GLAB 200.4.1 - Using Fields

Version 1.0, June 2023

Introduction

In this lab, you will enroll in the Using Fields (eLearning with labs) Splunk course and use the Splunk lab to practice.

The Splunk labs simulate an (imaginary) international video game company called Buttercup Games. The lab environment has several indexes and plenty of real-world-like data to play with.

Note: You must only complete **Lab Exercise 1 – Use Fields in Searches** on the Splunk lab.

Before You Begin - How to Submit This Activity

IMPORTANT: At the end of Lab Exercise 1 – Use Fields in Searches, you will be instructed to save your searches as **reports** with names such as **L1S1**.

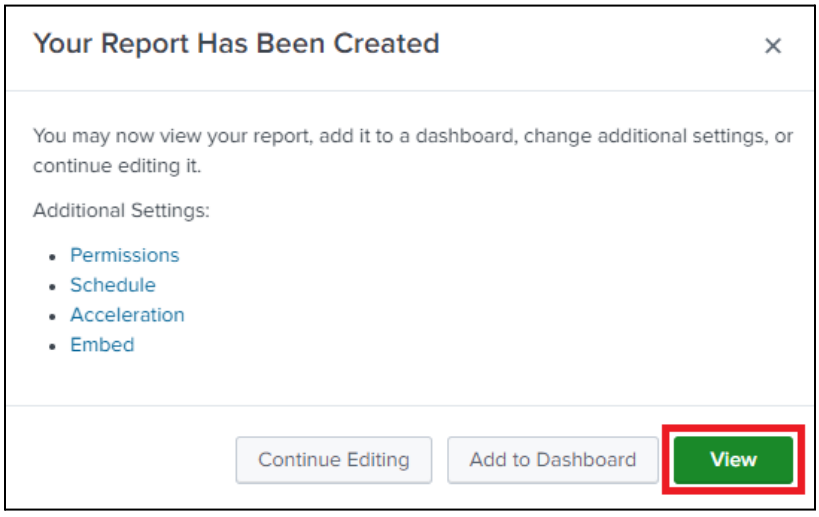
Once you have saved that report(s), you can export it in a **PDF** format. The Splunk lab instructions do not explain exporting a report, so we will explain the process here.

Once you have **exported your report(s)** in **PDF** format, you have to **upload** them to **Canvas**. The report(s) you submit is what we expect to receive, and are evidence of your lab completion.

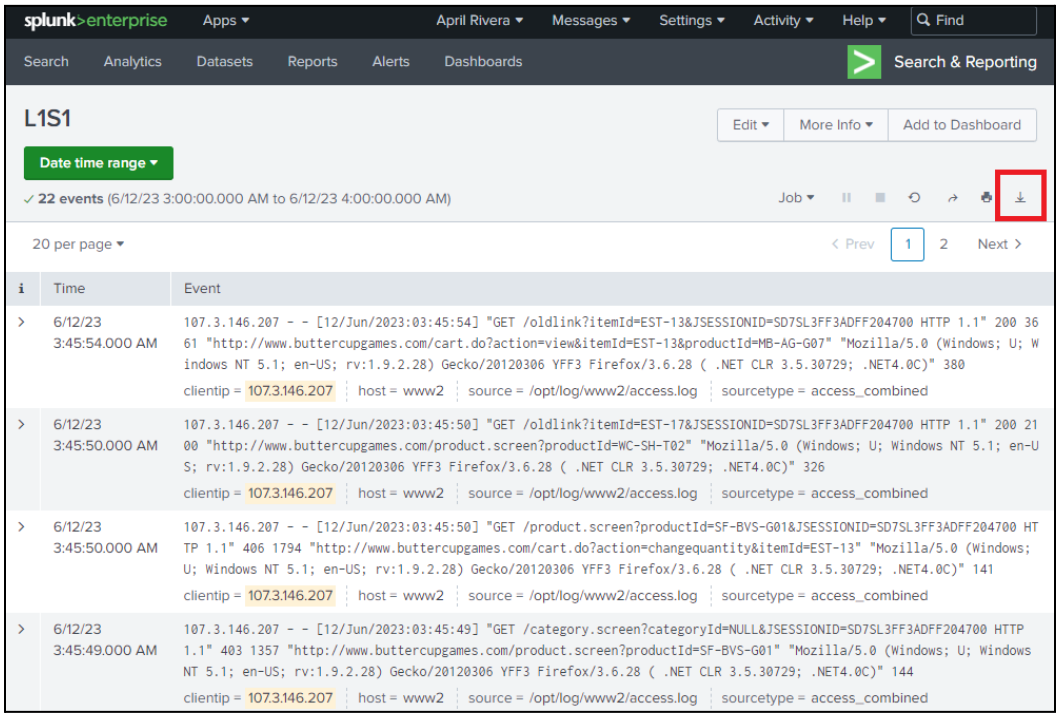
Exporting a Report from Splunk in PDF format.

NOTE: Do this step for every report you are instructed to save and report in the Splunk lab.

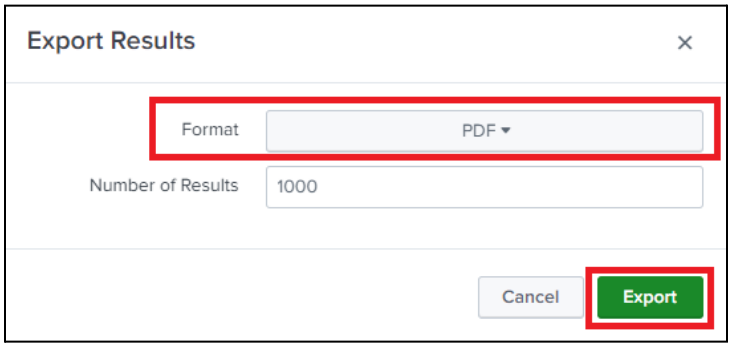
a. *After saving a report in Splunk, you can choose to view the report. Click the **View** button on the **Your Report Has Been Created** notification window.*



b. *When viewing the report, click the **Down pointing arrow** on the left-hand side to select an **export** option.*



c. *On the **Export Results** dialog box, set the **Format** to **PDF using the drop-down menu** and click on the **Export** button.*



d. *The report in **PDF format** will download to your computer. The file name will be the **report's name, followed by a timestamp**.*

e. *Upload the report to Canvas using the assignment's **Submit** button.*

Objectives

- Enroll in the Using Fields (eLearning with labs) Splunk course.
- Complete Lab Exercise 1 – Use Fields in Searches.

Equipment

- A laptop or PC with Internet connectivity or A Windows Virtual Machine with Internet connectivity.

- A splunk.com/perscholas account - previously created on ACT 200.1.1: Access Splunk learning resources.

Instructions

Part 1: Enroll in the Using Fields (eLearning with labs) Splunk course and launch the Server.

In this part, we assume that you have a splunk.com/perscholas account. If you do not have one, please complete the ACT 200.1.1: Access Splunk learning resources activity first.

Step 1: Enroll in the Using Fields (eLearning with labs) Splunk course.

If you need screenshots of the steps to enroll, see the instructions on the GLAB 200.2.1 - Splunk Fundamentals lab.

a. *Using your Web browser, navigate to https://workplus.splunk.com/perscholas. On the **Get Started with Splunk** section, click on the **Login** button.*
b. *On the **Splunk Account Login** section, enter the **Email or Username** you used to signup for splunk.com and click the **Next** button.*
c. *Next, enter your **password** and click on the **Splunk Account Login** button.*
d. *Once you are signed in, click on the Courses tab on the **WELCOME TO SplunkWork+ | Per Scholas** page.*
e. *Scroll to the **Splunk education** section and click the **Learn More >** link under **Single-Subject Courses**.*
f. *Scroll down on the **Splunk Pledge Education Benefits (SplunkWork+)** page, locate and click the **Using Fields (eLearning with labs)** course.*
g. *Scroll down on the **Using Fields (eLearning with labs)** page, and click the **BUY NOW** button (Don't worry, you will **not** have to pay for this course).*
h. *On the **My order** step, click on the **Apply coupon code** link.*
i. *Enter the coupon **SplunkPledge** into the box and click on the **APPLY** button.*
j. *Note that the **Total coupon discount is (100%): 300** and that the **Final amount is 0**. Next, click on the **CONFIRM** button.*
k. *Launch the course by clicking the **Data Models** link on the **Order Successful** page under the **Item Details** section.*

Step 2: Launch the Splunk lab environment.

You will launch the Splunk lab environment from the Using Fields (eLearning with labs) course in this step. Once the server is up, it will run for four hours.

If you need screenshots of the steps to launch the server, see the GLAB 200.2.1 - Splunk Fundamentals lab instructions.

Note: In this lab, you use the Splunk environment provided for the Using Fields (eLearning with labs) course as the actual lab.

You must only complete **Lab Exercise 1 – Use Fields in Searches** on the Splunk lab.

a. *If you still need to do so, go to your **Using Fields (eLearning with labs)** course (Note, you can also access the course via the registration confirmation email sent to the account used to register for the course)*
b. *On the **Using Fields In Progress page**, scroll down to the **Using Fields Labs** section and click the **LAUNCH** button.*
   *Review the welcome notification on the **Using Fields - Lab Work** page and click on the **I AGREE** link.*
c. *Under the **SERVERS** tab, click on the **CONNECT TO LAB SERVERS** button. Note it may take several minutes for the servers to be available.*
d. *Once the lab server is ready, the **Using Fields Labs** page will display the **SERVER URL**, a **SPLUNK USER NAME**, and **PASSWORD**. Click on the **SERVER URL** link.*
e. *The LAB DOCUMENT section on the **Using Fields Labs** page contains the lab instructions. Follow the instructions for **Lab Exercise 1 – Use Fields in Searches** section.*

Part 2: Complete Lab Exercise 1 – Use Fields in Searches.

a. ***Lab Exercise 1 – Use Fields in Searches** asks you to save your work as a report(s). Every time you do so, follow the instructions on the Before You Begin - How to Submit This Activity to submit your work.*