Scheduling Reports and Alerts – Lab Guide

Overview

Welcome to the Splunk Education lab environment. In these labs you will create and schedule a report, manage the report's settings, create scheduled and real-time alerts, define alert trigger conditions, define actions that respond to trigger conditions and view alert settings.

Scenario

You will use data from the international video game company, Buttercup Games. A list of source types is provided below.

NOTE: This is a lab environment driven by data generators with obvious limitations. This is not a production environment. Screenshots approximate what you should see, not the **exact** output.

Index	Type	Sourcetype	Interesting Fields
web	Online sales	**access_combined**	action, bytes, categoryId, clientip, itemId, JSESSIONID, price, productId, product_name, referer, referer_domain, sale_price, status, user, useragent
security	Web server	**linux_secure**	action, app, dest, process, src_ip, src_port, user, vendor_action

Common Commands and Functions

These commands and statistical functions are commonly used in searches but may not have been explicitly discussed in the module. Please use this table for quick reference. Click on the hyperlinked SPL to be taken to the Search Manual for that command or function.

SPL	Type	Description	Example
`sort`	command	Sorts results in descending or ascending order by a specified field. Can limit results to a specific number.	*Sort the first 100 `src_ip` values in descending order* `| sort 100 -src_ip`
`where`	command	Filters search results using eval-expressions.	*Return events with a `count` value greater than 30* `| where count > 30`
`rename`	command	Renames one or more fields.	*Rename `SESSIONID` to 'The session ID'* `| rename SESSIONID as "The session ID"`
`fields`	command	Keeps (+) or removes (-) fields from search results.	*Remove the `host` field from the results* `| fields - host`
`stats`	command	Calculates aggregate statistics over the results set.	*Calculate the total sales, i.e. the sum of `price` values* `| stats sum(price)`
`eval`	command	Calculates an expression and puts the resulting value into a new or existing field.	*Concatenate `first_name` and `last_name` values with a space to create a field called "`full_name`"* `| eval full_name=first_name." ".last_name`
`table`	command	Returns a table.	*Output `vendorCountry`, `vendor`, and `sales` values to a table* `| table vendorCountry, vendor, sales`
`sum()`	statistical function	Returns the sum of the values of a field. Can be used with **`stats`**, **`timechart`**, and **`chart`** commands.	*Calculate the sum of the `bytes` field* `| stats sum(bytes)`

`count` or `count()`	statistical function	Returns the number of occurrences of all events or a specific field. Can be used with **`stats`**, **`timechart`**, and **`chart`** commands.	*Count all events as "events" and count all events that contain a value for `action` as "action"*
			`| stats count as events,`
			`count(action) as action`

Refer to the Search Reference Manual for a full list of commands and functions.

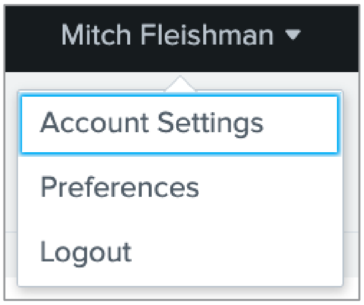
Lab Exercises

Configure the lab environment user account.

Task 1: Log into Splunk and change the account name and time zone.

Set up your lab environment to fit your time zone. This also allows the instructor to track your progress and assist you if necessary.

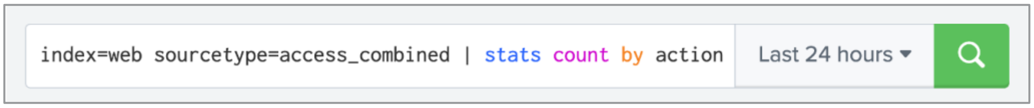
1. Log into your Splunk lab environment using the username and password provided to you.
2. You may see a pop-up window welcoming you to the lab environment. You can click **Continue to Tour** but this is not required. Click **Skip** to dismiss the window.
3. Click on the username you logged in with (at the top of the screen) and then choose **Account Settings** from the drop-down menu.
4. In the **Full name** box, enter your first and last name.
5. Click **Save**.
6. Reload your browser to reflect the recent changes to the interface. (This area of the web interface will be referred to as ***user name***.)



After you complete step 6, you will see your name in the web interface.

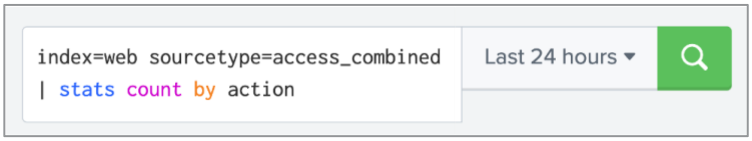
NOTE: Sometimes there can be delays in executing an action like saving in the UI or returning results of a search. If you are experiencing a delay, please allow the UI a few minutes to execute your action.

7. Navigate to ***user name*** **> Preferences.**
8. Choose your local time zone from the **Time zone** drop-down menu.
9. Click **Apply**.
10. (Optional) Navigate to ***user name*** **> Preferences > SPL Editor > Search auto-format** and click on the toggle to activate auto-formatting. Then click **Apply**. When the pipe character is used in search, the SPL Editor will automatically begin the pipe on a new line.



```
index=web sourcetype=access_combined | stats count by action
```

Search auto-format disabled (default)



```
index=web sourcetype=access_combined
| stats count by action
```

Search auto-format enabled

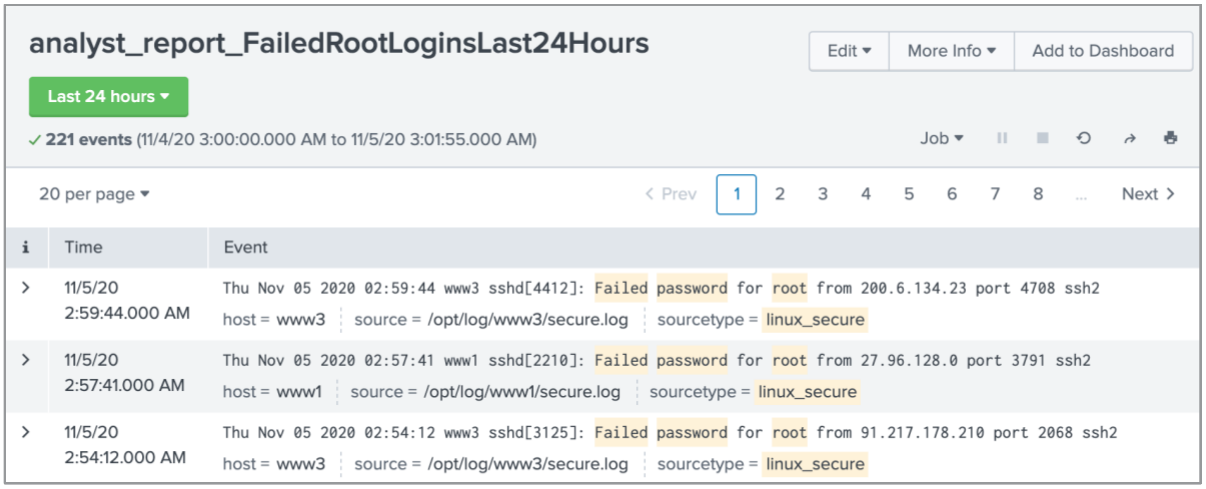
Scenario: Create a scheduled report for failed root logins over the last 24 hours.

Task 2: Save a search as a report.

1. Navigate to the **Apps > Search and Reporting**.
2. Execute the following search over the **Last 24 hours** to find failed root logins **(fail* root)** from the web server **(sourcetype=linux_secure)**:

```
index=security sourcetype=linux_secure password fail* root
```

3. From the **Save As** menu (located above the time picker), select **Report**.
   a. Title: **`analyst_report_FailedRootLoginsLast24Hours`**
   b. Time Range Picker: **Yes**
   c. Click **Save**.
4. In the Your Report Has Been Created dialog box, click **View**.

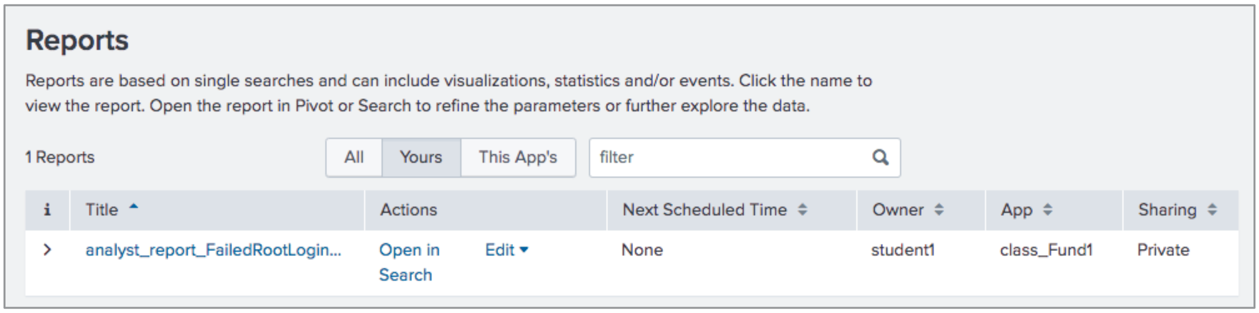


analyst_report_FailedRootLoginsLast24Hours

✓ 221 events (11/4/20 3:00:00.000 AM to 11/5/20 3:01:55.000 AM)

i	Time	Event
›	11/5/20 2:59:44.000 AM	Thu Nov 05 2020 02:59:44 www3 sshd[4412]: Failed password for root from 200.6.134.23 port 4708 ssh2 host = www3 source = /opt/log/www3/secure.log sourcetype = linux_secure
›	11/5/20 2:57:41.000 AM	Thu Nov 05 2020 02:57:41 www1 sshd[2210]: Failed password for root from 27.96.128.0 port 3791 ssh2 host = www1 source = /opt/log/www1/secure.log sourcetype = linux_secure
›	11/5/20 2:54:12.000 AM	Thu Nov 05 2020 02:54:12 www3 sshd[3125]: Failed password for root from 91.217.178.210 port 2068 ssh2 host = www3 source = /opt/log/www3/secure.log sourcetype = linux_secure

5. Click **Reports**. You can see the reports to which you have access. (You can re-execute a report by clicking the title, or view or edit the search by clicking **Open in Search**.) Examine the **All**, **Yours**, and **This App's** list of saved reports.



Reports

Reports are based on single searches and can include visualizations, statistics and/or events. Click the name to view the report. Open the report in Pivot or Search to refine the parameters or further explore the data.

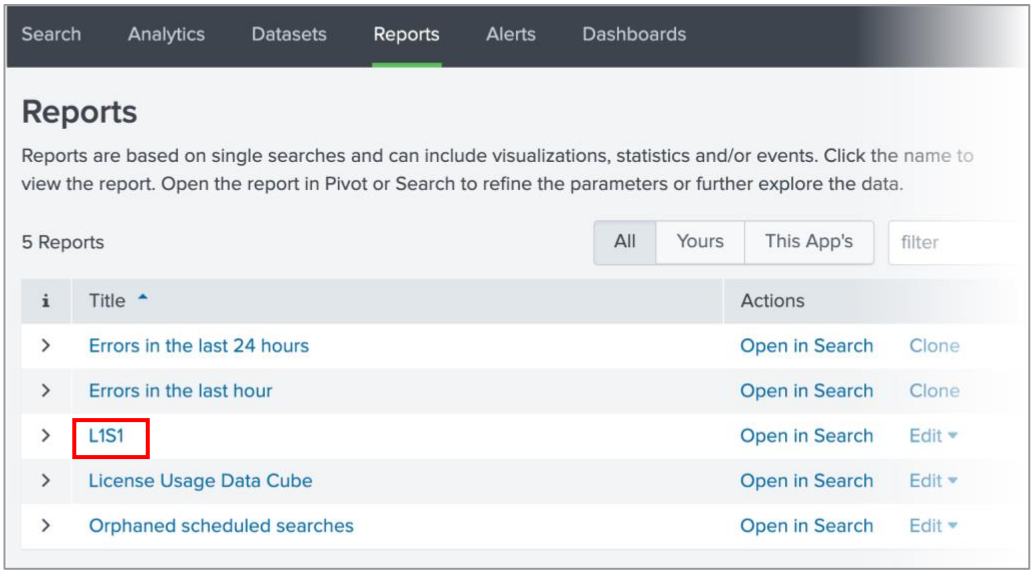
1 Reports

i	Title ▴	Actions		Next Scheduled Time ⇕	Owner ⇕	App ⇕	Sharing ⇕
›	analyst_report_FailedRootLogin...	Open in Search	Edit ▾	None	student1	class_Fund1	Private

6. For the **analyst_report_FailedRootLoginsLast24Hours** report, click **Open in Search**.
7. Save your search as a report with the name **L1S1**.
   a. Click **Save As** > **Report**
   b. For **Title**, enter L1S1.
   c. **Save**.

d. You can **View** your report or exit out of the **Your Report Has Been Created** window by clicking the **X** in the upper-right corner.

e. You can access your saved reports using the **Reports** tab in the application bar.



Reports

Reports are based on single searches and can include visualizations, statistics and/or events. Click the name to view the report. Open the report in Pivot or Search to refine the parameters or further explore the data.

5 Reports

i	Title	Actions	
>	Errors in the last 24 hours	Open in Search	Clone
>	Errors in the last hour	Open in Search	Clone
>	L1S1	Open in Search	Edit ▾
>	License Usage Data Cube	Open in Search	Edit ▾
>	Orphaned scheduled searches	Open in Search	Edit ▾

*Your recently saved **L1S1** report will be visible in the **Reports** tab.*

Task 3: Schedule the failed logins report (L1S1) to run daily at 6 am.

8. If necessary, from the App drop-down menu, choose **Search and Reporting** to return to the Search view.
9. In the App navigation bar, click **Reports**.
10. For the row containing your L1S1 report, click **Edit**.
11. Select **Edit Schedule**.
12. Select **Schedule Report**.
13. Make the following selections:
    a. **Schedule**: Run every day
    b. **At**: 6:00
    c. **Time Range**: Last 24 hours
    d. Schedule Priority: Default
    e. **Schedule Window**: 2 hours
14. Click the **+Add Actions** button to send an email when the scheduled report is triggered.
15. Select **Send email**.
16. Configure the Trigger Action as follows:
    a. **To**: admin@buttercupgames.com
17. Leave all other options as default.
18. Click **Save**.

Scenario: Create a real-time alert for multiple failed logins.

Task 4: Create a search to identify specific types of failed logins.

19. Click **Search**.
20. Search for all events in the Linux secure logs over the **Last 60 minutes**.
21. Add the keywords `failed password NOT invalid` then, re-run the search.

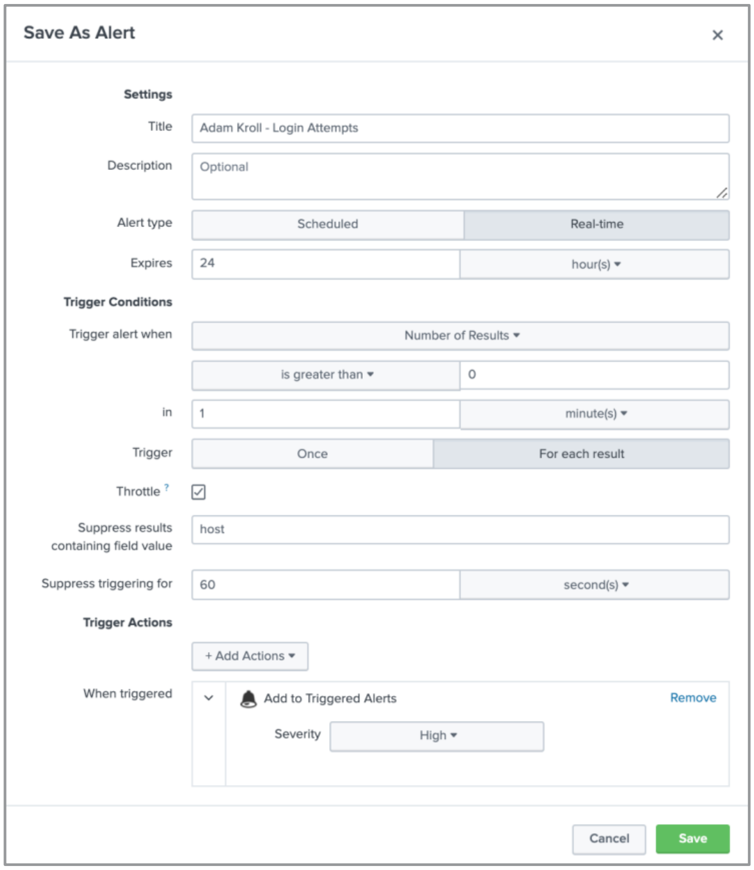
```
index=security sourcetype=linux_secure failed password NOT invalid
```

Task 5: Create and view an alert.

22. From the **Save As** menu, select **Alert.**
    a. **Title**: <student name>- Login Attempts
    b. **Permissions**: Private
    c. **Alert type**: Real-time
    d. **Expires**: 24 hour(s).
    e. **Trigger alert when**: Number of Results
    f. Set the number of results to **is greater** than 0 **in** 1 **minutes(s)**.

NOTE: This setting is set to 0 for testing. Once the alert is verified, you can change this value.

    g. **Trigger**: For each result
    h. Select **Throttle**.
    i. **Suppress results containing field value**: host
    j. **Suppress triggering for**: 60 second(s)
    k. Click **+Add Actions** and select **Add to Triggered Alerts**.
    l. Set the **Severity** to **High**.
    m. Click **Save**.



Save As Alert ×

Settings

Title: Adam Kroll - Login Attempts

Description: Optional

Alert type: Scheduled | **Real-time**

Expires: 24 hour(s) ▾

Trigger Conditions

Trigger alert when: Number of Results ▾

is greater than ▾ 0

in: 1 minute(s) ▾

Trigger: Once | **For each result**

Throttle ?: ☑

Suppress results containing field value: host

Suppress triggering for: 60 second(s) ▾

Trigger Actions

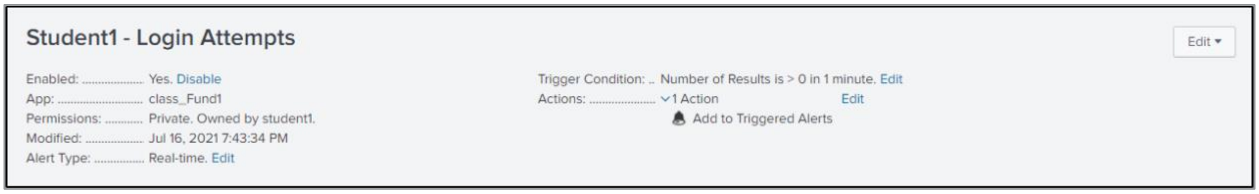
+ Add Actions ▾

When triggered: Add to Triggered Alerts — Remove

Severity: High ▾

Cancel | Save

23. Click **View Alert**. You should see an overview screen describing your new alert.



Student1 - Login Attempts

Edit ▾

Enabled: Yes. Disable

App: class_Fund1

Permissions: Private. Owned by student1.

Modified: Jul 16, 2021 7:43:34 PM

Alert Type: Real-time. Edit

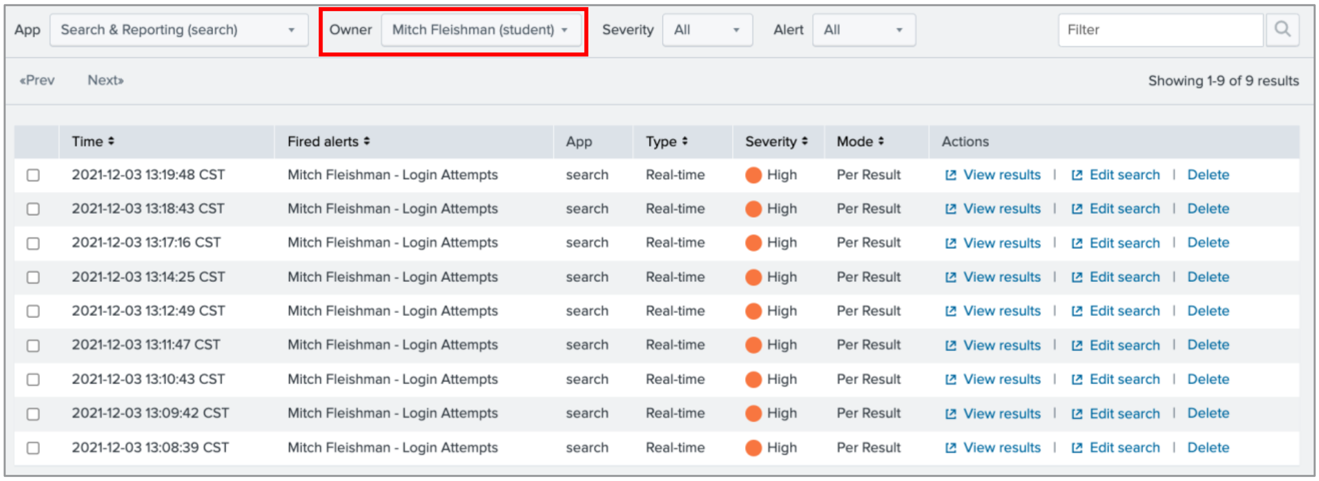
Trigger Condition: Number of Results is > 0 in 1 minute. Edit

Actions: 1 Action Edit

Add to Triggered Alerts

24. From the Splunk bar, click **Activity** > **Triggered Alerts**.
25. Select your name from the **Owner** menu and view the triggered alerts.

NOTE: It may take a few minutes for your alert to appear.

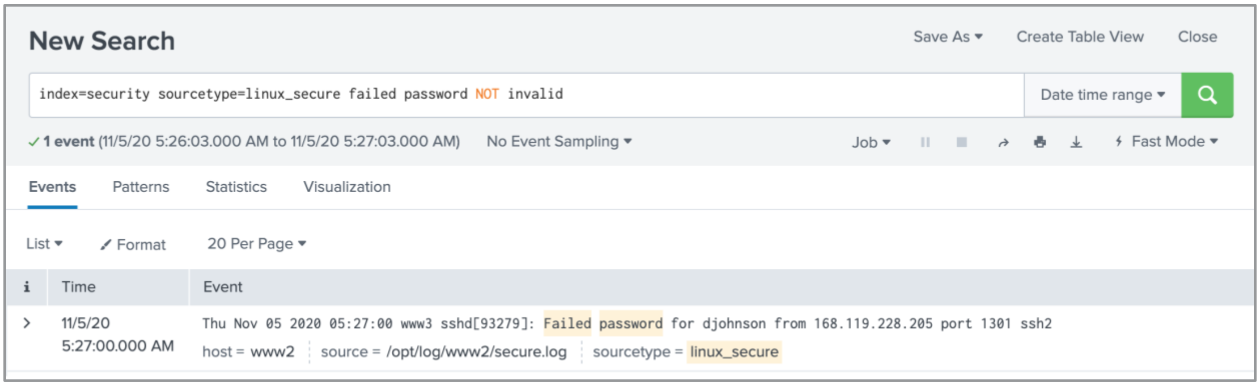


App: Search & Reporting (search) | Owner: Mitch Fleishman (student) | Severity: All | Alert: All | Filter

«Prev Next» Showing 1-9 of 9 results

	Time	Fired alerts	App	Type	Severity	Mode	Actions
□	2021-12-03 13:19:48 CST	Mitch Fleishman - Login Attempts	search	Real-time	● High	Per Result	View results | Edit search | Delete
□	2021-12-03 13:18:43 CST	Mitch Fleishman - Login Attempts	search	Real-time	● High	Per Result	View results | Edit search | Delete
□	2021-12-03 13:17:16 CST	Mitch Fleishman - Login Attempts	search	Real-time	● High	Per Result	View results | Edit search | Delete
□	2021-12-03 13:14:25 CST	Mitch Fleishman - Login Attempts	search	Real-time	● High	Per Result	View results | Edit search | Delete
□	2021-12-03 13:12:49 CST	Mitch Fleishman - Login Attempts	search	Real-time	● High	Per Result	View results | Edit search | Delete
□	2021-12-03 13:11:47 CST	Mitch Fleishman - Login Attempts	search	Real-time	● High	Per Result	View results | Edit search | Delete
□	2021-12-03 13:10:43 CST	Mitch Fleishman - Login Attempts	search	Real-time	● High	Per Result	View results | Edit search | Delete
□	2021-12-03 13:09:42 CST	Mitch Fleishman - Login Attempts	search	Real-time	● High	Per Result	View results | Edit search | Delete
□	2021-12-03 13:08:39 CST	Mitch Fleishman - Login Attempts	search	Real-time	● High	Per Result	View results | Edit search | Delete

26. Click the **View results** link on a triggered alert to see the event(s) that caused the alert.



```
index=security sourcetype=linux_secure failed password NOT invalid
```

✓ 1 event (11/5/20 5:26:03.000 AM to 11/5/20 5:27:03.000 AM) No Event Sampling ▾

i	Time	Event
>	11/5/20 5:27:00.000 AM	Thu Nov 05 2020 05:27:00 www3 sshd[93279]: Failed password for djohnson from 168.119.228.205 port 1301 ssh2 host = www2 source = /opt/log/www2/secure.log sourcetype = linux_secure

Task 6: Save the alert results as a report.

27. Click **Save As** and select **Report**.
28. For **Title**, enter L1S2.
29. Click **Save.**

Task 7: Disable the alert.

30. From the Apps drop-down menu, select **Search and Reporting** to return to the Search view.
31. In the App navigation bar, click **Alerts**.
32. For the row containing your alert, click **Edit**, then select **Disable**.
33. When the **Disable** dialog box appears, click **Disable**