Lab Exercise 9: Creating 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.

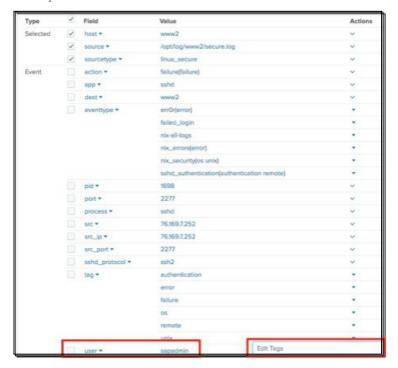
Task 1: Create tags to identify all admin accounts.

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. Performing an occasional inefficient ad hoc search shouldn't have too much of a performance impact, but such searches certainly shouldn't be used in reports, dashboards, dataset constraints, etc.

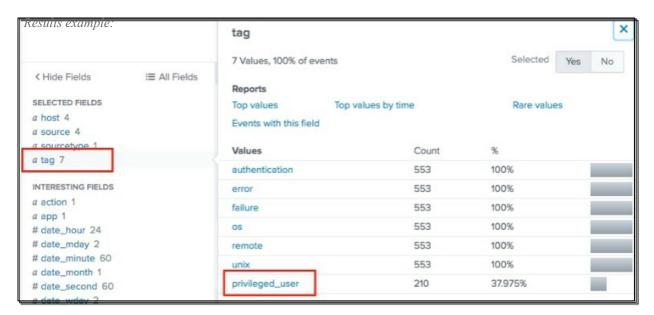
2. Expand an event and find the row for the **user** field. Click the **down arrow** under the **Actions** column and select **Edit Tags**.

Example:



2 Page 42

- 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.



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, it madmin, sapadmin

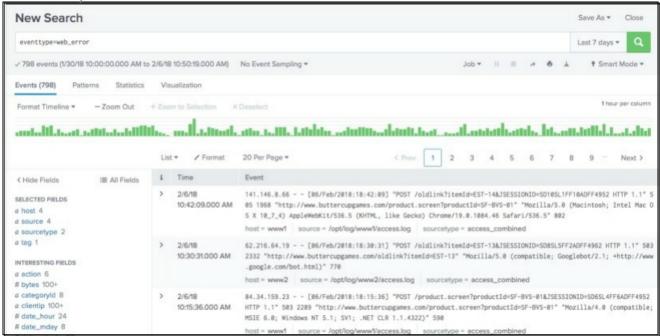
Sagravias — Customars are reporting issues twing to purchase items from the Dutteroup

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?





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

Page 44