

Splunk Fundamentals 1 Lab Exercises

Lab typographical conventions:

[sourcetype=db audit] OR [cs mime type] indicates either a source type or the name of a field.

NOTE: Lab work will be done on your personal computer or virtual machine, no lab environment is provided. We suggest you **DO NOT** do the lab work on your production environment.

The lab instructions refer to these source types by the types of data they represent:

Туре	Sourcetype	Fields of interest action, bytes, categoryId, clientip, itemId, JSESSIONID, productId, referer, referer_domain, status, useragent, file				
Web Application	access_combined_wcookie					
Database	db_audit	Command, Duration, Type				
Web server	linux_secure	COMMAND, PWD, pid, process				

Lab Module 13 – Creating Alerts

WARNING: This lab will not work with a free license. Please only do this lab if your trial license has not converted to a free license.

NOTE: This lab document has two sections. The first section includes the instructions without answers. The second section includes instructions with the expected search string (answer) in red. This course will use internal Splunk data and require an Admin account.

Description

In this lab exercise, you will create and trigger an alert that will display in the Splunk interface.

Scenario: For security reasons, you need to monitor failed login attempts on your Splunk search head. You are only interested in failed logins from the admin account. You want to be notified when there is more than one failed login attempt within one minute.

Task 1: Change user account and run a sample search.

- 1. Log out of Splunk Enterprise using the uname > Logout menu.
- 2. Enter admin for user name and the password of WrongPassword.
- 3. Now, enter admin for user name and the password you selected in Module 3.
- 4. Navigate to the Search view. (If you are in the **Home** app, click **Search & Reporting** from the column on the left side of the screen. You can also access the Search view by clicking the **Search** menu option on the green bar at the top of the screen.)



5. Search the _audit index for events where the action of "login attempt" returned a "failed" info value for the username of admin over the Last 15 Minutes.

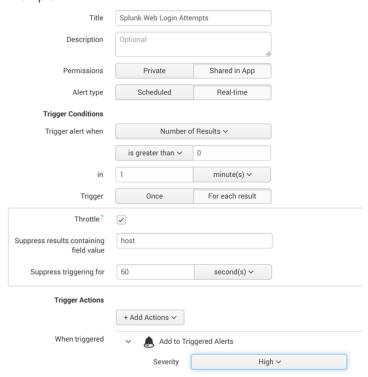
Example Results:

i	Time	Event					
>	5/4/17	Audit:[timestamp=05-04-2017 19:47:42.298, user=admin, action=login attempt, info=failed, src=127.0.0.1][n/a]					
	7:47:42.298 PM	host = cbreshears-mbp15r.sv.splunk.com source = audittrail sourcetype = audittrail					

Task 2: Create an alert.

- 6. From the Save As menu, select Alert.
- 7. Title the alert: Splunk Web Login Attempts
- 8. For Permissions, select Shared in App.
- 9. For Alert type, select Real-time.
- 10. For Trigger alert when, select Number of Results.
- 11. Set the number of results to: is greater than 0.
- 12. The in field should be set to 1 minute.
- 13. For Trigger, select For each result.
- 14. Check the Throttle checkbox.
- 15. For Suppress results containing field value, type: host
- 16. Make sure **Suppress triggering** for is set to 60 seconds.
- 17. Click Add Actions and select Add to Triggered Alerts.
- 18. Set the Severity to High.

Example:



19. Click Save and Click View Alert.

Task 3: Test alert.



- 21. Enter admin for user name and the password of WrongPassword three times in a row.
- 22. Now, enter admin for user name and the correct password.
- 23. From the Splunk bar, click **Activity** > **Triggered Alerts**.
- 24. Make sure **Search & Reporting** is selected for **App**.

Example:

Time ‡	Fired alerts ‡	App	Type \$	Severity \$	Mode	Actions		
2017-05-04 20:17:48 PDT	Splunk Web Login Attempts	search	Real-time	High	Per Result	✓ View results	🔁 Edit search	Delete

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



Splunk Fundamentals 1 Lab Exercises

Lab typographical conventions:

[sourcetype=db audit] OR [cs mime type] indicates either a source type or the name of a field.

NOTE: Lab work will be done on your personal computer or virtual machine, no lab environment is provided. We suggest you **DO NOT** do the lab work on your production environment.

The lab instructions refer to these source types by the types of data they represent:

Туре	Sourcetype	Fields of interest action, bytes, categoryId, clientip, itemId, JSESSIONID, productId, referer, referer_domain, status, useragent, file				
Web Application	access_combined_wcookie					
Database	db_audit	Command, Duration, Type				
Web server	linux_secure	COMMAND, PWD, pid, process				

Lab Module 13 - Creating Alerts with Solutions

WARNING: This lab will not work with a free license. Please only do this lab if your trial license has not converted to a free license.

NOTE: This lab document has two sections. The first section includes the instructions without answers. The second section includes instructions with the expected search string (answer) in red. This course will use internal Splunk data and require an Admin account.

Description

In this lab exercise, you will create and trigger an alert that will display in the Splunk interface.

Scenario: For security reasons, you need to monitor failed login attempts on your Splunk search head. You are only interested in failed logins from the admin account. You want to be notified when there is more than one failed login attempt within one minute.

Task 1: Change user account and run a sample search.

- 1. Log out of Splunk Enterprise using the uname > Logout menu.
- 2. Enter admin for user name and the password of WrongPassword.
- 3. Now, enter admin for user name and the password you selected in Module 3.
- 4. Navigate to the Search view. (If you are in the **Home** app, click **Search & Reporting** from the column on the left side of the screen. You can also access the Search view by clicking the **Search** menu option on the green bar at the top of the screen.)



5. Search the _audit index for events where the action of "login attempt" returned a "failed" info value for the username of admin over the Last 15 Minutes.

(index=_audit action="login attempt" info=failed user=admin)

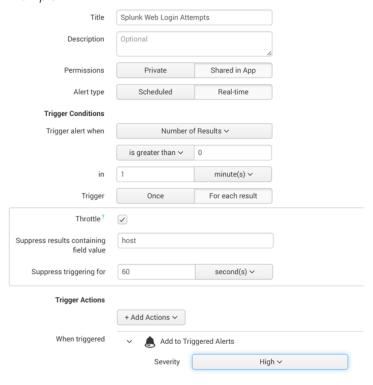
Example Results:

i	Time	Event					
>	5/4/17	Audit:[timestamp=05-04-2017 19:47:42.298, user=admin, action=login attempt, info=failed, src=127.0.0.1][n/a]					
	7:47:42.298 PM	host = cbreshears-mbp15r.sv.splunk.com source = audittrail sourcetype = audittrail					

Task 2: Create an alert.

- 6. From the Save As menu, select Alert.
- 7. Title the alert: Splunk Web Login Attempts
- 8. For **Permissions**, select **Shared in App**.
- 9. For Alert type, select Real-time.
- 10. For Trigger alert when, select Number of Results.
- 11. Set the number of results to: is greater than 0.
- 12. The in field should be set to 1 minute.
- 13. For Trigger, select For each result.
- 14. Check the **Throttle** checkbox.
- 15. For Suppress results containing field value, type: host
- 16. Make sure Suppress triggering for is set to 60 seconds.
- 17. Click Add Actions and select Add to Triggered Alerts.
- 18. Set the **Severity** to **High**.

Example:



19. Click Save and Click View Alert.



Task 3: Test alert.

- 20. Log out of Splunk Enterprise using the **Administrator > Logout** menu.
- $21. \ Enter \ {\tt admin} \ \ for \ user \ name \ and \ the \ password \ of \ {\tt WrongPassword} \ \ three \ times \ in \ a \ row.$
- 22. Now, enter admin for user name and the correct password.
- 23. From the Splunk bar, click **Activity** > **Triggered Alerts**.
- 24. Make sure **Search & Reporting** is selected for **App**.

Example:

Time	Fired alerts ‡	App	Type ‡	Severity \$	Mode ‡	Actions	
2017-05-04 20:17:48 PDT	Splunk Web Login Attempts	search	Real-time	High	Per Result	✓ View results	Edit search Delete

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