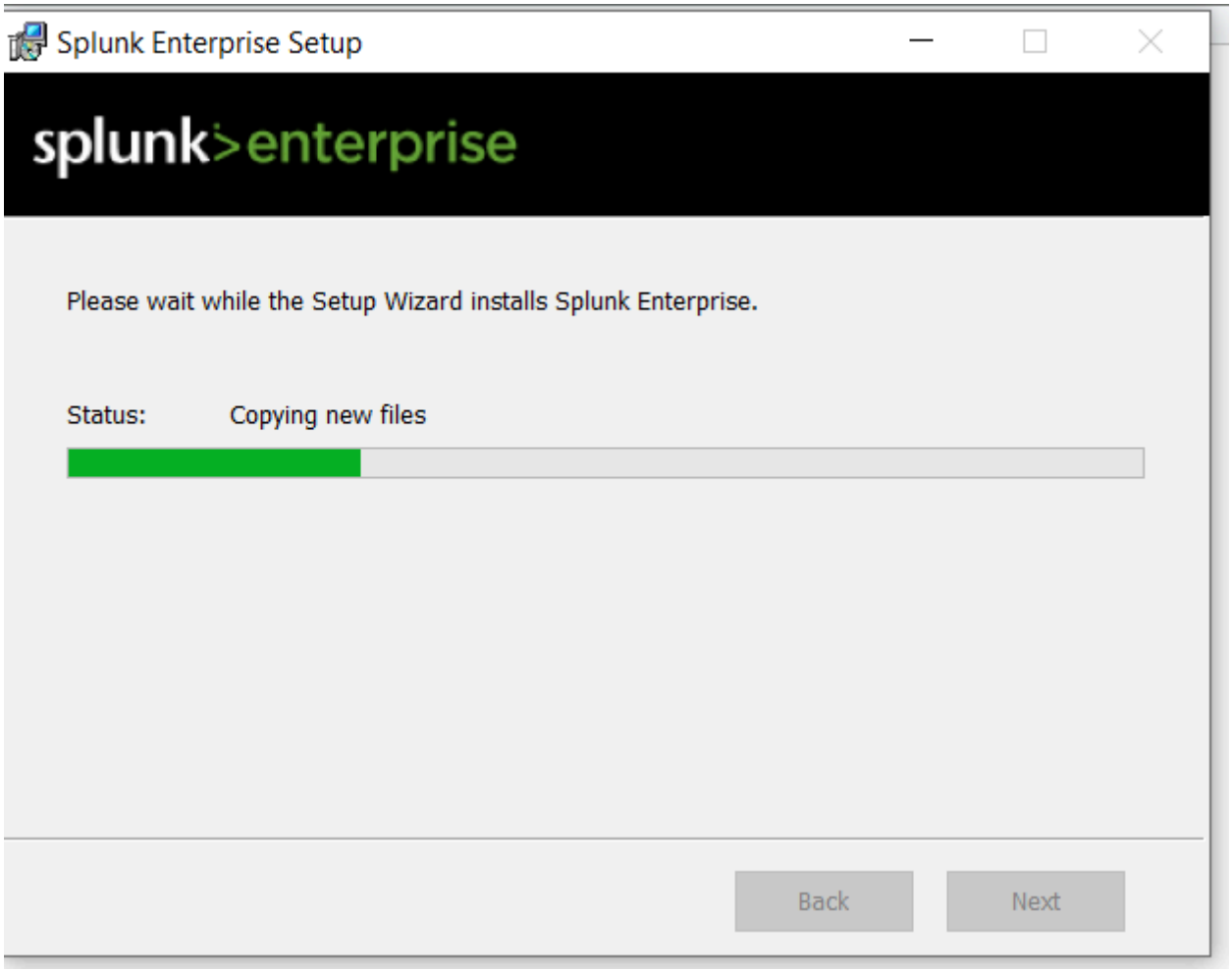
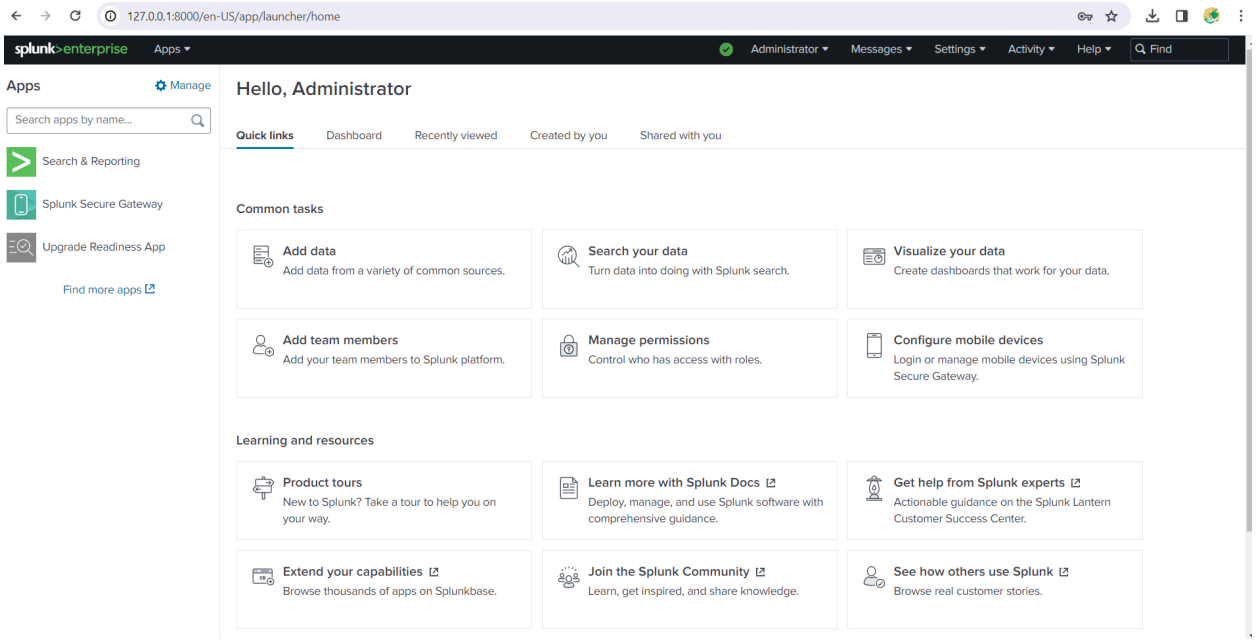
Splunk Introduction - Analysis of a Log

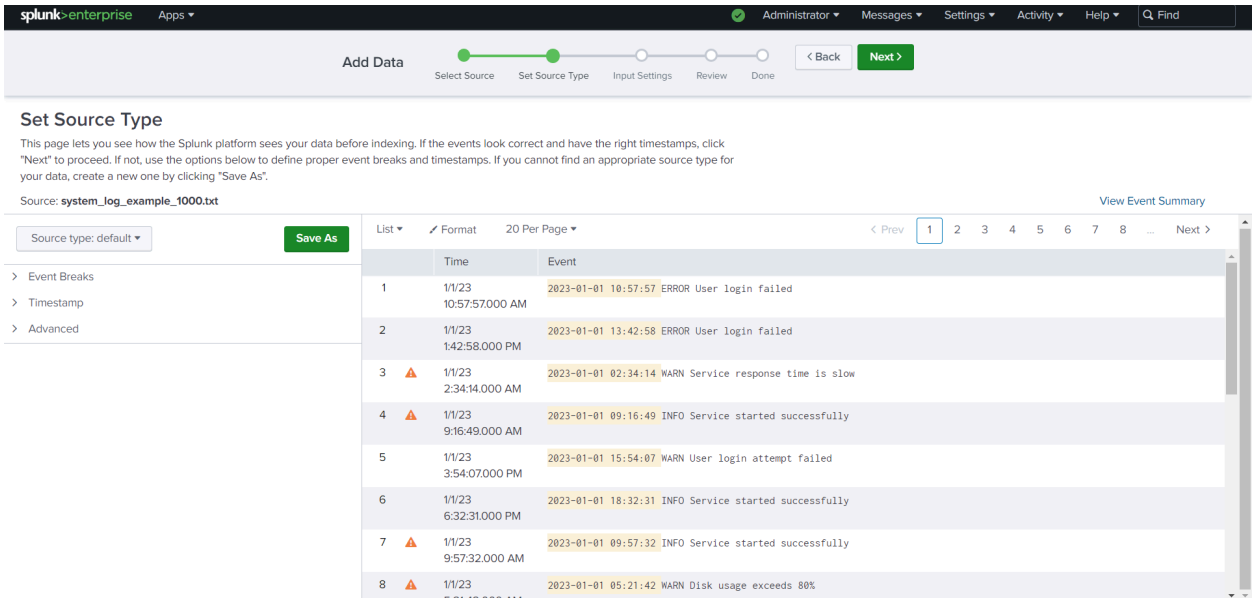
Installing splunk

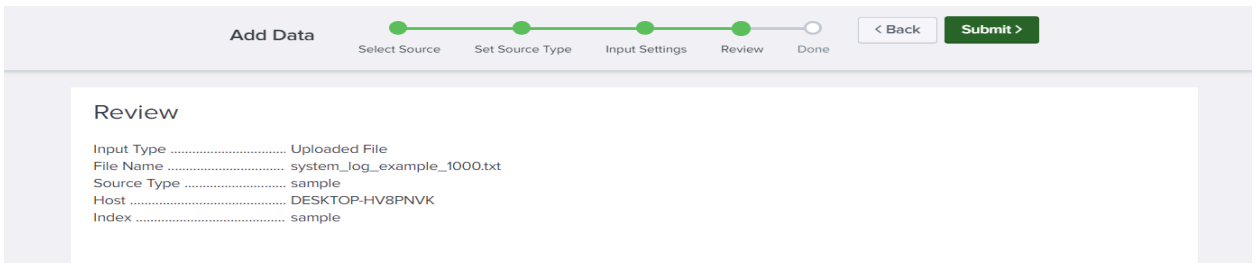


Splunk interface

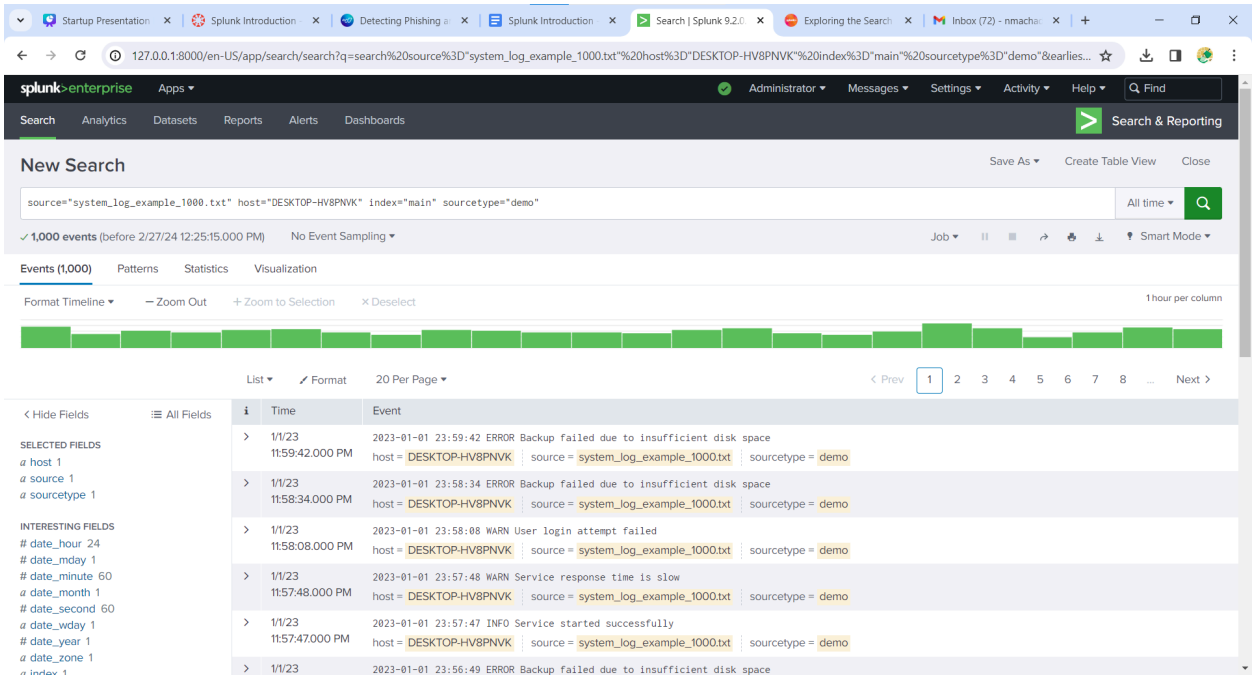


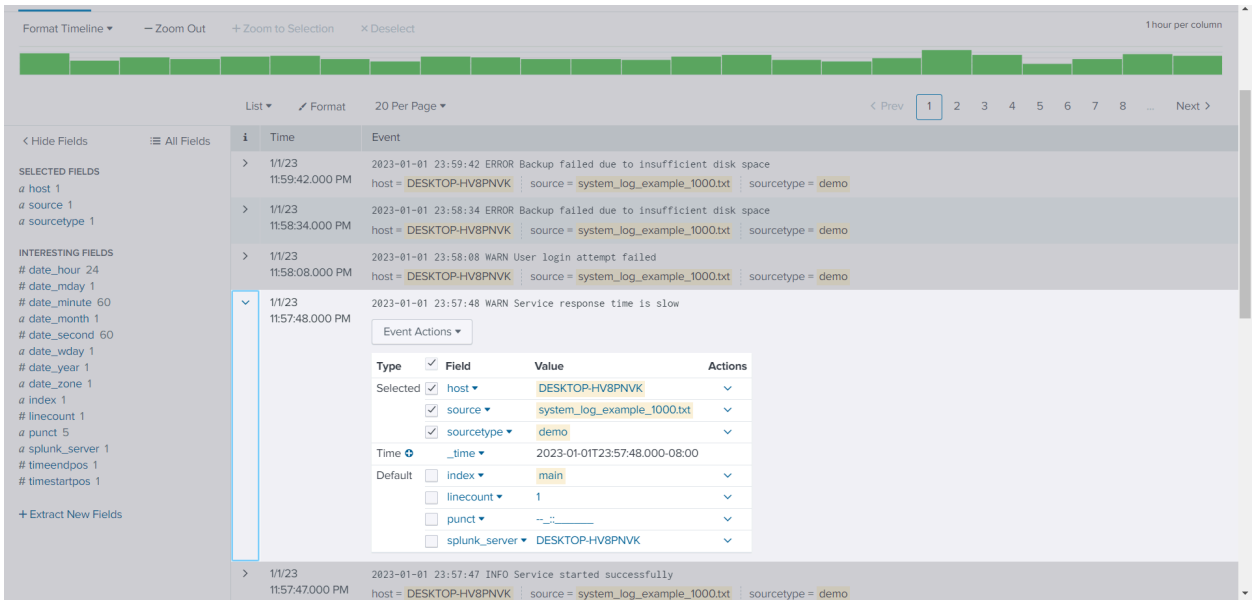
Adding the given file for analysis to inspect and analyze the logs.

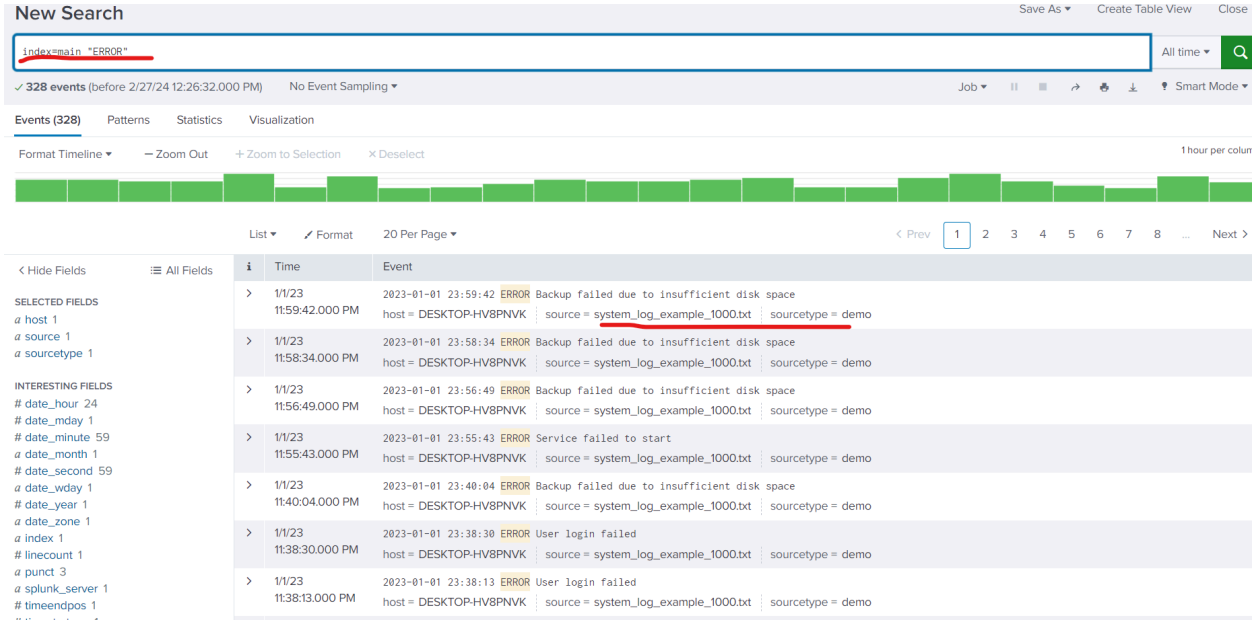




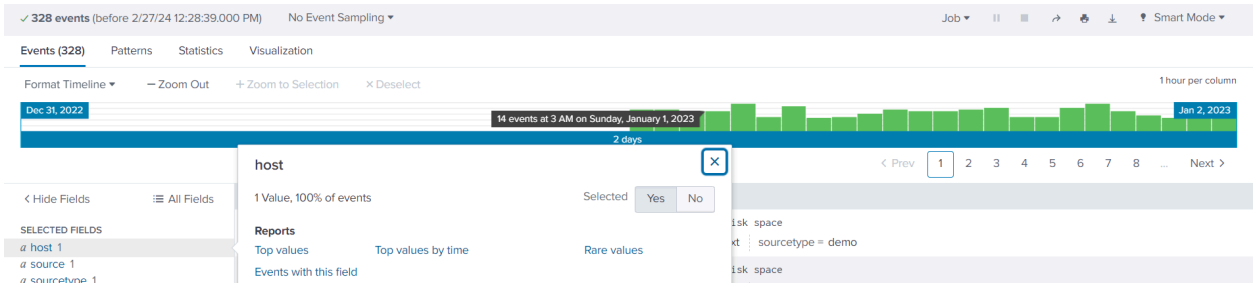
Lets analyze the logs from the splunk scan and report feature
After going through the scan and report we have to search * for all logs and “`index=main "ERROR"`” to check for the error files

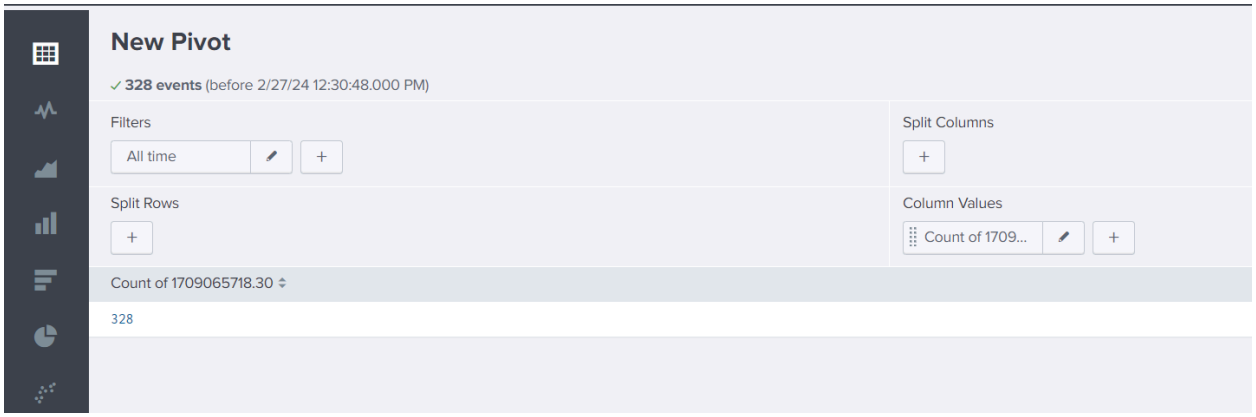






Using virtualization





New Search

```
index=main "ERROR"
```

✓ **328 events** (before 2/27/24 12:28:39.000 PM) No Event Sampling ▾

Events (328) **Patterns** Statistics Visualization

Smaller Larger

3 patterns based on a sample of 328 events

⚠ Less than 5,000 events may produce poor patterns. Try a search in a larger time range or with fewer constraints.

33.84% <timestamp>ERROR Backup failed due to insufficient disk space

33.23% <timestamp>ERROR User login failed

32.93% <timestamp>ERROR Service failed to start