splunk>

Lab Exercise 8: Field Extractions

Description

This lab exercise walks you through the process of creating field extractions based on either a Regular Expression (regex) or on Delimiters.

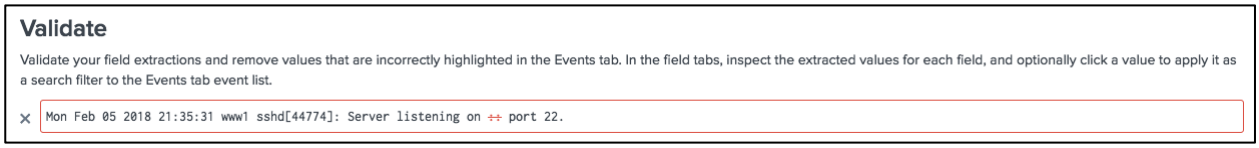
Steps

Scenario: Access to the Linux server needs to be monitored.

Task 1: Use the Field Extractor (FX) to extract the IP address and port fields using the Regular Expression method.

1. Search for all events in the **last 24 hours** for the `linux_secure` sourcetype that contain the keyword *port*.

   index=security sourcetype=linux_secure port
2. View the event details to see all the extracted fields. Click the > arrow under the i icon in the first event that contains an IP address value.
3. Click Event Actions > Extract Fields.
4. Select the **Regular Expression** method and click **Next**.
5. Highlight the IP address value in the sample event.
6. In the **Field name** box, type `src`.
7. Click Add Extraction.
8. Click on the src tab and verify the correct information is extracted. You may see that "**::**" is extracted as a src value. But within this **particular** set of data, "::" actually represents an **invalid** IP address. So you'll remove this value in the Validate process (Steps 12-13).
9. Highlight the port value.
10. In the **Field name** box, type `port`.
11. Click **Add Extraction** and click **Next**.
12. In the **Validate** step, click on the src tab. You will see "::" listed as a valid value. In the filter field, type `src=::` and click **Apply**.
13. Click the "x" next to the highlighted value of "**::**" for the src field. (It doesn't matter which event you choose.) The event sample will now show that "::" is an invalid value for the src field.



14. Click **Next**.
15. Review the Extractions Name and click **Finish**.
16. Wait for about 30 seconds, then search for events in the `linux_secure` sourcetype in the **last 24 hours**. List the top ports by IP address.

```
index=security sourcetype=linux_secure | top port by src
```

NOTE: It may take a few moments for the newly extracted fields to appear in the search. This is also true of all the other knowledge objects you'll create in this course. In general, it's best to wait about 30 seconds after object creation before submitting your search.

Results Example:

src	port	count	percent
107.3.146.207	3057	2	3.703704
107.3.146.207	4950	1	1.851852
107.3.146.207	4929	1	1.851852
107.3.146.207	4822	1	1.851852
107.3.146.207	4800	1	1.851852
107.3.146.207	4779	1	1.851852
107.3.146.207	4550	1	1.851852
107.3.146.207	4506	1	1.851852
107.3.146.207	4141	1	1.851852
107.3.146.207	4131	1	1.851852
108.50.217.115	8677	100	87.719298
108.50.217.115	7238	1	0.877193

Scenario: **The engineering team launched the beta of a new game called SimCube. To make improvements to the game, engineers want to see how users are playing the game. However, the log file doesn't contain headers and the fields are not auto-extracted.**

Task 2: Use FX to extract fields using the delimiters method.

17. Search for all events in the **last 30 days** for the SimCubeBeta sourcetype in the games index.

```
index=games sourcetype=SimCubeBeta
```

18. View the event details to see which fields are extracted.
19. Click the **>** arrow under the *i* icon in the first event.
20. Click Event Actions > Extract Fields.
21. Select the **Delimiters** method and click **Next**.
22. For the Delimiter type, select **Comma**.
23. Rename all the fields as follows (in this order):
    - field1 > time
    - field2 > src

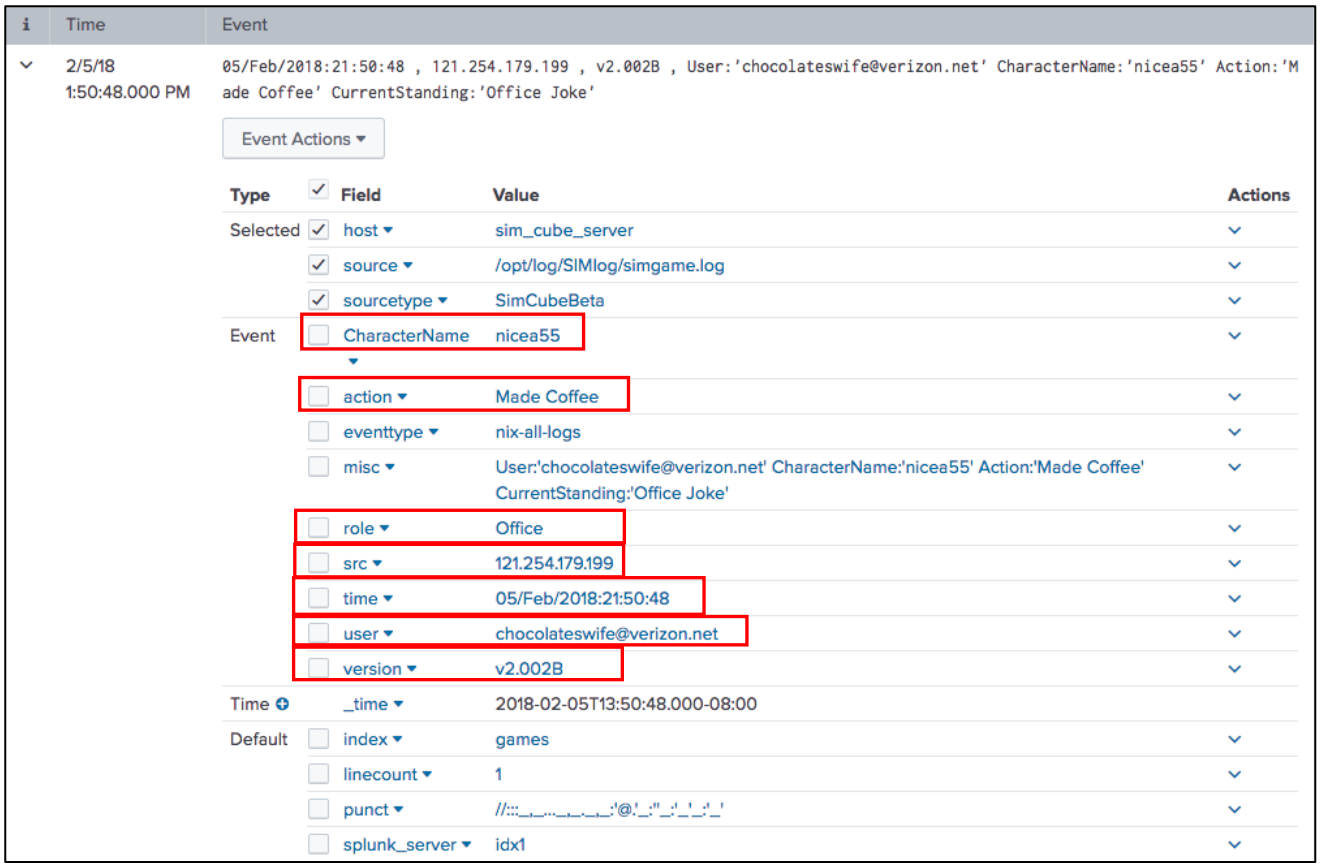
- field3 > version
- field4 > misc

24. After all the fields are renamed, click **Next**.
25. For Extractions Name, enter `simgame_log` and click **Finish>**.
26. Using the regex field extraction method, run the same search as you did in step 17 and extract the remaining fields (see results example below):
    - user
    - CharacterName
    - action
    - role
27. While still on the **Select fields** step (before the validation stage), click on **Non-Matches** to see whether any relevant events are being excluded. (If no events display when you click **Non-Matches**, proceed to step 31.)
28. Hover your cursor over any excluded event that you want to include, and click **+ Add sample event**.
29. Highlight each relevant value in the sample event and click **Select a Field**. For each value, choose the field name you want associated with that value and click **Add Extraction**.
30. Repeat steps 28 – 29 for each excluded event until there are no more **Non-Matches**.
31. Click **Next** to proceed to the **Validate** step.
32. When you're satisfied with your result, click **Next**.

NOTE: Be sure to thoroughly check your results during the validation stage. It's important to assure you've captured all characters inside the single quotes for the fields you've extracted.

33. Accept the prefilled Extractions Name and click **Finish>** to save.
34. Run your search again and check that all expected fields appear.

Results Example:



NOTE: It may take a few moments before the newly extracted fields appear in the search.