Splunk® Enterprise Knowledge Manager
Manual 7.3.1

About tags and aliases

Generated: 9/26/2019 2:54 am
About tags and aliases

In your data, you might have groups of events with related field values. To search more efficiently for these groups of event data, you can assign tags and aliases to your data.

If you tag tens of thousands of items, use field lookups. Using many tags will not affect indexing, but your search has better event categorization when using lookups. For more information on field lookups, see About lookups.

Tags

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

You can use tags to help you track abstract field values, like IP addresses or ID numbers. For example, you could have an IP address related to your main office with the value 192.168.1.2. Tag that IPAddress value as mainoffice, and then search for that tag to find events with that IP address.

You can use a tag to group a set of field values together, so that you can search for them with one command. For example, you might find that you have two host names that refer to the same computer. You could give both of those values the same tag. When you search for that tag, events that involve both host name values are returned.

You can give extracted fields multiple tags that reflect different aspects of their identity, which enable you to perform tag-based searches to help you narrow the search results.

Tags example

You have an extracted field called IPAddress, which refers to the IP addresses of the data sources within your company intranet. You can tag each IP address based on its functionality or location. You can tag all of your routers’ IP addresses as router, and tag each IP address based on its location, for example, SF or Building1. An IP address of a router located in San Francisco inside Building 1 could have the tags router, SF, and Building1.

To search for all routers in San Francisco that are not in Building1, use the following search.
Tags and the search-time operations sequence

When you run a search, Splunk software runs several operations to derive knowledge objects and apply them to events returned by the search. Splunk software performs these operations in a specific sequence.

Search-time operation order

Tags come last in the sequence of search-time operations.

Restrictions

The Splunk software applies tags to field/value pairs in events in ASCII sort order. You can apply tags to any field/value pair in an event, whether it is extracted at index time, search time, or added through some other method, such as an event type, lookup, or calculated field.

For more information

For more information about search-time operations, see search-time operations sequence.

Field aliases

Field aliases enable you to normalize data from multiple sources. You can add multiple aliases to a field name or use these field aliases to normalize different field names. The use of Field aliases does not rename or remove the original field name. When you alias a field, you can search for it with any of its name aliases. You can alias field names in Splunk Web or in props.conf. See Create field aliases in Splunk Web.

You can use aliases to assign different extracted field names to a single field name.

Field aliases for all source types are used in all searches, which can produce a lot of overhead over time.

Field Aliases example

One data model might have a field called http_referrer. This field might be misspelled in your source data as http_referer. Use field aliases to capture the
misspelled field in your original source data and map it to the expected field name.

**Field aliases and the search-time operations sequence**

*Search-time operations order*

Field aliasing comes fourth in the search-time operations order, before calculated fields but after automatic key-value field extraction.

*Restrictions*

Splunk software processes field aliases belonging to a specific host, source, or sourcetype in ASCII sort order. You can create aliases for fields that are extracted at index time or search time. You cannot create aliases for fields that are added to events by search-time operations that come after the field aliasing process.

*For more information*

For more information about search-time operations, see search-time operations sequence.