

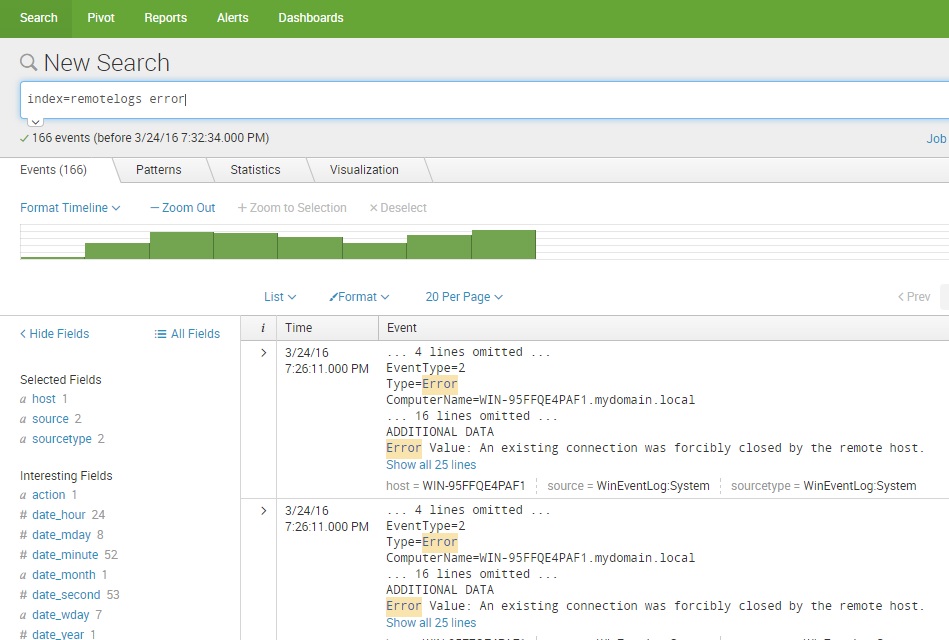
Schedule Alert- Like system is checking heartbeat, if it fails it will retry for next 10 minutes. If all fails then we will receive alert.

Realtime- continuously checking system.

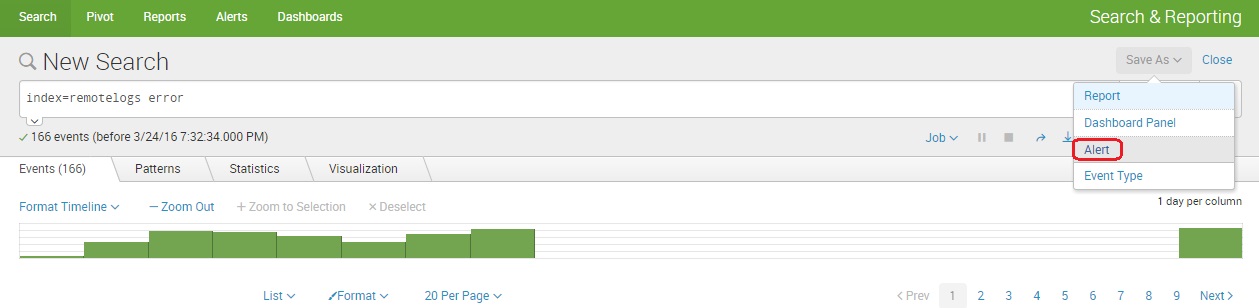
Dashboard- Set of runtime data showing on a webpage.

ou can create an alert from the most searches you run in **Splunk Web**. In this chapter we will show you how to create an alert that will be triggered if the number of search results is greater than 100.

First, we need to run our search:

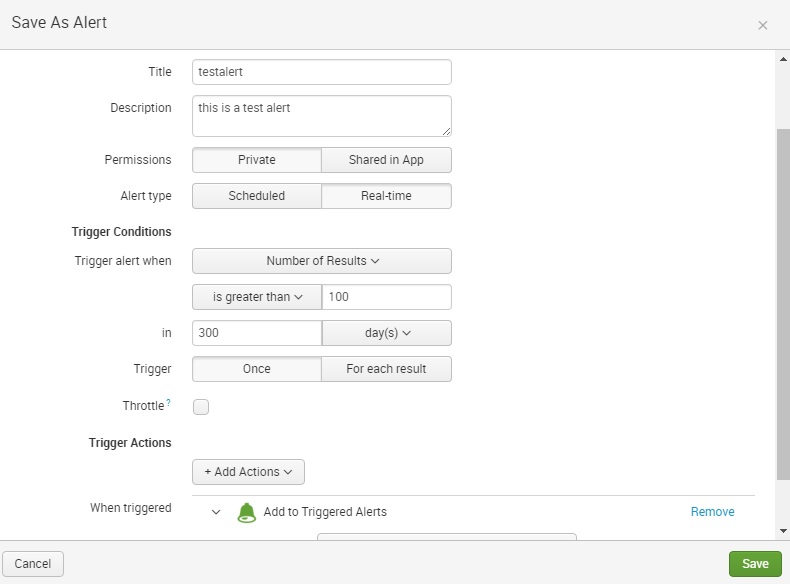
[](https://geek-university.com/wp-content/uploads/2016/03/splunk_search_for_an_alert.jpg)

Next, go to **Save As > Alert**:

[](https://geek-university.com/wp-content/uploads/2016/03/save_alert.jpg)

The **Save As Alert** dialog window opens. We need to define the following parameters:

* **Title** – the name of the alert.
* **Description** – the alert description.
* **Permissions** – select whether the alert will be private or shared with all other users of the app.
* **Alert type** – select whether you wish to schedule your alert to run when scheduled or in real-time.
* **Trigger alert when** – set the alarm trigger condition. In our example, we will trigger an alert when the number of search results during 300 days exceeds 100.
* **Trigger** – select whether you would like to trigger the alarm once or for each result.
* **Throttle** – select the throttle period during which alerts will not be triggered.
* **Triggered actions** – select the action that will be performed if the alarm is triggered. We’ve chosen to add an event to the **Triggered Alerts** page.

[](https://geek-university.com/wp-content/uploads/2016/03/save_as_alert.jpg)

And that’s it! If the number of search results during 300 days exceeds 100, an event will be displayed in the **Triggered Alerts** page.