ALLIANCE TECHNOLOGY GROUP

SentryWire

PACKET CAPTURE PLATFORM

USER GUIDE REV2.5

Software Version Number: 408.13

Version Date: January 30, 2020

Table of Contents

DOCUMENT REVISION HISTORY

Rev 2.0	Document Format and Design Revision	04/18/2018
Rev 2.1	Software update 408.10	11/1/2018
Rev 2.2	Software Update 408.11	3/12/2018
Rev 2.3	Software Update 408.12	5/1/19
Rev 2.4	Software Update 408.12_b13	8/26/19
Rev 2.5	Software Update 408.13	1/30/20

1 INTRODUCTION

The SentryWire appliance captures and stores network traffic and analytics data from a live network interface at rates up to 100 Gbps (Gigabits per Second), and writes them to files without packet loss. SentryWire uses the standard PCAP file format to store network traffic.

SentryWire also has the ability to search captured network traffic by time and packet envelope data. Search and capture can be performed simultaneously, the 10G and 20G editions support the ability to create clusters, expanding upon the overall data storage and computational ability, when compared to a single standalone server.

2 MAIN FEATURES

- Use of the standard PCAP file format.
- High-performance packet-to-disk recording.
- Cluster-capable to increase capture data capacity.
- Real-Time indexing. This application is able to produce an index on-the-fly during packet capturing. The index can be queried using BPF search filters to quickly retrieve interesting packets in a specified time interval.
- Detailed insight and review of various alerts, conditions, events for intrusion detection, network security monitoring, and log management.
- Threat hunting and policy management.

3 SUPPORTED WEB BROWSERS

The following web browsers support the SentryWire Application interface.

- Google Chrome 44.0.2403.157 or above.
- Mozilla Firefox version 45.0.1 or above.

> ***Note***:
> - *There is no native support for chrome browser on CentOS system*

4 LOGIN INFORMATION

On any remote system connected to the network, open a supported web browser and enter the IP address using port number 41395 over https.

For Example: https://<IP Address>:41395

When the login screen appears, enter the username and password. The username and password is established during installation.

Note:

- ***The account is locked after three failed login attempts in a ten minute period. The account is locked for 30 minutes. A system administrator can manually unlock the user account.***
- ***If the system is configured to accept LDAP user/password, there is no default username/password. To login you must have a valid LDAP username/password.***

5 DASHBOARD

The Federation Manager Dashboard is an interface that allows the users to configure groups and manage all Federated Nodes within the groups.

The dashboard has 2 display options:

1. Group View
2. Node View

The default view of the Dashboard is the Group View.

5.1 GROUP VIEW

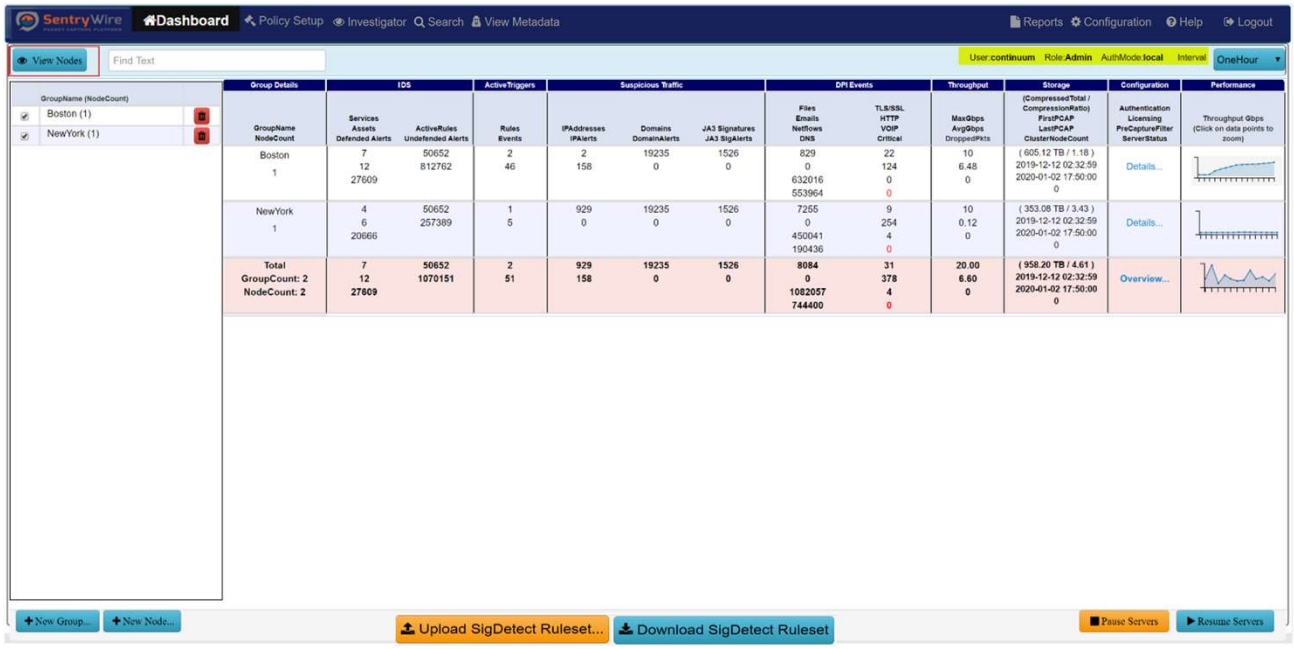


Figure 1-Default Dashboard Group View

The Group view dashboard displays the following:

- "View Nodes" button and Find Text search option. Clicking on "View Nodes" button shows the Federated Node view where each node's configuration, alert and storage information is displayed.
- UserName, License status and Authentication mode of the FM.
- Currently selected time interval and relevant data based on the selected option. The user can also change the duration of the data being displayed through the dropdown selection.

***Note**:* Default Interval is "One Hour".

- Group Names and Node count per group.

Notes:

- By Default, all groups are displayed in the FM.
- Any action performed on selected group from FM is applied to all the nodes included in the selected group only. If no group is selected, any action performed through FM applies to all groups in the FM.

- "+New Group" and "+New Node" buttons which allow the user to create new groups and add nodes to the groups. (Please refer to section 3.1.2 for more details)
- "Upload SigDetect Ruleset…" button at the bottom of the dashboard allows the user to upload SigDetect rules on Pcap data retrieved by searches for all the nodes that are part of the selected group.

Notes:

- If no group is selected this action will be applied to all groups/nodes in the federation.
- This Rule file is separate/independent of the 50K rules enabled for capture going forward.
- To see search results with SigDetect rules, goto Search→ Manager → Click on Log Data Hyperlink.

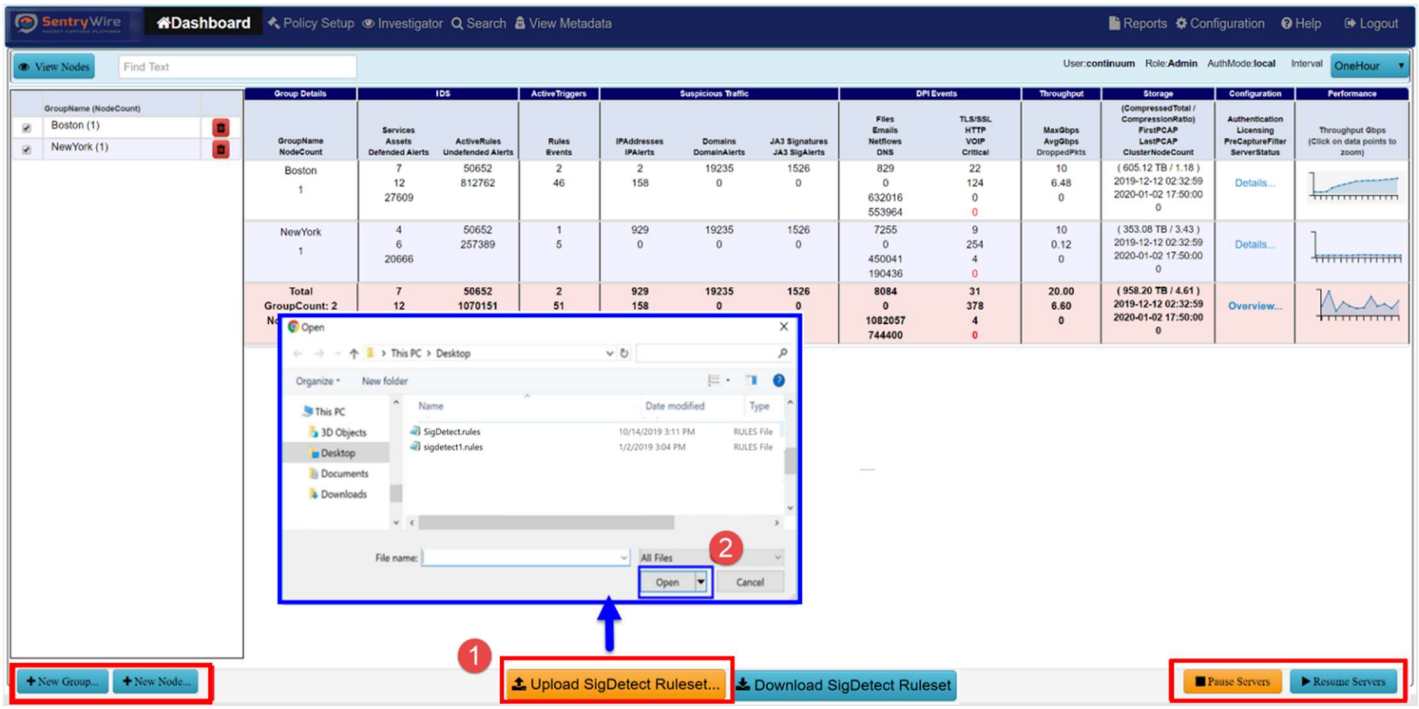


Figure 2-Upload SigDetect

- The "Download SigDetect Ruleset" button on FM Dashboard downloads the SigDetect rules (if any) from the FM Node itself.

  For example: If FM has 2 groups, 1 with 10 nodes including the current node and the other with 2 nodes. Upload SigDetect Ruleset option allows the user to upload to nodes of group1 or group2 or both. Download SigDetect Ruleset will download the last valid copy of SigDetect ruleset from the FM node itself.

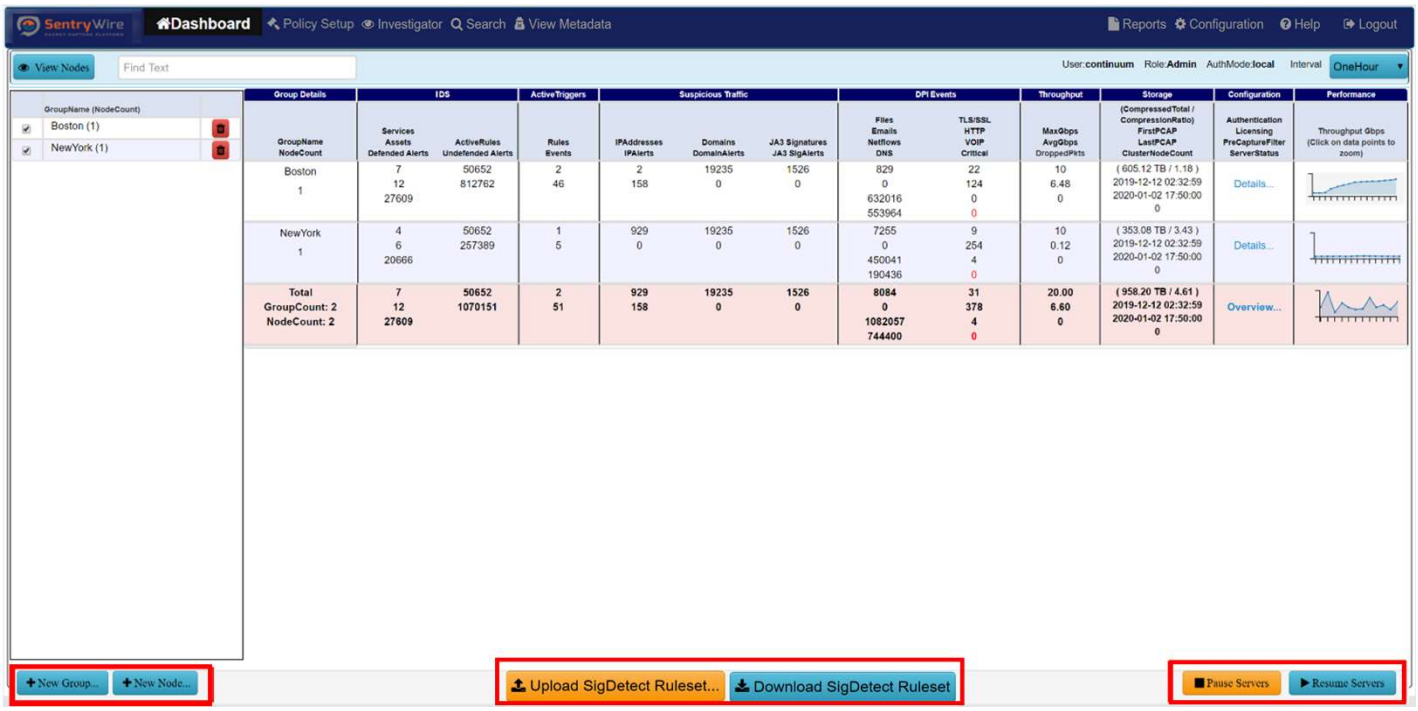


Figure 3-Upload Sig Detect Ruleset

- "Pause Servers" and "Resume Servers" buttons which allow the user to pause or resume all servers with just one click action.

***Notes**:*

- This is a global action and applies to the selected group only. If no group is selected, this action applies to all groups.
- If one or more of the nodes receiving the Pause Server message are already paused, this new request does not change the state of the servers. Each Paused server stays paused. Each server in running state will be paused.
- If one or more of the nodes receiving the Resume Server message are already running, this new request does not change the state of the servers. Each running server stays running. Each server in paused state will be resumed.

- The Group Details panel provides a quick insight into the selected group's aggregated data, events, alerts, throughput, storage, configuration and performance stat.

The **First column "Group Details"** provide the group name and the count of the nodes present in that group.

The **Second column IDS** has 2 subcategories:

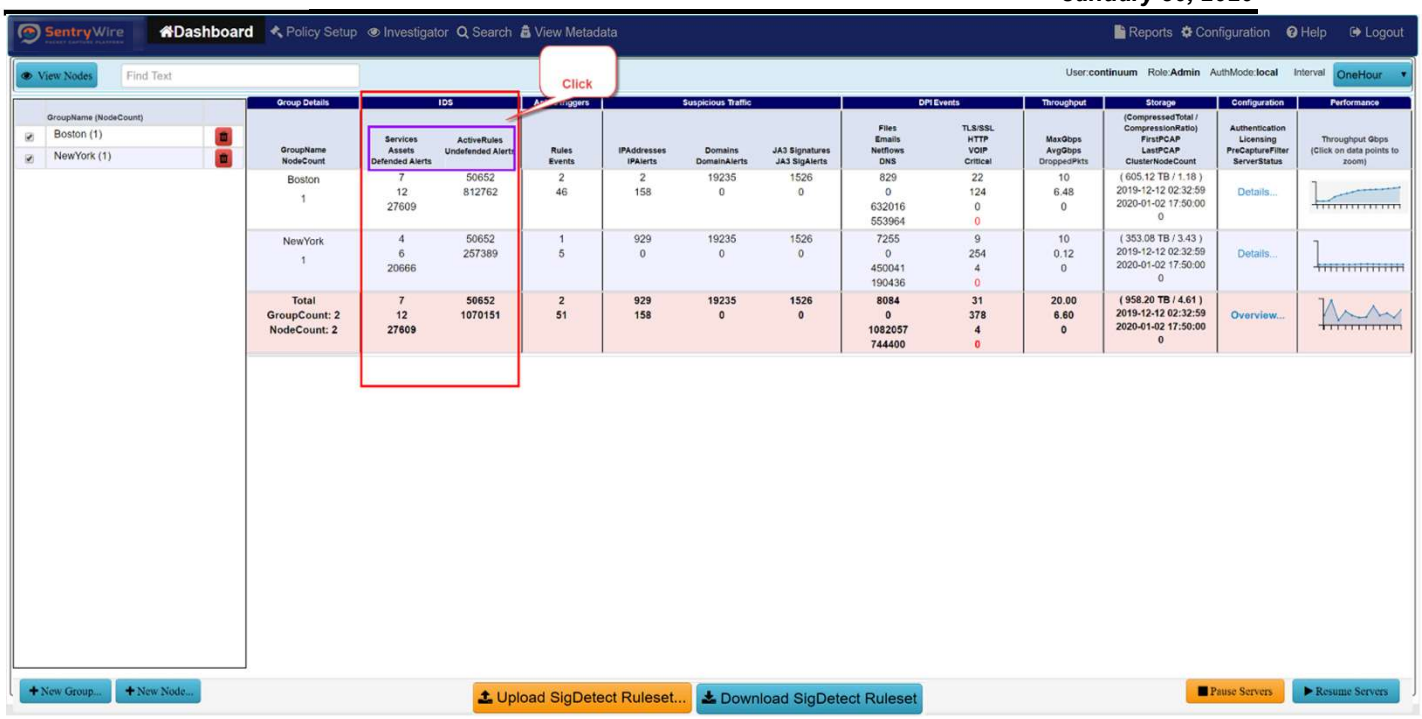


Figure 4-Dashboard IDS Column sub-categories

- **First** sub-category shows Services, Assets and Defended Alerts. Each of these are hyperlinked to pivot to their relevant screens.
  For example:
  - Clicking on "Services" sub-category pivots to Policy setup->Defended services screen.
  - Clicking on "Assets" sub-category pivots to Policy setup->Defended assets screen.
  - Clicking on "Defended Alerts" sub-category pivots to View Metadata->Defended Alerts screen.

- **Second** sub-category shows Active Rules and Undefended Alerts. Each of these are hyperlinked to pivot to their relevant screens.
  - Clicking on "Active Rules" sub-category pivots to Policy setup->IDS rule screen.
  - Clicking on "Undefended Alerts" sub-category pivots to View Metadata->Undefended Alerts screen.

Note:

- Total alerts generated is equal to the sum of Defended Alerts and Undefended Alerts.

The **Third column Active Trig**gers shows Rules that are defined by users for that group and Events generated as a result of these rules.

- Clicking on "Rules" pivots to Policy setup->Active Triggers screen.
- Clicking on "Events" pivots to View Metadata ->Active Triggers tab.

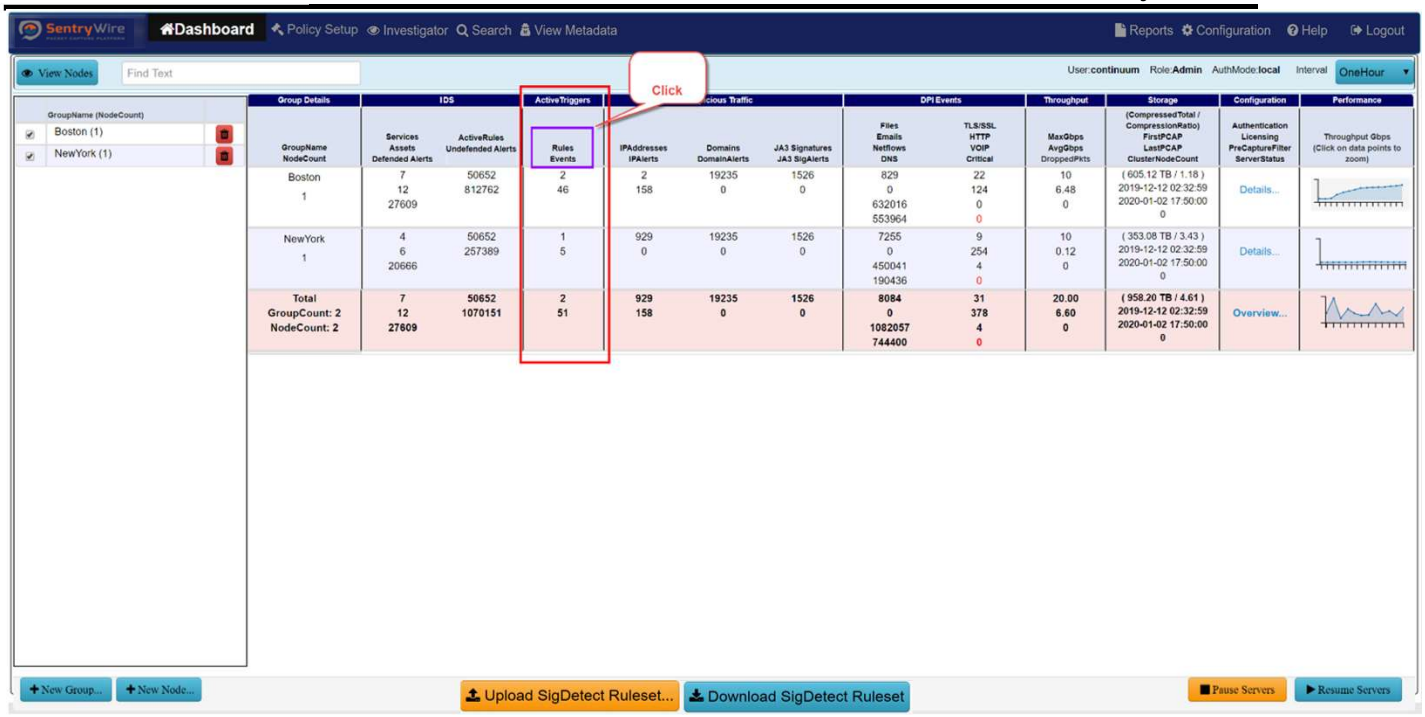


Figure 5-Dashboard Active Trigger column Rules Events

The **Fourth column "Suspicious Traffic"** has three sub-categories:

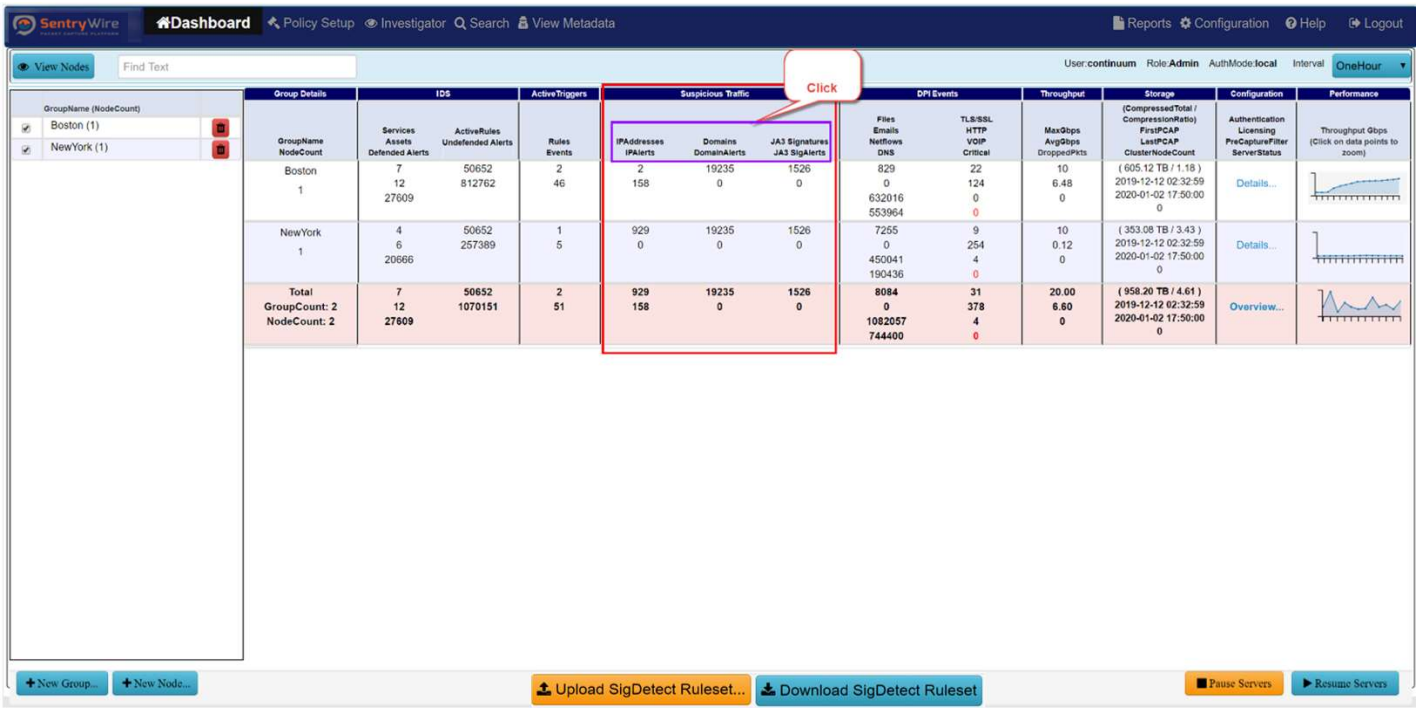


Figure 6-Dashboard Suspicious Traffic Column sub-categories

- **First** sub-category shows the count of Suspicious IP Addresses uploaded by the user for the group, and the IP Alerts generated due to the uploaded IP Addresses. Each of these are hyperlinked to pivot to their relevant screens.

- Clicking on “IP Addresses” sub-category pivots to Policy setup->Augmentation screen.
- Clicking on “IPAlerts” sub-category pivots to View Metadata->SuspIPAlerts screen.

- **Second** sub-category shows the count of Suspicious Domains uploaded by the user for this group, and the Domain Alerts generated due to the uploaded Domains.
  - Clicking on “Domains” sub-category pivots to Policy setup->Augmentation screen.
  - Clicking on “DomainAlerts” sub-category pivots to View Metadata->SuspDomains screen.

- **Third** sub-category shows the count of Suspicious (JA3) signatures uploaded by the user for this group, and the Signature Alerts generated due to the uploaded Signatures.
  - Clicking on “JA3 Signatures” sub-category pivots to Policy setup->Augmentation screen.
  - Clicking on “JA3SigAlerts” sub-category pivots to View Metadata-> SuspSig(JA3)Alerts screen.

The **Fifth column DPI Events** shows events generated by the DPI engine running on each node of the group. It has two sub-categories:

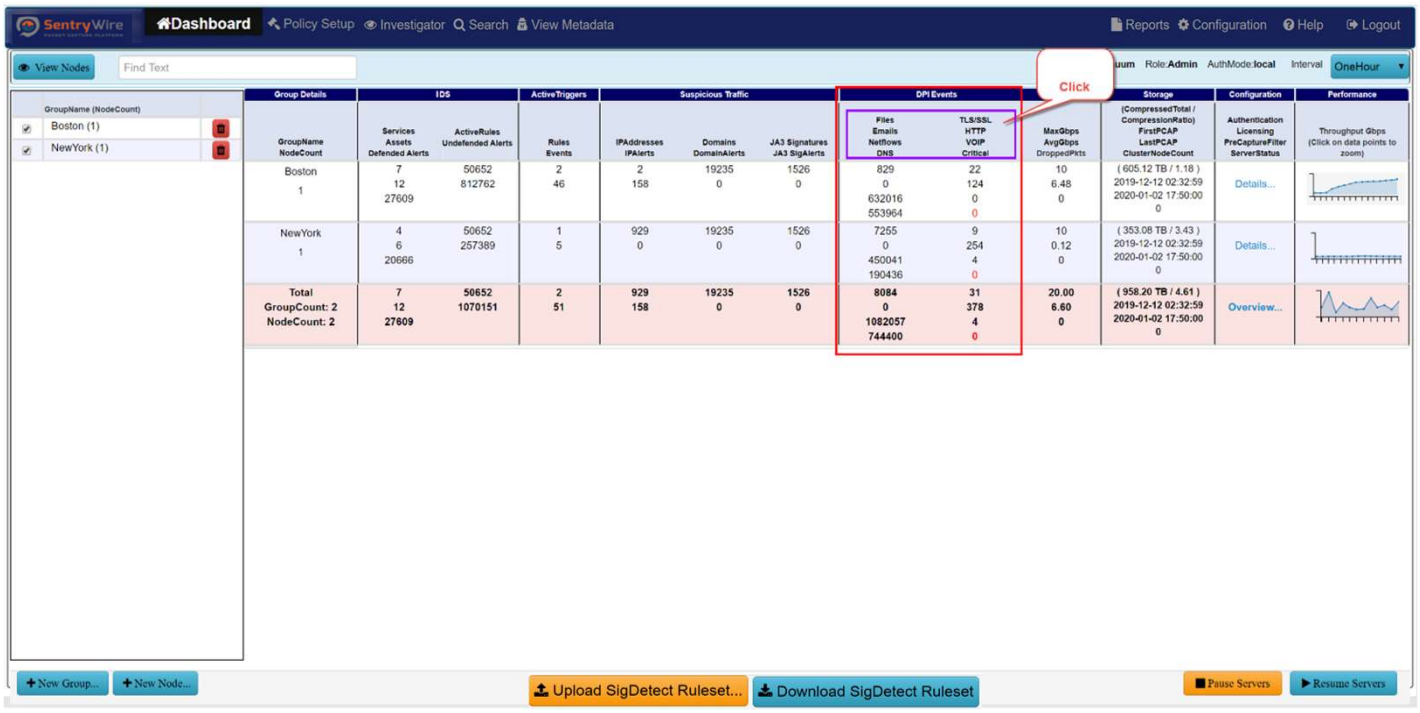


Figure 7-Dashboard DPI Events Column sub-categories

- **First** sub-category shows the counts for Files, Emails, Netflows, and DNS events. Each of these are hyperlinked to pivot to their relevant screens.

- Clicking on “Files” sub-category pivots to View Metadata-> Files screen.
- Clicking on “Emails” sub-category pivots to View Metadata-> Emails screen.
- Clicking on “Netflows” sub-category pivots to View Metadata-> Netflows screen.
- Clicking on “DNS” sub-category pivots to View Metadata-> DNS screen.

- **Second** sub-category shows the counts for TLS/SSL, HTTP, VOIP and Critical events.
  - Critical events counts are displayed in red.
  - Clicking on “TLS/SSL” sub-category pivots to View Metadata-> TLS/SSL screen.
  - Clicking on “HTTP” sub-category pivots to View Metadata-> HTTP screen.
  - Clicking on “VOIP” sub-category pivots to View Metadata-> VOIP screen.
  - Clicking on “Critical events” sub-category pivots to Configuration->System Events screen.

The **Sixth column Throughput** has three data elements:

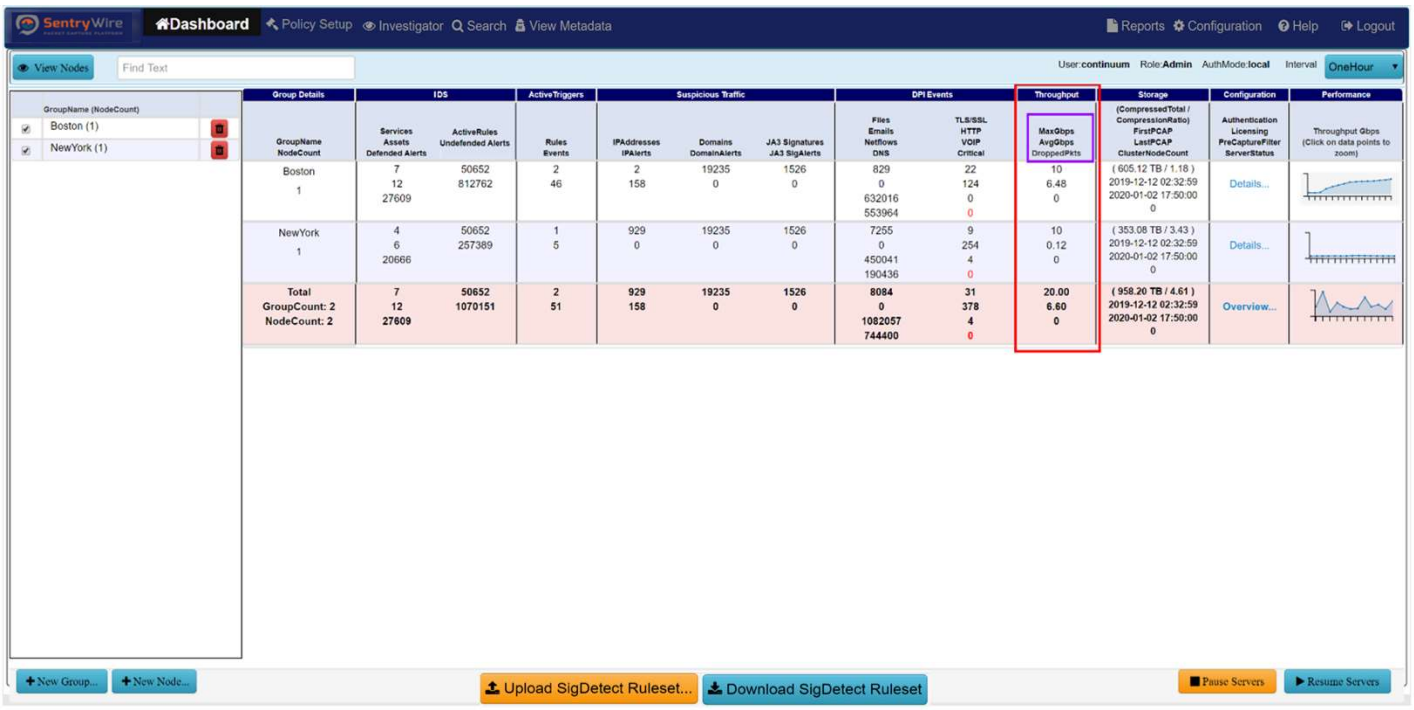
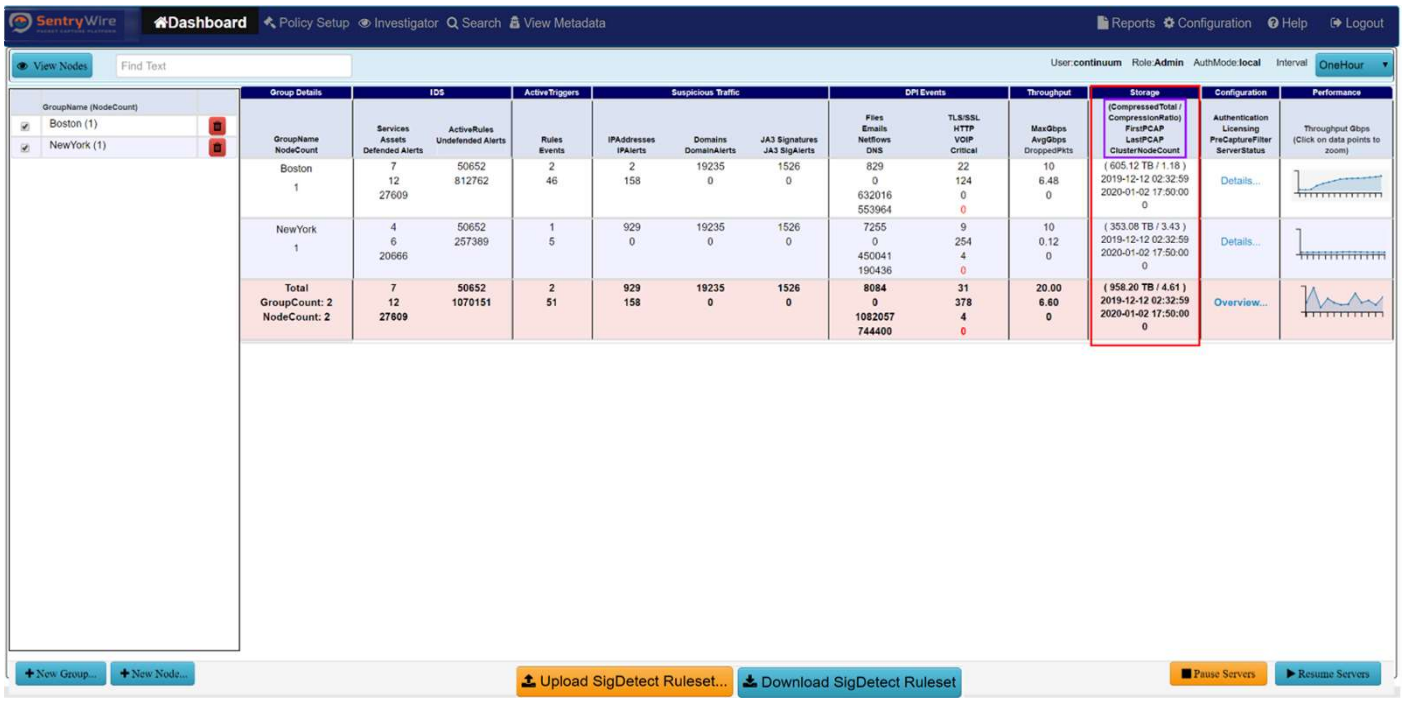


Figure 8-Dashboard Throughput Column

- **MaxGbps**: The maximum throughput of sum of the maximum throughput of the nodes.
- **AvgGbps**: The average throughput of sum of the average throughput of the nodes.
- **Dropped Packets**: The sum of each node's dropped packets of that group.

The **Seventh column Storage** has four data elements:

Figure 9-Dashboard Storage Column



- **CompressedTotal** is the total compressed storage used up by the capture data and **CompressionRatio** is the current compression ratio. (Dividing compressed storage by compression ratio gives the actual storage size.)
- **FirstPCAP** of each group is the earliest First PCAP among all nodes of the group.
- **LastPCAP** of each group is the latest Last PCAP among all nodes of the group. This allows users to see the full duration of data of the group.
- **ClusterNodeCount** shows the sum of all cluster nodes of each node of the group.

The **Eighth column Configuration** provides information about the Authentication, Licensing, PrecaptureFilter and ServerStatus.

- Clicking on "Authentication" sub-category pivots to Configuration-> Authentication screen.
- Clicking on "Licensing" sub-category pivots to Configuration -> Software Management screen.
- Clicking on "PrecaptureFilter" sub-category pivots to Policy Setup-> PrecaptureFilter screen. The entire group information can be viewed by clicking on the Details…." hyperlink for that group.
- Clicking on "Overview…" gives the aggregated information of all selected group.

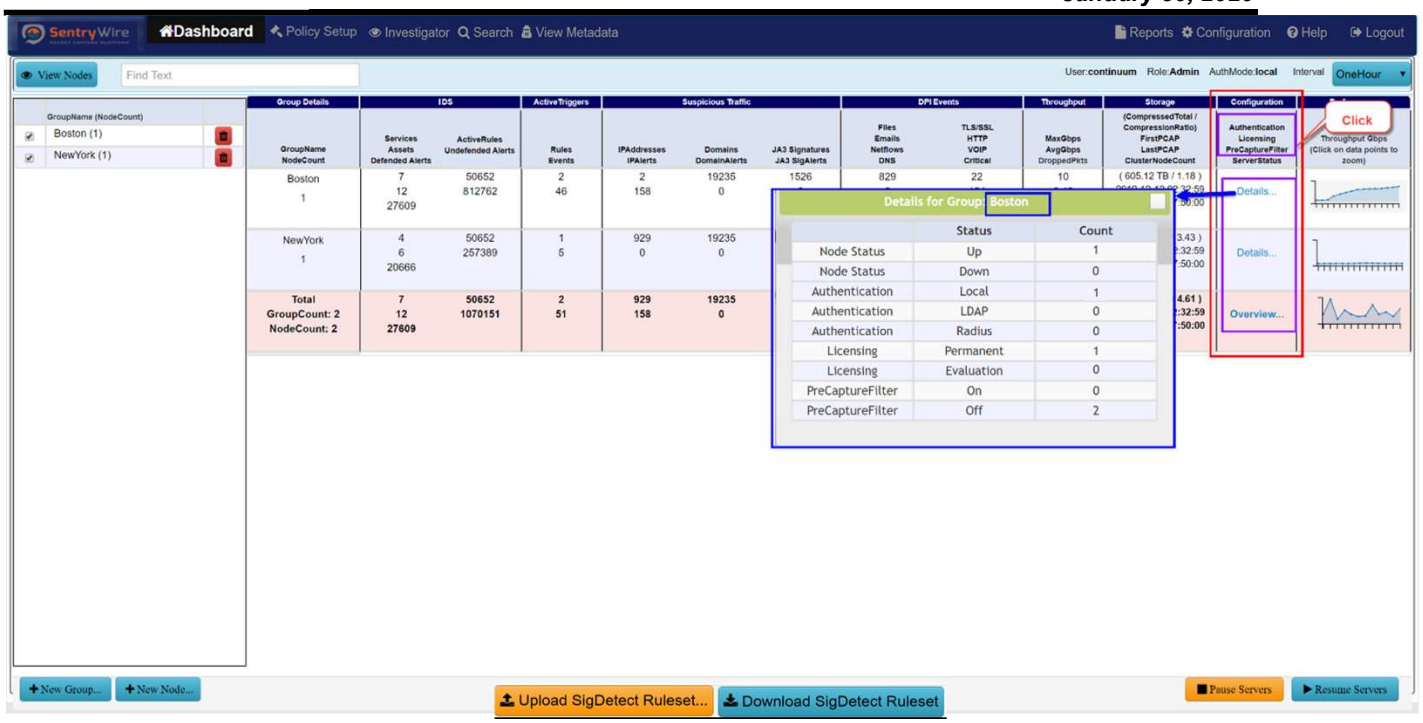


Figure 10-Dashboard Configuration Column

The **Performance Throughput Graph** allows the user to view thumbnail view of each group's aggregated throughput as a graph. Clicking on data points of the thumbnail shows a dialog box with more detailed version of the graph.

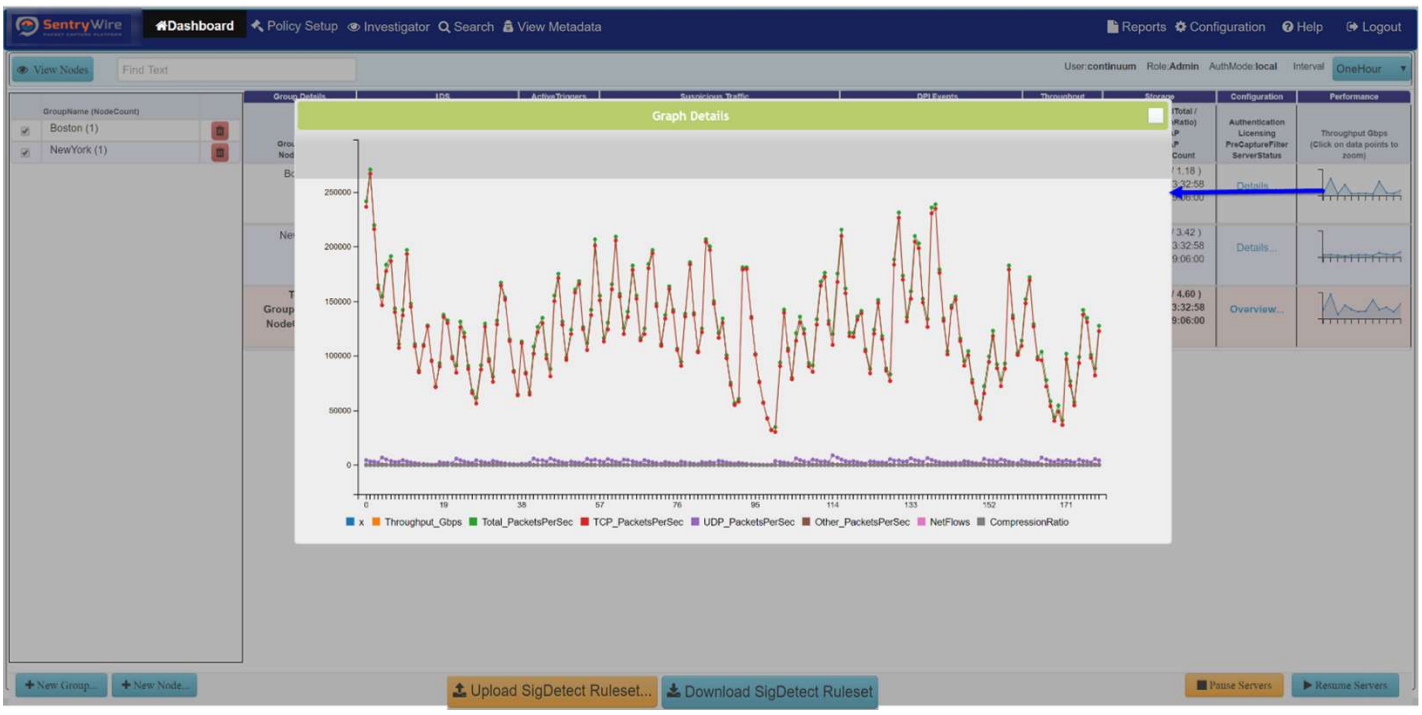


Figure 11-Dashboard Performance Throughput Graph

5.1.1 Understanding the Dashboard- Group View Counts

In Group view the elements that constitute the policy and have same property are listed below:

- IDS.Services
- IDS.Assets
- IDS.Active Rules
- ActiveTriggers.Rules
- SuspiciousTraffic.IPAddresses
- SuspiciousTraffic.Domains
- SuspiciousTraffic.JA3Signatures
- Storage.CompressionRatio

The Policy Counts for these items are the max of the policy counts of all the nodes in a group.

***For example*:** If node1 and node2 belong to group1, and node1 has 5 Defended Services while node 2 has 12 Defended Services, then the group1 count for defended services shows as Max(5,12) = 12.

In Group view the elements that show the additive property are listed below:

- IDS.DefendedAlerts
- IDS.UndefendedAlerts
- ActiveTriggers.Events
- SuspiciousTraffic.IPAlerts
- SuspiciousTraffic.DomainAlerts
- SuspiciousTraffic.JA3SigAlerts
- DPIEvents (Files, Emails, Netflows, DNS, TLS/SSL, HTTP, VOIP, Critical)
- Throughput (MaxGbps, AvgGbps, DroppedPkts)
- Storage.CompressedStorage

The Counts for these Event/Alert items is a summation of all nodes in the group.

For example: If node1 has 2000 Undefended Alerts and node2 has 1400 Undefended Alerts, and node1,node2 belong to group1, then group1's UndefendedAlerts column will be displayed as 2000+1400=3400.

In Group View following elements are handled as described:

- Storage.FirstPCAP/LastPCAP: Group's FirstPCAP is the earliest of the FirstPCAP values of its nodes and the LastPCAP is the latest of the LastPCAP values of its nodes.
- Licensing: Is displayed as count of nodes that are permanent and/or evaluation. To view the license count click on “Details…”.
- Authentication: Is displayed as count of nodes that have local authentication or Radius or LDAP. To view the authentication count click on “Details…”.

- PreCaptureFilter: Is displayed as the number of nodes within the group that have pre-capture filter on and number of nodes that have pre-capture off. To view the pre-capture count click on "Details…".

5.1.2 Add/Delete Federated Groups and Federated Nodes

- **Adding a Federated Group**
  - To add a new group, click on the "+New Group" button on the FM Group View Dashboard. This presents the user with a pop window. Fill in the necessary details and click "Add Group"
  - Once the group is added, user can now add nodes to the newly created group.

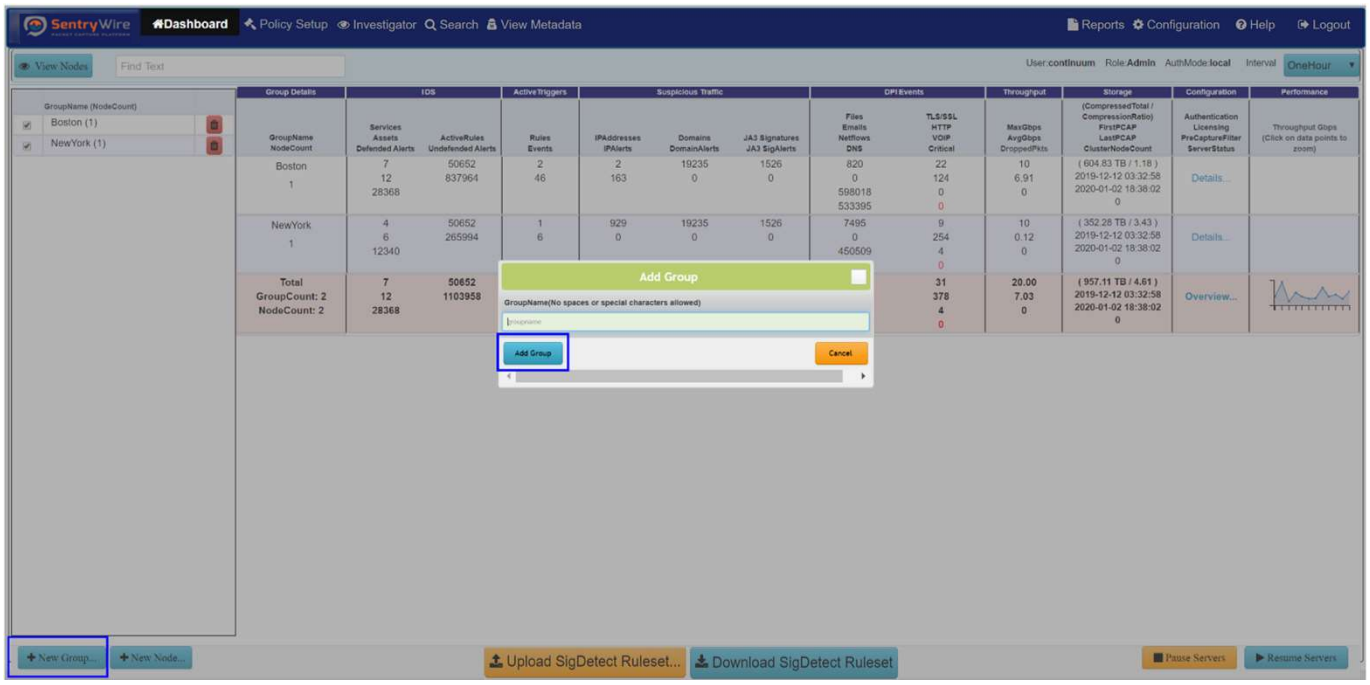


Figure 12-Dashboard Add Federated Group

- **Adding a Federated Node to a Group**
  - To add a new FN to a group, click on "+New Node" button.

***Note**:* You must have at least one group to be able to add a node.

  - Select Group selection drop down and select the desired group.
  - Enter the IPAddress, Username and Password of the node to be added.
  - Click on "Add Node".
  - If the username and password are correct, the node will be added.
  - Once the node is configured, it is available to the user under the desired group.

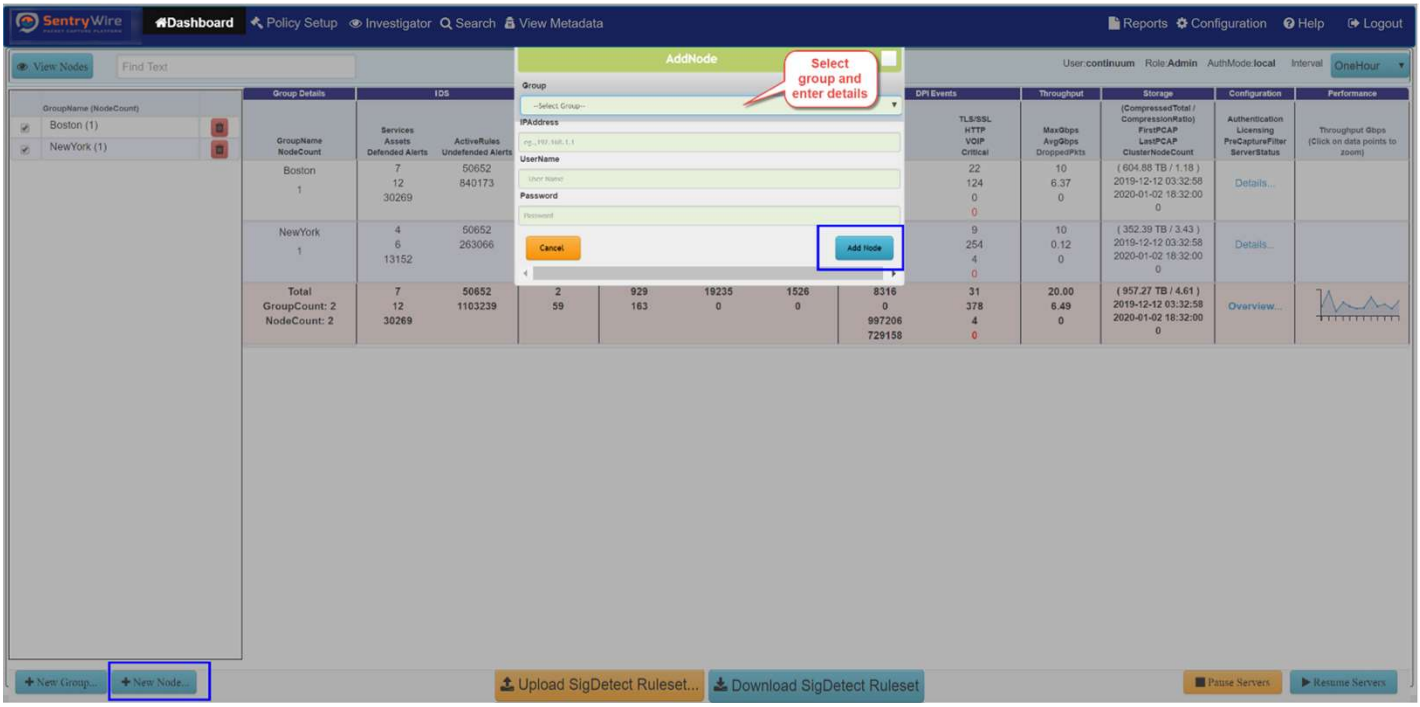


Figure 13-Dashboard Add Federated Node

- **Deleting a Federated Group or Federated Node**
    - To delete a **Group**, simply click on the delete button next to the group name.

Notes:

- A group with a node entry cannot be deleted. All the nodes in the group must be deleted individually.
- This group->node association is symbolic. A node is never affected by removal from a group. Each removed node can then be added to other groups.

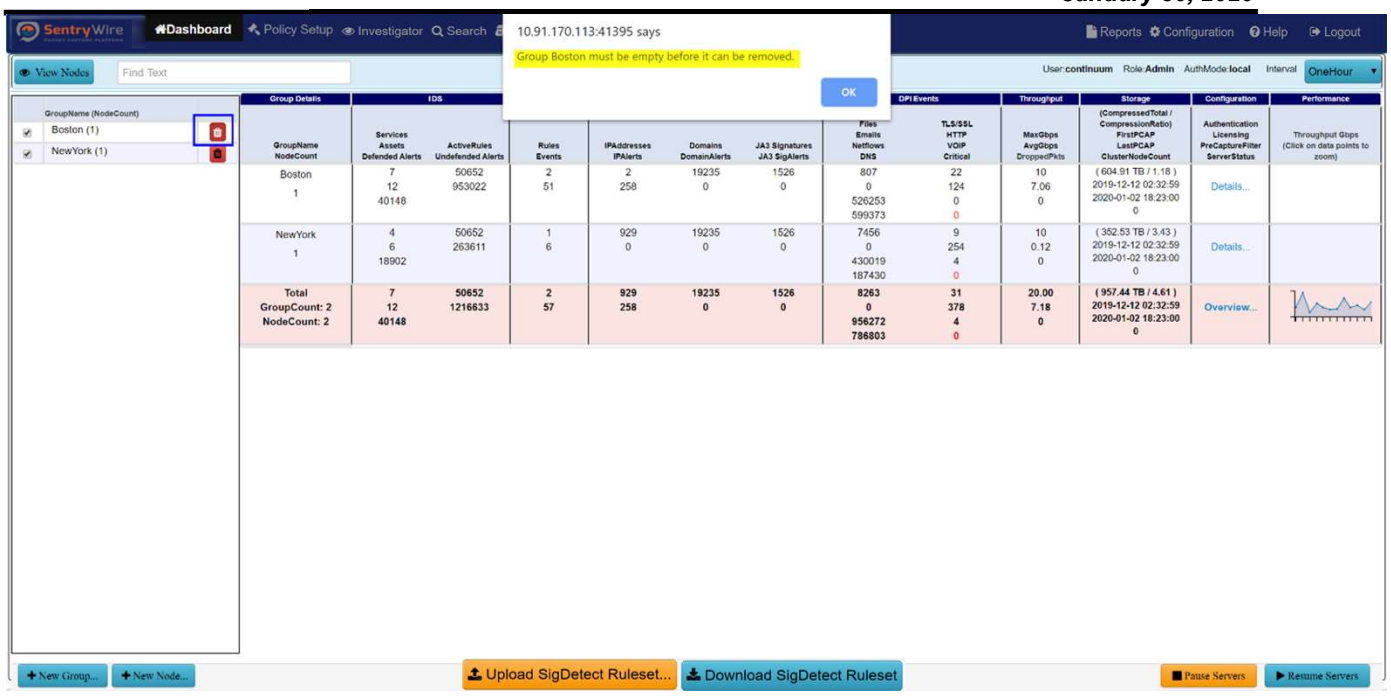


Figure 14-Dashboard Delete a Federated Group or Node Warning

- To delete an existing **Federated Node**, select the group to which the node belongs. Then click on the "**View Nodes**" button at the top. This brings you to the "**Node view**" dashboard. Once in the Node view dashboard, the user can delete the desired node by simply clicking on the delete icon under the action column.
- Once deleted, the Federation cannot monitor the node.

Notes:

- A node can exist only in one group.
- When a group is removed, all the nodes in that group are removed automatically.
- Each removed node can then be added to other groups.

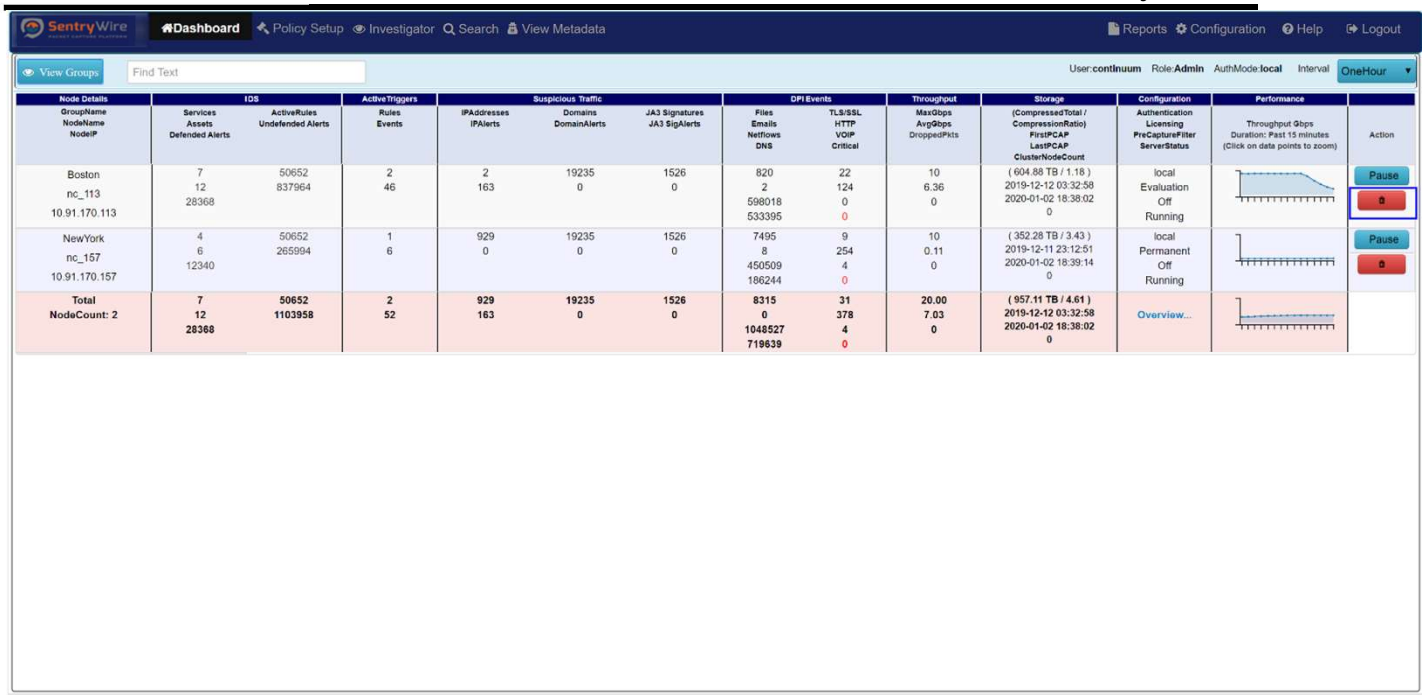


Figure 15-Dashboard Node View

5.2 NODE VIEW

The Node view of the dashboard can be accessed by clicking on the “View Nodes” button. Node View allows users to view node details, pivot to other panels for policy, alerts, events and configuration. Authorized users can remove a node from being monitored and pause/resume individual node's capture server.

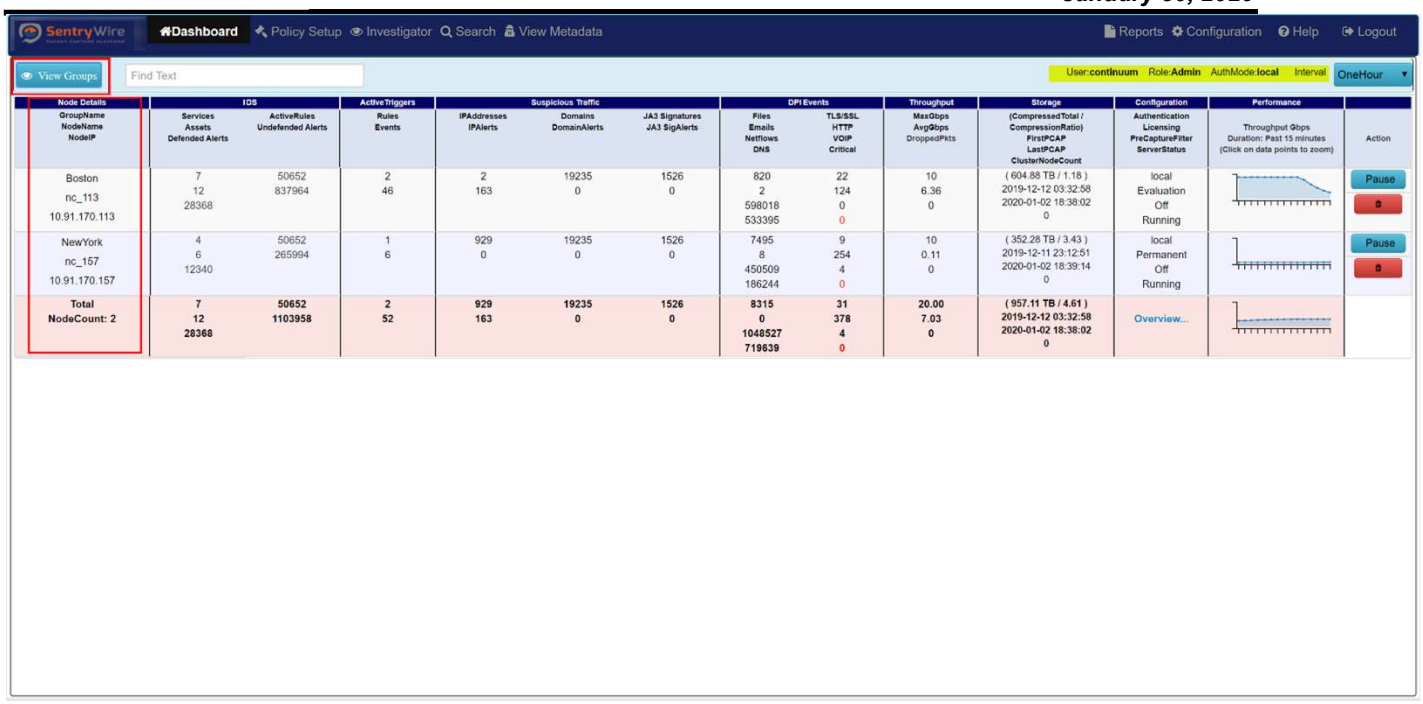


Figure 16-Dashboard Node View Node Details Column

This dashboard displays the following:

- "View Groups" button and Find Text search option. Clicking on "View Group" button switches the dashboard back to the group view where each group's aggregated configuration, alert and storage information is displayed.
- UserName, License status and Authentication mode of the FM.
- Currently selected time interval and relevant data based on the selected option.

***Note**:* Default Interval is "One Hour". Interval drop allows users to change the duration of the data being displayed below.

- The Node view dashboard provides the following information:

The **First column** displays the **Node Details** which includes:

- GroupName, NodeName and NodeIP.

***Notes**:*

- Only selected group's nodes are displayed in the first column.
- If one or more Federated Node servers are down/stopped or unreachable, the dashboard displays the NodeName and NodeIP in red.
- Only action that can be performed for a node that is down is "Delete"

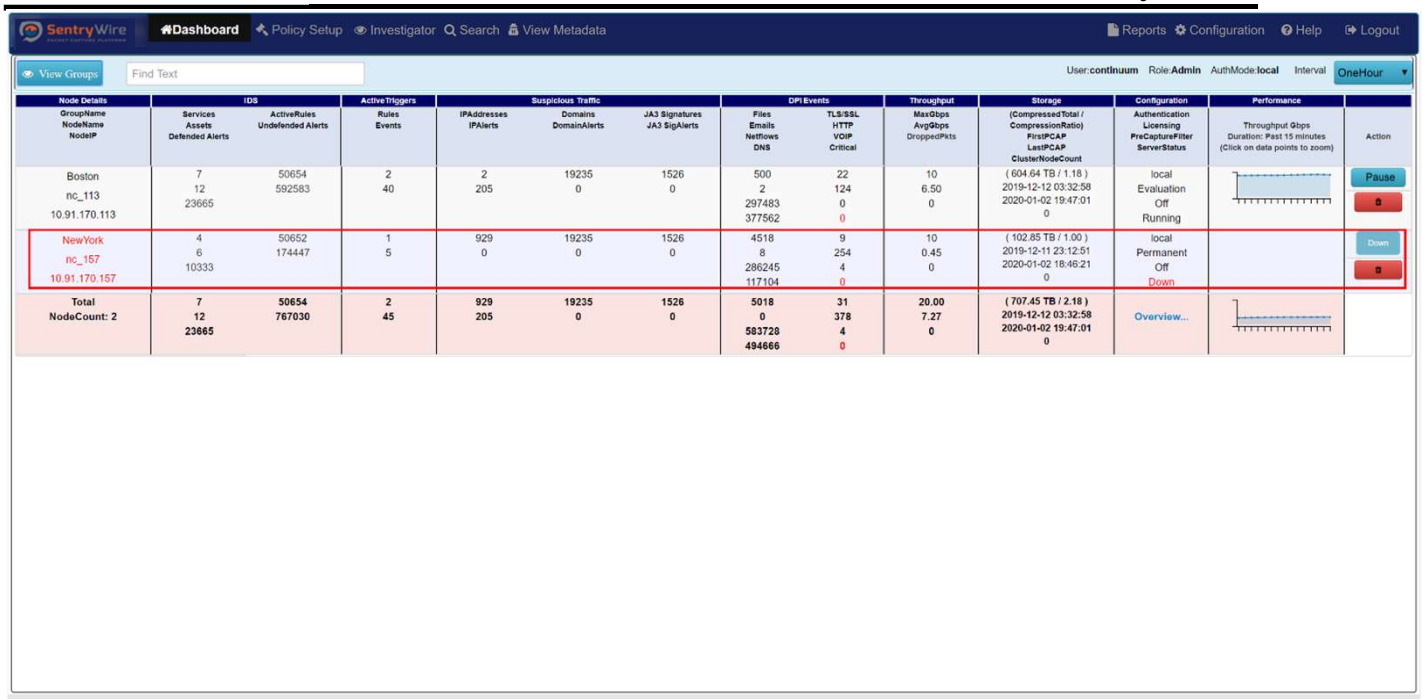


Figure 17-Dashboard Node Details

The **Second column IDS** has 2 subcategories:

- **First** sub-category shows Services, Assets and Defended Alerts. Each of these are hyperlinked to pivot to their relevant screens.

For example:

- Clicking on "Services" sub-category pivots to Policy setup->Defended services screen.
- Clicking on "Assets" sub-category pivots to Policy setup->Defended assets screen.
- Clicking on "Defended Alerts" sub-category pivots to View Metadata->Defended Alerts screen.

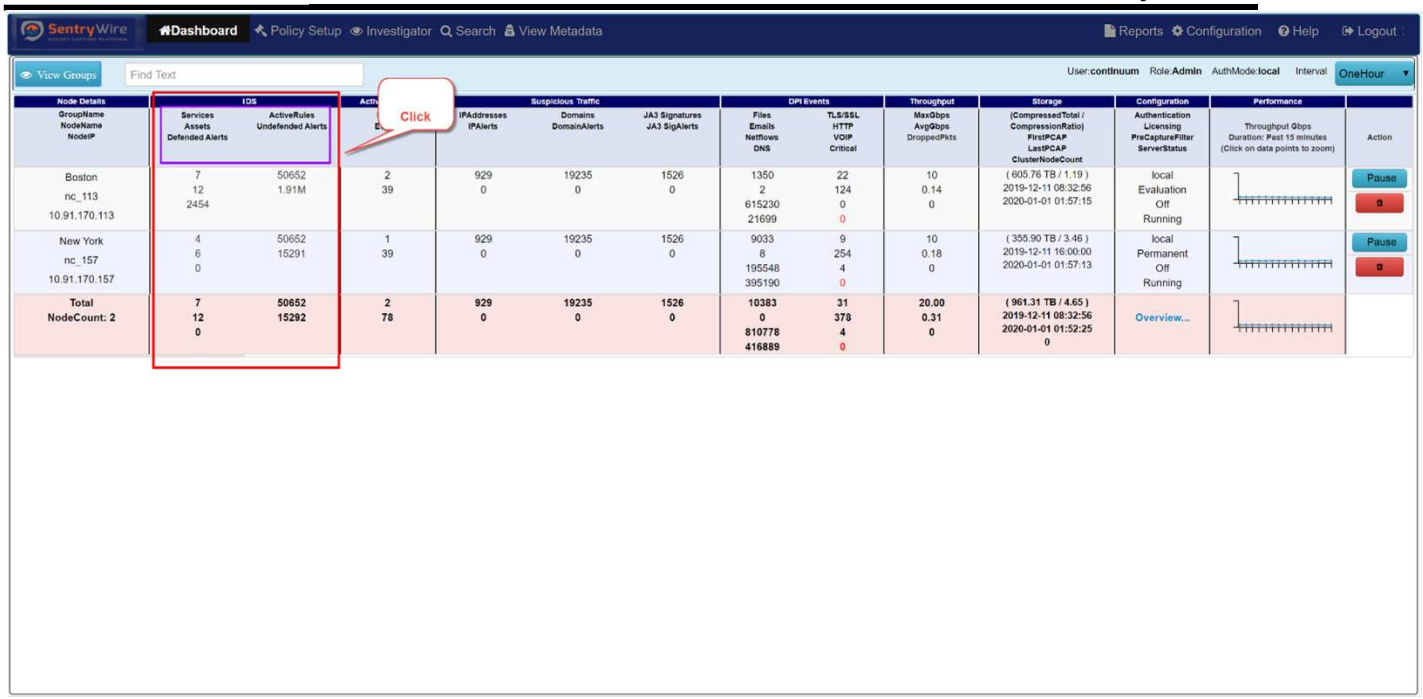


Figure 18-Dashboard Node View IDS Column sub-categories

- **Second** sub-category shows Active Rules and Undefended Alerts. Each of these are hyperlinked to pivot to their relevant screens. Clicking on "Active Rules" sub-category pivots to Policy setup->IDS rule screen. Clicking on "Undefended Alerts" sub-category pivots to View Metadata->Undefended Alerts screen.

Note:

- Total alerts generated is equal to the sum of Defended Alerts and Undefended Alerts.

The **Third column Active Triggers** shows Rules that are defined by users and Events generated as a result of these rules. Clicking on "Rules" pivots to Policy setup->Active Triggers screen. Clicking on "Events" pivots to View Metadata ->Active Triggers tab.

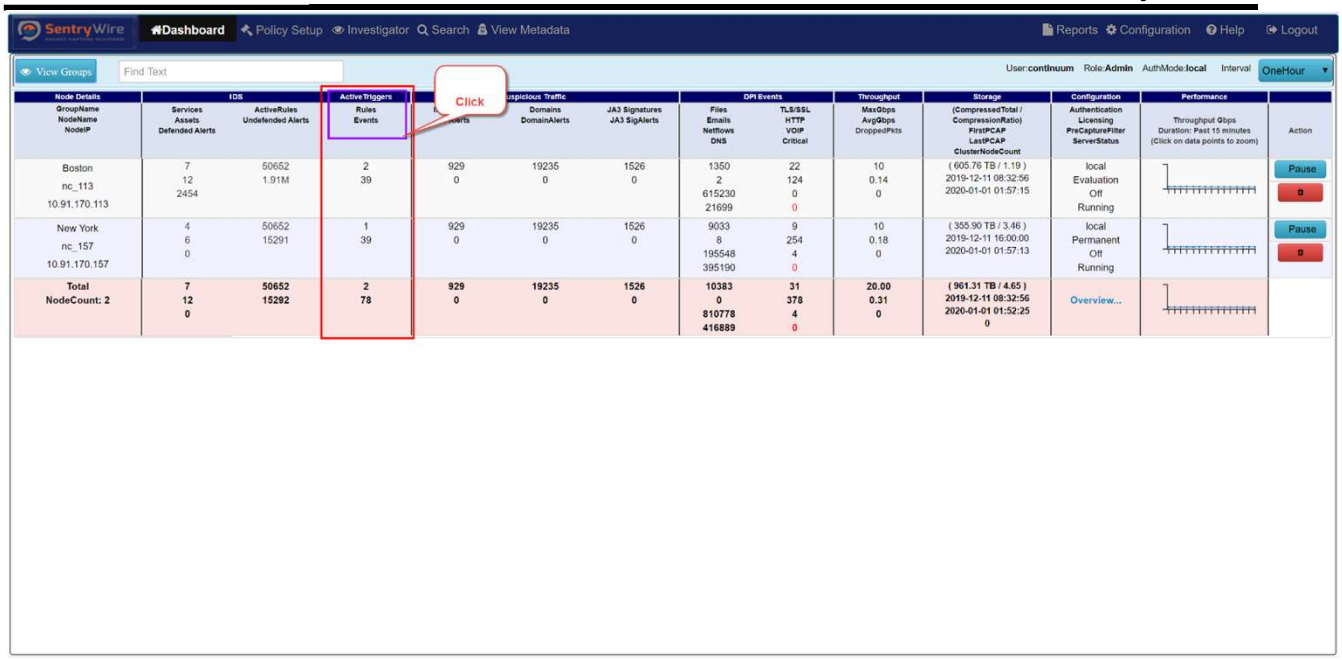


Figure 19-Dashboard Node View Active Triggers Column Rules Events

The **Fourth column Suspicious Traffic** has three sub-categories:

- **First** sub-category shows the count of Suspicious IP Addresses uploaded by the user for that node, and the IP Alerts generated due to the uploaded IP Addresses. Each of these are hyperlinked to pivot to their relevant screens. Clicking on “Ip Addresses” sub-category pivots to Policy setup->Augmentation screen. Clicking on “IPAlerts” sub-category pivots to View Metadata->SuspIPAlerts screen.

- **Second** sub-category shows the count of Suspicious Domains uploaded by the user for the node, and the Domain Alerts generated due to the uploaded Domains. Clicking on “Domains” sub-category pivots to Policy setup->Augmentation screen. Clicking on “DomainAlerts” sub-category pivots to View Metadata->SuspDomains screen.

- **Third** sub-category shows the count of Suspicious (JA3) signatures uploaded by the user for that group, and the Signature Alerts generated due to the uploaded Signatures. Clicking on “JA3 Signatures” sub-category pivots to Policy setup->Augmentation screen. Clicking on “JA3SigAlerts” sub-category pivots to View Metadata-> SuspSig(JA3)Alerts screen.

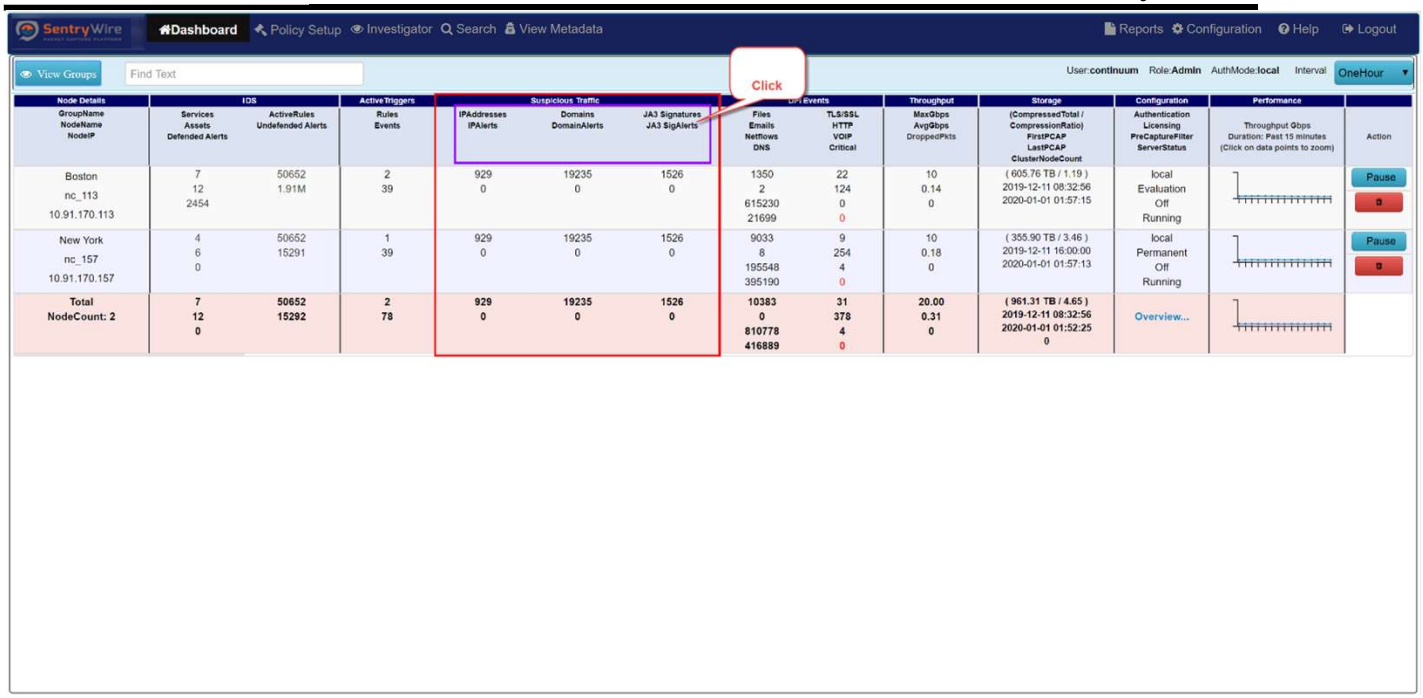


Figure 20-Dashboard Node View Suspicious Traffic Column sub-categories

The **Fifth column DPI Events** shows events generated by the DPI engine running on each node. It has two sub-categories:

- First sub-category shows the counts for Files, Emails, Netflows, and DNS events. Each of these are hyperlinked to pivot to their relevant screens. Clicking on “Files” sub-category pivots to View Metadata-> Files screen. Clicking on “Emails” sub-category pivots to View Metadata-> Emails screen. Clicking on “Netflows” sub-category pivots to View Metadata-> Netflows screen. Clicking on “DNS” sub-category pivots to View Metadata-> DNS screen.
- Second sub-category shows the counts for TLS/SSL, HTTP, VOIP and Critical events. Critical events counts are displayed in red. Clicking on “TLS/SSL” sub-category pivots to View Metadata-> TLS/SSL screen. Clicking on “HTTP” sub-category pivots to View Metadata-> HTTP screen. Clicking on “VOIP” sub-category pivots to View Metadata-> VOIP screen. Clicking on “Critical events” sub-category pivots to Configuration->System Events screen.

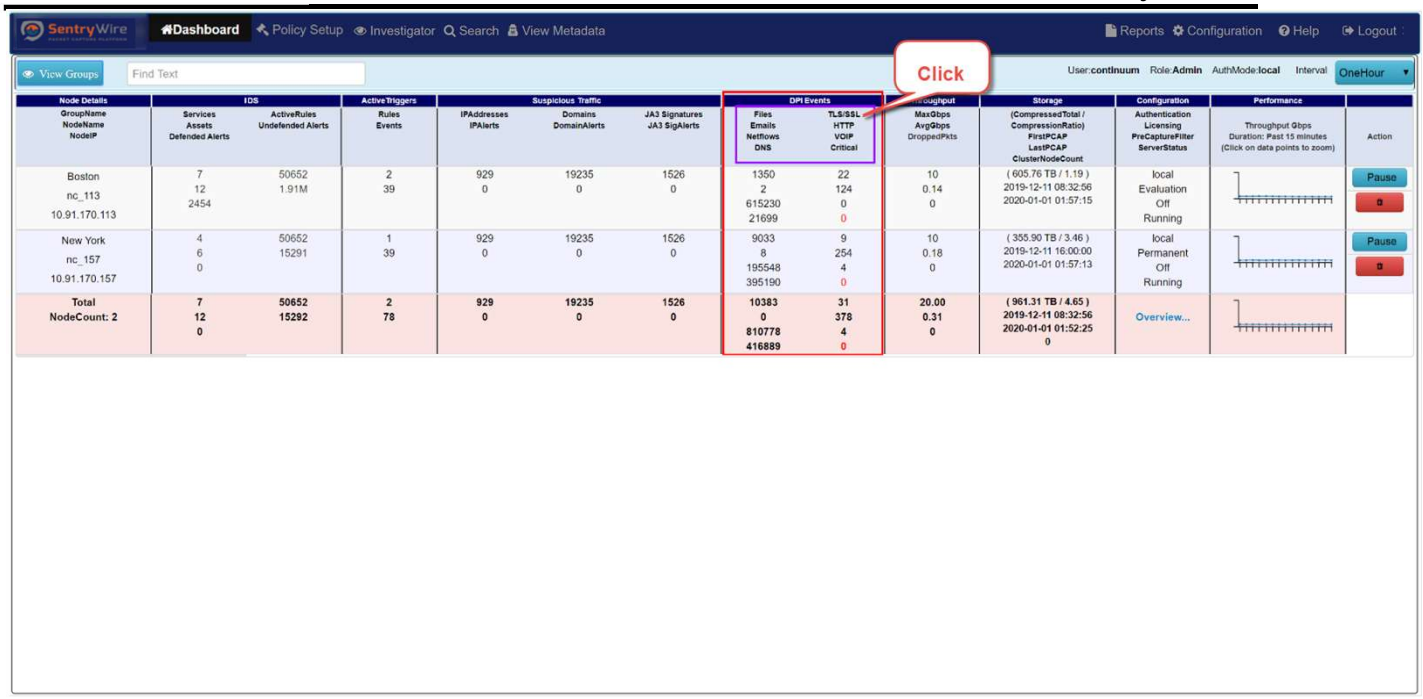


Figure 21-Dashboard DPI Events Column sub-categories

The Sixth column **Throughput** has three data elements:

- MaxGbps: The maximum throughput of each node.
- AvgGbps: The average throughput of each node.
- Dropped Packets: The number of packets dropped packets of that node.

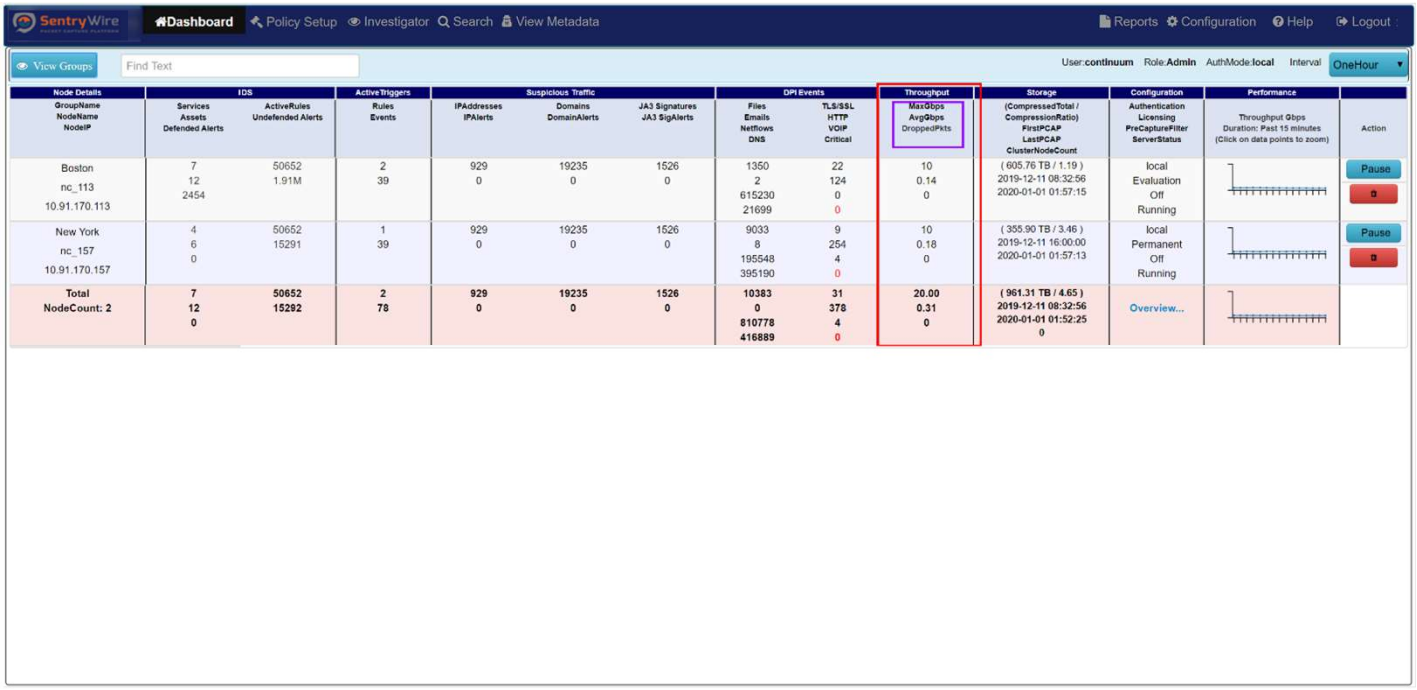


Figure 22-Dashboard Node View Throughput Column

The Seventh column Storage has four data elements:

- CompressedTotal is the total compressed storage used up by the capture data and CompressionRatio is the current compression ratio. (Dividing compressed storage by compression ratio gives the actual storage size.)
- FirstPCAP of each node. This value changes every time oldest capture files are removed to make space for the new capture files.LastPCAP of each node is the time when the latest PCAP has been stored. This allows users to see the full duration of data of the node.
- ClusterNodeCount shows the count of cluster nodes attached to the master node.

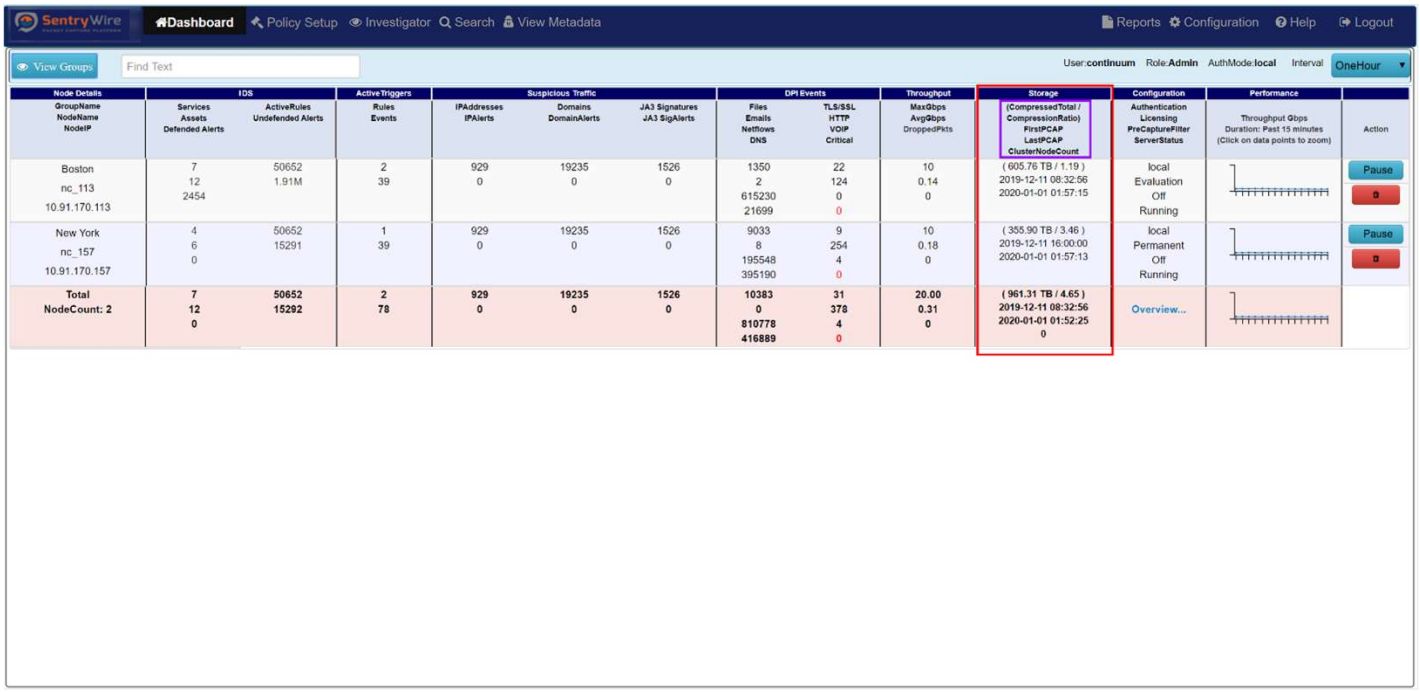


Figure 23-Dashboard Storage Column

The Eighth column Configuration provides information about the Authentication, Licensing, PrecaptureFilter and ServerStatus of the node.

- Clicking on “Authentication” sub-category pivots to Configuration-> Authentication screen.
- Clicking on “Licensing” sub-category pivots to Configuration -> Software Management screen.
- Clicking on “PrecaptureFilter” sub-category pivots to Policy Setup-> PrecaptureFilter screen. The aggregated configuration of all nodes in the group can be viewed by clicking on the Overview….” hyperlink.

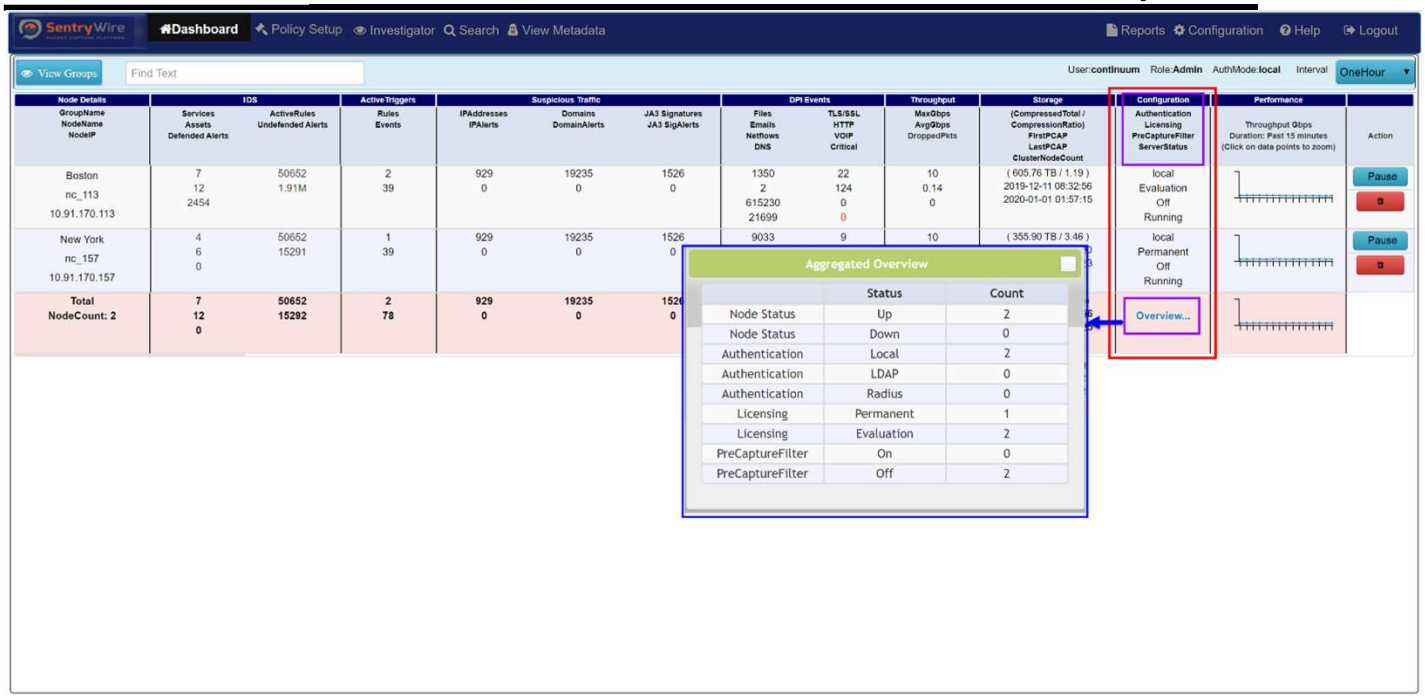


Figure 24-Dashboard Configuration Column Aggregated Overview details

The **Performance Throughput Graph** allows the user to view thumbnail view of each node's throughput. Clicking on data points of the thumbnail shows a dialog box with more detailed version of the graph.

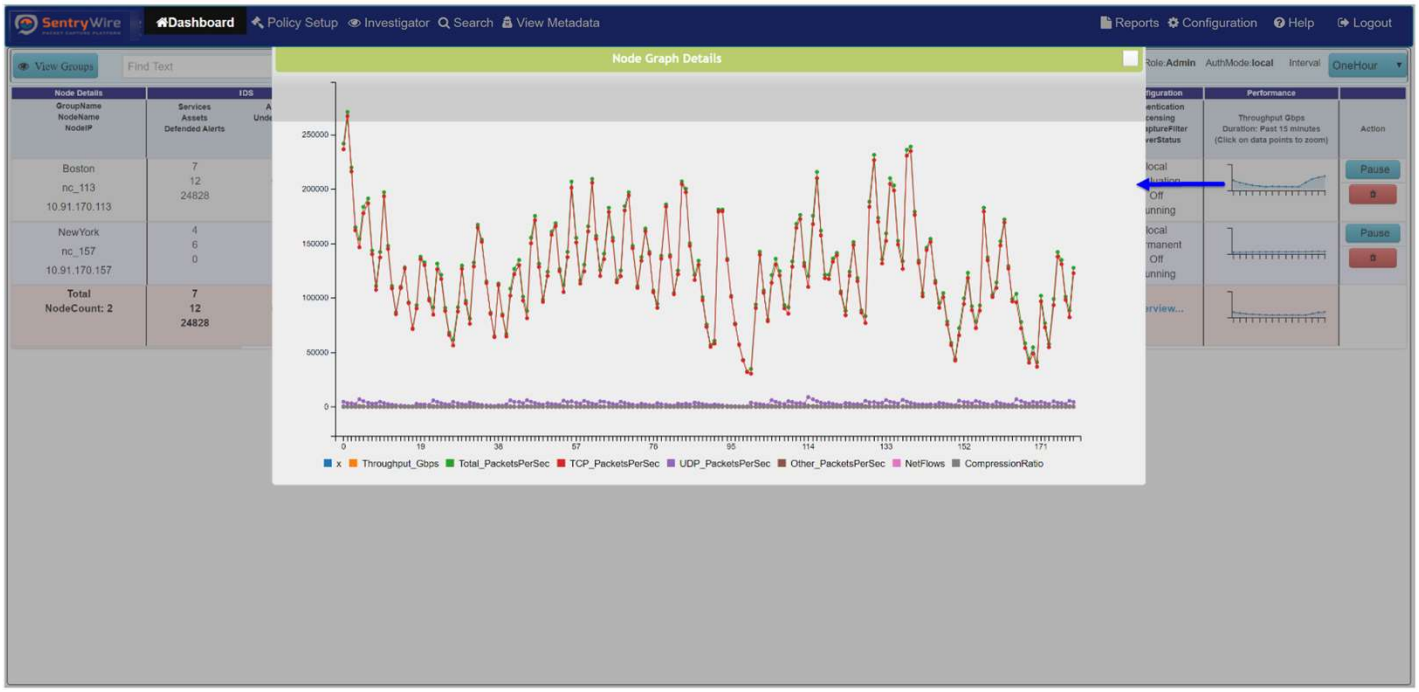


Figure 25-Dashboard Node View Performance Throughput Graph

The **Action** column has the Pause/Resume button and delete button. User can pause or resume the capture server of an individual node by clicking on the Pause/Resume button. Clicking on the delete button deletes the node from the associated group.

Note:

- The node→group association is symbolic. A node is never affected by removal from a group. The deleted node can be added to a different node or re-added to the same group if desired.

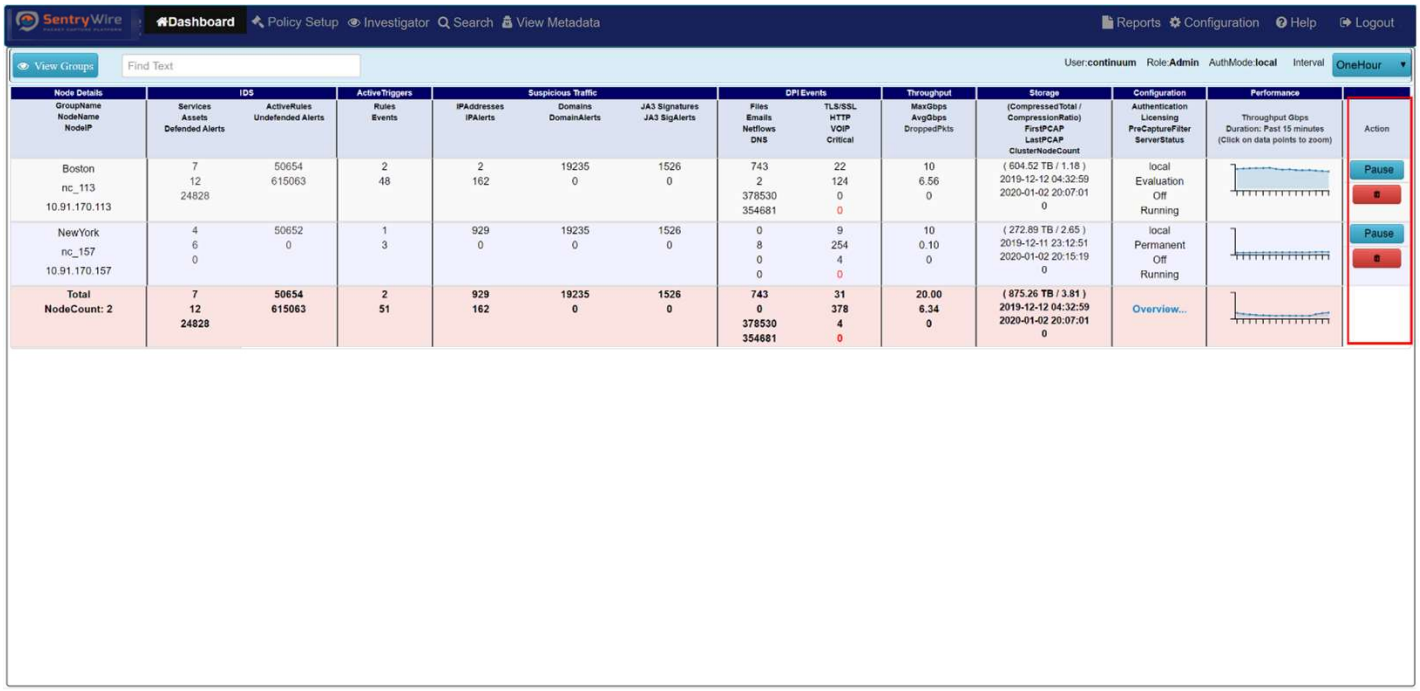
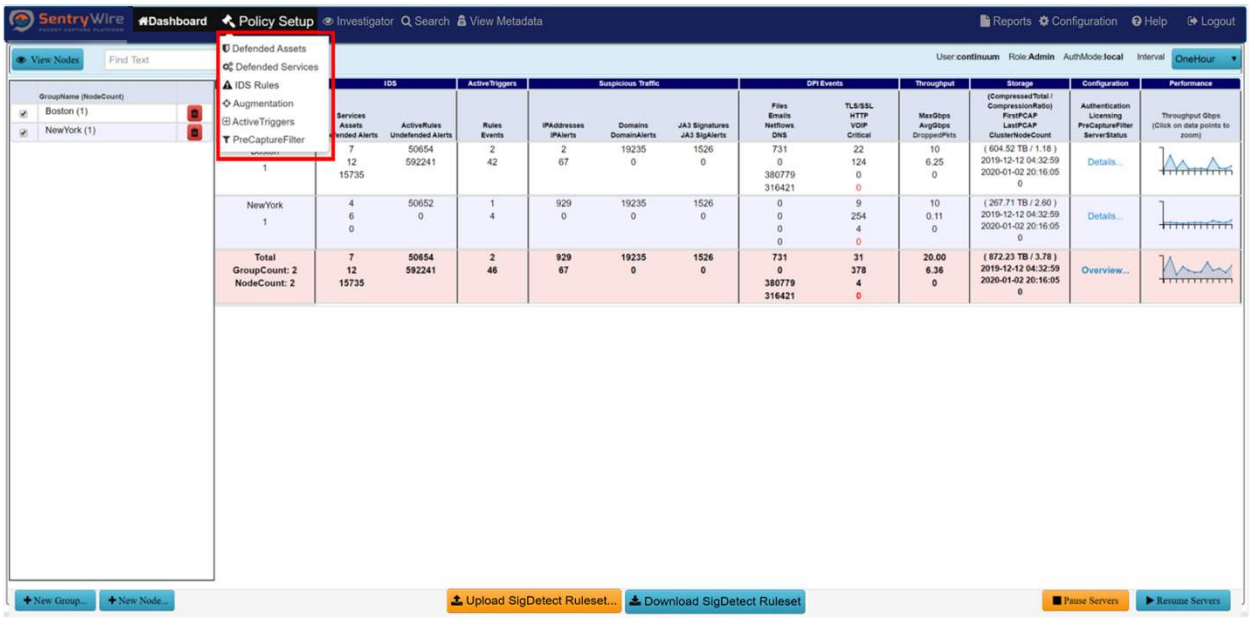


Figure 26-Dashboard Node View Action Column

6 POLICY SETUP TOOL

The policy setup tab allows the user to upload and update a category of policies for all the federated nodes in a group. The sub-menu items are as follows:

- Defended Assets – Trusted Assets defined by IP address.
- Defended Services – Defended Services defined port, priority, and description.
- IDS Rules – Intrusion Detection System Rules.
- ThreatIPs – Unsafe IPs that generate an alert.
- Active Triggers – Generate an alert based on a specific event.
- PreCapture Filter – Filters network traffic before writing it to disk.



6.1 DEFENDED ASSETS

Assets are registers of IP addresses that are approved or recognized and considered to be safe within the network traffic. Since assets are considered as a reliable resource, a low priority alert is generated, and no further action is taken. Assets can be defined based on two categories.

- **Critical IPs** - These IPs represent critical infrastructure of an organization.
- **Trusted IPs** – These IPs represent hosts that are part of an organization or its partners. They are well-known and their state/purpose well-understood.

This application allows the user to create a user-defined list of Critical IPs /Trusted IPs and upload/apply them for alert monitoring.

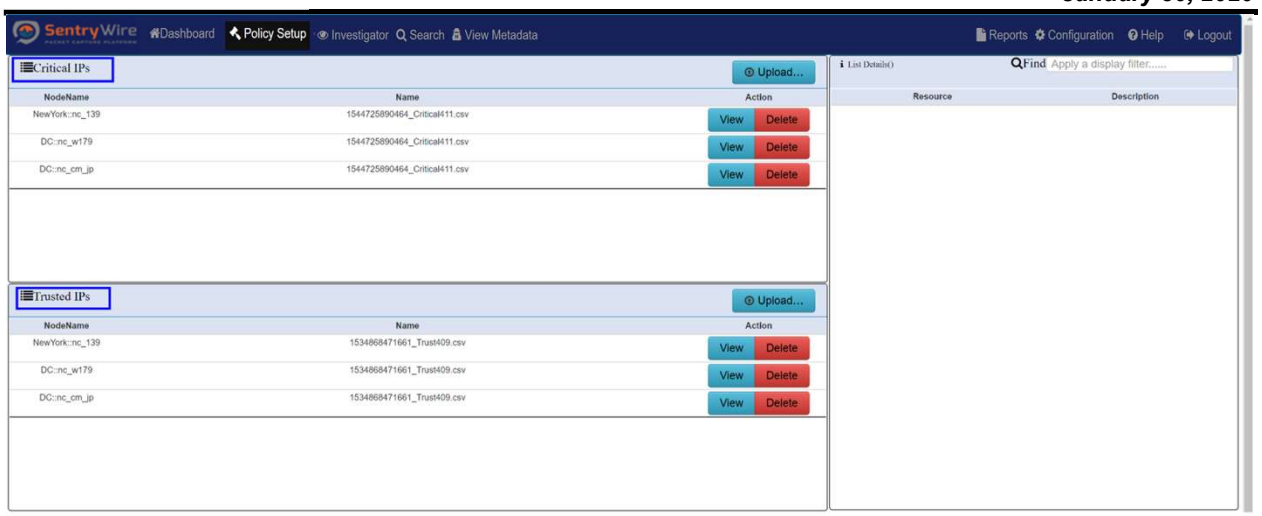


Figure 27-Policy Setup Overview

6.1.1 User Defined Assets File Format

Users can define a list of assets in a **csv** file as per the format below:

- **First column** of each row should state an IP address (resource)
- **Second column** (**optional**) of each row should describe the resource in the first column. This is optional but generally a good practice for easy reference.

Example of a CriticalIPs csv file:

192.1.1.1, System1

10.1.1.2

1.2.3.4, System2

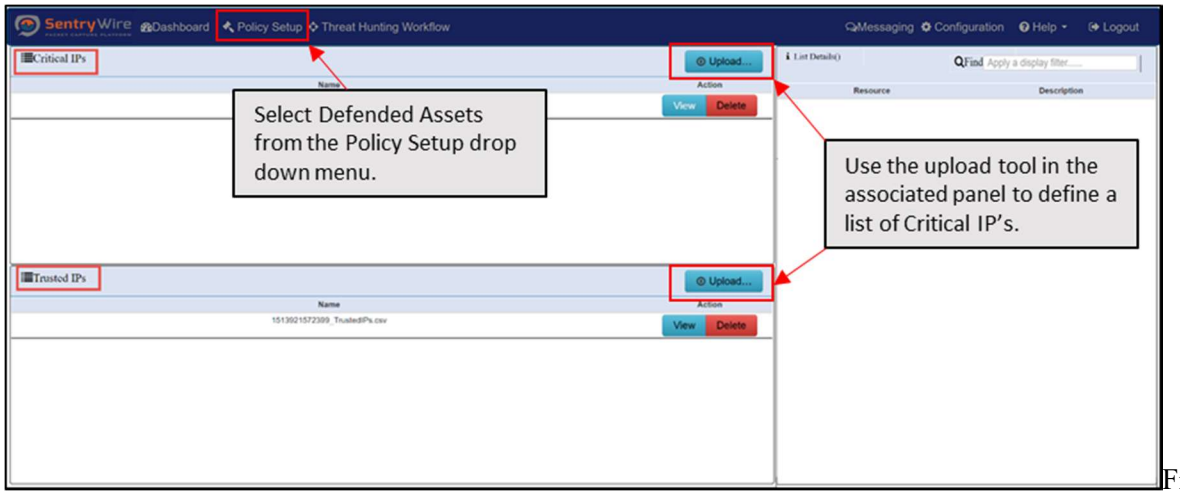


Figure 28-Policy Setup Upload

6.1.2 Upload User Defined Assets File

- Create a <Filename>.csv file on your local system.
- Click on Upload button.
- Select file from the local system to be uploaded.

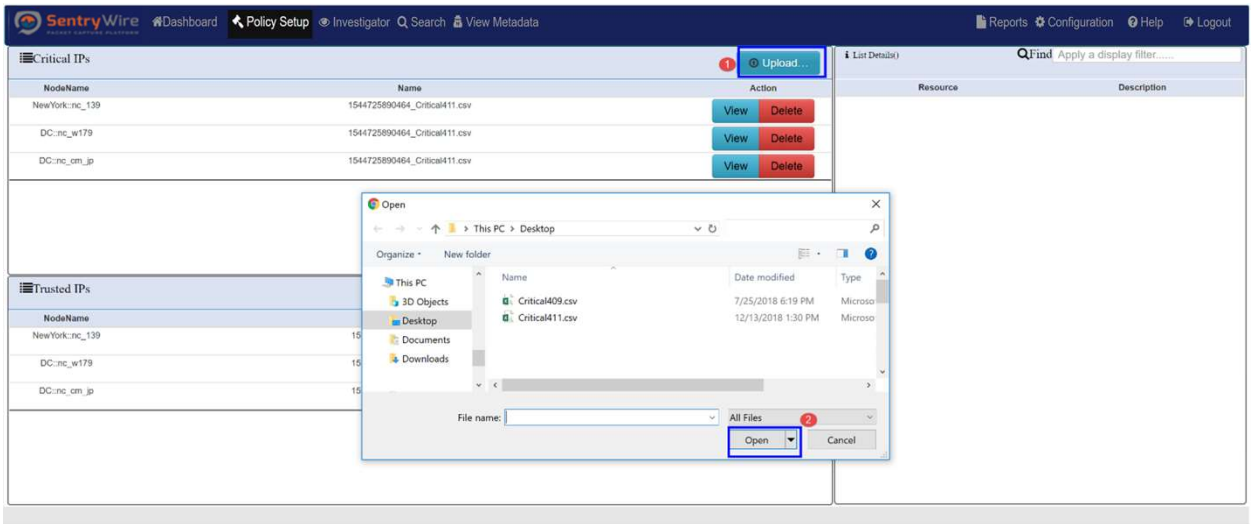


Figure 29-Policy Setup Upload User Defined Assets

- If the file contents are valid, the server adds the file to the list and prepends a timestamp to the filename.
- When an alert is generated due to a rule, the alert is displayed in Threat Hunting Workflow → IoC Manager → Defended Alerts tab, if the alert's source or destination IP address is a defended asset **AND** the alert's source or destination port is a defended service.
- When an alert is generated due to a rule, the alert is displayed in Threat Hunting Workflow→IoC Manager → Undefended Alerts tab if the alert's source or destination IP address is **NOT** a defended asset **OR** the alert's source or destination port is **NOT** a defended service.

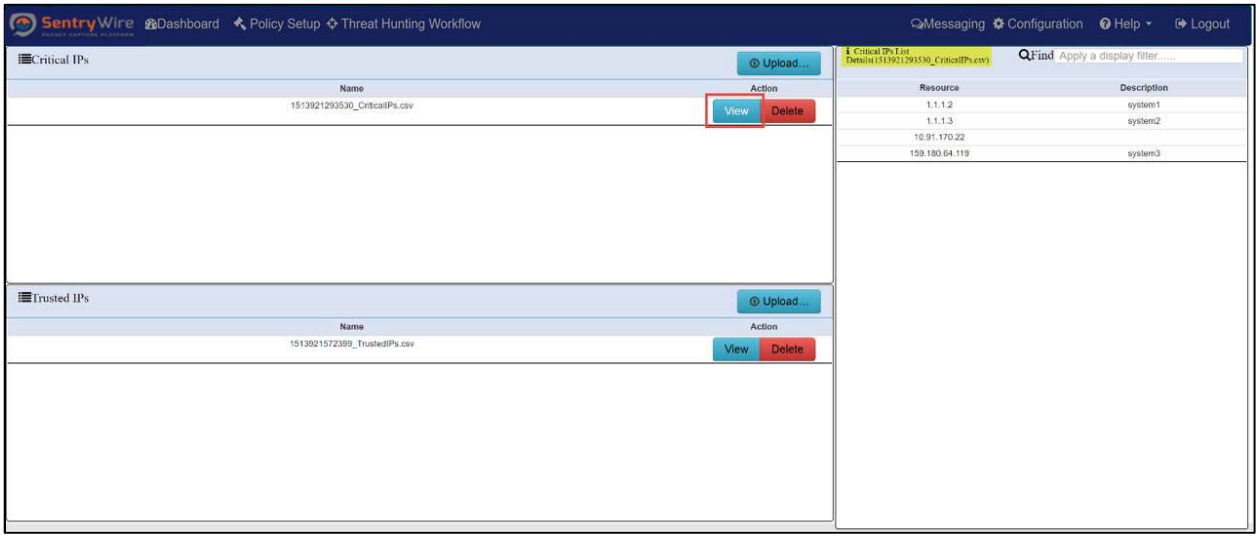


Figure 30 - Policy Setup View User Defined Assets

- To view the contents of the file uploaded simply click view button next to the file.
- To do a text lookup simply type in the desired string in the Find textbox.

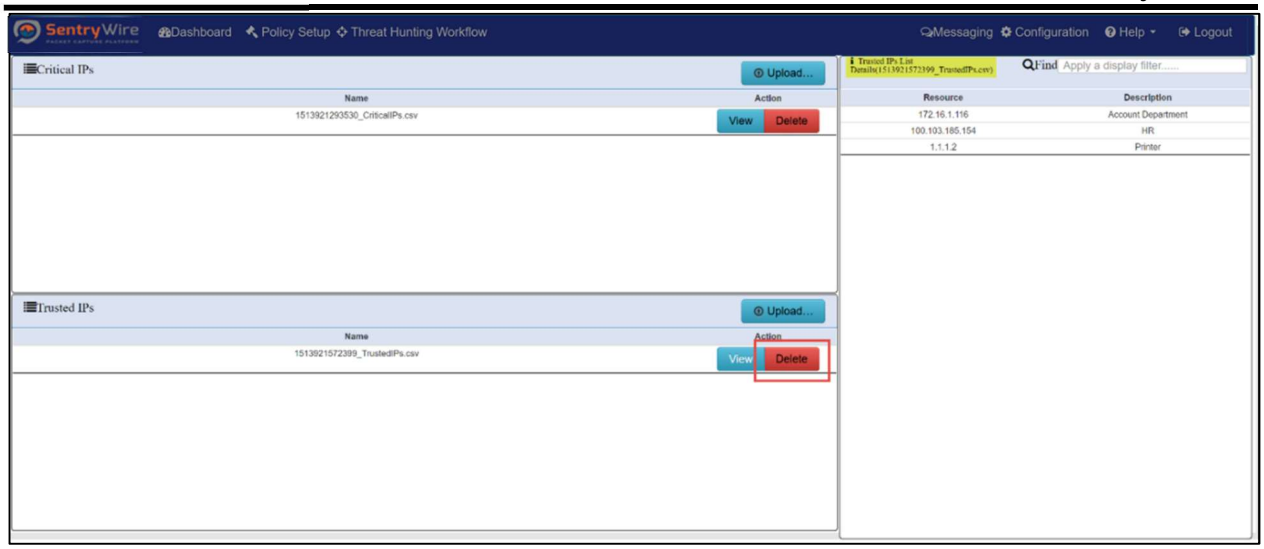


Figure 31 - Policy Setup Delete Critical/Trusted IP List

- To delete an active Critical/TrustedIP list, click the delete button. Once deleted, the resources contained in the list are no longer active.

***Note**: A guest user cannot Upload/Delete CriticalIPs or TrustedIPs.*

6.2 DEFENDED SERVICES

This tool is used to define the list of services that are defended. There are four types of defended services discussed in this section:

- Predefined Unmapped Services
- Activated Defended Services
- Defended Services
- Unmapped Services

6.2.1 Predefined Unmapped Services

These are list of frequently used service ports included with the application. These can be activated by clicking on the activate button. Once activated, an alert is triggered with defended asset and a defended service as part of its 5-tuple. This alert is displayed in Threat Hunting Workflow → IoC Manager → Defended Alerts tab.

***Note**: When an alert is triggered with either a defended asset or a defended service or neither, the alert is displayed in Threat Hunting Workflow → IoC Manager → Undefended Alerts tab.*

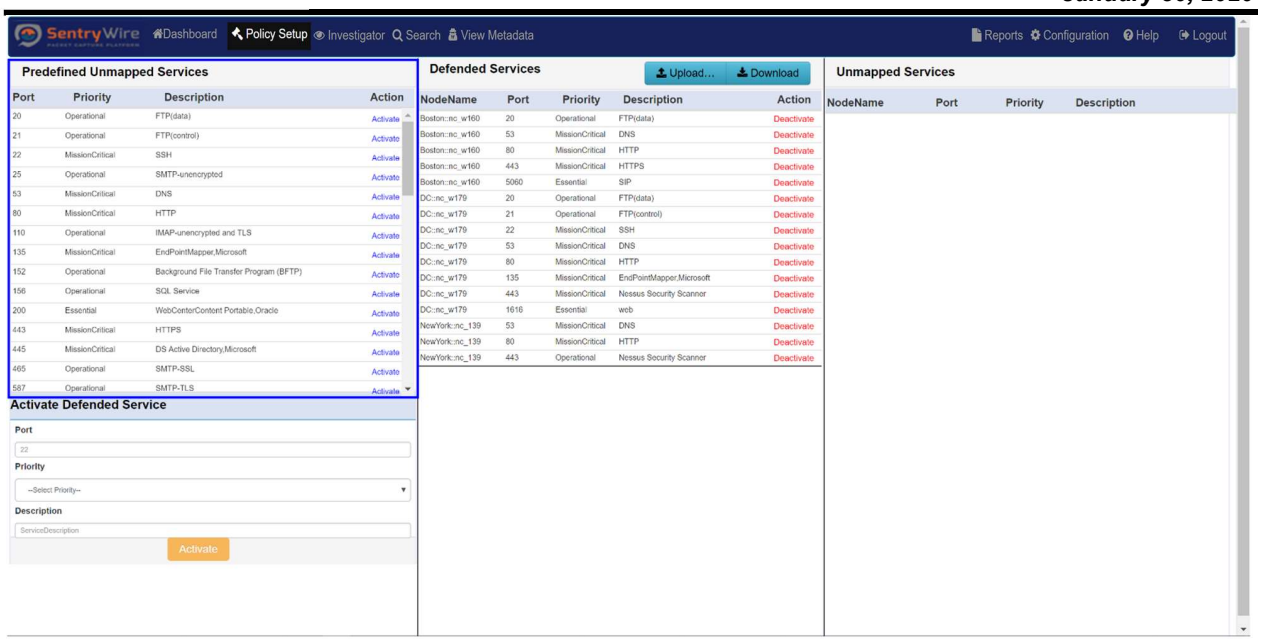


Figure 32 – Policy Setup Predefined Unmapped Services

6.2.2 Activate Defended Services

Besides a predefined list, the application also allows the user to create/activate their own defended services by entering the port number, priority and description. Once activated these appear under the Defended Services column as activated.

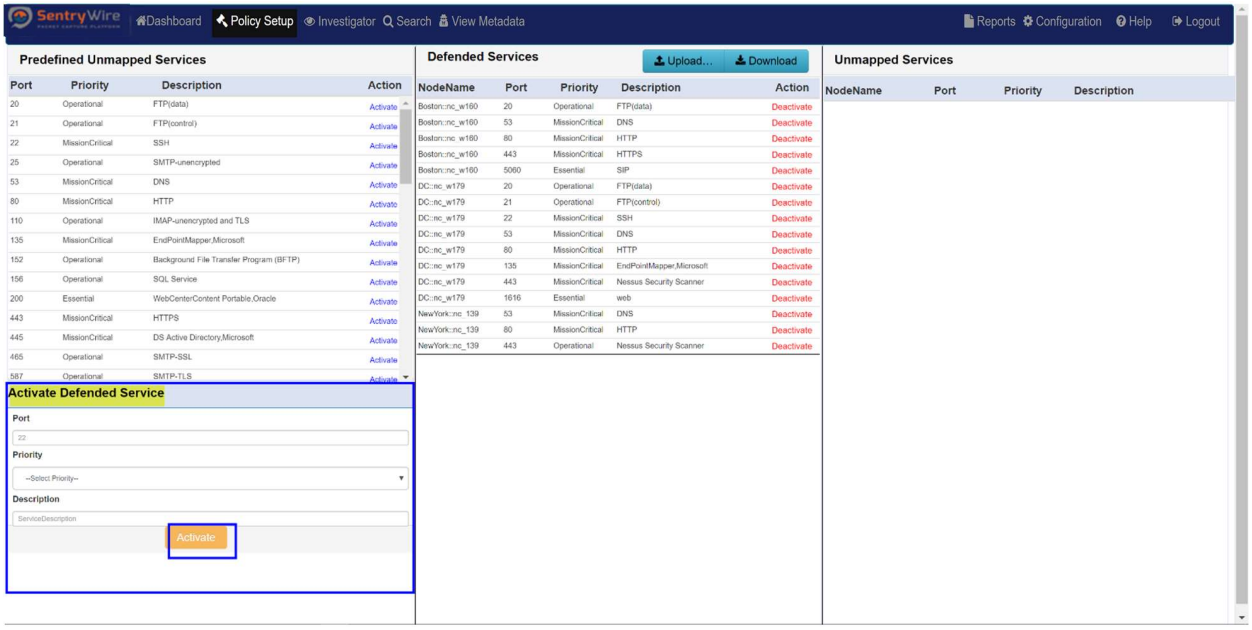


Figure 33 – Policy Setup Activate Defended Services

6.2.3 Defended Services

This panel displays all the active defended service ports. These defended services are also displayed in the dashboard defended services graph if there is a match for defended IP and defended port. Whenever an alert is triggered with defended asset and a defended service as part of its 5-tuple it is displayed in Threat Hunting Workflow → IoC Manager → Defended Alerts tab.

***Note**: When an alert is triggered with either a defended asset or a defended service or neither, the alert is displayed in Threat Hunting Workflow → IoC Manager → Undefended Alerts tab.*

- Clicking on upload allows the user to upload a csv file with multiple service ports.
    - File Format must be <port number>, <Priority>, <Description>

***Note**:* The Priority is case sensitive. There are 3 priority namely: Mission Critical, Operational and Essential.

Clicking on Download allows the user to download all activated service ports.

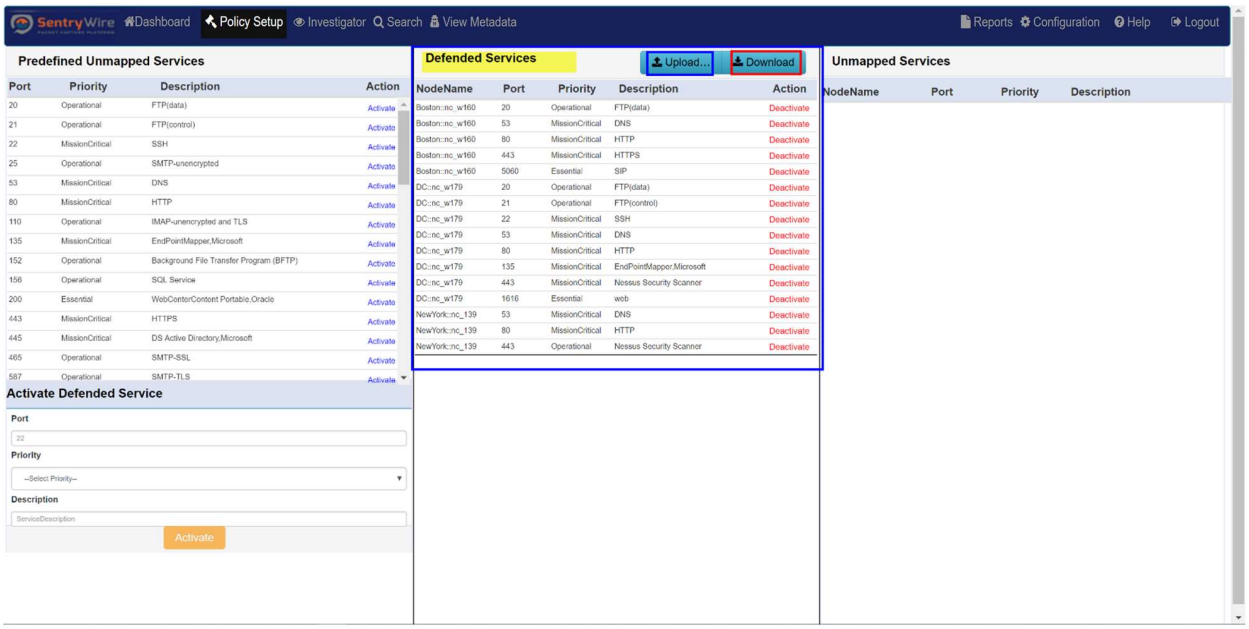


Figure 34 – Policy Setup Defended Services

6.2.4 Unmapped Services

This panel displays any services that were once active. These services can be reactivated by clicking activate or deleted by clicking delete button respectively.

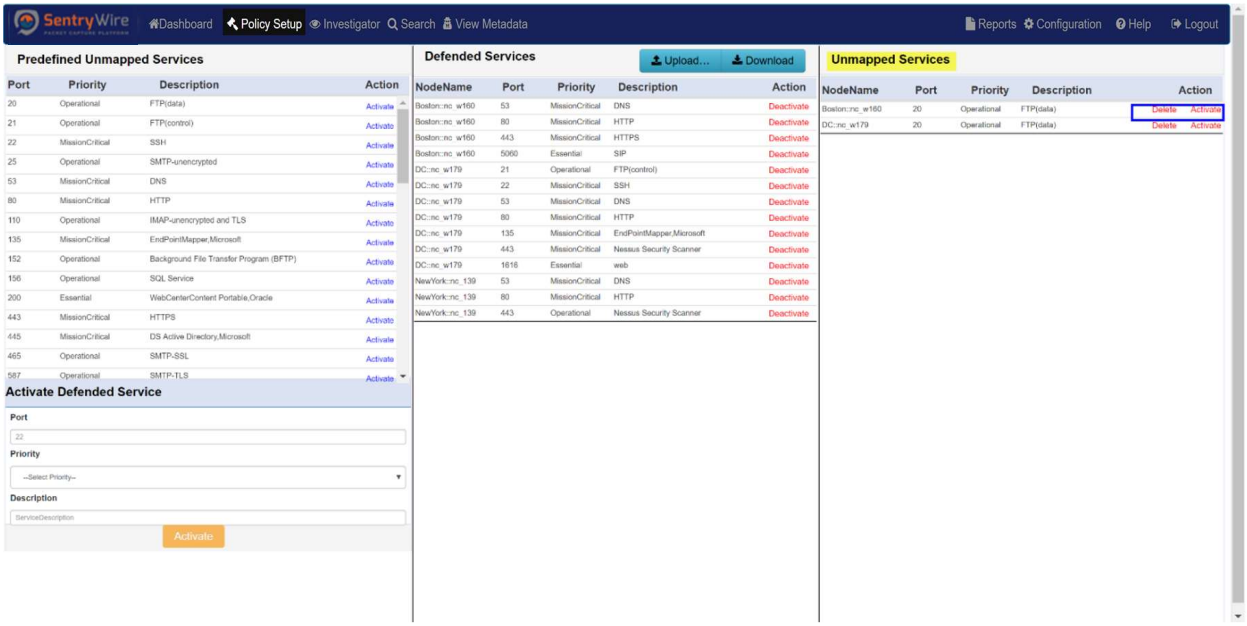


Figure 35– Policy Setup Unmapped Services

6.3 IDS RULES

Signatures play a very important role in Suricata. The system is shipped with several packaged rulesets. When enabled these rules generate alerts based on the actions specified in the rules. These alerts can be viewed in the Threat Hunting Workflow→IoC Manager → Defended Alerts (Only if the alert's source or destination IP address is a defended asset **AND** the alert's source or destination port is a defended service.) or Undefended Alerts tab (Only if the alert's source or destination IP address is **NOT** a defended asset **OR** the alert's source or destination port is **NOT** a defended service). The IDS rules tab allows the user to:

- Choose a set of available rules sets to be loaded for monitoring. Each ruleset has its own count which is displayed in brackets next to the rule name.
- Clicking on an available alert rule set, displays the details of the rules for that category. These rules can also be downloaded to the system.
- User can view, activate, deactivate or delete pre-installed and user defined rules.
- Deleting an active ruleset also deletes the ruleset from the active list and the ruleset is no longer available.

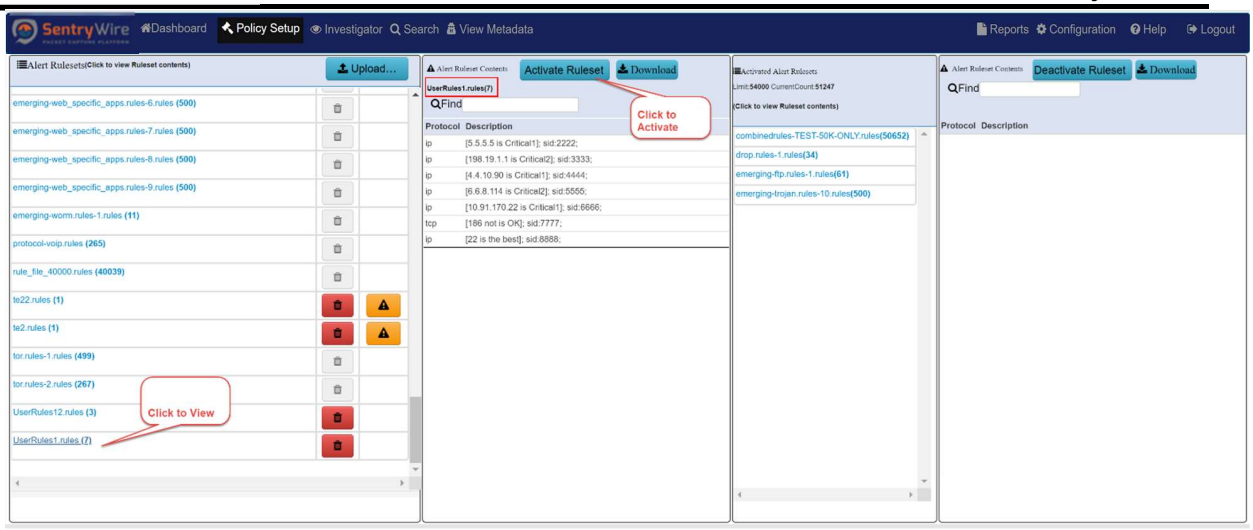


Figure 36 – Policy Setup IDS Rules

- Create/upload user defined rulesets and activate them in the application. (Refer section 6.3.1 for more details)
- Only the type of protocol and associated description is displayed for a listed alert rule file.
- To view an alert rule file the user must click the desired alert file for display (Only the selected alert rule file data is displayed)
- The monitoring application allows up to 54K set of rules to be active at any one time.
- If a user uploaded IDS ruleset has one or more errors, this ruleset is shown with  icon. Clicking on this icon will download a csv file with error text.

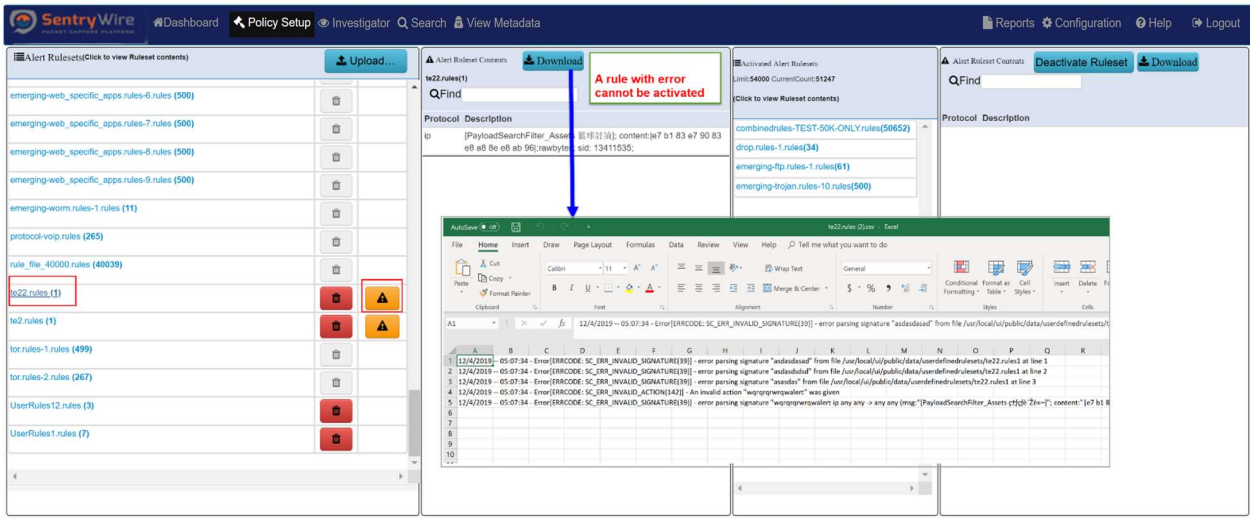


Figure 37- Policy Setup Error

- IDS **does not** allow duplicate file names. If a user uploads a rule file which has same name, the user is prompted to remove the existing file or to rename the file to be loaded.

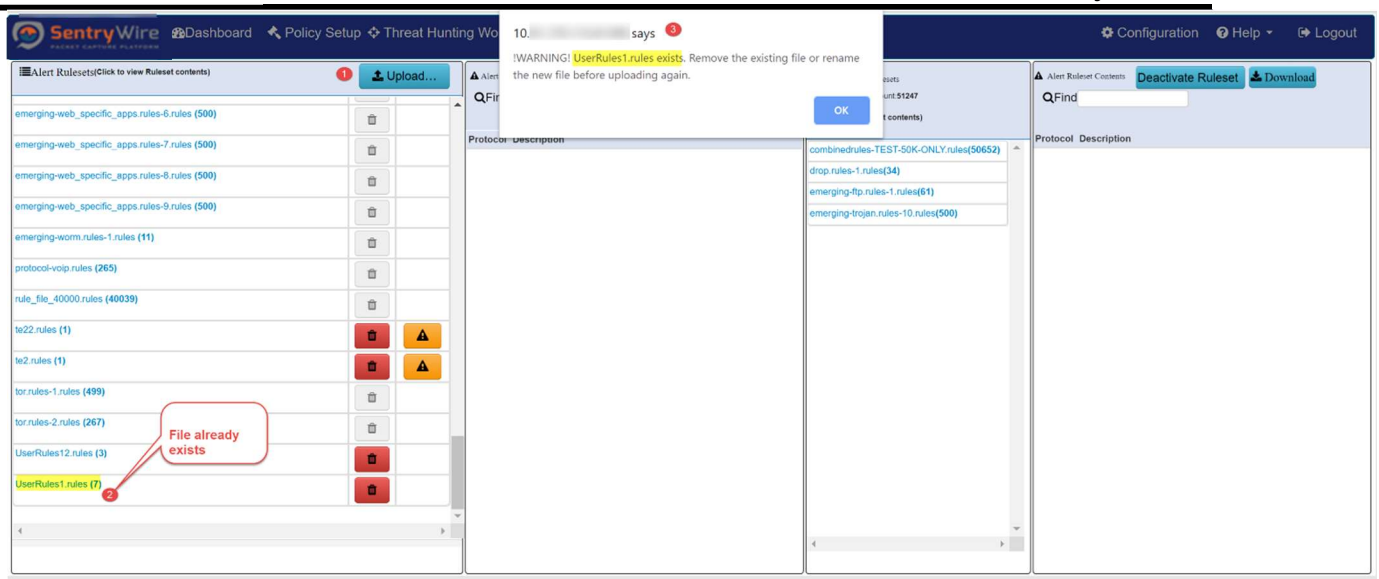


Figure 38-Policy Setup Duplicate Filename Error Warning

- The monitoring application allows up to 54K set of rules to be active at any one time.

6.3.1 Creating and Uploading User Defined IDS Alert Rulesets

Besides the list of extensive rules and signature based alerts which come packaged with the system, the application also allows the user to define their own rulesets and upload/activate them for alert monitoring based on their specific needs.

- In order to create a ruleset, it is important to understand the rule format supported by Suricata.

Note: Please refer to **Appendix G "Understanding Rulesets"** for more details).

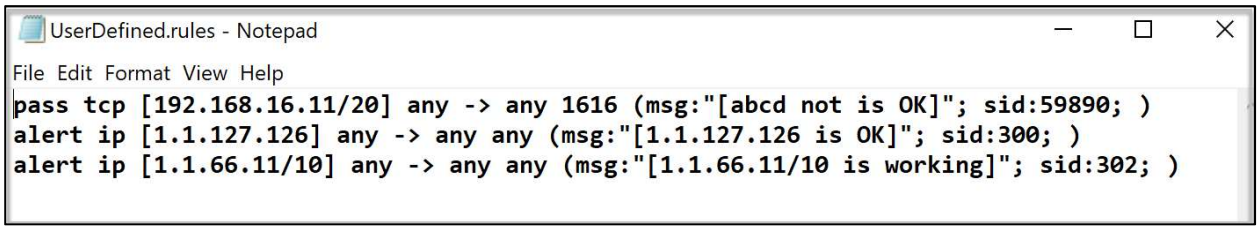
- Once the user is familiar with the rule format it is easy to create user defined rule-set. These rules must be created in a **plain text file** and saved with extension **(.rules),** in order to be recognized by the application.
- Once the rule is created/saved, it can be uploaded into the application to produce desired alerts.

Perform the following to create and upload a user defined ruleset file:

Step 1

- Create a plain text file using a note pad (Windows) or vi editor (Linux/Unix)
- Type in the ruleset in the correct format (Described in the section - **Understanding a ruleset Appendix F**) and save with extension as (.rules).

Example:



Step 2

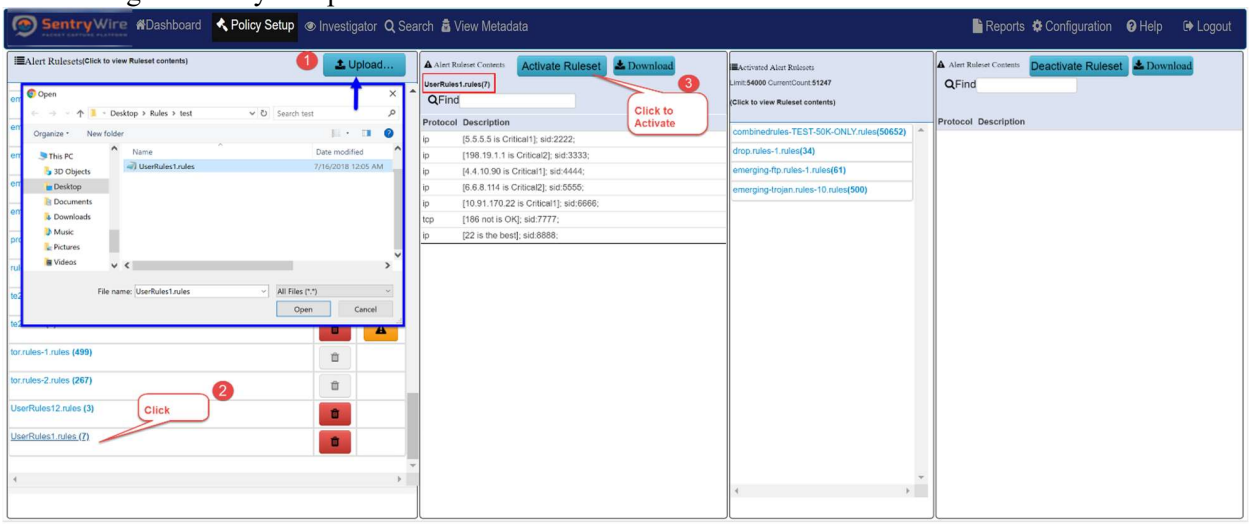
- On the UI go to Policy Setup→IDS Rules tab.
- 

Figure 39-Policy Setup Upload Step 2

- Click on upload button at the top.
- Select the ruleset you want to upload.
- Once uploaded, click the ruleset to display its contents.
- Click "Activate Ruleset" to activate the User Defined ruleset. All activated rules appear in the activated ruleset column.
- Once the ruleset is activated, the capture server generates an alert, as defined by the alert ruleset. These alerts can be viewed in the Threat Hunting Workflow→IoC Manager → Defended Alerts (Only if defended asset and a defended service are part of its 5-tuple, and alert's source or destination IP address is a defended asset **AND** the alert's source or destination port is a defended service) or Undefended Alerts tab (Only if the alert's source or destination IP address is **NOT** a defended asset **OR** the alert's source or destination port is **NOT** a defended service).

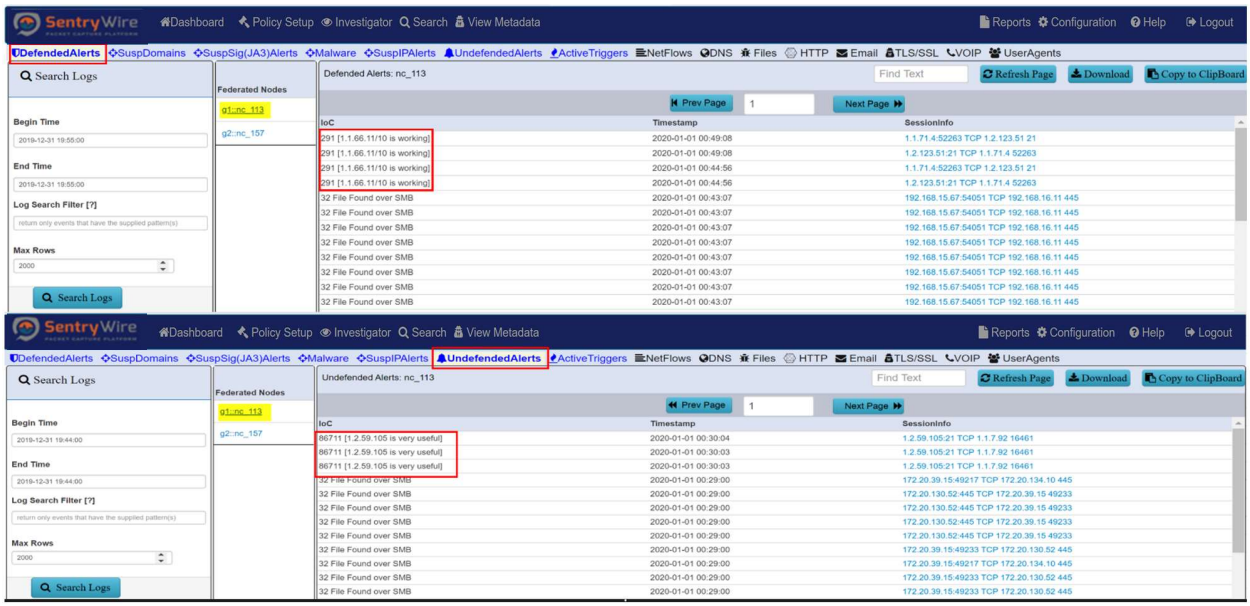
- 

Figure 40-Defended vs. Undefended Alerts

- To stop receiving alerts for User Defined Ruleset simply click on the Deactivate ruleset button. The ruleset is still available in the Ruleset library and can be reactivated until deleted permanently.

***Note**: A guest user cannot Add or Delete rules.*

6.4 AUGMENTATION

Augmentation allows users to upload additional data that can be used to enhance the value of stored data and allow data correlation.

Augmentation panel allows users to upload 4 types of meta-metadata that allows analysts and the DPI engine to augment it. **Note**: The system comes preloaded with all Suspicious TLS/SSL Signatures, Suspicious IP Addresses, Suspicious Domains and Malware . A user can also upload their own list for monitoring.

- Suspicious TLS/SSL Signatures
    - JA3 is a method for creating TLS/SSL client fingerprints that should be easy to produce on any platform and can be easily shared for threat intelligence.
    - Clicking on the hyperlink **Suspicious TLS/SSL Signatures** will display all the currently uploaded Suspicious TLS/SSL clients in Kibana.

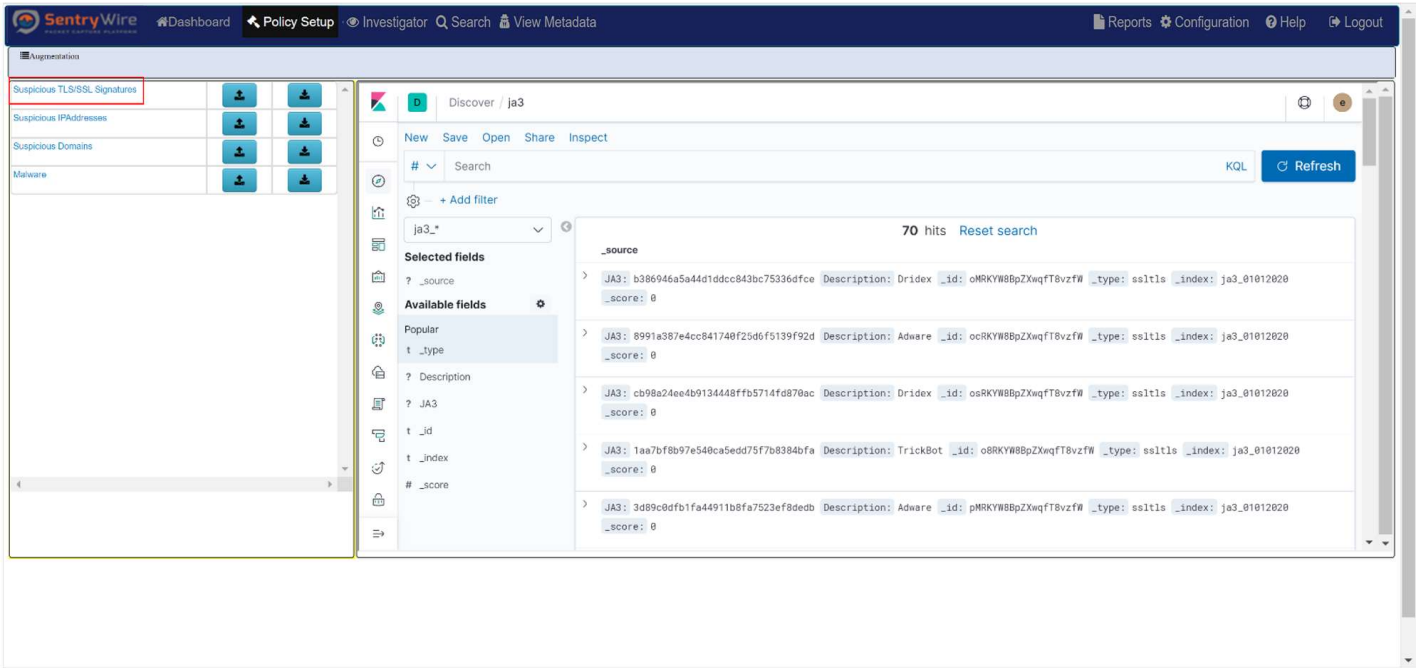


Figure 41-Policy Setup Suspicious TLS/SSL Signatures

    - When a Suspicious JA3 appears in the traffic the system generates an alert. This can be viewed in View Metadata→SuspSig(JA3)Alert tab for each Group:Node.
    - To upload a user desired list for JA3 simply click on the upload icon. The user can then upload a .csv file that must contain JA3 signature name, comma separator and an optional description. (For more details on upload please refer to section 4.4.1)
    - The user can also download a list by clicking the download button as a csv.

- Suspicious IP Addresses

- These are class of IP addresses that are considered as unsafe and unreliable within a network traffic.
- Clicking on the hyperlink Suspicious IPAddresses will display all the currently uploaded Suspicious IPAddresses in Kibana.

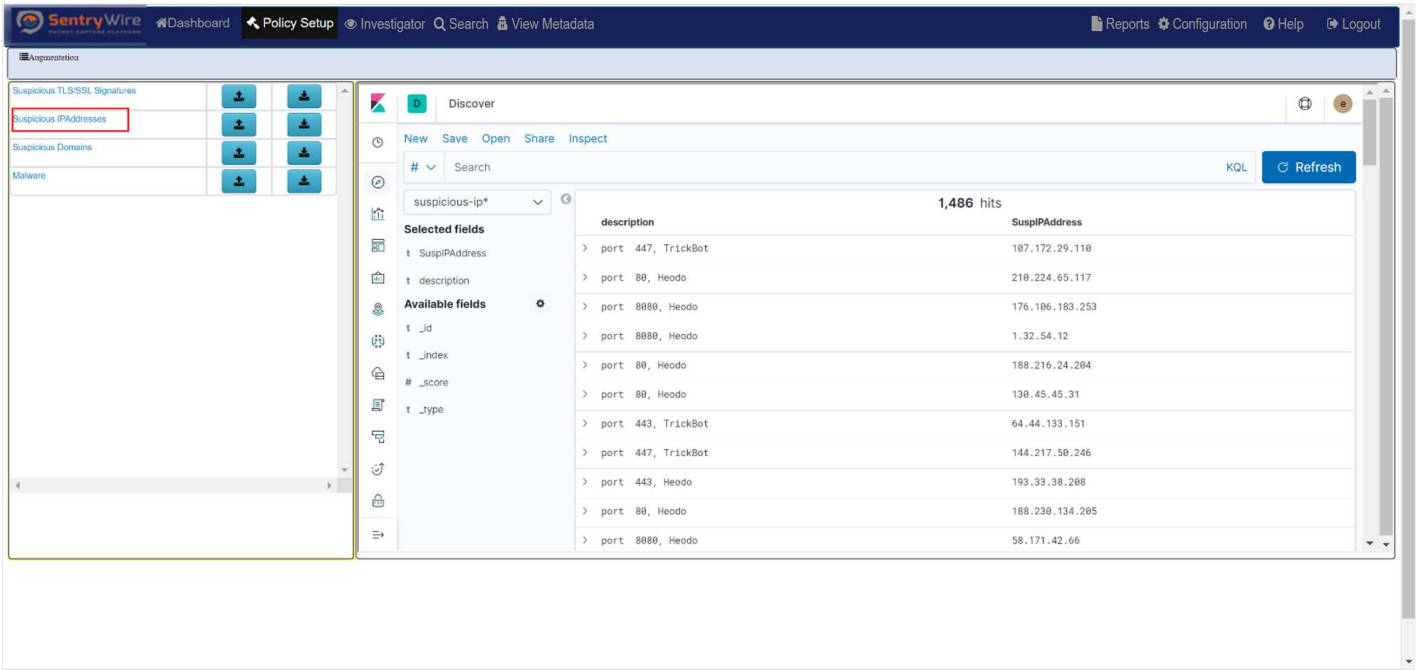


Figure 42-Policy Setup Suspicious IPAddresses

- When a SuspiciousIP appears as source IP or destination IP in the traffic the system generates an alert. This can be viewed in View Metadata→SuspIPAlert tab for each Group:Node
- To upload a user desired list for SuspiciousIPs simply click on the upload icon. The user can then upload a .csv file that must contain SuspiciousIPs name, comma separator and an optional description. (For more details on upload please refer to section 4.4.1)
- The user can also download a list by clicking the download button as a csv.

- Suspicious Domains
  - Domain names are an important avenue to investigate security incidents or to prevent some malicious activity to occur on your network.
  - Clicking on the hyperlink Suspicious Domains will display all the currently uploaded Suspicious Domains in Kibana.

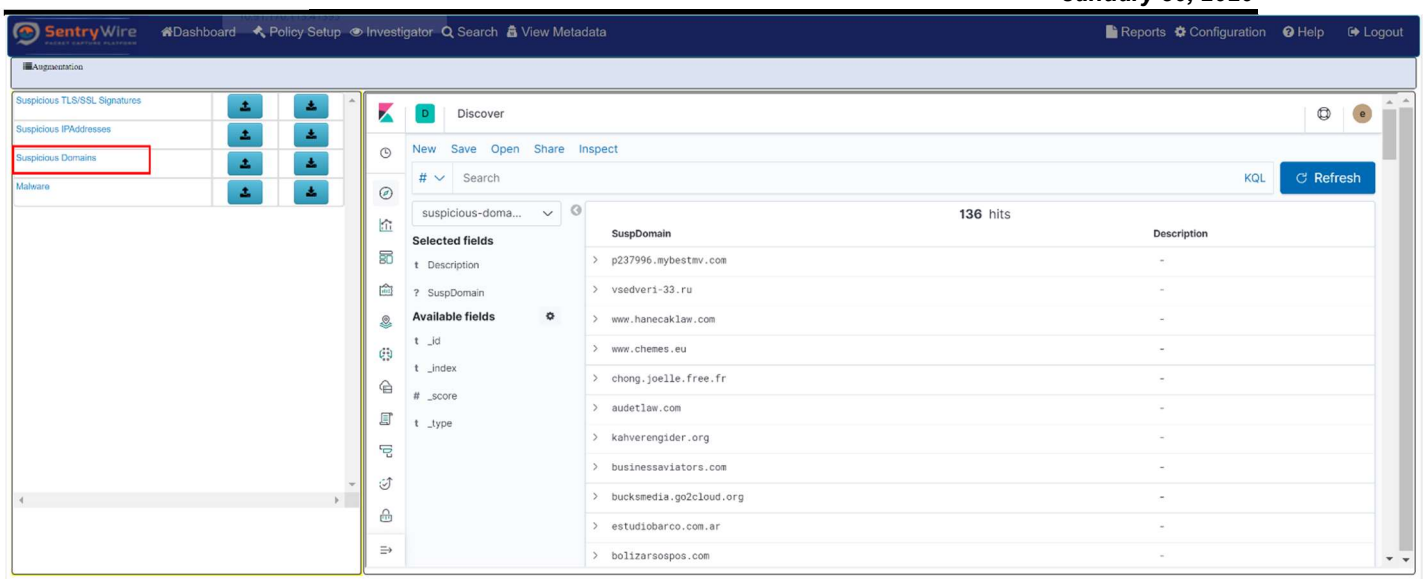


Figure 43-Policy Setup Suspicious Domain

- When a Suspicious Domain appears in the traffic the system generates an alert. This can be viewed in View Metadata→SuspDomain alert tab for each Group:Node
- To upload a user desired list for Suspicious Domain simply click on the upload icon. The user can then upload a .csv file that must contain Suspicious Domain name, comma separator and an optional description. (For more details on upload please refer to section 4.4.1)
- The user can also download a list by clicking the download button as a csv.

- Malware
  - This category allows users to upload known bad md5sums for allowing the software to identify/alert when a file with bad md5sum is being transmitted.
  - Clicking on the hyperlink Malware will display all the currently uploaded md5sum in Kibana.

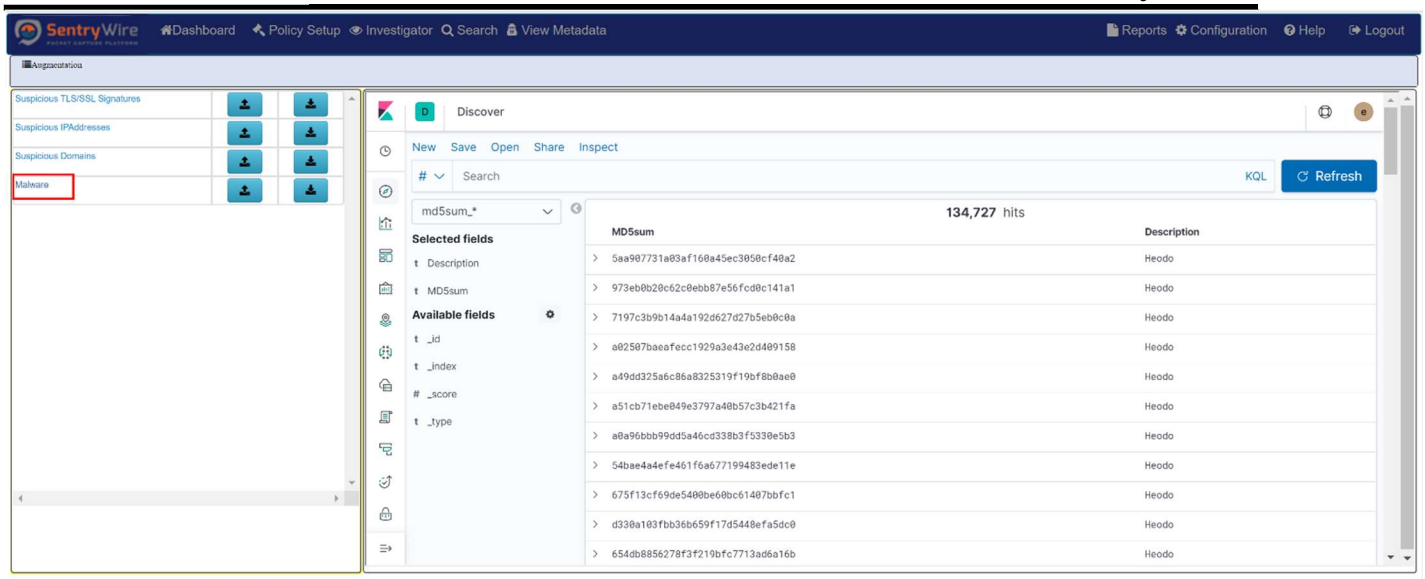


Figure 44-Policy Setup Malware

- When a Suspicious Malware appears in the traffic the system generates an alert. This can be viewed in View Metadata→Malware alert tab for each Group:Node
- To upload a user desired list for Malware simply click on the upload icon. The user can then upload a .csv file that must contain Malware name, comma separator and an optional description. For more details on upload please refer to section 6.4.1
- The user can also download a list by clicking the download button as a csv.

6.4.1 Uploading Augmentation

User can upload augmentation data in a csv file format as below.

- **First column** of each row should state a resource
- **Second column** (**optional**) of each row should describe the resource in the first column. This is optional but generally a good practice for easy reference.

Example of a SuspiciousIPs csv file:

172.20.17.67, system1
100.100.100.104, system2
8.8.8.8
8.8.4.4, system3

To upload the data simply click on upload icon. Once uploaded they are displayed in Kibana.

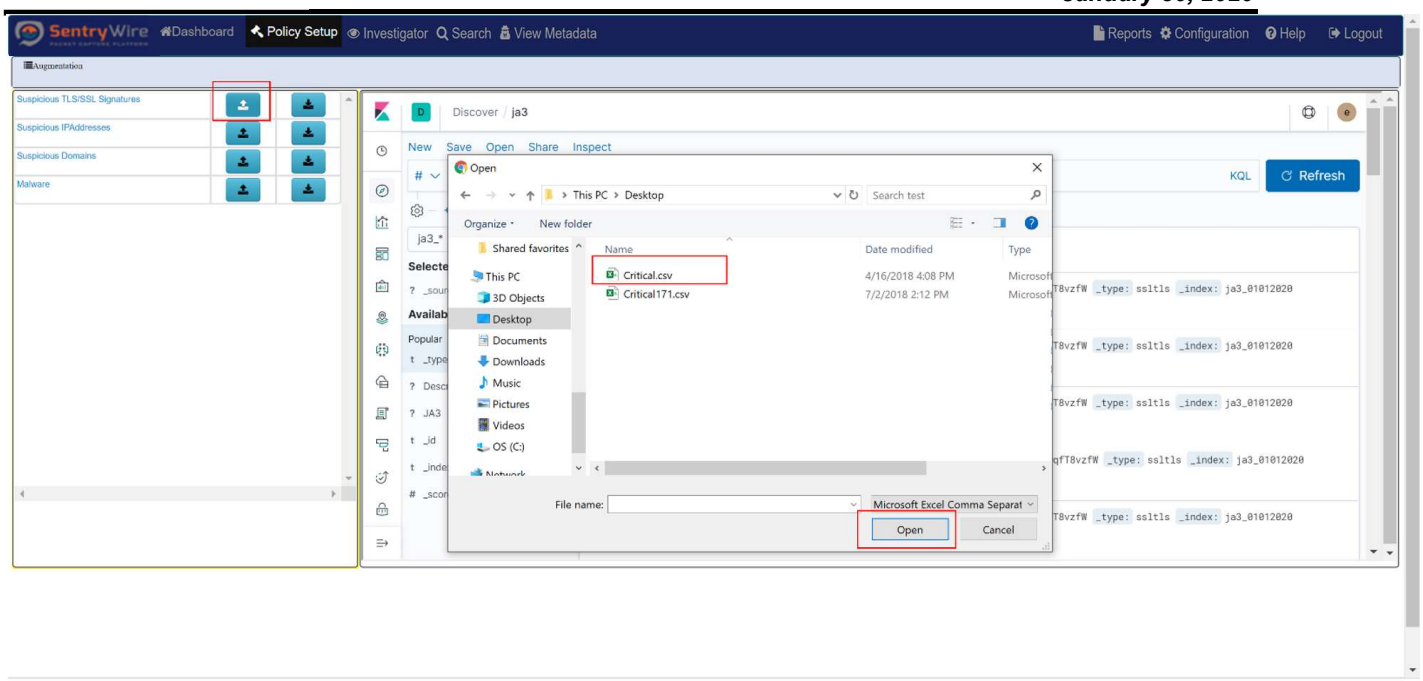


Figure 45-Policy Setup Upload Augmentation file

6.5 ACTIVE TRIGGERS

Active triggers allow you to get alerts when you specify an event to cause the trigger.

***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.
- The Add button allows the user to create an active trigger (max 100)
- The delete button allows you to delete the configured trigger.

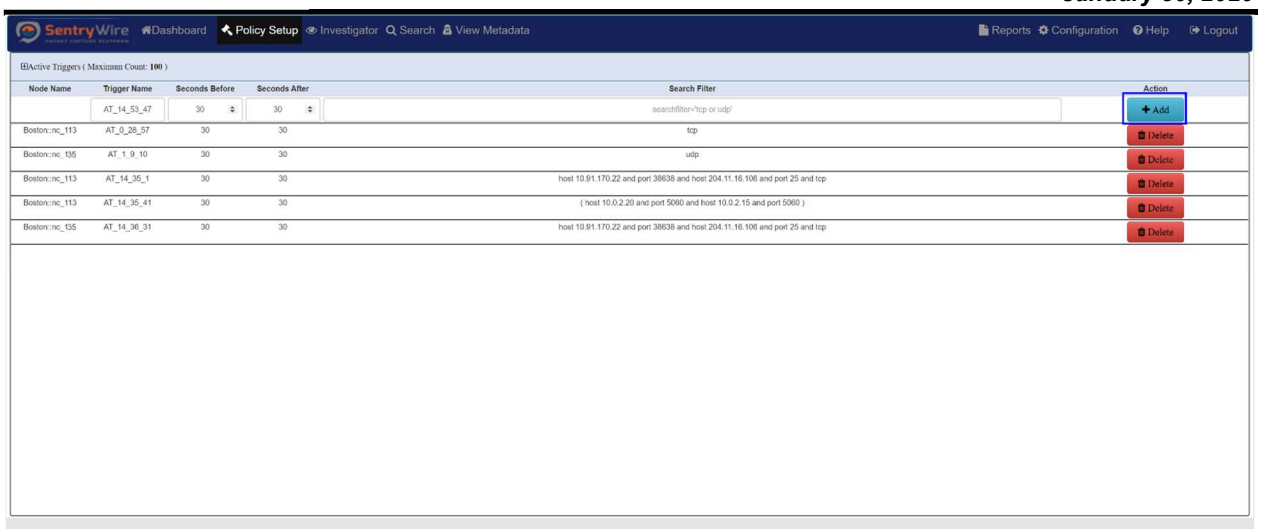


Figure 46 Add Active Trigger

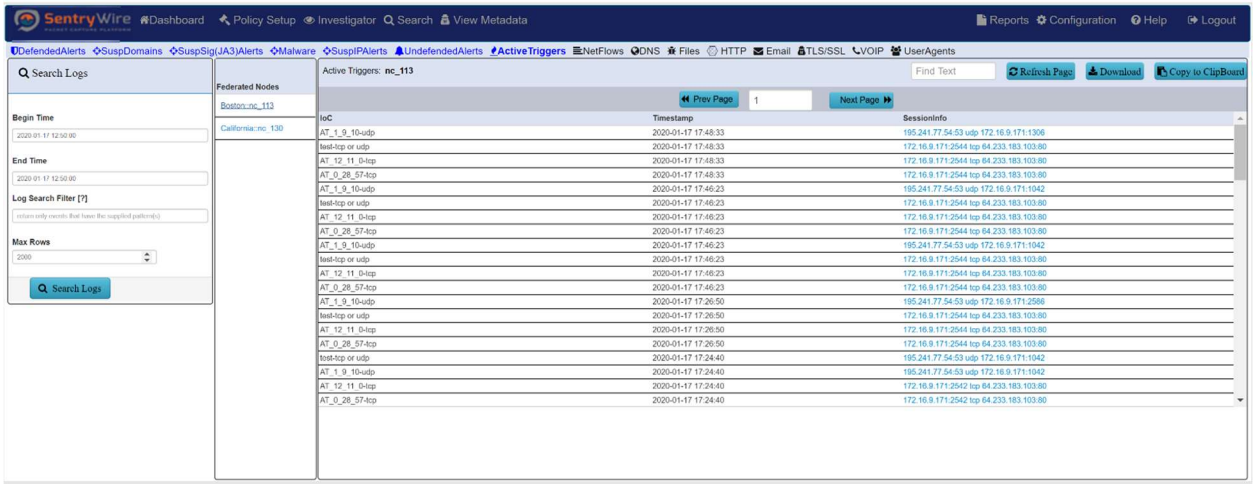
- 

Figure 47 - View Active Trigger Events

- The trigger events can be seen in the Threat Hunting Workflow → IoC Manager → Active triggers tab.
- Clicking on an active trigger event will automatically fill out a search request within the specified time parameters around the triggered event (Seconds Before and Seconds After).

***Note**:*
*Please refer to **Appendix D** for more information about the BPF filters supported by the application*
A guest user cannot add or delete Active Trigger.

6.6 PRECAPTURE FILTER

PreCapture filter filters network traffic before writing the traffic to disk. A PreCapture filter can be specified within the PreCapture Filter menu. PreCapture Filter can be set in one of two methods discussed in the following sections.

> ***Note**:*
> *If a BPF filter is set and a set of IPaddresses are loaded, the **BPF** filter is **ignored**.*
> *A guest user cannot add or delete PreCapture*

6.6.1 Applying a Berkeley Packet Filter (BPF)

A capture filter can be applied in the form of a BPF filter. As a BPF filter the PreCapture takes the form of primitive expressions connected by conjunctions (and/or) and optionally preceded by not.

- To specify a PreCapture filter fill out the "Filter Name" and "Search Filter", then select the "Set" button to apply the PreCapture filter.
- Select the delete button to permanently delete the filter.

Below are some use cases examples of PreCapture filter application:

- "not dst port 80" will drop all traffic destined for port 80
- "host 1.2.3.4 or host 1.1.1.1" captures only the traffic for these two hosts while filtering out the rest of the traffic.

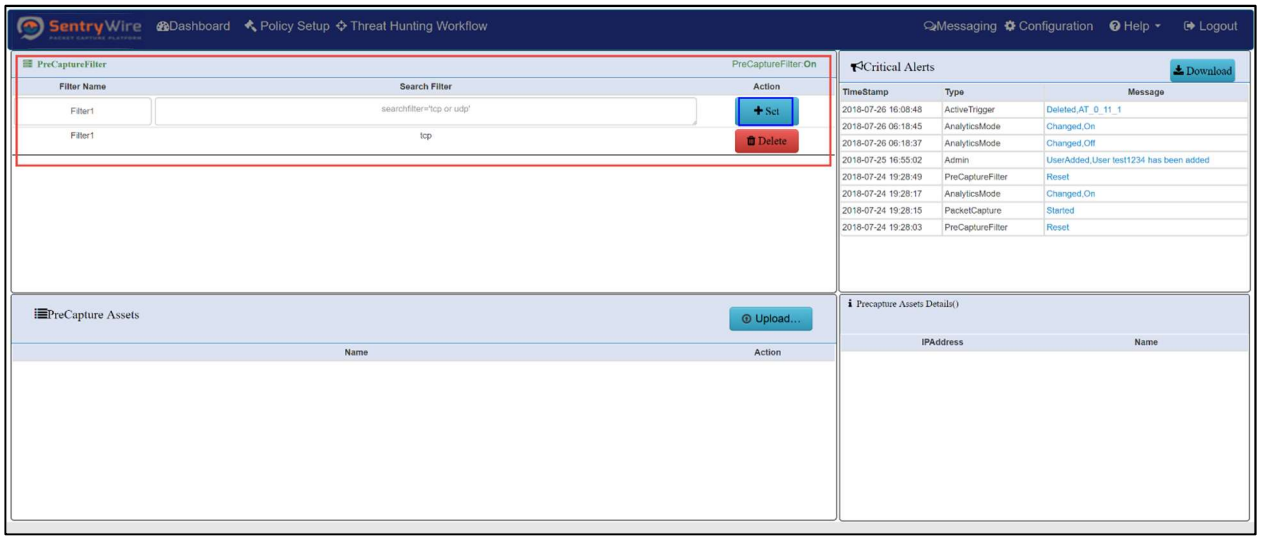


Figure 48-Applying BPF Filter

Notes:

- *A detailed list of valid BPF filters supported is provided in **Appendix D***
- *When a valid BPF filter is applied the status bar reports "PreCapture filter: **On**"*
- *When an invalid filter is applied "PreCapture filter: **Off**" status is displayed both on dashboard and PreCapture filter tab status bar.*

6.6.2 Uploading PreCapture Assets as a File

In addition to the BPF filter, the application also allows the user to upload a list of IP addresses to be applied as a PreCapture filter. Multiple files that contain a list of valid IP addresses can be uploaded at the same time. The application allows only a maximum of 32 unique IP addresses to be applied at a given time.

***Note**: If a BPF filter is set and a set of IP addresses are loaded, the **BPF** filter is **ignored**.*

Perform the following to create and upload a PreCapture Filter:

<u>Step 1: PreCapture Assets File Format</u>

Users can define a list of IPs intended to be applied as PreCapture filters, in a **csv** file as per the format below:

- **First column** of each row should state an IP address (resource).
- **Second column (optional)** of each row should describe the resource in the first column. This is optional but generally a good practice for easy reference.

Example of a PreCapture Assets csv file:

1.2.112.6, System1
1.2.30.6

Step 2: Uploading a User PreCapture Assets File

- Create a <Filename>.csv file on your local system.
- Click on Upload button.
- Select file from the local system to be uploaded.

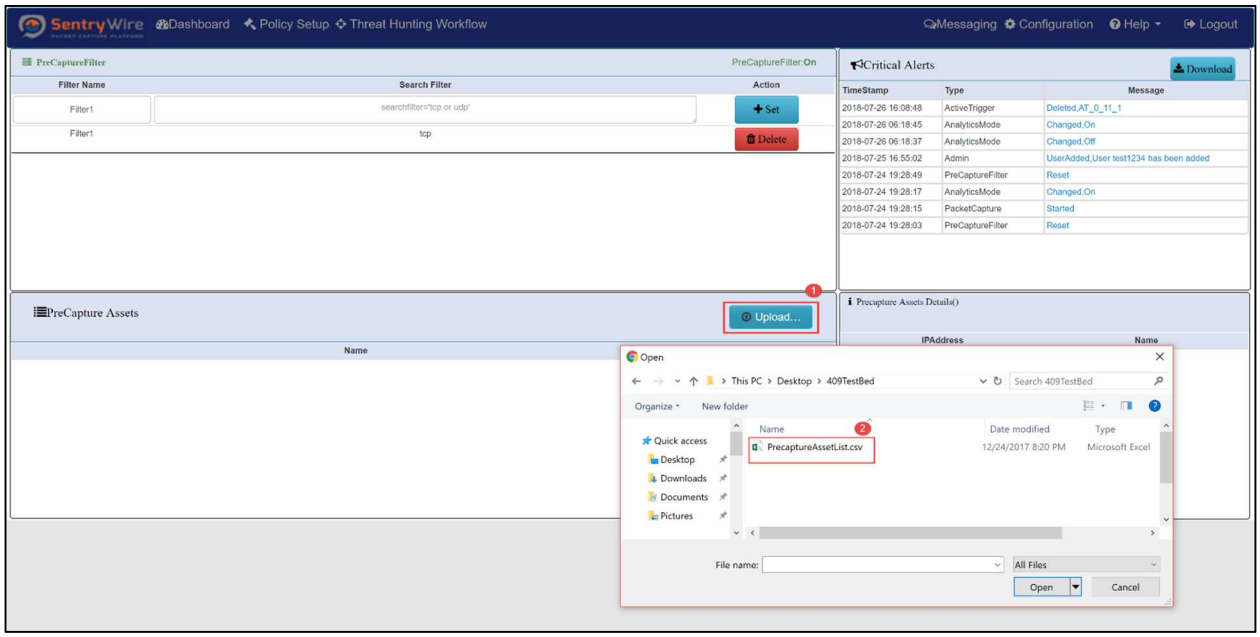


Figure 49 Uploading PreCapture Asset File

- The figure below depicts one PreCapture IP asset list containing 13 IP addresses.

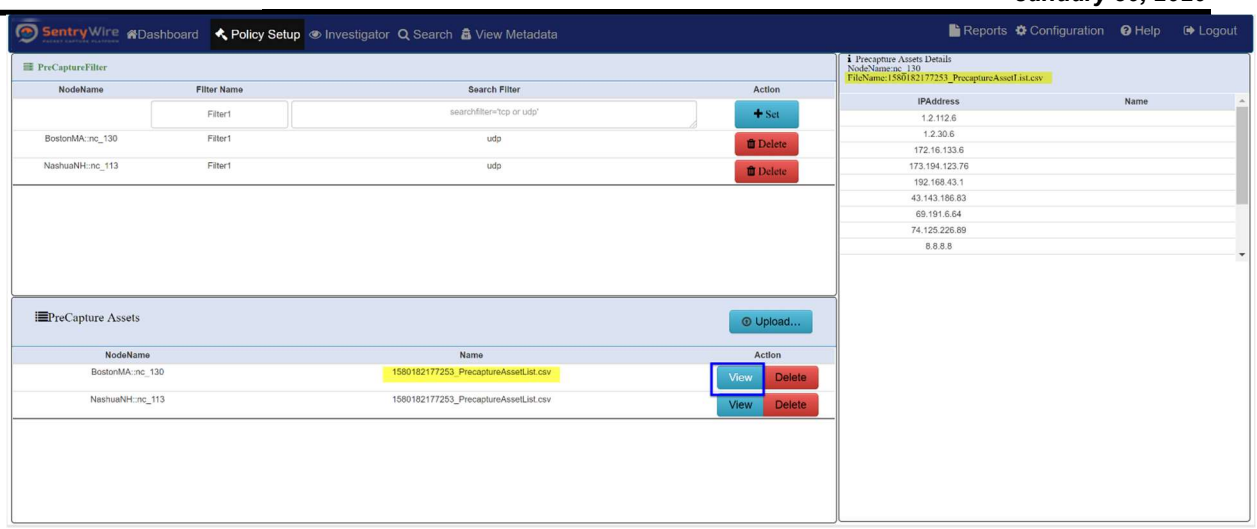
- 

Figure 50-Sample Pre-capture IP Asset List

- As more files are uploaded, the application takes the first 32 unique IP addresses and allows the traffic only if source IP or destination IP is among these 32 addresses.

***Note**: A guest user cannot add or delete PreCapture.*

7 INVESTIGATOR

Investigator panel allows users to view Kibana Dashboard and Discover views of each federated node. It also allows the users to create a search across all selected nodes for further analysis.

Users can switch to the desired Kibana Discover window by selecting a node from the list displayed in the left sub panel.

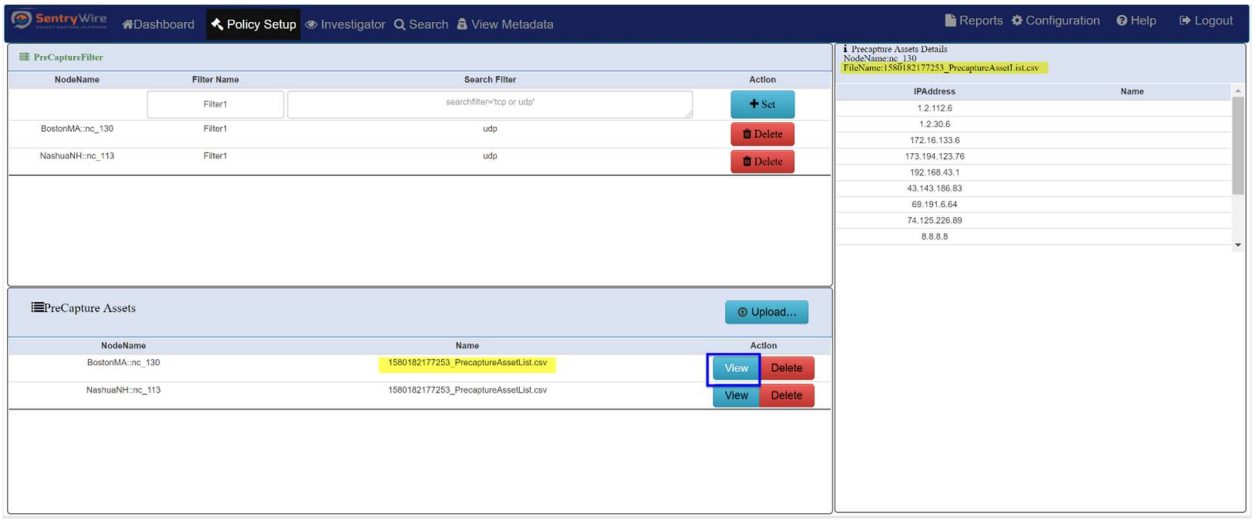


Figure 51-Policy Setup Kibana Node Selection

The following types of metadata are available for analysis and discovery through Kibana:

Event Type	KQL Search Filter
Alert	event_type:'alert'
File	event_type:'fileinfo'
DNS	event_type:'dns'
SMTP	event_type:'smtp'
ActiveTrigger	event_type:’activetrigger’
HTTP	event_type:'http'
TLS/SSL	event_type:'tls'
SMB	event_type:’smb’
VOIP	event_type:’voip’
Suspicious IP Alerts	event_type:’suspip’
Suspicious Signature Alerts	event_type:’ja3’
Suspicious Domains	event_type:’suspdomain’

7.1 CREATE SEARCH WORKFLOW

1. Once inside the Kibana Discover view of the node, select one of the displayed documents to view details(by clicking on the > of the document).

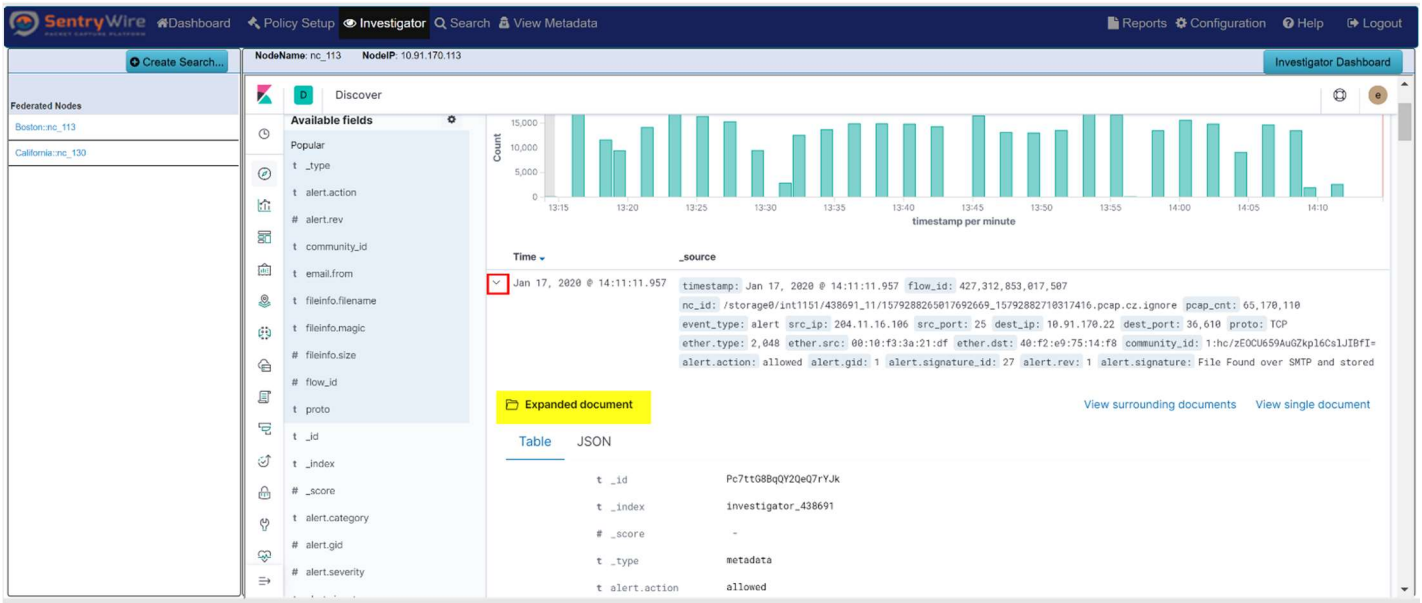
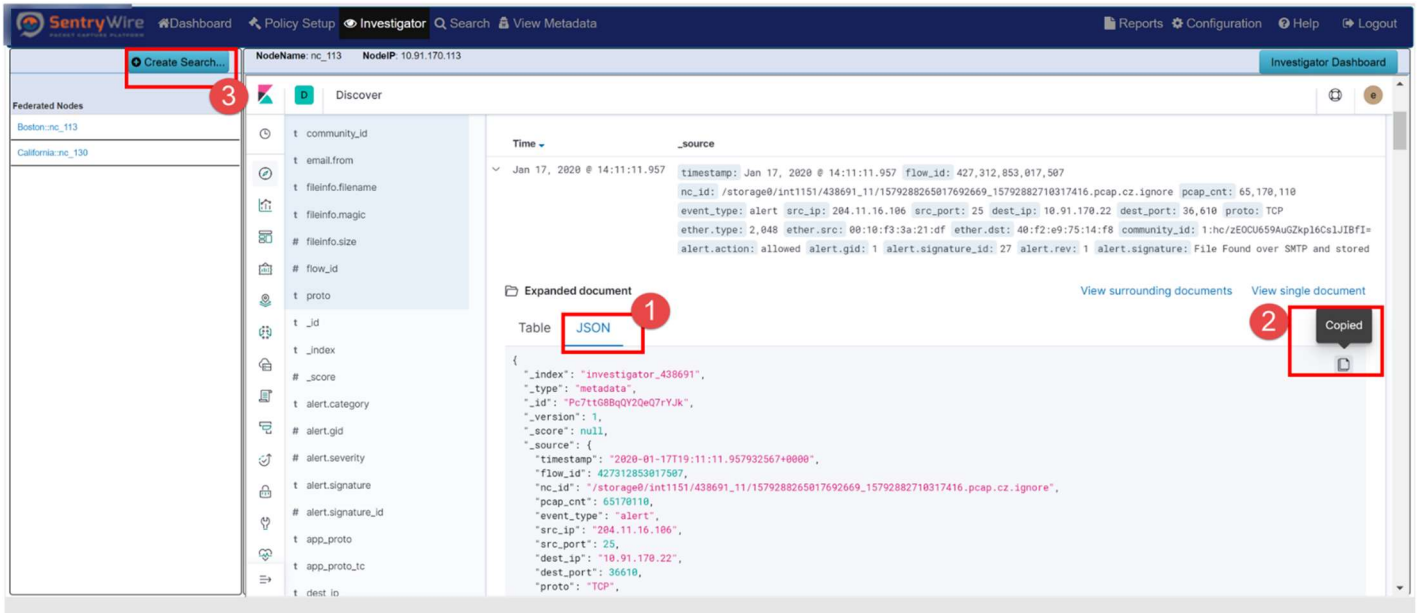


Figure 52-Investigator Window

2. Click on JSON hyperlink. This shows the JSON data for this document. Top right corner of the JSON view panel shows an icon that allows users to copy the JSON data being shown.



3. Click on Create button of the left sub-panel. A dialog box appears with a search name filled in and an area to paste the copied json data.
4. Users can modify the search name if desired.
5. Paste the copied JSON data and click the “Create Search” button.

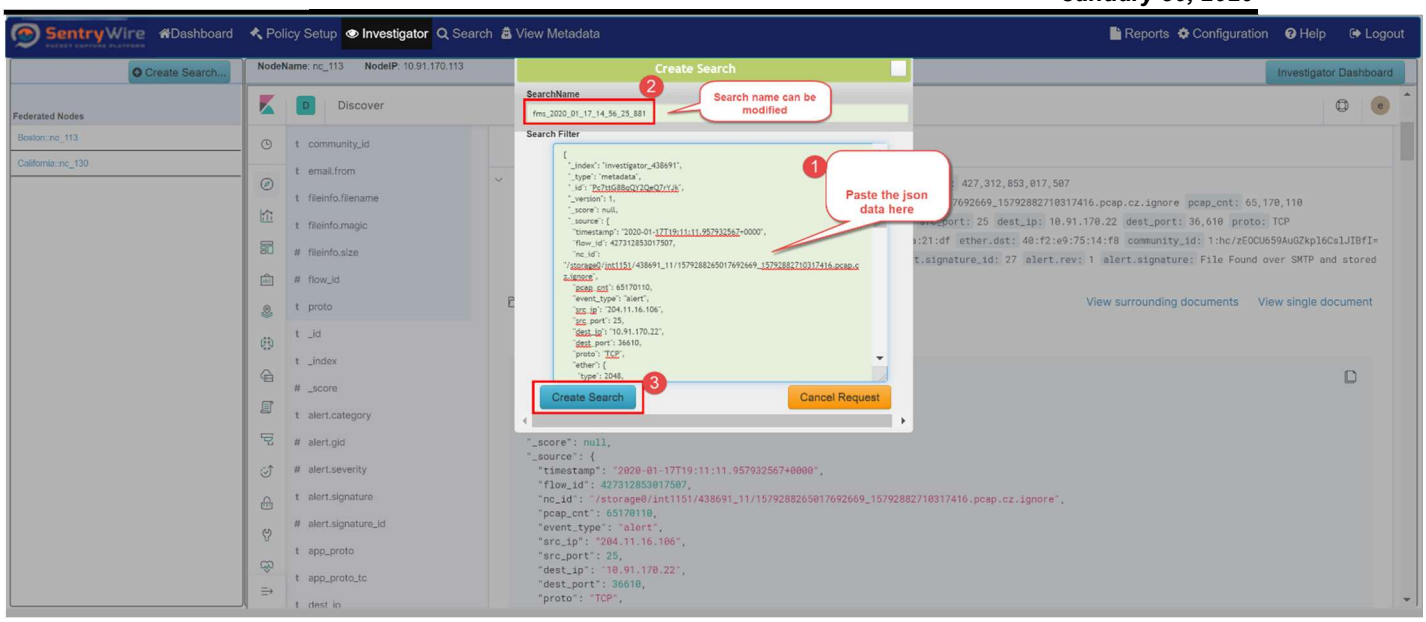


Figure 53-JSON Create Search

6. This allows the server to create a search based on the pasted JSON data on all the selected federated nodes.
7. Once the search is submitted successfully, the following alert is displayed.

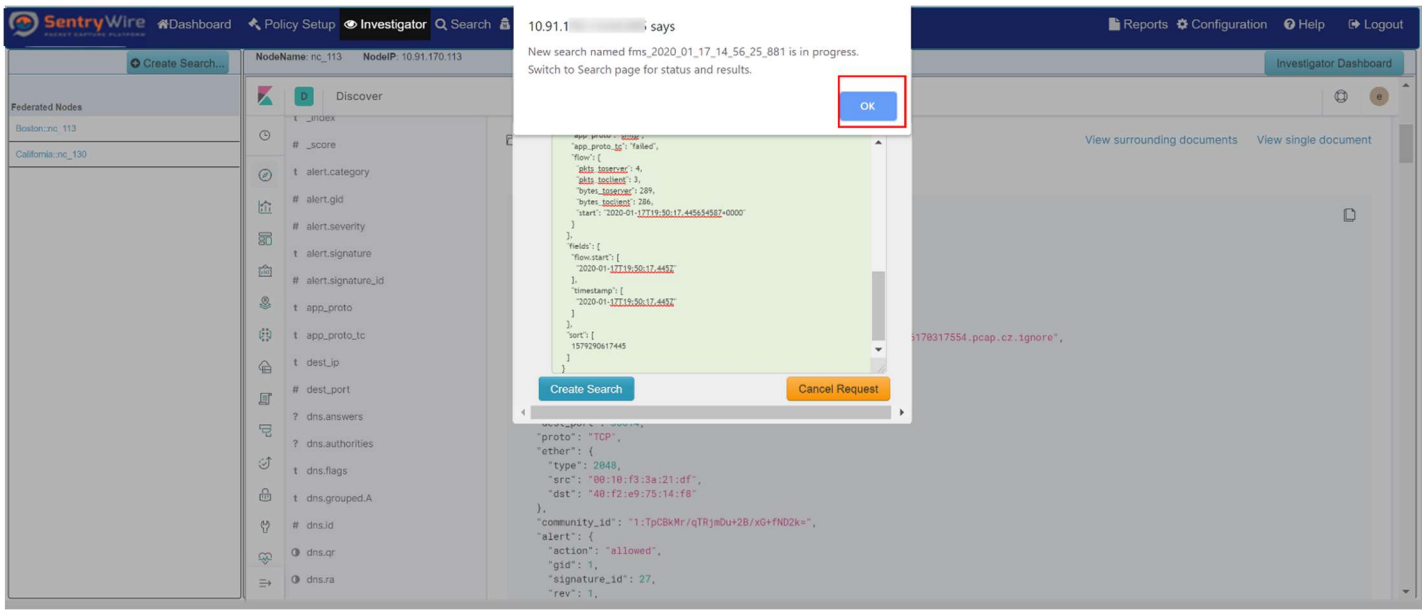


Figure 54-JSON Search Success Alert

8. Each selected node will perform the search and return results to the Search panel.
9. To view and manage these searches, switch to the Search panel from the main menu.

7.2 INVESTIGATOR DASHBOARD

Once inside the Kibana Discover view of the node, clicking on the Investigator Dashboard button will switch to Kibana Dashboard view for the selected node.

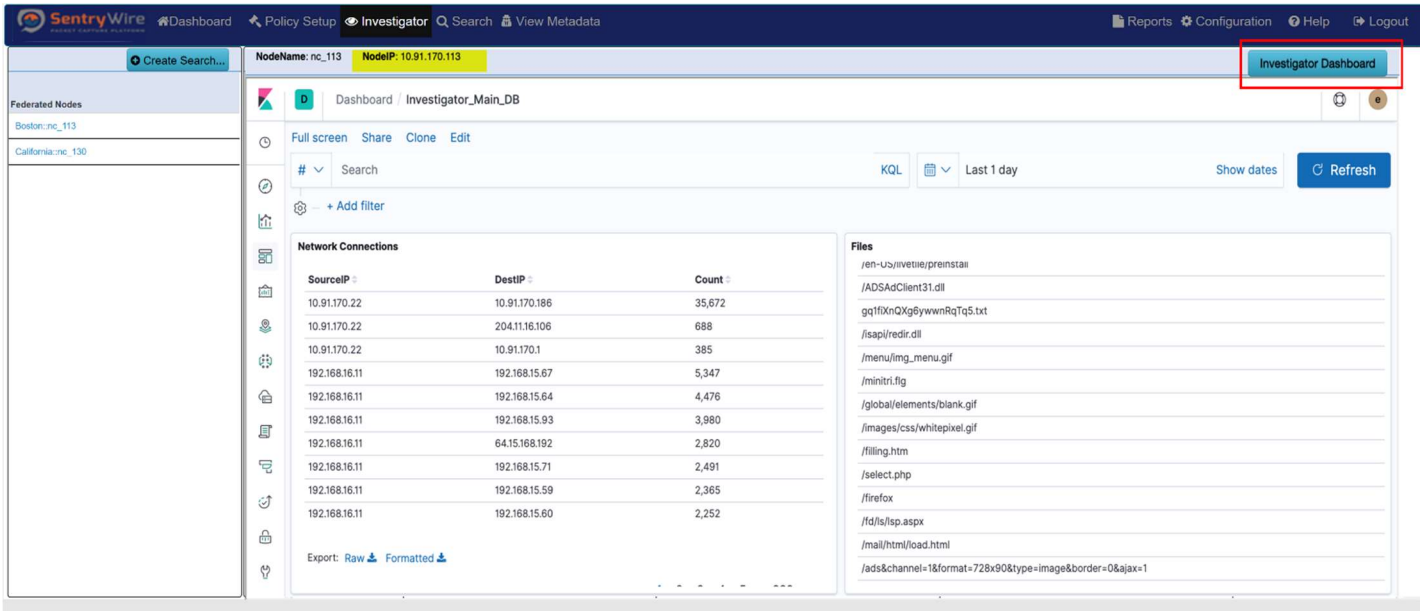


Figure 55-Investigator Dashboard

8 SEARCH

8.1 SEARCH PANEL OVERVIEW

The Search panel allows users to create and manage searches, view individual streams, objects and packets of each search. All search data can be viewed, analyzed and optionally downloaded by authorized users for further analysis.

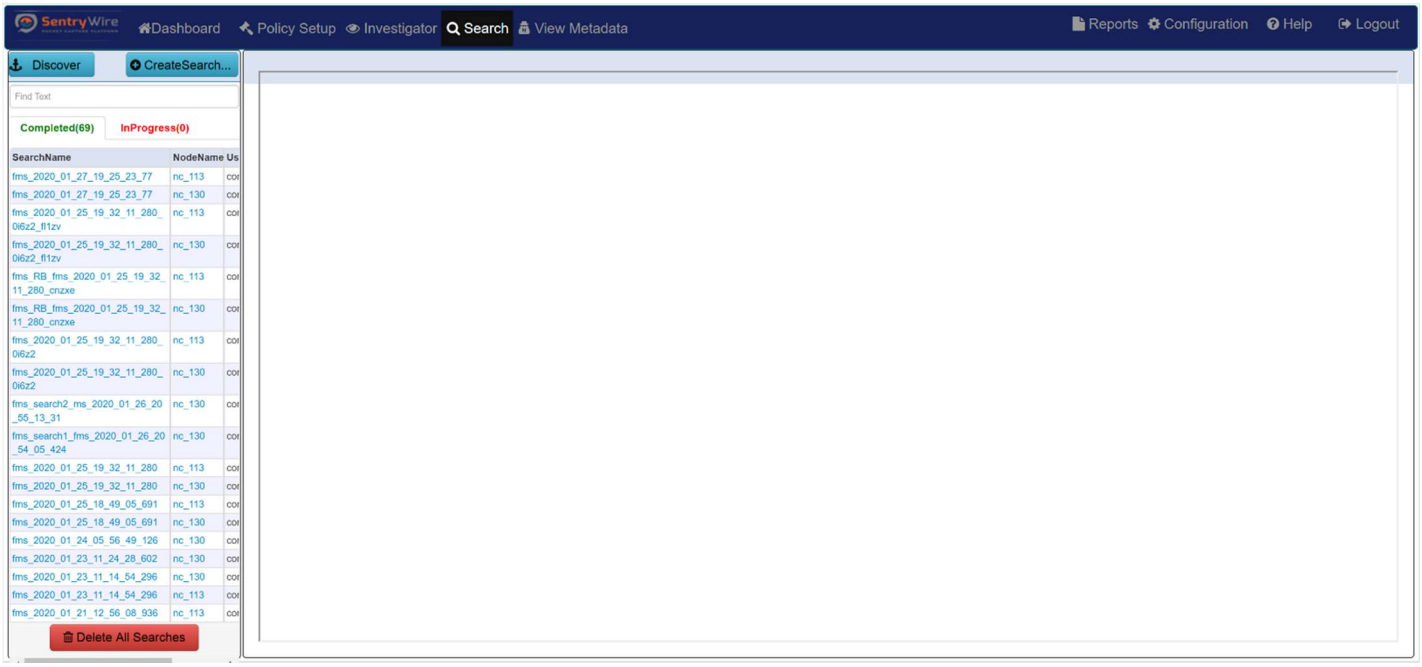


Figure 56-Search Screen

The Search screen is divided into two main panels:

1. Left panel allows the user to :

   - **Discover** - This button shows search events as logged in ElasticSearch/Kibana store. Search creation events, search completion events, search deletion events and any other search related events are displayed in this window in reverse chronological order.

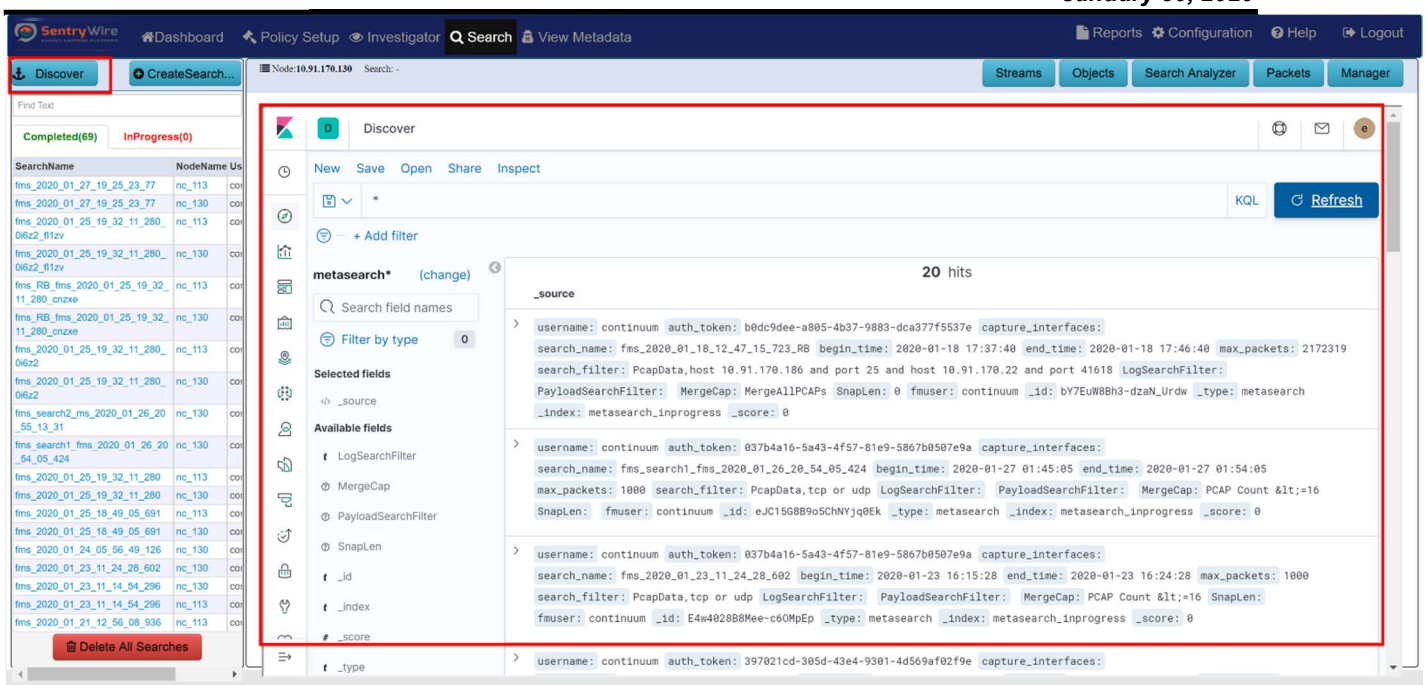


Figure 57-Search Discover Button

- **Create Search** - This button opens a popup window to allow users to create a search. For more info on creating a search please refer to section 6.1

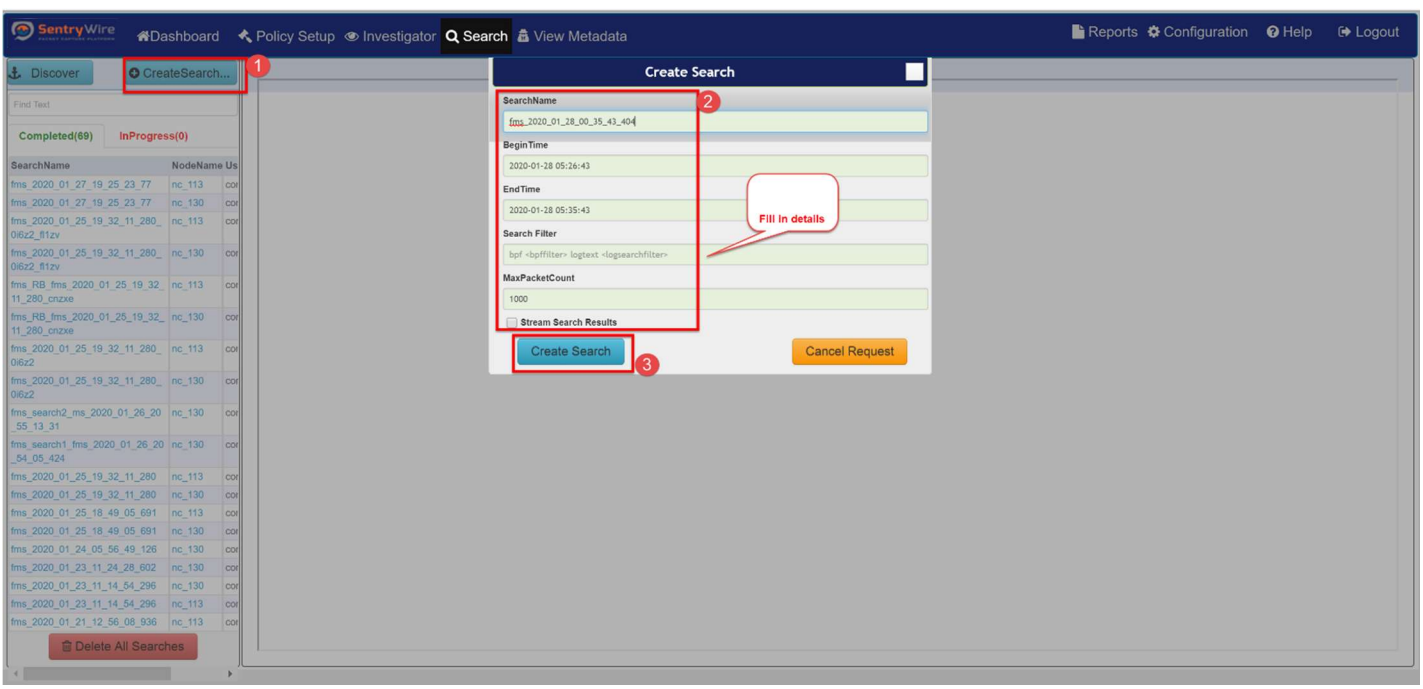


Figure 58-Create Search Button

- **Find Text** area – Displays content with the matching text only.
- **Completed**- This tab shows all the completed and cancelled searches. To see the username of each search and delete option, search scroll to the right (as shown in the

picture below). Clicking on the hyperlinked Search name or node name displays the stream view of the clicked search.

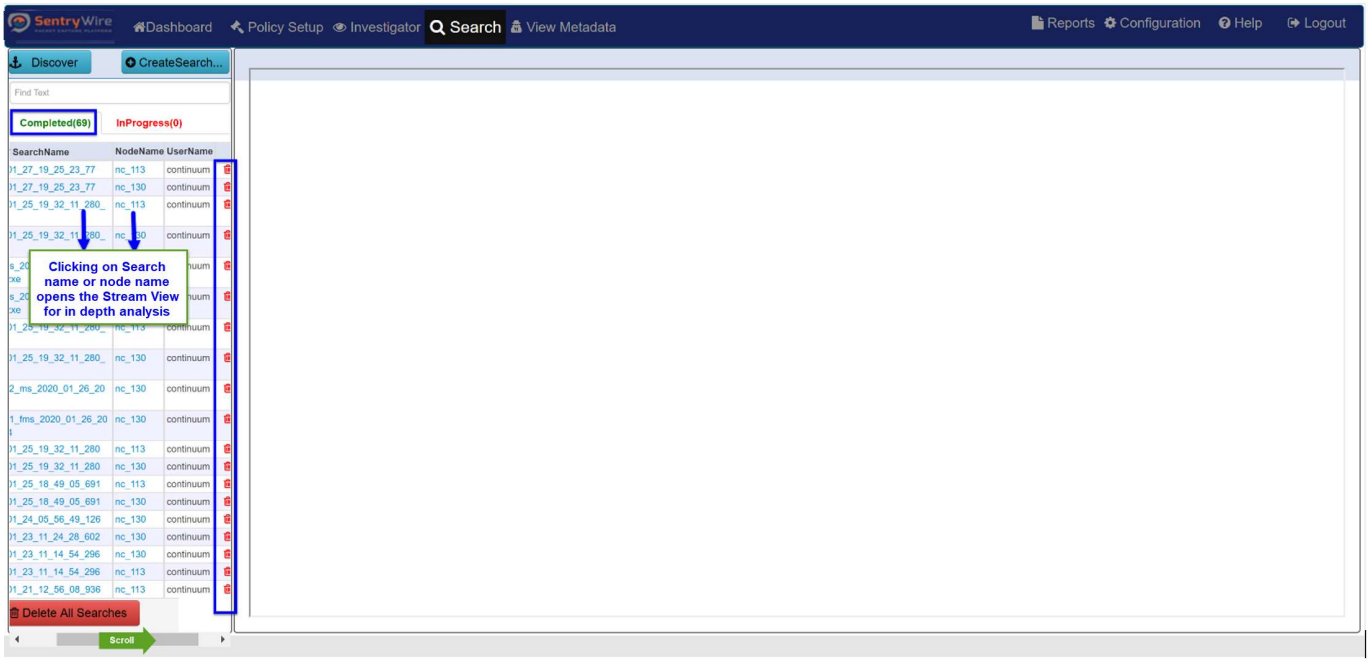


Figure 59-Completed Search View

- **InProgress-** This tab shows the list of searches that are in Pending/InProgress state. Scrolling to the right allows the user to delete any search in Pending/InProgress state by clicking on the delete icon.

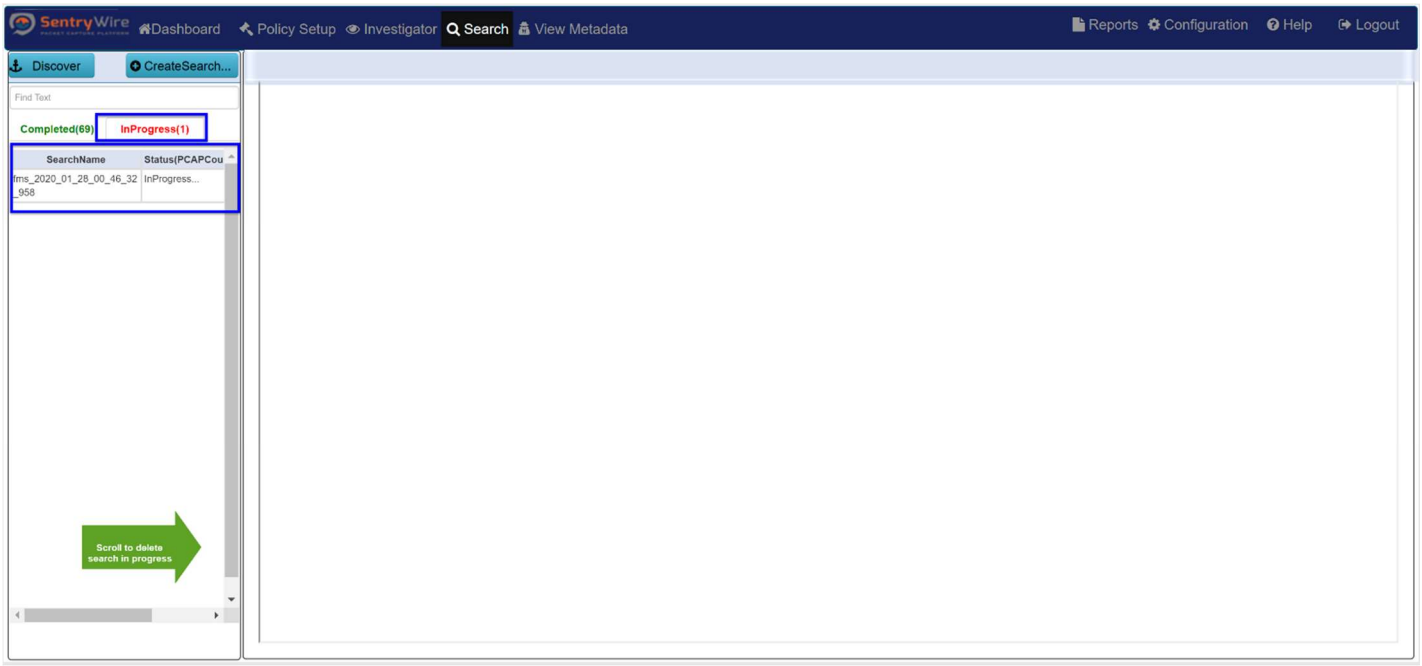
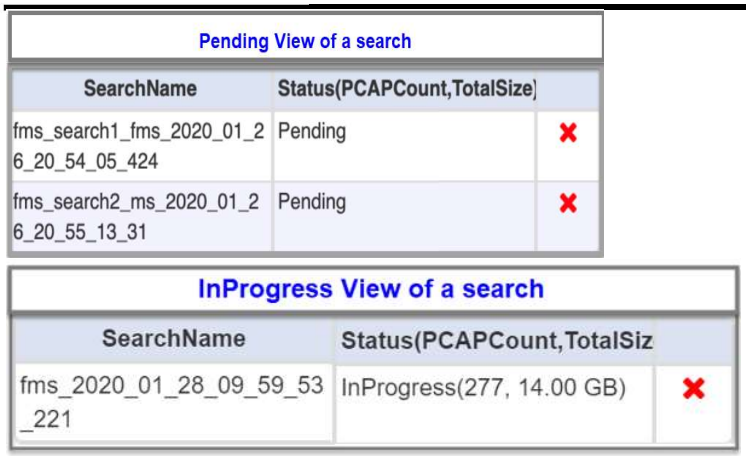


Figure 60-Search InProgress screen



Pending View of a search

SearchName	Status(PCAPCount,TotalSize)	
fms_search1_fms_2020_01_26_20_54_05_424	Pending	✖
fms_search2_ms_2020_01_26_20_55_13_31	Pending	✖

InProgress View of a search

SearchName	Status(PCAPCount,TotalSiz	
fms_2020_01_28_09_59_53_221	InProgress(277, 14.00 GB)	✖

Note:

- Searches are split into 64MB PCAPs for ease of downloading and viewing by tools such as Wireshark. For small searches, the search may be completed before the status changes from InProgress… to include the pcap count. For larger searches, user will see the count and the search size in bytes go up while the search is in progress.
- Multiple searches can be in progress simultaneously.
- Clicking on **X** cancels a search in progress. It can then be deleted from **Completed** searches tab**.**

- **Delete All Searches**- This button allows the user to delete **ALL** searches across all nodes of all selected groups. This action is not reversible.

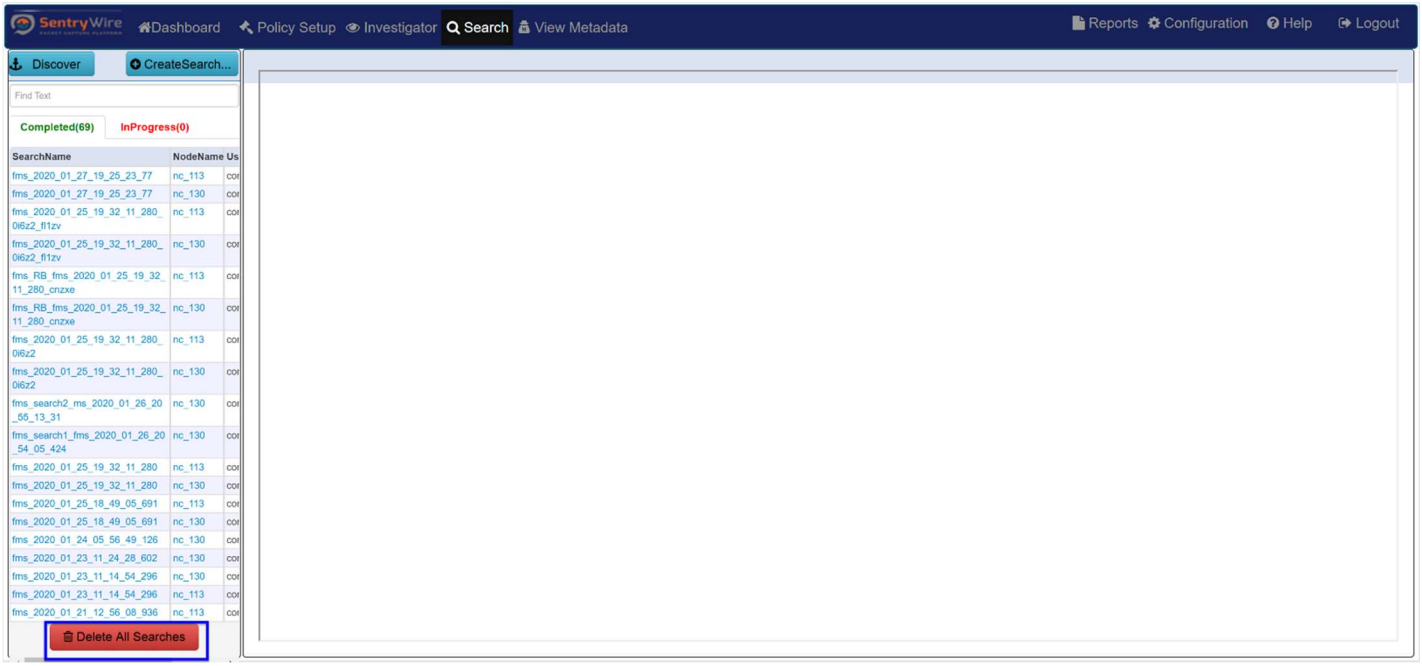


Figure 61-Delete All Search screen and button

2. Right panel allows the user to:

- View and analyze the search streams and packets, objects extracted, and, manage a specific search.
- To view search streams, simply click on a search. This displays the **Streams List** available for the search selected.
- The **Streams view** is further divided into a **Packet list** and **Stream info** sections.
    - Clicking on a particular stream displays packet data within the selected stream along with the stream info (the Follow TCP|UDP Stream view of the selected stream) **Note**: **Packets list** and **StreamInfo** are not populated until a stream from this list is selected.
    - Once a stream is selected from the Streams list, the packets belonging to this stream are displayed in Packets list as shown the picture below.

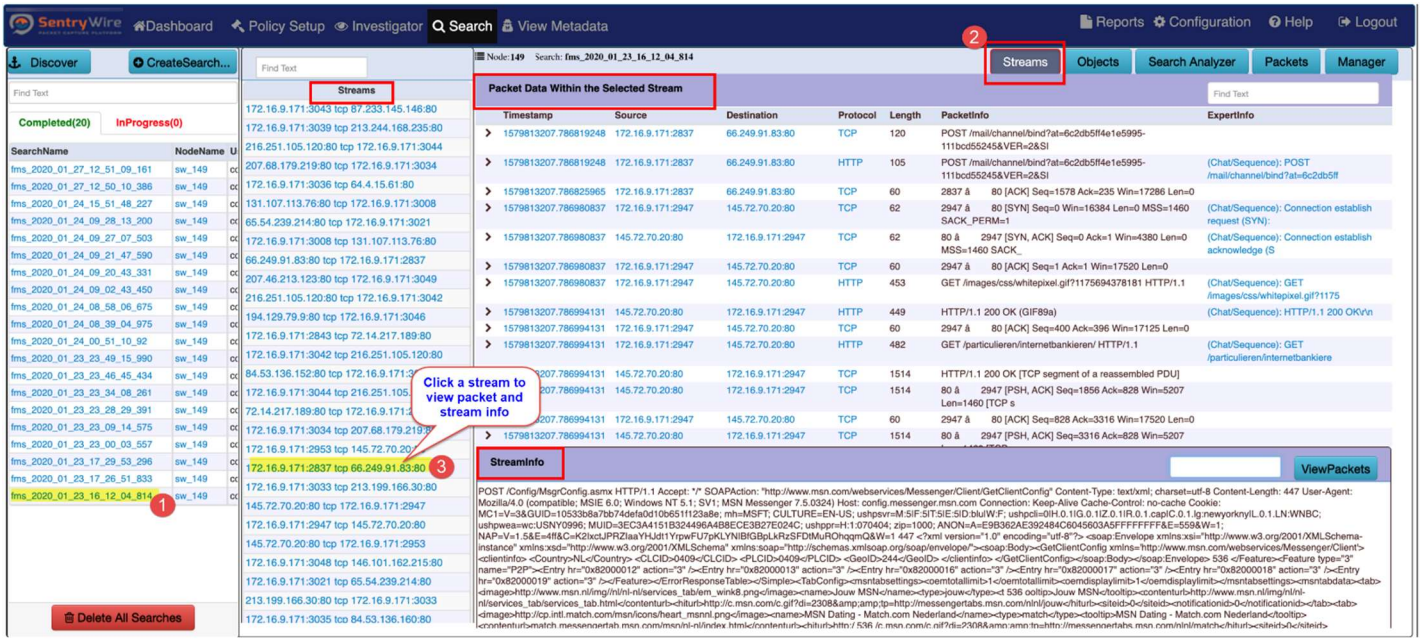


Figure 62-Search Stream view

- Several column data have been hyperlinked.
    - Clicking on any hyperlinked info takes to the All Packet view for further analysis.
    - Clicking on a packet's Timestamp hyperlink in this column will pivot to Packets tab to display all the packets with the same timestamp.
    - Clicking on a packet's Source hyperlink will pivot to Packets tab to display all the packets with the same source IP and source port.
    - Clicking on a packet's Destination hyperlink will pivot to Packets tab to display all the packets with the same dest IP and dest port.
    - Clicking on a packet's Protocol hyperlink will pivot to Packets tab to display all the packets with the same Protocol.
- The Find Text input area allows the user to find packets with the supplied text within the Packets list. This will not pivot to Packets tab.

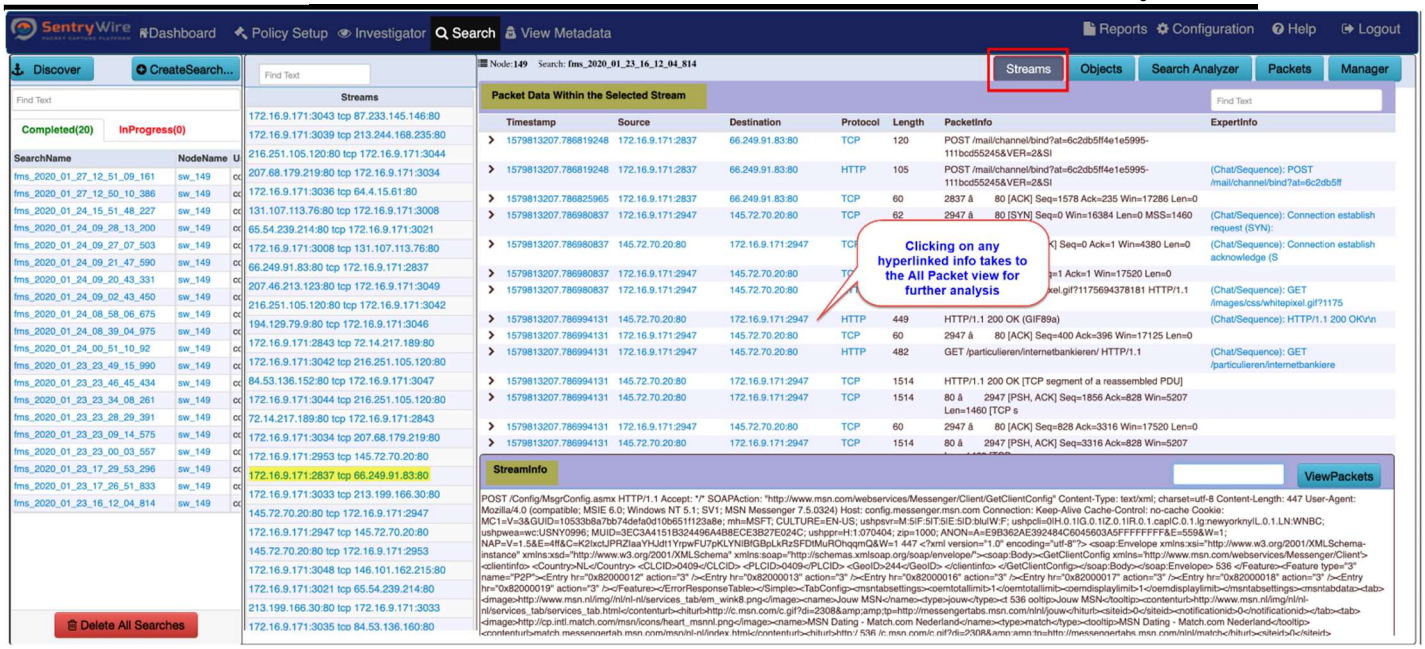


Figure 63-Search Screen Packet Data within Stream view

- Clicking on the View Packets button allows the user to view packet details of a selected stream for a specific text of interest. This Packet view is more focused on the packet data which contain the search string as requested by the user.

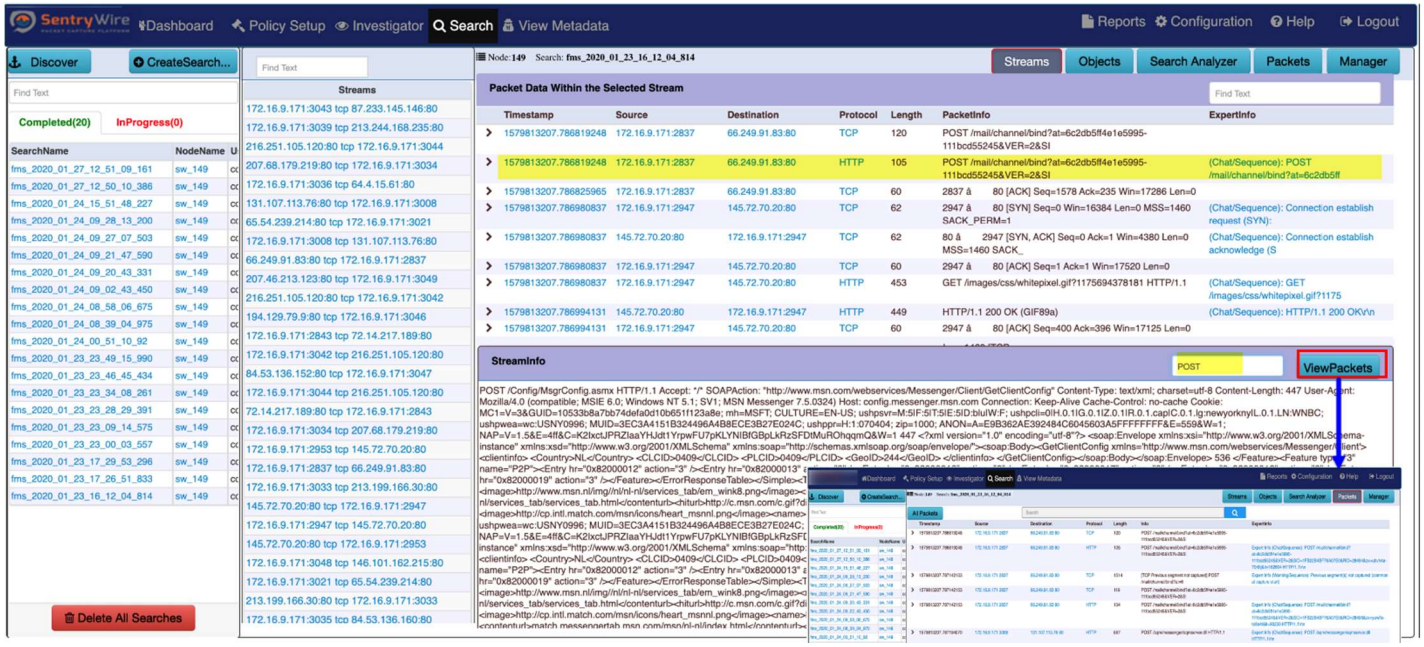


Figure 64-Search View Packets button

- **Objects Button**: Clicking on the **Objects** button for a search displays the object info including the FileName, Size, MD5 and View action.

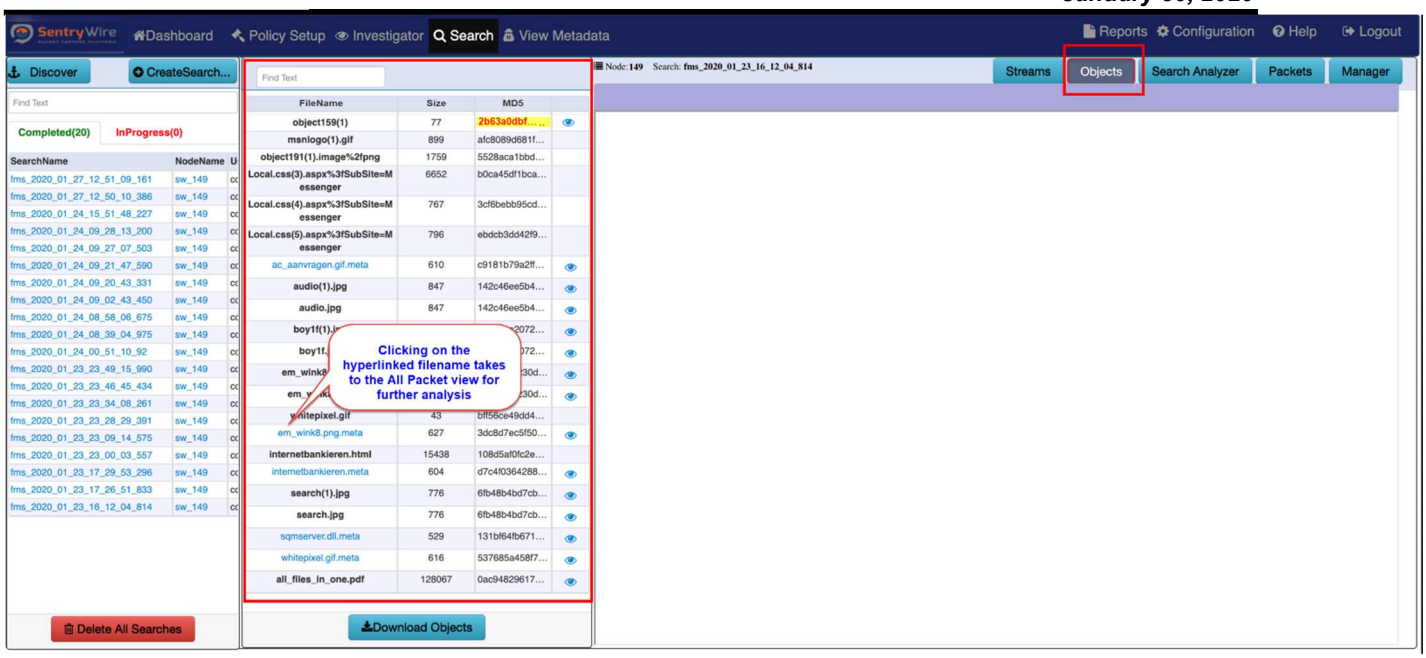


Figure 65-Search Object button

- If a file name is hyperlinked, clicking on the link will pivot to Packets View to show the packets that are related to the hyperlinked file.
- The MD5sum value of the file is displayed in red color and hyperlinked if the md5sum matches one of the known bad md5sum values uploaded via Policy→ Augmentation → Malware. Clicking on this hyperlink will display corresponding description of the MD5sum entry.
- Clicking on View icon allows the user to view the extracted object as a pdf (if it is viewable)

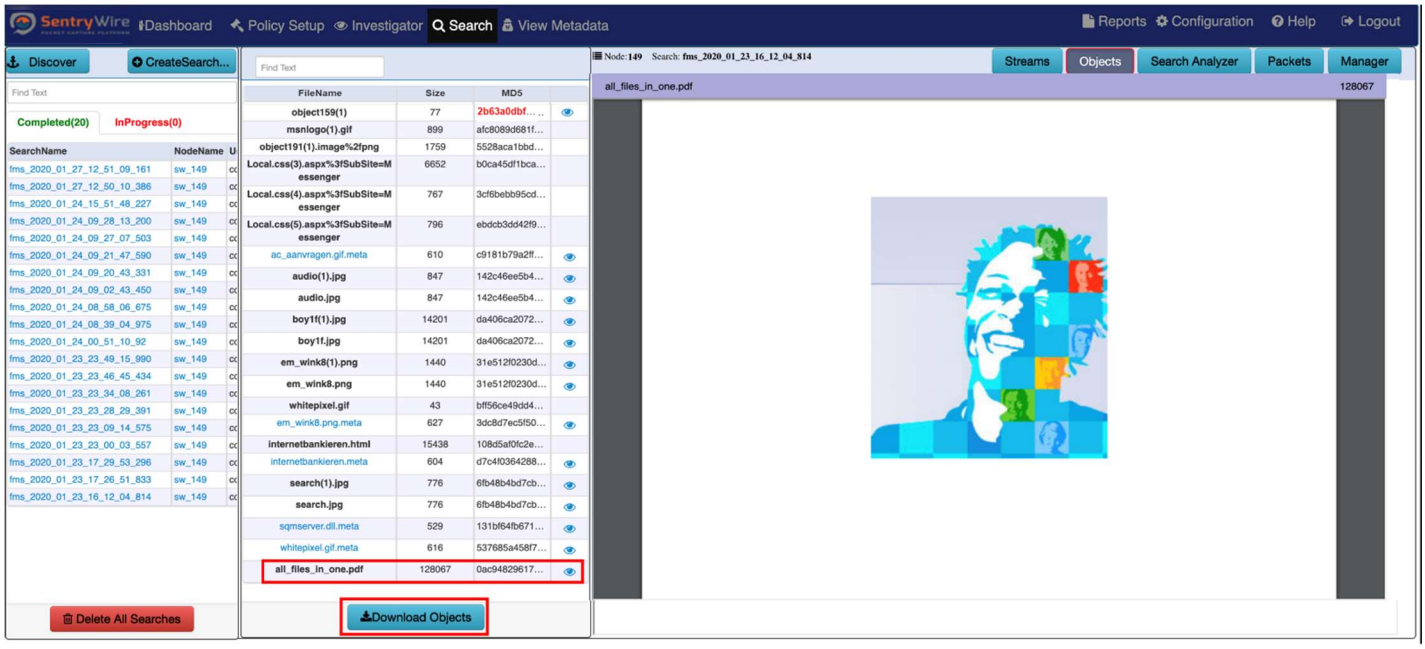


Figure 66-Search Download Objects button

- Clicking on Download Objects button downloads the zip file that contains the raw files as they are extracted.

- **Search Analyzer button:** Clicking on the Search Analyzer button displays the Kibana investigator that shows all metadata related to the selected search.

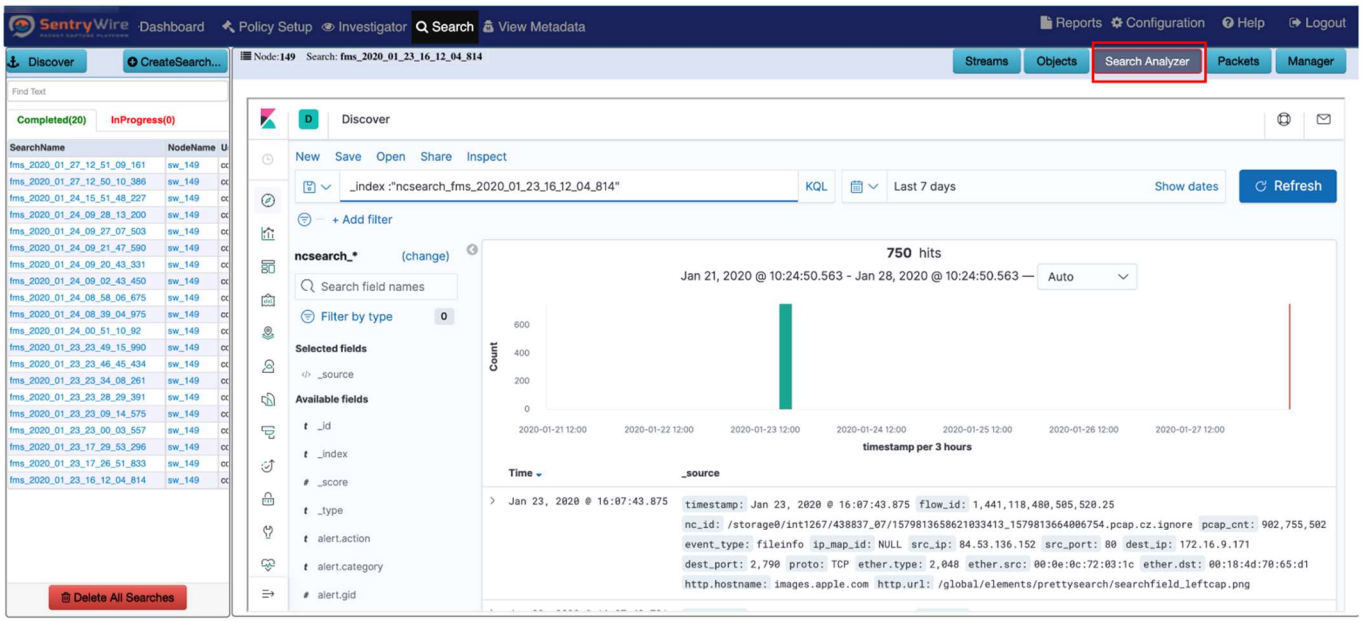


Figure 67-Search Analyzer Button

- The default view filter is the selected search name only.
- To search for a specific metadata type, add the type to the filter

For example:
The following change will show only the **38** file events(out of **750** total events of all types) that belong to the search being analyzed.

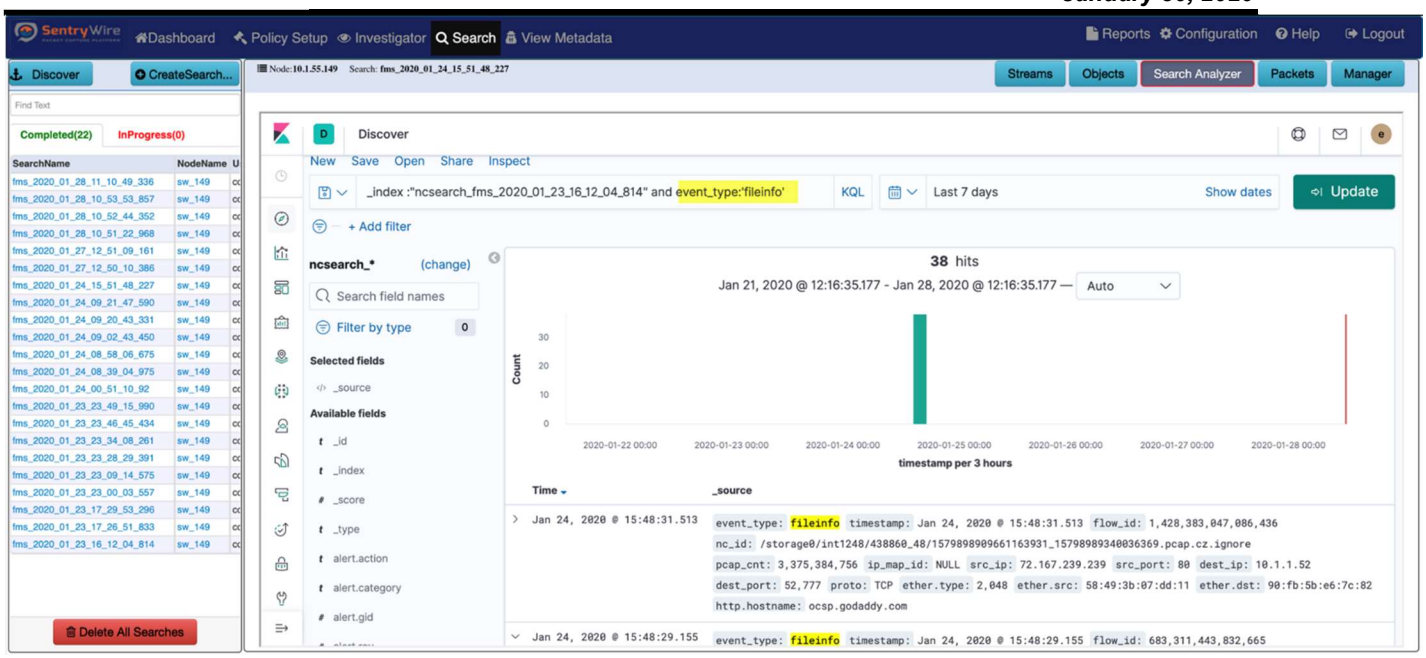


Figure 68-Search Analyzer Results view

The following types of metadata are available for analysis and discovery through Kibana:

Event Type	KQL Search Filter
Alert	event_type:'alert'
File	event_type:'fileinfo'
DNS	event_type:'dns'
SMTP	event_type:'smtp'
ActiveTrigger	event_type:’activetrigger’
HTTP	event_type:'http'
TLS/SSL	event_type:'tls'
SMB	event_type:’smb’
VOIP	event_type:’voip’
Suspicious IP Alerts	event_type:’suspip’
Suspicious Signature Alerts	event_type:’ja3’
Suspicious Domains	event_type:’suspdomain’

- **Packets** button: Clicking on the **Packets** button displays the first page of packets of the search. If the search contains multiple pages of packets, each page can be viewed one after the other. The user can also switch to a specific page before going to next page or previous page.

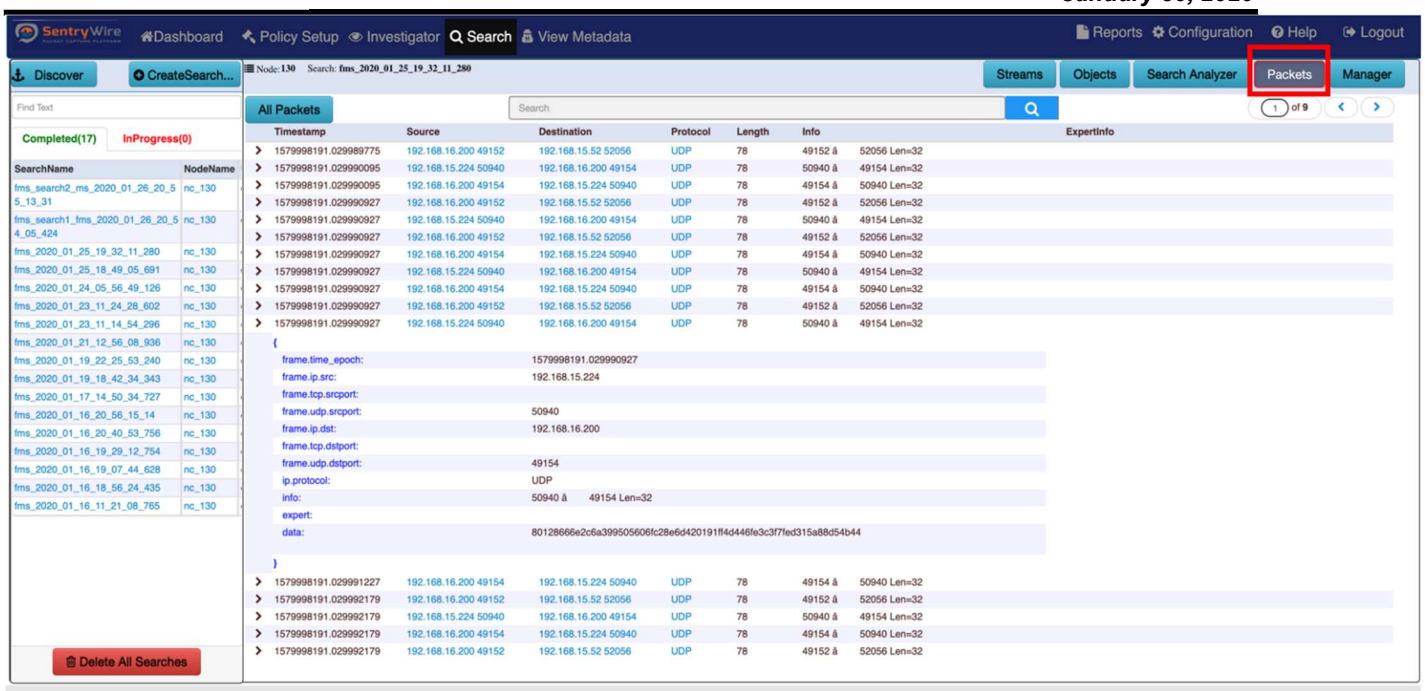


Figure 69-Search Packets results

- Clicking on the Search bar allows free form text search for packets. In the image below, the search string is Application.

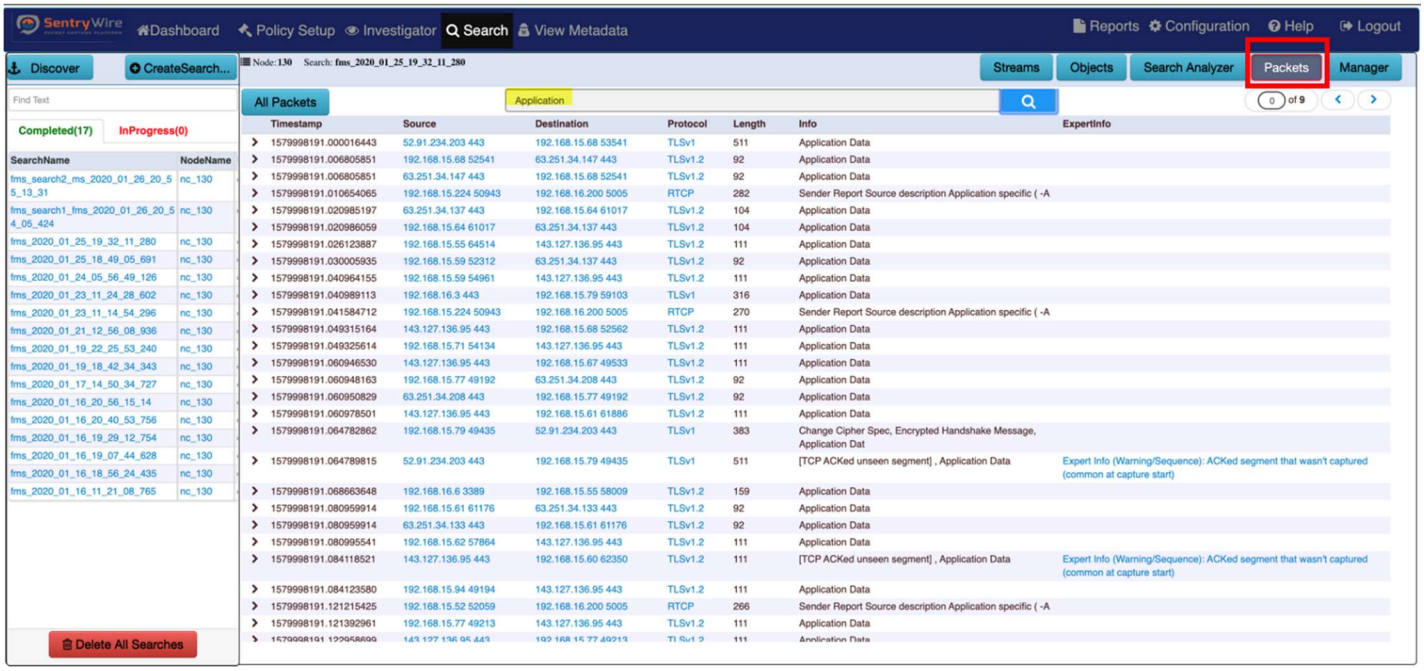


Figure 70-Search Packets Search Bar

- Clicking on All Packets button reverts to display all packets.
- Clicking on Source or Destination hyperlink displays all packets with IP and port matching the ones selected. In the example below, clicking on the hyperlinked source (192.168.16.3 443), displays all packets that have IP address 192.168.16.3 and port 443.

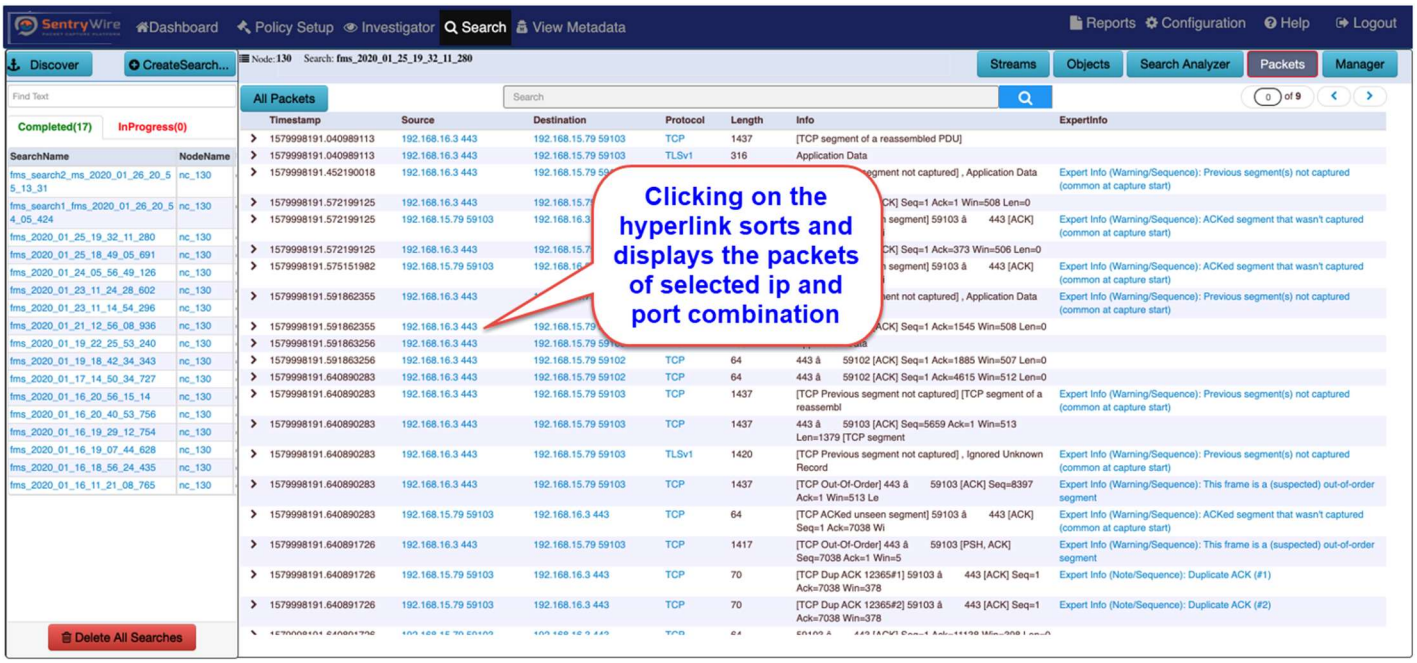


Figure 71-Search Packets Results Source or Destination

- Clicking on a packet's Protocol hyperlink displays all packets with the same protocol. In the following example, all packets with protocol TLSv1 or TLSv1.2 are displayed.

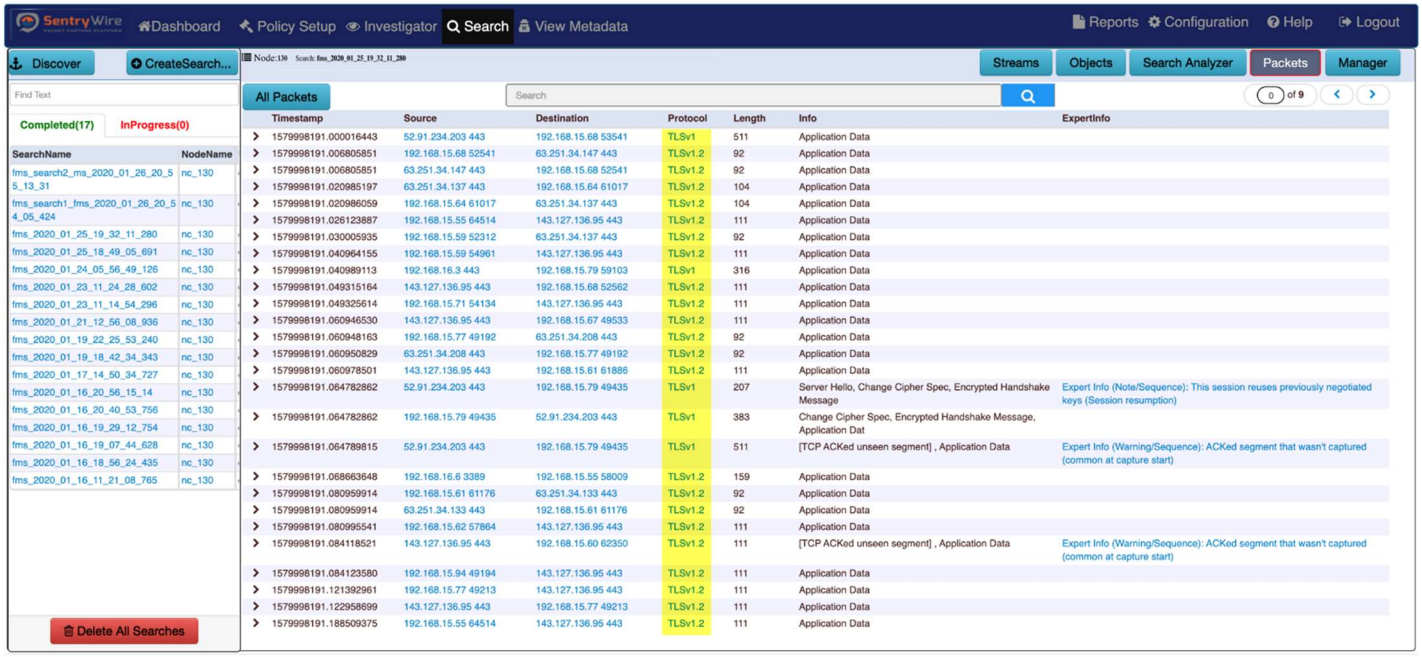


Figure 72-Search Packets Results Protocols view

- **Manager** button: Clicking on the **Manager** button displays the search details of the search including UserName, SearchName, BeginTime, EndTime, Duration, SearchFilter and Results.

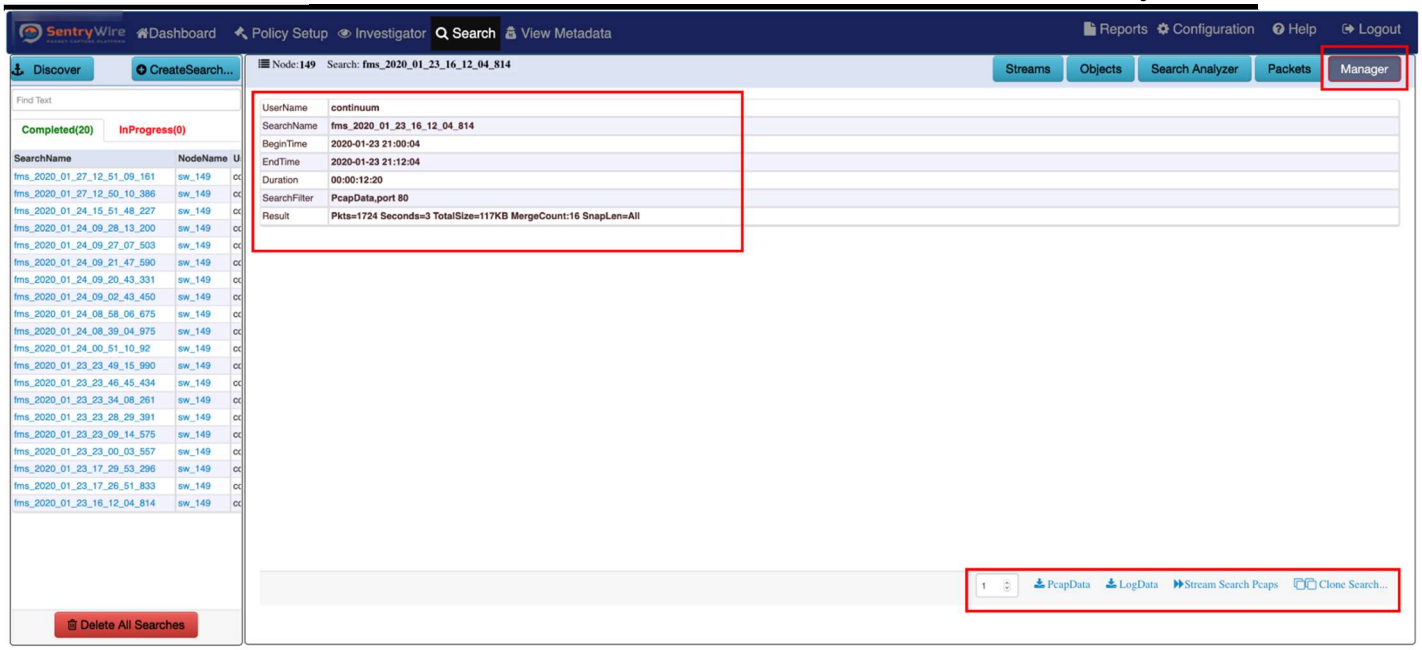


Figure 73-Search Manager Button view

The links at the bottom are as follows:

- **PcapData link**: This link allows the user to view/download the PCAPs available for the respective search. Select a pcap number and choose PcapData link to download the specified pcap.
- **LogData link:** Clicking on this link downloads a zip file of the metadata of the search.

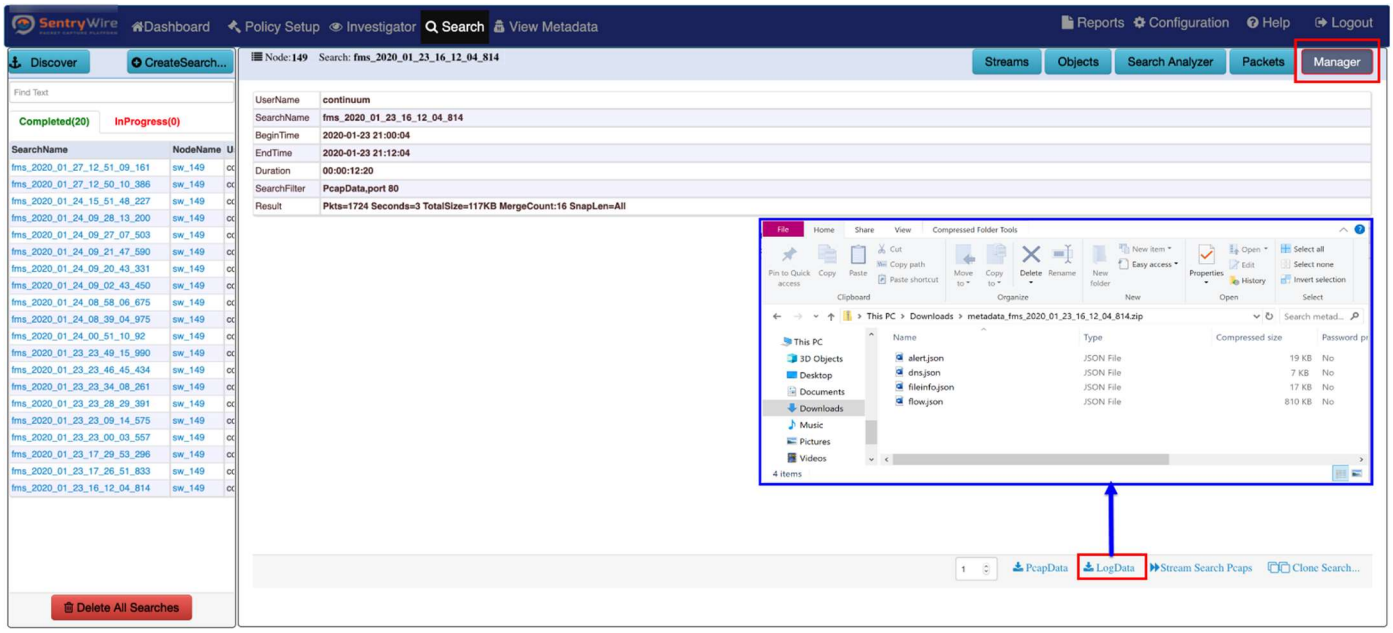


Figure 74-Search Packets Manager LogData results

- **Stream Search PCAPs link**: Clicking on this link allows the user to stream pcap data of the search to an external interface, for other applications to further analyze

the data. Stream Search Results option checkbox is available under "**Create Search**". Search Results can also be streamed after the search is completed. The results of a stream search are logged and available as part of metadata zip file.

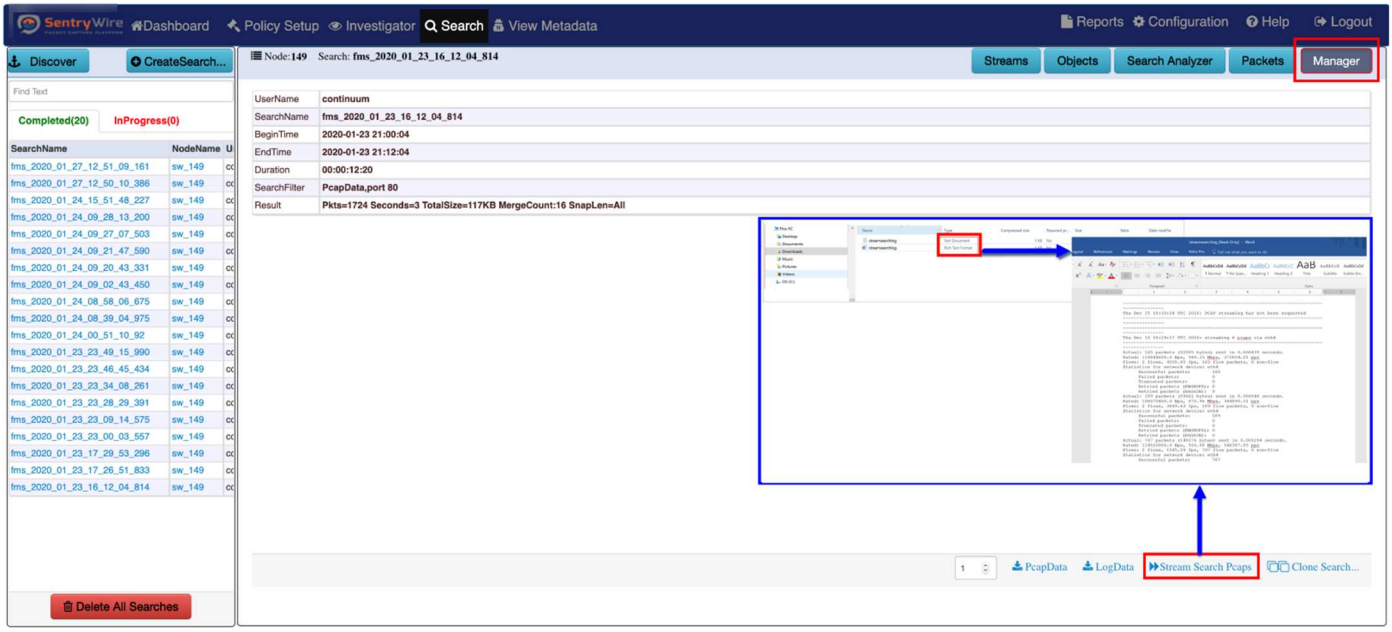


Figure 75-Search Manager Button Stream Search PCAPs view

- **Clone Search link:** Clicking on this link allows the user to recreate or clone the search. The new search name by auto filling the search parameters. The new search name is appended with a unique tag in the end in order to separate it from the original search. Begin/End Time, Search Filter are copied from the selected search. The user can modify any of these fields before submitting a clone search request.

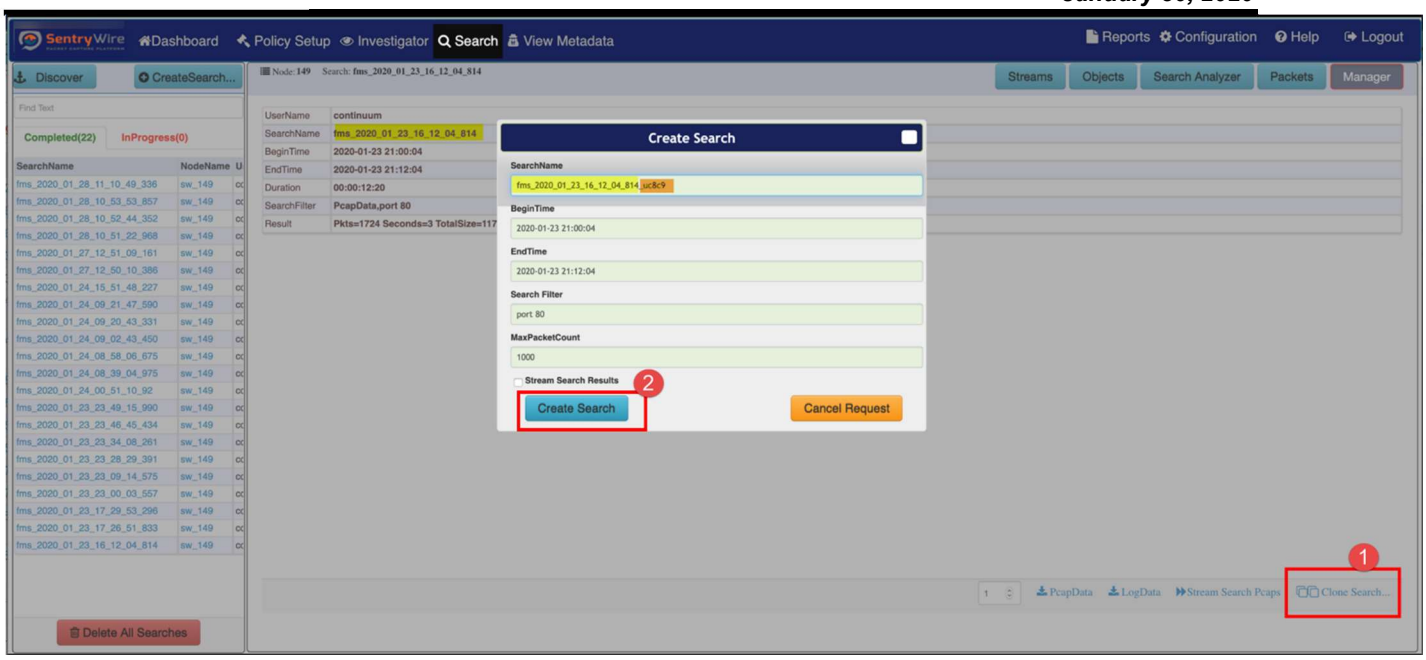


Figure 76-Search Manager Button Stream Clone Search view

8.2 CREATING A NEW SEARCH

- To create a new search, click on **CreateSearch** button. This will pop up Create Search dialog.

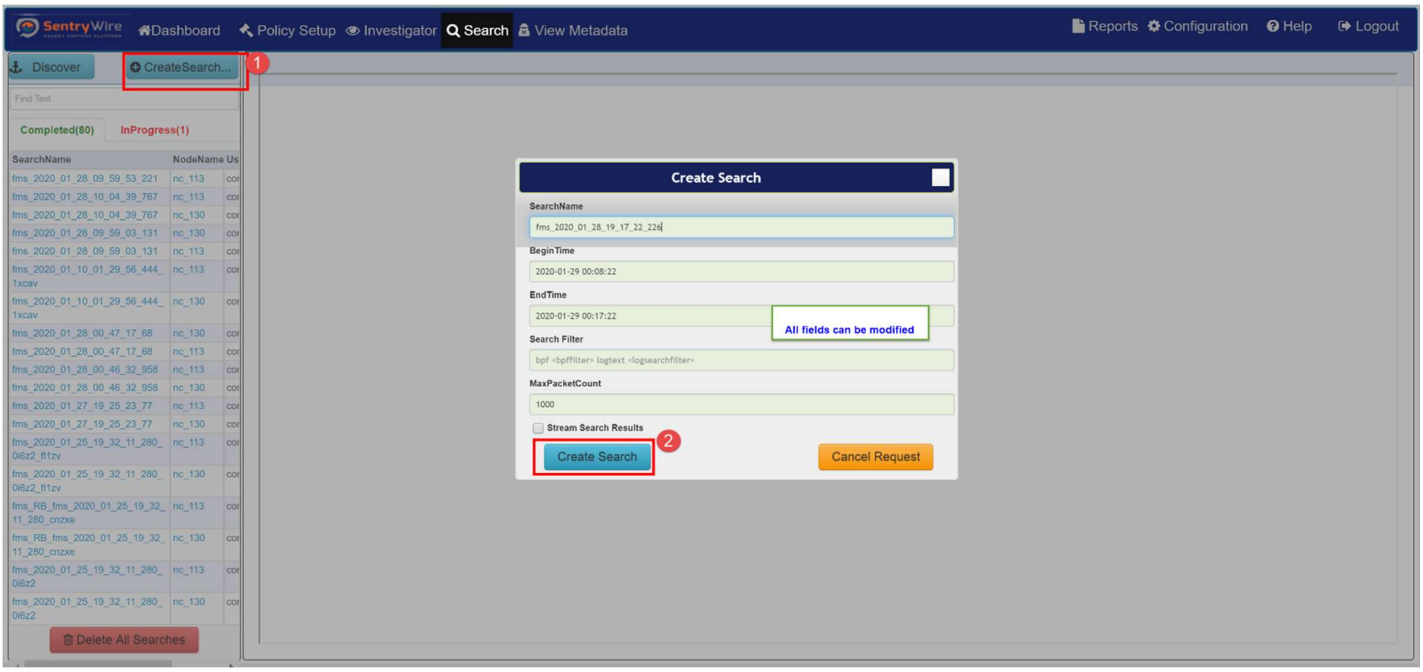


Figure 77- Search Create New Search view

- The SearchName field is auto filled but editable.

- Provide a value or change the defaults for the begin time and end time. The begin time field is auto filled to be 4 minutes prior to the current UTC time. The end time field is auto filled to be the current UTC time. The user can change them as needed.
- The Search Filter can be specified as a **bpf** or log**text or both.**
    - Enter a valid bpf packet filter following the keyword **bpf. (For more information on bpf filters refer to Appendix D)**
    - Enter text search string following the keyword **text**
    - If search string has bpf and text strings, **bpf** must precede **text**
    - If neither keyword is entered, the search filter is taken as a bpf string.

The following are examples of some **valid** search strings:

bpf port 80 text hello

IP host 192.168.0.1

tcp or udp text hello

port 80 text hello

text hello

The following are examples of some **invalid** search strings:

Hello

text hello port 80

blah hello

bpf weqrwr

- The MaxPacketCount field allows the user to specify the packet count as desired for a search within a specific timestamp. To get all packets for a particular timestamp the max packet count must be set to 0.
- **Stream Search Results** checkbox when checked, allows the user to stream search results to an external interface, for other applications to further analyze the data. Search Results can also be streamed after the search is completed.

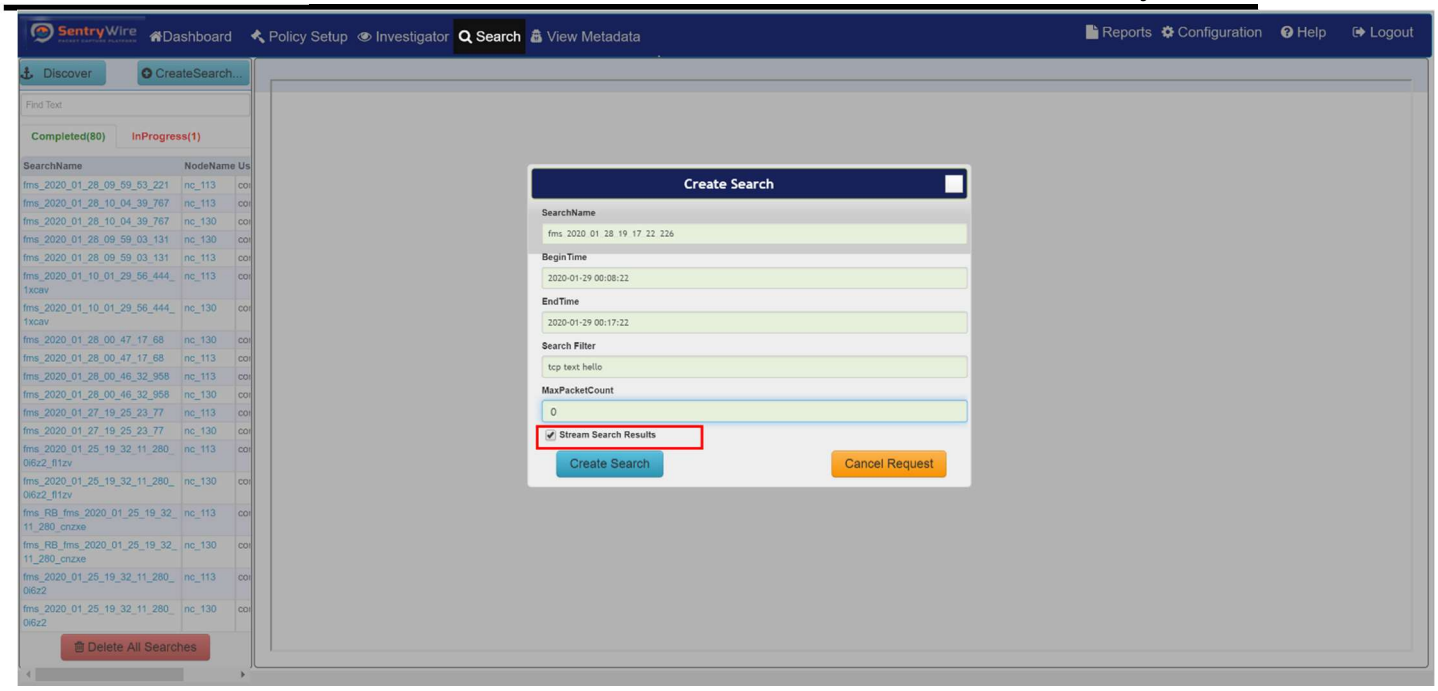


Figure 78-Stream Search Results button

- Once all the details are provided, click on **Create Search** button to create a search.
- The search created can be seen under the Pending searches tab while in progress. A pending or InProgress search can be cancelled at any time.
- Once completed the search appears under the completed search tab for further analysis.

- **Note**: If no group is selected the search request goes to all groups/nodes in the federation

9 VIEW METADATA

The application collects, analyzes, stores and reports on network security log events from each included federated node to help monitor threats, attacks and security breaches. This application engine provides useful information by converting raw events from network and security devices, servers and operating systems, applications, endpoints and more into actionable, investigable intelligence data.

The View Metadata screen presents the user with several menu tabs. Clicking on each tab and selecting the desired node, displays the corresponding details for the selected node.

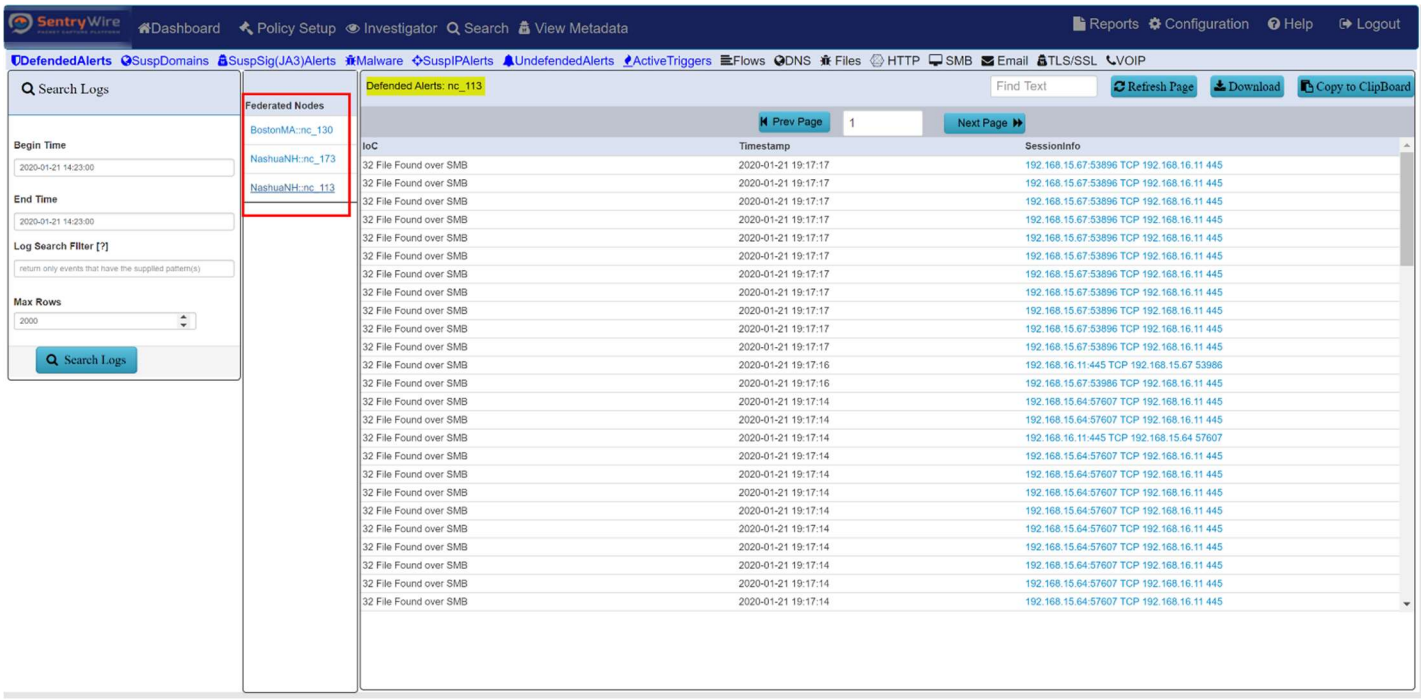


Figure 79-View Metadata screen view

- The "**Find Text**" option allows the user to enter a desired string to specify the type of event or alert message the user is interested in. This will display the messages containing the specified search text string only. If there is text entered in "Find Text" box, the text must be cleared for all the data to be displayed.

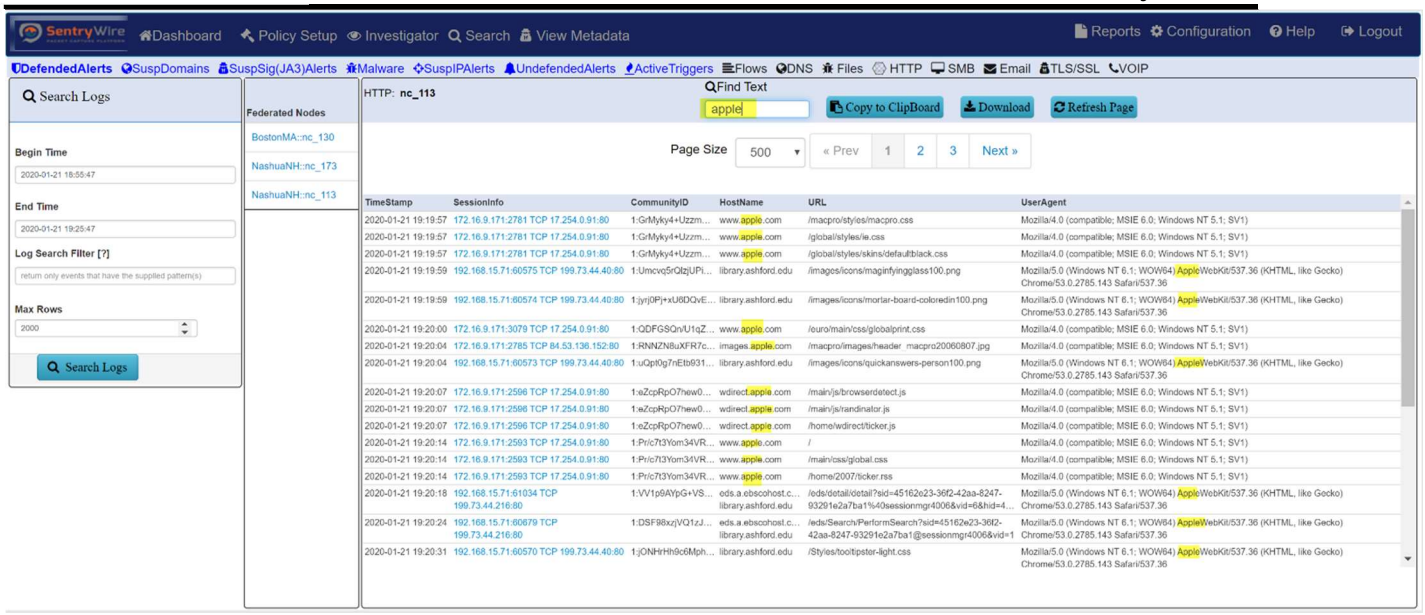


Figure 80-View Metadata Find Text Option view

- The "**Copy to Clipboard**" option allows the user to copy the entire event/message display to any location or application allowing the user to share the information via email for reporting or recording purpose.

- The **"Download"** option allows the user to download data to help record and monitor both existing and new events, threats, alerts and rules to maintain uninterrupted log source data collection and storage. This can be done by clicking the download button on the top allowing the user to download the data in a .csv format.

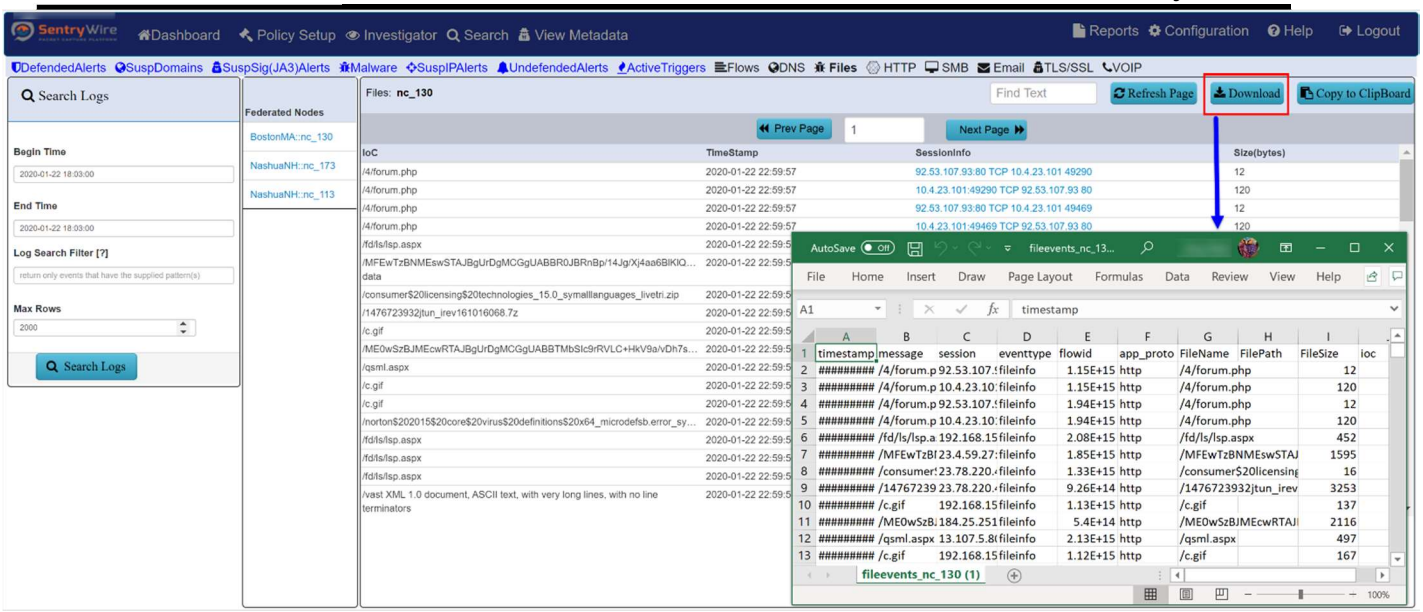


Figure 81-View Metadata Download Button view

- The "**Refresh**" option allows the user to retrieve the most recent event data from the server for display. Note: This is the only way to bring in the most recent event data associated with the tab option selected. This retrieved data remains current as the user navigates through different option tabs allowing the user to investigate multiple tabs at a time. In order to view the current event data the user must click refresh for each tab option within that tab.

- The "**Page Size**" option allows the user to choose the number of rows the user would like to see in one page. By default this count is 500. When the user selects a different display count the number of pages change accordingly. User can easily navigate through pages by scrolling through previous or next page option or clicking on the desired page number.

- The "**Search Log**" option allows the user to display alerts and events within the specified range of time. It also allows the user to specify a log search filter for a more specific search within the logs. User needs to click refresh again to see the current events.

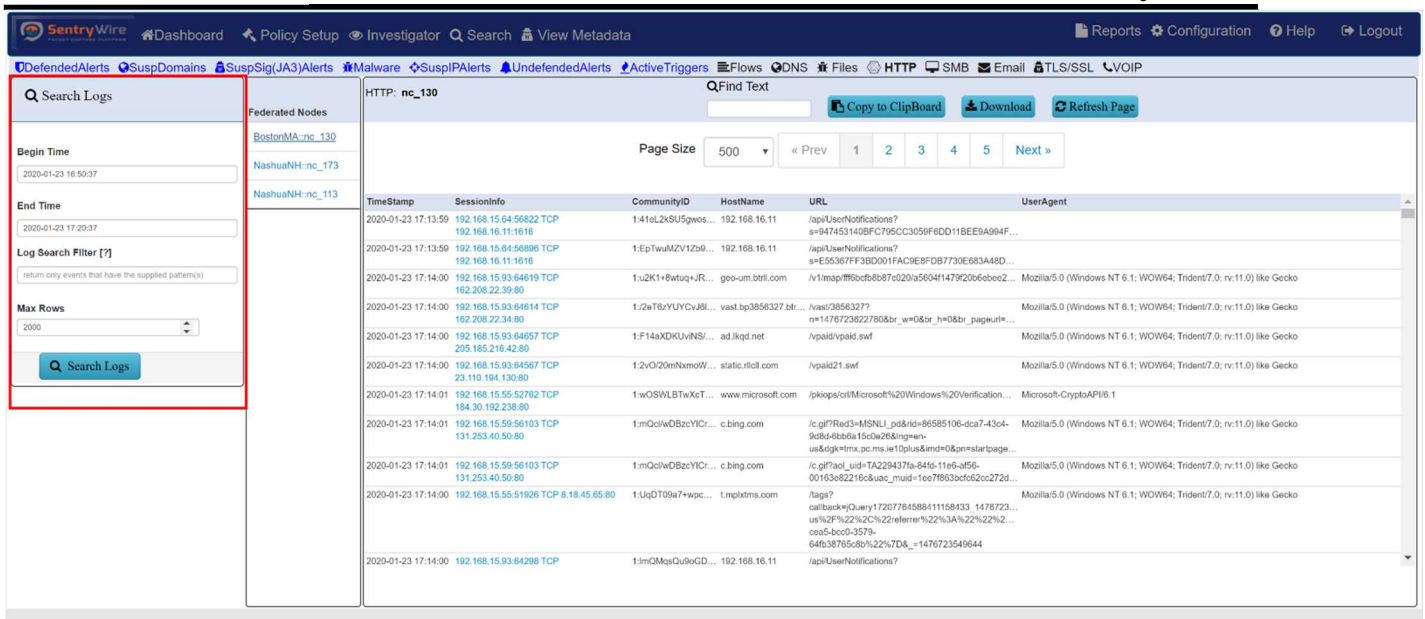


Figure 82-View Metadata Search Logs Function view

9.1 DEFENDED ALERTS

The FM displays alerts generated due to a rule for each node in the federation, only if the alert's source or destinationIPaddress is a defended asset **AND** the alert's source or destination port is a defended service.

Note: The defended asset and defended service that are assigned by the "Policy Setup" tab from FM are global and apply to all nodes. (For more information refer to section 4.1 and 4.2)

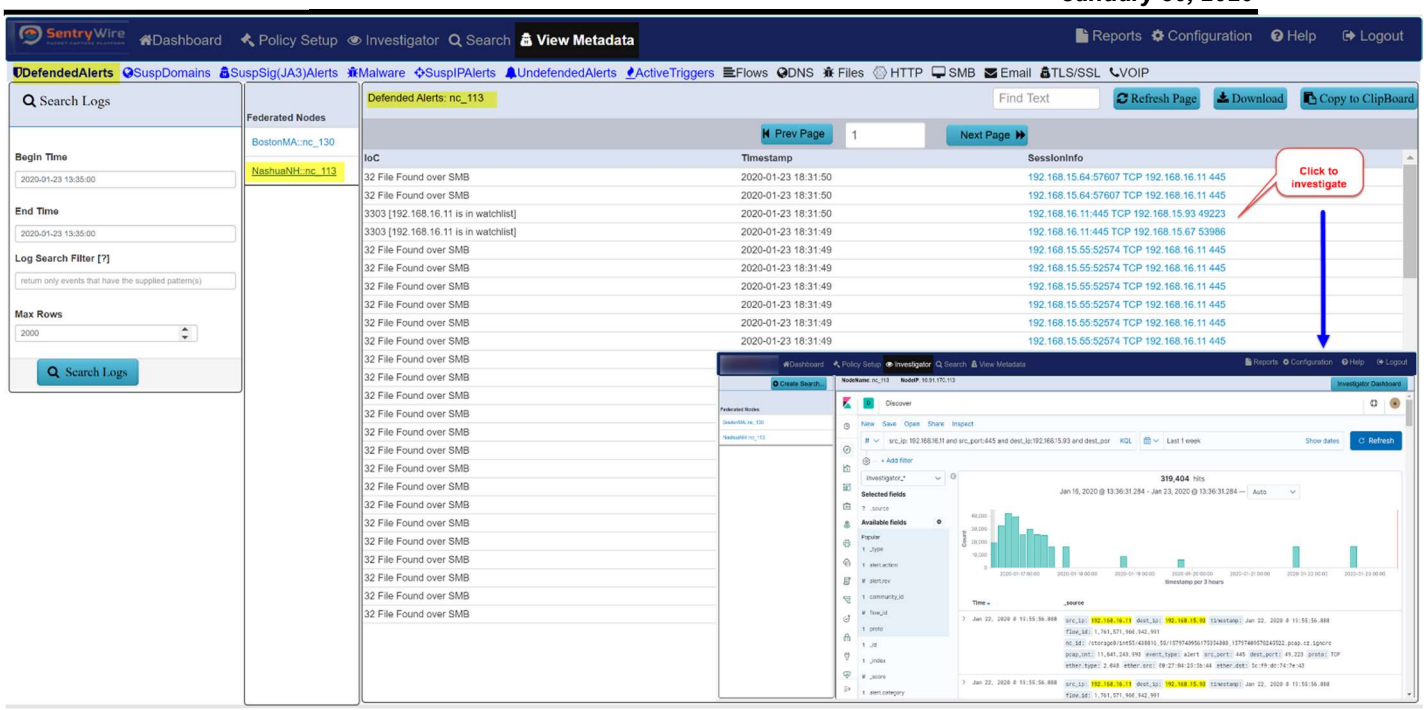


Figure 83-View Metadata Defended Alerts view

- Clicking on the hyperlinked sessioninfo pivots to the investigator screen that shows the events with the same 5 tuple information for further analysis.

9.2 SUSPDOMAINS

The SuspDomains alerts are generated when a domain from DNS event is one of the suspicious domains that have been uploaded via the Policy→ Augmentation→Suspicious Domains list. Clicking on the hyperlinked sessioninfo pivots to the investigator screen that shows the events with the same 5 tuple information for further analysis.

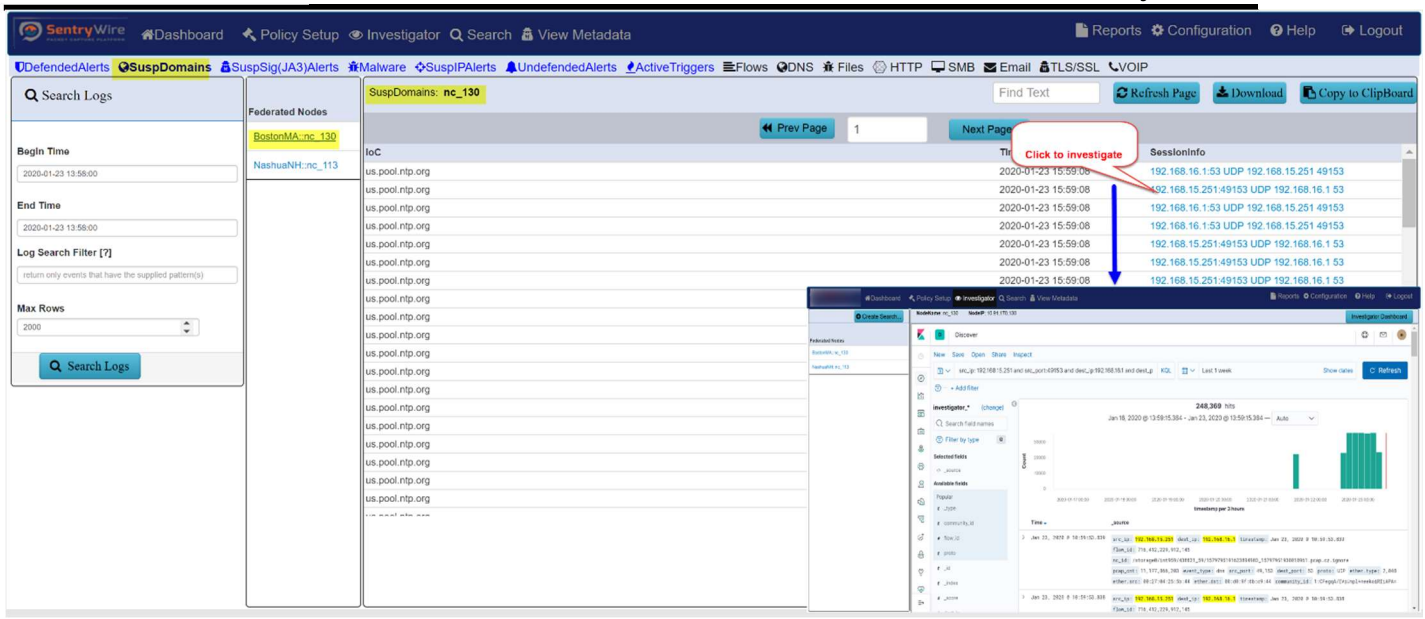


Figure 84-View Metadata SuspDomains Function view

9.3 SUSPSIG(JA3)ALERTS

The SuspSig(JA3) alerts are generated when JA3 hash of the TLS event matches with one of the JA3 hash values uploaded via the Policy→ Augmentation→Suspicious TLS/SSL Signatures list.

Clicking on the hyperlinked sessioninfo pivots to the investigator screen that shows the events with the same 5 tuple information for further analysis.

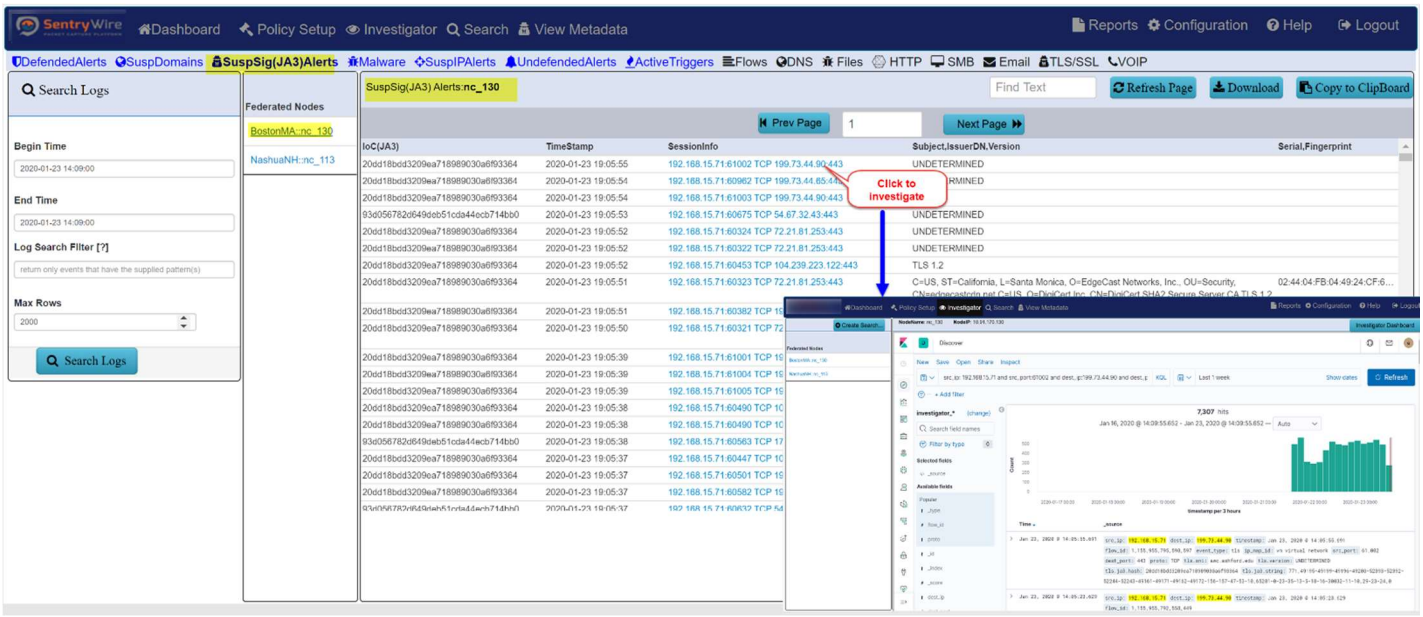


Figure 85- View Metadata SuspSig(JA3) Alerts view

9.4 MALWARE

The Malware alerts are generated when a MD5 value of an object produced by a search matches one of the MD5 values uploaded via the Policy→ Augmentation→Malware list.

Clicking on the hyperlinked IoC pivots to the investigator screen that shows the matching MD5 information for further analysis.

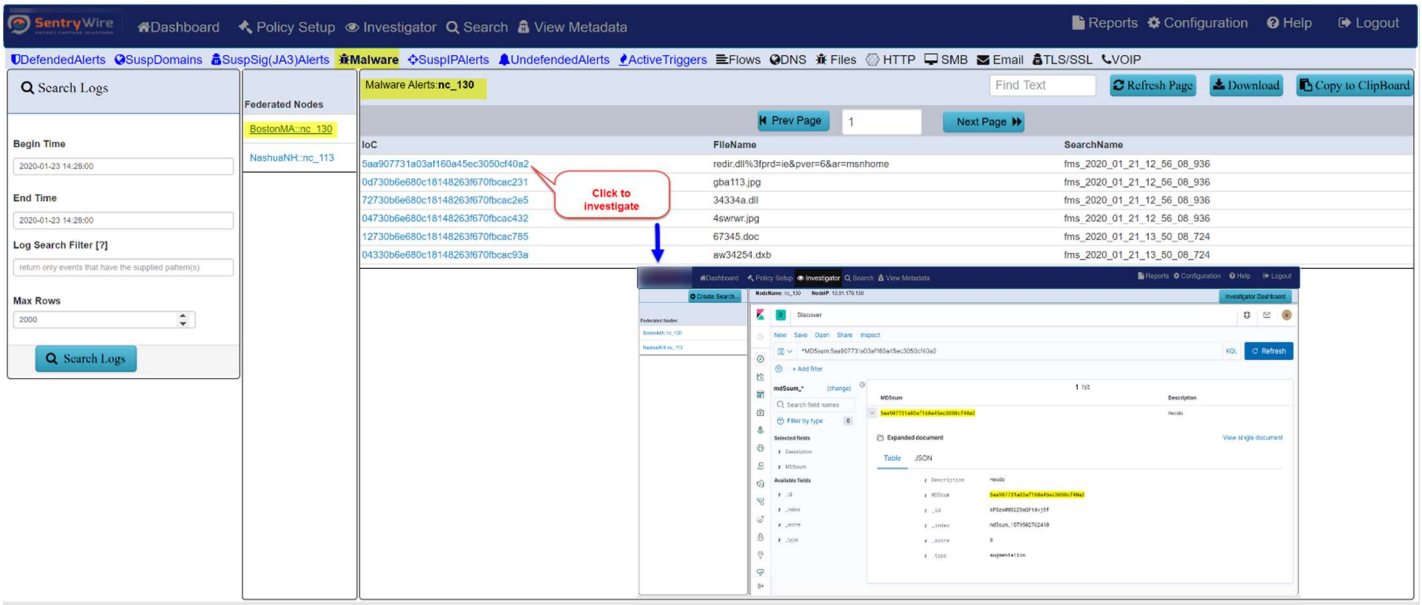


Figure 86-View Metadata Malware Alerts view

9.5 SUSPIPALERTS

The SuspIP alerts are generated when an IP address matches with one of the suspicious IP that have been uploaded via the Policy→ Augmentation→Suspicious IPAddresses list.

Clicking on the hyperlinked sessioninfo pivots to the investigator screen that shows the events with the same 5 tuple information for further analysis.

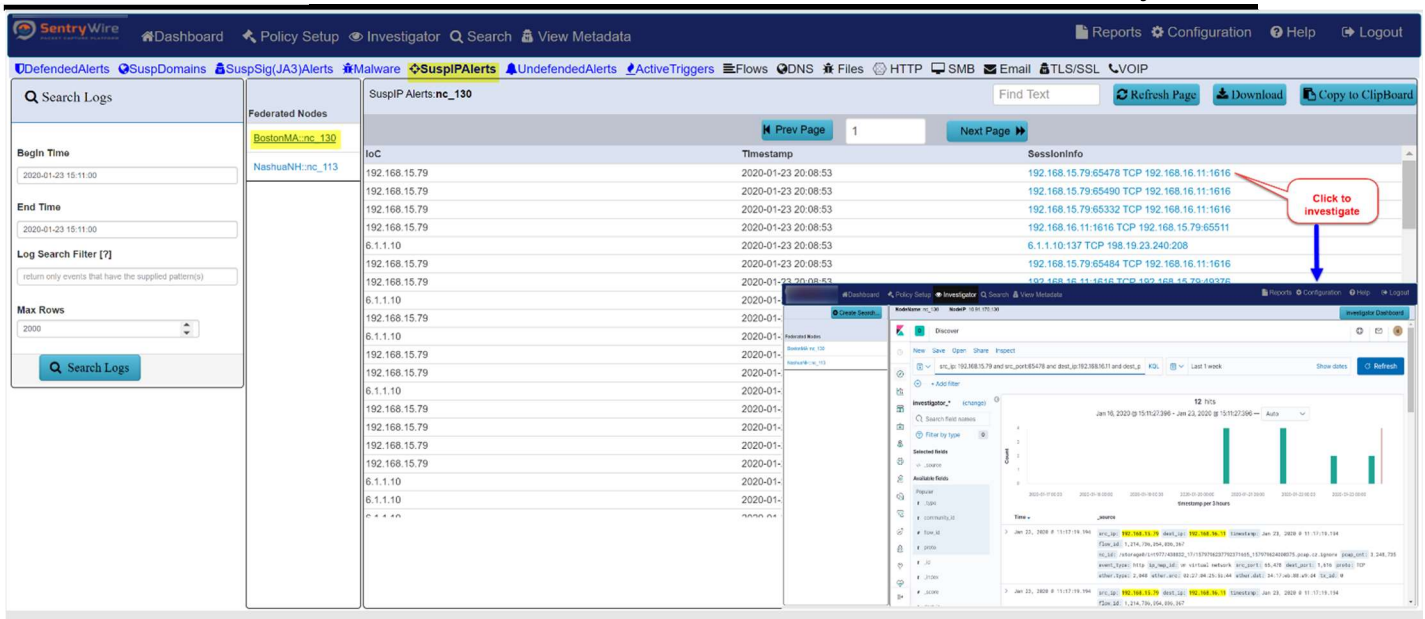


Figure 87-View Metadata SuspIPAlerts view

9.6 UNDEFENDEDALERTS

These alerts are generated when the alert's source or destinationIPaddress is **NOT** a defended asset **OR** the alert's source or destination port is **NOT** a defended service.

Clicking on the hyperlinked sessioninfo pivots to the investigator screen that shows the events with the same 5 tuple information for further analysis.

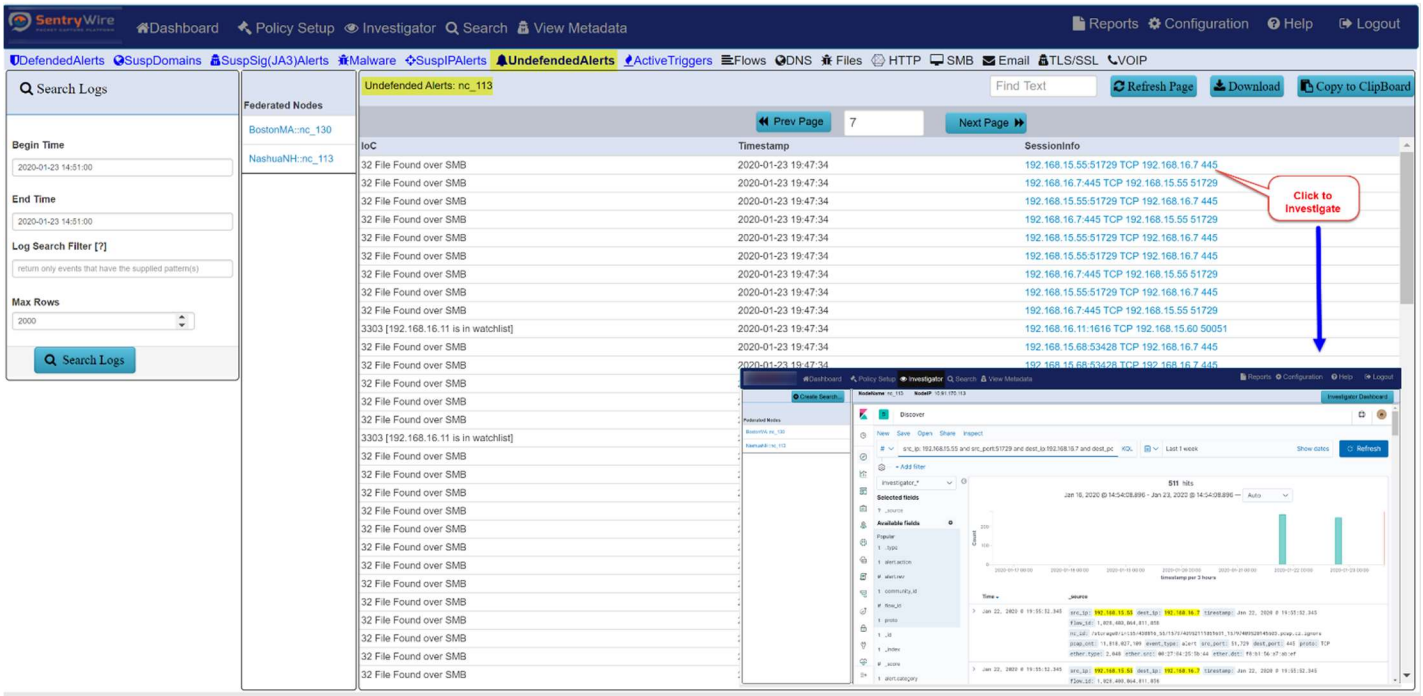


Figure 88-View Metadata Undefended Alerts view

9.7 ACTIVE TRIGGERS

The Active triggers are generated when a user specified BPF filter, through Policy Setup→ Active Triggers, causes an alert.

Clicking on the hyperlinked sessioninfo pivots to the investigator screen that shows the events with the same 5 tuple information for further analysis.

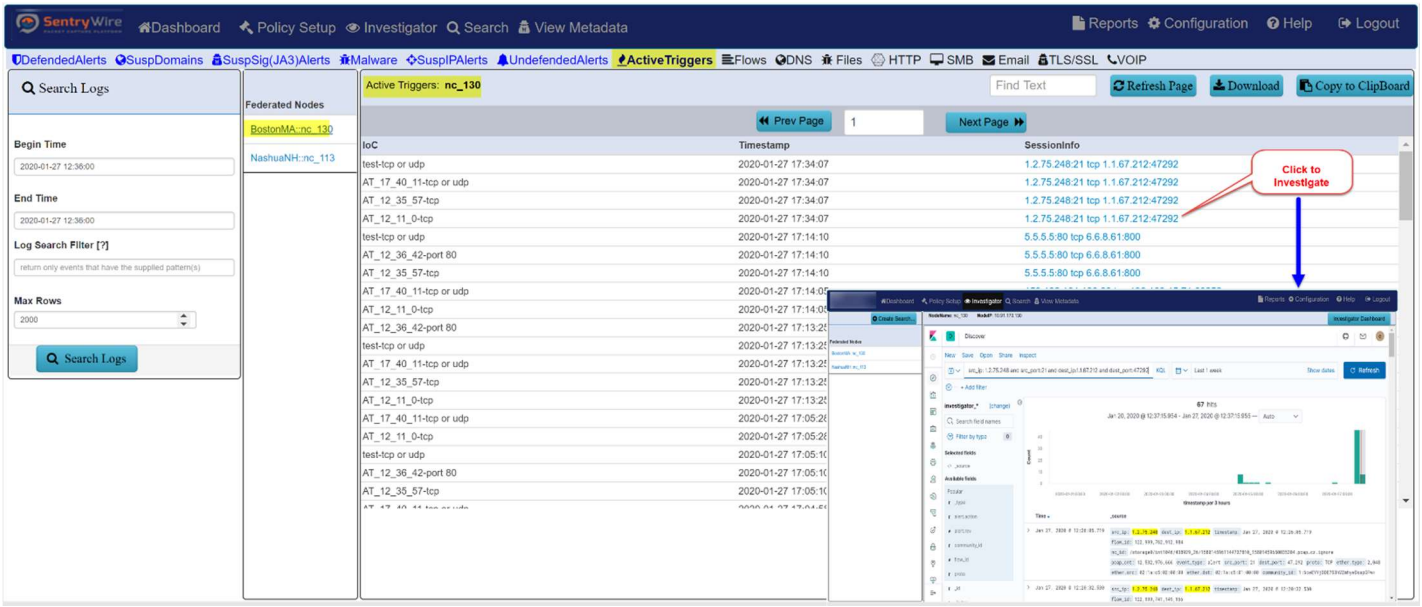


Figure 89-View Metadata Active Triggers view

9.8 FLOWS

The Flows tab shows bi-directional and one-way flows found in received network traffic for each node in the federation. FlowInfo shows community id, packet count, byte count, start time and end time of each flow. Clicking on the hyperlinked sessioninfo pivots to the investigator screen that shows the events with the same 5 tuple information for further analysis.

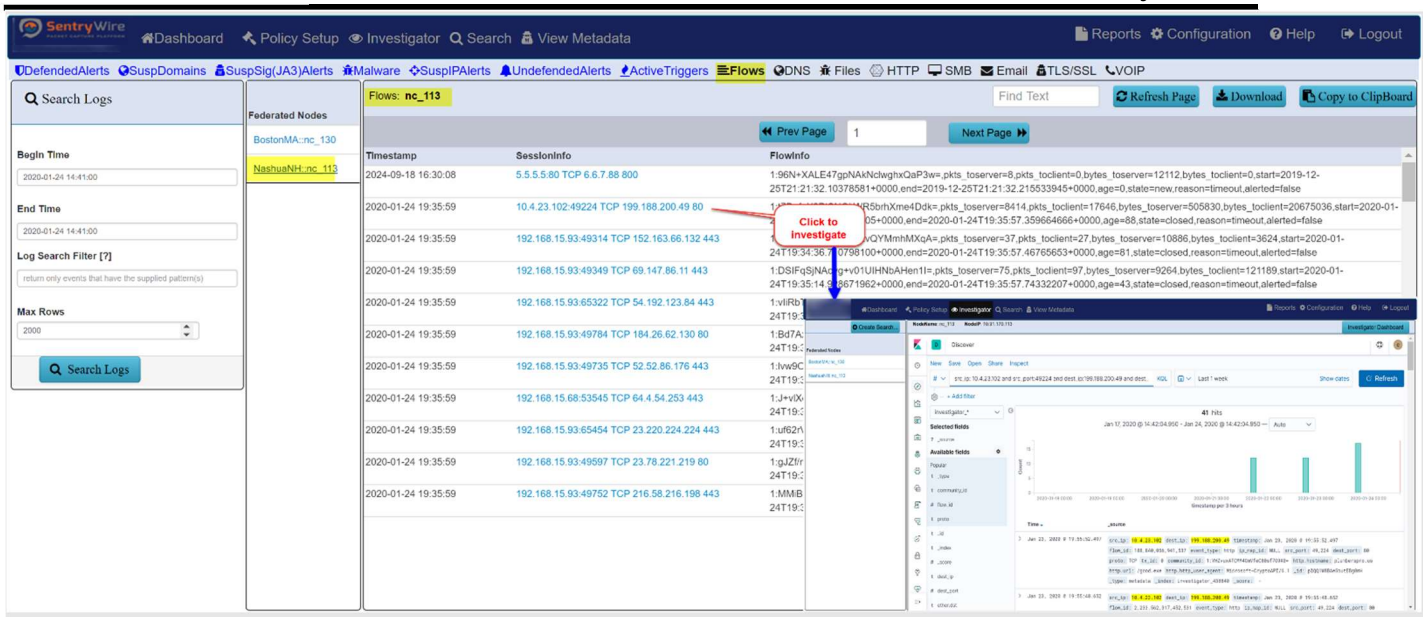


Figure 90-View Metadata Flows view

9.9 DNS

The DNS tab displays the displays DPI events for port 53.

Clicking on the hyperlinked sessioninfo pivots to the investigator screen that shows the metadata events with the same 5 tuple information for further analysis.

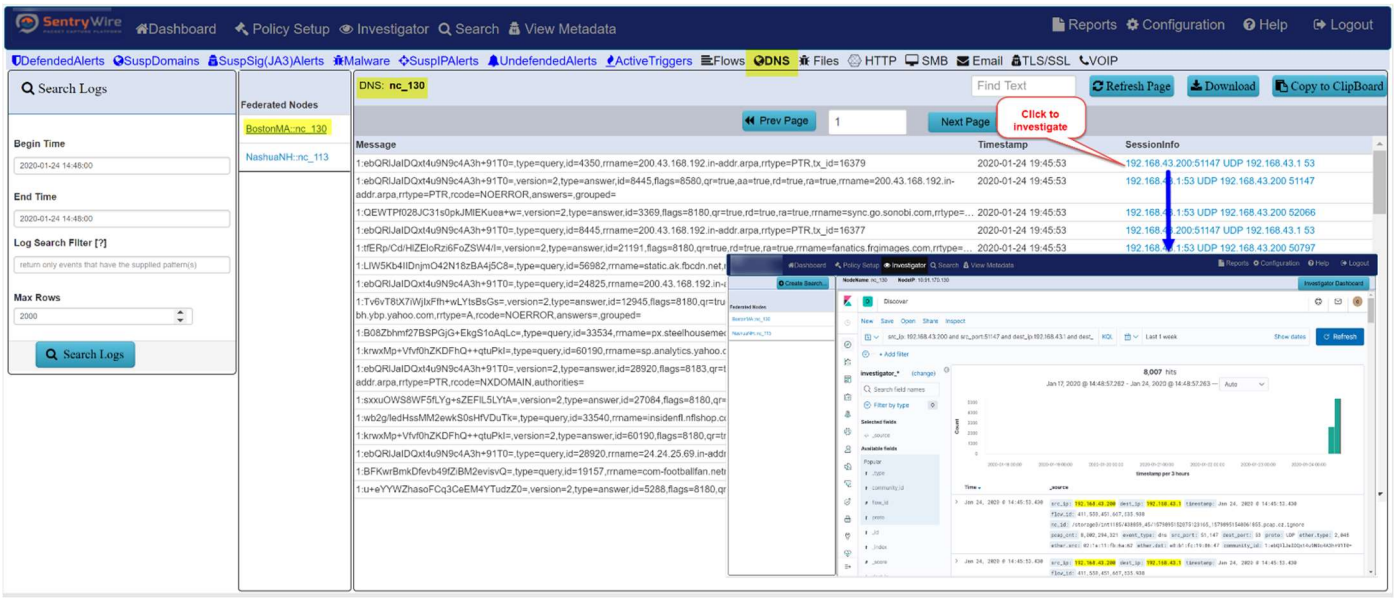


Figure 91-View Metadata DNS view

9.10 FILES

The Files tab displays IDS alerts of type 'file_type'.

Clicking on the hyperlinked sessioninfo pivots to the investigator screen that shows the events with the same 5 tuple information for further analysis.

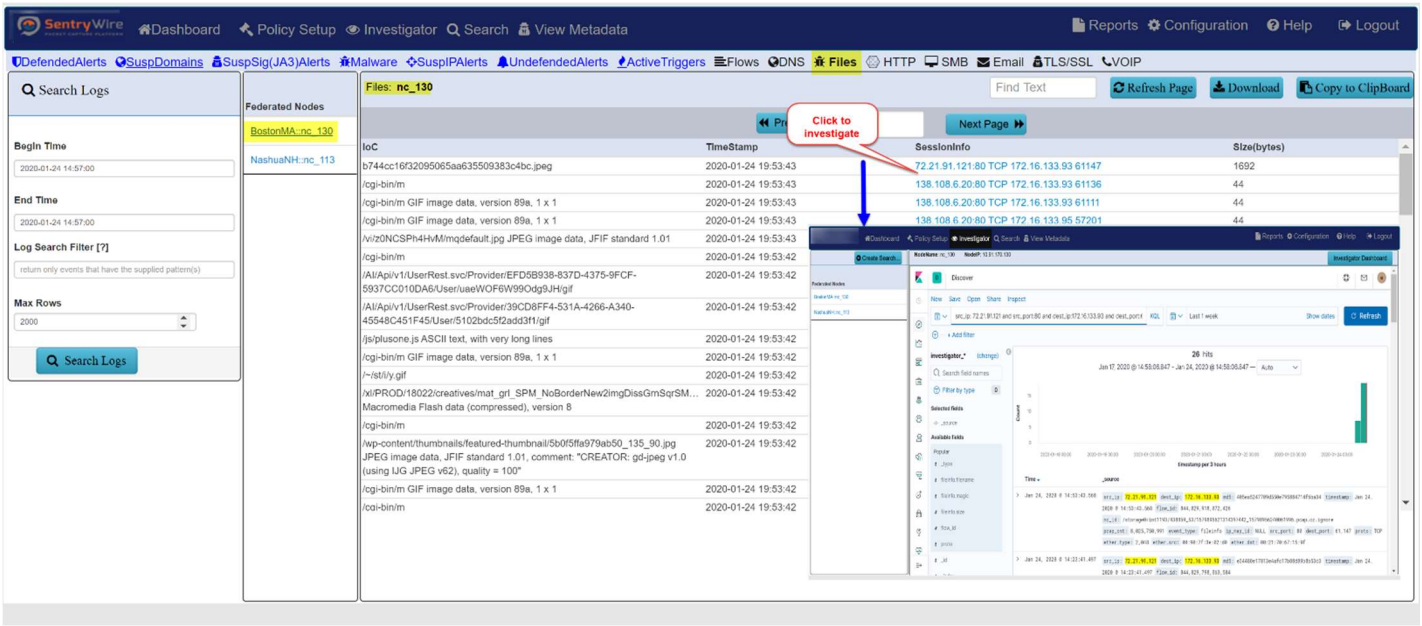


Figure 92--View Metadata Files view

9.11 HTTP

The HTTP tab displays the DPI events for port 80 for each node selected.

Clicking on the hyperlinked sessioninfo pivots to the investigator screen that shows the events with the same 5 tuple information for further analysis.

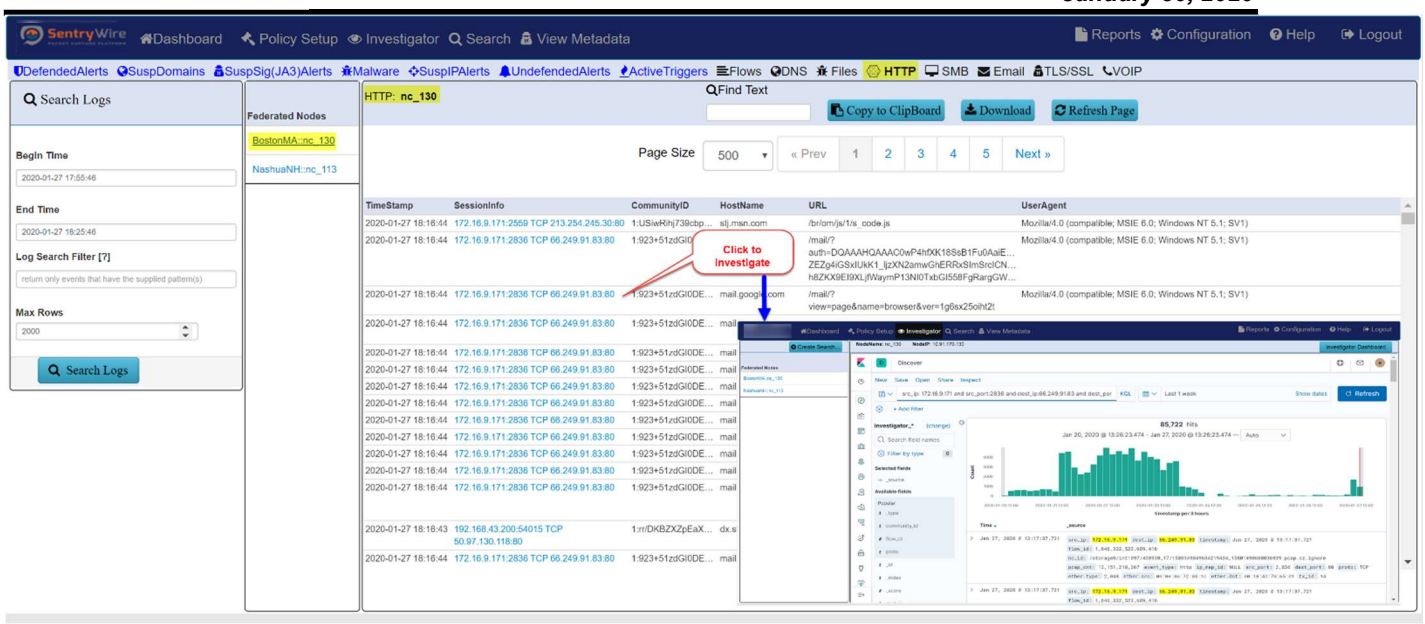


Figure 93-View Metadata HTTP view

9.12 SMB

SMB panel displays DPI events for port 445.

Clicking on the hyperlinked sessioninfo pivots to the investigator screen that shows the events with the same 5 tuple information for further analysis.

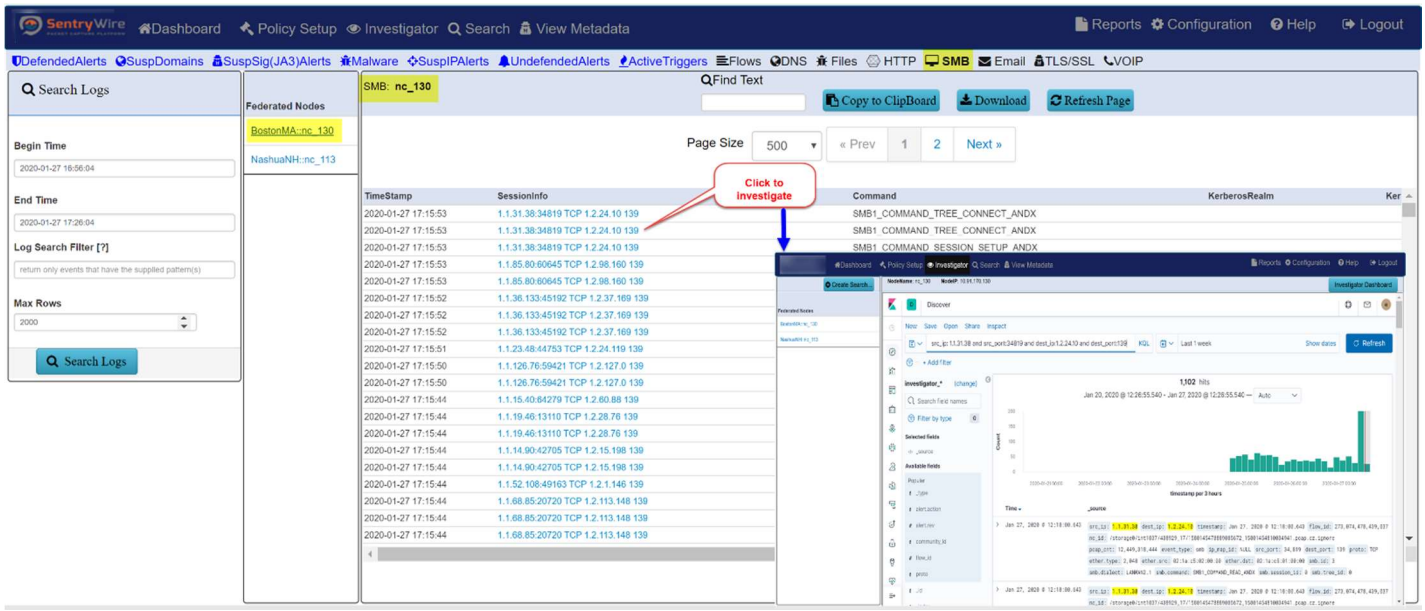


Figure 94-View Metadata SMB view

9.13 EMAIL

The Email tab displays the DPI events for port 25 for each node in the Federation.

Clicking on the hyperlinked sessioninfo pivots to the investigator screen that shows the events with the same 5 tuple information for further analysis.

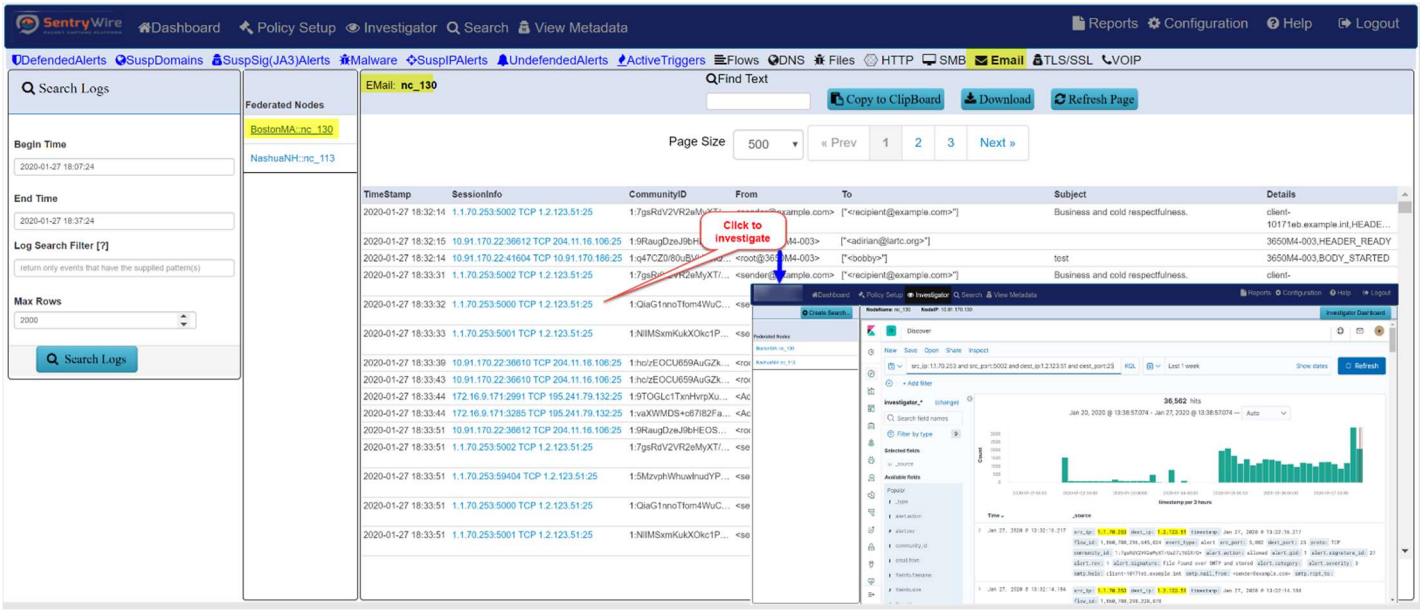


Figure 95-View Metadata Email view

9.14 TLS/SSL

The TSL/SSL tab displays the DPI events for port 443 for each node in the Federation. All events are clickable and searchable.

Clicking on the hyperlinked sessioninfo pivots to the investigator screen that shows the events with the same 5 tuple information for further analysis.

If a TLS/SSL event's JA3 signature matches known bad JA3 signatures uploaded via Augmentation panel, this event also appears as a Suspicious Signature event.

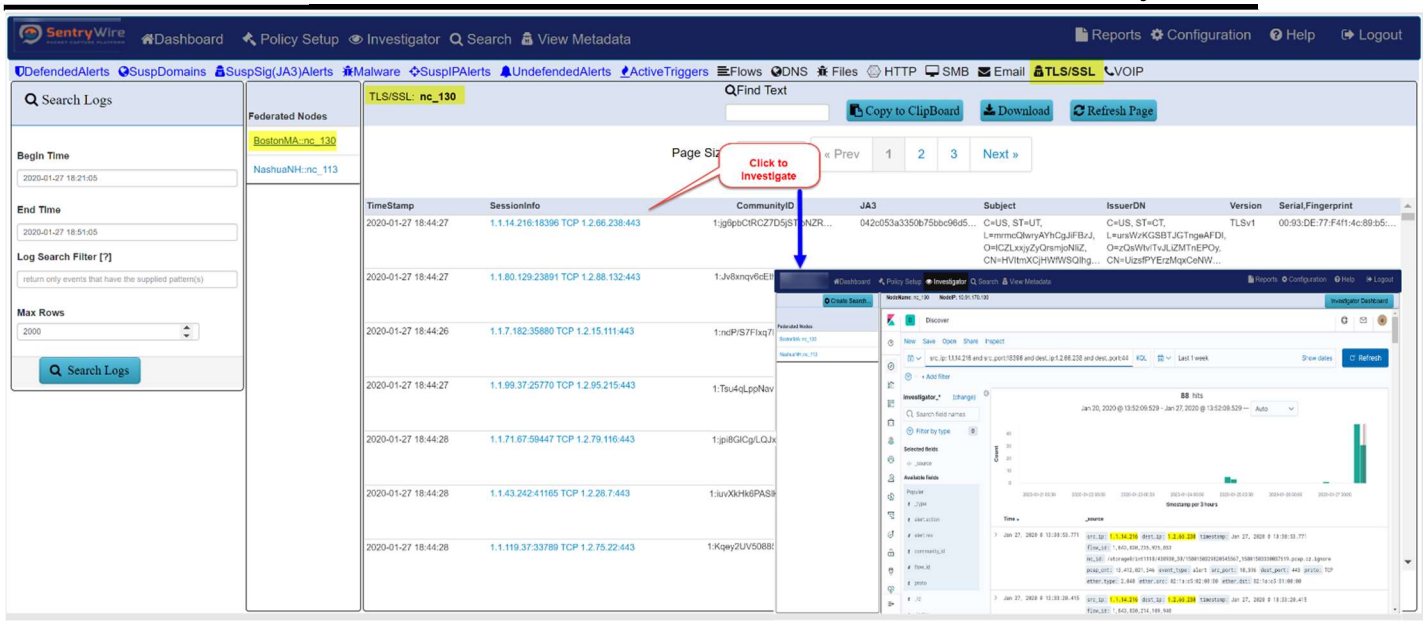


Figure 96-View Metadata TLS/SSL view

9.15 VOIP

Each VOIP session entry displays Begin time of the session, Sessioninformation, RequestMethod, From (From, From_tag), Call-id, CSeq (Call sequence), ResponseMethod, To (To, To_tag) and the Jitter value for the session.

The VOIP tab provides two ways of filtering VOIP session data displayed.

- "Find Text" Filter:
  - When this field is empty, all VOIP sessions are displayed.

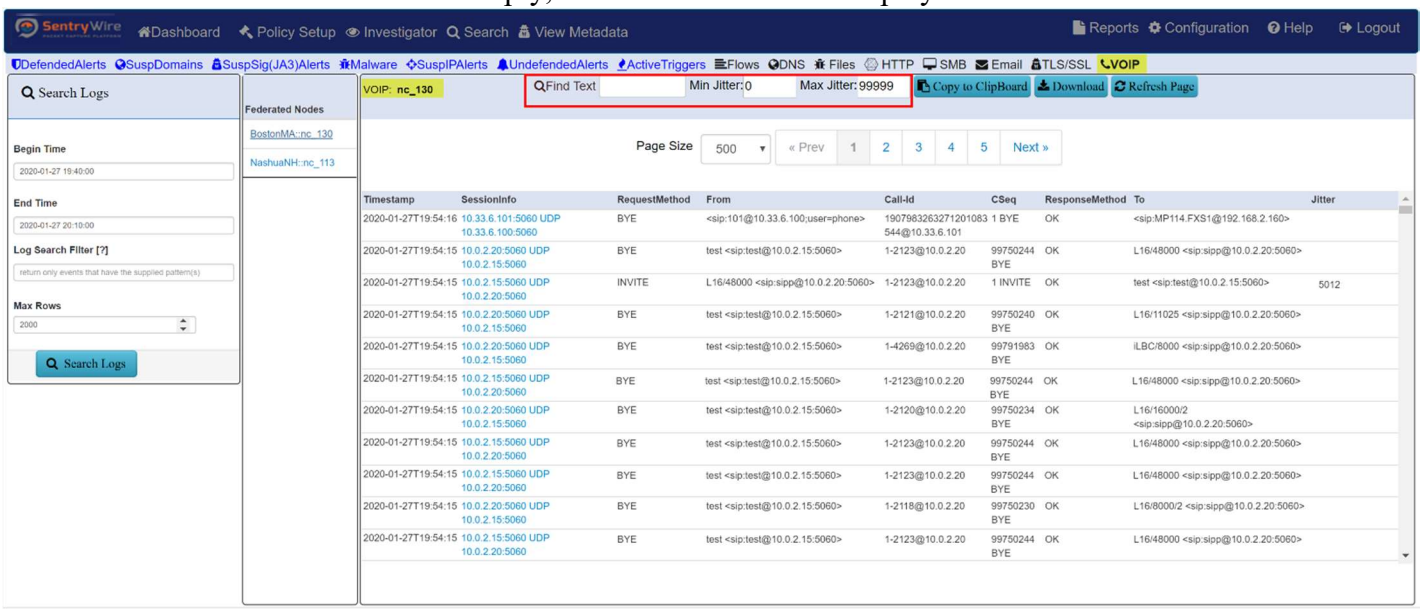


Figure 97-View Metadata VIOP view

- As the user enters text into this text field, only the matching rows are displayed.

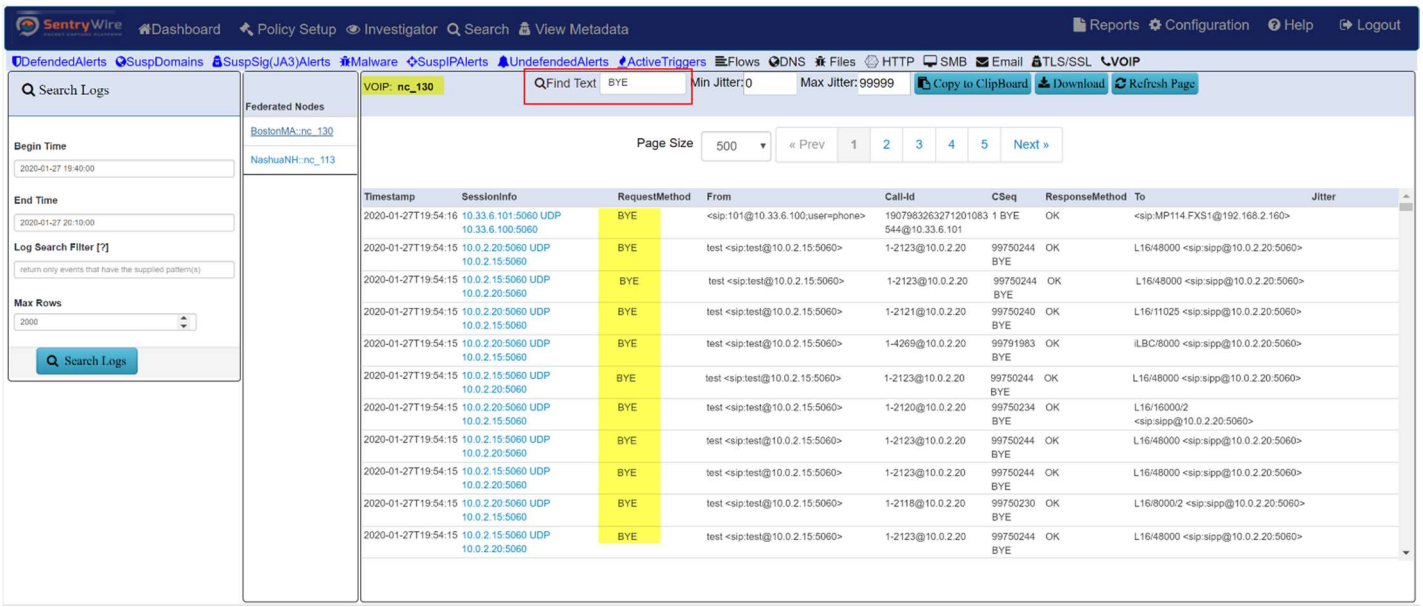


Figure 98-View Metadata VOIP Find Text view

- "Min Jitter" and "Max Jitter" Filter:
  - When both "Min Jitter" and "Max Jitter" fields are empty, only the sessions without RTCP packets are displayed.

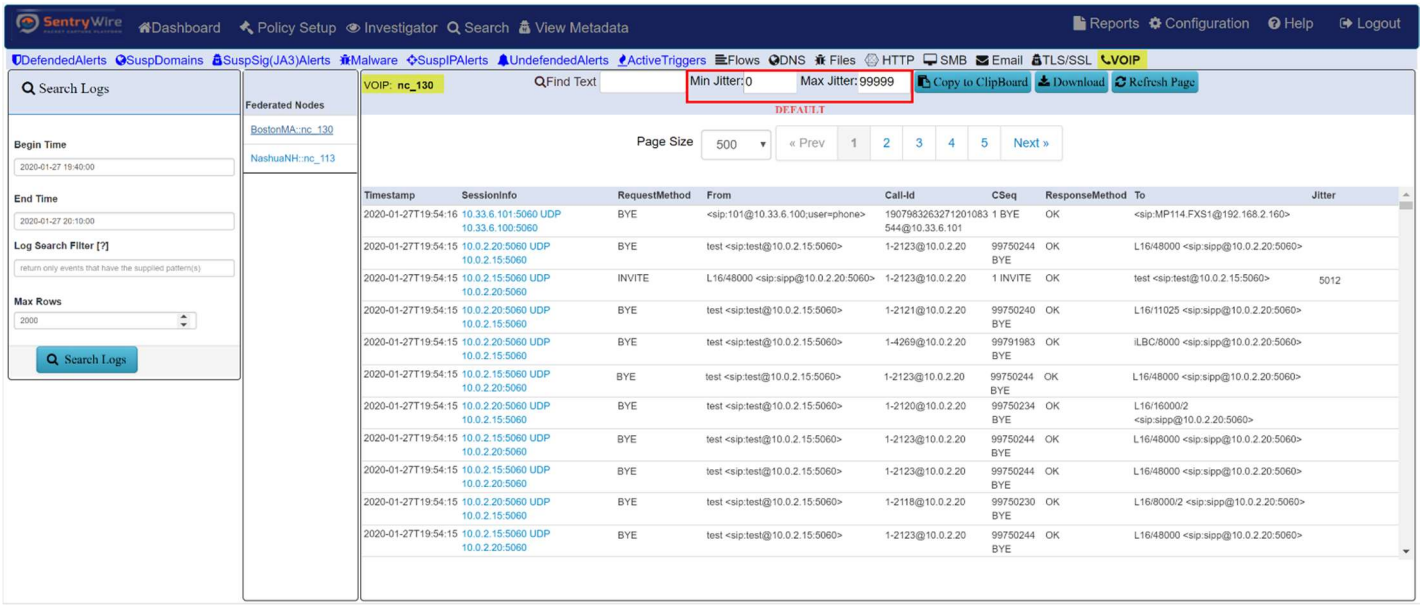


Figure 99-View Metadata VOIP Min and Max Jitter field view

- When the user enters values into both “Min Jitter” and “Max Jitter” fields, only the sessions with jitter values that are >= “Min Jitter” and <= “Max Jitter” are displayed.

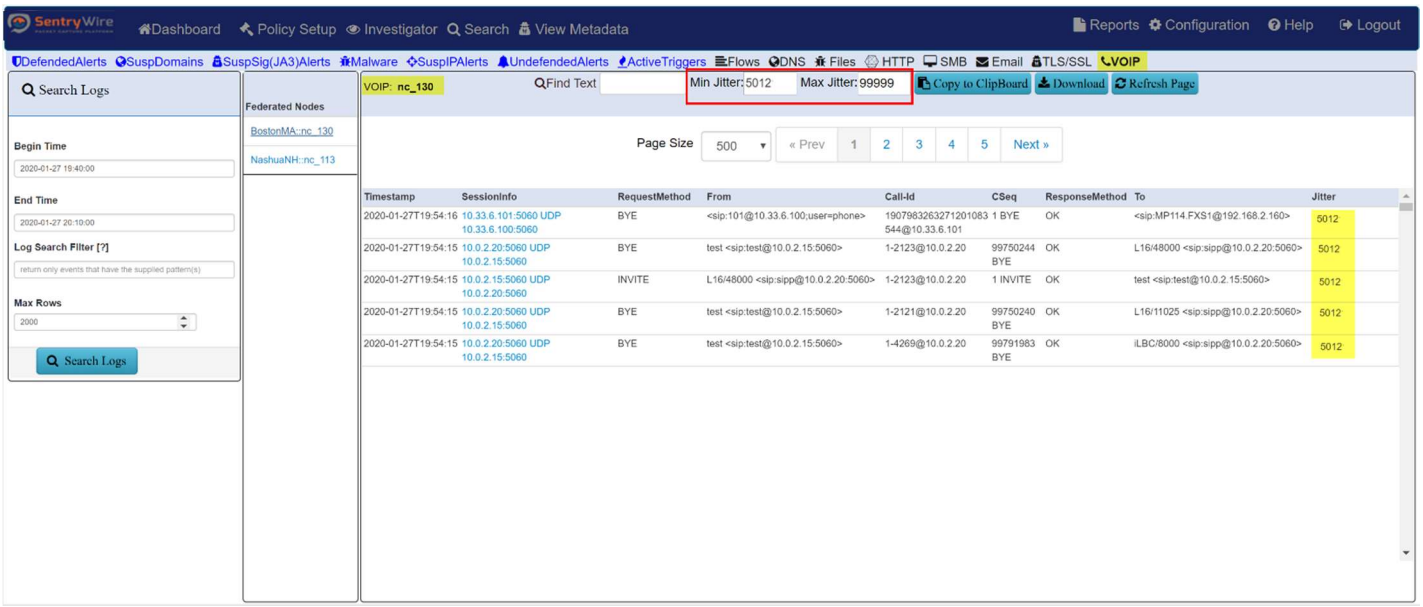


Figure 100-View Metadata VOIP Min and Max Jitter results

- Both “Find Text” and Jitter filters can be used together:

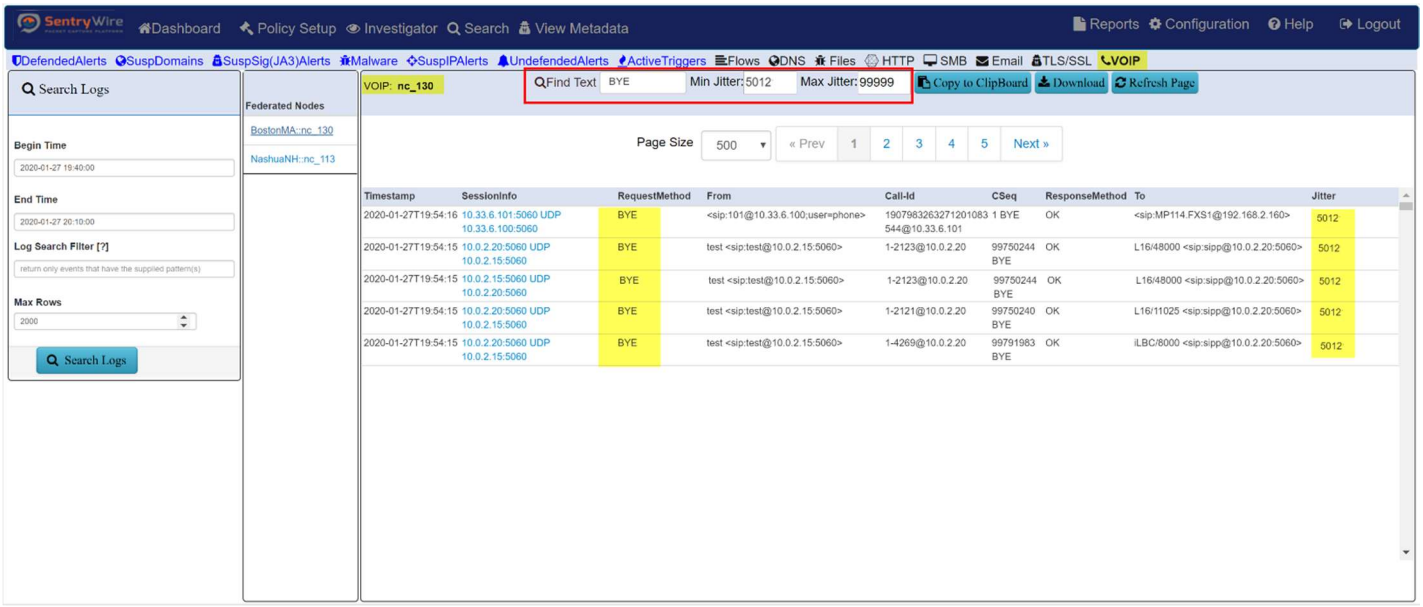


Figure 101-View Metadata VOIP Min and Max Jitter and Find Text combined field view

VOIP sessions allow searching for SIP, RTP and RTCP packets for each session.

“SessionInfo” column for SIP sessions displays:

- SIP source IP address, SIP source port

- SIP destination IP address, SIP destination port
- RTP inviter IP address, RTP inviter port.
- RTP invitee IP address, RTP invitee port.

"SessionInfo" column for RTP and RTCP sessions displays:

- SIP source IP address, SIP source port
- SIP destination IP address, SIP destination port
- RTP inviter IP address, RTP inviter port.
- RTP invitee IP address, RTP invitee port.

Jitter summary column displays the data extracted from RTCP packets for the session:

Note: If the session does not contain any RTCP packets the Jitter summary column can be blank.

Clicking on the hyperlinked sessioninfo pivots to the investigator screen that shows the events with the same 5 tuple information for further analysis.

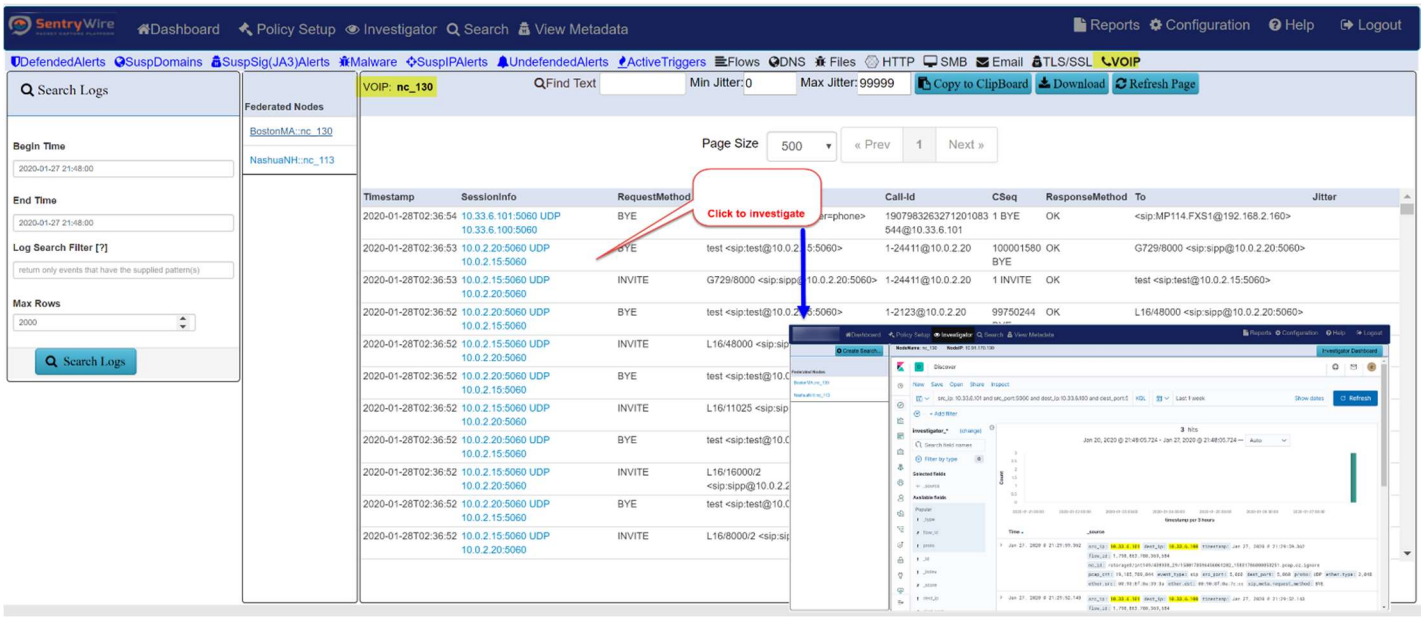


Figure 102-View Metadata VOIP SessionInfo Results view

10 REPORTS

The Reports tab allows the users to initiate requests for several types of reports that can be viewed and printed.

To generate a report, follow the steps below:

1. Select a Federated Node
2. Set Reports Settings(optional)
    - FilterString to be passed on to Kibana as a query filter.
    - Duration for the report data. Default Is 1 hour.
3. Click on one of the hyperlinks available in Reports List portion of the panel

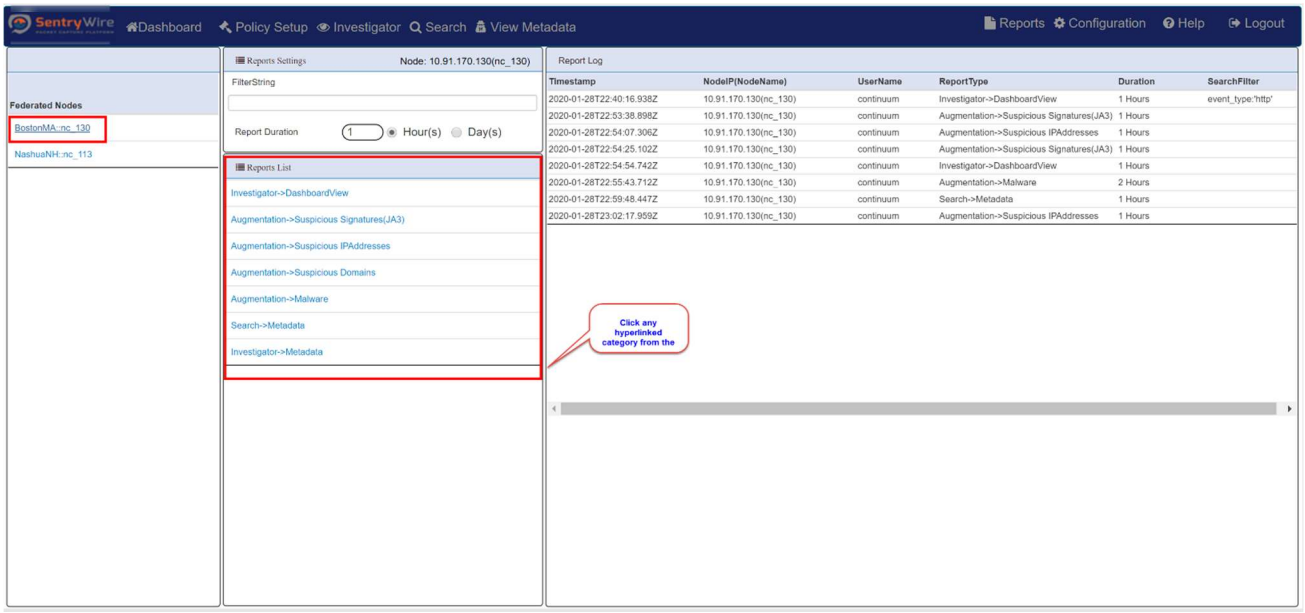


Figure 103-Reports Screen

4. A new browser tab will appear with the relevant Kibana interface.
5. Review data and modify the duration as needed.
6. From the browser's File Menu, choose Print.

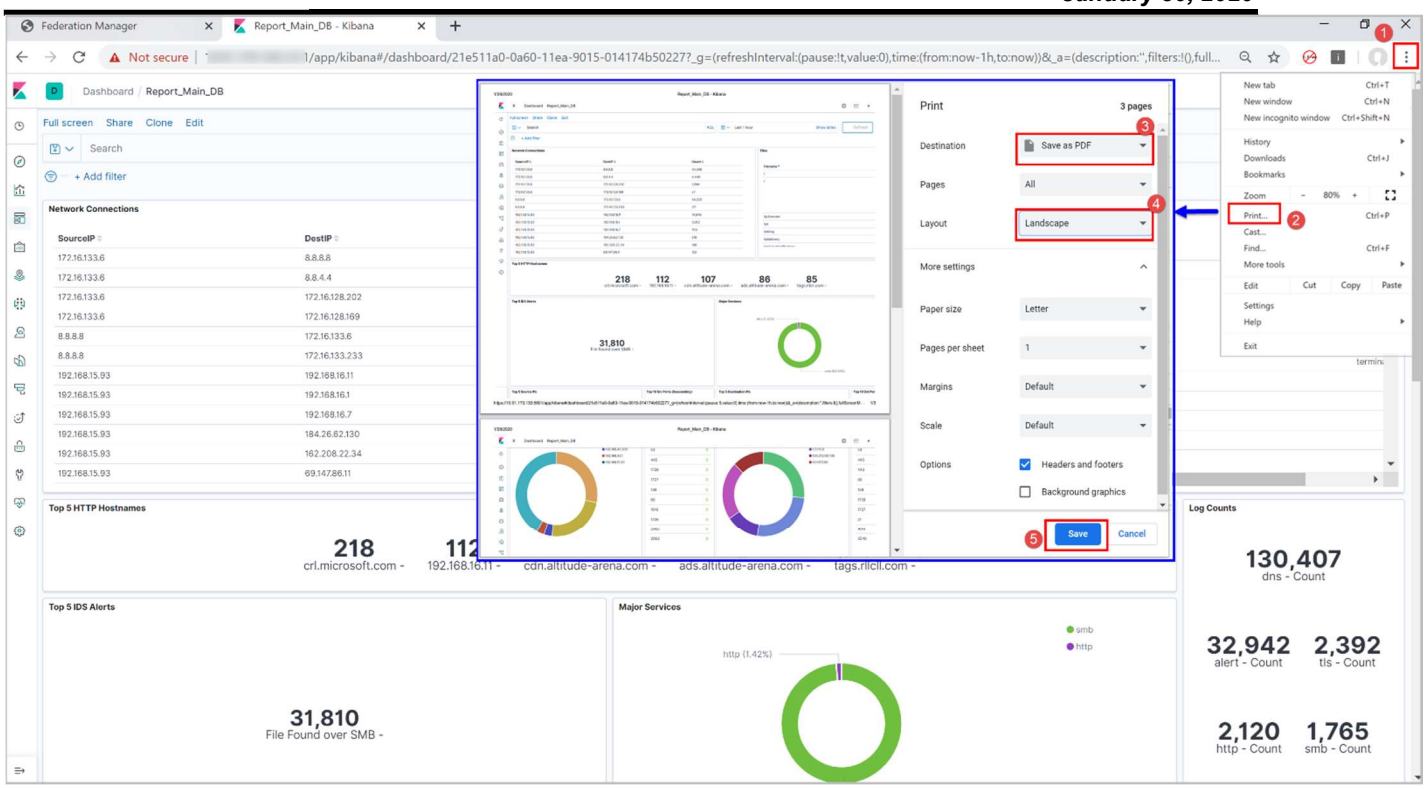


Figure 104-Reports Results Screen

7. When a print dialog appears, choose landscape layout, and the destination to be 'Save As PDF'
8. Report is saved as PDF on user's system.

11 CONFIGURATION

The Configuration tab is a drop down menu providing access to the following functions:

- Software Management – License and Cluster management.
- Authentication – User Management
- Authorization – User roles and permissions.
- Auditing - Rsyslog configuration, SNMP configuration, and Log Manager settings.
- View System Events – Observe system events.
- Generate Report – Custom Reporting

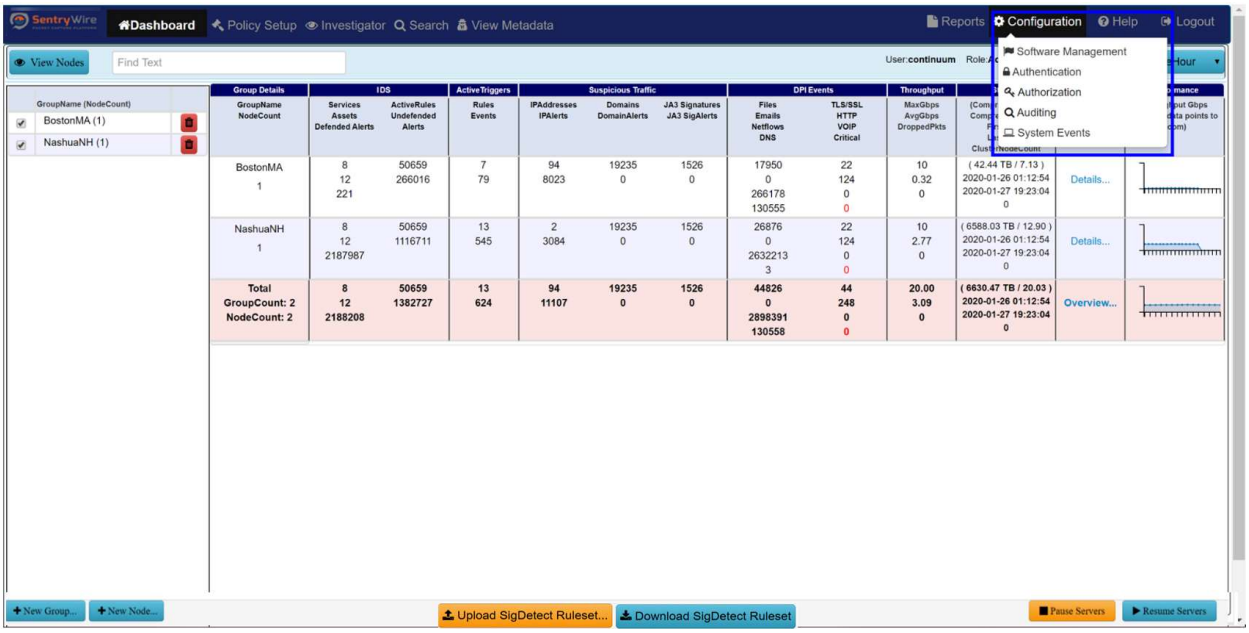


Figure 105-Configuration Options

11.1 SOFTWARE MANAGEMENT

This panel allows the user to perform license management and software update management.

11.1.1 License Management

Once a license key has been forwarded, copy and paste the provided string into the License Installer in the web user interface. Note: If it is cluster enabled configuration each node needs to be licensed individually.

If you do not have any data nodes, you will only need to apply the master license.

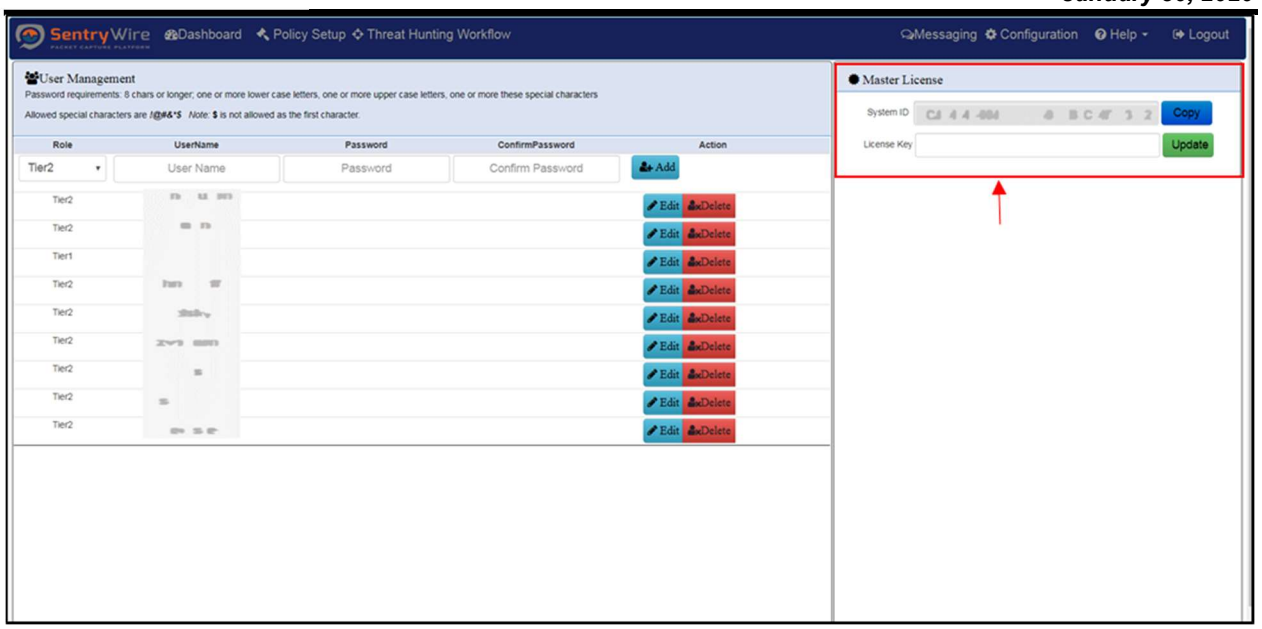


Figure 106-Configuration Master License Update function

11.1.2 System Information

Clicking on Show System Info button displays a pop up window containing the following information:

- Storage capacity of the Master and enabled Cluster nodes
- Search Storage Statistics
- Memory Statistics
- Five most recent Pcap files stored
- Interfaces configured for capture

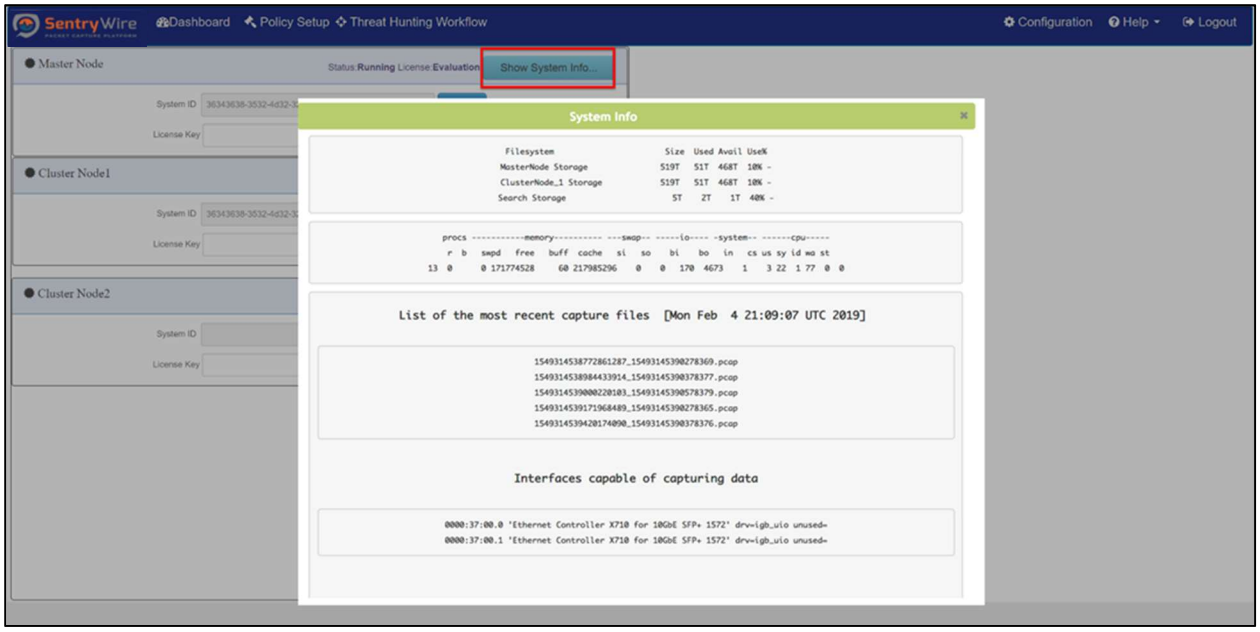


Figure 107-Configuration Show System Info Button results

11.1.3 Cluster Management

The appliance can function as a standalone server or a cluster of servers. This allows for the expansion of data storage and computational ability of the system. Software Configuration panel displays the Master

Node and the configurable Cluster Nodes as shown below.

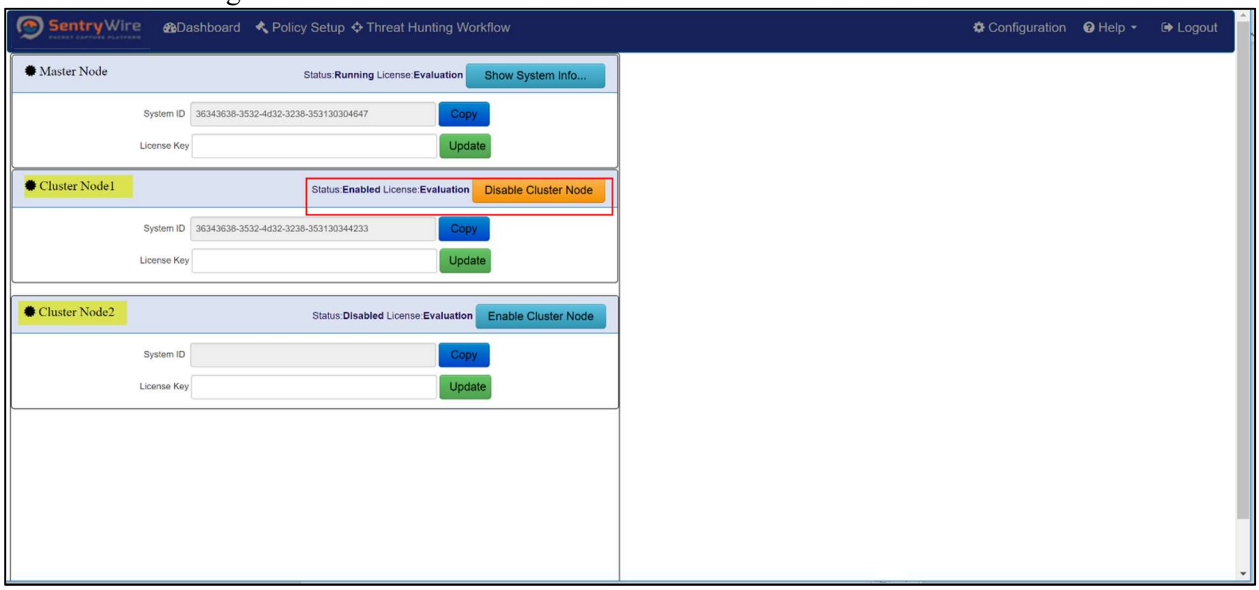


Figure 108-Cluster Node Management view

Note: By default – Cluster Nodes are disabled.

11.1.3.1 Enable Cluster Node

- Before enabling a data node, the user must ensure the capture server is running and the Cluster node is connected to the master node.
- When the Cluster Node1 is ready to be included in the cluster, the user must press “Enable Cluster Node” button for Cluster Node1. This will change button label to “Disable Cluster Node”.
- Now the server is aware of the newly enabled Cluster Node(s).
- If these servers are enabled, up and connected - the status of the respective nodes in the cluster will change to “Running”.
- If Data Node1 and/or any node available are licensed, then the license label will display Permanent/Evaluation based on the license used.

11.1.3.2 Disable Cluster Node

- To disable the Data Node, the user should click the “Disable Cluster Node” button for that node under the cluster tab.
- Now the disabled Cluster Node is not associated with the master.
- The node will no longer store data.

11.1.3.3 Software Update Management

This panel allows downloading capture software upgrades from a central server and pushing these updates to the Nodes.

User provides the URL for checking/downloading software updates and click on “Check for Update” button.

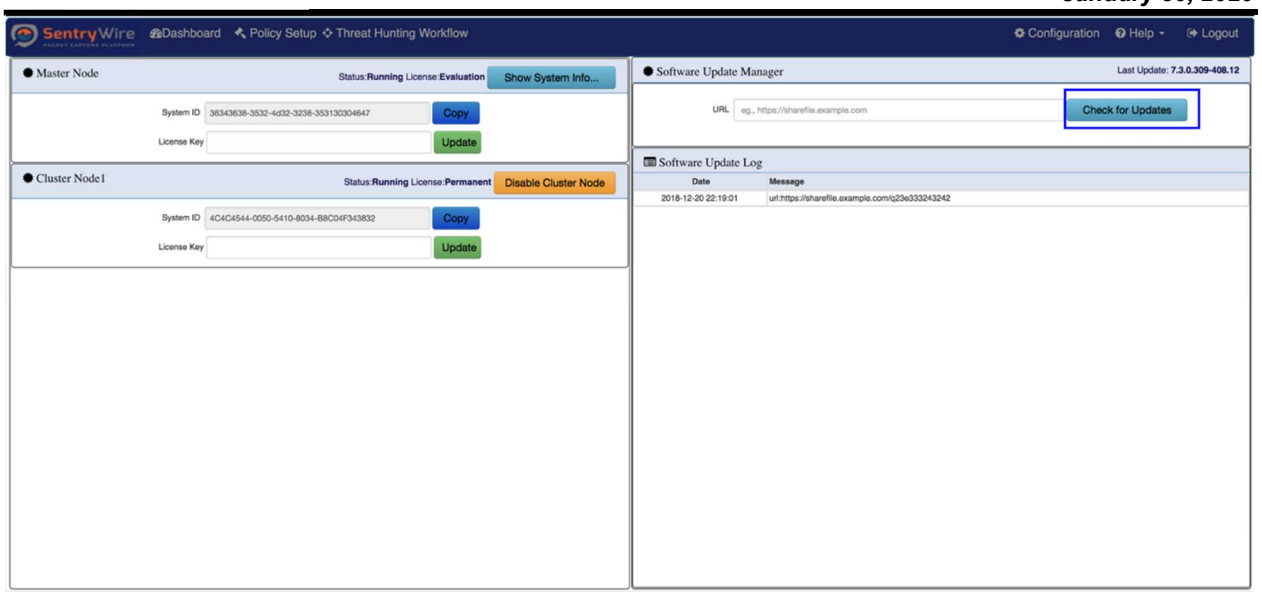


Figure 109-Software Update Manager view and Check for Updates button

If an update is available, “Apply Update” button is displayed. Clicking on this button updates the software.

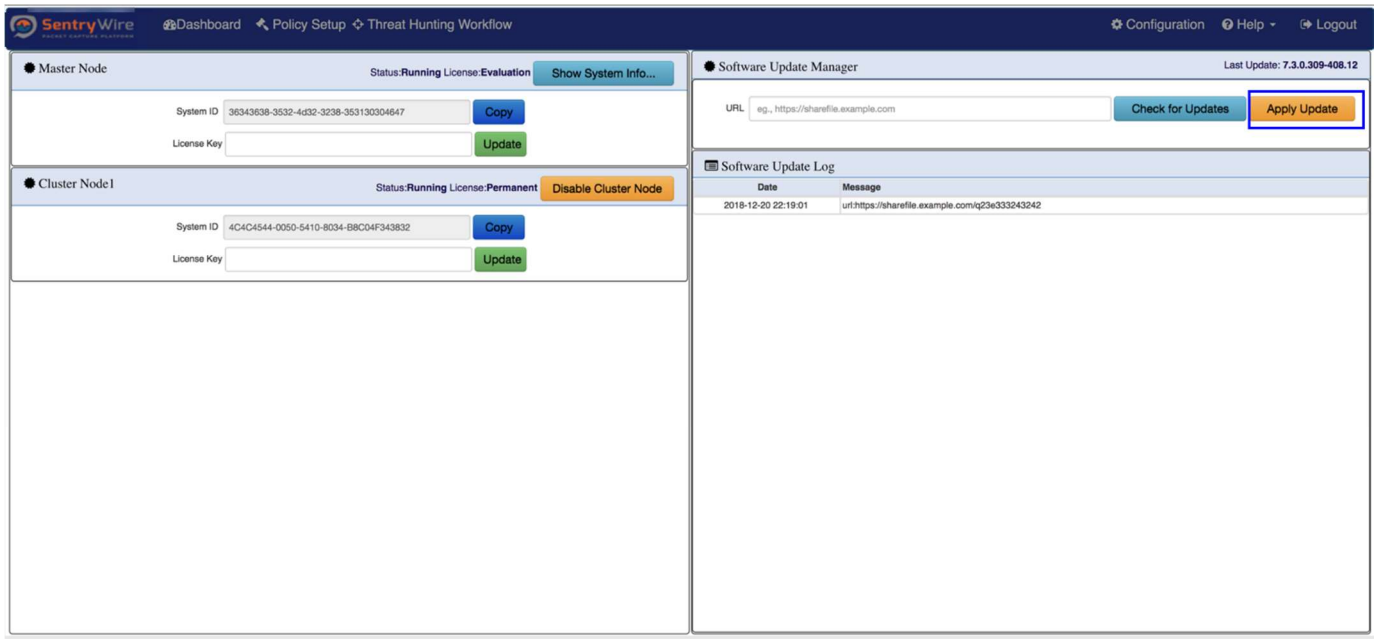


Figure 110-Software Update Manager function and Apply Update button

11.2 AUTHENTICATION

This panel allows users to choose from one of the following authentication mechanisms:

1. Local Authentication

   - This is the default Authentication.
   - Backward compatible with earlier versions of the software.
   - Server switches over to Local Authentication if SSO, LDAP, or other allowed/configured authentications fail.

2. Remote Authentication

   - This tab allows the user to switch to SSO, LDAP, Radius or other allowed/configured authentication modes.
   - Note: Only one authentication mode can be active at a given time.

11.2.1 Local Authentication

Local authentication is used to manage local users.

11.2.1.1 Adding Users

Perform the following to add a new user:

1. Select the role for the user being created from the drop down
   a. Roles are created and assigned through Configuration→ Authorization tab. Please refer to section 9.3 for more details.
2. Enter Username and Password for the new user
3. Retype and confirm the password
4. Click on the Add button.
5. Once the user is added, the users list is refreshed to show the newly added user. This may take few seconds.

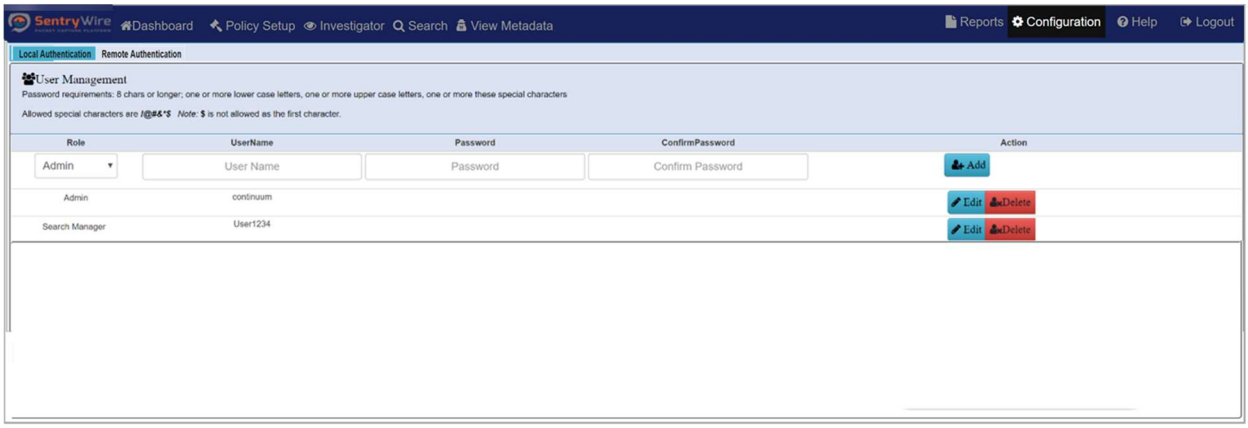


Figure 111-Add Users view

11.2.1.2 Activate Local Authentication Mode

This button appears on the Authentication → Local screen only if the currently logged user is not a local user. If the current user is a LDAP, SSO or Radius user and wants to change back to a local user the user is presented with "Activate Local Authentication Mode" button. Clicking on this button, closes any active connection to LDAP, SSO or Radius server. The user can login again using the local user from the local database.

Note:

- In case of any failure, the user automatically falls back to the local user.
- At a given time only one authentication mode is active. If the user wants to change to a different authentication mode, the user has to first fall back/activate the local mode, re-login as local user and then activate desired authentication mode. Once the new authentication is activated, the user can now logout as local user and login back using the newly activated authentication mode.

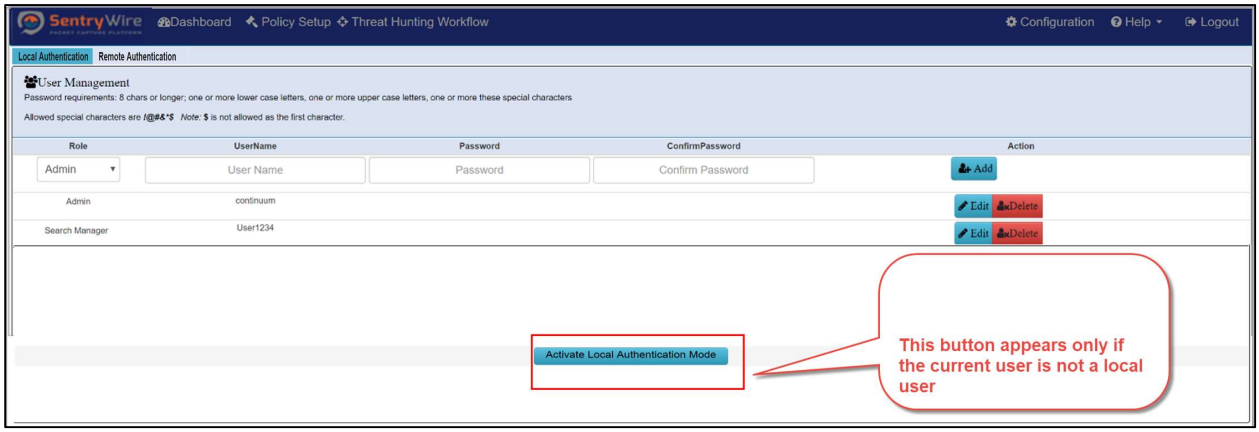


Figure 112-Activate Local Authentication Mode button view

11.2.1.3 Deleting Users

Perform the following to delete a user:

1. To delete a user, click on the Delete button of the user to be deleted.
2. Once a user has been deleted, this username and password cannot be used for either UI login or REST login.
3. To delete an existing user, you must be logged in to the system as admin.

Note:

- Any user who is currently logged into the system cannot be deleted.

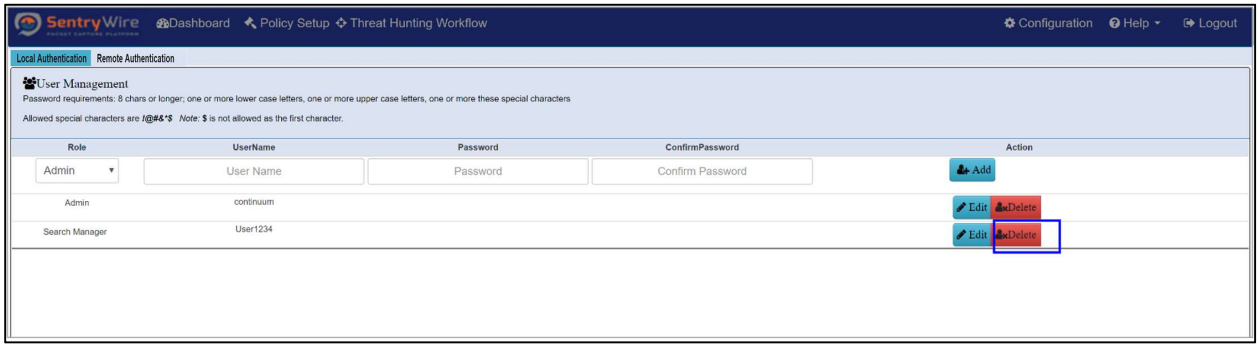


Figure 113-User Management Delete User Button view

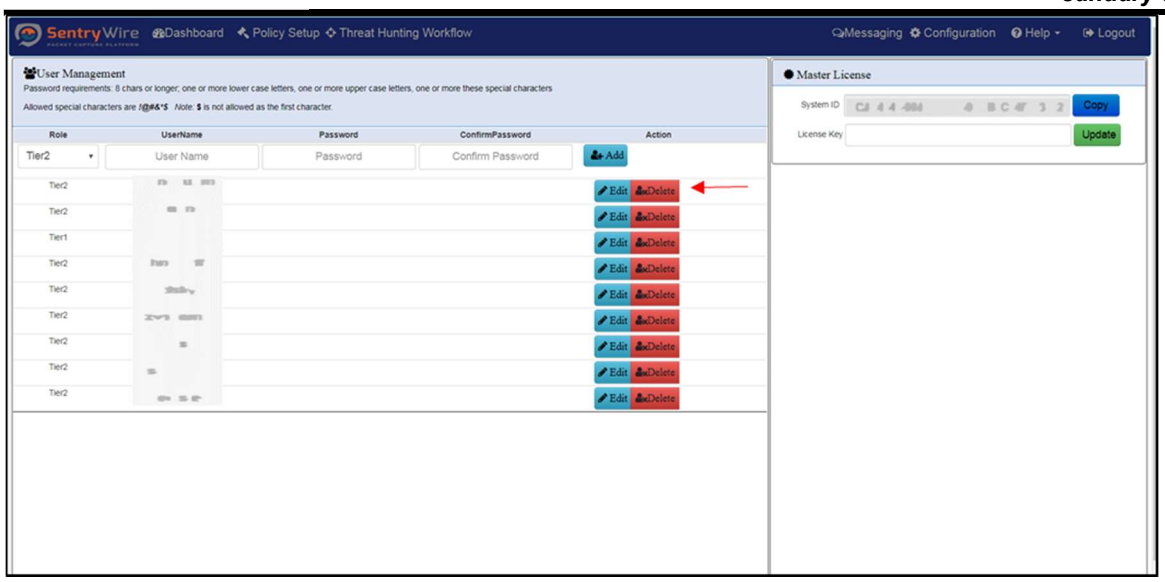


Figure 114-User Management Delete User Button view

11.2.1.4 Modifying Users

1. To modify a password for a user click the Edit button for that user.

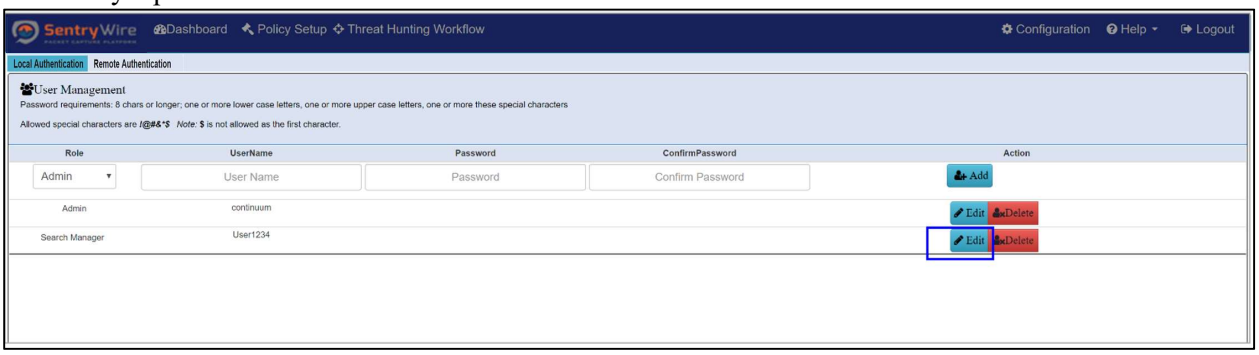


Figure 115-Manage Users Modify/Edit User button

2. Enter a new password and confirm password. Click save.

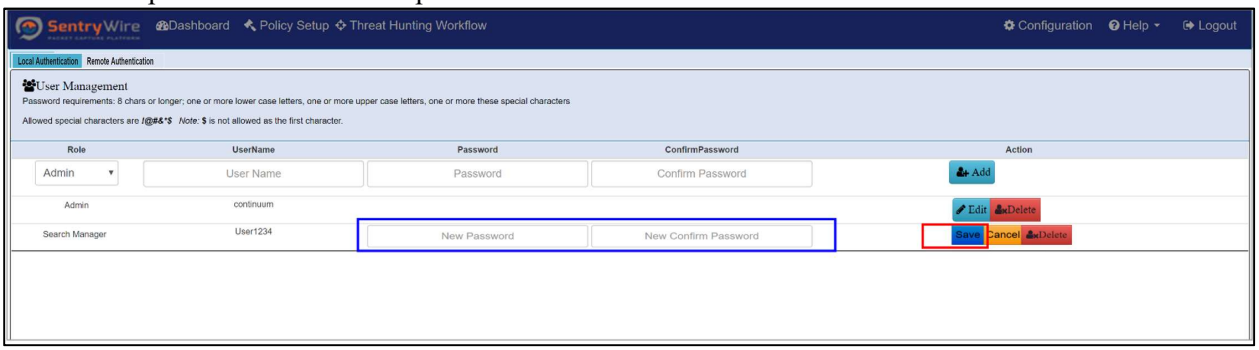


Figure 116-Manage Users Change Password button

***Note**:*

- *Only Tier2 user can modify the password for a user (including himself or another Tier2(admin)/ Tier1(Guest))*
- *If the user is currently logged into the session, he should be prompted to login again with the new password. The previous login session is no longer valid.*

11.2.1.5 Unlock User

To unlock a user login to the system as admin. Click on the unlock button for that user.

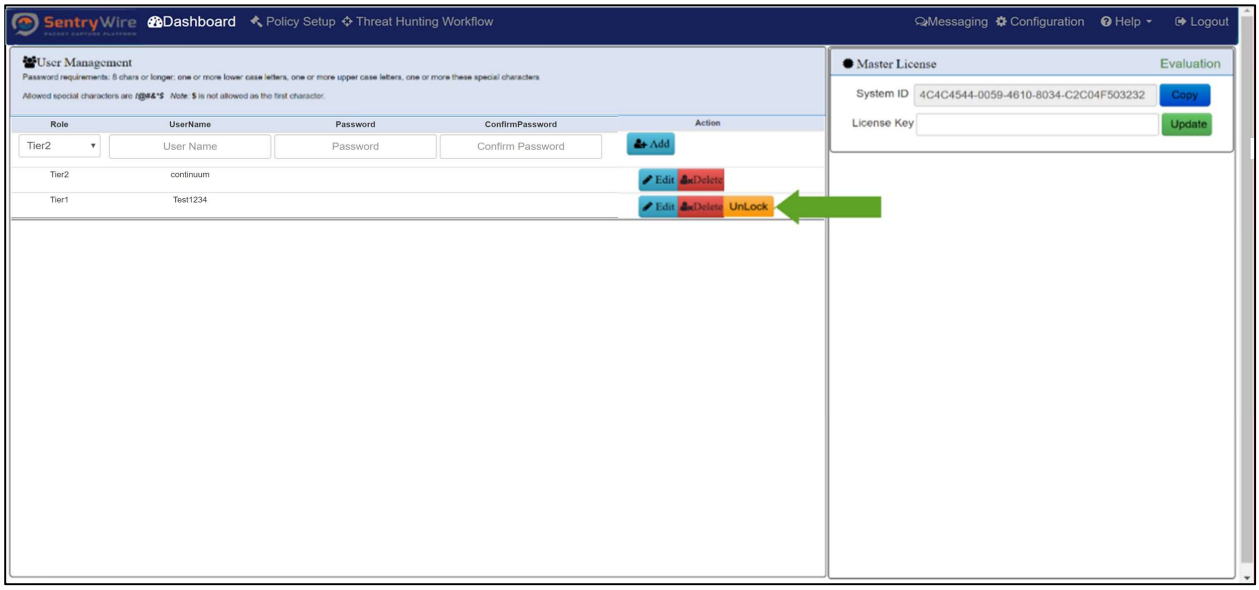


Figure 117-Manage Users Unlock User button

11.2.2 Remote Authentication

Use Remote Authentication to configure and enable SSO, LDAP, or Radius authentication methods.

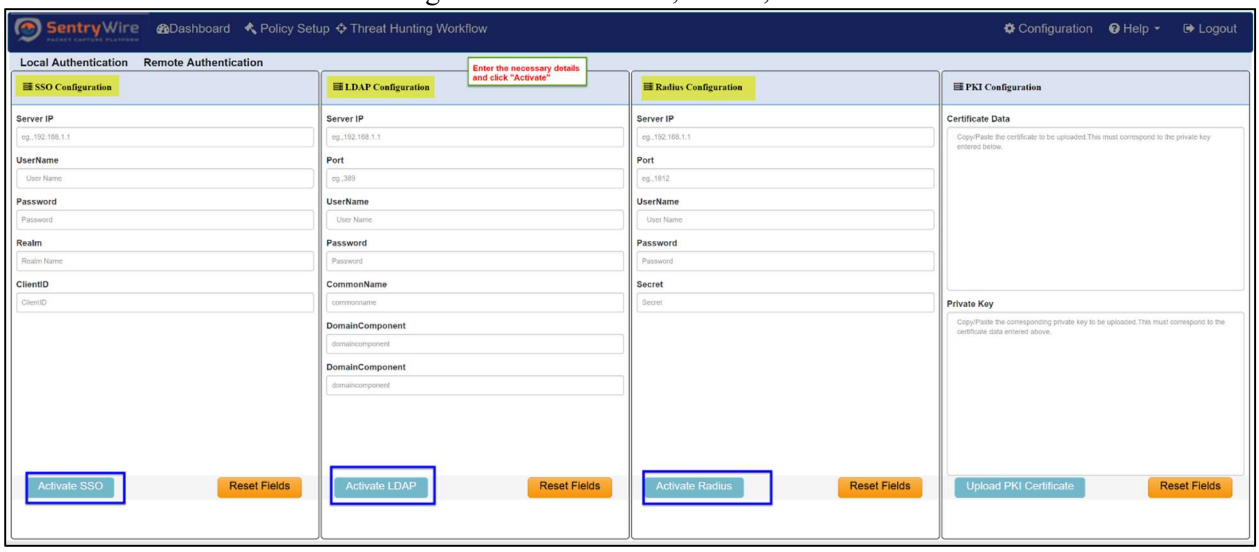


Figure 118-Remote Authentication Configuration view

> ***Note***:
> - In case of any failure, the user automatically falls back to the local user.
> - At a given time only one authentication mode is active. If the user wants to change to a different authentication mode, the user has to first fall back/activate the local mode, re-login as local user and then activate desired authentication mode. Once the new authentication is activated, the user can now logout as local user and login back using the newly activated authentication mode.

11.2.2.1 Activate SSO Authentication

- Enter SSO server IP address, UserName, Password, Realm, and ClientID.
- Click "**Activate SSO**" button and confirm.
- If the SSO IP Address, username, password are valid for the specified Realm and Client, the Node server switches to SSO mode.
- User must log out and log back in using the SSO credentials.

11.2.2.2 Activate LDAP Authentication

- Enter LDAP server IP address, Port, UserName, Password, CommonName, and DomainComponent.
- Click "**Activate LDAP**" button and confirm.
- If the LDAP IP Address, Port, UserName, Password, CommonName, and DomainComponent are valid, the Node server switches to LDAP mode.
- User must log out and log back in using the LDAP credentials.

11.2.2.3 Activate RADIUS Authentication

- Enter RADIUS server IP address, Port, UserName, Password, and Secret.
- Click "**Activate Radius**" button and confirm.
- If the RADIUS IP Address, Port, UserName, Password, and Secret are valid, the Node server switches to RADIUS mode.
- User must log out and log back in using the RADIUS credentials.

11.2.2.4 Mapping a role to a RADIUS user

The **Map Role** button allows mapping Radius users to roles defined via Authorization tab.

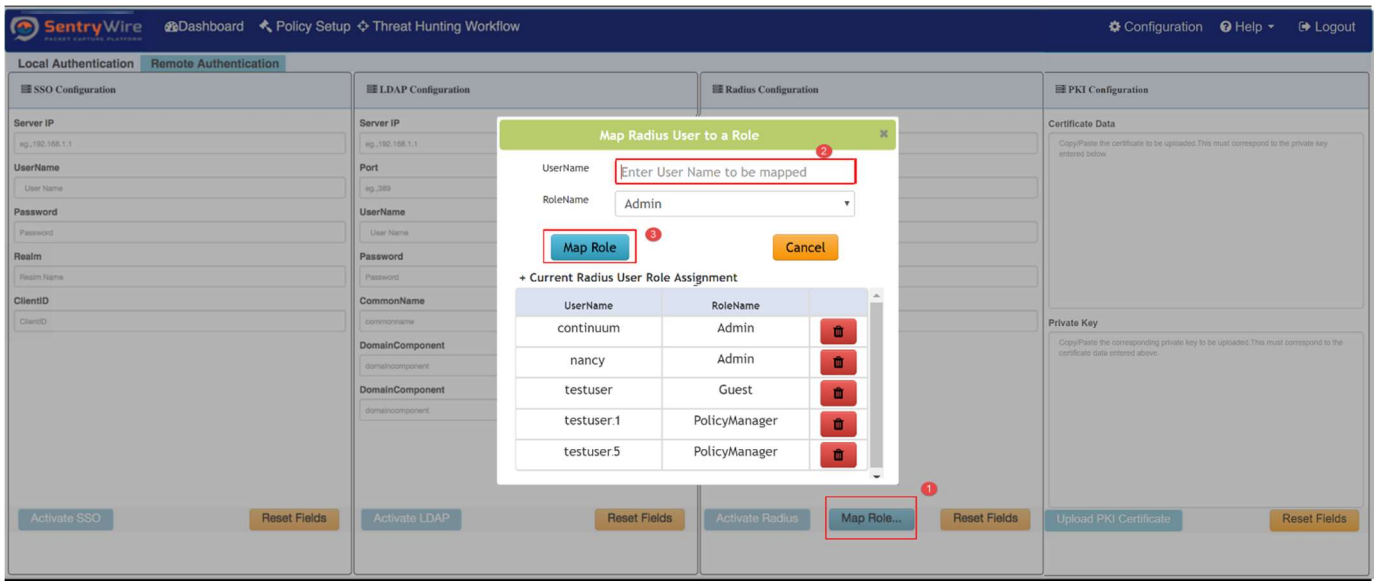


Figure 119-Mapping a Role to a RADIUS user

- Click on the "Map Role…" button.
- Enter radius UserName.
- Choose a RoleName from the drop-down list of available roles and click on "Map Role" button to map a radius user to the role.

- The newly assigned role and username are displayed as a list for quick reference. To delete a role mapping, simply click on the delete icon next to the role.
- When a radius user logs into the capture UI, the capture server checks the role status and use the assigned role to determine the authorization level of the user. If the signed in user us not mapped to a role, the capture server assigns "Guest" role.

11.2.2.5 Upload PKI Certificate

This panel allows PKI (Public Key Infrastructure) certificate to be uploaded to be used by the application web server. Copy and Paste Certificate data and Private key data into text areas shown below and press Upload PKI Certificate button. If the certificate and private key are valid and md5sums match, the server will restart with the new certificate. The user must login again.

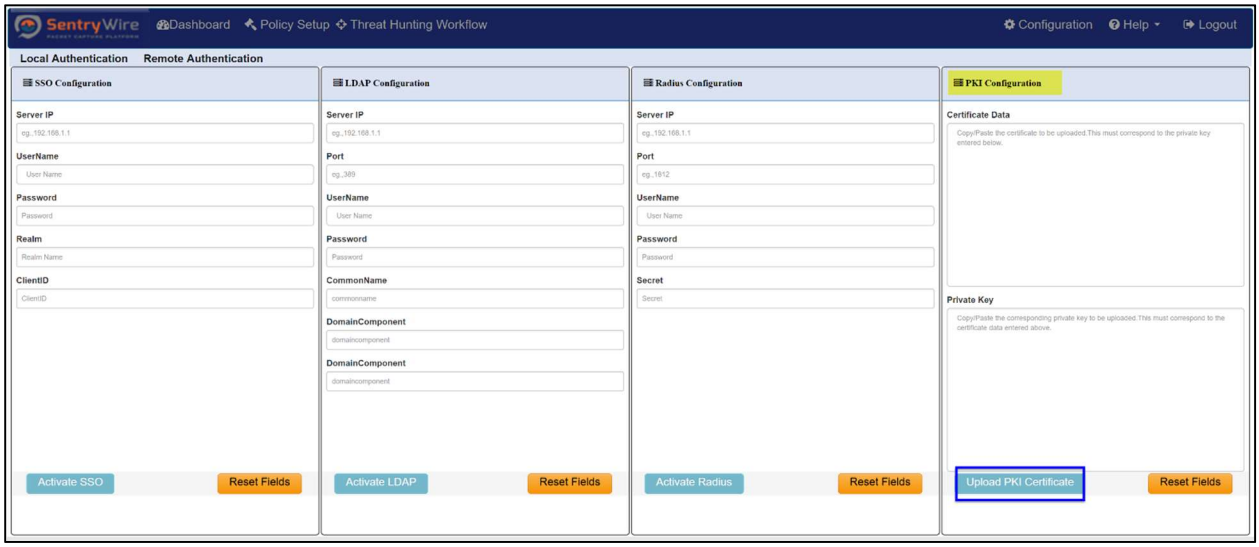


Figure 120-Upload PKI Certificate view

11.3 AUTHORIZATION

Authorization tab allows adding new roles and setting permissions for each role. When a user is assigned a role, the node UI menus 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.

Note:

- Authentication permission controls Authentication tab
- Licensing permission controls Software management tab and licensing.
- DeleteSearch permission can Delete Searches.
- Auditing permission controls Auditing features.
- Dashboard permission controls all dashboard features.
- Policy permission controls Policy menu items and Authorization tab.
- Default role "Admin" and "Guest" cannot be modified.
- Guest role allows view only permission
- Policy permission DOES NOT control Authentication, Licensing, Delete Search, Auditing, or Dashboard.

- To add a role click on the "Add Role" button at the top right of the panel.

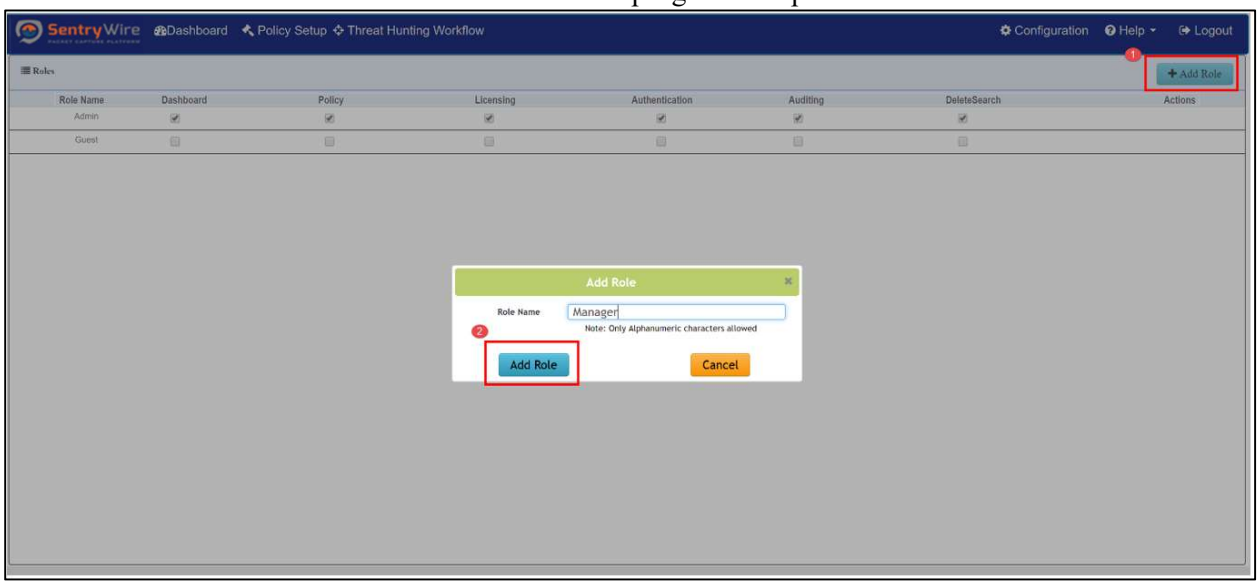


Figure 121-Authorization Add Role button

- Once a role is created assign the permission by checking the boxes.
- Click "**Apply**"
- Once created these roles are provided as a drop down list for each of the authentication modes under the Authentication tab and are available to be assigned to the users.

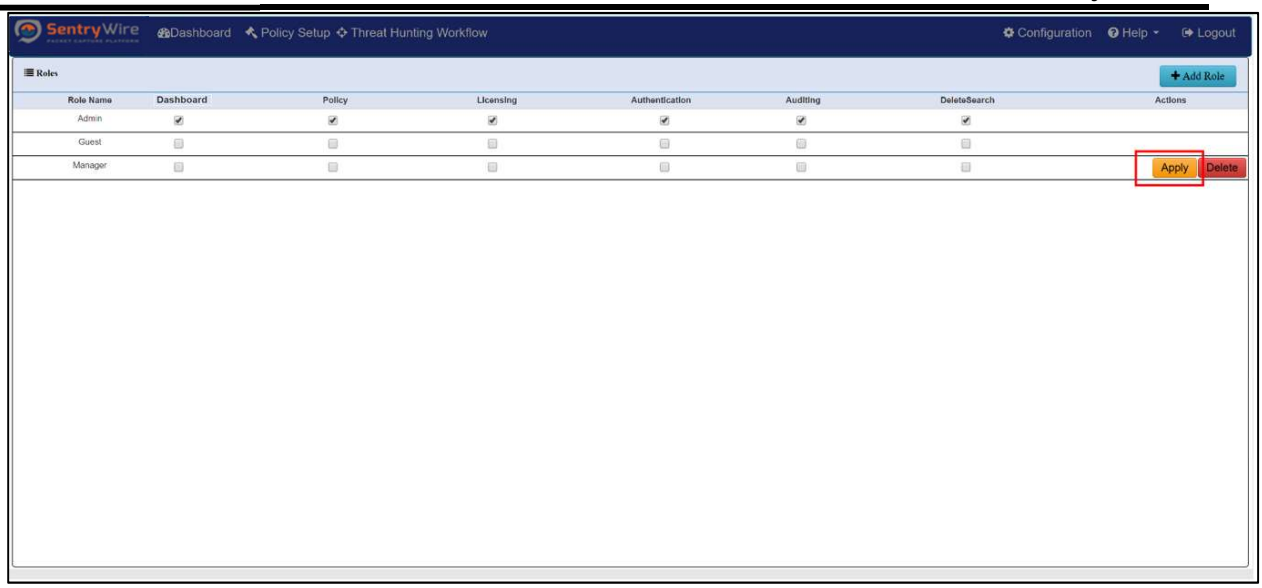


Figure 122-Authorization Apply Role button

11.3.1 SSO, LDAP and RADIUS Authorization

Capture server platform honors any role associated with users created via SSO, LDAP or RADIUS authentication modes. If this role is not defined as part of the Authorization in the capture application, any user associated with this role will have READ-ONLY access to the application.

This role must be added to the application via the Authorization panel and assigned the desired permissions. From here on, any user with this role will be authorized to access the functions based on the permissions assigned.

> ***Note***: It is advisable to create required roles and assign permissions via the Authorization panel before logging in to the application as a SSO, LDAP, or RADIUS user.

> ***Use Case:***
>
> When a user logs in with an authentication mode other than the Local and has permission to only view the content of the application, there may be two scenarios:
>
> Scenario1- The role of the user exists in the capture application but has "read-only" permission to all the functions of the application. In this case, the user must request an Admin user to login and modify the permissions of the role.
>
> Scenario 2- The role of the user does not exist in the capture application. In this case, the user must request an Admin user to create the role and assign permissions to the role.
>
> In either scenario, the user must logout and log back in for the authorization changes to take effect.

11.4 AUDITING

Auditing has three separate functional groups: Rsyslog configuration, SNMP configuration, and Log Manager settings. Each of these can be configured independent of the other. Two Rsyslog server settings can be provided for high-availability. Similarly, two SNMP server can be provided for high-availability.

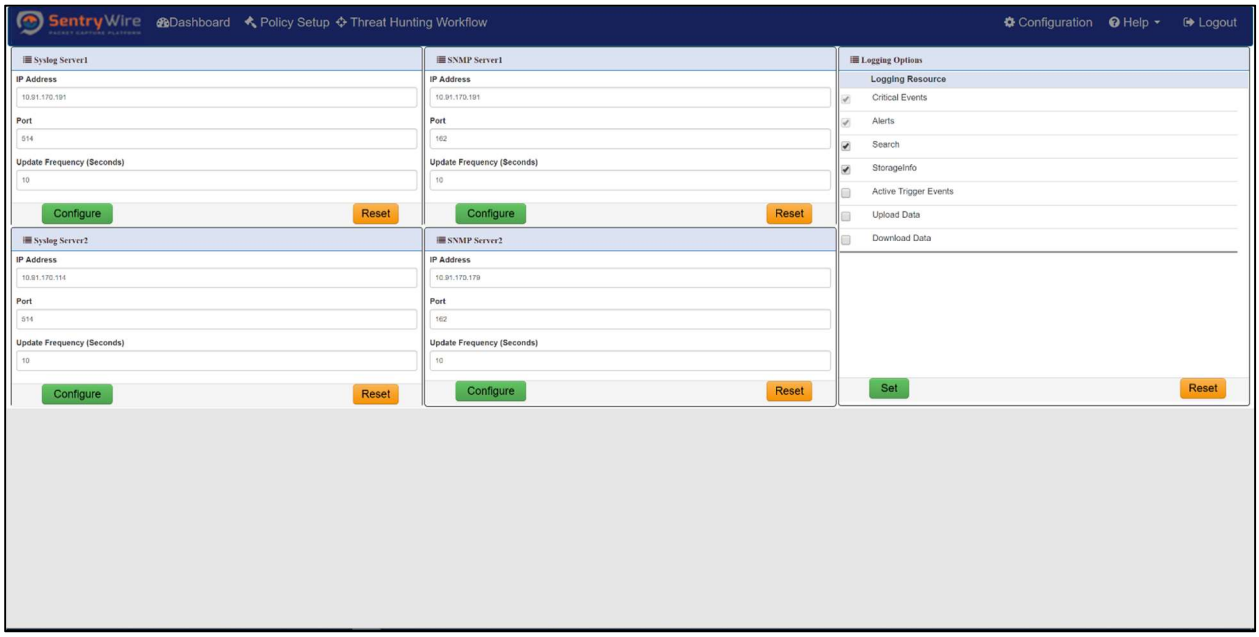


Figure 123-Auditing Function view

Each of the syslog servers can be setup to receive syslog messages at the configured frequency. Reset button on each panel removes the Syslog server setting. (Refer to Appendix A for Syslog server setup)

Each of the SNMP servers can be setup to receive SNMP traps. Reset button removes on each panel the SNMP server setting.

Logging options panel shows options to enable/disable logging for different functions:

- **Critical Events** – this is always enabled, cannot be disabled. Log all critical events such as disk space full, critical component failure
- **Alerts** – this is always enabled, cannot be disabled. Suricata rule-based alerts of any severity
- **Search** – Log events for create/delete/cancel search, search completion, pause, resume.
- **StorageInfo** – Log events to show how much of Capture Storage is used/free, Search Storage is used/free.
- **Active Trigger Events** – Log active trigger events
- **Upload Data** – Log every upload file action from the UI (Upload search back rules, upload critical IPs and so on)
- **Download Data** – Log Download actions from the UI (Download PCAP data, Download searchback rules and so on)

11.5 SYSTEM EVENTS

The System event tab displays the Timestamp, Type and associated Message with severity. All events are clickable and searchable.

Severity can be one of three values: 1: Severe, 2: Warning, 3: Informational

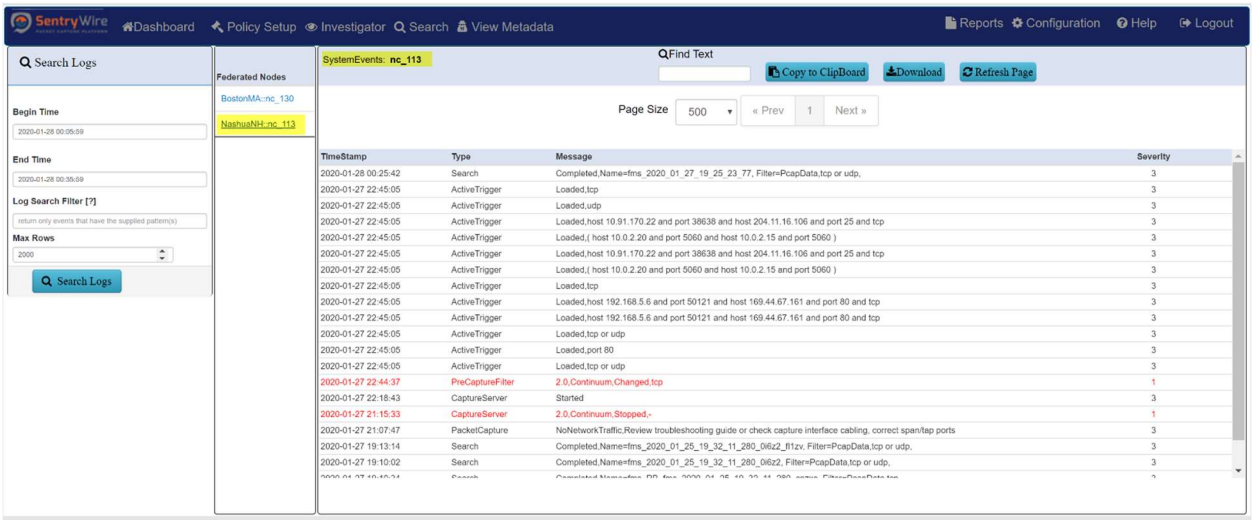


Figure 124-Node System Events view

11.5.1 Generate Report

The Generator Report tab allows the user to specify various parameters for generating reports that can be downloaded for review and analysis.

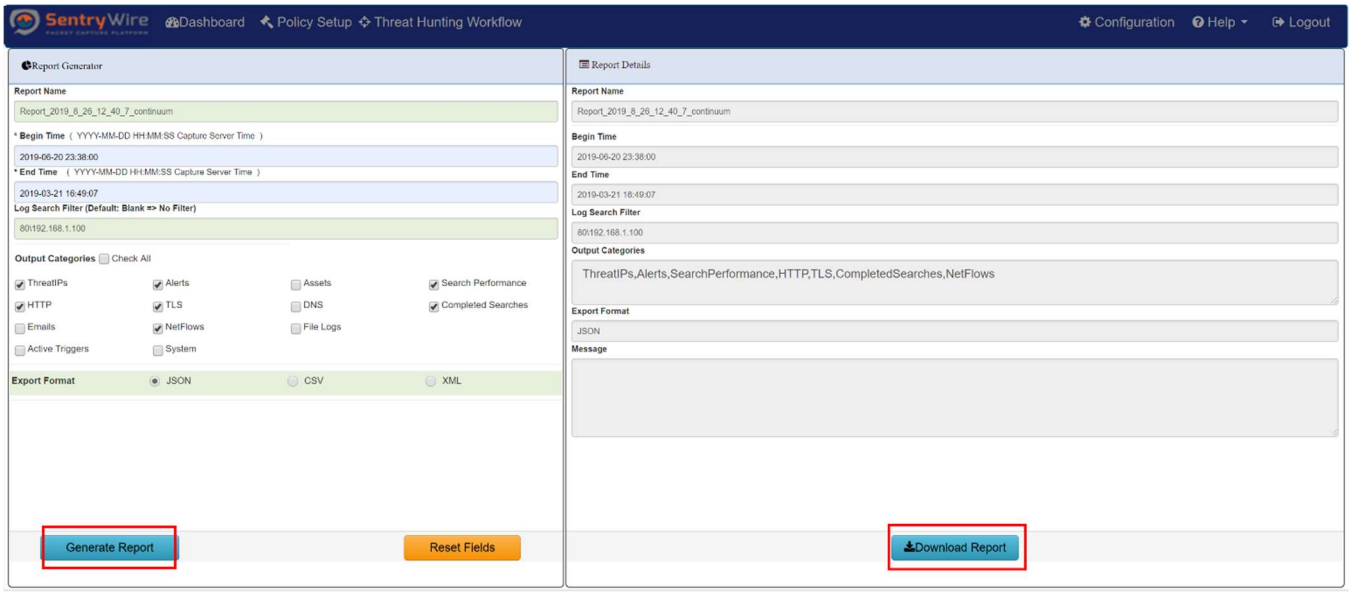


Figure 125-Report Generator view

- Report Name – System provides a default used name based on the current time. This can be edited to provide a suitable name.
- Begin/End time – The report output is restricted to the events and alerts between the times specified in these fields.
- Log Search Filter – The report output can be further restricted by log search filter. The rules of the Linux *grep* command's search string apply to this field.

Use Case

OR condition:

- *pattern1\|pattern2* returns strings that have either pattern1 OR pattern2 or both.

  For example: *google\|Microsoft* search filter returns strings like the ones shown below. This filter skips any string that does not include neither google nor Microsoft.
  - google may have been the first to implement this technology.
  - Microsoft is not too far behind.
  - Both google and Microsoft are fighting to take market share.

AND condition:

- *pattern1.*pattern2* returns strings that contain pattern1 before pattern2 in a string. It does not return strings that have pattern2 before pattern1.

  For example: *google.*Microsoft* search filter will return strings such as follows:
  - Both google and Microsoft are fighting for market share
- The above string skips the following sentences:
  - google has not commented on the news. (only *pattern1*, no *pattern2*)
  - Microsoft and google are fighting for market share (*pattern2* followed by *pattern1*)

- Output Categories – Allows user to select different types of event and alert data to be included in the report.
- Export Format – By default format is JSON. User can also specify the output to be in XML or CSV format.

To generate a report, user must click the "Generate Report" button, once the required fields are filled. The server will generate a *<ReportName>.zip* file that includes one file for each selected category. This zip file can be downloaded by clicking on Download Report button.

12 NETWORK CONFIGURATION

In order for this application to be accessible remotely, an IP address must be assigned to one of the Ethernet ports (typically eth0, eth1, or eth2). For initial configuration you may need to connect a VGA compatible monitor, boot up the system locally, login, and configure a static or DHCP IP address for your own network. After starting the system login as the root user (username: root, password: Contact support for default password to access the system or to change the password.)

Remote Login: 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.

Network Settings

Protocol	Description

DHCP	RHEL/CentOS, edit the following settings at: "/etc/sysconfig/network-scripts/ifcfg-eth2" (or eth3, etc.). • BOOTPROTO=dhcp • NM_CONTROLLED=yes • ONBOOT=yes
Static IP	***For example***: edit the following settings at: "/etc/sysconfig/network-scripts/ifcfg-eth2" (or ifcfg-eth3, etc.). • BOOTPROTO=static • BROADCAST=192.168.1.255 • DNS1=75.75.75.75 • DNS2=75.75.75.76 • GATEWAY=192.168.1.2 • IPADDR=192.168.1.1 • NETMASK=255.255.255.0 • NM_CONTROLLED=yes • ONBOOT=yes

APPENDIX A: CLIENT SYSLOG CONFIGURATION PROCEDURES

1. Edit /etc/rsyslog.conf

```
[root@client ~]# vi /etc/rsyslog.conf
```

2. At the end of file place the following line to point the client message log to the server

```
*.info;mail.none;authpriv.none;cron.none   @192.168.0.105
```

Note: Optionally choose hostname or IP address.

3. Restart the syslog service

```
[root@client ~]# service rsyslog restart
```

Message logs are now sent to both the central log server and local log files.

4. Verify Firewall Port opening(optional)

Generally production environments are protected by a hardware firewall. The following ports need to be opened: TCP & UDP 514. Verify the port opening by issuing the following command from the client:

```
[root@client ~]# telnet 192.168.0.105 514


Trying 192.168.0.105...
Connected to 192.168.0.105.
Escape character is '^]'.
```

If telnet is not available, use ssh to verify communications with server on port 514.

```
[root@localhost ~]# ssh -p 514 -v root@10.91.170.20
OpenSSH_5.3p1, OpenSSL 1.0.1e-fips 11 Feb 2013
debug1: Reading configuration data /etc/ssh/ssh_config
debug1: Applying options for *
debug1: Connecting to 10.91.170.20 [10.91.170.20] port 514
debug1: Connection established
debug1: permanently_set_uid: 0/0
debug1: identify file /root/.ssh/identify type -1
debug1: identify file /root/.ssh/identify-cert type -1
debug1: identify file /root/.ssh/id_rsa type -1
debug1: identify file /root/.ssh/id_rsa-cert type -1
debug1: identify file /root/.ssh/id_dsa type -1
debug1: identify file /root/.ssh/id_dsa-cert type -1
debug1: identify file /root/.ssh/id_ecdsa type -1
debug1: identify file /root/.ssh/id_ecdsa-cert type -1
```

5. To test that it is working perform the following command, and then confirm a record of the command restart is recorded in the logs:

```
[root@client~]# service ntpd restart
Shutting down ntpd:                                        [OK]
Shutting down ntpd                                         [OK]
```

Verify that similar messages appear in /var/log/messages
Client:

```
Aug 18 20:10:33 R730-2 ntpd[40092]: 0.0.0.0 c016 06 restart
Aug 18 20:10:34 R730-2 ntpd[40092]: 0.0.0.0 c012 02 freq_set kernel 4.085 PPM
```

Server:

```
Aug 18 20:10:33 R730-2 ntpd[40092]: 0.0.0.0 c016 06 restart
Aug 18 20:10:33 R730-2 ntpd[40092]: 0.0.0.0 c012 02 freq_set kernel 4.085 PPM
Aug 18 20:10:34 R730-2 ntpd[40092]: 0.0.0.0 c615 05 clock_sync
```

APPENDIX B: LEEF MESSAGE FORMAT

The syslog messages are generated and reported in the format

<DateTime> <localhost> LOGMSG: 2.0| OrgName |BrandName |Version|<ID>|cat=<category> msg=<message>

For example: when capture server starts on the localhost, the following syslog message is added to /var/log/messages file:

Jan 06 22:27:49 localhost LOGMSG: 2.0| OrgName | BrandName|Version| Started |cat= PacketCapture

LOGMSG: 2.0| OrgName|BrandName|Version| Changed |cat=PrecaptureFilter msg= <text> - This event is generated when a PreCapture filter is added or updated.

LOGMSG: 2.0| OrgName|BrandName|Version| Reset |cat=PrecaptureFilter msg<text> This event is generated when a PreCapture filter is deleted.

LOGMSG: 2.0| OrgName|BrandName|Version|Loaded|cat=ActiveTrigger msg <text>-This event is generated when an active trigger is added.

LOGMSG: 2.0| OrgName|BrandName|Version| Updated |cat=ActiveTrigger msg <text>- This event is generated when an active trigger is updated.

LOGMSG: 2.0| OrgName|BrandName|Version| Deleted|cat=ActiveTrigger msg <text>- This event is generated when an active trigger is deleted.

LOGMSG: 2.0| OrgName|BrandName|Version|Triggered|cat=ActiveTrigger msg <text>- This event is generated when an active trigger is fired.

LOGMSG: 2.0| OrgName|BrandName|Version| Created|cat= Search msg <text>- This event is generated when a search is created.

LOGMSG: 2.0| OrgName|BrandName|Version| Completed|cat= Search msg <text>- This event is generated when a search is completed.

LOGMSG: 2.0| OrgName|BrandName|Version| Deleted|cat= Search msg <text>- This event is generated when a search is deleted.

LOGMSG: 2.0| OrgName|BrandName|Version| Cancelled|cat= Search msg <text> - This event is generated when a search is cancelled.

LOGMSG: 2.0| OrgName|BrandName|Version| Failed|cat= Search msg="Search storage full. Remove old search data and try again" - This event is generated when a search storage is full.

LOGMSG: 2.0| OrgName|BrandName|Version| Pause|cat= Search msg="Search storage full. Remove old search data. Search will automatically resume after old search data removed." - This event is generated when an ongoing search pauses because the search storage is full.

LOGMSG: 2.0| OrgName|BrandName|Version| Resume|cat= Search msg="Search resumed as the storage space freed up" - This event is generated when a currently paused search resumes as the user has freed up search storage space by deleting old search(es).

LOGMSG: 2.0| OrgName|BrandName|Version| SessionReset|cat= Admin - This event is generated when a user with Admin privilege has pressed the "Reset Session" button.

LOGMSG: 2.0| OrgName|BrandName|Version|UserAdded|cat= Admin- This event is generated when a user new user has been added.

LOGMSG: 2.0| OrgName|BrandName|Version| UserDeleted|cat= Admin- This event is generated when an existing user has been deleted.

LOGMSG: 2.0| OrgName|BrandName|Version| UserError|cat= Admin -This event is generated when an error occurred on adding/updating/deleting a user.

LOGMSG: 2.0| OrgName|BrandName|Version| UserChanged|cat= Admin -This event is generated when an existing user's password or role has been changed.

LOGMSG: 2.0| OrgName|BrandName|Version| UserLocked|cat= Admin -This event occurs to alert that a user has been locked after 3 unsuccessful attempts to login with a span of 30 minutes

LOGMSG: 2.0| OrgName|BrandName|Version| UserUnlocked|cat= Admin - This event occurs to alert that a previously locked user has been unlocked by an Admin user or 30 minutes have elapsed since the user has been locked.

LOGMSG: 2.0| OrgName|BrandName|Version|Demo|cat=Licensing msg <text> - This event is generated to alert that the license that has been applied is a Demo license.

LOGMSG: 2.0| OrgName|BrandName|Version| Expired|cat=Licensing msg <text> -This event is generated to alert that the license has expired.

LOGMSG: 2.0| OrgName|BrandName|Version| Permanent|cat=Licensing msg <text> -This event is generated to alert that the license that has been applied is a Permanent license.

LOGMSG: 2.0| OrgName|BrandName|Version| HyperThreading NotEnabled|cat=PacketCapture msg ="Warning: HyperThreading must be enabled." - This event is generated to alert that hyper threading has not been enabled as it is a requirement for successful operation of a capture server.

LOGMSG: 2.0| OrgName|BrandName|Version| Started|cat=PacketCapture - This event is generated to alert that capture server has been started.

LOGMSG: 2.0| OrgName|BrandName|Version| Stopped|cat=PacketCapture - This event is generated to alert that the capture server has been stopped.

LOGMSG: 2.0| OrgName|BrandName|Version| NoNetworkTraffic|cat= PacketCapture msg="Review troubleshooting guide or check capture interface cabling, correct span/tap ports"- This event is generated to alert that the capture server is not receiving any traffic at the moment.

LOGMSG: 2.0| OrgName|BrandName|Version| CaptureStats |cat= PacketCapture msg="LOGMSG: 2.0| OrgName|BrandName|Version| PacketCapture|cat=CaptureStats msg=Throughput:7.71, PacketsPerSec:1357894, TCP:1357794, UDP:100, Other:0, CompressionRatio:1.21" - This is a stat reporting event, occurs once every minute.

LOGMSG: 2.0| OrgName|BrandName|Version|System|cat=RootFileSystem msg=WARNING: / file system usage is above 70%.0..the system will be shut down if above 90%

LOGMSG: 2.0| OrgName|BrandName|Version|CaptureServerSetup|cat=System msg=WARNING: One or more directories/symlinks are invalid. Please contact support.

APPENDIX C: PCAP PORT INFORMATION

The following list of TCP ports need to be opened for external access on a PCAP master:

- 4477 - ssh port
- 41395 - WEB UI access
- 41392 - PCAP REST API access

In Clustered environments, the following list of TCP ports must be opened for **Data Node** access on a PCAP master:

- 41391, 41393 through 41396 - data node send node status, license info, system usage info and search lists and search data
- 41500 - data node send node status, license info, system usage info and search lists and search data

In case of Cluster, the following list of TCP ports must be opened for PCAP **Master Node** access on EACH PCAP data node:

- 4477 - ssh port
- 5000 through 5021 - PCAP master sends PCAP data and status requests. All of these ports must be open

Note: *All the ports mentioned above are TCP.*

Note: *There should be no ports open for external access on a PCAP data node.*

APPENDIX D: 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, port range. If there is no qualifier, host is assumed

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

proto
qualifiers restrict the match to the particular protocol. Possible protocols are: ether, fddi,tr, wlan, IP, IPv6, arp, rarp, decnet, tcp and udp.

Primitive Filters
Allowable primitives are given below for reference:

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

Primitive Filters	Description
[src|dst] net <network> E.g., dst net 192.168.1.0 src net 192.168.1 dst net 172.16 src net 10 net 192.168.1.0 net 192.168.1.0/24 src net 192.168.1/24	Matches packets to or from source/destination or either, residing in a network. An IPv4 network number can be specified as: • Dottedquad(e.g.,192.168.1.0) • Dotted triple (e.g., 192.168.1) • Dotted pair (e.g., 172.16) • Or single number (e.g., 10)
[src|dst] net <network> mask <netmask> **or** [src|dst] net <network>/<len> E.g., dst net 192.168.1.0 mask 255.255.255.255 **or** dst net 192.168.1.0/24 src net 192.168.1 mask 255.255.255.0 **or** src net 192.168.1/24 dst net 172.16 mask 255.255.0.0 src net 10 mask 255.0.0.0	Matches packets with specific netmask. /len can also be specified to capture traffic from range of IP addresses. • Netmask for dotted quad (e.g., 192.168.1.0) is 255.255.255.255 • Netmask for dotted triple (e.g., 192.168.1) is 255.255.255.0 • Netmask for dotted pair (e.g.,172.16) is 255.255.0.0 • Or single number (e.g.,10) is 255.0.0.0
[src|dst] port <port> or [tcp|udp] [src|dst] port <port> e.g., src port 443 dst port 20 port 80	Matches packets sent to/from port • Protocols (e.g., tcp/udp/IP etc.) can be applied to a port to get specific results
[src|dst] portrange <p1>-<p2> or [tcp|udp] [src|dst] portrange <p1>-<p2> E.g., src portrange 80-88 tcp portrange 1501-1549	Matches packets to/from a port in the given range • Protocols can be applied to port range to filter specific packets within the range
less <length> E.g., less 300	Matches packets less than or equal to length
greater <length> E.g., greater 301	Matches packets greater than or equal to length
(ether|ip|ip6) proto <protocol> E.g., ether proto 0x888e IP proto 50	Matches an Ethernet, IPv4, or IPv6 protocol • 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

Primitive Filters	Description
(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) o vlan && vlan 300 && IP (filters IPv4 protocols encapsulated in vlan 300 encapsulated within any higher order vlan)	Matches 802.1Q frames optionally with a VLAN ID of vlan
mpls [<label>] o E.g., mpls 100000 && mpls 1024	Matches MPLS packets, optionally with a label of label
(filters packets with outer label 100000 and inner Label 1024) o 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)	• mpls expression may be used more than once, to filter on MPLS hierarchies.

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

Modifiers

Types of valid modifiers/operators:

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

Examples of some filters using operators and modifiers:

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

APPENDIX E: DECRYPTING PCAPS WITH SSL SESSION KEYS

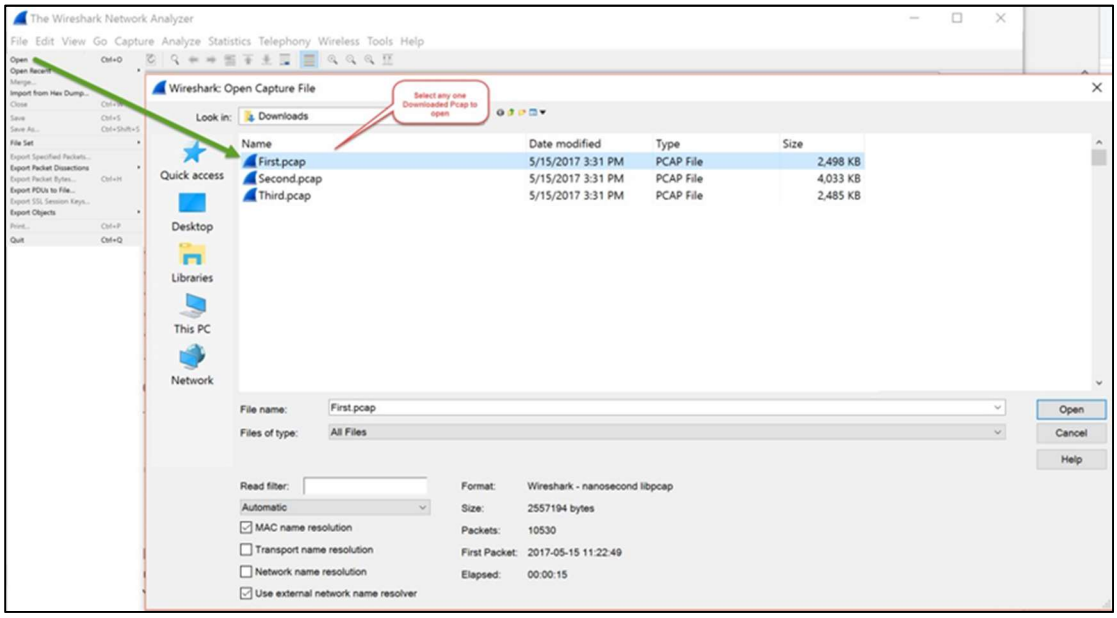
Decrypting PCAP data using SSL session key

This workflow presumes a set of SSL Session keys for decrypting PCAP data is available.

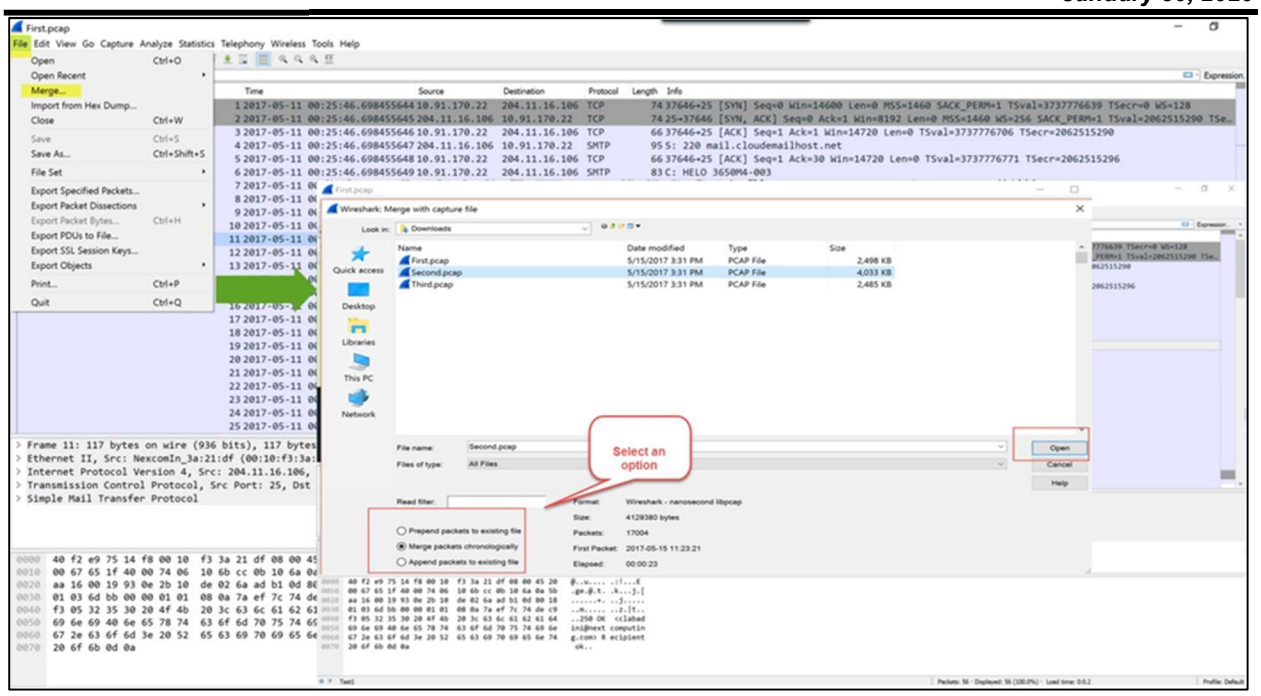
1. Download one or more (encrypted) PCAPs from a completed PCAP search.

Note: If the sessionized TLS/SSL search results in more than 1 PCAP, the PCAPs must be merged into a single PCAP so that one complete session can be loaded into Wireshark in order to decrypt it with a key.

2. User can download all PCAPs using the "Download All" option.
3. Once downloaded the PCAPs should be merged.
    a. To merge PCAPs on a windows operating system follow the below steps:
        i. Click "Download All" to download the PCAPs on the system.
        ii. Launch Wireshark and select any one downloaded PCAP to open it.



        iii. Once opened, the File→Merge option will be available for use.
        iv. Select the PCAP that needs to be merged. Once the PCAP is merged save the new merged PCAP and repeat the steps to merge all PCAPs associated with that session.



b. To merge PCAPs on a unix operating system follow the below steps:
   i. Click "Download All PCAP" hyperlink to download all PCAPs on to a unix system. This will download the .zip file containing all the PCAPs.
   ii. cd <downloads folder>
   iii. unzip the .zip file that has just been downloaded.

   Example: unzip 46106e0a-fce5-4cc5-8046-fb8090767e16.zip

   Where 46106e0a-fce5-4cc5-8046-fb8090767e16 is the search uuid

   iv. cd 46106e0a-fce5-4cc5-8046-fb8090767e16
   v. ls -l*.PCAP
   vi. This will show all downloaded PCAPs

   Example Figure:

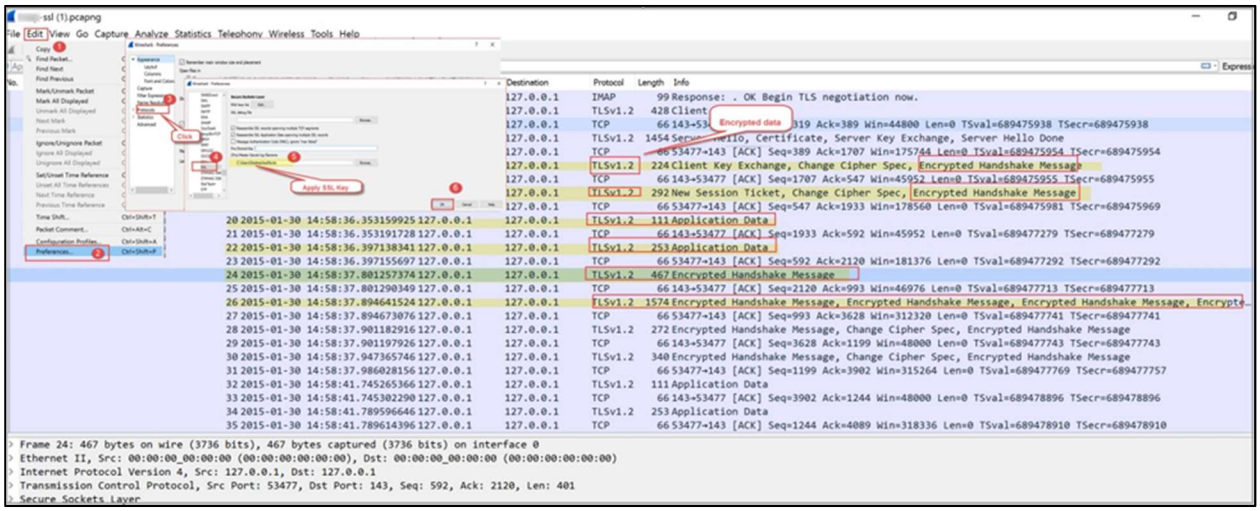
```
ls -l *.pcap
-rw-r--r--. 1 root root  347304 May  7 16:32 0.pcap
-rw-r--r--. 1 root root  351645 May  7 16:32 1.pcap
-rw-r--r--. 1 root root 1046205 May  7 16:32 2.pcap
-rw-r--r--. 1 root root 1775493 May  7 16:32 3.pcap
-rw-r--r--. 1 root root 2652375 May  7 16:32 4.pcap
```

   vii. Use mergecap command to combine these PCAPs into a single PCAP.
   viii. Perform the following command:

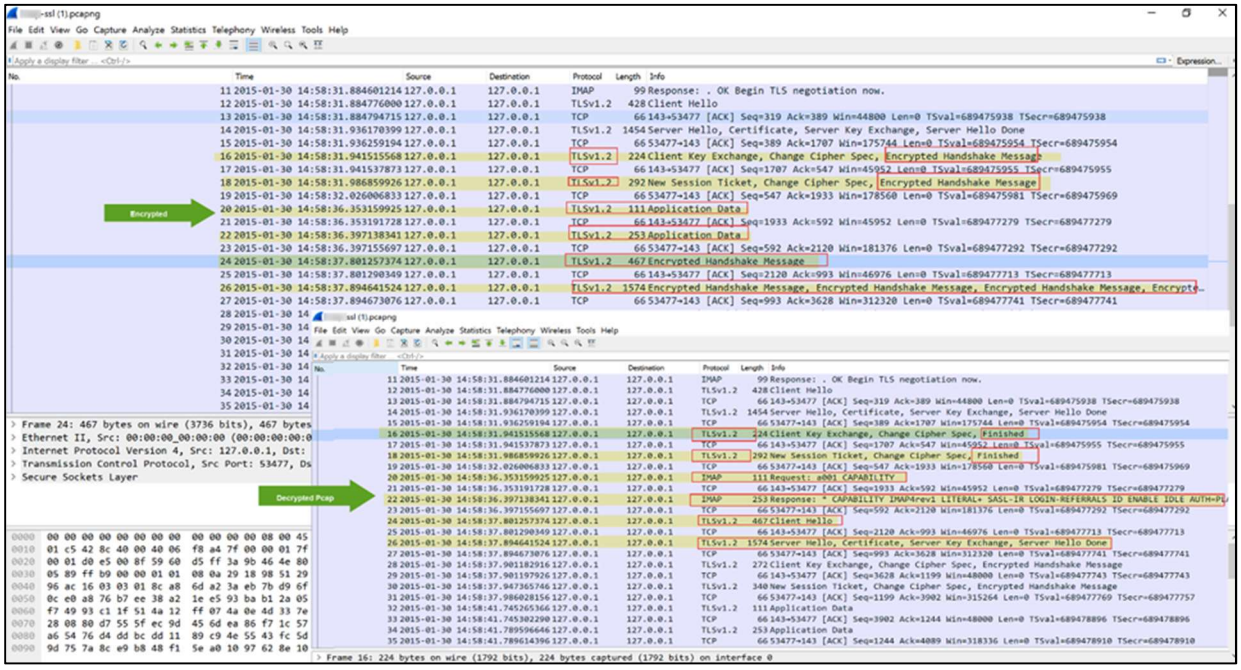
```
mergecap -a -w combined.pcap 0.pcap 1.pcap 2.pcap 3.pcap 4.pcap
ls -l combined.pcap
```

   ix. This PCAP contains all the data produced by the search.
   x. Copy/Download this PCAP to a system that has Wireshark application.

4. Now open the merged PCAP in Wireshark
5. Select Edit → Preferences…
6. Select and expand Protocols, scroll down and select SSL (or type ssl)



7. Click Browse button under (Pre)-Master-Secret log filename.
8. Select the Session Key filename to be loaded.
9. [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.
10. Click OK
11. 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 F: UNDERSTANDING BEHAVIOR SEARCH

This feature provides sessioninfo of a URL based relationship between a HTTP and Email session or between a DNS, HTTP and Email session. Alerts are generated if a particular URL is present in both a HTTP stream AND an email body. If the domain/sub-domain associated with that particular URL appears in a DNS session, then DNS session is also included in the alert. These alerts help to analyze and track activities based on user's behavior/actions.

For example:

- Has the user clicked on a URL received in an email body?
- Does the URL string indicate the domain of a well-known company (bofa.com) but the underlying hostname resolves to a blacklisted IP address?
- Has the user visited the web page?
- What kind of links are attracting the users to click on and what kinds are being ignored?

The Behavior search feature under Log Manager is a user-friendly capability that requires no setup nor prior knowledge of which domains to look for.

The following use cases provide a better understanding of this feature:

Use Case 1: Email, DNS, HTTP correlation event

1. A user receives an email. The email body contains invitation to click on a URL: http://www.visitparadise.us.
2. This action will result in one email alert under Log Manager → Email tab
3. The user clicks on the URL.
4. As this host is unknown, the system generates a DNS query for www.visitparadise.us.
5. This action results in one DNS alert under Log Manager → DNS tab.
6. When the http request is successful and the user is now on http://www.visitparadise.us page an HTTP alert is produced/displayed under Log Manager → HTTP tab.
7. As the same URL appears in both HTTP and Email sessions and its associated domain request appears in a session, a new alert appears under Log Manager → Behavior Search tab.

Note*: The Log Manager → Behavior Search → DNS, HTTP, Email Correlation Alert is NOT generated if either step 3, step 4 OR 6 is skipped.*

Use Case 2: Email, HTTP correlation event

1. A user receives another email. The email body contains invitation to click on http://www.visitparadise.us again.
2. This action will result in one email alert under Log Manager → Email tab.
3. The user clicks on the URL.
4. As this host is now known, there is no DNS query hence no DNS alert.
5. The http request is successful and the user is now on http://www.visitparadise.us page.
6. This will generate/display one HTTP alert under Log Manager → HTTP tab.
7. As the same URL appears in both HTTP and Email sessions, a new alert appears under Log Manager → Behavior Search tab with session details for HTTP and Email.

***Note**: The Log Manager → Behavior Search → HTTP, Email Correlation Alert is NOT generated if step 3 is skipped.*

APPENDIX G: UNDERSTANDING RULESETS

In order to create a ruleset it is important to understand the rule format supported by Suricata. A rule/signature consists of the following Action, Header and Rule-options.

Example: alert IP [100.64.0.0/10] 1024 → 5.6.7.8 80 (msg:"[100.64.0.0/10]"; sid:300;)

In the above example: alert is an action.
IP [100.64.0.0/10] 1024 → 5.6.7.8 80 is a header.
(msg:"[100.64.0.0/10]"; sid:300;) is a rule-option.

Action:
The action property determines what will happen when a signature matches. Suricata processes these rules based on priorities associated with the signature. The most important signatures will be scanned first.

Below is a summary of actions in default order based on priority:

Action	Description
Pass	If a signature matches and contains pass, Suricata stops scanning the packet and skips to the end of all rules (only for the current packet).
Drop	This only concerns the IPS/inline mode. If the program finds a signature that matches, containing drop, it stops immediately. The packet will not be sent any further. Drawback: The receiver does not receive a message of what is going on, resulting in a time-out (certainly with TCP). Suricata generates an alert for this packet.
Reject	This is an active rejection of the packet. Both receiver and sender receive a reject packet. There are two types of reject packets that will be automatically selected. If the offending packet concerns TCP, it will be a Reset-packet. For all other protocols it will be an ICMP-error packet. Suricata also generates an alert. When in Inline/IPS mode, the offending packet will also be dropped like with the 'drop' action.
Alert	If a signature matches and contains alert, the packet will be treated like any other non-threatening packet, except for this one an alert will be generated by Suricata. Only the system administrator can notice this alert.

Example Rule: alert IP [100.64.0.0/10] 1024 → 5.6.7.8 80 (msg:"[100.64.0.0/10]"; sid:300;)

This rule sets an alert action when source IP [100.64.0.0/10] matches with the destination IP 5.6.7.8

Header:

The header part of the rule allows to keep a watch on the protocols concerned, the source and destination IP- addresses, ports involved and their direction of flow.

Protocol:

This keyword in a signature tells Suricata which protocol we want our rule to keep an eye out for. Below are the five options to choose from.

1. IP - When IP is specified it will watch for all or any packets on the network.
2. tcp - When tcp is specified it will match a rule against TCP traffic.
3. udp - When udp is specified it will match a rule against UDP packets.
4. icmp - When icmp is specified it will match a rule for ICMP packets.
5. Suricata also allows you to specify layer 7 protocols like HTTP (http), SSL and TLS (tls for both), FTP (ftp) and SMB (smb) as well.

Source and Destination IP and Port:

This allows you to assign source and destination IP-addresses (IPv4 and IPv6 combined as well as separated) and the desired ports.

You can specify multiple IPs and ports. Below are some example and guidelines:

Sign	Description	Example
!	An exclamation specifies “not”	**Ex**: !1.1.1.1 which means any IP except 1.1.1.1
[ ] and ,	A square bracket is used to specify multiple IPs or ports separated by comma	**Ex**: ![1.1.1.1,1.1.1.2] Every IP address but 1.1.1.1 and 1.1.1.2 **Ex**: [10.0.0.0/24, !10.0.0.5] Except 10.0.0.5 matches all 10.0.0.0/24
:	A colon is used to specify range	**Ex.**: [80, 81, 82] Includes port 80, port 81,port82 **Ex**: [80:82] Includes port range from 80 till 82 **Ex**: [1024:] From 1024 till the highest port-number **Ex**: !80 Every port but 80 **Ex**: [80:100,!99] Range from 80 till 100 but 99 excluded

***Note**: In addition to set specific IP addresses you can also use a Yaml-file to set IP- addresses for variables such as HOME_NET or EXTERNAL_NET. These settings will be used when you use these variables in a rule. In source and destination you can make use of signs like ! And [ ].*

Using variable HOME_NET allows you to set the relevant IP-address for several rules. This option contains the address group vars that will be passed in a rule.

Using EXTERNAL_NET signifies ! HOME_NET

(For more information on using variable see refer to the link below -
http://suricata.readthedocs.io/en/latest/configuration/suricata-yaml.html#suricata-yaml-rule-vars

Direction Specification:
Between the IP and ports is the direction of packet flow. The direction tells in which way the signature has to match.

□	This is the most common and means only check if the source IP and port are coming in to the destination IP and port
<>	This will match packet flow in either direction

Example Rule1:

alert tcp [100.64.0.0/10] 1024 → 5.6.7.8 80 (msg:"[100.64.0.0/10]"; sid:300;)

This rule sets an alert action when protocol tcp, source [100.64.0.0/10], port 1024 matches with the destination IP 5.6.7.8, port 80

Example Rule2:

drop tcp $HOME_NET any → $EXTERNAL_NET any (msg:"[OK to drop]"; sid:500;)

This rule sets a drop action when protocol tcp, source $HOME_NET port any matches with the destination
$EXTERNAL_NET and port any

Where: $HOME_NET and $EXTERNAL_NET are variables set for IP-addresses as defined in the Yaml-file.

Rule-options:
There are many rule-options but they can be categorized mainly into 5 categories.

1. Meta-settings: This is the most used rule-option. Meta-settings have no effect on Suricata's

inspection, but they do affect the way event are reported in Suricata. The 3 main meta-settings are:

- msg: The keyword msg gives more information about the signature and the possible alert. Example- msg: "Attack Forbidden";

- sid: The keyword sid gives every signature its own unique id. This id is stated with a number Example- sid:123;

- rev: The sid keyword is almost every time accompanied by rev. Rev represents the version of the signature. If a signature is modified, the number of rev will be incremented by the signature writers. Example- rev:123;

Example Rule: alert tcp [100.64.0.0/10] 1024 → 5.6.7.8 80 (msg:"[100.64.0.0/10]"; sid:300; rev2;)

For more information on meta-settings, please refer to the following link:

http://suricata.readthedocs.io/en/latest/rules/meta.html

2. Payload: Payload keywords inspect the content of the payload of a packet or stream (the packet data itself, such as IRC commands). For more information on meta-settings, please refer to the following link:

   http://suricata.readthedocs.io/en/latest/rules/payload-keywords.html

3. HTTP: These keywords make sure the signature checks only specific parts of the network traffic. For instance, to check specifically on the request URI, cookies, or the HTTP request or response body, etc. For more information on meta-settings, please refer to the following link:

   http://suricata.readthedocs.io/en/latest/rules/http-keywords.html

4. Flowbits: Flowbits consists of two parts. The first part describes the action it is going to perform, the second part is the name of the flowbit. Flowbits can make sure an alert will be generated when, for example two different packets match. An alert will only be generated when both packets match. For more information on meta-settings, please refer to the following link-
   http://suricata.readthedocs.io/en/latest/rules/flow- keywords.html

5. IP Reputation Rules: Gives an idea if an IP is legit or known to be associated with malware, spam, etc. For more information on meta-settings, please refer to the following link- http://suricata.readthedocs.io/en/latest/reputation/ipreputation/ip-reputation-rules.html

***Note**: For a more descriptive information about creating user defined rule-sets please refer to the link below:*

http://suricata.readthedocs.io/en/latest/rules/intro.html

APPENDIX H: FASTCOPY WORKFLOW

FastCopy workflow allows Federation Manager initiated search data from multiple Federation Nodes to be merged to a single Federation Node.

Workflow

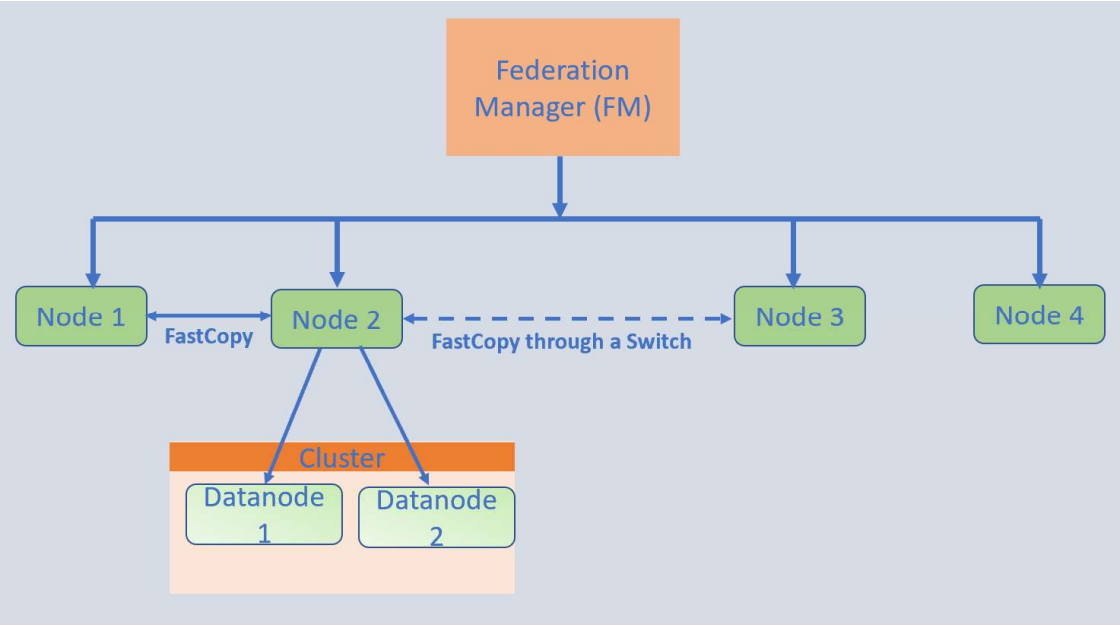
- When a search is created from Federation Manager, the search request goes to all selected Federated Nodes.
- When a search is complete, the PCAPs are merged based on the connectivity and connection status of each node.
- Each Federation Node is in one of the given FastCopy states:

Icon	Action	Description
	FastCopyOff	When a Federation Node does not participate in FastCopy workflow
	FastCopyDisabled	When a Federation Node is configured to participate in FastCopy workflow, but it is currently disabled
 or 	FastCopySingle	When a Federation Node is connected to one other Federation Node for FastCopy
	FastCopyDual	When a Federation Node is connected to two other Federation Node for FastCopy

<u>UseCase</u>

For Example:

Node 1 is FastCopySingle node, Node 2 is FastCopyDual node, Node 3 is FastCopySingle node and Node 4 is FastCopyOff.



- **Scenario 1**:
    - If Node1 and Node3 are connected to Node2.
    - And a search is sent to three nodes Node1, Node2, and Node3 from FM
    - Node1 and Node3 send their search PCAPs to Node2.
    - Federation Manager will show one row for a single merged pcap for the pcap data from Node1, Node2 and Node3

- **Scenario 2**:
    - If Node1 and Node3 are connected to Node2.
    - And a search is sent to all four nodes in the federation - Node 1, Node 2, Node 3 and Node 4.
    - Where Node4 is not connected to Node2.
    - Node1 and Node3 send their search PCAPs to Node2.
    - Node4 does not send its PCAPs.
    - Federation Manager will show two rows:
    - One row for a single merged pcap for the pcap data from Node1, Node2 and Node3
    - 2nd row for a single pcap for the pcap on Node4

APPENDIX I: TECHNICAL SUPPORT

SentryWire is proud to offer 24x7 support for all SentryWire products.

SentryWire support requests will be acknowledged on the following schedule:

Features	Product Support Response Time	Support Request Method
Hours of Operation	Normal Business Hours: 8AM to 11PM EST 24 Hours/Day 7 Days/Week 365 Days/Year	**Phone:** 443-561-0510 **Web:** http: //support.sentrywire.com
Critical (Severity 1) - Includes hardware based issues that impact the ability to capture and search	30 Min or Less: 24x7	**Phone support only after Normal Business Hours**
Major (Severity 2) - Includes non-hardware related issues that impact the ability to capture and search	1 hour or Less: 24x7	**Phone support only after Normal Business Hours**
Minor (Severity 3) - Includes issues that do not impact capture or search capability such as product updates	Within 8 hours: Normal Business Hours	**Phone or Web**
Informational (Severity 4) - Includes How-To and What-If type questions	Within 12 hours: Normal Business Hours	**Phone or Web**

Software:

12 Months of software support

Hardware:

Includes 36 Months of Hardware Service and Support provided on all parts and labor by hardware manufacturer.

On-site, On-Line VIP Service Portal, Global Remote Service and On Site Engineer as required, 7x24x365.

APPENDIX J: KEY TERMS

The following table provides definitions and explanations for terms and acronyms relevant to the content presented within this document.

TERM	DEFINITION
BPF	Berkely Packet Filter
Gbps	Gigabits per second
IP	Internet Protocol
HTTP	Hyper Text Transfer Protocol
IDS	Intrusion Detection System
IoC	Indicators of Compromise
LEEF	Log Event Extended Format
PCAP	In the field of computer network administration, PCAP consists of an application programming interface for capturing network traffic.
Suricata	Suricata is a free and open source, mature, fast and robust network threat detection engine. The Suricata engine is capable of real time intrusion detection (IDS), inline intrusion prevention (IPS), network security monitoring (NSM) and offline PCAP processing.
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UI	User Interface