### flowsearch

Loads a flow rule consisting of the subnet of the IP network, ports, and protocol conditions defined by a subquery, compares them with input records, and assigns all searched flow identifiers as arrays in the **\_flow** field.

#### Syntax

flowsearch [ SUBQUERY ]

Required Parameter

**[ SUBQUERY ]**

Subquery to define the flow rules, enclosed in a pair of square brackets ([ ]).

#### Description

You can load the flow rule from any location, including a file, table, remote RDBMS, and the like, and the field configuration and type must match to be recognized as a valid rule. The number of flow rules to be applied to a subquery cannot exceed 10,000. From the 10,001st rule, they are ignored.

If the subquery fails, the cause of the error is output in the \_flowsearch\_error field. If you add an exception handling command that checks for the existence of the \_flowsearch\_error field value after the flowsearch command, unintended errors or malfunctions can be prevented.

**Definition of input fields**

|  |  |  |  |
| --- | --- | --- | --- |
| Field | Type | Required | Description |
| src\_ip | IP address | Yes | Source IP address |
| src\_port | Integer | No (null allowed) | Source port number |
| dst\_ip | IP address | Yes | Destination IP address |
| dst\_port | Integer | No (null allowed) | Destination port number |
| protocol | String | No (null allowed) | Protocol |

If the field type in the input record does not match, or if required fields are missing, the command outputs the record as it is without checking the flow rule.

**Definition of flow rule fields**

|  |  |  |  |
| --- | --- | --- | --- |
| Field | Type | Required | Description |
| src\_ip | IP address | Yes | Source IP address |
| src\_cidr | Integer | Yes | Source netmask (0-32) |
| src\_port | Integer | No (null allowed) | Source port number (0-65535) |
| dst\_ip | IP address | Yes | Destination IP address |
| dst\_cidr | Integer | Yes | Destination netmask (0-32) |
| dst\_port | Integer | No (null allowed) | Destination port number (0-65535) |
| protocol | String | No (null allowed) | Protocol (TCP, UDP, ICMP, ...) |
| flow | Arbitrary | Yes | Flow identifier |

Each time a record is provided into the flowsearch command, it compares the 5-tuple value input with the flow rule and assigns the matching flow identifier as a list in the **\_flow** field.

Both the **ip** and **cidr** of the flow rule are required fields, but if the **src\_ip** of the rule is 0.0.0.0 and the **src\_cidr** is 0, it is true for all source IP addresses. So set 0.0.0.0/0 for the rule to allow all values for the source or destination.

For example, for the flow rule below, if the input record is src\_ip=106.75.11.63, src\_port=57776, dst\_ip=106.246.20.67, dst\_port=80, and protocol=TCP, then it matches with the flow 2, so the **\_flow=["flow2"]** field is added to the output record.

**Examples of flow rules**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| src\_ip | src\_cidr | src\_port | dst\_ip | dst\_cidr | dst\_port | protocol | flow |
| 211.36.133.0 | 24 | null | 106.246.20.67 | 32 | 80 | TCP | flow1 |
| 106.75.11.0 | 24 | null | 106.246.20.67 | 32 | null | TCP | flow2 |

#### Usage

json "{}"| eval src\_ip=ip("106.75.11.63"), src\_port=57776| eval dst\_ip=ip("106.246.20.67"), dst\_port=80, protocol="TCP"| # Initiating the flowsearch command that defines the flow search rule| flowsearch [ union [ json "{}" | eval src\_ip=ip("211.36.133.0"), dst\_ip=ip("106.246.20.67"), flow="flow1" ] | union [ json "{}" | eval src\_ip=ip("106.75.11.0"), dst\_ip=ip("106.246.20.67"), flow="flow2" ] | eval src\_cidr=24, dst\_cidr=32]| fields src\_ip, src\_port, dst\_ip, dst\_port, protocol, \_flow