Error and failure events on a host

While metrics help you isolate which hosts are having problems and when those problems began, logs and events generally contain information needed to get to the true cause of the issue. You want to use Splunk to isolate logs and events coming from the host and look for any common indicators of trouble such as “error” or “failed”.

Data required

System log data

Procedure

1. Run the following search. You can optimize it by specifying an index and adjusting the time range.

   host=* sourcetype=* (error OR fail*)

Search explanation

The table provides an explanation of what each part of this search achieves. You can adjust this query based on the specifics of your environment.

<table>
<thead>
<tr>
<th>Splunk Search</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>host=*</td>
<td>Search any host in your deployment.</td>
</tr>
<tr>
<td>sourcetype=* (error OR fail*)</td>
<td>Search any source type in your deployment.</td>
</tr>
<tr>
<td>(error OR fail*)</td>
<td>Search for error or failure events.</td>
</tr>
</tbody>
</table>

Next steps

These search results give you easy and quick visibility into which hosts and data sources you need to investigate.

You might be interested in other processes associated with the Recovering lost visibility of IT infrastructure use case.