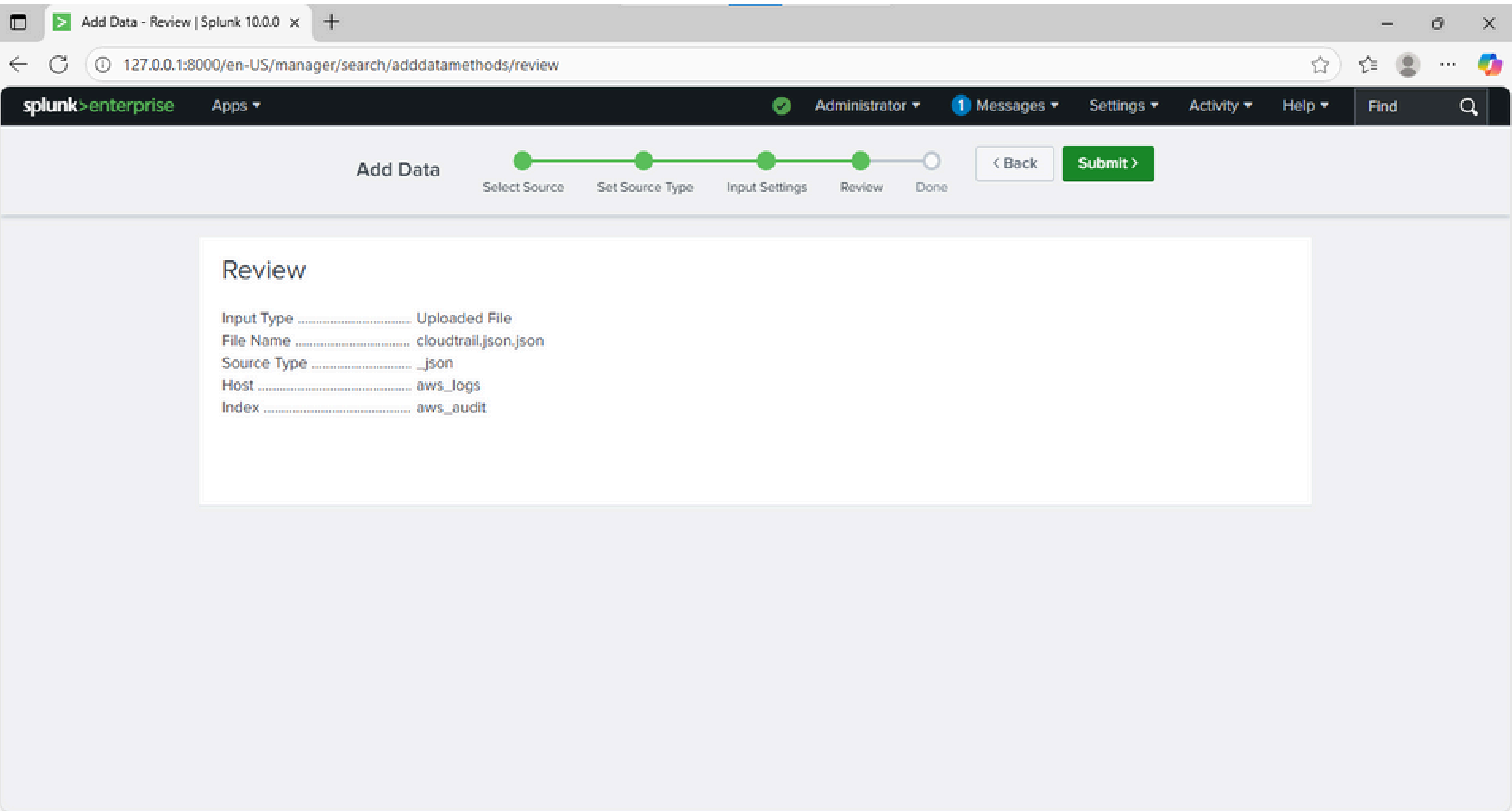
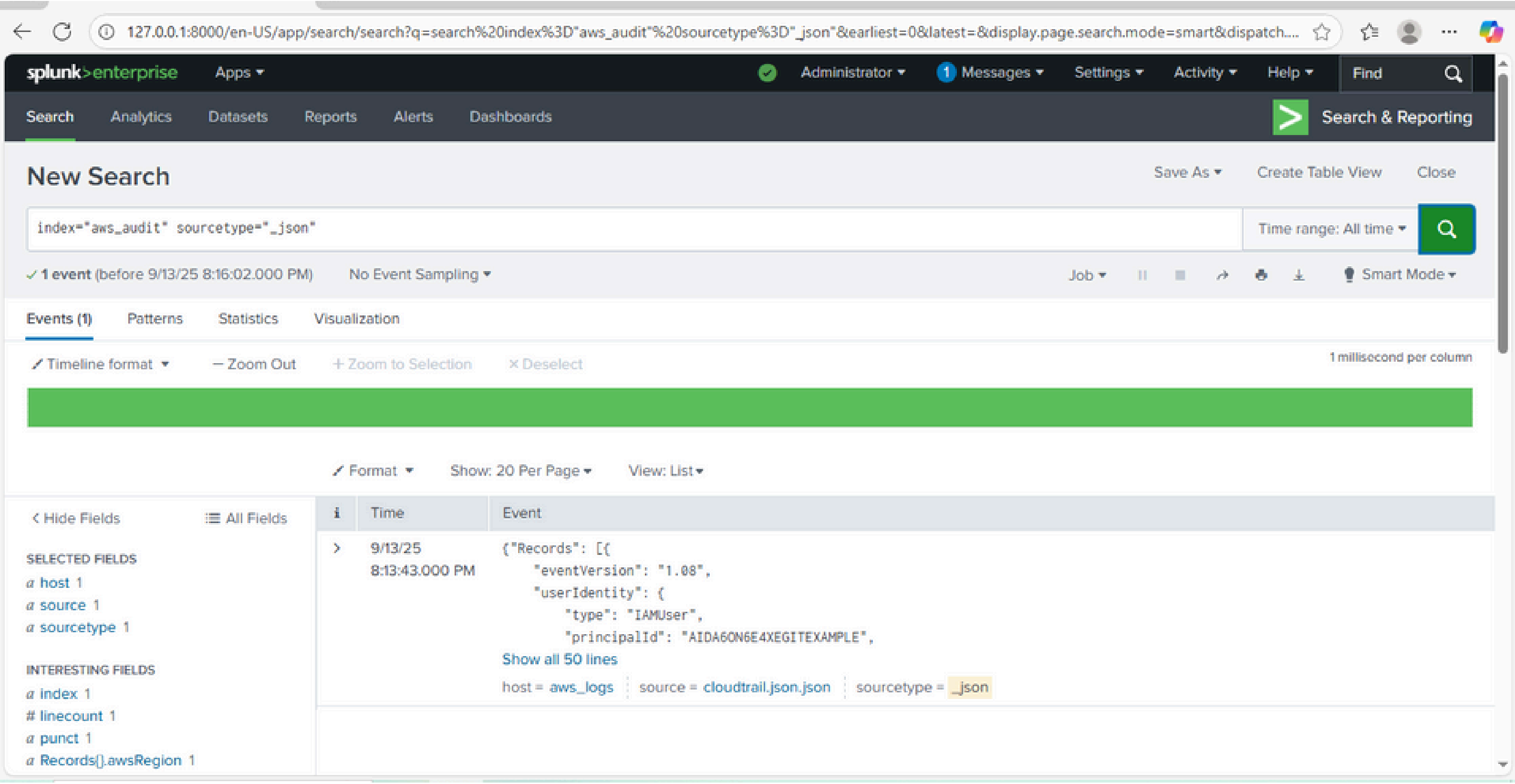
→ Screenshot 1: Adding sample log data to splunk in JSON format



Review

Input Type .... Uploaded File
File Name .... cloudtrail.json.json
Source Type .... _json
Host .... aws_logs
Index .... aws_audit

→ Screenshot 2: Shows simple search retrieving raw data



New Search

```
index="aws_audit" sourcetype="_json"
```

Time range: All time

✓ 1 event (before 9/13/25 8:16:02.000 PM)   No Event Sampling

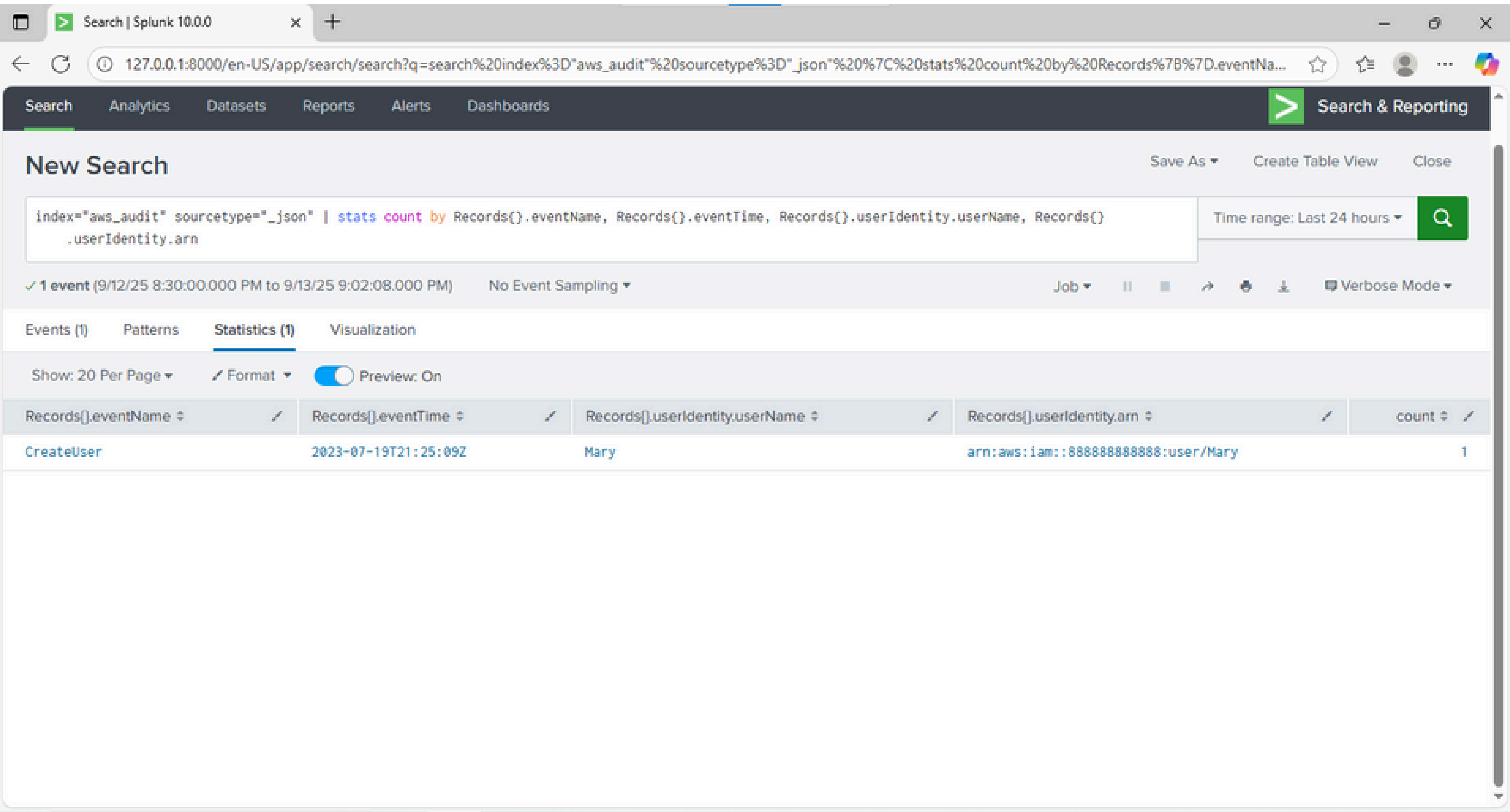
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a index 1
# linecount 1
a punct 1
a Records{}.awsRegion 1

i	Time	Event

>	9/13/25
	8:13:43.000 PM
		{"Records": [{
		"eventVersion": "1.08",
		"userIdentity": {
		"type": "IAMUser",
		"principalId": "AIDA6ON6E4XEGITEXAMPLE",
		Show all 50 lines
		host = aws_logs source = cloudtrail.json.json sourcetype = _json

→ Screenshot 3: Searching a query using stats to summarize data .



New Search

```
index="aws_audit" sourcetype="_json" | stats count by Records{}.eventName, Records{}.eventTime, Records{}.userIdentity.userName, Records{}
    .userIdentity.arn
```

✓ 1 event (9/12/25 8:30:00.000 PM to 9/13/25 9:02:08.000 PM)

Records{}.eventName	Records{}.eventTime	Records{}.userIdentity.userName	Records{}.userIdentity.arn	count
CreateUser	2023-07-19T21:25:09Z	Mary	arn:aws:iam::888888888888:user/Mary	1