Investigating user login issues

Your help desk has been taking calls from users unable to log in. Several analysts on an incident bridge have been investigating for the last few hours, but nobody seems to be sure what is causing the problem. As an analyst, you need to find the root cause of the problem, and work out who to refer the issue to next.

How to use Splunk software for this use case

Ensure you're collecting enough data to ensure you can troubleshoot across all of your systems. By collecting, retaining, and searching all data, Splunk provides complete visibility across time, allowing operations teams to answer fundamental questions about system behavior and more.

1. From the default Splunk home screen, click **Search & Reporting**.
2. Run a search with the following criteria:
   1. Select the timeframe you want to search within, for example, the last 4 hours. You can optimize it further by specifying an index.
   2. Search for keywords that you might expect to see within the data during an incident or outage. Search for single keywords or broaden the search more by adding the boolean expression OR into the search. You can also use a wildcard character to search for any keyword that starts with fail, such as failed, failing, failure. If a problem is occurring in the environment, you might expect to see a lot of these types of events. An example search could be:

```
crash OR error OR fail* OR critical
```

3. Run the search and check the events that return. Use the histogram to spot trends and outliers and pinpoint when the problem started. You can click on a green bar to see more information about the timeframe and events occurring at that time. Now you can focus your investigation around a short window of time.

4. Check fields of interest on the left side of the screen using the fields sidebar, which lists every field found within the data. Clicking on each field helps to answer additional questions you might ask during an investigation. Some fields you might want to investigate include:
   1. Click **hosts** to find out which hosts are currently reporting errors and appear to be affected.
   2. Click **sourcetype** to check the status of every piece of technology in the environment, for example, web servers, database servers, or the network.
3. Focus your investigation. Since users were complaining about inability to authenticate, you could focus the investigation down to the authentication servers. You can do this by clicking on the first auth server displayed within sourcetype. You'll notice that Splunk automatically adds a field/value filter to the search, and from there you can then add a wildcard character to look across all auth servers. Your search should look like this:

```
crash OR error OR fail* OR critical host="auth-x**"
```

5. Look through the data on the auth servers to locate trends or correlations that reveal root cause. For example, if every error in the webserver is correlated to a stacktrace error in the java code, you can expand the stacktrack event to see that it indicates that the call to the database failed. That indicates to you that the database team should be contacted to help you troubleshoot further.

**Next steps**

Once you've found the source of the problem, you may want to re-run the search using a longer timeframe, for example, the year to date. This allows you to determine when a problem was first introduced into the environment and find out how long a problem has been going on for. You could also focus in on a specific date and time range to see what might have occurred in the environment at some specific and important point in time, such as right after a system patching event.

These additional Splunk resources might help you understand and implement these recommendations:

- Blog: [A fast lane to value: Introducing IT Essentials Apps](#)
- Blog: [IT Essentials Work: A centralized app for all things IT Ops](#)
- Tech Talk: [IT Essentials Learn](#)
- Tech Talk: [IT Essentials Work](#)