

# Metrics, Dashboards and Alerts in Splunk

Indexing application log

The screenshot shows the Splunk Search interface. The search bar contains the query: `source="/Users/ciscodelgado/code/training/udacity/e-commerce/logs/activity.log" host="localhost" index="ecommerce" sourcetype="log4j"`. The results show 32 events. The left sidebar shows the search fields and the event list. The event list shows the following data:

Time	Event
2021-02-28 19:41:03.064	[http-nio-8888-exec-4] c.e.demo.controllers.UserController : User "leonard" created successfully host = localhost level = INFO log_message = User "leonard" created successfully source = /Users/ciscodelgado/code/training/udacity/e-commerce/logs/activity.log sourcetype = log4j
2021-02-28 19:41:03.076	[http-nio-8888-exec-4] c.e.demo.controllers.UserController : User name set with "leonard" host = localhost level = INFO log_message = User name set with "leonard" source = /Users/ciscodelgado/code/training/udacity/e-commerce/logs/activity.log sourcetype = log4j
2021-02-28 19:40:43.160	[http-nio-8888-exec-3] c.e.demo.controllers.UserController : User "sheldon" created successfully host = localhost level = INFO log_message = User "sheldon" created successfully source = /Users/ciscodelgado/code/training/udacity/e-commerce/logs/activity.log sourcetype = log4j
2021-02-28 19:40:43.034	[http-nio-8888-exec-3] c.e.demo.controllers.UserController : User name set with "sheldon" host = localhost level = INFO log_message = User name set with "sheldon" source = /Users/ciscodelgado/code/training/udacity/e-commerce/logs/activity.log sourcetype = log4j
2021-02-28 19:40:26.073	[http-nio-8888-exec-2] c.e.demo.controllers.UserController : User "homer" created successfully host = localhost level = INFO log_message = User "homer" created successfully source = /Users/ciscodelgado/code/training/udacity/e-commerce/logs/activity.log sourcetype = log4j
2021-02-28 19:40:25.934	[http-nio-8888-exec-2] c.e.demo.controllers.UserController : User name set with "homer" host = localhost level = INFO log_message = User name set with "homer" source = /Users/ciscodelgado/code/training/udacity/e-commerce/logs/activity.log sourcetype = log4j
2021-02-28 19:40:25.872	[http-nio-8888-exec-2] o.s.web.servlet.DispatcherServlet : Completed initialization in 6 ms host = localhost level = INFO log_message = Completed initialization in 6 ms source = /Users/ciscodelgado/code/training/udacity/e-commerce/logs/activity.log sourcetype = log4j
2021-02-28 19:40:25.866	[http-nio-8888-exec-2] o.s.web.servlet.DispatcherServlet : Initializing Servlet 'dispatcherServlet' host = localhost level = INFO log_message = Initializing Servlet 'dispatcherServlet' source = /Users/ciscodelgado/code/training/udacity/e-commerce/logs/activity.log sourcetype = log4j
2021-02-28 19:40:25.866	[http-nio-8888-exec-2] o.a.c.c.[Tomcat].[localhost].[/] : Initializing Spring DispatcherServlet 'dispatcherServlet' host = localhost level = INFO log_message = Initializing Spring DispatcherServlet 'dispatcherServlet' source = /Users/ciscodelgado/code/training/udacity/e-commerce/logs/activity.log sourcetype = log4j

## Searching

The screenshot shows the Splunk Search interface with a refined search. The search bar contains the query: `source="/Users/ciscodelgado/code/training/udacity/e-commerce/logs/activity.log" host="localhost" index="ecommerce" sourcetype="log4j" level="INFO" | regex log_message = "User \"[a-z]+\" created successfully"`. The results show 3 events. The left sidebar shows the search fields and the event list. The event list shows the following data:

Time	Event
2021-02-28 19:41:03.064	[http-nio-8888-exec-4] c.e.demo.controllers.UserController : User "leonard" created successfully host = localhost level = INFO log_message = User "leonard" created successfully source = /Users/ciscodelgado/code/training/udacity/e-commerce/logs/activity.log sourcetype = log4j
2021-02-28 19:40:43.160	[http-nio-8888-exec-3] c.e.demo.controllers.UserController : User "sheldon" created successfully host = localhost level = INFO log_message = User "sheldon" created successfully source = /Users/ciscodelgado/code/training/udacity/e-commerce/logs/activity.log sourcetype = log4j
2021-02-28 19:40:26.073	[http-nio-8888-exec-2] c.e.demo.controllers.UserController : User "homer" created successfully host = localhost level = INFO log_message = User "homer" created successfully source = /Users/ciscodelgado/code/training/udacity/e-commerce/logs/activity.log sourcetype = log4j

# Create alert from search

The screenshot shows the Splunk Search interface. The search bar contains the query: `source="/Users/ciscodlgado/code/training/udacity/e-commerce/logs/activity.log" host="localhost" index="ecommerce" sourcetype="log4j" level="INFO" | search log_message = "Order submitted successfully"`. The search results show 2 events from 27/02/2021 21:00:00.000 to 28/02/2021 21:06:41.000. The events are listed in a table with columns: Time, Event, and Source. The first event is from 28/02/2021 21:01:18.199, and the second is from 28/02/2021 20:57:07.337. Both events are from the source `/Users/ciscodlgado/code/training/udacity/e-commerce/logs/activity.log` and have a sourcetype of `log4j`. The log message for both is `Order submitted successfully`.

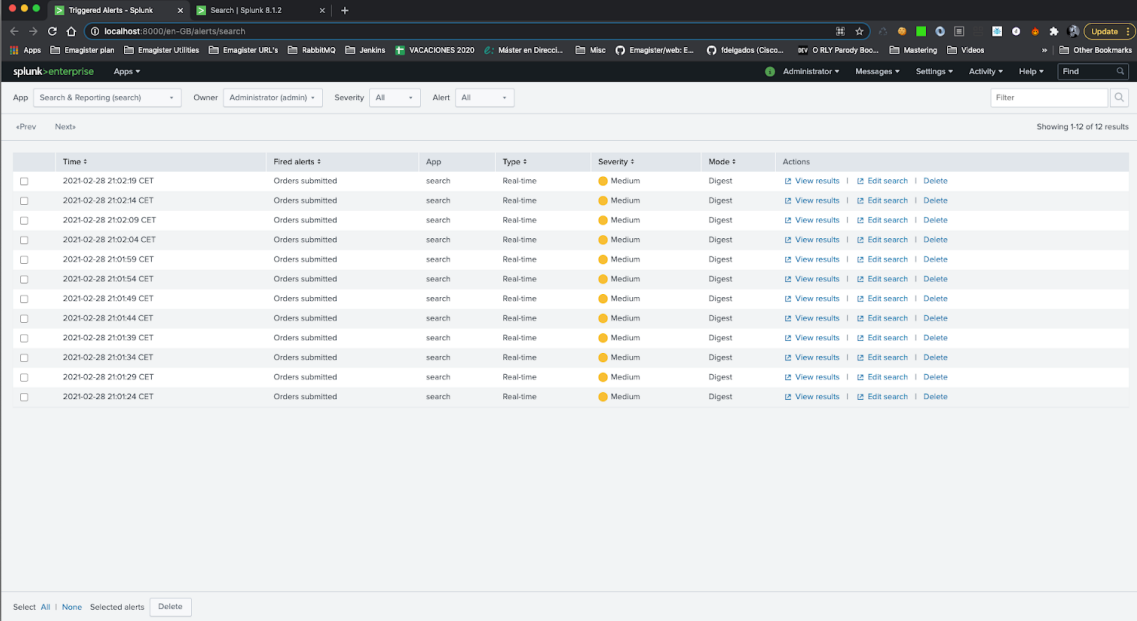
Time	Event	Source
28/02/2021 21:01:18.199	[http-nio-8888-exec-1] c.a.demo.controllers.OrderController : Order submitted successfully host = localhost level = INFO log_message = Order submitted successfully source = /Users/ciscodlgado/code/training/udacity/e-commerce/logs/activity.log sourcetype = log4j	/Users/ciscodlgado/code/training/udacity/e-commerce/logs/activity.log
28/02/2021 20:57:07.337	[http-nio-8888-exec-8] c.a.demo.controllers.OrderController : Order submitted successfully host = localhost level = INFO log_message = Order submitted successfully source = /Users/ciscodlgado/code/training/udacity/e-commerce/logs/activity.log sourcetype = log4j	/Users/ciscodlgado/code/training/udacity/e-commerce/logs/activity.log

The screenshot shows the Splunk Search interface with the 'Save As Alert' dialog box open. The dialog box has the following settings:

- Title:** Orders submitted
- Description:** Optional
- Permissions:** Private
- Alert type:** Real-time
- Expires:** 24 hours(s)
- Trigger Conditions:**
  - Trigger alert when: Number of Results
  - is greater than: 1
  - in: 1 minute(s)
  - Trigger: Once
- Trigger Actions:**
  - Send email
  - Add to Triggered Alerts

The 'Save' button is highlighted in green.

# Triggered alerts



The screenshot shows the Splunk Enterprise web interface. At the top, there's a navigation bar with 'splunk>enterprise' and various menu items like 'Apps', 'Search & Reporting', 'Alerts', etc. Below the navigation bar, there's a search bar and a filter section. The main content area displays a table of triggered alerts. The table has columns for 'Time', 'Fired alerts', 'App', 'Type', 'Severity', 'Mode', and 'Actions'. There are 12 rows of data, all showing 'Orders submitted' as the fired alert, 'search' as the app, 'Real-time' as the type, 'Medium' as the severity, and 'Digest' as the mode. Each row has a checkbox on the left and a set of links (View results, Edit search, Delete) in the Actions column. At the bottom of the table, there's a 'Select' button and a 'Delete' button.

	Time	Fired alerts	App	Type	Severity	Mode	Actions
<input type="checkbox"/>	2021-02-28 21:02:19 CET	Orders submitted	search	Real-time	Medium	Digest	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
<input type="checkbox"/>	2021-02-28 21:02:14 CET	Orders submitted	search	Real-time	Medium	Digest	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
<input type="checkbox"/>	2021-02-28 21:02:09 CET	Orders submitted	search	Real-time	Medium	Digest	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
<input type="checkbox"/>	2021-02-28 21:02:04 CET	Orders submitted	search	Real-time	Medium	Digest	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
<input type="checkbox"/>	2021-02-28 21:01:59 CET	Orders submitted	search	Real-time	Medium	Digest	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
<input type="checkbox"/>	2021-02-28 21:01:54 CET	Orders submitted	search	Real-time	Medium	Digest	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
<input type="checkbox"/>	2021-02-28 21:01:49 CET	Orders submitted	search	Real-time	Medium	Digest	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
<input type="checkbox"/>	2021-02-28 21:01:44 CET	Orders submitted	search	Real-time	Medium	Digest	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
<input type="checkbox"/>	2021-02-28 21:01:39 CET	Orders submitted	search	Real-time	Medium	Digest	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
<input type="checkbox"/>	2021-02-28 21:01:34 CET	Orders submitted	search	Real-time	Medium	Digest	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
<input type="checkbox"/>	2021-02-28 21:01:29 CET	Orders submitted	search	Real-time	Medium	Digest	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
<input type="checkbox"/>	2021-02-28 21:01:24 CET	Orders submitted	search	Real-time	Medium	Digest	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>

Select All | None Selected alerts [Delete](#)