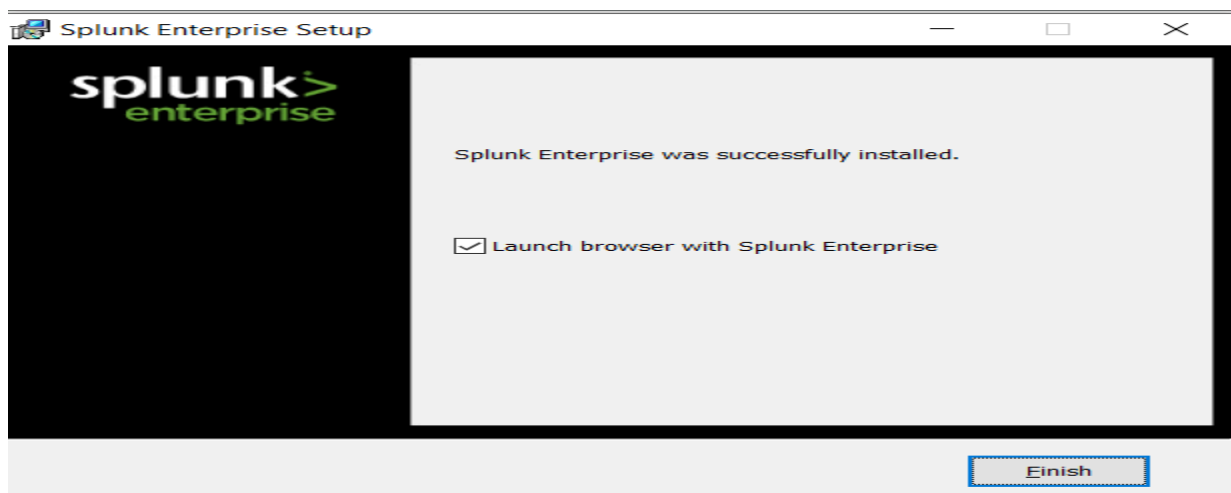
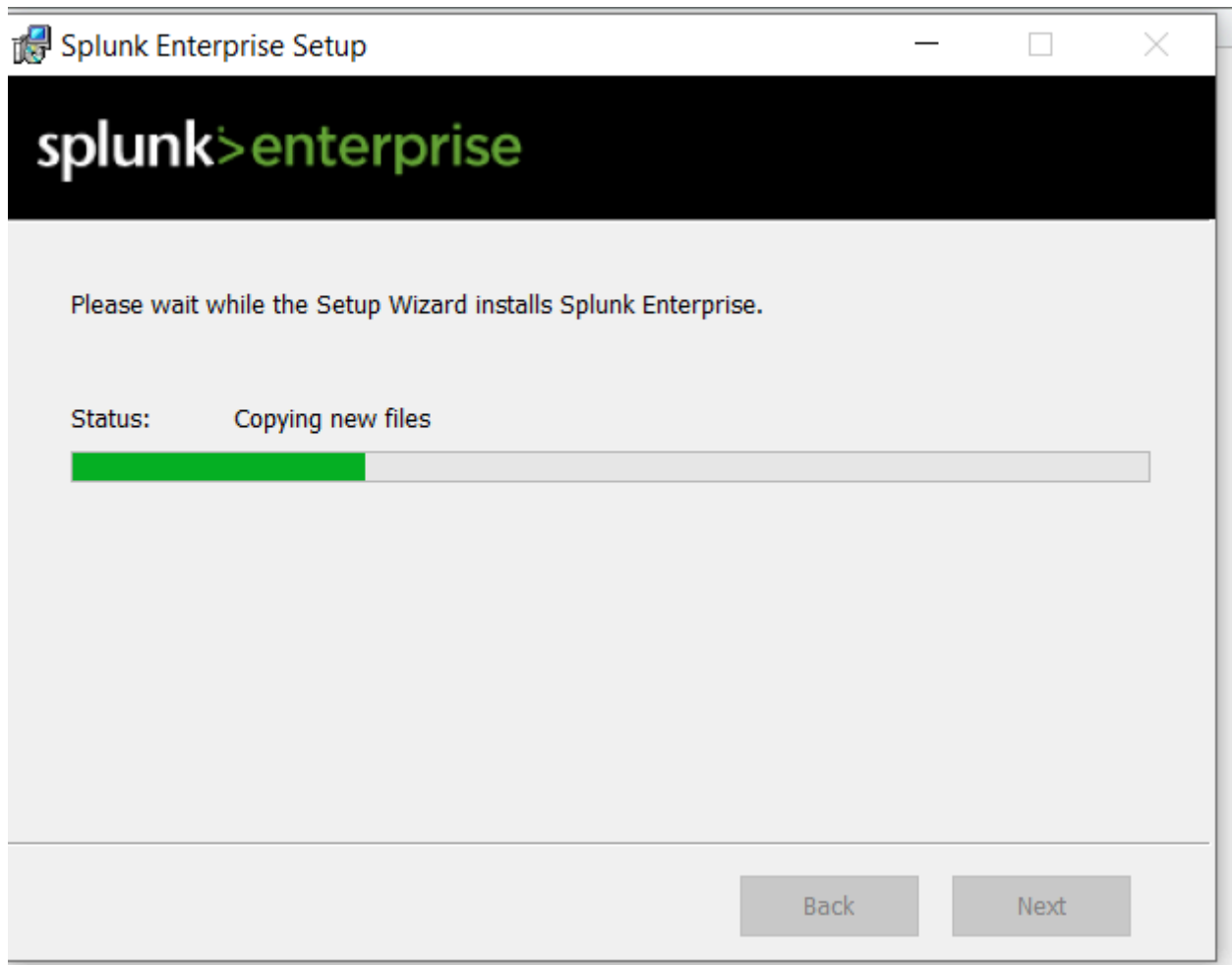


Splunk Introduction - Analysis of a Log

Installing splunk



Splunk interface

The screenshot shows the Splunk Enterprise interface. The top navigation bar includes the Splunk logo, 'splunk>enterprise', and a dropdown menu for 'Apps'. The main header area says 'Hello, Administrator' and includes tabs for 'Quick links', 'Dashboard', 'Recently viewed', 'Created by you', and 'Shared with you'. The left sidebar contains a search bar and a list of apps: 'Search & Reporting', 'Splunk Secure Gateway', and 'Upgrade Readiness App'. The main content area is divided into two sections: 'Common tasks' and 'Learning and resources'. The 'Common tasks' section includes cards for 'Add data', 'Search your data', 'Visualize your data', 'Add team members', 'Manage permissions', and 'Configure mobile devices'. The 'Learning and resources' section includes cards for 'Product tours', 'Learn more with Splunk Docs', 'Get help from Splunk experts', 'Extend your capabilities', 'Join the Splunk Community', and 'See how others use Splunk'.

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

The screenshot shows the 'Add Data' wizard in the Splunk interface. The progress bar indicates the current step is 'Set Source Type'. The 'Add Data' section shows a list of events from a source named 'system_log_example_1000.txt'. The events are displayed in a table with columns for 'Time' and 'Event'. The 'Set Source Type' section includes a 'Source type: default' dropdown and a 'Save As' button. The 'Review' section shows the input type as 'Uploaded File', the file name as 'system_log_example_1000.txt', the source type as 'sample', the host as 'DESKTOP-HV8PNVK', and the index as 'sample'.

| Time | Event |
|------------------------|--|
| 1/1/23 10:57:57.000 AM | 2023-01-01 10:57:57 ERROR User login failed |
| 1/1/23 1:42:58.000 PM | 2023-01-01 13:42:58 ERROR User login failed |
| 1/1/23 2:34:14.000 AM | 2023-01-01 02:34:14 WARN Service response time is slow |
| 1/1/23 9:16:49.000 AM | 2023-01-01 09:16:49 INFO Service started successfully |
| 1/1/23 3:54:07.000 PM | 2023-01-01 15:54:07 WARN User login attempt failed |
| 1/1/23 6:32:31.000 PM | 2023-01-01 18:32:31 INFO Service started successfully |
| 1/1/23 9:57:32.000 AM | 2023-01-01 09:57:32 INFO Service started successfully |
| 1/1/23 05:21:42 | 2023-01-01 05:21:42 WARN Disk usage exceeds 80% |

After going through the scan and report we have to search * for all logs and "index=main" "ERROR" to check for the error files

[illegible]

New Search

Save As Create Table View Close

indexmain "ERROR"

All time

Q

328 events (before 2/27/24 12:26:32.000 PM) No Event Sampling

Job II Smart Mode

Events (328) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect

1 hour per column

List Format 20 Per Page

Prev 1 2 3 4 5 6 7 8 Next

Hide Fields All Fields

SELECTED FIELDS

a host 1

a source 1

a sourcetype 1

INTERESTING FIELDS

date_hour 24

date_mday 1

date_minute 59

a date_month 1

date_second 59

a date_wday 1

a date_year 1

a date_zone 1

a index 1

linecount 1

a punct 3

a splunk_server 1

timeendpos 1

| i | Time | Event |
|---|------------------------|---|
| > | 1/1/23 11:59:42.000 PM | 2023-01-01 23:59:42 ERROR Backup failed due to insufficient disk space host = DESKTOP-HV8PNVK source = system_log_example_1000.txt sourcetype = demo |
| > | 1/1/23 11:58:34.000 PM | 2023-01-01 23:58:34 ERROR Backup failed due to insufficient disk space host = DESKTOP-HV8PNVK source = system_log_example_1000.txt sourcetype = demo |
| > | 1/1/23 11:56:49.000 PM | 2023-01-01 23:56:49 ERROR Backup failed due to insufficient disk space host = DESKTOP-HV8PNVK source = system_log_example_1000.txt sourcetype = demo |
| > | 1/1/23 11:55:43.000 PM | 2023-01-01 23:55:43 ERROR Service failed to start host = DESKTOP-HV8PNVK source = system_log_example_1000.txt sourcetype = demo |
| > | 1/1/23 11:40:04.000 PM | 2023-01-01 23:40:04 ERROR Backup failed due to insufficient disk space host = DESKTOP-HV8PNVK source = system_log_example_1000.txt sourcetype = demo |
| > | 1/1/23 11:38:30.000 PM | 2023-01-01 23:38:30 ERROR User login failed host = DESKTOP-HV8PNVK source = system_log_example_1000.txt sourcetype = demo |
| > | 1/1/23 11:38:13.000 PM | 2023-01-01 23:38:13 ERROR User login failed host = DESKTOP-HV8PNVK source = system_log_example_1000.txt sourcetype = demo |

Using virtualization

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

Job II Smart Mode

Events (328) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect

1 hour per column

Dec 31, 2022

14 events at 3 AM on Sunday, January 1, 2023

2 days

Jan 2, 2023

host

1 Value, 100% of events

Selected Yes No

Rare values

isk space

st sourcetype = demo

isk space

Hide Fields All Fields

SELECTED FIELDS

a host 1

a source 1

a sourcetype 1

Reports

Top values Top values by time

Events with this field

New Pivot

328 events (before 2/27/24 12:30:48.000 PM)

Filters

All time

+

Split Rows

+

Count of 1709065718.30

328

Split Columns

+

Column Values

Count of 1709...

+

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**