**Splunk - Event Types**

In Splunk search, we can design our own events from a dataset based on certain criteria. For example, we search for only the events which have a http status code of 200. This event now can be saved as an event type with a user defined name as **status200** and use this event name as part of future searches.

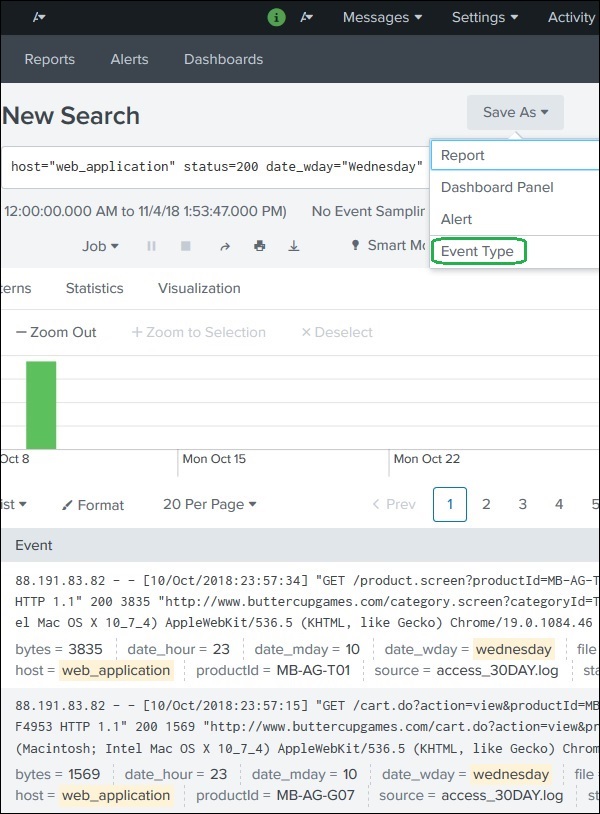
In short, an event type represents a search that returns a specific type of event or a useful collection of events. Every event that can be returned by the search gets an association with that event type.

Creating Event Type

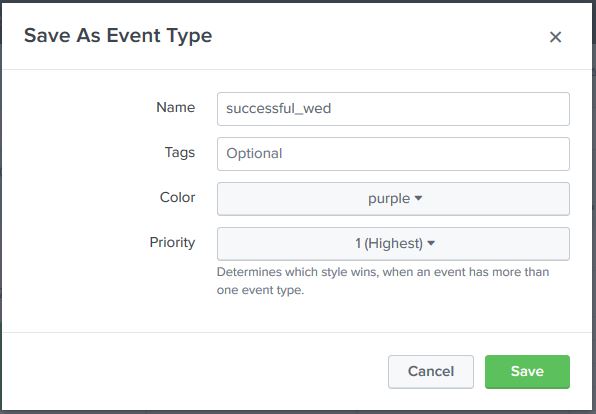
There are two ways to create an event type after we have decided the search criteria. One is to **run** a search and then save it as an Event Type. Another is to **add a new Event Type from the settings tab**. We will see both the ways of creating it in this section.

Using a Search

Consider the search for the events which have the criteria of successful http status value of 200 and the event type run on a Wednesday. After running the search query, we can choose **Save As** option to save the query as an Event Type.



The next screen prompts to give a name for the Event Type, choose a Tag which is optional and then choose a colour with which the events will be highlighted. The priority option decides which event type will be displayed first in case two or more event types match the same event.

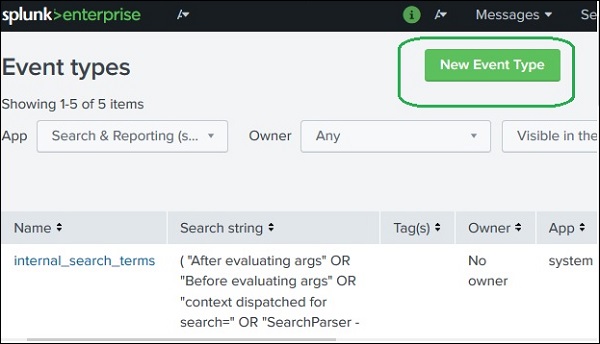


Finally, we can see the Event Type has been created by going to the **Settings → Event Types** option.

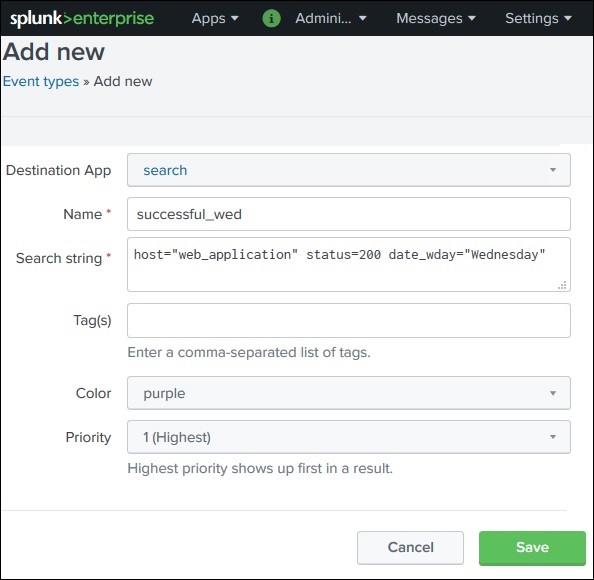
Ezoic

Using New Event Type

The other option to create a new Event Type is to use the **Settings → Event Types** option as shown below where we can add a new Event Type −



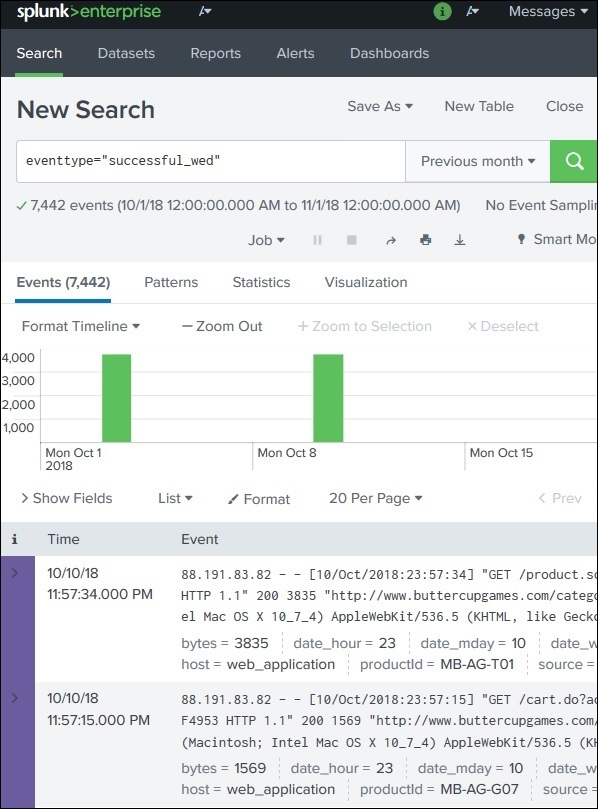
On clicking the button **New Event Type** we get the following screen to add the same query as in the previous section.



[Explore our](https://www.tutorialspoint.com/latest/courses?utm_source=tutorialspoint&utm_medium=tutorials_3p&utm_campaign=internal" \t "_blank)**[latest online courses](https://www.tutorialspoint.com/latest/courses?utm_source=tutorialspoint&utm_medium=tutorials_3p&utm_campaign=internal" \t "_blank)**[and learn new skills at your own pace. Enroll and become a certified expert to boost your career.](https://www.tutorialspoint.com/latest/courses?utm_source=tutorialspoint&utm_medium=tutorials_3p&utm_campaign=internal" \t "_blank)

Viewing the Event Type

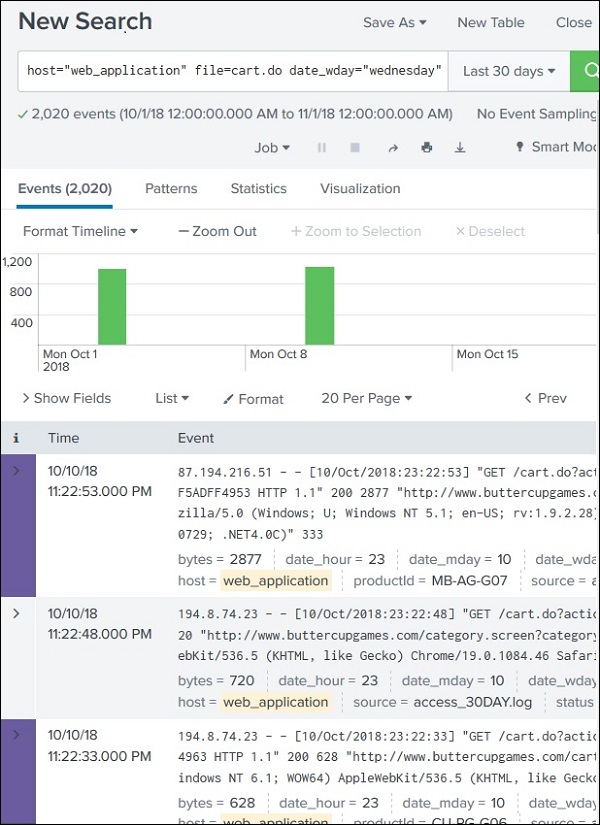
To view the event we just created above, we can write the below search query in the search box and we can see the resulting events along with the colour we have chosen for the event type.



Ezoic

Using the Event Type

We can use the Event type along with other queries. Here we specify some partial criteria from the Event Type and the result is a mix of events which shows the coloured and non-coloured events in the result.



Print Page