splunk>

Lab Exercise 9: Field Aliases and Calculated Fields

Description

This lab exercise walks you through the process of creating field aliases and calculated fields.

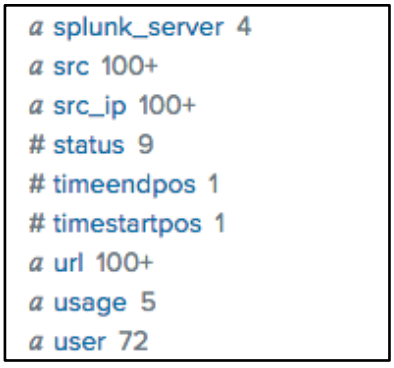
Steps

Scenario: **The IT Ops team runs reports for all employee access but the user name field is not consistent across the different source types.**

Task 1: Create a field alias so that *cs_username* also appears as *user*.

1. Search for all events in the `cisco_wsa_squid` sourcetype over the **last 7 days**.
2. Note the `cs_username` field values.
3. Go to **Settings > Fields > Field aliases**. Create a field alias with the following values:
   - Destination app: search
   - Name: cisco_wsa_squid_aliases
   - Apply to: sourcetype
   - Named: cisco_wsa_squid
   - Field aliases: cs_username = user
4. Click **Save**.
5. Return to the **Search & Reporting app**. Re-run your search and examine the user field and values.

Results Example:



6. Search for all events in the `cisco_firewall` sourcetype over the **last 30 days**.
7. Note the `Username` field values.
8. Create another field alias for sourcetype `cisco_firewall` with the following values:
   - Destination app: search
   - Name: cisco_firewall_aliases
   - Apply to: sourcetype
   - Named: cisco_firewall
   - Field aliases: Username = user
9. Perform the following search: `index=network sourcetype=cisco* user=*` over the last 30 days. Do you receive results from the `cisco_wsa_squid` and `cisco_firewall` sourcetypes?

   Yes, you should see both source types.

NOTE: It may take a few moments before the field aliases are applied and appear in searches.

Scenario: **The IT Ops team is monitoring bandwidth usage for all users for the last month, but the data is reported in bytes. The team needs the usage to be measured in megabytes.**

Task 2: Create a calculated field that converts bytes to MB.

10. Search for all events in the **last 7 days** for the `cisco_wsa_squid` sourcetype.

    index=network sourcetype=cisco_wsa_squid

11. Note the `sc_bytes` field. This field displays the amount of bytes used for that event.
12. Go to Settings > Fields > Calculated fields.
13. Create a calculated field named **sc_megabytes** that converts the value of `sc_bytes` to MB with the following values:
    - Destination app: search
    - Apply to: sourcetype
    - Named: cisco_wsa_squid
    - Name: sc_megabytes
    - Eval expression: sc_bytes/(1024*1024)
    -
14. Return to the **Search & Reporting app**. Perform a search on the `cisco_wsa_squid` sourcetype that shows the total bandwidth by usage.

    index=network sourcetype=cisco_w* | stats sum(sc_megabytes) as "Bandwidth (MB)" by usage

Results Example:

usage	Bandwidth (MB)
Borderline	6.86968708038330100000
Business	17.08714580535888700000
Personal	54.93885517120361000000
Unknown	17.56064128875732400000
Violation	0.8761548995971680000

Task 3: Create field aliases for the access_combined sourcetype.

Scenario: **The IT Ops team wants to correlate data from multiple source types using the `http_action` and `http_method` fields. In the `access_combined` source type, these fields are currently called `action` and `method`.**

Task 1: Create two field aliases for the access_combined sourcetype called http_action and http_method, based on the existing access_combined fields action and method.

1. Create the field aliases.

2. Run a search to verify that the field aliases were created correctly.