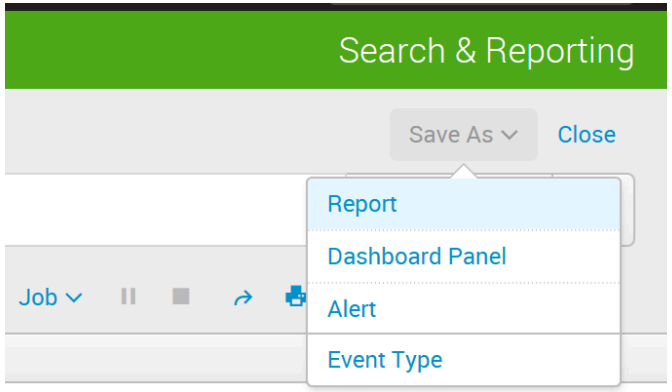
Splunk Knowledge Objects>

- Knowledge Objects add knowledge to and enrich your data
- User or app created
- Include
  - Saved searches, field extractions, tags, event types, lookups, reports, alerts, data-models, and more

Splunk Knowledge Objects>

Saved Searches

- Can be saved as reports, alerts, dashboard panels, or event types
- Defined in `savedsearches.conf`



Splunk Knowledge Objects>

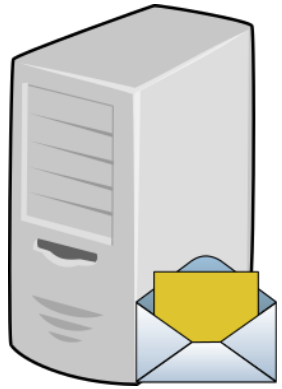
Field Extractions

- Fields can be extracted using the field extraction editor
  - Regex or Delimiter
- Defined in `props.conf`

Splunk Knowledge Objects>

Tags

- Allow you to assign names to specific field and value combinations
- Example: you might have a server named `east-uk-server-1433-mail1.east.uk.local`



`east-uk-server-1433-mail1.east.uk.local`

Splunk Knowledge Objects>

Tags

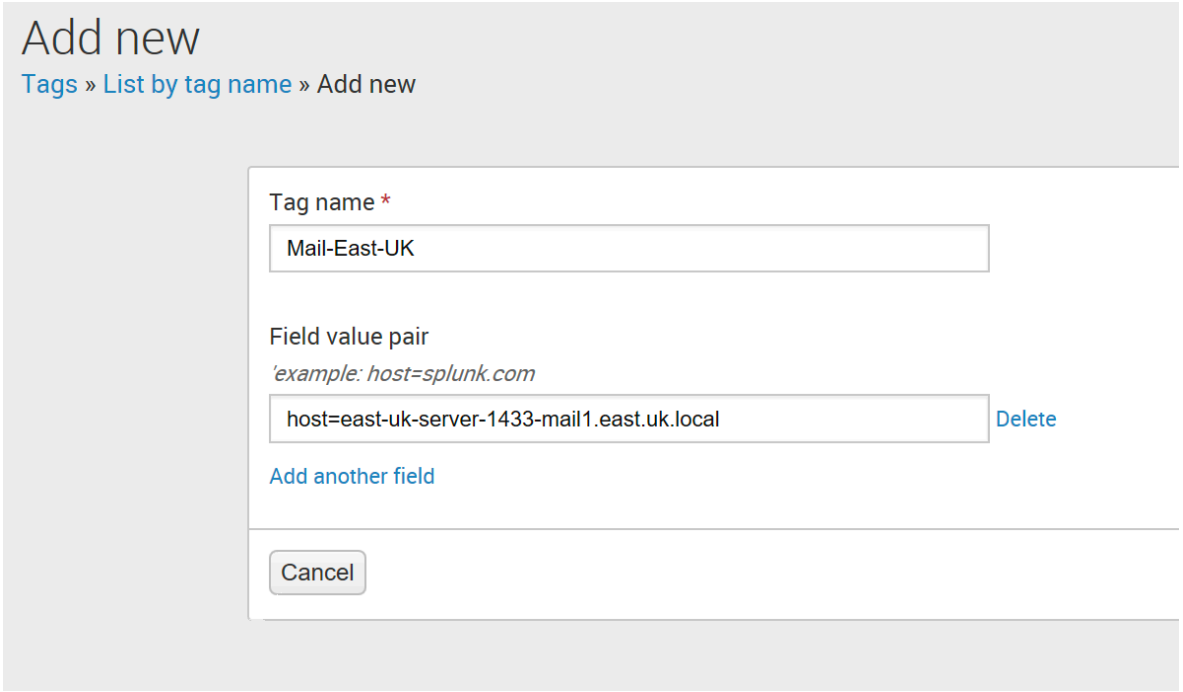
- You know that this server is the *mail server* for the *eastern UK region* and it resides in building *1433*
- Splunk and other users do not know that

Splunk Knowledge Objects>

Tags

- Create a tag!

- `Tag=Mail-East-UK`



Splunk Knowledge Objects>

Event Types

- A named saved search
- A “tag +”
- Suppose you have a search that your organization runs frequently, perhaps even with small additions

```
host=homeworkdata usr=* state=*  domain="east.us.domain.lcl" level=error
```

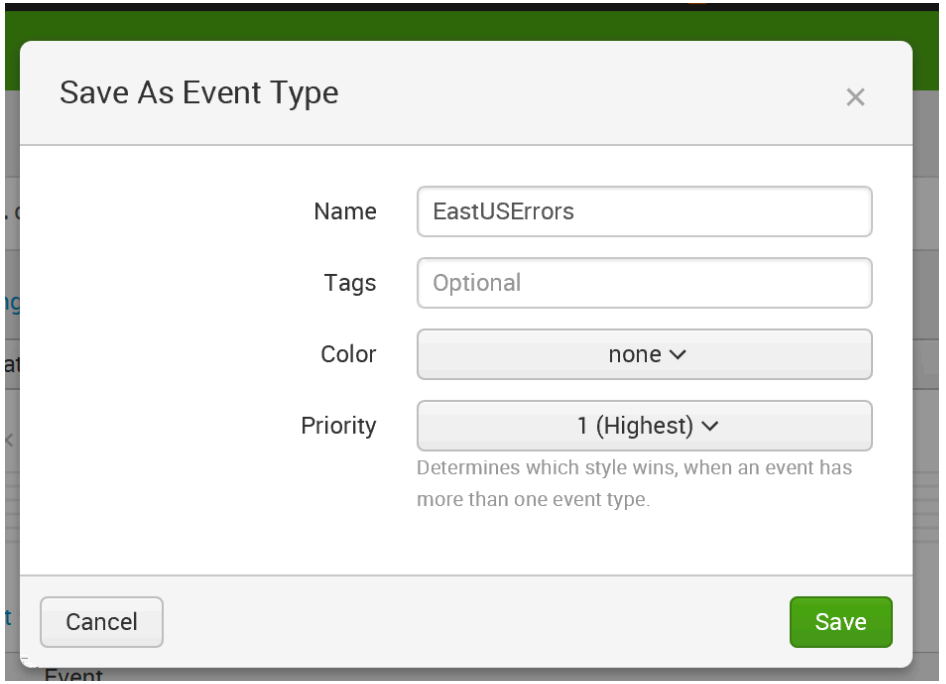
Splunk Knowledge Objects>

Event Types

- Instead of typing that in every time, just create an event type!

- `Eventtype=EastUSErrors`

- You can even include tags!



Splunk Knowledge Objects>

Lookups

- Add custom fields to events from external sources, like csv files

Not user friendly

regioncodes.csv

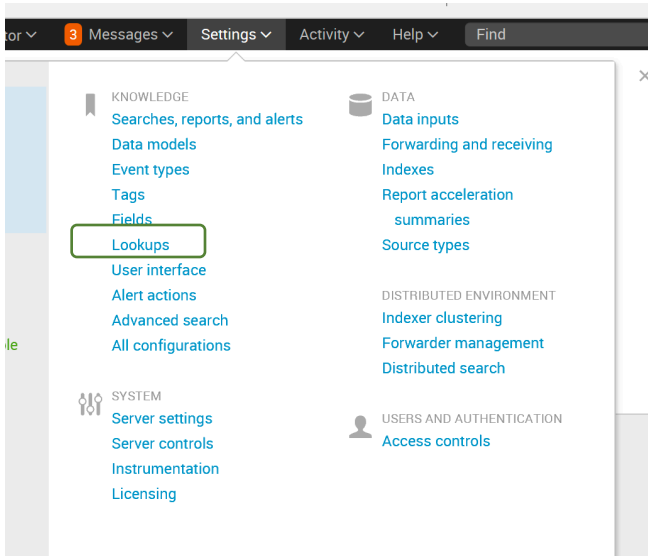
Region Code	Region Name
1012	West US
2443	East US
3839	West UK
4443	East UK

User friendly

Splunk Knowledge Objects>

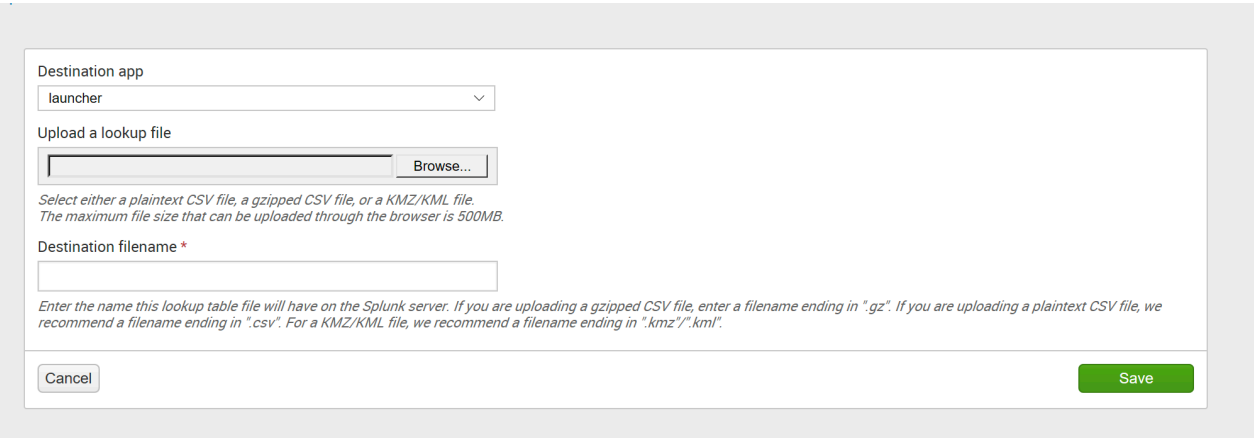
Lookups

1



2

3



Splunk Knowledge Objects>

Lookups

```
| lookup <lookup-table-name> <lookup-field1>
AS <event-field1>
| lookup regioncodes.csv “Region Code” AS
regcode
```

Splunk Knowledge Objects>

Data Models

- Hierarchically structured data set that includes
  - Events
  - Searches
  - Transactions

Splunk Knowledge Objects>

Data Models

- Event objects contain
  - Constraints
    - A search string broken down into a hierarchy
    - `host=router1`
    - `sourcetype=csv`
  - Attributes
    - Fields and properties associated with the event
    - `evals`, `lookups`, `extracted fields`

Splunk Knowledge Objects>

Data Models

- Power the Splunk Pivot tool
- To get to the Pivot tool
  - Through the datasets page
  - Through the data model page in settings
  - Through the search results page, visualization tab

Demo: Knowledge Objects

Thanks, Splunkers!