All logs and events on a *nix host

The log files and events collected from a Linux host provide valuable information that can be used during an investigation to facilitate answering questions about the hosts behavior, state, health, or performance. You want to be able to see all logs and event on a particular host.

Data required

*nix operating system logs

Procedure

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

```
host="<name of host to check>" source="<name of source to check>"
<optional keywords>
```

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><code>host=&quot;&lt;name of host to check&gt;&quot; source=&quot;&lt;name of</code>&lt;br&gt;<code>source to check&gt;&quot;</code></td>
<td>Enter the name of the host and source you want to examine. You can also search <code>source=*</code> to search all logs on the host.</td>
</tr>
<tr>
<td><code>&lt;optional keywords&gt;</code></td>
<td>Use keywords to narrow the search results if you are searching for specific, known events or logs. For instance adding &quot;start&quot; &quot;service&quot; to the search might help uncover instances where a service was started on the host.</td>
</tr>
</tbody>
</table>

Next steps

Use the results to facilitate answering questions about the host’s behavior, state, health, or performance.

You might be interested in other processes associated with the [Maintaining *nix systems](#) use case.

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.