

Lab Exercise 12: Creating and Using Workflow Actions

Description

These steps create GET, POST, and Search workflow actions.

Steps


Scenario: Hackers are continually trying to log into the Linux server. IT Ops analysts need to track ongoing attempts by external sources trying to log in with invalid credentials.

Task 1: Create a GET workflow action that opens a new browser window with information about the source IP address.

1. Navigate to Settings > Fields > Workflow actions.
2. Click **New Workflow Action** to create a workflow action.
3. For the Destination App, select search.
4. For **Name**, type: get_whois_info
5. For **Label**, type: Get info for IP: \$src_ip\$
6. For Apply only to the following fields, type: src_ip
7. For **Action type**, make sure link is selected.
8. For **URI**, type: http://who.is/whois-ip/ip-address/\$src_ip\$
9. From the **Open link in** dropdown menu, verify New window is selected.
10. From the **Link Method** dropdown menu, verify get is selected.
11. Save your workflow action.
12. Verify your workflow action works as expected. Return to the **Search & Reporting app** and search for `index=security sourcetype=linux_secure src_ip=*` over the **last 24 hours**. (You may need to refresh your browser for the workflow action to appear.)
13. Expand the first event containing a value for `src_ip` and click **Event Actions**.
14. Click **Get info for IP: {src_ip}**. A secondary browser window should open to the URI and display the IP address information.

NOTE: If whois is not behaving as expected, try `http://whois.domaintools.com/src_ip`.

Results Example:



2/6/18 Tue Feb 06 2018 19:09:54 mailsv1 sshd[32768]: Accepted password for nsharpe from 119.142.102.182 port 1341 ssh2
11:09:54.000 AM

Event Actions ▼

- Build Event Type
- Get info for IP: 119.142.102.182**
- Extract Fields
- Show Source

IP Information for 119.142.102.182

— Quick Stats

IP Location	China Zhongshan Chinanet Guangdong Province Network
ASN	AS4134 CHINANET-BACKBONE No.31,Jin-rong Street, CN (registered Aug 01, 2002)
Whois Server	whois.apnic.net
IP Address	119.142.102.182

inetnum: 119.128.0.0 - 119.143.255.255
netname: CHINANET-GD
descr: CHINANET Guangdong province network
descr: Data Communication Division
descr: China Telecom
country: CN
admin-c: CH93-AP
tech-c: IC83-AP
remarks: service provider
status: ALLOCATED PORTABLE

Scenario: The revenue accounting department is having issues with sales transactions not posting to the accounting system. This issue is causing revenue recognition discrepancies and the IT department is tasked with notifying the accounting system administrators when there is a transaction error in the system.

Task 2: Create a POST workflow action that will use fields from events with errors to create a ticket in the IT ticket tracking system.

15. Perform a search on the `sales_entries` sourcetype for events posting errors.

`index=sales sourcetype=sales_entries error`

16. These events contain two fields that are needed when creating tickets in the tracking system: TransactionID and CustomerID. Create a field extraction with a field name of **result** for the string "error." This allows you to easily search for events where **result=error**.

NOTE: If the **result=error** field extraction is not done, the rest of this task will **not** work.

17. Navigate to Settings > Fields > Workflow actions.

18. Select New Workflow Action.

19. For the Destination App, select **search**.

20. For **Name**, type: Create accounting system ticket

21. For **Label**, type: Open accounting ticket for transaction \$TransactionID\$

22. For Apply only to the following fields, type: result

23. For **Show Action in**, select Event menu.

24. For **Action type**, make sure link is selected.

25. For **URI**, type: `http://52.3.246.206`

26. From the **Open link in** dropdown menu, select **New window**.

27. From the **Link Method** dropdown menu, select **post**.

28. Enter the following values for the **Post arguments**:

- details = `$_raw$`
- environment = `$host$`
- occurred = `$_time$`
- priority = Urgent
- summary = sales transaction error on `$host$`

29. Click **Save**.

30. Rerun your search for events where **result=error** and view the details of one of the returned events. Does your POST workflow action appear?

31. Click on your workflow action. A new browser window should appear with the ticket details.

Results Example:

2/6/18 Tue Feb 06 2018 20:08:04 ecomm engine response TransactionID=121814 CustomerID=dwsvn65u error

12:08:04.000 PM

Event Actions ▼

Open accounting ticket for transaction 121814

Build Event Type

Extract Fields

Show Source

Value

ecommsv1

/opt/log/ecommsv1

sales_entr

error

Bug Tracker 4000

Ticket Added:

Ticket Summary: sales transaction error on ecommsv1

Priority: Urgent

Time of Occurrence: 2018-02-06T12:08:04.000-08:00

Environment: ecommsv1

Details: Tue Feb 06 2018 20:08:04 ecomm engine response TransactionID=121814 CustomerID=dwsvn65u error

Task 3: Create a Search workflow action that performs a search for all failed password events associated with a specific IP address.

32. Navigate to Settings > Fields > Workflow actions.
33. Click New Workflow Action.
34. For the Destination App, select **search**.
35. For **Name**, type: search_access_by_ipaddress
36. For **Label**, type: Search failed login by IP: \$src_ip\$
37. For Apply only to the following fields, type: src_ip
38. From the **Action Type** dropdown menu, select search.
39. In the **Search string** field, type: index=security sourcetype=linux_secure failed src_ip=\$src_ip\$
40. From the **Run in app** dropdown, select **search**.
41. From the **Run search in** dropdown menu, verify New window is selected.
42. Select the Use the same time range as the search that created the field listing checkbox.
43. Save your workflow action.
44. Verify your workflow action works as expected. Return to the **Search & Reporting app** and search for index=security sourcetype=linux_secure src_ip=* over the **last 24 hours**. (You may need to refresh your browser for the workflow action to appear.)
45. Expand an event with an IP address field and click **Event Actions**.
46. Select Search failed login by IP: {src_ip}
47. A secondary search window should open with the search results for the IP address.

Results Example:

2/6/18 12:33:41.000 PM Tue Feb 06 2018 20:33:41 www2 sshd[1961]: Failed password for invalid user list from 175.44.1.122 port 4130 ssh 2

Event Actions ▾

- Build Event Type
- Get info for IP: 175.44.1.122
- Extract Fields
- Search failed login by IP: 175.44.1.122**
- Show Source

Value	Actions
www2	▾
/opt/log/www2/secure.log	▾
linux_secure	▾
authentication	▾
error	▾

New Search

Save As ▾ Close

index=security sourcetype=linux_secure failed src_ip=175.44.1.122 Last 24 hours ▾ 🔍

✓ 32 events (2/5/18 12:00:00.000 PM to 2/6/18 12:35:10.000 PM) No Event Sampling ▾ Job ▾ || ▮ ↗ ⌵ ⬇ ⚙ Smart Mode ▾

Events (32) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect 1 hour per column

List ▾ ✎ Format 20 Per Page ▾ < Prev 1 2 Next >

< Hide Fields	≡ All Fields	i	Time	Event
SELECTED FIELDS			> 2/6/18 12:33:41.000 PM	Tue Feb 06 2018 20:33:41 www2 sshd[1961]: Failed password for invalid user list from 175.44.1.122 port 4130 ssh 2
a host 4				host = www2 source = /opt/log/www2/secure.log sourcetype = linux_secure
a source 4				tag = authentication tag = error tag = failure tag = os tag = remote tag = unix
a sourcetype 1				