Atomic Fishbowl

Context Menu Actions for NetWitness

Summary

Atomic Fishbowl provides the means to drill directly from the Investigate area of NetWitness back into Atomic Fishbowl. This allows an analyst to visualize individual IP addresses, hostnames, and usernames using Atomic Fishbowl. For this, it will be necessary to create Context Menu Actions in the NetWitness configuration.

Note: Unfortunately, due to limitations in NetWitness, it is not possible at this time to visualize the entire current drillpoint in a NetWitness Investigation. We hope that this will become possible in the future.

Also Note: the screenshots for this procedure are taken from NetWitness 11.3.x. While screenshots from other NetWitness versions may differ slightly, the procedure is substantially the same.

There are five JSON files for which the procedure will need to be performed (provided with this document, in the same directory). The procedure is identical for each of the files. They are:

- **nw-investigation-ad-username-dst-action.json** – Allows an analyst to visualize usernames by putting the username on the **destination** side of Atomic Fishbowl's NetWitness query. E.g. *ad.username.dst = 'someuser'.*
    - It works with the following meta keys:
        - **user.src**
        - **user.dst**
        - **username**
        - **ad.username.src**
        - **ad.username.dst**

- **nw-investigation-ad-username-src-action.json** - Allows an analyst to visualize usernames by putting the username on the **source** side of Atomic Fishbowl's NetWitness query. E.g. *ad.username.src = 'someuser'*
    - It works with the following meta keys:
        - **user.src**
        - **user.dst**
        - **username**
        - **ad.username.src**
        - **ad.username.dst**

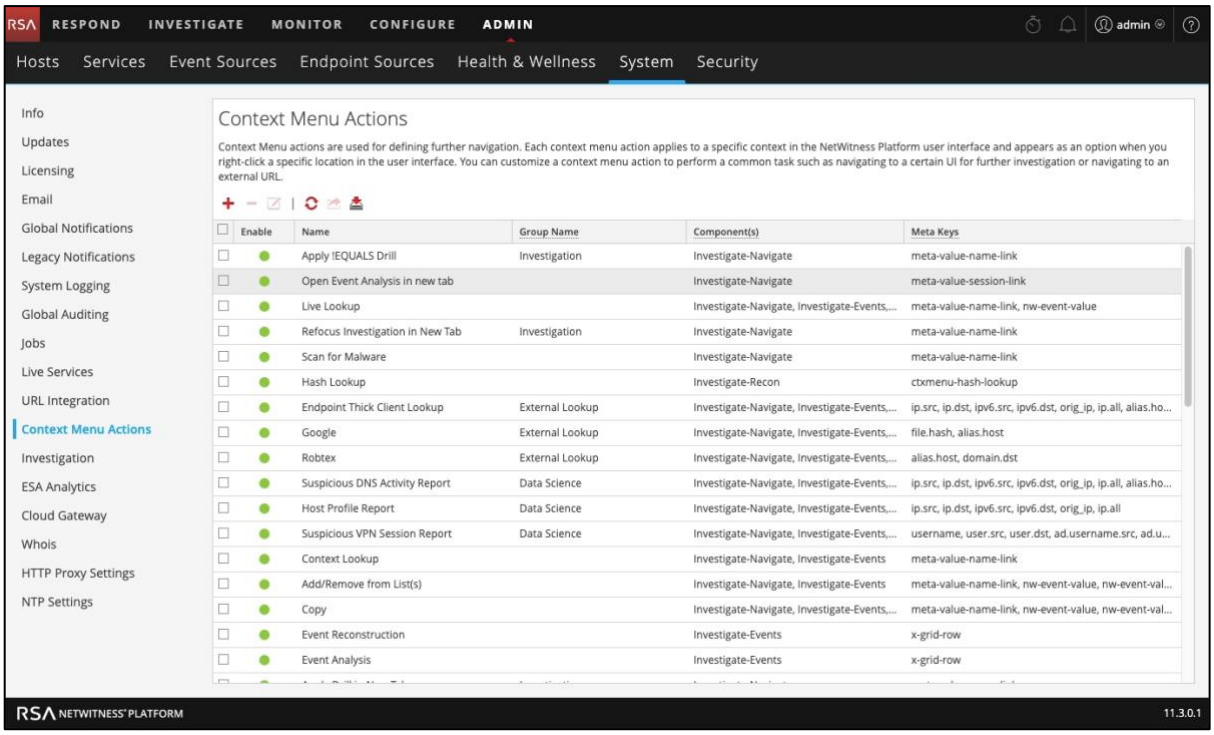
- **nw-investigation-host-action.json** - Allows an analyst to visualize hostnames. E.g. *alias.host = 'somehost'*.
    - It works with the following meta keys:
        - **alias.host**
        - **host.src**
        - **host.dst**

- **nw-investigation-ip-dst-action.json** - Allows an analyst to visualize IP addresses by putting the address on the **destination** side of Atomic Fishbowl's NetWitness query.
    - It works with the following meta keys:
        - ip.src
        - ip.dst
        - orig.ip
        - device.ip
        - ip.addr
        - alias.ip

- **nw-investigation-ip-src-action.json** - Allows an analyst to visualize IP addresses by putting the address on the **source** side of Atomic Fishbowl's NetWitness query.
    - It works with the following meta keys:
        - ip.src
        - ip.dst
        - orig.ip
        - device.ip
        - ip.addr
        - alias.ip

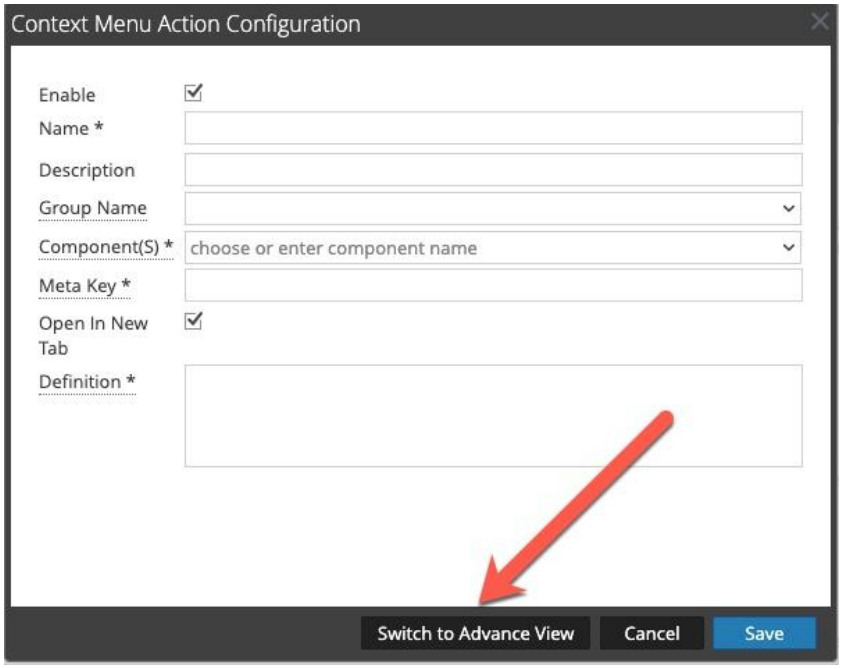
Installation Procedure

1. In the NetWitness user interface, navigate to **Admin > System > Context Menu Actions**.



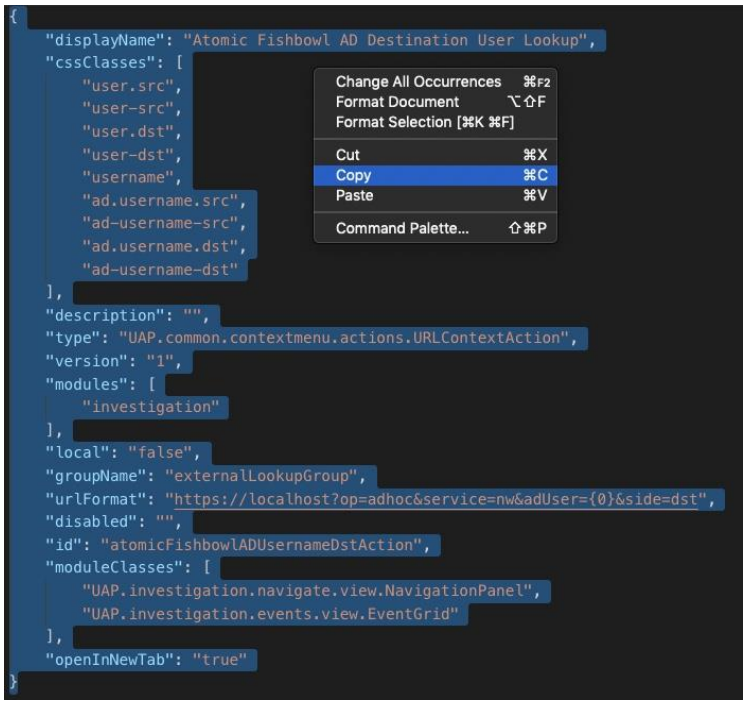
2. Click the '+' sign near the top of the page to add a new context menu definition.

3. Click the “**Switch to Advance View**” button at the bottom of the “Context Menu Action Configuration” dialog.



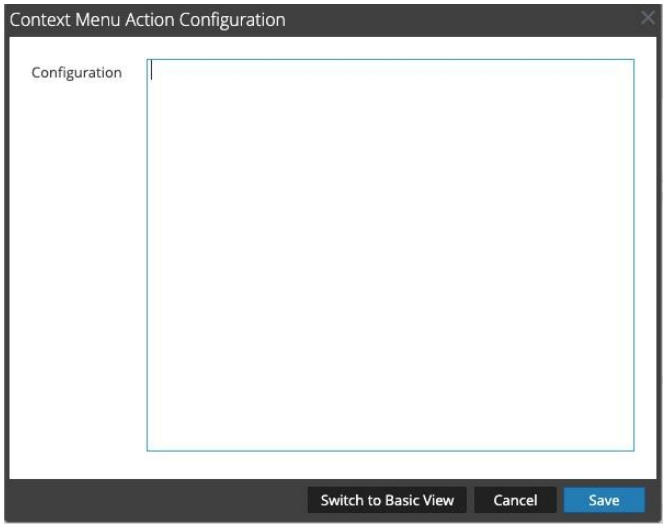
4. From the same directory from which you opened this document, using your favorite text editor (but not Windows Notepad – it doesn’t handle UNIX line breaks properly), open the file **nw-investigation-ad-username-dst-action.json**.

5. Highlight and copy the contents of the JSON file to the clipboard.




```
{
    "displayName": "Atomic Fishbowl AD Destination User Lookup",
    "cssClasses": [
        "user.src",
        "user-src",
        "user.dst",
        "user-dst",
        "username",
        "ad.username.src",
        "ad-username-src",
        "ad.username.dst",
        "ad-username-dst"
    ],
    "description": "",
    "type": "UAP.common.contextmenu.actions.URLContextAction",
    "version": "1",
    "modules": [
        "investigation"
    ],
    "local": "false",
    "groupName": "externalLookupGroup",
    "urlFormat": "https://localhost?op=adhoc&service=nw&adUser={0}&side=dst",
    "disabled": "",
    "id": "atomicFishbowlADUsernameDstAction",
    "moduleClasses": [
        "UAP.investigation.navigate.view.NavigationPanel",
        "UAP.investigation.events.view.EventGrid"
    ],
    "openInNewTab": "true"
}
```

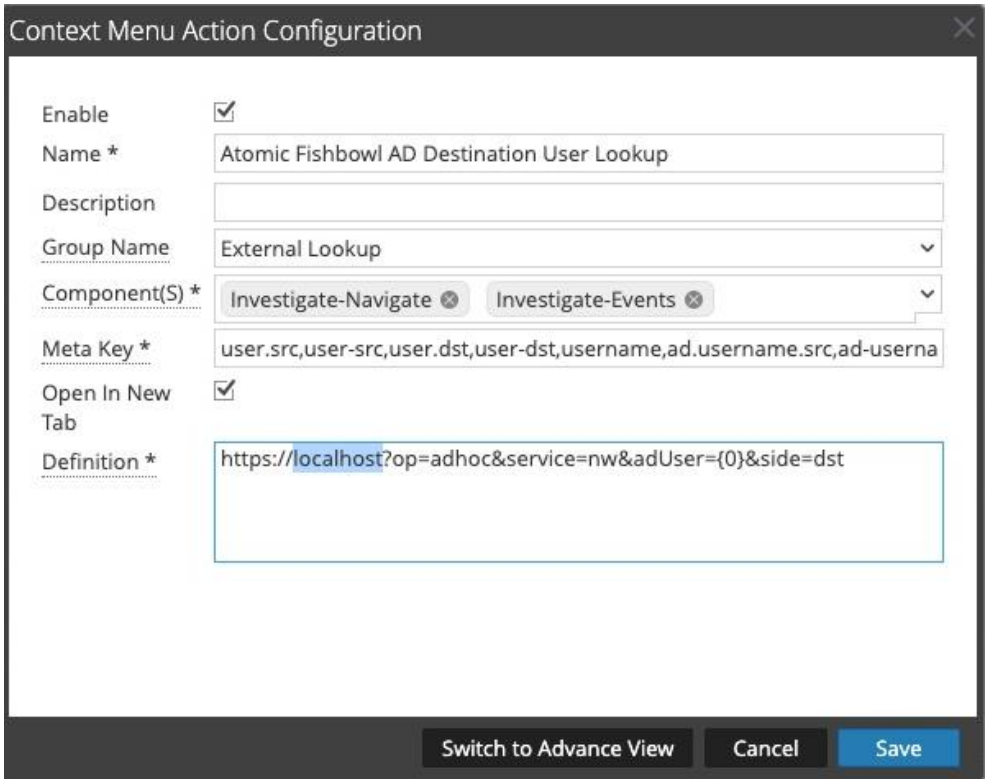
6. Back in NetWitness, highlight the JSON text that's populated by default in the configuration, and press your **delete** key.



7. Paste the Atomic Fishbowl JSON text you copied into the configuration.

8. Click the "**Switch to Basic View**" button.

9. In the Definition box, change the hostname from **localhost** to match the hostname of your Atomic Fishbowl host.



10. Click **Save**.

11. Repeat the procedure for the other **.json** files contained in the archive. When finished, you should be able to observe the actions in the configuration.

Atomic Fishbowl AD Destination User Lo...	External Lookup	Investigate-Navigate, Investigate-Events	user.src, user-src, user.dst, user-dst, username, ad.use
Atomic Fishbowl AD Source User Lookup	External Lookup	Investigate-Navigate, Investigate-Events	user.src, user-src, user.dst, user-dst, username, ad.use
Atomic Fishbowl Host Lookup	External Lookup	Investigate-Navigate, Investigate-Events	alias-host, host-src, host-dst
Atomic Fishbowl Destination IP Lookup	External Lookup	Investigate-Navigate, Investigate-Events	ip-src, ip-dst, orig_ip, device-ip, ip-addr, alias-ip
Atomic Fishbowl Source IP Lookup	External Lookup	Investigate-Navigate, Investigate-Events	ip-src, ip-dst, orig_ip, device-ip, ip-addr, alias-ip

Using the Context Menu Actions

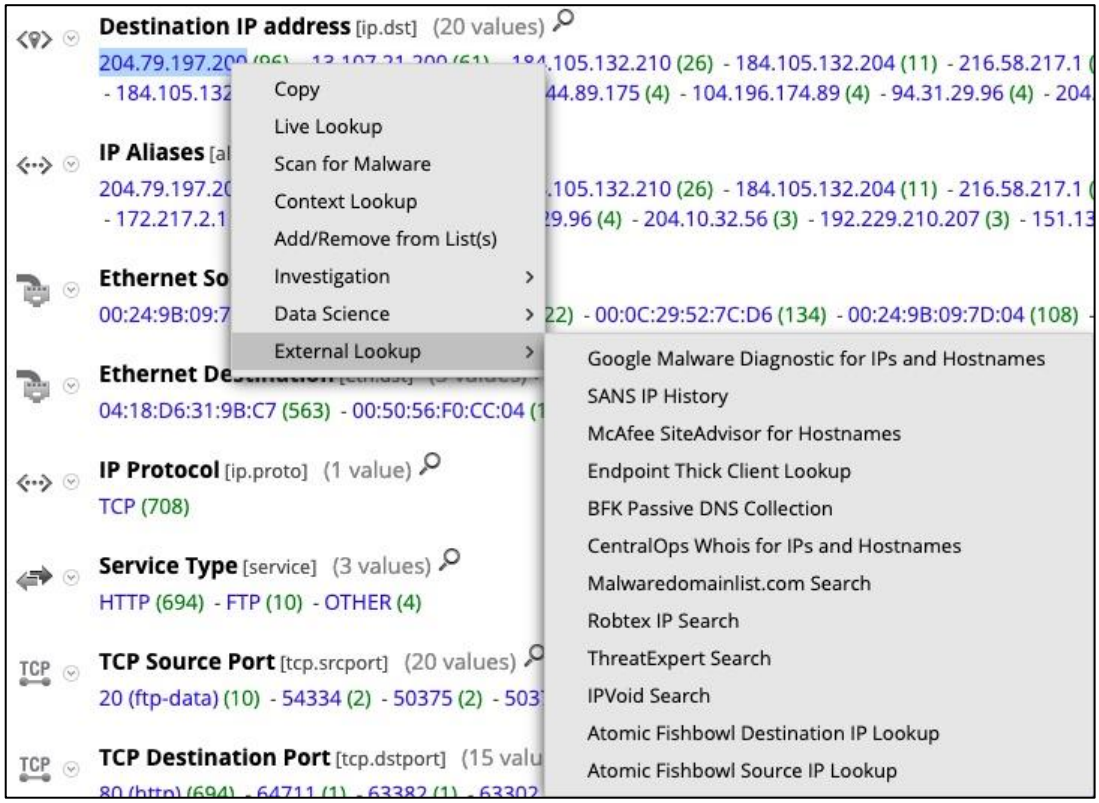
To use the context menu actions that you just installed:

1. Navigate to **Investigate**, choose your data source, load your data, and locate a hostname, IP address, or username that you wish to investigate.

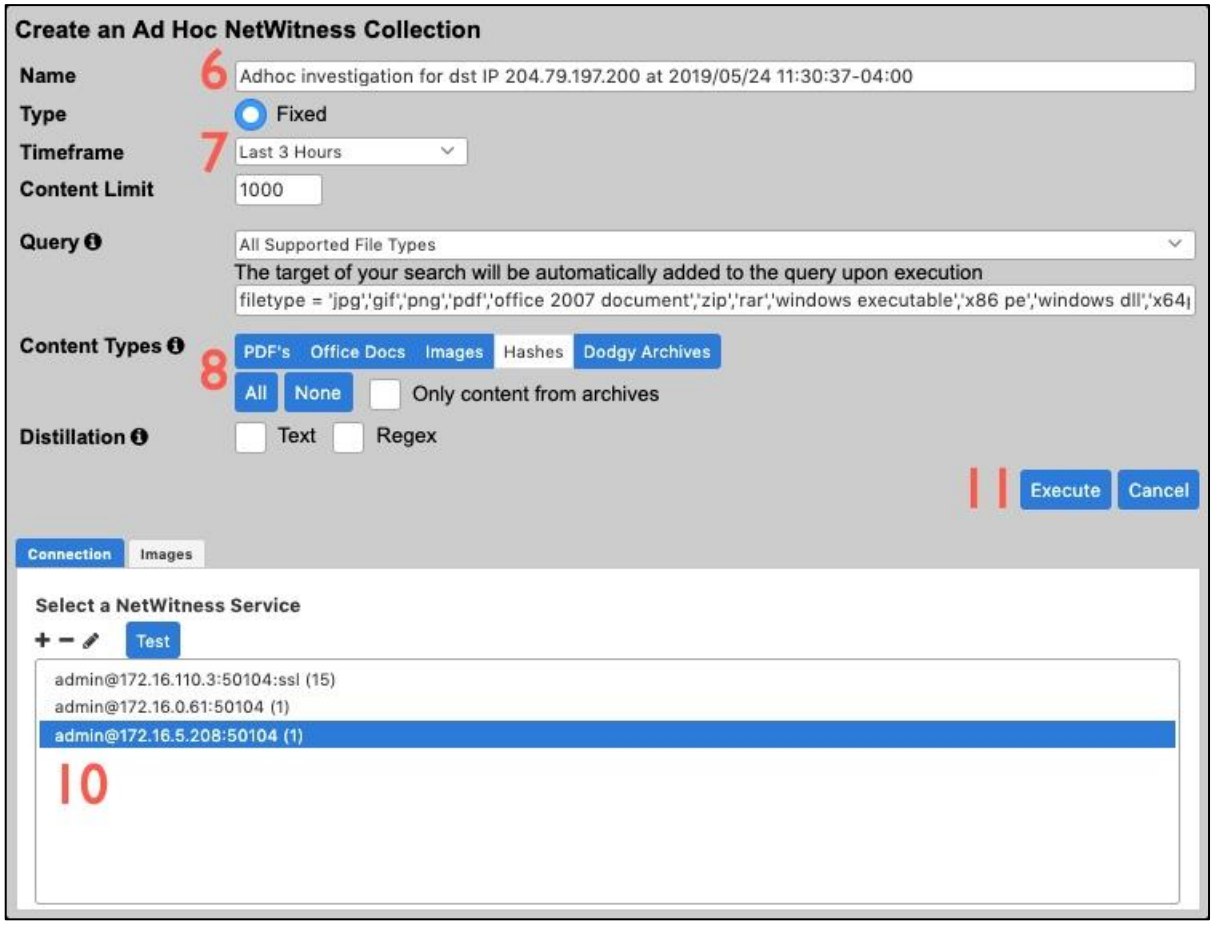
2. Right-click on the value and mouse over **External Lookup**.

3. Assuming all has gone well, you should see the new context menu actions in the menu that's displayed.

   Top Tip: 'Source' and 'Destination' actions will instruct Atomic Fishbowl to search either the '.src' or '.dst' side of a key. I.e. choosing "**Atomic Fishbowl Source IP Lookup**" will cause Atomic Fishbowl to add the chosen address to its NetWitness query as **ip.src**. Choosing "**Atomic Fishbowl Destination IP Lookup**" will use meta key **ip.dst**, and so on.



4. Click on one of them.



5. Atomic Fishbowl will now open in a new browser tab. It will display a dialog which will prompt the analyst to create an Ad Hoc collection.

   TOP TIP: An Ad Hoc collection is the same as a Fixed collection, with some key differences:

   a. Use cases aren't available.
   b. The query you see will not actually contain the host, IP address, or username you selected in NetWitness. It will automatically be appended to the query when the collection is executed.

6. A default name is provided, but it can be changed if so desired.

7. Select a timeframe for the query.

8. Customize the types of content that you wish to be pulled into the collection, or you can accept the defaults.

9. Customize any other collection parameters that you so desire.

10. Select a NetWitness service to perform the query on.

11. Click the **Execute** Button.

12. Atomic Fishbowl will now build a fixed collection based on the target you selected from within NetWitness.