Splunk® Enterprise Knowledge Manager Manual 8.0.1

Create field aliases in Splunk Web

Generated: 12/30/2019 12:50 pm
Create field aliases in Splunk Web

In your data, you might have groups of events with related field values. To help you search for these groups of fields, you can assign field aliases to their field values.

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. A field can have multiple aliases, but a single alias can only apply to one field. For example, the field vendor_action can be an alias of the original fields action or message_type, but not both original fields at the same time. An alias does not replace or remove the original field name.

For more information on aliases, see About tags and aliases.

Preserve existing field values

You can change the behavior of a field alias by selecting Overwrite field values when you define it. This affects how the Splunk software handles situations where the original field has no value or does not exist, as well as situations where the alias field already exists as a field in your events, alongside the original field.

Overwrite field values is not selected by default.

This table shows you how Overwrite field values affects the behavior of a field alias. Say you have a field alias definition where the original field src has been given dst as an alias.

<table>
<thead>
<tr>
<th>When Overwrite field values...</th>
<th>And the events we search for contain both src and dst...</th>
<th>And the events we search contain only dst...</th>
</tr>
</thead>
<tbody>
<tr>
<td>is not selected...</td>
<td>The value of the field alias dst is unchanged.</td>
<td>The field alias dst remains as-is.</td>
</tr>
<tr>
<td></td>
<td>The search head replaces the value of the field alias dst with the value of the original field src, because dst is an alias of src.</td>
<td>The search head removes dst from the event because dst is an alias of a field that is not present.</td>
</tr>
</tbody>
</table>

1
Where field aliases fit in the search-time sequence of operations

When you run a search, Splunk software runs several operations to derive various knowledge objects and apply them to the events returned by the search. Splunk software applies field aliases to a search after it performs key-value field extraction, but before it processes calculated fields, lookups, event types, and tags.

This means that you can create aliases for fields that are extracted at index time or search time, but you cannot create aliases for calculated fields, event types, tags, or fields that are added to your events by a lookup.

On the other hand, you can reference field aliases in the configurations for search-time operations that follow the field aliasing process. For example, you can design a lookup table that is based on a field alias. You might do this if one or more fields in the lookup table are identical to fields in your data but have different names.

See The sequence of search-time operations.

Create a field alias with Splunk Web

You can use Splunk Web to assign an alternate name to a field, allowing you to use that name to search for events that contain that field.

Prerequisites

- See About tags and aliases for more information on aliases.

Steps

1. Locate a field within your search that you would like to alias.
2. Select Settings > Fields > Field aliases.
3. (Required) Select an app to use the alias.
4. (Required) Enter a name for the alias. Currently supported characters for alias names are a-z, A-Z, 0-9, or _.
5. (Required) Select the host, source, or sourcetype to apply to a default field.
6. (Required) Enter the name for the existing field and the new alias. The existing field should be on the left side, and the new alias should be on the right side.
7. (Optional) Select **Overwrite field values** if you want your field alias to remove the alias field name when the original field does not exist or has no value, or replace the alias field name with the original field name when the alias field name already exists.

8. Click Save.

View your new field alias on the **Field Aliases** page.

**If you must associate a single alias field name with multiple original field names**

You should not design field alias configurations that apply a single alias field name to multiple original field names. If you must do this, set the field alias up as a **calculated field** that uses the `coalesce` function to create a new field that takes the value of one or more existing fields. This method lets you be explicit about ordering of input field values in the case of NULL fields. For example: `EVAL-ip = coalesce(clientip, ipaddress)`.