

You can checkout windows summary and get the brief description of the events and the log file which is been imported in splunk.

Here are the windows logs and files

The screenshot displays the Splunk Enterprise search interface. The top navigation bar includes 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. The 'Search & Reporting' section is active, showing a 'New Search' page. The search bar contains the query: `source="wIndows_event_log_example_fixed.xml" host="DESKTOP-HV8PNVK" index="windows" sourcetype="windows"`. The results show 202 events (before 2/27/24 2:43:25.000 PM). The table view displays three events with their respective timestamps and XML data. The second query shows 303 events (before 2/27/24 2:50:34.000 PM) with a similar table view showing three events.

i	Time	Event
>	2/27/24 2:43:22.000 PM	<?xml version="1.0" ?> <Events> <Event> host = DESKTOP-HV8PNVK source = windows_event_log_example_fixed.xml sourcetype = windows
>	2/27/24 2:42:13.000 PM	<?xml version="1.0" ?> <Events> <Event> host = DESKTOP-HV8PNVK source = windows_event_log_example_fixed.xml sourcetype = Windows
>	2/25/24 5:50:08.000 PM	<DateandTime>2024-02-25 17:50:08</DateandTime> <Source>Application</Source> <EventID>1886</EventID> <TaskCategory>Configuration</TaskCategory> <Level>Error</Level>

i	Time	Event
>	2/27/24 2:50:27.000 PM	<?xml version="1.0" ?> <Events> <Event> host = DESKTOP-HV8PNVK source = windows_event_log_example_fixed.xml sourcetype = windows
>	2/27/24 2:43:22.000 PM	<?xml version="1.0" ?> <Events> <Event> host = DESKTOP-HV8PNVK source = windows_event_log_example_fixed.xml sourcetype = windows
>	2/27/24 2:42:13.000 PM	<?xml version="1.0" ?> <Events> <Event> host = DESKTOP-HV8PNVK source = windows_event_log_example_fixed.xml sourcetype = Windows
>	2/25/24 5:50:08.000 PM	<DateandTime>2024-02-25 17:50:08</DateandTime> <Source>Application</Source> <EventID>1886</EventID> <TaskCategory>Configuration</TaskCategory> <Level>Error</Level>

There are all total 303 events in the field and it can be made easily understandable to read in the table view.

This process shows the advance findings and searchable queries to find the new events.

New Search

index="windows" | streamstats count as EventCount by Source

✓ 303 events (2/1/24 12:00:00.000 AM to 3/1/24 12:00:00.000 AM) No Event Sampling ▾

Events (303) Patterns Statistics Visualization

Smaller  Larger

4 patterns based on a sample of 303 events

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

21.78%	<DateandTime><timestamp></DateandTime> <Source>System</Source> <EventID>1888</EventID> <TaskCategory>Startup/Shutdown</TaskCategory> <Level>Warning</Level> <Description>User login failed due to incorrect credentials.</Description> </Event> <Event>
20.79%	<DateandTime><timestamp></DateandTime> <Source>Security</Source> <EventID>1498</EventID> <TaskCategory>Startup/Shutdown</TaskCategory> <Level>Warning</Level> <Description>The system has successfully booted.</Description> </Event> <Event>
18.81%	<DateandTime><timestamp></DateandTime> <Source>System</Source> <EventID>1503</EventID> <TaskCategory>Startup/Shutdown</TaskCategory> <Level>Error</Level> <Description>Configuration settings were changed.</Description> </Event> <Event>
18.81%	<DateandTime><timestamp></DateandTime> <Source>System</Source> <EventID>1503</EventID> <TaskCategory>Performance</TaskCategory> <Level>Error</Level> <Description>Application error occurred.</Description> </Event> <Event>