

Lab Exercise 10: Tags and Event Types

Description

This lab exercise walks you through the steps to create tags and event types.

Steps

Scenario: The IT Operations team needs to monitor failed login attempts made with any variation of admin/administrator user accounts to their network devices. To avoid lengthy searches, include all events with these user accounts and create tags.

Task 1: Create tags to identify all admin accounts.

1. Run a search over the **Last 24 hours** for all failed login attempts for any variation of the user *admin* under the security index. You should see the following five users: admin, administrator, sysadmin, itmadmin, and sapadmin.

NOTE: Only trailing wildcards make efficient use of indexes. For that reason, it's generally a best practice *not* to use wildcards at the beginning of a string, as such searches have to scan all events within the specified time frame. However, doing a search with a wildcard at the beginning of a string is *possible* and sometimes necessary in particular scenarios. Be advised, however, that such searches are inefficient and, in general, should be avoided.

2. Expand an event and find the row for the **user** field. Click the **down arrow** under the **Actions** column and select **Edit Tags**.

Example:

Type	Field	Value	Actions
Selected	<input checked="" type="checkbox"/> host	www2	▼
	<input checked="" type="checkbox"/> source	/opt/log/www2/secure.log	▼
	<input checked="" type="checkbox"/> sourcetype	linux_secure	▼
Event	<input type="checkbox"/> action	failure(failure)	▼
	<input type="checkbox"/> app	sshd	▼
	<input type="checkbox"/> dest	www2	▼
	<input type="checkbox"/> eventtype	err0r(error)	▼
		failed_login	▼
		nix-all-logs	▼
		nix_errors(error)	▼
		nix_security(os unix)	▼
		sshd_authentication(authentication remote)	▼
	<input type="checkbox"/> pid	1698	▼
	<input type="checkbox"/> port	2277	▼
	<input type="checkbox"/> process	sshd	▼
	<input type="checkbox"/> src	76.169.7.252	▼
	<input type="checkbox"/> src_ip	76.169.7.252	▼
	<input type="checkbox"/> src_port	2277	▼
	<input type="checkbox"/> sshd_protocol	ssh2	▼
	<input type="checkbox"/> tag	authentication	▼
		error	▼
		failure	▼
		os	▼
		remote	▼
		unix	▼
	<input type="checkbox"/> user	sapadmin	Edit Tags

3. In the **Tag(s)** field, type **privileged_user** and click **Save**.

4. Create tags for each variation of the user *admin* (admin, administrator, sysadmin, itmadmin, and sapadmin). You can create the subsequent tags the same way you created the first one, from the Events tab of the search results. Alternatively, you can also create the subsequent tags by going to the **Settings > Tags > List by tag name** screen, choosing the newly created **privileged_user** tag, adding the other four types of admins, and clicking **Save**.
5. Run the search again and check to see that the privileged_user tag was created.
6. If it isn't already, add **tag** to your list of Selected Fields.

Results Example:

The screenshot shows the 'tag' configuration interface in Splunk. On the left, under 'SELECTED FIELDS', the 'tag' field is highlighted with a red box. The main panel displays '7 Values, 100% of events' and a table of values. The 'privileged_user' tag is highlighted with a red box in the table.

Values	Count	%
authentication	553	100%
error	553	100%
failure	553	100%
os	553	100%
remote	553	100%
unix	553	100%
privileged_user	210	37.975%

Task 2: Use tags in a search.

7. Search for all failed login attempts by privileged user accounts for the **Last 7 days**. You should see the following five users: admin, administrator, sysadmin, itmadmin, sapadmin

Scenario: Customers are reporting issues trying to purchase items from the Buttercup Games online store and internal users get errors trying to access the internet. IT Ops wants an easy way to determine if there is any correlation when both systems encounter problems.

Task 3: Create an event type for status errors greater than 500 on web servers/devices.

8. Search for all online sales and Web security appliance data with status error codes greater than 500 in the **last 7 days**.
9. Select **Save As > Event Type**.
10. Name your event type: **web_error**
11. Leave the **Priority** set to 1 (Highest).
12. Click **Save**.
13. Perform a search for the web_error event type for the **Last 7 days**.

14. Expand an event and click the checkbox next to **eventtype** to add it to the Selected fields.
15. How many sourcetypes are returned?

Results Example:

The screenshot shows the Splunk Search interface with the search query `eventtype=web_error`. The results are displayed in a table format. The left sidebar shows the 'SELECTED FIELDS' and 'INTERESTING FIELDS' sections. The main table has columns for 'Time' and 'Event'. The 'Event' column contains detailed log entries for web errors.

Time	Event
2/6/18 10:42:09.000 AM	141.146.8.66 - - [06/Feb/2018:18:42:09] "POST /oldlink?itemId=EST-14&JSESSIONID=SD10SL1FF10ADFF4952 HTTP 1.1" 505 1968 "http://www.buttercupgames.com/product.screen?productId=SF-BVS-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 802 host = www1 source = /opt/log/www1/access.log sourcetype = access_combined
2/6/18 10:30:31.000 AM	62.216.64.19 - - [06/Feb/2018:18:30:31] "POST /oldlink?itemId=EST-13&JSESSIONID=SD8SL5FF2ADFF4962 HTTP 1.1" 503 2332 "http://www.buttercupgames.com/oldlink?itemId=EST-13" "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)" 770 host = www2 source = /opt/log/www2/access.log sourcetype = access_combined
2/6/18 10:15:36.000 AM	84.34.159.23 - - [06/Feb/2018:18:15:36] "POST /product.screen?productId=SF-BVS-01&JSESSIONID=SD6SL4FF6ADFF4952 HTTP 1.1" 503 2289 "http://www.buttercupgames.com/product.screen?productId=SF-BVS-01" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 590 host = www1 source = /opt/log/www1/access.log sourcetype = access_combined

NOTE: Depending upon add-ons or apps you have installed, additional event types may be displayed.