

---

## Lab Exercise 11 : 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 class\_Fund2.
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 **CLASS: Intermediate** 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 or tab 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\\$](http://whois.domaintools.com/$src_ip$).

*Results Example:*

The screenshot shows the Splunk interface. On the left, a search results table displays an event from 'Tue Feb 06 2018 19:09:54' with a message about an accepted password for 'nsharpe' from IP '119.142.102.182'. Below the event, the 'Event Actions' menu is open, and the action 'Get info for IP: 119.142.102.182' is highlighted with a red box. A red arrow points from this action to a secondary window on the right titled 'IP Information for 119.142.102.182'. This window displays 'Quick Stats' and detailed WHOIS information for the IP address, including its location (China), ASN (AS4134 CHINANET-BACKBONE), and various network details.

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:	CB93-AP
tech-c:	IC93-AP
remarks:	service provider
status:	ALLOCATED PORTABLE

**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 **class\_Fund2**.
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 **class\_Fund2**.
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 **CLASS: Intermediate** 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:*

The screenshot illustrates the process of creating a search workflow action. The top part shows the 'Event Actions' menu for a specific event, with 'Search failed login by IP: 175.44.1.122' highlighted. The bottom part shows the 'New Search' window with the search string 'index=security sourcetype=linux\_secure failed src\_ip=175.44.1.122' entered. The search results show 32 events, with the first event expanded to show details like host, source, sourcetype, and tags.

**Event Actions Menu:**

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

**New Search Window:**

Search string: `index=security sourcetype=linux_secure failed src_ip=175.44.1.122`

Results: 32 events (2/5/18 12:00:00.000 PM to 2/6/18 12:35:10.000 PM) No Event Sampling ▼

**Event Details:**

Time	Event
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

**Selected Fields:**

- host 4
- source 4
- sourcetype 1

**Tags:** host = www2 | source = /opt/log/www2/secure.log | sourcetype = linux\_secure | tag = authentication tag = error tag = failure tag = os tag = remote tag = unix