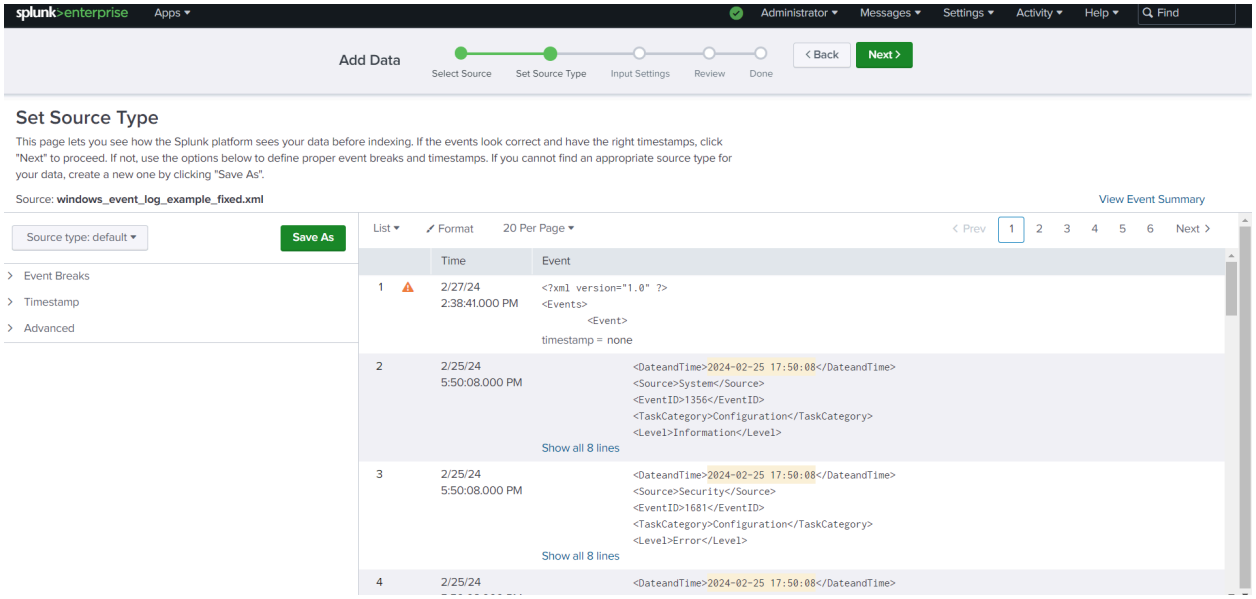
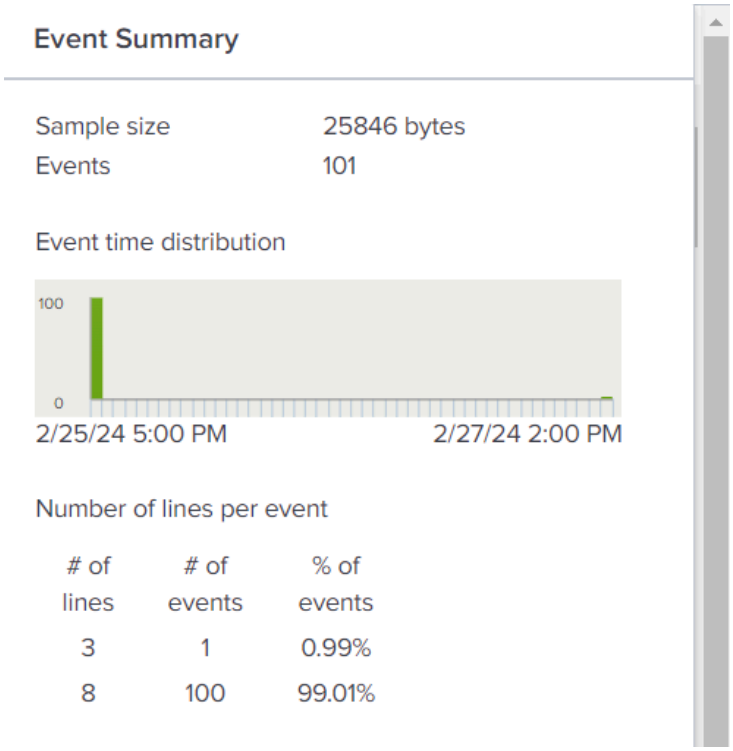
Splunk Analysis Assignment: Windows Event Log Investigation

Adding the windows log xml file

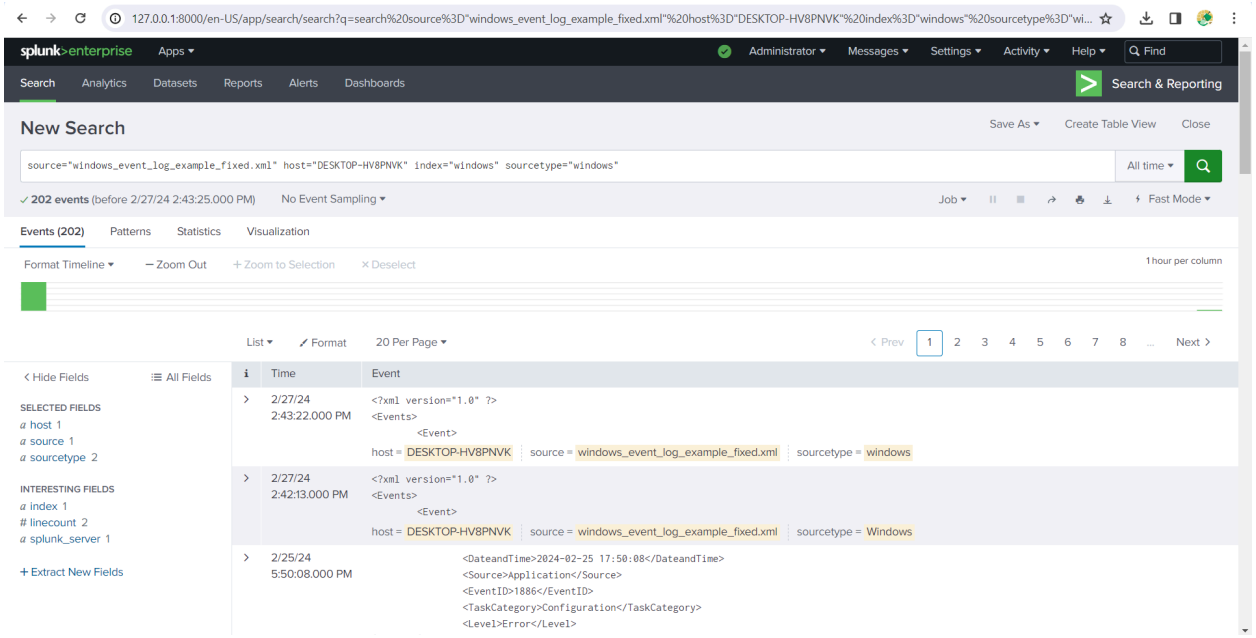


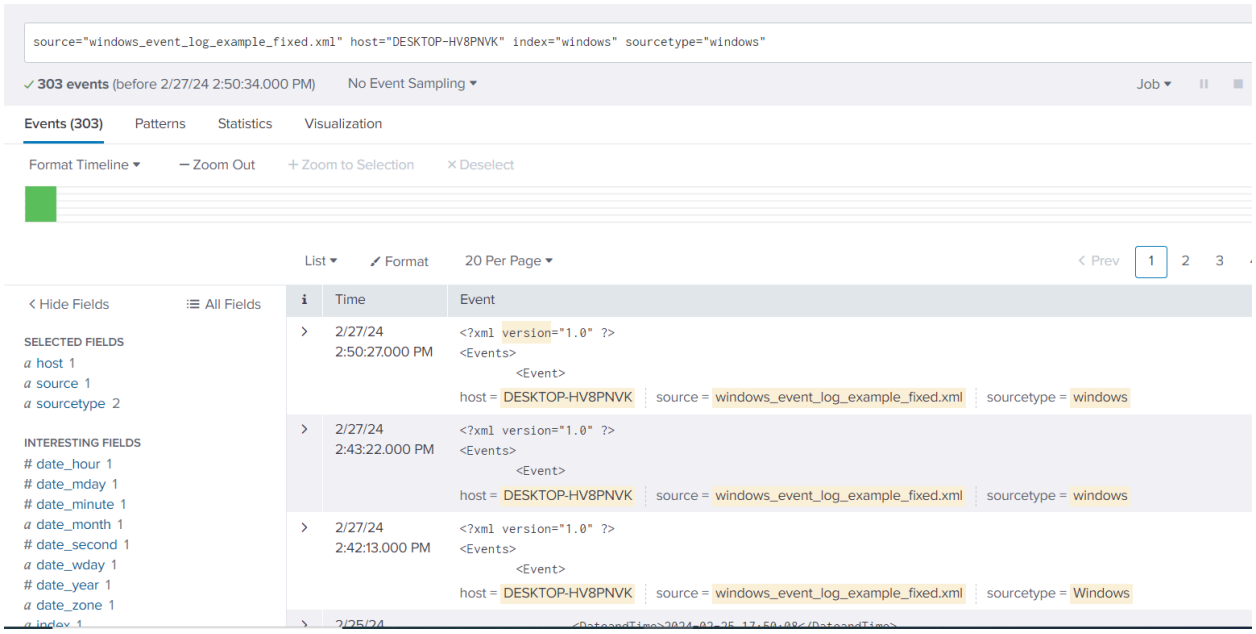
Event summary:-



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

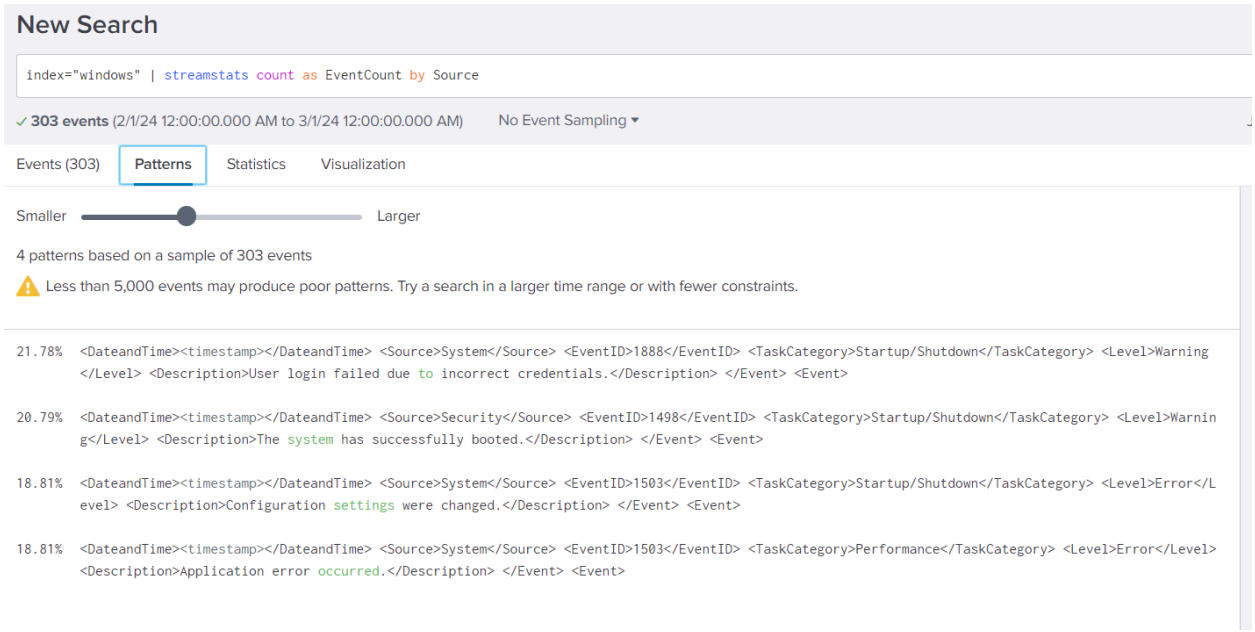
Here are the windows logs and files





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>Warnin
g</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</L
evel> <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>