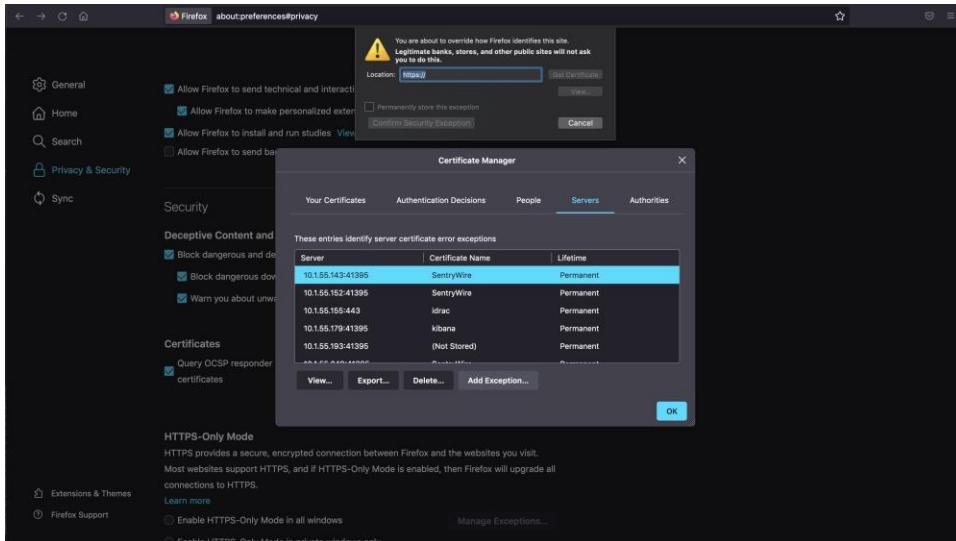
Select Privacy & Security and scroll to Certificates portion of the page:



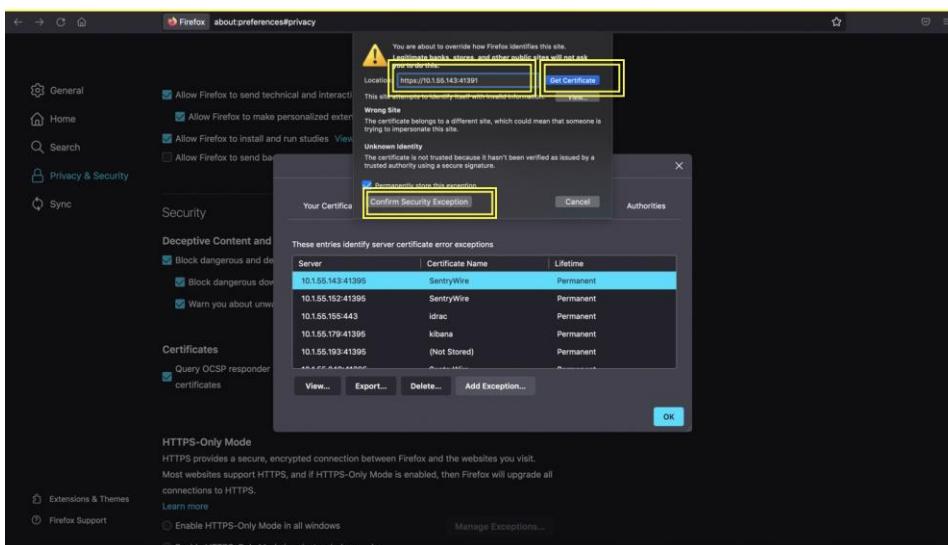
Click on View Certificates... to show Certificate Manager dialog box:



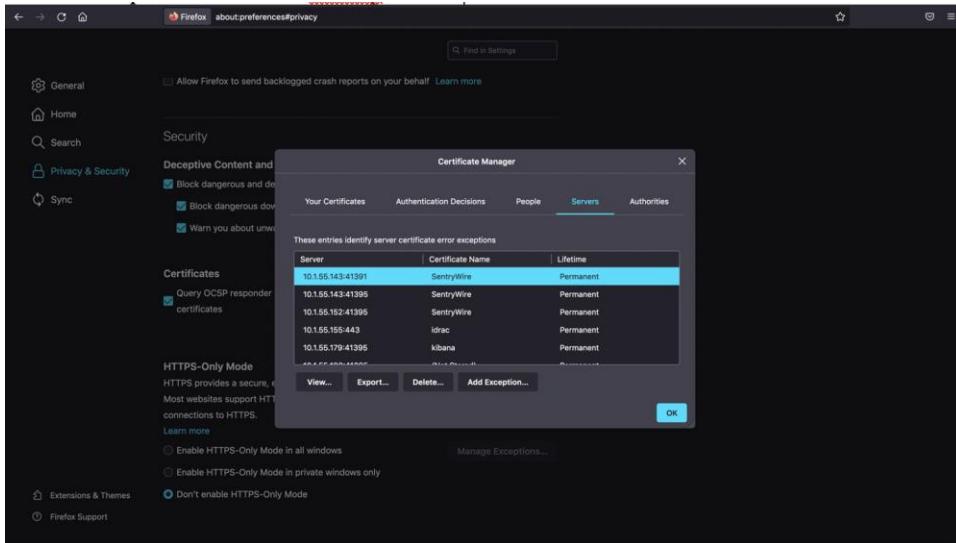
Click on Add Exception... button to add an exception:



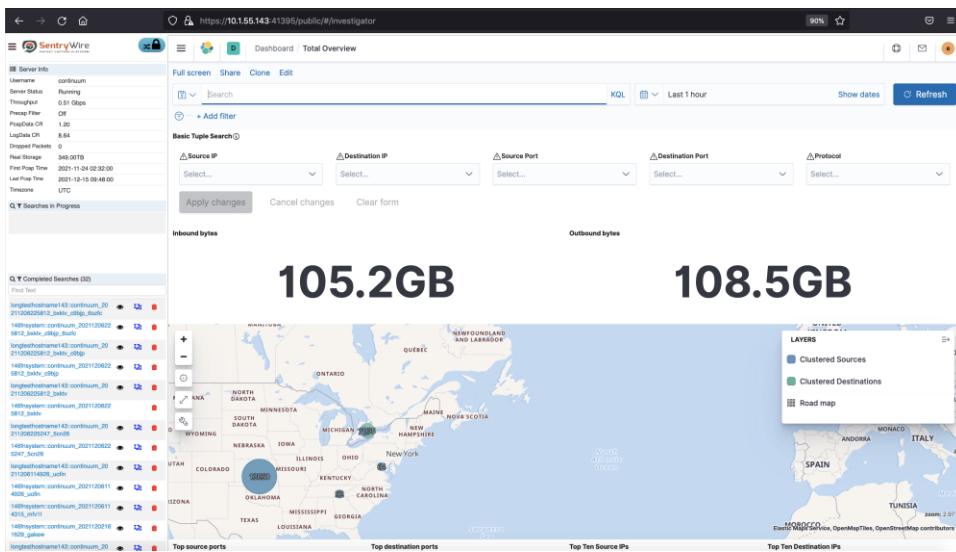
Enter <https://<serverip>:41391>, click on Get Certificate button, then click on Confirm Security Exception button:



The new exception is added for <serverip>:41391:



Refresh the Investigator page:



APPENDIX G – SYSTEM CONFIGURATION (NTP AND DNS)

To begin modifying the system NTP or DNS configuration, login to the OS (via SSH, KVM, etc).

NTP Configuration

1. Run the following command to open the config file
\$ vi /etc/ntp.conf
2. Add the appropriate information to this file. For example:
server 10.1.55.202 //set this to your primary NTP server
server 0.pool.ntp.org //set this to your Secondary NTP server (Optional)
3. Restart the NTP process using the following command:
\$ systemctl restart ntpd
4. Ensure NTP loads on system startup using the following command:
\$ systemctl enable ntpd
5. To test that the changes have been applied and taken effect, run the following command and ensure the output matches the desired NTP servers:
\$ ntpq -p

DNS Configuration

1. Identify the system management interface using the “ifconfig” command. Most likely, the management interface will be “eno1”
2. Open the matching file /etc/sysconfig/network-scripts/ifcfg-<interface>. For example:
\$ vi /etc/sysconfig/network-scripts/ifcfg-eno1
3. Edit (or append) the “DNS1” and “DNS2” fields to the appropriate values
4. Save and close the configuration file
5. Reload the system networking using the following command:
\$ service network restart
6. (Optional) Attempt to ping the DNS server(s) to verify the connection.