
Lab Exercise 11: Creating and Using Macros

Description

This lab exercise walks you through the steps for creating a basic macro and a macro with arguments.

Steps

Scenario: The VP of Sales wants to run ad-hoc searches to determine how much product is being sold in a given month in various countries. He also wants to easily convert international sales to US Dollars based on current exchange rates.

Task 1: Write a basic macro to create a table displaying the total sales of each product sold in Europe.

1. Using the stats command, create a table showing the total retail sales for each product sold in Europe (combining sales from Germany, France, and Italy) over the **Last 30 days** and rename the total sales column as USD.
2. Using the eval command, convert the numeric values in the total sales column to strings and concatenate them with a \$ sign.
Hint: After typing this search string, you may want to copy it into a notepad, as you'll be using it to create a macro later in this exercise.
3. Navigate to Settings > Advanced search > Search macros.
4. Click New Search Macro.
5. Verify the Destination app is set to **search**.
6. Name the macro: Europe_sales
7. In the **Definition** field, type the search string in step 2.
8. Save the macro.

Task 2: Use a basic macro.

9. Return to the Search & Reporting app.
10. In the search bar, type `Europe_sales` and search over the **Last 30 days**. Examine the results.

NOTE: Remember to type the macro name between backticks, not single quotes.

Results Example:

product_name	USD
Benign Space Debris	\$474.81
Curling 2014	\$379.81
Dream Crusher	\$799.80
Final Sequel	\$249.90
Fire Resistance Suit of Provolone	\$135.66
Holy Blade of Gouda	\$167.72
Manganiello Bros.	\$1,919.52
Manganiello Bros. Tee	\$569.43
Mediocre Kingdoms	\$1,349.46

Task 3: Create a macro that enables users to specify currency when performing a search. This macro uses currency, currency symbol, and rate as variables (arguments).

- Run the following search to determine total sales for each product from vendors in Europe in the **last 30 days**:

```
sourcetype=vendor_sales VendorCountry=Germany OR VendorCountry=France OR
VendorCountry=Italy
| stats sum(price) as USD by product_name
| eval euro = "€" + tostring(round(USD*0.79,2), "commas"), USD = "$" +
tostring(USD, "commas")
```

Now you're going to use the second portion of this search string, where the evaluations are done, to create a dynamic macro with arguments.

- Navigate to Settings > Advanced search > Search macros.
- Click New Search Macro.
- Verify the Destination app is set to **search**.
- Name the macro: `convert_sales(3)`
- To make things easy for the user, the currency, currency symbol and exchange rate are arguments. Enter the following search string (the arguments are encapsulated by the \$ signs):

```
stats sum(price) as USD by product_name
| eval $currency$="$symbol$".tostring(round(USD*$rate$,2), "commas"), USD="$" +
tostring(USD, "commas")
```

NOTE: Be sure to include the pipe symbol (|) before the `eval` command.

- In the **Arguments** field, type the arguments, separated by commas.
Hint: currency, symbol, rate (order of variables must match the search string)
- Save the macro.

Task 4: Use your macro with arguments in a search.

19. Return to the Search & Reporting app.
20. Perform a search for `sourcetype=vendor_sales` where the `VendorCountry` is Germany, France, or Italy. Use the macro and pass the arguments `euro`, `€`, and `0.79` for results in the **Last 30 days**.
Hint: ``convert_sales(currency,symbol,rate)``

NOTE: You can copy/paste the € symbol from this document or go to the following web site for the keyboard shortcuts:

<http://bit.ly/2BqMmR0>

21. Run the search again for sales in the UK with the following arguments `GBP`, `£`, and `0.64`. Copy/paste the £ symbol from this document.

Results Example:

product_name ↕	USD ↕	GBP ↕
Benign Space Debris	\$374.85	£239.90
Curling 2014	\$259.87	£166.32
Dream Crusher	\$479.88	£307.12
Final Sequel	\$74.97	£47.98
Fire Resistance Suit of Provolone	\$95.76	£61.29
Holy Blade of Gouda	\$101.83	£65.17
Manganiello Bros.	\$759.81	£486.28
Manganiello Bros. Tee	\$199.80	£127.87
Mediocre Kingdoms	\$349.86	£223.91
Orvil the Wolverine	\$399.90	£255.94
Puppies vs. Zombies	\$4.99	£3.19
SIM Cubicle	\$319.84	£204.70
World of Cheese	\$499.80	£319.87
World of Cheese Tee	\$169.83	£108.69

Task 5: Edit your macro and use the `isnum` expression to validate the rate field.

22. Navigate to Settings > Advanced search > Search macros.
23. Choose your user name from the Owner dropdown list.
24. Click on the **convert_sales(3)** link.
25. In the Validation Expression text box, type: `isnum($rate$)`
26. In the Validation Error Message text box, type: This macro is expecting to be called as `'convert_sales(currency,symbol,rate)'` where rate is a numeric value.


27. Click **Save**.
28. Return to the Search & Reporting app.
29. Perform a search for `sourcetype=vendor_sales` for the **Last 30 days** where the `VendorCountry` is Germany, France, or Italy. Use the macro, but deliberately pass a non-numeric value for the rate argument (for example, pass the arguments `GBP`, `£`, and `.xxx`).
30. Check to see that your error message displays.

Results Example:

New SearchClose

index= sales sourcetype=vendor_sales VendorCountry=Germany OR VendorCountry=France OR VendorCountry=Italy | 'convert_sales(euro,£,.xxx)'

Last 24 hours 

 Error in 'SearchParser': Encountered the following error while validating macro 'convert_sales(euro,£,.xxx)': This macro is expecting to be called as 'convert_sales(currency,symbol,rate)' where rate is a numeric value..