SentryWire
PACKET CAPTURE PLATFORM

REST API Guide
Software Version 7.3.0.309-408.14

03/05/2022

Document Revision History

Rev 1.0	Initial Release	06/25/2021
Rev 1.1	Updates/Corrections	07/07/2021
Rev 1.2	FM Node API merged into the FM Unified API	09/10/2021
Rev 1.3	File Carving, Selectable Nodes	10/30/2021
Rev 1.4	Updates/corrections	11/15/2021
Rev 1.5	/v2/exportpolicy	03/05/2022

Notes

The example requests (curl commands) can be copy/pasted. Please double check quotes, spaces, newlines before using the curl commands.
Login requests require username and password. All operations require a valid rest_token.
All requests are sent to port 41395
This API is compatible with FM version 7.3.0-309-408.14r2.23 or later

Federation Manager - Login

This is a HTTP POST request to the server’s /v2/fmlogin endpoint to login.

Request

Name	Type	Remarks
username	string	Required
password	string	Required

Return Codes and Response

200	username and password are valid for access. The server sends a token to be used for all subsequent requests.
400	username and/or password are missing; the server sends error information as part of the response.
401	Invalid username and/or password

Example

Request

```
curl --silent --insecure -X POST -H 'Content-Type: application/json' -d '{"username":"testuser123","password":"A@R3t08Dc
}' https://10.1.55.152:41395/v2/fmlogin
```

Response

```
{"rest_token":"8e1eeb1f-106d-1f5b-2166-1c1e2e136611"}
```

Configuration – Add Group

This is a HTTP POST request to the server's /v2/fmgroup endpoint to add a FM group. A group can have zero or more FM nodes.

Request

Name	Type	Remarks
rest_token	string	Required
group_name	string	Required

Return Codes and Response

200	Required parameters have been specified; all parameters are valid.
400	A required parameter is missing
401	rest_token does not refer to a valid login request or a group with group_name already exists.

Example

Request

```
curl --silent --insecure -X POST -H 'Content-Type: application/json' -d '{"group_name":"group3","rest_token":"714821c8-3c54-b8a8-a0b6-a471267b9a79" }' https://10.91.170.179:41395/v2/fmgroup
```

Response

```
{
  "message": "added group group3"
}
```

Configuration – Add a Federation Node

This is a HTTP POST request to the server’s /v2/fmnode endpoint to add a FM node to a group. A group can have zero or more FM nodes.

Request

Name	Type	Remarks
rest_token	string	Required
group_name	string	Required – this group must exist
nodeaddr	string	Required – this is the ip address of the federation node to be added.

Return Codes and Response

200	Required parameters have been specified; all parameters are valid.
400	A required parameter is missing, group_name is invalid
401	rest_token does not refer to a valid login request

Example

Request

```
curl --silent --insecure -X POST -H 'Content-Type: application/json' -d
'{"group_name":"group3",”nodeaddr”:”10.91.170.179”, "rest_token":"714821c8-3c54-b8a8-a0b6-a471267b9a79" }'
https://10.91.170.179:41395/v2/fmnode
```

Response

```
{
  “message”:”added node nc179”
}
```

Configuration – Get Status

This is a HTTP GET request to the server’s /v2/fmping endpoint to get FM server status.

Request

Name	Type	Remarks
rest_token	alphanumeric string	Required

Return Codes and Response

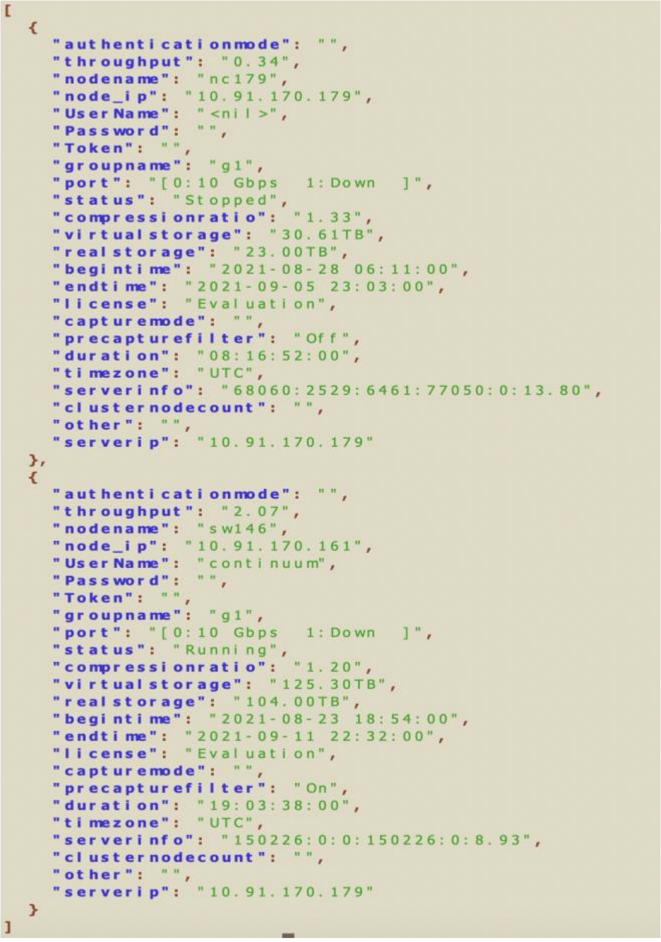
200	rest_token is valid
400	rest_token is missing
401	rest_token is invalid

Example

Request

```
curl --silent --insecure -X GET 'https://10.91.170.179:41395/v2/fmping?rest_token=714821c8-3c54-b8a8-a0b6-
```

Response



```
[
  {
    "authenticationmode": "",
    "throughput": "0.34",
    "nodename": "nc179",
    "node_ip": "10.91.170.179",
    "UserName": "<nil>",
    "Password": "",
    "Token": "",
    "groupname": "g1",
    "port": "[0:10 Gbps   1:Down   ]",
    "status": "Stopped",
    "compressionratio": "1.33",
    "virtualstorage": "30.61TB",
    "realstorage": "23.00TB",
    "begintime": "2021-08-28 06:11:00",
    "endtime": "2021-09-05 23:03:00",
    "license": "Evaluation",
    "capturemode": "",
    "precapturefilter": "Off",
    "duration": "08:16:52:00",
    "timezone": "UTC",
    "serverinfo": "68060:2529:6461:77050:0:13.80",
    "clusternodecount": "",
    "other": "",
    "serverip": "10.91.170.179"
  },
  {
    "authenticationmode": "",
    "throughput": "2.07",
    "nodename": "sw146",
    "node_ip": "10.91.170.161",
    "UserName": "continuum",
    "Password": "",
    "Token": "",
    "groupname": "g1",
    "port": "[0:10 Gbps   1:Down   ]",
    "status": "Running",
    "compressionratio": "1.20",
    "virtualstorage": "125.30TB",
    "realstorage": "104.00TB",
    "begintime": "2021-08-23 18:54:00",
    "endtime": "2021-09-11 22:32:00",
    "license": "Evaluation",
    "capturemode": "",
    "precapturefilter": "On",
    "duration": "19:03:38:00",
    "timezone": "UTC",
    "serverinfo": "150226:0:0:150226:0:8.93",
    "clusternodecount": "",
    "other": "",
    "serverip": "10.91.170.179"
  }
]
```

Investigator – Create a FM Search

This is a HTTP POST request to the server's /v2/fmsearch endpoint to start a new search on each Federation node.

Request

Name	Type	Remarks
rest_token	string	Required**.** REST token from a valid login request
search_name	string	Required
search_filter	string	• Optional – Default: *tcp or udp* • **bpf <***bpffilter***> logtext <***logsearchfilter***> payload <***payloadfilter***> extends bpf <***bpffilter***> logtext <***logsearchfilter***> payload** • ***logtext*** is optional. If specified, gets only entries that have the *logsearchfilter*. Otherwise, gets all the alert/dpi data of the search. • ***payload*** is optional. If specified, gets only those packets that satisfy *bpffilter* AND have the payload specified by *payloadfilter*. Otherwise, gets all packets that satisfy *bpffilter* • ***extends*** is optional. This allows multiple independent search filters to be combined Examples: • bpf tcp or udp logtext example.com payload HTTP • tcp or udp logtext example.com • port 80 payload example.com • host 1.2.3.4 and port 110 • port 80 payload example.com extends port 53 payload abcd
begin_time	string	Required – UTC time - YYYY-MM-DD hh:mm:ss eg., 2015-04-10 15:55:01
end_time	string	Required – UTC time - YYYY-MM-DD hh:mm:ss eg., 2015-04-10 15:57:01
max_packets	non-negative integer	Optional - Default: 0 => get all packets example: 1000 – search stops on finding 1000 packets.

Return Codes and Response

200	All the required parameters have been supplied and valid. The server sends a search token
400	A required parameter is missing or one or more parameters such as search_filter is invalid;
401	Invalid rest_token

Example

Request

```
curl  --insecure --silent -X POST -H 'Content-Type: application/json' -d '{"rest_token":"4c8b8917-8926-37bd-46a9-
73a153273c58","search_name":"rest2","begin_time":"2021-09-11 10:00:00","end_time":"2021-09-11
12:00:00","max_packets":"1000","PayloadSearchFilter":"", "LogSearchFilter":"", "search_filter":"tcp" }'
https://10.91.170.179:41395/v2/fmsearch
```

Response

```
{
  "searchname”: " continuum_1631377579_1_rest2"
}
```

Investigator – Get Search Status

This is a HTTP GET request to the server's /v2/fmsearch/status endpoint to get the current status of a search. This is an idempotent operation.

Request

Name	Type	Remarks
rest_token	string	Required Valid token from the server after login.
searchname	string	Required. Valid searchname (either returned by /v2/fmsearch POST or the name of FM UI created search)
nodename	string	Required. Federation node name where the search ran or is running

Return Codes and Response

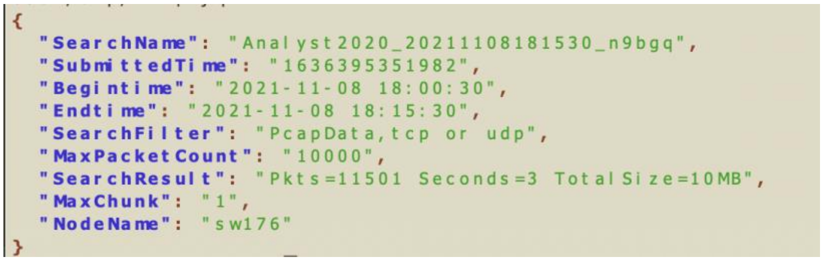
200	searchname refers to a valid search. JSON response from the server indicates if the search is in progress, waiting or has completed, how many chunks are available. valid status strings are: Pending, InProgress, Done, NoSpace, NoData, Cancelled
400	Required parameters missing
401	Invalid rest_token or searchname

Example

Request

```
curl --silent --insecure -X GET https://10.91.170.179:41395/v2/fmsearch/status?rest_token=8da0edd5-a17f-72a3-8479-
\&searchname= Analyst2020_20211108181530_n9bgq\&nodename=nc176
```

Response



```
{
   "SearchName": "Analyst2020_20211108181530_n9bgq",
   "SubmittedTime": "1636395351982",
   "Begintime": "2021-11-08 18:00:30",
   "Endtime": "2021-11-08 18:15:30",
   "SearchFilter": "PcapData,tcp or udp",
   "MaxPacketCount": "10000",
   "SearchResult": "Pkts=11501 Seconds=3 TotalSize=10MB",
   "MaxChunk": "1",
   "NodeName": "sw176"
}
```

Investigator – Download PcapList

This is a HTTP GET request to the server's /v2/fmsearch/data endpoint to download a list of pcaps zip from a Federation node. Unzip the file to retrieve the object files.

Request

Name	Type	Remarks
rest_token	string	Required**.** REST token from a valid FM login request
searchname	string	Required
type	string	Required – must be equal to *PcapList*
nodename	string	Required

Return Codes and Response

200	All the required parameters have been supplied and valid. The server sends zip file of the requested pcap list.
400	A required parameter is missing or invalid
401	Invalid rest_token

Example

Request

```
curl --insecure -X GET 'https://10.91.170.179:41395/v2/fmsearch/data?rest_token=714821c8-3c54-b8a8-a0b6-
a471267b9a79&searchname=continuum_1630711551_1_REST5&type=PcapList&nodename=nc179' -J -O
```

Response

```
curl: Saved to filename 'continuum_1630711551_1_REST5_nc179_PcapList_1.zip'
```

Investigator – Download pcap

This is a HTTP GET request to the server's /v2/fmsearch/data endpoint to download a search pcap zip from a Federation node. Unzip the file to retrieve the pcap file.

Request

Name	Type	Remarks
rest_token	alphanumeric string	Required**.** REST token from a valid FM login request
searchname	alphanumeric string	Required
type	integer	Pcap number starting from 1
nodename	string	Required

Return Codes and Response

200	All the required parameters have been supplied and valid. The server sends zip file of the requested pcap.
400	A required parameter is missing or one or more parameters such as search_filter is invalid; the server sends error information as part of the response.
401	Invalid rest_token

Example

Request

```
curl --insecure -X GET 'https://10.1.55.179:41395/v2/fmsearch/data?rest_token=e29ec17b-62fc-73e7-fd1d-
c289b0670296&searchname=continuum_1625803772_1_rest1&type=1&nodename=sw152' -J -O
```

Response

```
curl: Saved to filename 'continuum_1625803772_1_rest1_sw152_1_1.zip'
```

Investigator – Download LogData

This is a HTTP GET request to the server's /v2/fmsearch/data endpoint to download a search logdata zip from a Federation node. Unzip the file to retrieve the metadata files.

Request

Name	Type	Remarks
rest_token	string	Required**.** REST token from a valid FM login request
searchname	string	Required
type	string	Required – must be equal to *LogData*
nodename	string	Required

Return Codes and Response

200	All the required parameters have been supplied and valid. The server sends zip file of the requested metadata.
400	A required parameter is missing or invalid
401	Invalid rest_token

Example

Request

```
curl --insecure -X GET 'https://10.91.170.179:41395/v2/fmsearch/data?rest_token=714821c8-3c54-b8a8-a0b6-
a471267b9a79&searchname=continuum_1630711551_1_REST5&type=LogData&nodename=nc179' -J -O
```

Response

```
curl: Saved to filename 'continuum_1630711551_1_REST5_nc179_LogData_1.zip'
```

Investigator – Download ObjectList

This is a HTTP GET request to the server's /v2/fmsearch/data endpoint to download a search object list zip from a Federation node. Unzip the file to retrieve the object files.

Request

Name	Type	Remarks
rest_token	string	Required**.** REST token from a valid FM login request
searchname	string	Required
type	string	Required – must be equal to *ObjectList*
nodename	string	Required

Return Codes and Response

200	All the required parameters have been supplied and valid. The server sends zip file of the requested metadata.
400	A required parameter is missing or invalid
401	Invalid rest_token

Example

Request

```
curl --insecure -X GET 'https://10.91.170.179:41395/v2/fmsearch/data?rest_token=714821c8-3c54-b8a8-a0b6-
a471267b9a79&searchname=continuum_1630711551_1_REST5&type=ObjectList&nodename=nc179' -J -O
```

Response

```
curl: Saved to filename 'continuum_1630711551_1_REST5_nc179_ObjectList_1.zip'
```

Investigator – Download Object Data

This is a HTTP GET request to the server's /v2/fmsearch/data endpoint to download a search object data zip from a Federation node. Unzip the file to retrieve the object files.

Request

Name	**Type**	**Remarks**
rest_token	string	Required**.** REST token from a valid FM login request
searchname	string	Required
type	string	Required – must be equal to *SearchObjects*
nodename	string	Required

Return Codes and Response

200	All the required parameters have been supplied and valid. The server sends zip file of the requested metadata.
400	A required parameter is missing or invalid
401	Invalid rest_token

Example

Request

```
curl --insecure -X GET 'https://10.91.170.179:41395/v2/fmsearch/data?rest_token=714821c8-3c54-b8a8-a0b6-
a471267b9a79&searchname=continuum_1630711551_1_REST5&type=SearchObjects&nodename=nc179' -J -O
```

Response

```
curl: Saved to filename 'continuum_1630711551_1_REST5_nc179_SearchObjects_1.zip'
```

Investigator – Delete Search

This is a HTTP DELETE request to the server’s /v2/fmsearch endpoint to delete all data associated with a completed/stopped search.

Request

Name	Type	Remarks
rest_token	string	Required
searchname	string	Required

Return Codes and Response

200	rest_token is valid; searchname refers to a valid search that has been completed/stopped
202	searchname refers to a search in progress.
400	rest_token and/or searchname parameter is missing
401	rest_token and/or searchname are invalid

Example

Request

```
curl --silent --insecure -X DELETE 'https://10.91.170.179:41395/v2/fmsearch?rest_token=714821c8-3c54-b8a8-a0b6-
a471267b9a79&searchname=continuum_1630711551_1_REST5'
```

Response

```
{
  "message": "deleted search continuum_1630711551_1_REST5"
}
```

Investigator – Create a FM Log Search

This is a HTTP POST request to the server’s /v2/fmsearch endpoint to start a new search on each Federation node with a special search filter “logsearch”

Request

Name	Type	Remarks
rest_token	string	Required**.** REST token from a valid login request
search_name	string	Required
search_filter	string	Must be specified as **logsearch**
begin_time	string	Required – UTC time - YYYY-MM-DD hh:mm:ss eg., 2015-04-10 15:55:01
end_time	string	Required – UTC time - YYYY-MM-DD hh:mm:ss eg., 2015-04-10 15:57:01
max_bytes	non-negative integer	Optional - Default: 0 => get all metadata example: 10000 – search stops when 10000 bytes of logdata is collected. This is only a hint as the search may continue up to a logical stopping point.

Return Codes and Response

200	All the required parameters have been supplied and valid. The server sends a search token
400	A required parameter is missing or one or more parameters such as search_filter is invalid;
401	Invalid rest_token

Example

Request

```
curl --silent --insecure --silent -X POST -H 'Content-Type: application/json' -d
'{"rest_token":"e508b555-7f31-3396-77a4-
07af9e7dd413","search_name":"test1","begin_time":"2021-11-11 10:18:00","end_time":"2021-
11-11 15:10:00","max_packets":"10000","PayloadSearchFilter":"", "LogSearchFilter":"",
"search_filter":"logsearch" }' https://10.1.55.176:41395/v2/fmsearch
```

Response

```
{
  "searchname”: " continuum_1631377579_1_rest2"
}
```

Search Manager - Get Pending Searches

This is a HTTP GET request to /v2/fmsearch /pending endpoint to get the list of N pending searches. This is an idempotent operation.

Request

Name	Type	Remarks
rest_token	string	Required
count	integer	Optional limit the number of pending searches returned to this number. Default : 0 return all pending searches

Return Codes and Response

200	rest_token refers to a valid login. JSON response from the server lists the pending searches (<= 'count')
400	rest_token parameter is missing
401	rest_token does not refer to any valid login tokens

Example

Request

```
curl --silent --insecure -X GET 'https://10.91.170.186:41395/v2/fmsearch/pending?rest_token=16baf3a9-51ed-4aea-87b3-
b74c187b772a&count=2'
```

Response

```
[
  {
    "PayloadSearchFilter": "",
    "CaseName": "fms_2020_11_27_22_04_07_797",
    "SearchName": "fms_2020_11_27_22_04_07_797",
    "Begintime": "2020-11-12 02:49:07",
    "Endtime": "2020-11-28 03:04:07",
    "SearchFilter": "PcapData,host 100.100.100.100",
    "LogSearchFilter": "",
    "SearchStatus": "Pending"
  },
  {
    "PayloadSearchFilter": "",
    "CaseName": "fms_2020_11_27_22_05_20_646",
    "SearchName": "fms_2020_11_27_22_05_20_646",
    "Begintime": "2020-11-12 02:50:20",
    "Endtime": "2020-11-28 03:05:20",
    "SearchFilter": "PcapData,host 100.100.100.100",
    "LogSearchFilter": "",
    "SearchStatus": "Pending"
  }
```

Search Manager - Get Completed Searches

This is a HTTP GET request to /v2/fmsearch /completed endpoint to get the list of N completed searches. This is an idempotent operation.

Request

Name	Type	Remarks
rest_token	string	Required
count	integer	Optional - limit the number of pending searches returned to this number. Default : 0 return all pending searches

Return Codes and Response

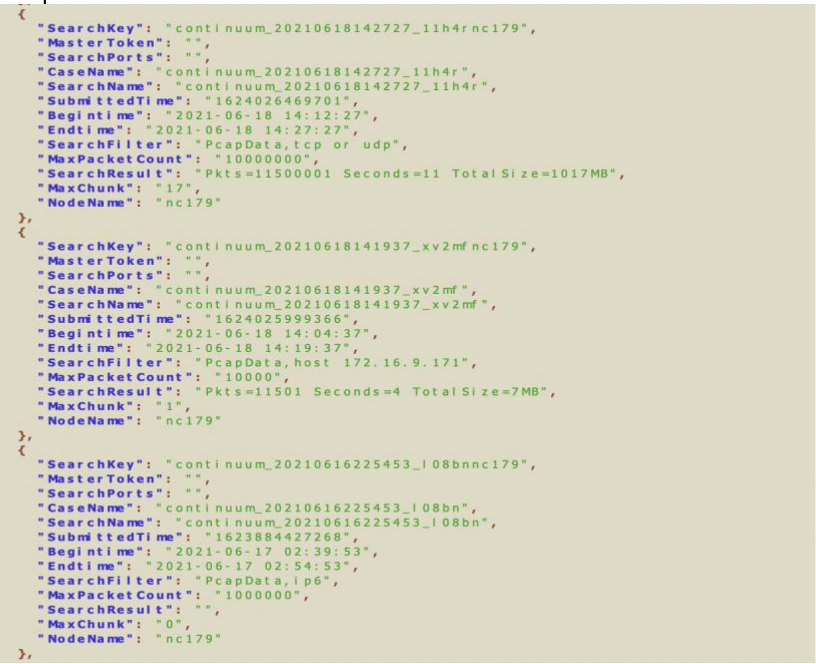
200	rest_token refers to a valid login. JSON response from the server lists the pending searches (<= 'count')
400	rest_token parameter is missing
401	rest_token does not refer to any valid login tokens

Example

Request

```
curl --silent --insecure -X GET 'https://10.91.170.186:41395/v2/fmsearch/completed?rest_token=16baf3a9-51ed-4aea-87b3-b74c187b772a&count=3'
```

Response



```
{
   "SearchKey": "continuum_20210618142727_11h4rnc179",
   "MasterToken": "",
   "SearchPorts": "",
   "CaseName": "continuum_20210618142727_11h4r",
   "SearchName": "continuum_20210618142727_11h4r",
   "SubmittedTime": "1624026469701",
   "Begintime": "2021-06-18 14:12:27",
   "Endtime": "2021-06-18 14:27:27",
   "SearchFilter": "PcapData,tcp or udp",
   "MaxPacketCount": "10000000",
   "SearchResult": "Pkts=11500001 Seconds=11 TotalSize=1017MB",
   "MaxChunk": "17",
   "NodeName": "nc179"
},
{
   "SearchKey": "continuum_20210618141937_xv2mfnc179",
   "MasterToken": "",
   "SearchPorts": "",
   "CaseName": "continuum_20210618141937_xv2mf",
   "SearchName": "continuum_20210618141937_xv2mf",
   "SubmittedTime": "1624025999366",
   "Begintime": "2021-06-18 14:04:37",
   "Endtime": "2021-06-18 14:19:37",
   "SearchFilter": "PcapData,host 172.16.9.171",
   "MaxPacketCount": "10000",
   "SearchResult": "Pkts=11501 Seconds=4 TotalSize=7MB",
   "MaxChunk": "1",
   "NodeName": "nc179"
},
{
   "SearchKey": "continuum_20210616225453_l08bnnc179",
   "MasterToken": "",
   "SearchPorts": "",
   "CaseName": "continuum_20210616225453_l08bn",
   "SearchName": "continuum_20210616225453_l08bn",
   "SubmittedTime": "1623884427268",
   "Begintime": "2021-06-17 02:39:53",
   "Endtime": "2021-06-17 02:54:53",
   "SearchFilter": "PcapData,ip6",
   "MaxPacketCount": "1000000",
   "SearchResult": "",
   "MaxChunk": "0",
   "NodeName": "nc179"
},
```

Configuration – Get Group List

This is a HTTP GET request to the server’s /v2/fmgroup endpoint to get a list of FM groups.

Request

Name	Type	Remarks
rest_token	string	Required

Return Codes and Response

200	rest_token is valid
400	rest_token is missing
401	rest_token is invalid

Example

Request

```
curl --silent --insecure -X GET 'https://10.91.170.186:41395/v2/fmgroup?rest_token=b83fe574-471f-4908-8ff0-
38c62aab8e5a'
```

Response

```
[
  {
    "groupname": "qa-group",
    "groupcount": 1,
    "aggregate_throughput": 0,
    "userslist": "analyst123,Analyst2020"
  },
  {
    "groupname": "qa2-group",
    "groupcount": 1,
    "aggregate_throughput": 0,
    "userslist": "Analyst2020"
  }
]
```

Configuration - Delete Federation Node

This is a HTTP DELETE request to the server’s /v2/fmnode endpoint to delete a federation node (FN).

Request

Name	Type	Remarks
rest_token	string	Required
nodeaddr	string	Required. IP address of a federated node that has been added.

Return Codes and Response

200	rest_token and nodeaddr are valid.
400	rest_token and/or nodeaddr missing
401	Invalid rest_token
404	nodeaddr does not exist in the list of added Federation nodes

Example

Request

```
curl --insecure -X DELETE 'https://10.91.170.179:41395/v2/fmnode?rest_token=714821c8-3c54-b8a8-a0b6-a471267b9a79&nodeaddr=10.91.170.161'
```

Response

```
{
  “message": "deleted node 10.91.170.161"
}
```

Configuration – Delete Federation Group

This is a HTTP DELETE request to the server’s /v2/fmgroup endpoint to delete a FM group. A group must be empty before it can be deleted.

Request

Name	Type	Remarks
rest_token	string	Required
group_name	string	Required

Return Codes and Response

200	Required parameters have been specified; all parameters are valid. Group is empty.
400	rest_token and/or group_name missing
401	rest_token is invalid
403	Group is not empty. If the group is not empty, the nodes within the group must be removed before deleting this group.

Example

Request

```
curl --silent --insecure -X DELETE 'https://10.91.170.186:41395/v2/fmgroup?rest_token=b83fe574-471f-4908-8ff0-38c62aab8e5a&group_name=Cambridge'
```

Response

```
{
  "message": "deleted group Cambridge"
}
```

Configuration – Set Precapture Filter

This is a HTTP POST request to the server's /v2/precapturefilters endpoint to create a new pre-capture filter. The pre-capture filter is applied on all received packets.

Request

Name	Type	Remarks
rest_token	string	Required
search_filter	string	Required Valid BPF filter eg., dst port 80

Return Codes and Response

200	Required parameters have been specified; all parameters are valid.
400	A required parameter is missing or one or more parameters such as search_filter is invalid; the server sends error information as part of the response.
401	rest_token is invalid

Example

Request

```
curl --insecure -X POST -H 'Content-Type: application/json' -d '{"rest_token":"0e06a00c-71de-492a-9bc5-
57d25005f784","search_filter":"tcp"}' https://10.91.170.186:41395/v2/precapturefilters
```

Response

```
{
  "message": "pre-capture filter set."
}
```

Configuration– Get Precapture Filter

This is a HTTP GET request to the server's /v2/precapturefilters endpoint to get one or all pre-capture filter(s).

Request

Name	Type	Remarks
rest_token	string	Required

Return Codes and Response

200	rest_token is valid
400	rest_token is missing
401	rest_token is invalid

Example

Request

```
curl --silent --insecure -X GET 'https://10.91.170.186:41392/v2/precapturefilters?rest_token=0e06a00c-71de-492a-9bc5-57d25005f784'
```

Response

```
[
  {
    "filtername": "Precapturefilter”,
    "searchfilter": "tcp",
    "createdtime": "2020-11-28T12:36:32.301Z"
  }
]
```

Configuration – Reset Precapture Filter

This is a HTTP DELETE request to the server’s /v2/precapturefilters endpoint to delete a pre-capture filter.

Request

Name	Type	Remarks
rest_token	string	Required

Return Codes and Response

200	rest_token is valid
400	rest_token is missing
401	rest_token is invalid

Example

Request

```
curl --silent --insecure -X DELETE 'https://10.91.170.186:41395/v2/precapturefilters?rest_token=0e06a00c-71de-492a-9bc5-57d25005f784'
```

Response

```
{
  "message": "pre-capture filter reset"
}
```

Configuration/Investigator - Create Active Trigger

This is a HTTP POST request to the server’s /v2/activetriggers endpoint to create a new active trigger. Each Federated Node is configured to handle a fixed set of active triggers simultaneously.

Request

Name	Type	Remarks
rest_token	string	Required
trigger_name	alphanumeric string	Required Must not be duplicate of any existing active filters
search_filter	string	Required Valid BPF filter eg., dst port 80
seconds_before	non-negative integer	Required Indicates the duration (in seconds) to go back from the time a trigger occurs.
seconds_after	non-negative integer	Indicates the duration (in seconds) of the search from the time a trigger occurs.

Return Codes and Response

200	Required parameters have been specified; all parameters are valid; Response indicates how many triggers are currently active.
400	A required parameter is missing or one or more parameters such as search_filter is invalid; the server sends error information as part of the response.
401	rest_token does not refer to a valid login request
429	The server cannot add any more active triggers as the predefined limit for active triggers is reached. The server returns the max number of active triggers allowed as part of the error message. {error_message: ‘No more active triggers can be defined: 100’}

Example

Request

```
curl --silent --insecure -X POST -H 'Content-Type: application/json' -d '{"rest_token": "714821c8-3c54-b8a8-a0b6-a471267b9a79",
"trigger_name":"t1", "capture_interfaces":"0", "seconds_before":"30", "seconds_after":"30", "searchfilter":"port 80",
"search_filter":"port 80"}' https://10.91.170.179:41395/v2/activetriggers
```

Response

```
{
  "currTriggerCount": 2,
  "maxTriggerCount": 100
}
```

Configuration - Get Active Trigger List

This is a HTTP GET request to the server's /v2/activetriggers endpoint to get one or all trigger(s) that are currently active.

Request

Name	Type	Remarks
rest_token	string	Required
trigger_name	string	Optional If specified, the response will include information about this trigger only. Default: Get information of all active triggers

Return Codes and Response

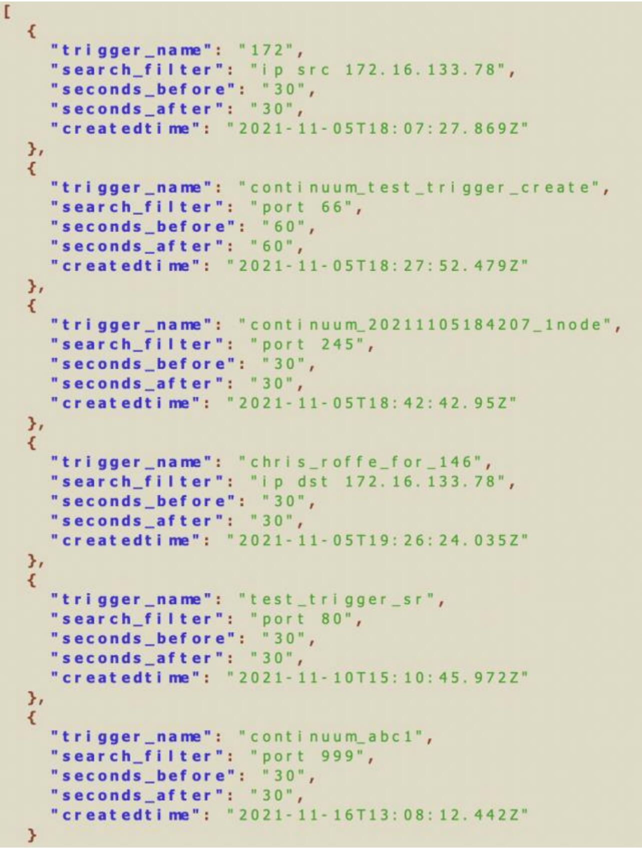
200	required parameters have been specified; all specified parameters are valid Response indicates information of one (if requested) or all(by default) active triggers.
400	a required parameter is missing
401	rest_token does not refer to a valid login request

Example

Request

```
curl --insecure -X GET 'https://10.91.170.179:41395/v2/activetriggers?rest_token=714821c8-3c54-b8a8-a0b6-a471267b9a79'
```

Response



```
[
  {
    "trigger_name": "172",
    "search_filter": "ip src 172.16.133.78",
    "seconds_before": "30",
    "seconds_after": "30",
    "createdtime": "2021-11-05T18:07:27.869Z"
  },
  {
    "trigger_name": "continuum_test_trigger_create",
    "search_filter": "port 66",
    "seconds_before": "60",
    "seconds_after": "60",
    "createdtime": "2021-11-05T18:27:52.479Z"
  },
  {
    "trigger_name": "continuum_20211105184207_1node",
    "search_filter": "port 245",
    "seconds_before": "30",
    "seconds_after": "30",
    "createdtime": "2021-11-05T18:42:42.95Z"
  },
  {
    "trigger_name": "chris_roffe_for_146",
    "search_filter": "ip dst 172.16.133.78",
    "seconds_before": "30",
    "seconds_after": "30",
    "createdtime": "2021-11-05T19:26:24.035Z"
  },
  {
    "trigger_name": "test_trigger_sr",
    "search_filter": "port 80",
    "seconds_before": "30",
    "seconds_after": "30",
    "createdtime": "2021-11-10T15:10:45.972Z"
  },
  {
    "trigger_name": "continuum_abc1",
    "search_filter": "port 999",
    "seconds_before": "30",
    "seconds_after": "30",
    "createdtime": "2021-11-16T13:08:12.442Z"
  }
```

Configuration - Delete Active Trigger

This is a HTTP DELETE request to the server’s /v2/activetriggers endpoint to delete an active trigger.

Request

Name	Type	Remarks
rest_token	string	Required
trigger_name	string	Required This points to an existing active trigger to be deleted

Return Codes and Response

200	Required parameters have been specified
400	rest_token and/or trigger_name is missing. trigger_name is invalid
401	rest_token Is invalid

Example

Request

```
curl --insecure -X DELETE 'https://10.91.170.179:41395/v2/activetriggers?rest_token=714821c8-3c54-b8a8-a0b6-
a471267b9a79&trigger_name=continuum_ac4'
```

Response

```
{
  "message": "deleted active trigger continuum_ac4"
}
```

Configuration – Pause Capture

This is a HTTP PUT request to the server’s /v2/fmcapture endpoint to pause data capture on all federation nodes.

Request

Name	Type	Remarks
rest_token	alphanumeric string	Required.
action	string	Required. Set to ”pause” to pause capture servers.

Return Codes and Response

200	action string and rest_token are valid.
400	rest_token and/or action parameter is missing
401	Invalid rest_token

Example

Request

```
$curl --silent --insecure -X PUT 'https://10.91.170.186:41395/v2/fmcapture?rest_token=b83fe574-471f-4908-8ff0-38c62aab8e5a&action=pause'
```

Response

```
{
  "message": "pause request submitted"
}
```

Configuration – Resume Capture

This is a HTTP PUT request to the server’s /v2/fmcapture endpoint to resume data capture on all federation nodes.

Request

Name	Type	Remarks
rest_token	alphanumeric string	Required.
action	string	Required. Set to ”resume” to resume capture servers.

Return Codes and Response

200	action string and rest_token are valid.
400	rest_token and/or action parameter is missing
401	Invalid rest_token

Example

Request

```
$curl --silent --insecure -X PUT 'https://10.91.170.186:41395/v2/fmcapture?rest_token=b83fe574-471f-4908-8ff0-
38c62aab8e5a&action=resume'
```

Response

```
{
  "message": "resume request submitted"
}
```

AAA - Auditing - Configure Alert/Event Log Receiver

This is a HTTP POST request to the server's /v2/logreceiver endpoint to add configure an auditlog receiver. Each receiver can receive one or more of the event types.

Request

Name	Type	Remarks
rest_token	string	Required
ipaddress	ip address	Required
port	integer	Required
preferences	string	Optional. Comma separated list of one or more types of logs to be forwarded: *Alerts,ActiveTriggerEvents,Files,DNS,Netflows,HTTP, EMail,TLS* If not supplied, metadata of all event types will be sent to the supplied log receiver server.

Return Codes and Response

200	Required parameters have been specified; all parameters are valid.
400	A required parameter is missing or one or more parameters such as serveraddr invalid; the server sends error information as part of the response.
401	rest_token does not refer to a valid login request or unable to connect to the audit server

Example

Request

```
curl --insecure -X POST -H 'Content-Type: application/json' -d '{"rest_token": "714821c8-3c54-b8a8-a0b6-
a471267b9a79", "ipaddress":"10.2.3.4","port":"3414",”preferences”:”Aleerts,TLS” }'
```

Response

```
{
  "message": "saved auditlog receiver"
}
```

AAA - Auditing - Reset Alert/Event Log Receiver

This is a HTTP DELETE request to the server's /v2/logreceiver endpoint to reset audit server configuration.

Request

Name	Type	Remarks
rest_token	string	Required
ipaddress	string	Required
port	Integer	Required

Return Codes and Response

200	valid rest_token, ipaddress and port
400	required parameters missing
401	Invalid rest_token

Example

Request

```
curl --insecure -X DELETE 'https://10.91.170.179:41395/v2/logreceiver?rest_token=714821c8-3c54-b8a8-a0b6-
a471267b9a79&ipaddress=10.91.170.152&port=23322'
```

Response

```
{
  "message": "deleted audit log receiver",
```

AAA - Auditing - Get Alert/Event Log Receiver configuration

This is a HTTP GET request to the server’s /v2/logreceiver endpoint to get audit server configuration.

Request

Name	Type	Remarks
rest_token	string	Required

Return Codes and Response

200	Valid rest_token
400	rest_token missing
401	Invalid rest_token

Example
Request

```
curl --insecure -X GET 'https://10.91.170.179:41395/v2/logreceiver?rest_token=714821c8-3c54-b8a8-a0b6-
a471267b9a79'
```

Response

```
{
  "ipaddress": "10.91.170.12",
  "port": "1234",
  "preferences": "Alerts"
},
{
  "ipaddress": "10.91.170.123",
  "port": "12345",
  "preferences": "TLS,Netflows"
}
```

AAA - Auditing - Set Alert/Event Log Forwarder Options

This is a HTTP POST request to the server’s /v2/logforwarder endpoint to set auditing preferences.

Request

Name	Type	Remarks
rest_token	string	Required
options	string	Comma separated list of types of logs to be forwarded: Alerts,ActiveTriggerEvents,Files,DNS,Netflows,HTTP,EMail,TLS

Return Codes and Response

200	Required parameters have been specified; all parameters are valid;
400	A required parameter is missing, or one or more parameters is invalid; the server sends error information as part of the response.
401	rest_token does not refer to a valid login request

Example

Request

```
curl --insecure -X POST -H 'Content-Type: application/json' -d '{"rest_token": "714821c8-3c54-b8a8-a0b6-
a471267b9a79", "options":"Alerts,ActiveTriggerEvents" }' https://10.91.170.179:41395/v2/logforwarder
```

Response

```
{
  "message": "log forwarder options set"
}
```

AAA - Auditing - Reset Alert/Event Log Forwarding Options

This is a HTTP DELETE request to the server’s /v2/logforwarder endpoint to reset log forwarder options.

Request

Name	Type	Remarks
rest_token	string	Required

Return Codes and Response

200	Valid rest_token
400	Rest_token missing
401	Invalid rest_token

Example
Request

```
curl --insecure -X DELETE 'https://10.91.170.179:41395/v2/logforwarder?rest_token=714821c8-3c54-b8a8-a0b6-
a471267b9a79'
```

Response

```
{
  "message": "log forwarder options reset"
}
```

AAA - Auditing - Get Alert/Event Log Forwarder configuration

This is a HTTP GET request to the server’s /v2/logforwarder endpoint to get audit server configuration.

Request

Name	Type	Remarks
rest_token	string	Required

Return Codes and Response

200	Valid rest_token
400	rest_token missing
401	Invalid rest_token

Example

Request

```
curl --silent --insecure -X GET 'https://10.91.170.186:41392/v2/logforwarder?rest_token=b83fe574-471f-4908-8ff0-38c62aab8e5a'
```

Response

```
{
  "ActiveTriggerEvents": true,
  "CriticalEvents": true,
  "Alerts": true,
  "DNS": false,
  "Netflows": false,
  "HTTP": false,
  "TLS": false,
  "Files": false,
  "VOIP": false,
  "EMail": false,
  "UserAgents": false
}
```

AAA - Authentication - Activate LDAP

This is a HTTP POST request to the server’s /v2/ldap endpoint to activate ldap authentication

Request

Name	Type	Remarks
rest_token	string	Required
connection_string	alphanumeric string	Required serverip:portnum
username	alphanumeric string	Required
password	alphanumeric string	Required
commonname	alphanumeric string	Required
domaincomponent1	alphanumeric string	Optional
domaincomponent2	alphanumeric string	Optional

Return Codes and Response

200	Required parameters have been specified; all parameters are valid;
400	A required parameter is missing or one or more parameters such as connection_string is invalid; the server sends error information as part of the response.
401	rest_token is invalid

Example

Request

```
curl --silent --insecure -X POST -H 'Content-Type: application/json' -d '{"rest_token": "b83fe574-471f-4908-8ff0-
38c62aab8e5a","connection_string":"10.1.1.1:389","username":"joeldap","password":"GTp9ZU8HlSiQPsdGlSyW","com
monname":"HighSpeedM","domaincomponent1":"myldap.test","domaincomponent2":"com"}'
https://10.91.170.186:41395/v2/ldap
```

Response

```
{
  "message": "activated LDAP authentication"
}
```

AAA - Authentication - Activate SSO

This is a HTTP POST request to the server’s /v2/sso endpoint to configure sso server

Request

Name	Type	Remarks
rest_token	string	Required
connection_string	alphanumeric string	Required serverip:portnum
username	alphanumeric string	Required
password	alphanumeric string	Required
realm	alphanumeric string	Required
clientid	alphanumeric string	Required

Return Codes and Response

200	Required parameters have been specified; all parameters are valid.
400	A required parameter is missing or one or more parameters such as connection_string is invalid; the server sends error information as part of the response.
401	rest_token is invalid

Example

Request

```
curl --silent --insecure -X POST -H 'Content-Type: application/json' -d '{"rest_token": "b83fe574-471f-4908-8ff0-
38c62aab8e5a","connection_string":"10.2.5.1:8080","username":"joeclock","password":"GTp9ZU8HlSiQP","realm":"real
m1","clientid":"clientid2"}' https://10.91.170.186:41395/v2/sso
```

Response

```
{
  "message": "activated SSO authentication”
}
```

AAA - Authentication - Activate RADIUS

This is a HTTP POST request to the server’s /v2/radius endpoint to switch to radius authentication mode.

Request

Name	Type	Remarks
rest_token	string	Required
connection_string	string	Required serverip:portnum
secret	string	Required

Return Codes and Response

200	Required parameters have been specified; all parameters are valid;
400	A required parameter is missing or one or more parameters such as connection_string is invalid; the server sends error information as part of the response.
401	rest_token does not refer to a valid login request

Example

Request

```
curl --silent --insecure -X POST -H 'Content-Type: application/json' -d '{"rest_token": "b83fe574-471f-4908-8ff0-38c62aab8e5a","connection_string":"10.4.4.1:1812","secret":"secret123"}' https://10.91.170.186:41395/v2/radius
```

Response

```
{
  "message": "activated RADIUS authentication"
}
```

AAA - Authentication - Activate Local Authentication

This is a HTTP POST request to the server's /v2/localauth endpoint to switch to local authentication, irrespective of the server's current authentication mode.

Request

Name	Type	Remarks
rest_token	string	Required

Return Codes and Response

200	Valid rest_token
400	Rest_token is missing
401	Invalid rest_token

Example

Request

```
curl --silent --insecure -X POST -H 'Content-Type: application/json' -d '{"rest_token": "b83fe574-471f-4908-8ff0-
38c62aab8e5a"}' https://10.91.170.186:41395/v2/localauth
```

Response

```
{
  "message": " activated local authentication"
}
```

AAA - Authorization - Add Role

This is a HTTP POST request to the server’s /v2/authorization endpoint to add a role.

Request

Name	Type	Remarks
rest_token	string	Required
rolename	string	Required
permissions	string	Required Comma separated list of permissions: Groups,Licensing,Authentication,Authorization,Auditing,Search,Policy

Return Codes and Response

200	Required parameters have been specified; all parameters are valid;
400	A required parameter is missing or one or more parameters such as rolename is invalid; the server sends error information as part of the response.
401	rest_token does not refer to a valid login request

Example

Request

```
curl --silent --insecure -X POST -H 'Content-Type: application/json' -d '{"rest_token": "b83fe574-471f-4908-8ff0-38c62aab8e5a", "rolename": "auditor", "permissions":"Licensing,Auditing"}' https://10.91.170.186:41395/v2/authorization
```

Response

```
{
  "message": "added role auditor"
}
```

AAA - Authorization - Delete Role

This is a HTTP DELETE request to the server’s /v2/authorization endpoint to delete role.

Request

Name	Type	Remarks
rest_token	string	Required
rolename	string	Required

Return Codes and Response

200	Required parameters have been specified; all parameters are valid.
400	A required parameter is missing or one or more parameters such as rolename is invalid; the server sends error information as part of the response.
401	rest_token does not refer to a valid login request
404	Specified rolename is not found.

Example

Request

```
curl --silent --insecure -X DELETE 'https://10.91.170.186:41395/v2/authorization?rest_token=16baf3a9-51ed-4aea-87b3-b74c187b772a&rolename=new2'
```

Response

```
{
  "message": "deleted role new2"
}
```

AAA - Authorization - Get Roles List

This is a HTTP GET request to the server’s /v2/authorization endpoint get list of roles.

Request

Name	Type	Remarks
rest_token	string	Required.

Return Codes and Response

200	Valid rest_token
400	rest_token is missing
401	Invalid rest_token

Example

Request

```
curl --silent --insecure -X GET 'https://10.91.170.186:41395/v2/authorization?rest_token=b83fe574-471f-4908-8ff0-38c62aab8e5a'
```

Response

```
[{
   "rolename": "Supervisor",
   "Groups": true,
   "Licensing": true,
   "Authentication": true,
   "Authorization": true,
   "Auditing": true,
   "Search": true,
   "Policy": true
 }, {
   "rolename": "Analyst",
   "Groups": false,
   "Licensing": false,
   "Authentication": false,
   "Authorization": false,
   "Auditing": false,
   "Search": false,
   "Policy": false
 }, {
   "Groups": true,
   "Licensing": false,
   "rolename": "SeniorAnalyst",
   "Authentication": false,
   "Authorization": false,
   "Auditing": false,
   "Search": false,
   "Policy": false
 }
]
```

IDS Rules - Upload RuleSet

This is a HTTP POST request to /v2/idsruleset endpoint to upload ruleset. If the ruleset already exists, the old file is *replaced*. If the old ruleset is already activated, the new ruleset is *autoactivated*.

Request

Name	Type	Remarks
rest_token	string	Required. Must be valid rest_token
file	string	Full path to the ruleset being uploaded. Basename of the file is used to any operations related to this ruleset.

Return Codes and Response

200	rest_token is valid, and file path is correct.
400	rest_token and/or file is missing
401	Invalid rest_token

Example

Request

```
curl -k -i -X POST -F rest_token=714821c8-3c54-b8a8-a0b6-a471267b9a79 -F fileUploadName=@./rules411.rules
https://10.91.170.179:41395/v2/idsruleset
```

Response

```
{
  "message": "uploaded ruleset rules411.rules",
}
```

IDS Rules - Delete RuleSet

This is a HTTP DELETE request to /v2/idsruleset endpoint to delete a rule set.

Request

Name	Type	Remarks
rest_token	string	Required
rulesetname	string	Required. Name of the ruleset to be removed.

Return Codes and Response

200	rest_token, rulesetname are valid
400	rest_token and/or rulesetname missing
401	Invalid rest_token
404	rulesetname does not exist

Example

Request

```
curl --insecure -X DELETE 'https://10.91.170.179:41395/v2/idsruleset?rest_token=714821c8-3c54-b8a8-a0b6-a471267b9a79&rulesetname=rules411.rules'
```

Response

```
{
  "message": "deleted ruleset rules411.rules"
}
```

IDS Rules – Activate/Deactivate RuleSet

This is a HTTP PUT request to /v2/idsruleset endpoint to activate/deactivate a rule set.

Request

Name	Type	Remarks
rest_token	string	Required.
rulesetname	string	Required. Name of the ruleset to be removed.
action	string	Required. Set to ***activate*** to activate the ruleset, ***deactivate*** to deactivate a ruleset.

Return Codes and Response

200	rest_token is valid, rulesetname is valid
400	rest_token is missing and/or rulesetname is missing
401	Invalid rest_token
403	action is *activate* and the ruleset is already activated action is *deactivate* and the ruleset is already deactivated
404	ruleset does not exist

Examples

Request

```
curl --insecure -X PUT 'https://10.91.170.179:41395/v2/idsruleset?rest_token=714821c8-3c54-b8a8-a0b6-a471267b9a79&rulesetname=rules411.rules&action=activate'
```

Response

```
{
  "message": "activated ruleset rules411.rules"
}
```

Request

```
curl --insecure -X PUT 'https://10.91.170.179:41395/v2/idsruleset?rest_token=714821c8-3c54-b8a8-a0b6-a471267b9a79&rulesetname=rules411.rules&action=deactivate'
```

Response

```
{
  "message": "deactivated ruleset rules411.rules"
}
```

IDS Rules – Get RuleSet List

This is a HTTP GET request to /v2/idsruleset endpoint to get a list of activated or deactivated rulesets

Request

Name	Type	Remarks
rest_token	string	Required.
type	string	Required. Set to ***activated*** to get activated ruleset, ***deactivated*** to get deactivated ruleset.

Return Codes and Response

200	rest_token is valid; type is set to ***activated*** or ***deactivated***
400	rest_token is missing type is missing or invalid
401	Invalid rest_token

Examples

Request

```
curl --insecure -X GET 'https://10.91.170.179:41395/v2/idsruleset?rest_token=714821c8-3c54-b8a8-a0b6-
a471267b9a79&type=activated'
```

Response

```
[
  {
    "name": "UserRules1.rules",
    "count": 3,
    "error": "false"
  },
  {
    "name": "Now.rules",
    "count": 5,
    "error": "true"
  },
  {
    "name": "emerging-web_specific_apps.rules",
    "count": 4723,
    "error": "false"
  },
  {
```

IDS Rules – Download RuleSet

This is a HTTP GET request to /v2/ idsrulesetcontent endpoint to download a ruleset

Request

Name	Type	Remarks
rest_token	string	Required.
rulesetname	string	Required. Name of the ruleset to be downloaded.

Return Codes and Response

200	rest_token is valid, rulesetname is valid
400	rest_token or guest_token is missing rulesetname is missing
401	Invalid rest_token
404	rulesetname does not exist

Examples

Request

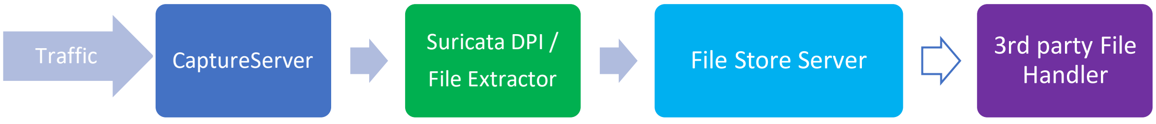
```
curl --insecure -X GET 'https://10.91.170.179:41395/v2/idsrulesetcontent?rest_token=714821c8-3c54-b8a8-a0b6-
a471267b9a79&rulesetname=rules411.rules'
```

Response

```
alert ip [10.91.170.1] any -> any any (msg:"[10.91.170.1 is Criticalfor160]"; sid:9999; )
alert ip [172.16.9.171] any -> any any (msg:"[172.16.9.171 is Critical160139179]"; sid:8888; )
alert ip [192.168.1.1] any -> any any (msg:"[192.168.1.1 is Critical179]"; sid:7777; )
alert ip [84.53.136.152] any -> any any (msg:"[84.53.136.152 is Critical179]"; sid:6666; )
alert ip [62.26.220.5] any -> any any (msg:"[62.26.220.5 is Critical139]"; sid:5555; )
```

File Carving – Set Configuration of File Store Server

This is a HTTP POST request to /v2/filecarving/configuration end point to save the attribute values to store/forward extracted files to an external server.



Request

Name	Type	Remarks
rest_token	string	Required**.** REST token from a valid fm admin login request
connectioninfo	string	url for the external file carving server eg., http://10.12.22.21
credentials	string	optional; username: password to login to the external server
filetransferfrequency	numeric	Optional; in minutes; how often a File Store Server sends a POST request to the configured 3rd party server.
cacheretentionduration	numeric	Optional; how long a 3rd party server can be down; If a 3rd party server is down longer than this duration, server generates a severity 1 system alert and deletes the zip files older than this duration. Default: 60 minutes, minimum:30 minutes, maximum:120 minutes
maxfilestoresize	numeric	Optional; GB; default: 50, settable to 2% of the storage space or 250 GB whichever is lower

Return Codes

200	All the required parameters have been supplied and valid.
400	A required parameter is missing or one or more parameters such as vlan is invalid;
401	Invalid rest_token

Request

```
curl  --insecure --silent -X POST -H 'Content-Type: application/json' -d '{"rest_token":"4c8b8917-8926-37bd-46a9-73a153273c58”,”filetransferfrequency”: 10, “cacheretentionduration”:1440}' https://10.91.170.179:41395/v2/filecarving/configuration
```

File Carving – Get Configuration of File Store Server

This is a HTTP GET call to the end point /v2/filecarving/configuration retrieves the current attribute values.

Request

Name	Type	Remarks
rest_token	string	Required**.** REST token from a valid fm admin login request

Return Codes and Response

200	Valid rest_token
400	rest_token is missing
401	Invalid rest_token

Request

```
curl  --insecure --silent -X GET https://10.91.170.179:41395/v2/filecarving/configuration?rest_token=4c8b8917-8926-37bd-46a9-73a153273c58
```

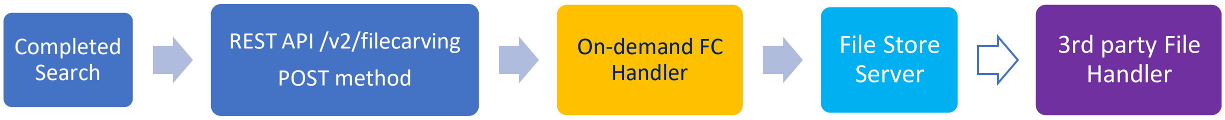
Response

```
{
"ipaddress": "100.2.0.0/16",
 "connectioninfo": "10.91.170,112:2032",
 "cacheretentionduration": "20",
 "maxfilestoresize": "50",

}
```

File Carving - On-demand

On-demand File Carving POST request to /v2/filecarving/ondemand allows users to forward objects of a completed search. On-demand FC workflow may be throttled to ensure that the capture, indexing, or search performance is not impacted.



Request

Name	Type	Remarks
rest_token	string	Required**.** REST token from a valid fm admin login request
searchname	string	Required. Forward any objects generated by this search.

Return Codes and Response

200	All the required parameters have been supplied and valid.
400	A required parameter is missing or one or more parameters such as vlan is invalid;
401	Invalid rest_token

Request

```
curl  --insecure --silent -X POST -H 'Content-Type: application/json' -d '{"rest_token":"4c8b8917-8926-
37bd-46a9-73a153273c58",” searchname”: “continuum_abcde22433” }'
https://10.91.170.172:41395/v2/filecarving/ondemand
```

Configuration – Export Policy

This is a HTTP POST request to the server's /v2/exportpolicy endpoint to save FM policy info such as list of users, groups, nodes. This can be forwarded to federated nodes so that any such node is ready to be designated HA node.

Request

Name	Type	Remarks
rest_token	string	Required

Return Codes and Response

200	Required parameters have been specified; all parameters are valid.
401	rest_token is invalid

Example

Request

```
curl --insecure -X POST -H 'Content-Type: application/json' -d '{"rest_token":"0e06a00c-71de-492a-9bc5-57d25005f784"}'
https://10.91.170.186:41395/v2/exportpolicy
```

Response

```
{
  "message": "FM policy exported"
}
```

Configuration – Get Exported Policy List

This is a HTTP GET request to the server's /v2/exportpolicy endpoint to get a list of currently available policy zip files. This list can be used to select a file to be removed or forwarded to federation nodes.

Request

Name	Type	Remarks
rest_token	string	Required

Return Codes and Response

200	Required parameters have been specified; all parameters are valid.
401	rest_token is invalid

Example

Request

```
curl --insecure -X GET 'https://10.91.170.176:41395/v2/exportpolicy?rest_token=958d7c49-5872-081f-a164-bcad4e534c96'
```

Response

```
{
  "message": "[exportpolicy.1646792643.zip exportpolicy.1646797181.zip]}"
}
```

Configuration – Delete Exported Policy

This is a HTTP DELETE request to the server’s /v2/exportpolicy endpoint to remove a zip file of a previous POST call. This allows clean-up of exported policy zip files so only the relevant zip files are in the store.

Request

Name	Type	Remarks
rest_token	string	Required
zipfilename	string	Required

Return Codes and Response

200	Required parameters have been specified; all parameters are valid.
400	zipfilename points to a file that does not exist
401	rest_token is invalid

Example

Request

```
curl --insecure -X DELETE 'https://10.91.170.176:41395/v2/exportpolicy?rest_token=958d7c49-5872-081f-a164-
bcad4e534c96&zipfilename=exportpolicy.1646792643.zip'
```

Response

```
{
  "message": "Deleted exportpolicy.1646792643.zip"
}
```

Configuration – Forward Exported Policy

This is a HTTP PUT request to the server's /v2/exportpolicy endpoint to forward a zip file of a previous POST call to Federated nodes.

Request

Name	Type	Remarks
rest_token	string	Required
zipfilename	string	Required

Return Codes and Response

200	Required parameters have been specified; all parameters are valid.
400	zipfilename points to a file that does not exist
401	rest_token is invalid

Example

Request

```
curl --insecure -X PUT 'https://10.91.170.176:41395/v2/exportpolicy?rest_token=958d7c49-5872-081f-a164-
bcad4e534c96&zipfilename=exportpolicy.1646792643.zip'
```

Response

```
{
  "message": "Forwarded exportpolicy.1646792643.zip to all the FNs"
}
```

Federation Manager – Logout

This is a HTTP PUT request to the server's /v2/fmlogin endpoint to logout. The rest_token can no longer be used for future access to the FM.

Request

Name	Type	Remarks
rest_token	string	Required

Return Codes and Response

200	rest_token is valid. Note: This rest_token can no longer be used for future access to the FM
400	rest_token is missing
401	Invalid rest_token

Example

Request

```
curl --silent --insecure -X PUT 'https://10.91.170.186:41395/v2/fmlogin?rest_token=ce6aaf48-5209-42f0-bf0f-
c983b1acf078'
```

Response

```
{
  "message": "logged out"
}
```

Appendix A – BPF Filter

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

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

type

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

dir

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

proto

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

1. Primitive Filters

Allowable primitives are given below for reference:

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

[src|dst] net <network> E.g., dst net 192.168.1.0 src net 192.168.1 dst net 172.16 src net 10 net 192.168.1.0 net 192.168.1.0/24 src net 192.168.1/24	Matches packets to or from source/destination or either, residing in a network. An IPv4 network number can be specified as: - Dotted quad (e.g., 192.168.1.0) - Dotted triple (e.g., 192.168.1) - Dotted pair (e.g., 172.16) - Or single number (e.g., 10)
[src|dst] net <network> mask <netmask> **or** [src|dst] net <network>/<len> E.g., dst net 192.168.1.0 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 (or len <300)	Matches packets less than or equal to length
greater <length> E.g., greater 301 (or len >300)	Matches packets greater than or equal to length

(ether|ip|ip6) proto <protocol> E.g., ether proto 0x888e ip proto 50	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
(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 (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)	Matches MPLS packets, optionally with a label of label • mpls expression may be used more than once, to filter on MPLS hierarchies.

1.2 Protocols

- Various protocols can be combined with primitive BPF filters using modifiers and operators.

  Types of valid Protocols are given below:

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

1.3 Modifiers

Types of valid modifiers/operators:

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

1.4 Examples of some filters using operators and modifiers:

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