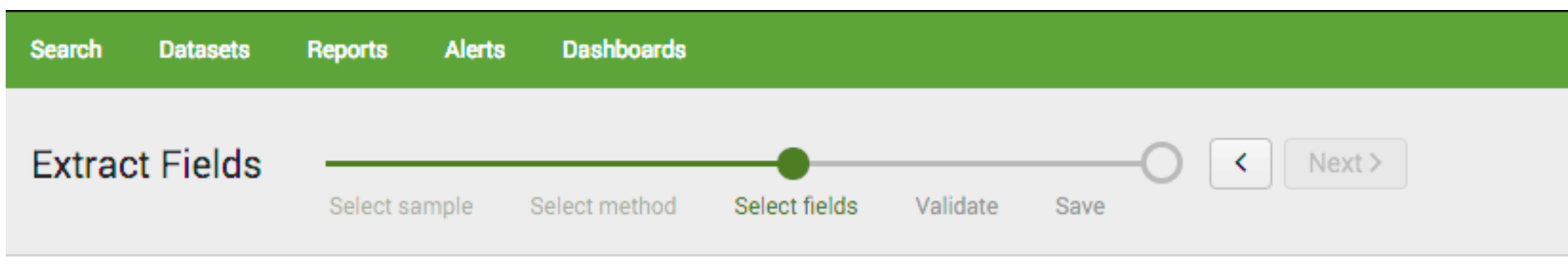


1. Extract a field name or use an existing field name to map.

I have Priority already extracted  
Using all lower case for fields to be uniform.



Select Fields

Highlight one or more values in the sample event to create fields. You can indicate one value is required, meaning it must exist in an event for the regular sample event to modify them. To highlight text that is already part of an existing extraction, first turn off the existing extractions. [Learn more](#)

```
<157>Oct 8 17:41:14 ip-172-31-7-6 event: SYSTEM: SYSTEM_AUTHENTICATION_SESSION_CLOSED: - - CLI session pts/1 [
```

2. Create CSV file.

To simplify , use same source field name (severity) as you just extracted.

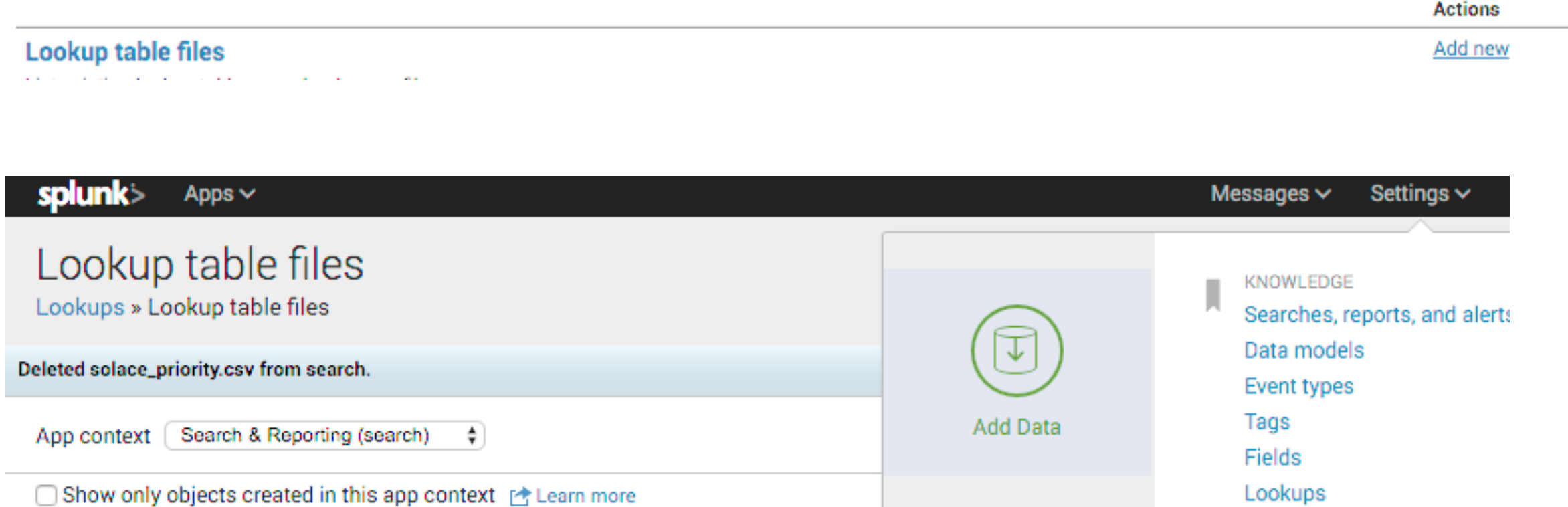
```
hermosa:~$ head solace_priority.csv
```

```
priority,severity,facility
128,EMERGENCY,local0
129,ALERT,local0
130,CRITICAL,local0
131,ERROR,local0
132,WARNING,local0
133,NOTICE,local0
134,INFO,local0
135,DEBUG,local0
136,EMERGENCY,local1
```

3. Create New Lookup

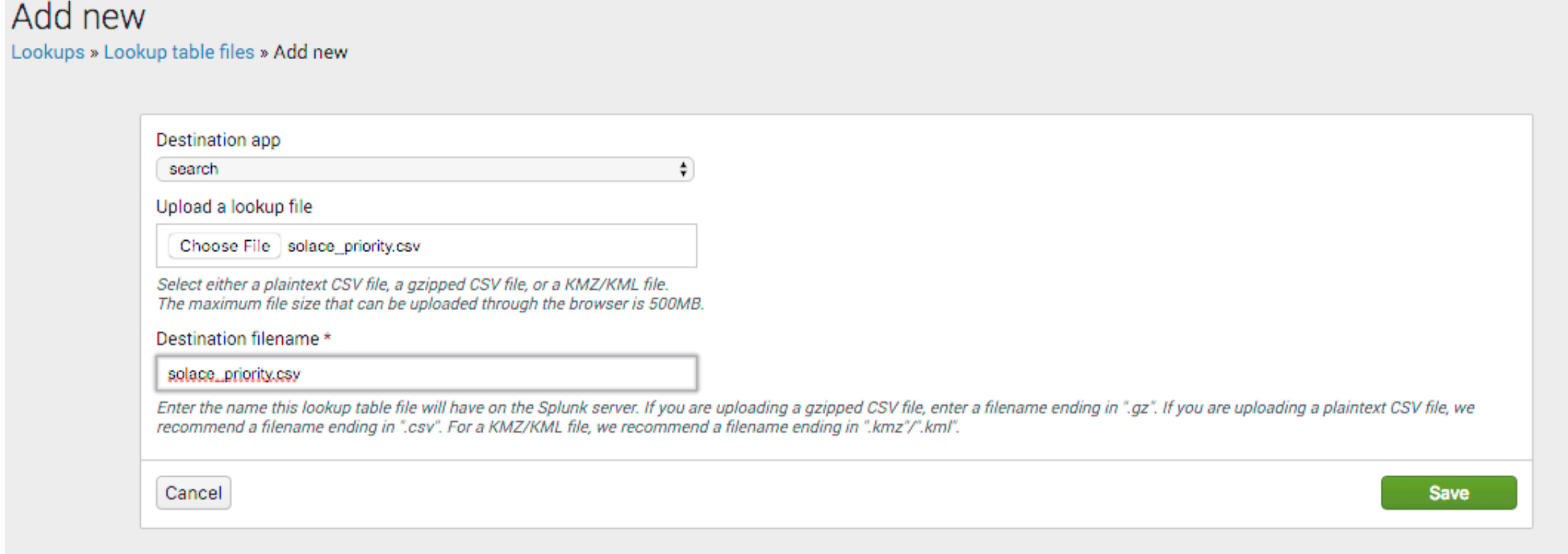
## Lookups

Create and configure lookups.



4. Select CSV file.

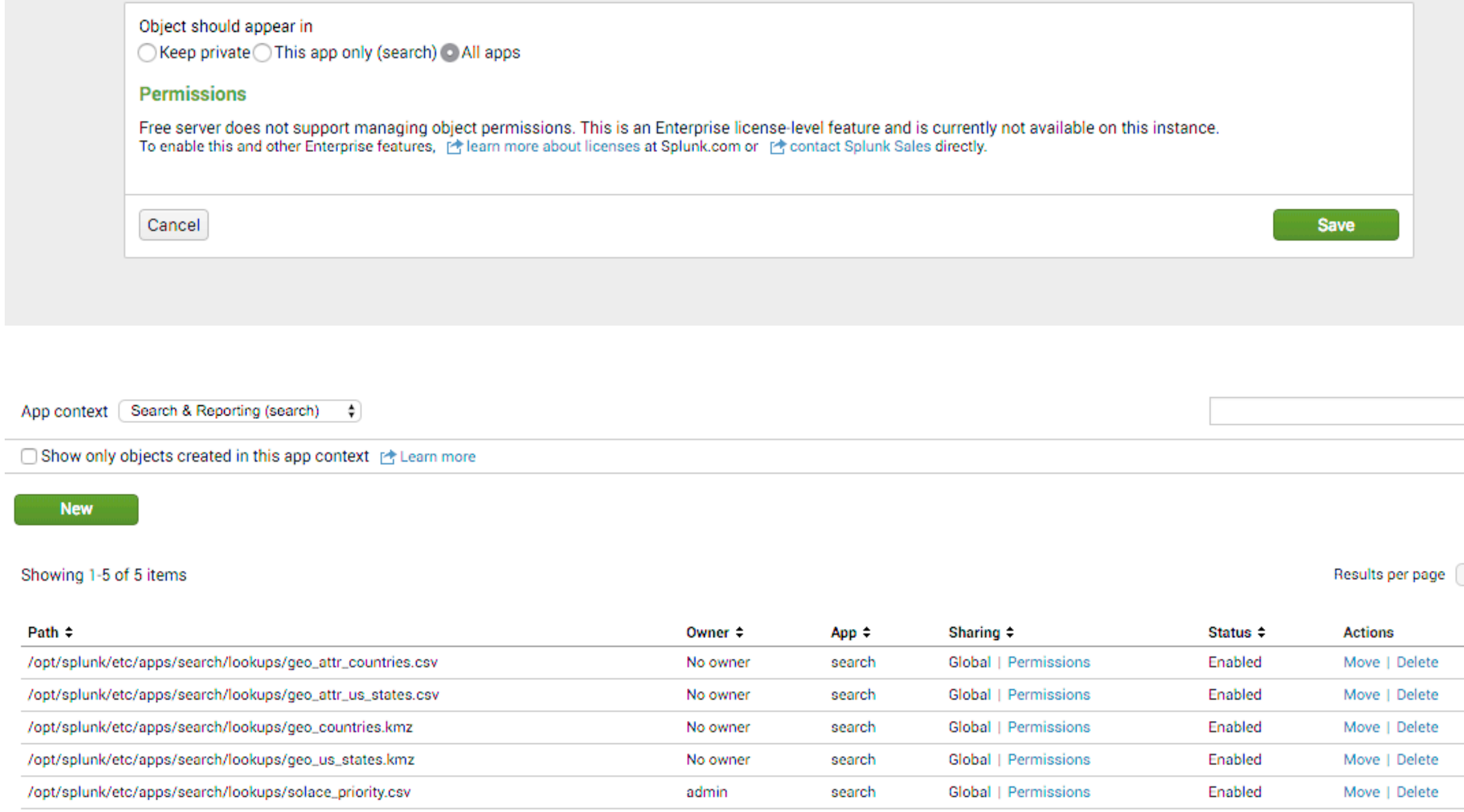
Using same name as file to simplify



5. Change Permissions

## Permissions

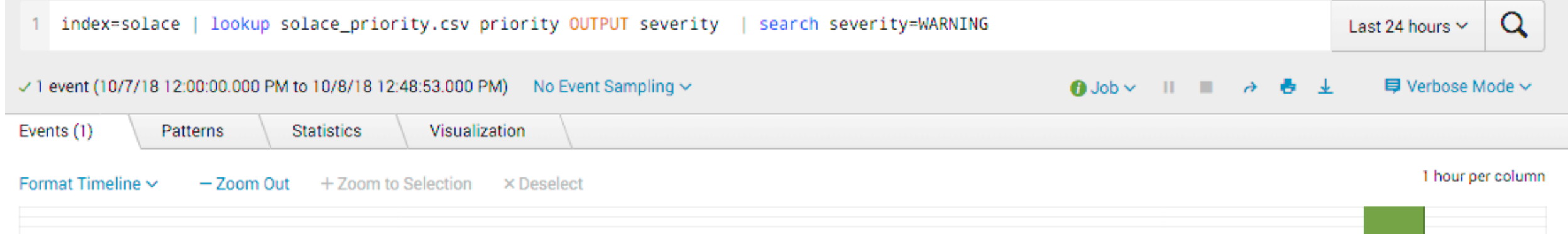
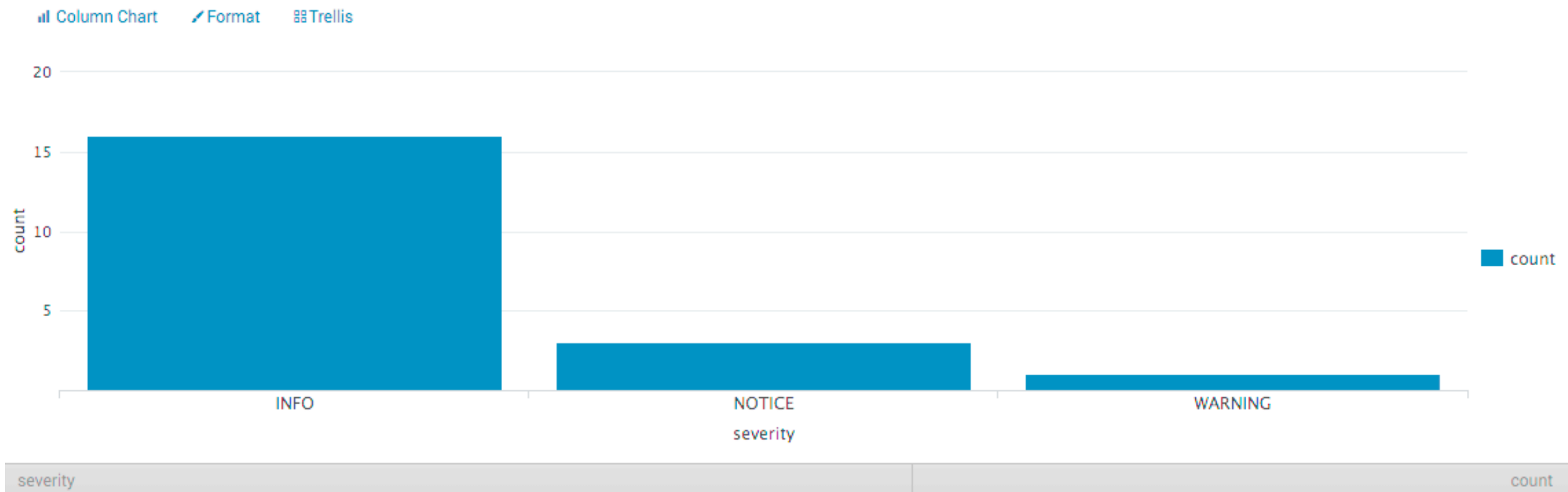
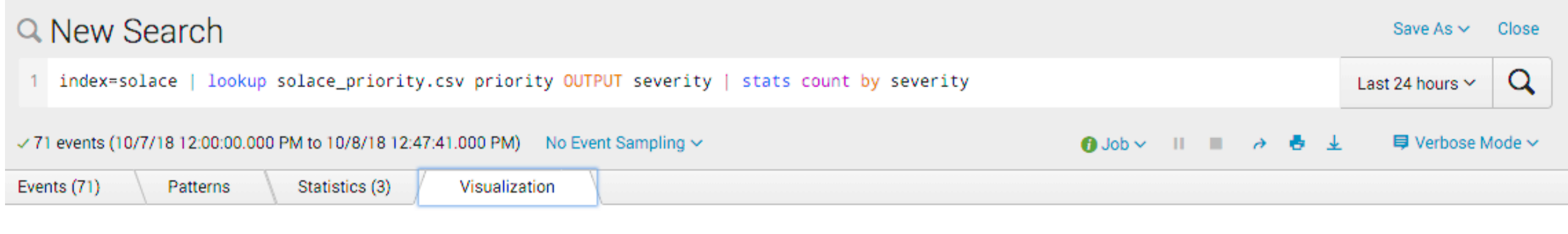
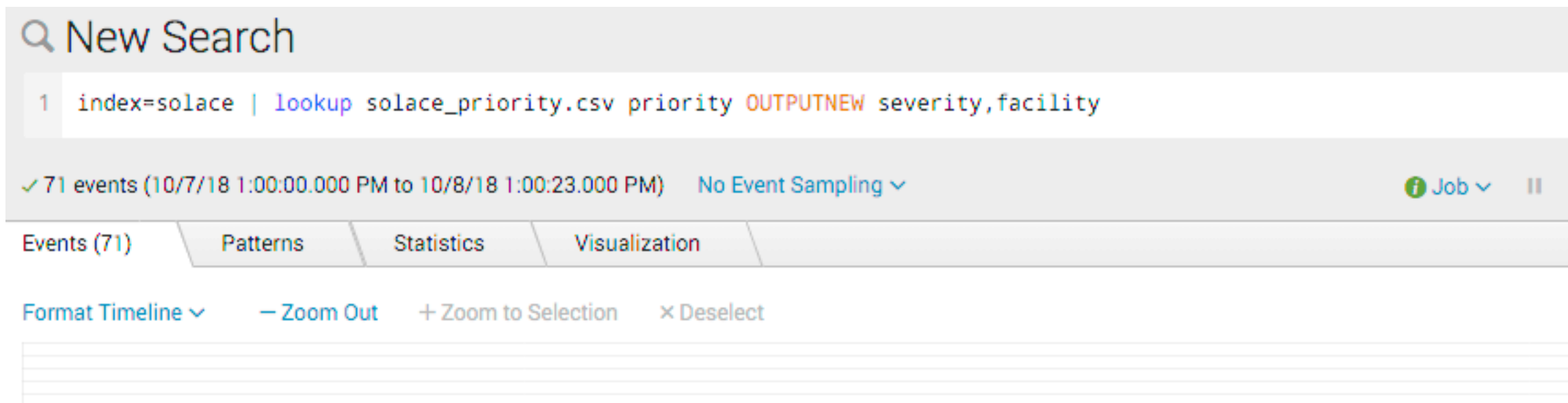
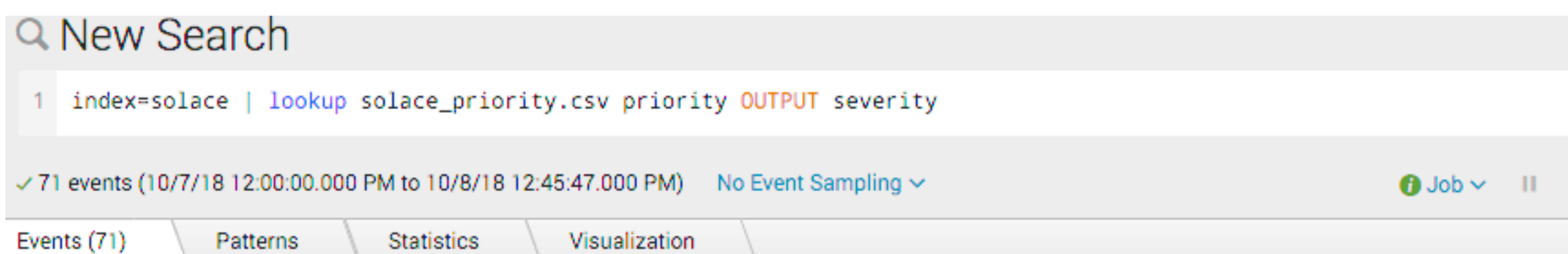
Lookups » Lookup table files » solace\_priority.csv » Permissions



6. Use search and pipe to lookup command

You can map to multiple fields (priority -> severity, facility)  
or search on new fields.

```
index=solace | lookup solace_priority.csv priority OUTPUT severity
index=solace | lookup solace_severity.csv PRI OUTPUT Severity | stats count by Severity
index=solace | lookup solace_priority.csv priority OUTPUTNEW severity,facility
```



i Time Event		
>	10/8/18 10:32:43.000 AM	<156>Oct 8 15:32:43 ip-172-31-7-6 event: VPN: VPN_VPN_STATE_CHANGE: default - Message VPN (0) default t State Changed to: down host = ip-172-31-7-6   priority = 156   severity = WARNING   source = tcp:515   sourcetype = syslog