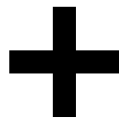


---

# SIEM – Splunk Knowledge Base

By

Aastha Sahni



# Agenda



Splunk Knowledge Objects



Fields & Field Extraction



Tags & Aliases



Lookups & Workflow Action



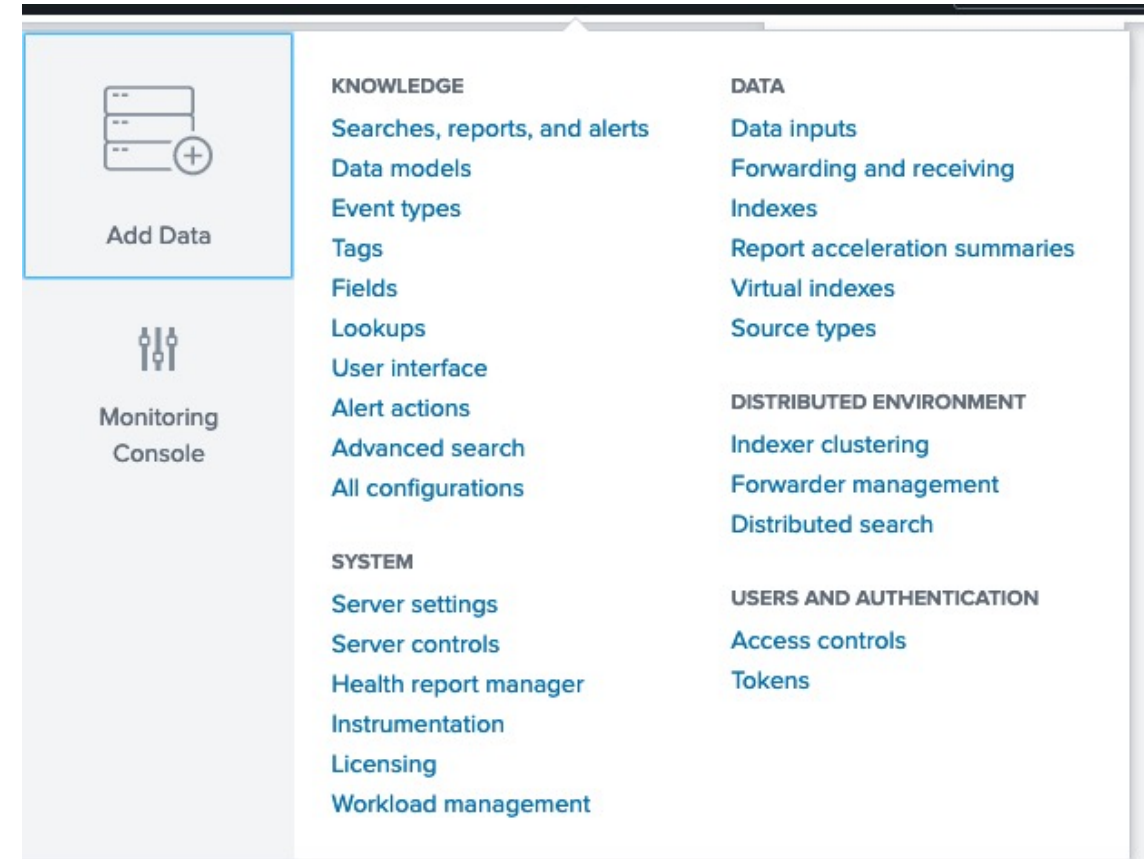
Event Types & Transactions



Data Models

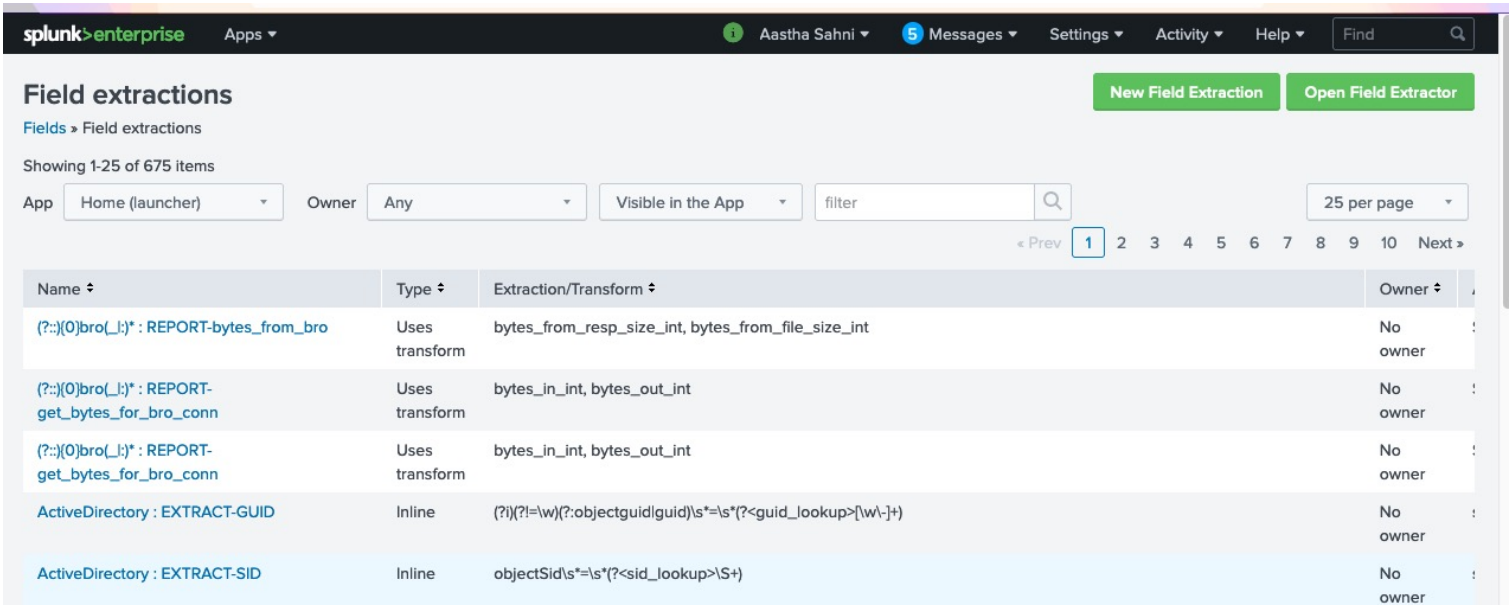
# Splunk Knowledge Objects

- Splunk software extracts different kinds of knowledge from the indexed data which is useful for performing necessary detection and analysis.



# Data Interpretation -Fields & Field Extraction

- Fields are name-value pair which are powerful part of searching in Splunk.



The screenshot shows the 'Field extractions' page in the Splunk Enterprise web interface. The top navigation bar includes the Splunk logo, user 'Aastha Sahni', and various menu items like Messages, Settings, Activity, and Help. Below the navigation bar, the page title 'Field extractions' is displayed along with buttons for 'New Field Extraction' and 'Open Field Extractor'. A filter section shows 'Showing 1-25 of 675 items' with dropdowns for 'App' (Home (launcher)), 'Owner' (Any), and 'Visible in the App'. A search bar and a 'filter' button are also present. The main content area is a table listing field extractions. The table has columns for Name, Type, Extraction/Transform, and Owner. The first three rows show transformations for 'REPORT-bytes\_from\_bro' and 'REPORT-get\_bytes\_for\_bro\_conn'. The last two rows show inline extractions for 'ActiveDirectory : EXTRACT-GUID' and 'ActiveDirectory : EXTRACT-SID'.

Name	Type	Extraction/Transform	Owner
(?::)(0)bro(_):* : REPORT-bytes_from_bro	Uses transform	bytes_from_resp_size_int, bytes_from_file_size_int	No owner
(?::)(0)bro(_):* : REPORT-get_bytes_for_bro_conn	Uses transform	bytes_in_int, bytes_out_int	No owner
(?::)(0)bro(_):* : REPORT-get_bytes_for_bro_conn	Uses transform	bytes_in_int, bytes_out_int	No owner
ActiveDirectory : EXTRACT-GUID	Inline	(?i)(?!=\\w)(?:objectguid\\guid)s*=\\s*(?<guid_lookup>{\\w\\-}+)	No owner
ActiveDirectory : EXTRACT-SID	Inline	objectSid\\s*=\\s*(?<sid_lookup>\\S+)	No owner



# Data Normalization: Tags & Aliases

Field aliases are an alternate name that you assign to a field. You can use that alternate name to search for events that contain that field.

**Tags** enable user to assign names to specific field and value combinations, including event type, host, source, or source type.

**Field aliases** New Field Alias

Fields > Field aliases

Showing 1-25 of 1083 items

App: Home (launcher) Owner: Any Visible in the App: filter 25 per page

« Prev 1 2 3 4 5 6 7 8 9 10 Next »

Name	Field aliases	Owner	App	Sharing	Status	Actions
(?:{0}bro_{:})* : FIELDALIAS-TC	TC AS flag	No owner	Splunk_TA_bro	Global   Permissions	Enabled	Clone
(?:{0}bro_{:})* : FIELDALIAS-body_msg	msg AS body	No owner	Splunk_TA_bro	Global   Permissions	Enabled	Clone
(?:{0}bro_{:})* : FIELDALIAS-content_len	content_len AS message_size	No owner	Splunk_TA_bro	Global   Permissions	Enabled	Clone
(?:{0}bro_{:})* : FIELDALIAS-dest	id_resp_h AS dest	No owner	Splunk_TA_zeek	Global   Permissions	Enabled	Clone
(?:{0}bro_{:})* : FIELDALIAS-dest	id_resp_h AS dest	No owner	Splunk_TA_bro	Global   Permissions	Enabled	Clone
(?:{0}bro_{:})* : FIELDALIAS-dest_ip	id_resp_h AS dest_ip	No owner	Splunk_TA_zeek	Global   Permissions	Enabled	Clone
(?:{0}bro_{:})* : FIELDALIAS-dest_ip	id_resp_h AS dest_ip	No owner	Splunk_TA_bro	Global   Permissions	Enabled	Clone

**Tags**  
Manage tags on field values.

List by field value pair	+ Add new
List by tag name	+ Add new
All unique tag objects	+ Add new



# Data Enrichment: Lookups

Look-ups help in enriching your log data with additional key-value combinations.



## Types of look-ups

CSV	External	KV Store	Geospatial
-----	----------	----------	------------

### Lookups

Create and configure lookups.

[Lookup table files](#)  
List existing lookup tables or upload a new file.

+ Add new

[Lookup definitions](#)  
Edit existing lookup definitions or define a new file-based or external lookup.

+ Add new

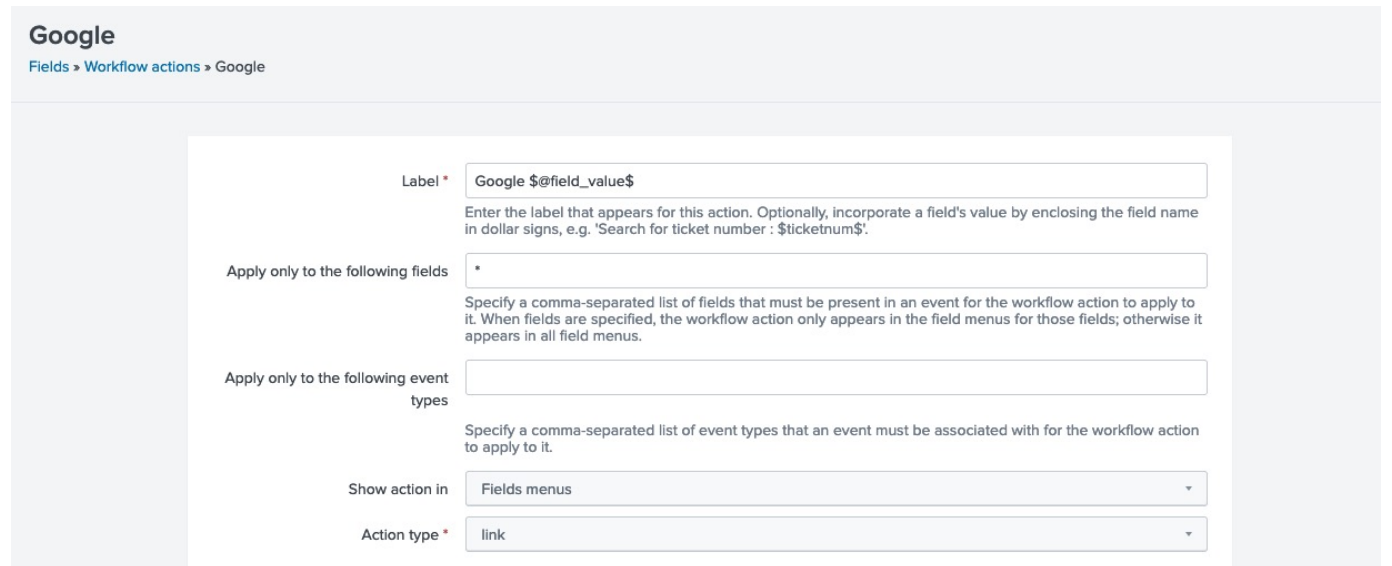
[Automatic lookups](#)  
Edit existing automatic lookups or configure a new lookup to run automatically.

+ Add new



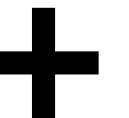
# Data Enrichment: Workflow Actions

- Workflow actions helps in automated interaction of indexed log data with external web sources
- Types of workflow actions:
  - Get Workflow
  - Post Workflow
  - Search Workflow




The screenshot shows the 'Google' workflow action configuration page in the Google Cloud Platform. The breadcrumb trail is 'Fields > Workflow actions > Google'. The configuration form includes the following fields:

- Label \***: A text input field containing 'Google \${field\_value}'. Below it, a note states: 'Enter the label that appears for this action. Optionally, incorporate a field's value by enclosing the field name in dollar signs, e.g. 'Search for ticket number : \$ticketnum\$'.'
- Apply only to the following fields**: A text input field containing '\*'. Below it, a note states: 'Specify a comma-separated list of fields that must be present in an event for the workflow action to apply to it. When fields are specified, the workflow action only appears in the field menus for those fields; otherwise it appears in all field menus.'
- Apply only to the following event types**: A text input field. Below it, a note states: 'Specify a comma-separated list of event types that an event must be associated with for the workflow action to apply to it.'
- Show action in**: A dropdown menu with 'Fields menus' selected.
- Action type \***: A dropdown menu with 'link' selected.



# Data Classification: Event Types

- Event types is a categorization system to help you make some sense of the indexed data.



### Event types

Showing 1-25 of 545 items

App Home (launcher) Owner Any Visible in the App filter 25 per page

« Prev **1** 2 3 4 5 6 7 8 9 10 Next »

Name	Search string	Tag(s)	Owner	App	Sharing	Status
DhcpSrvLog	sourcetype=DhcpSrvLog	dhcp network session windows	No owner	Splunk_TA_windows	Global   <a href="#">Permissions</a>	Enabled
DhcpSrvLog_end	sourcetype=DhcpSrvLog (msdhcp_id=12 OR msdhcp_id=16 OR msdhcp_id=17)	end	No owner	Splunk_TA_windows	Global   <a href="#">Permissions</a>	Enabled
DhcpSrvLog_start	sourcetype=DhcpSrvLog (msdhcp_id=10 OR msdhcp_id=11 OR msdhcp_id=13)	start	No owner	Splunk_TA_windows	Global   <a href="#">Permissions</a>	Enabled
Failed_SU	(NOT sourcetype=stash) ("failed SU to another user" AND "Agent platform:" AND "linux-x86") OR ("failed SU to another user" AND "authentication failure" AND "for su service") OR ("failed SU to another user" AND logname=) OR (exe="/bin/su"	authentication	No owner	Splunk_TA_nix	Global   <a href="#">Permissions</a>	Enabled



# Data Classification: Transactions

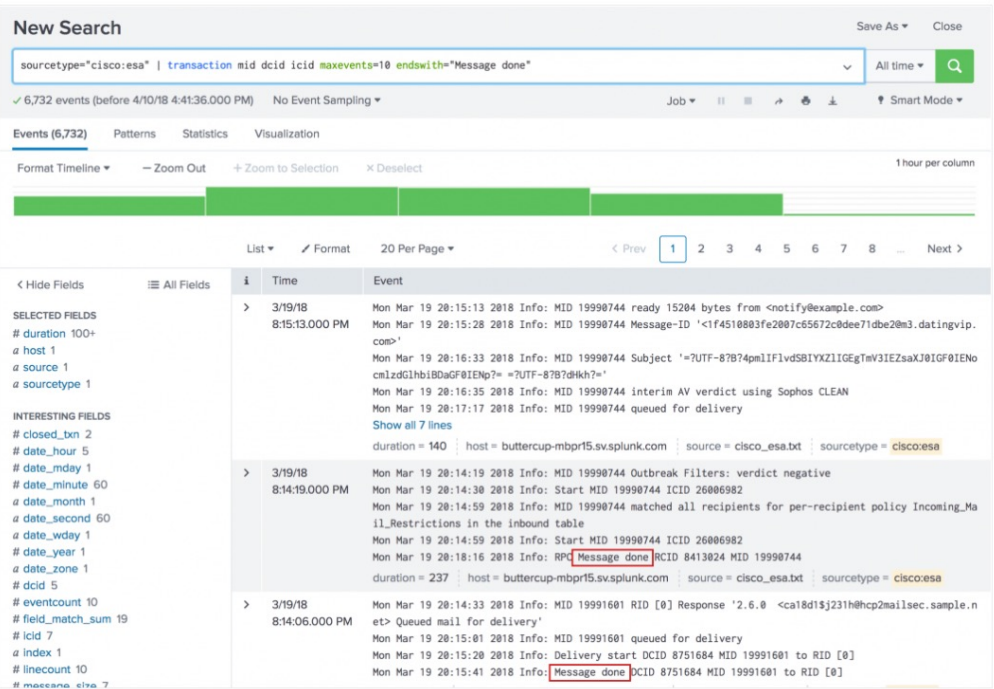
A transaction is  
group of  
conceptually  
related events  
that spans time.

Transactions  
can include:

- Different events from the same source and the same host.
- Different events from different sources from the same host.
- Similar events from different hosts and different sources.

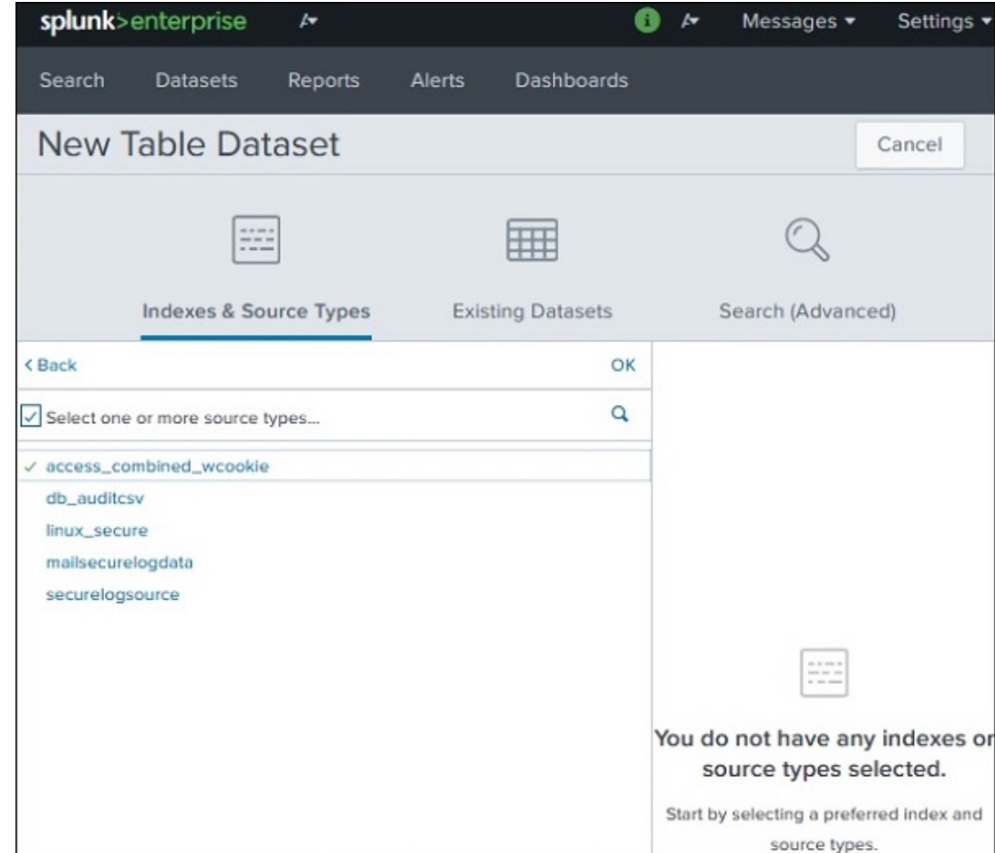
```
sourcetype="cisco:esa" | transaction mid dcid icid maxevents=10 endswith="Message done"
```

This search produces the following list of events:



# Data Models

- Data models enable users of Pivot to create compelling reports and dashboards without designing the searches that generate them.
- Data Models consist of datasets.



Questions

