Vertex

Synapse Bootcamp - Module 22

Views, Layers, and Quorum - Exercises

Objectives

In these exercises you will:

- Obtain information about a view and its layers
- Use the ANATOMY tab to see which components of a node reside in which layer
- Use Synapse tools and features to view differences between a view's write layer and the underlying layers
- Use Synapse commands and features to merge data into an underlying layer

Note: We are constantly updating Synapse and its Power-Ups! We do our best to make sure our course documents (slides, exercises, and answer keys) are up-to-date. However, you may notice small differences (such as between a screen capture in the documents and the appearance of your current instance of Synapse).

If something is unclear or if you identify an error, please reach out to us so we can assist!

Exercises

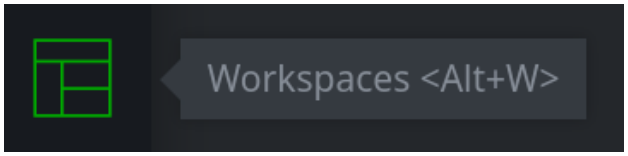
Views and Layers

Exercise 1

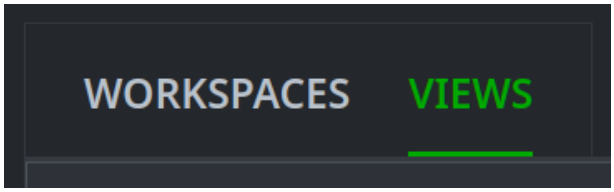
Objective:
- **Obtain information about a view and its layers.**

You want to examine the composition of views in your Synapse demo instance.

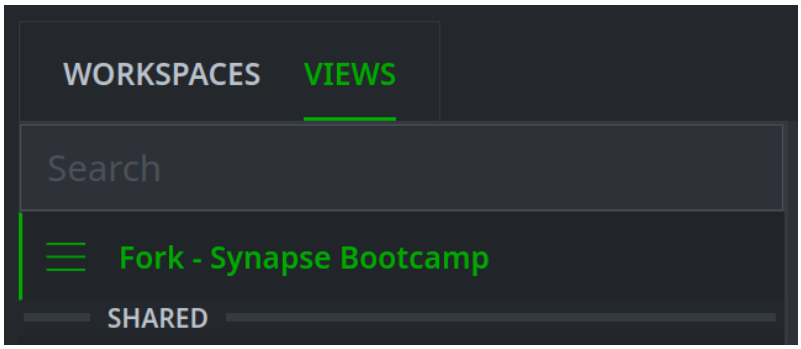
- From your **Toolbar,** select the **Workspaces Tool:**



- In the **Workspaces Tool,** click on the **VIEWS** tab:

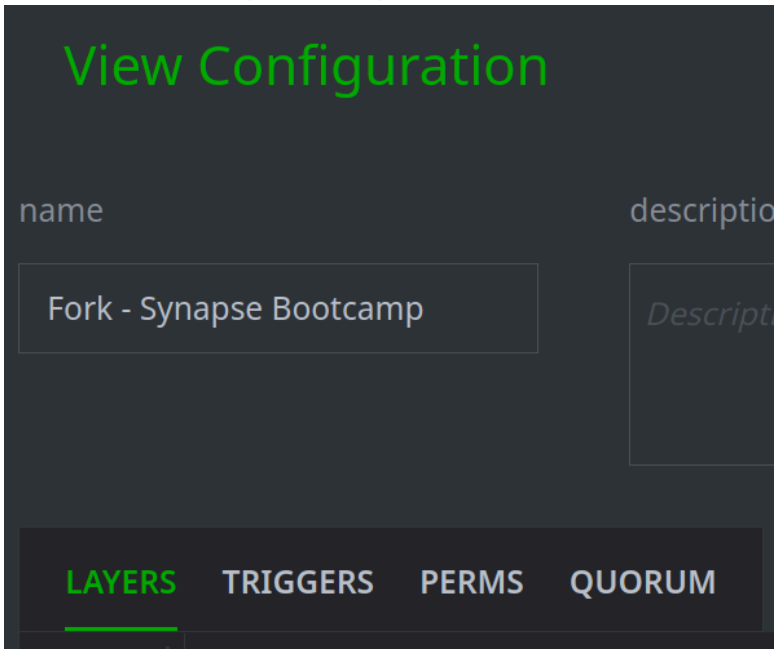


- On the **VIEWS** tab, from the **View List,** select your **Fork - Synapse Bootcamp** view:



Tip: You may have given your forked view a different name. Just ensure you select your fork.

- In the **View Configuration** panel, select the **LAYERS** tab:



Question 1: How many layers are in your forked view?

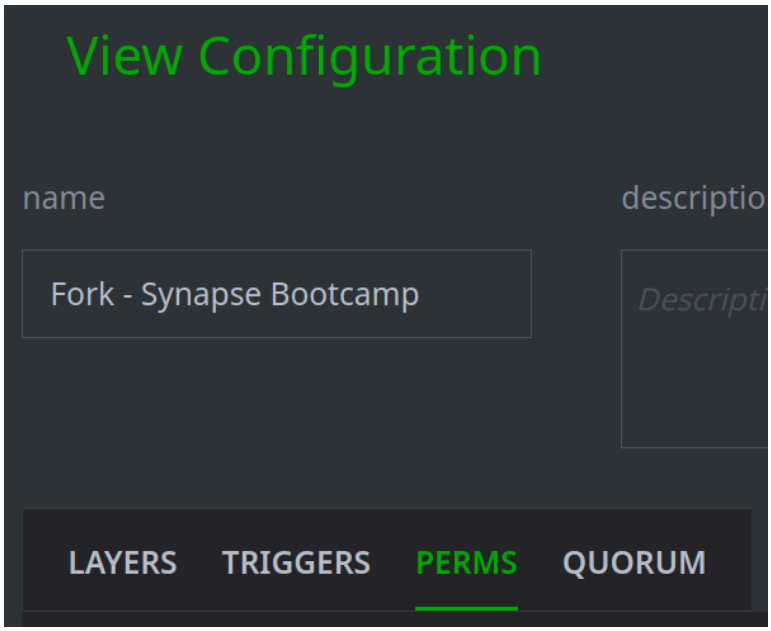
Question 2: Which layer contains the most data (by size)?

Question 3: Who is the owner of the Synapse Bootcamp layer?

Question 4: Who is the owner of the Fork - Synapse Bootcamp layer?

Now you want to view permissions associated with this view.

- In the **View Configuration** panel, select the **PERMS** tab:



Question 5: What user(s) and/or role(s) have access to the Fork - Synapse Bootcamp view?

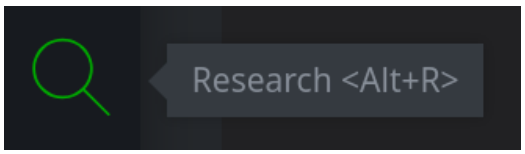
Exercise 2

Objective:

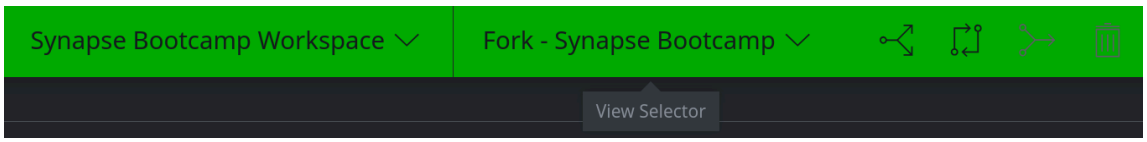
- **Use the ANATOMY tab to see which components of a node reside in which layer.**

You want to examine a node to see where its properties and tags reside.

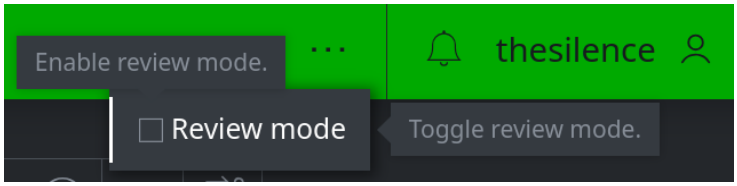
- In the **Toolbar,** select the **Research Tool:**



- In the **View Selector,** ensure that your **Fork - Synapse Bootcamp** view is selected:



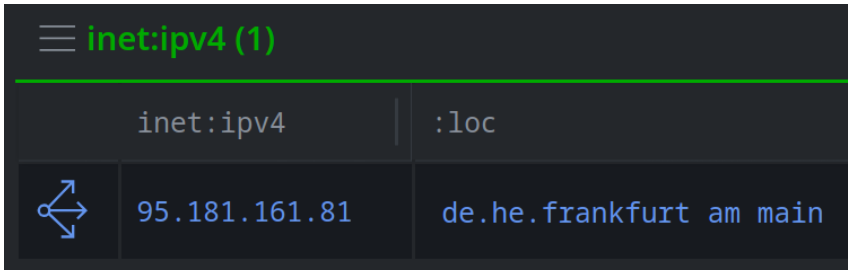
- In the **Top Bar,** click the **meatball menu** (three horizontal dots) and toggle **Review mode** to **ON:**



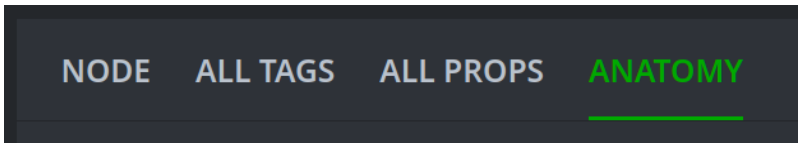
- In the **Storm Query Bar,** enter the following and press **Enter** to lift the specified IPv4 address:

```
inet:ipv4=95.181.161.81
```

- In the **Results Panel, select** the node:



- In the **Details Panel,** select the **ANATOMY** tab:



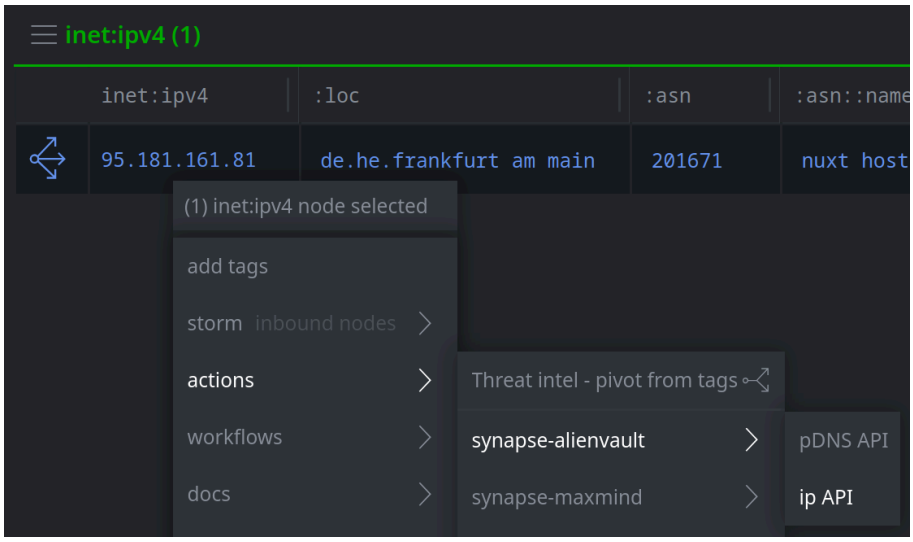
Question 1: In which view/layer does the inet:ipv4 node reside?

Question 2: In which view/layer does the #rep.talos.muddywater tag reside?

Question 3: For this inet:ipv4 node, which properties differ between the APT1 Scavenger Hunt layer and the Synapse Bootcamp layer?

Now we'll add some data to our current forked view to see what changes.

- In the **Results Panel, right-click** the `inet:ipv4` node and select **actions > synapse-alienvault > ip API:**



Question 4: For this inet:ipv4 node, what new (or changed) properties / tags now reside in your Fork - Synapse Bootcamp layer?

Exercise 3

Objective:

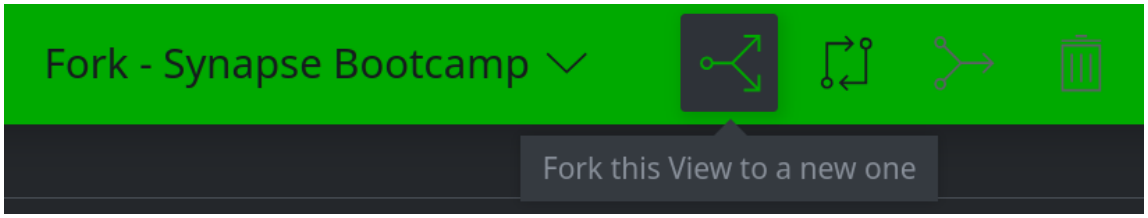
- **Use Synapse tools and features to view differences between a view's write layer and the underlying layers.**

Part 1

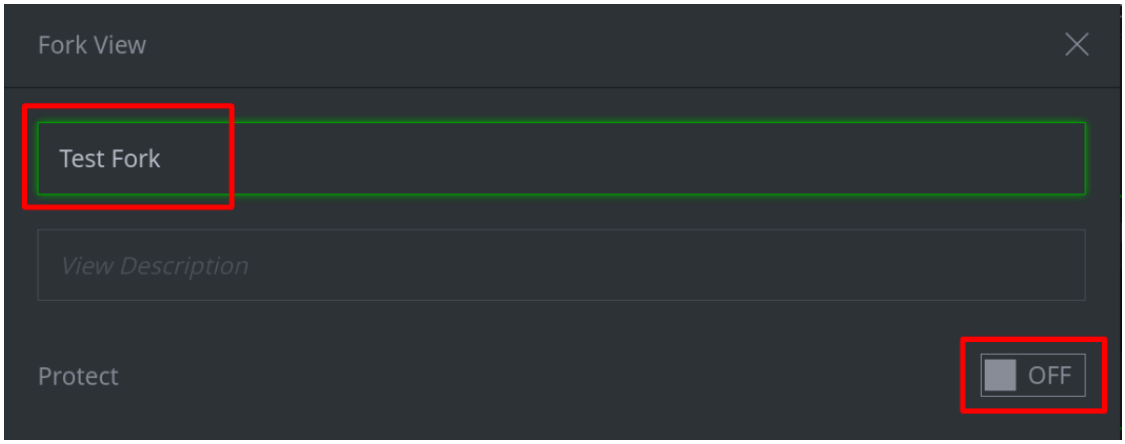
Create a temporary fork of your Synapse Bootcamp fork.

- Ensure that your **Fork - Synapse Bootcamp** view is selected in the **View Selector:**

- In the **View Task Bar,** click the **fork icon** to create a new fork:

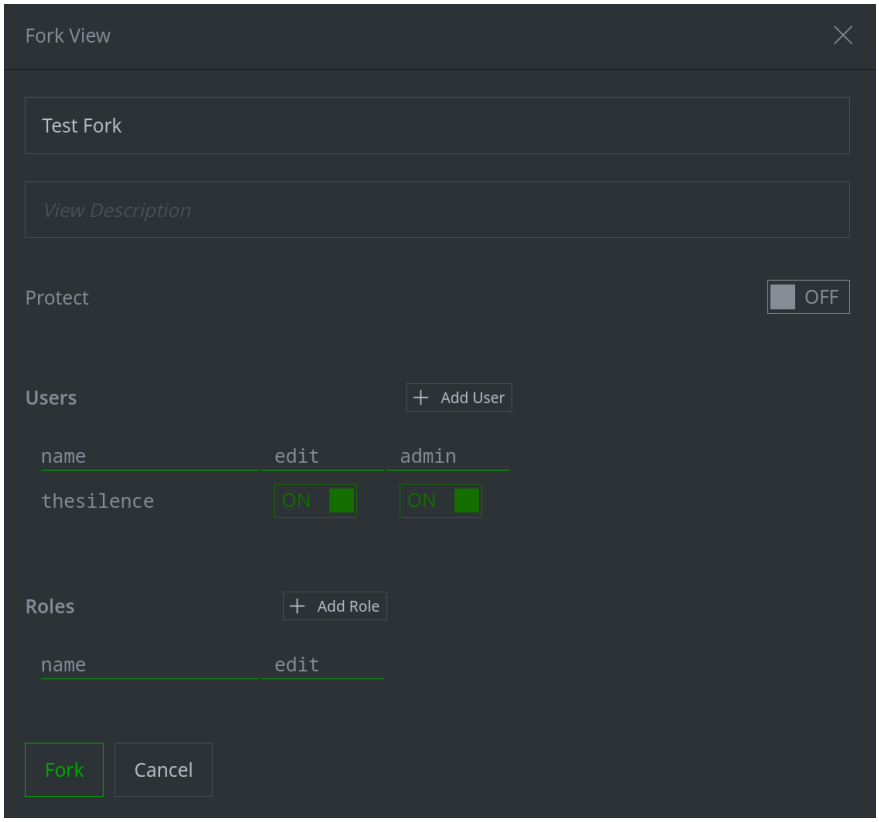


- In the **Fork View** dialog, in the *View Name* field, enter the name **Test Fork.** Leave the **Protect** toggle to **OFF:**



> **Note:** Normally, it's a good idea to protect your fork! We'll leave it off for this exercise to save us a few steps later.

- Click the **Fork** button to create the fork:



Tip: Review mode should still be enabled from the previous exercise. This will help you to visualize the changes we'll make during the next part of this exercise.

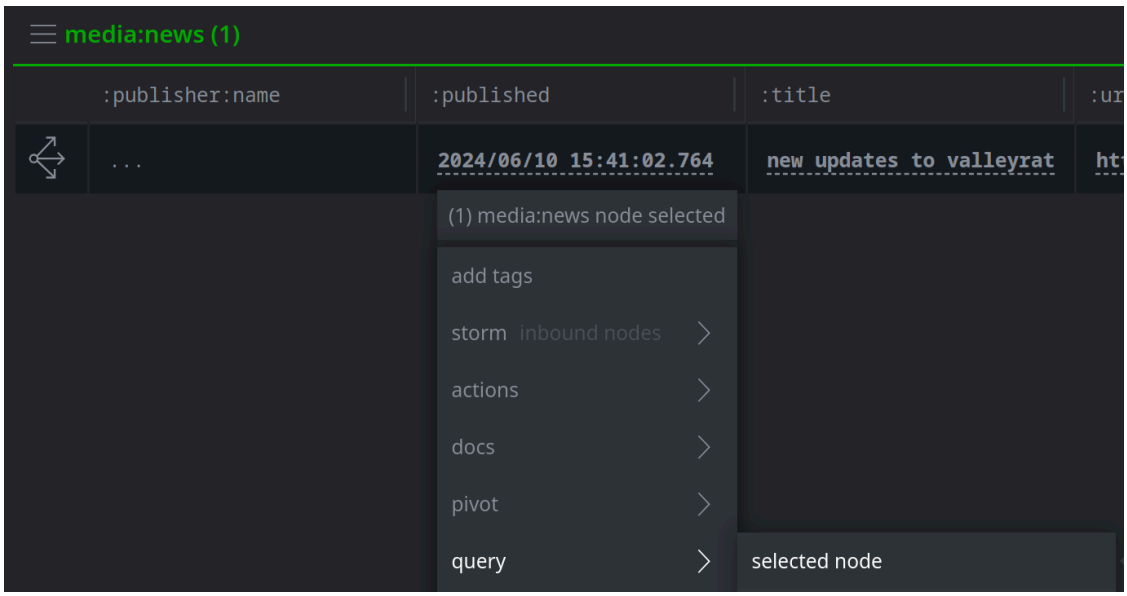
Part 2

Run Power-Ups to simulate performing research and analysis in your fork.

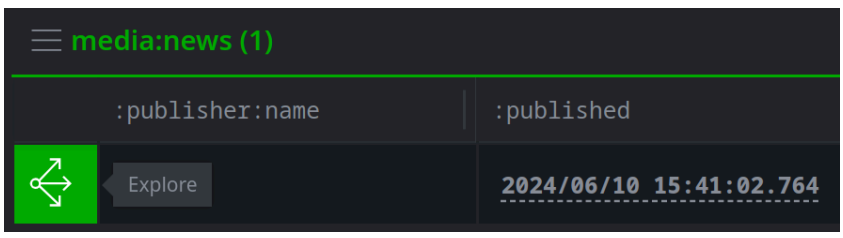
- In the **Research Tool,** in the **Storm Query Bar,** enter the following and press **Enter** to retrieve the specified pulse from AlienVault:

```
alienvault.otx.pulses.byid 66671e8ed37c903dcf36edbd --yield
```

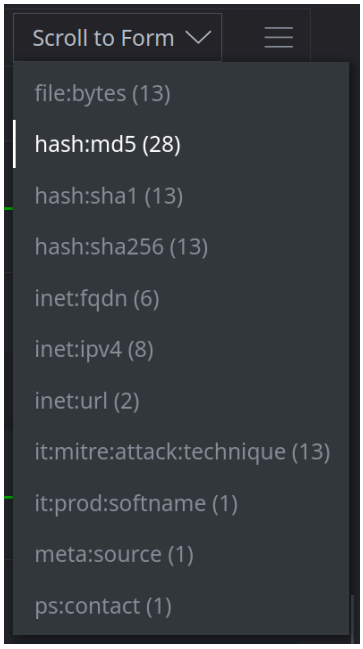
- In the **Results Panel, right-click** the media:news node and select **query > selected node** to lift the new `media:news` node:



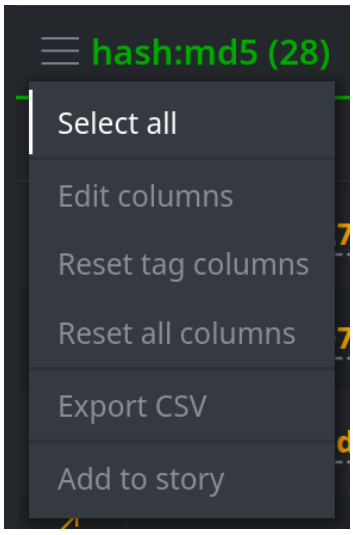
- Click the **Explore button** next to the **`media:news`** node to navigate to adjacent nodes:



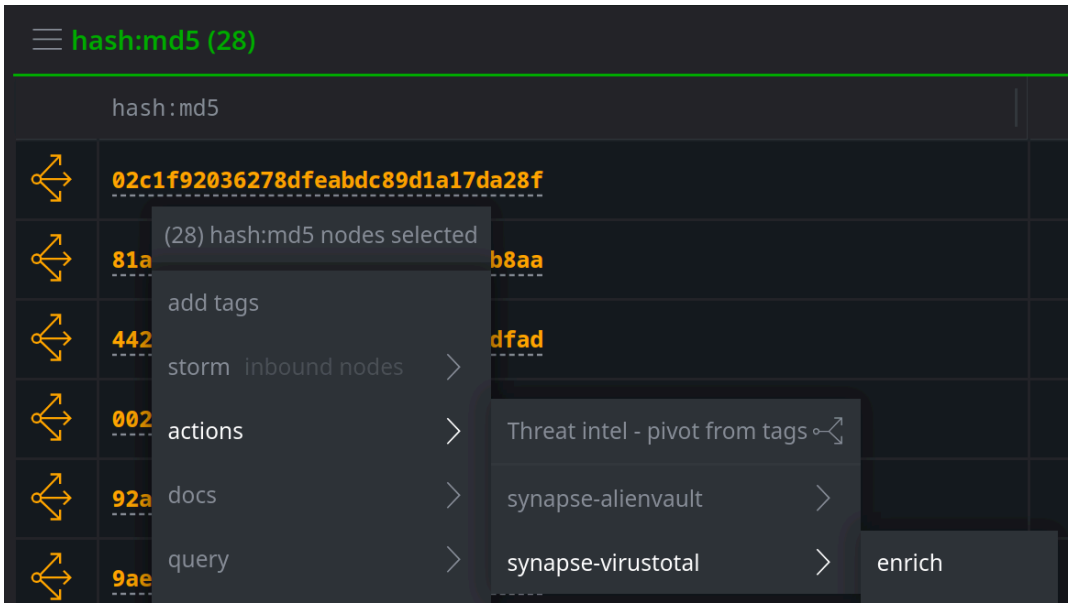
- Click the **Scroll to form** button and select **hash:md5** to navigate to the `hash:md5` nodes:



- Click the **hamburger menu** next to the **hash:md5** header and choose **Select all:**



- **Right-click** any of the selected nodes and select **actions > synapse-virustotal > enrich** to retrieve any available information about the hashes from VirusTotal:



- Wait for the enrichment to complete (it may take a minute or so, depending on the current information available from VirusTotal).

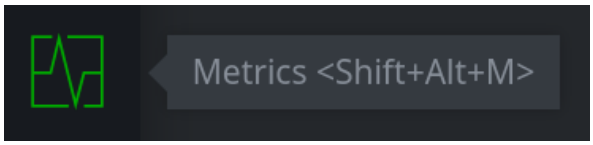
> **Note:** you may see some warning messages - for example, if VirusTotal does not have any information about some of the hashes. This is fine.

Part 3

Metrics Tool

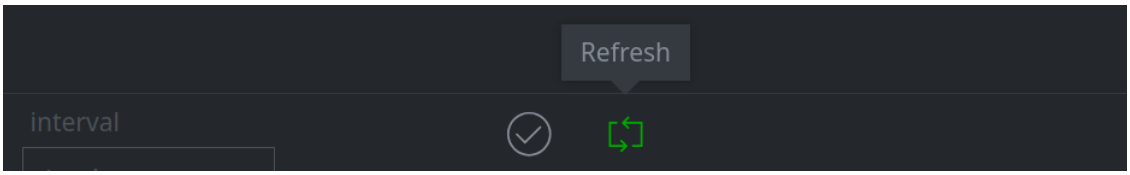
Use the Metrics Tool to examine changes made in your forked view.

- In the **Toolbar,** select the **Metrics Tool:**

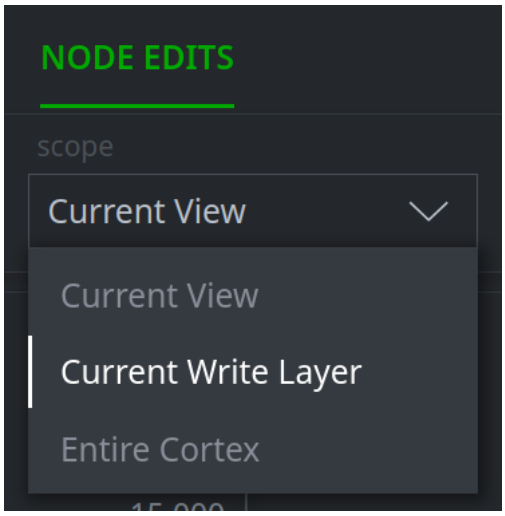


Question 1: What are the default scope and timerange used for the metrics display?

Tip: The Metrics data should display automatically. If for some reason it does not, click the **Refresh** button in the top center of the display:



- Use the **scope** selector to change the scope to **Current Write Layer:**



- View the **high-level information** about changes made using the **top half** of the Metrics Tool.

  Question 2: How many changes in total were made to the current write layer?

- View the **detailed information** about the various changes in the **bottom half** of the Metrics Tool.

  Question 3: What is the default breakdown for how changes are displayed?

- Use the **breakdown** selector to examine some of the different options for displaying changes.
  - Note how the information displayed changes as you select different options.
  - Try hovering over sections of the histogram (bar chart) bars to see what is displayed.

- Try navigating the sunburst chart to see how you can drill down into various changes.

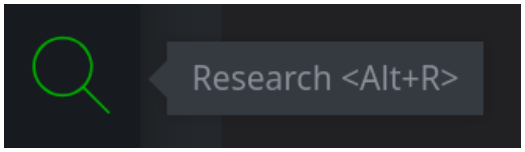
Tip: The Metrics Tool is useful for getting a high-level overview of changes in a layer. This may help you scope what needs to be reviewed before reviewing and merging it.

The Metrics Tool is also useful for simply getting an idea of the changes occurring in your Cortex. Some analysts use it as an informal "leaderboard" to see who is generating the most data / analysis in Synapse!

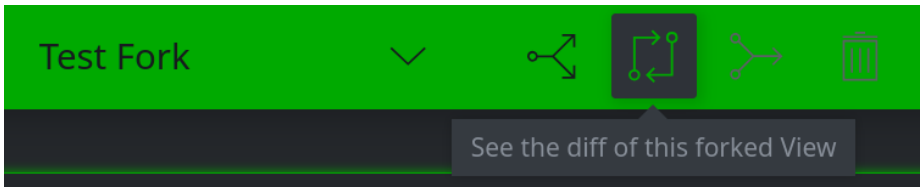
Diff Icon - View Task Bar

Next we want to use the diff icon in the View Task Bar to examine changes made in our forked view.

- In the **Toolbar,** select the **Research Tool:**

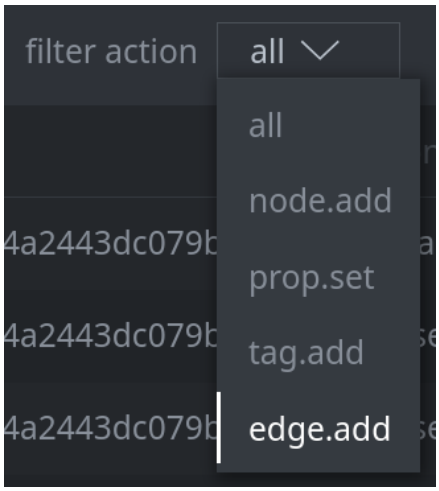


- In the **View Task Bar,** click the **diff icon** to open the **Layer Merge Diff** window:



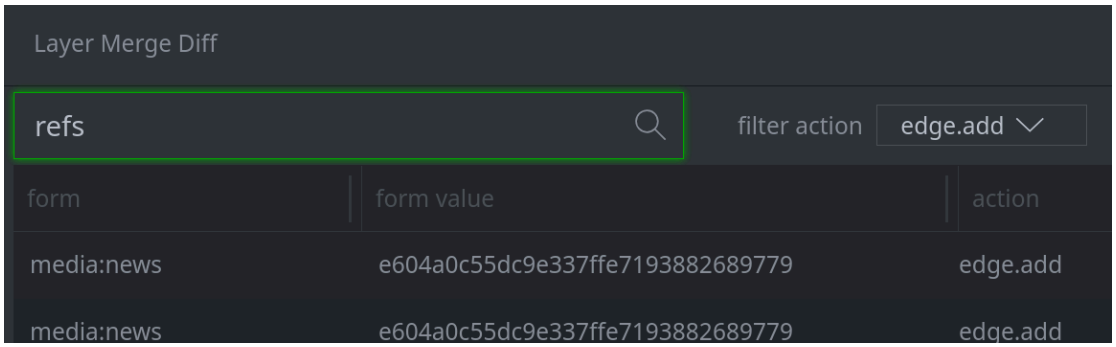
Question 4: How many total edits were made in this layer?

- In the **Layer Merge Diff** window, use the **filter action** selector to choose **edge.add** to see edges that were created in this layer:



Question 5: What kinds of edges (edge names) were created?

- In the **Layer Merge Diff** window, in the **search** field, enter **refs** to limit the edges displayed to `refs` edges:



Question 6: How does the number of edits change after you enter the search term? How many nodes were modified by creating `refs` edges?

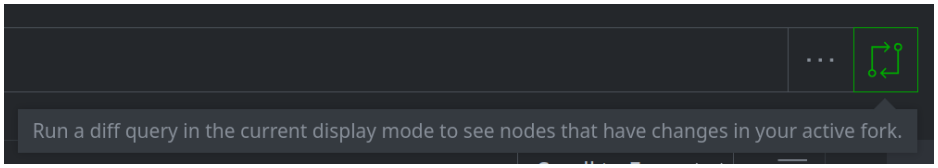
- Spend some time examining the options for viewing changes using the **Layer Merge Diff** window.
  - Try choosing other options using the **filter action** selector (you may need to **clear** your search field).
  - Use the **search** field (on its own or with the filter action selector) to narrow the visible results.
  - Try **sorting** the display using the various column headers.
  - Use the **right-click** context menu to query or examine nodes in the Research Tool.

- When you are finished, click the **X** in the upper right to exit the Layer Merge Diff window to close the window.

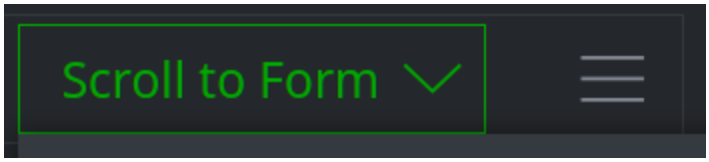
Diff Icon - Storm Query Bar

Use the diff icon in the Storm Query Bar to examine changes made in your forked view.

- In the **Research Tool,** in the **Storm Query Bar,** click the **diff icon** to load and run the `diff` Storm command:

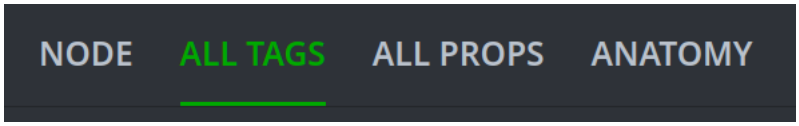


- Click the **Scroll to form** button to get an overview of the kinds of nodes that were created or modified in your forked layer/view:



Question 7: What kinds of forms were created by the AlienVault and VirusTotal Power-Ups?

- In the **Details Panel,** select the **ALL TAGS** tab to view all of the tags present on the changed nodes:



Question 8: What kinds of tags are present on the nodes?

Exercise 4

Objective: • **Use Synapse commands and features to merge data into an underlying layer.**

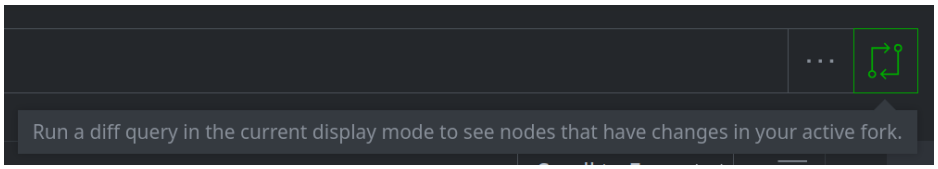
Part 1

When reviewing changes, you (or your organization) may decide that only a **subset** of data and analysis requires vetting by a human user. These "higher value" changes may include things like:

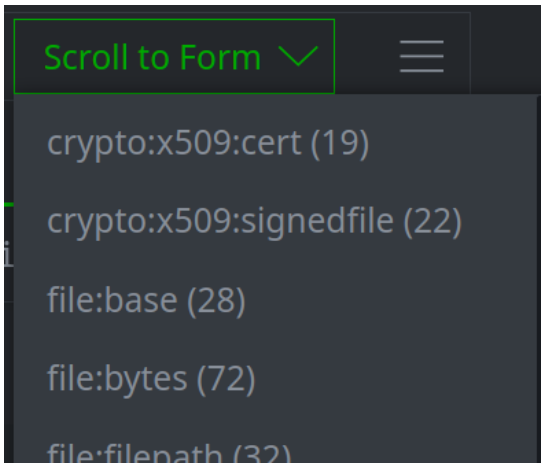
- nodes that are manually modeled (e.g., organizations / `ou:org` nodes, various `risk:*` nodes) to ensure they have been created properly; or
- newly applied tags representing your own analytical assessments.

We want to use the **`diff`** and **`merge`** commands to merge the data we don't care about so that only a subset of data remains in our forked view for further review.

- In the **Research Tool,** in the **Storm Query Bar,** click the **diff icon** to load and run the **`diff`** Storm command:



- Click the **Scroll to form** button to get an overview of the kinds of nodes that were created or modified:



Note that there are two **`syn:tag`** nodes in the list (at the very bottom):

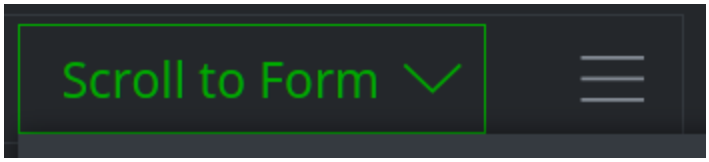
We want to **review** any **`syn:tag`** nodes (e.g., to ensure they have definitions set). We also want to review any **tags applied to nodes** in our forked layer, although it is fine to merge the nodes themselves (i.e., merge the data, but keep the "analysis" in our fork for further vetting).

- In the **Query Bar,** enter the following query and press **Enter** to send the output of the `diff` command (the new or modified nodes) to the `merge` command with the `--no-tags` option:

```
diff | merge --no-tags
```

> **Note:** by default, the `merge` command **does not** merge changes; it simply returns the nodes that **would** be affected by the merge command, so that you can review your results. (In addition, a detailed list of every change to be made, based on your command, is output in the Console Tool.)
>
> To **actually** merge the changes, you need to add the **`--apply`** switch to the `merge` command.

- When the query completes click the **Scroll to form** button to view the nodes returned by the query:



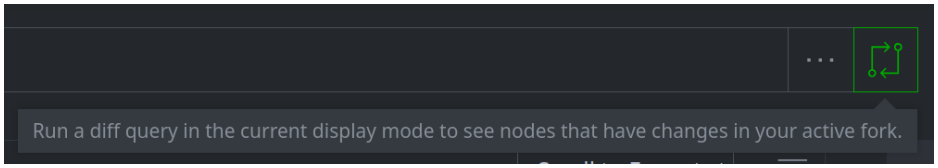
Question 1: Are the syn:tag nodes present in the output?

Perform the partial merge that you just tested.

- In the **Query Bar,** enter the following query and press **Enter** to **run** (apply) the specified `merge`:

```
diff | merge --no-tags --apply
```

- When the query completes, in the **Storm Query Bar,** click the **diff icon** to load and run the **`diff`** Storm command:



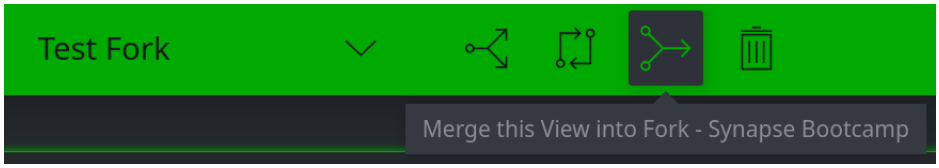
Question 2: How many nodes are returned by the command?

Part 2

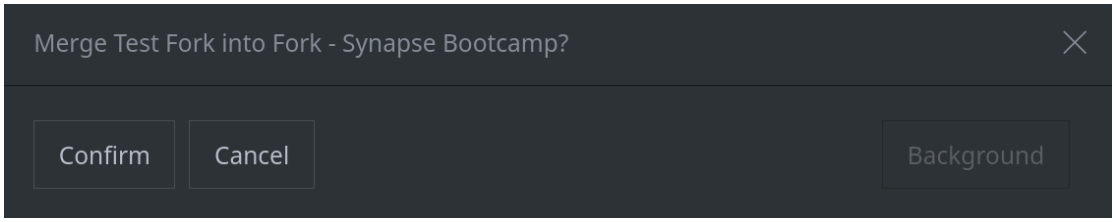
Use the merge icon to merge the remaining changes.

Once any remaining changes have been reviewed and approved, you can merge the changes and delete the fork using the merge icon.

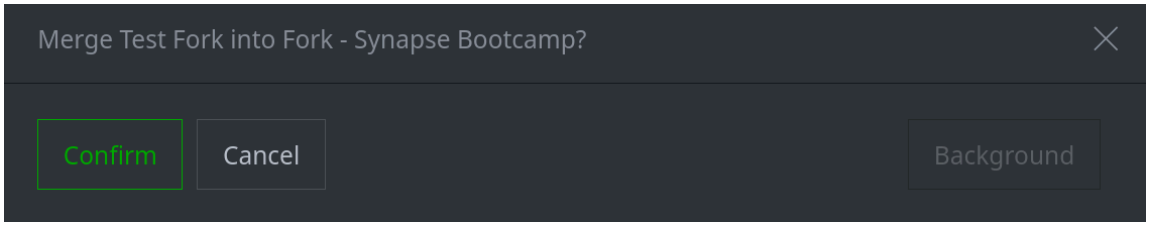
- In the **Research Tool,** in the **View Task Bar,** click the **merge icon:**



- Review the popup dialog:



- Click the **Confirm** button to perform the merge:



Question 3: What happens when you click the Confirm button?
