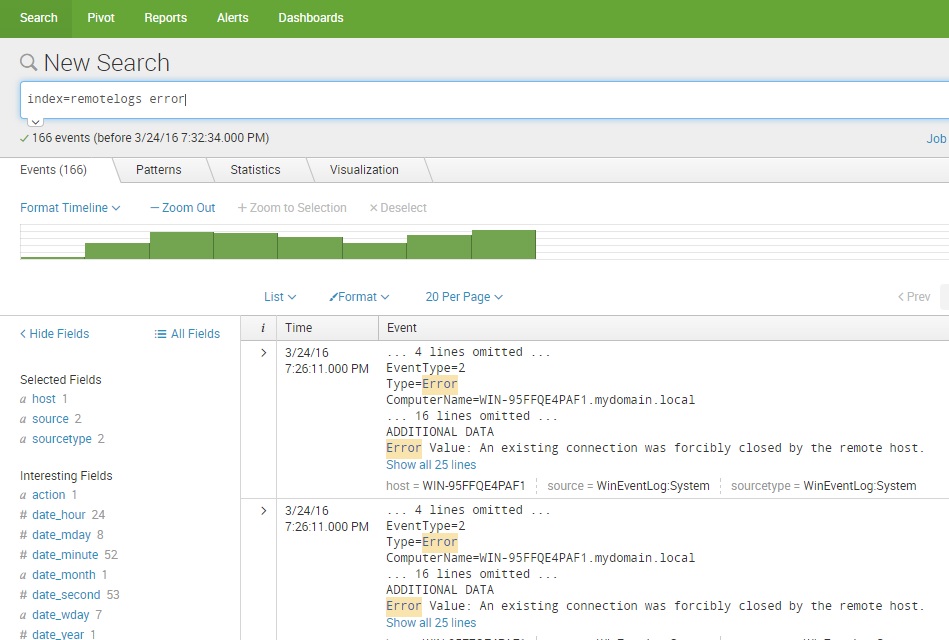
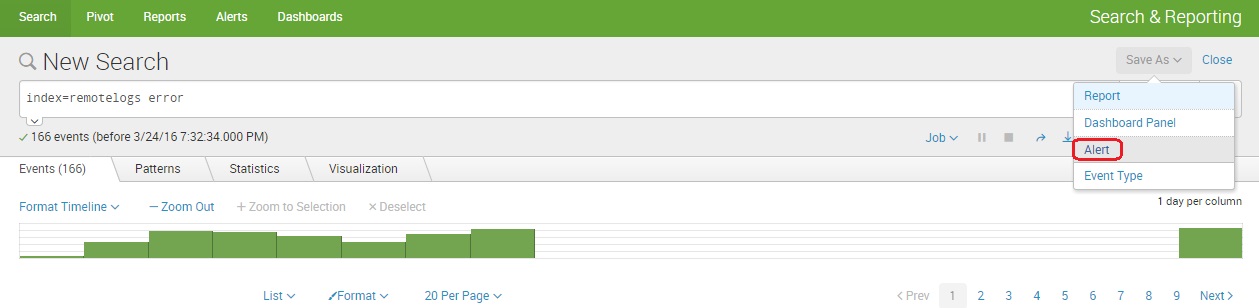
You can create an alert from any searches you run in **Splunk Web**. The searches can be as complex or simple as you can create, can inject visualizations, tables or \_raw data directly to your outputted desire. These searches can be scheduled on a CRON or standard timing interval.   
  
In this example 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:

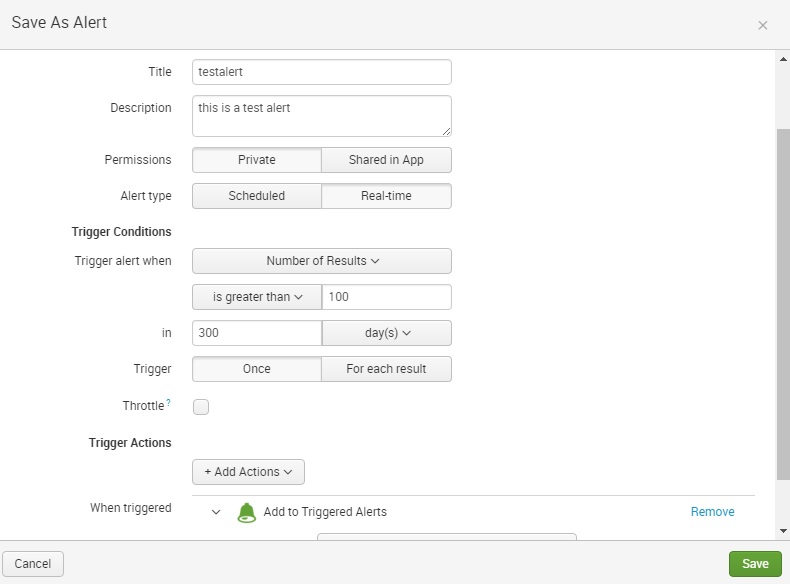
[](https://geek-university.com/wp-content/uploads/2016/03/splunk_search_for_an_alert.jpg)

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.  
  
Another option for Triggered Actions is to **Send Email**, for this we need to define the following parameters:

* **To** – the email of the recipient.
* **Priority** – speed at which the request is processed.
* **Subject** – Subject line of the email (A ‘$’ symbol is what splunk uses to identify a veriable, all fields listed in the edit alert or results.[field] can be called by this method)
* **Message** – Body of the email, this can contain veriables and HTML input as well
* **Include** – any of these checkboxes will add additional information to the email including attachments or results from the queryGraphical user interface, text, application

  Description automatically generated

To create a ticket in **Service Now**, the Splunk to SNOW App can be used to inject field data into a custom table. This will be flagged more in depth in the How to use Splunk to SNOW document, The following are screenshots of a successfully configured alert

Graphical user interface, application

Description automatically generated

Graphical user interface, application

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated