Synapse Bootcamp - Module 5

Power-Ups - Exercises

Objectives

Note: Prior to the start of this course, you received an email with instructions to register for several free API keys to be used in this course. You will need those API keys for this set of exercises (and the remainder of the course).

In these exercises you will learn:

- How to locate information about Installed and Available Power-Ups
- How to install and update Power-Ups
- How to configure a Power-Up API key
- How to use Power-Ups to enrich data
- How to explore data ingested by Power-Ups

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

Installing Power-Ups

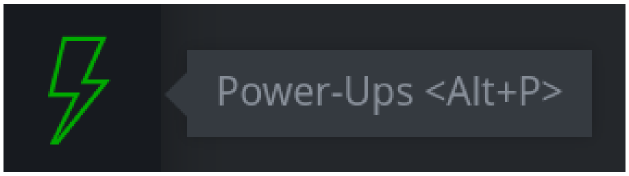
Exercise 1

Objective:

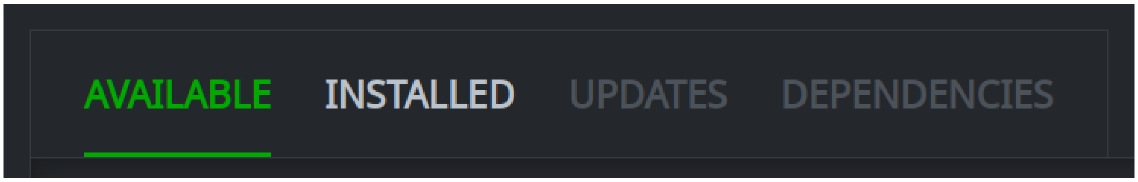
- **Understand how to view and install Power-Ups.**

Install the **synapse-virustotal** Power-Up.

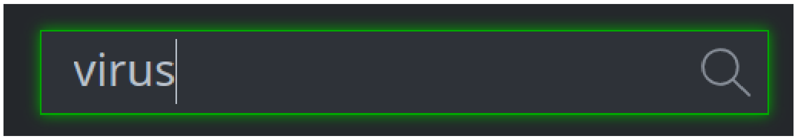
- From your **Toolbar,** select the **Power-Ups Tool:**



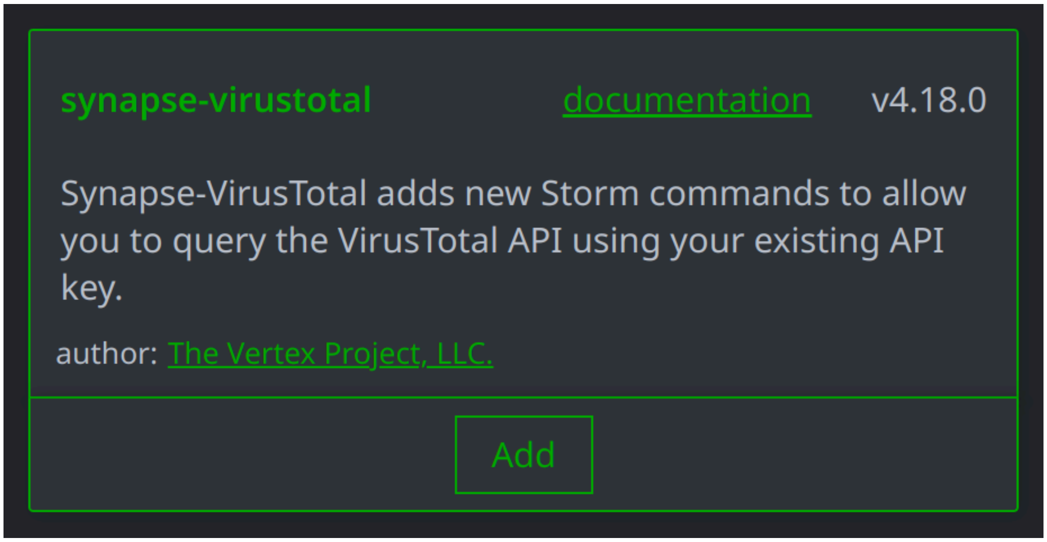
- In the Power-Ups Tool, click the **AVAILABLE** tab:



- Locate the **synapse-virustotal** Power-Up. (You can use the **Search** bar to easily locate it.):


virus

- Click the **Add** button to install the Power-Up:

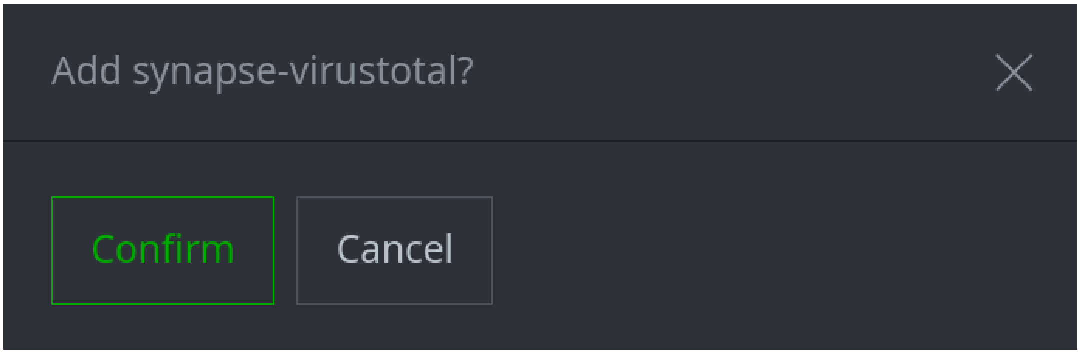


synapse-virustotal documentation v4.18.0

Synapse-VirusTotal adds new Storm commands to allow you to query the VirusTotal API using your existing API key.

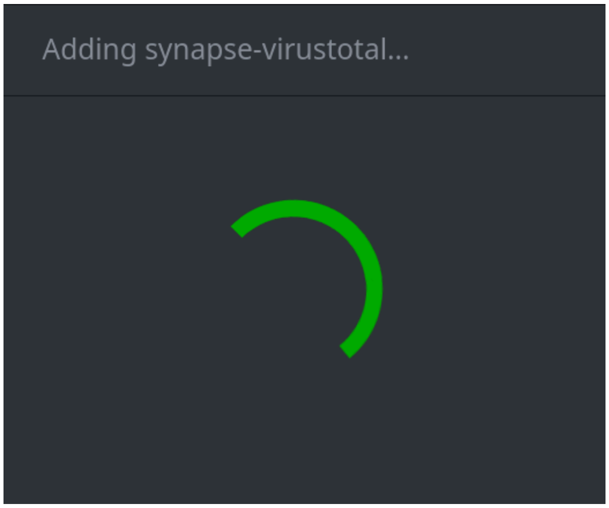
author: The Vertex Project, LLC.

- Click **Confirm** to continue:



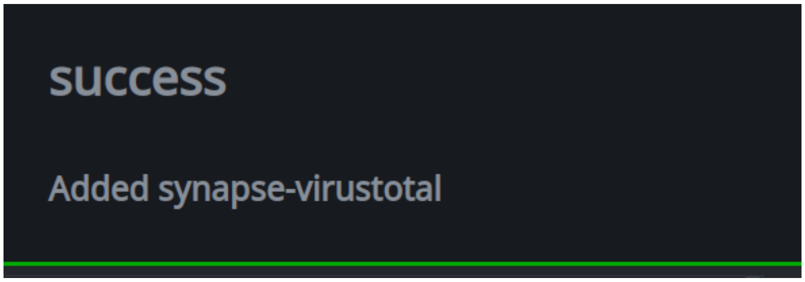
Add synapse-virustotal?

- You will see a progress window while the Power-Up is installed:



Adding synapse-virustotal...

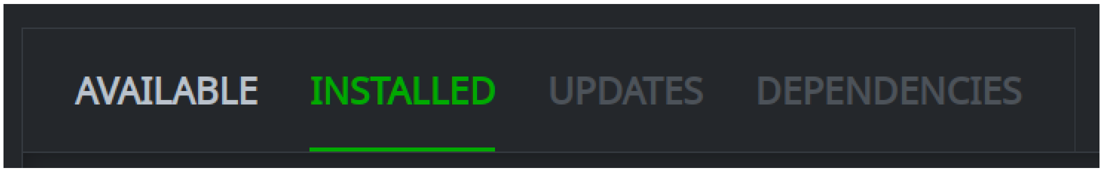
- You will see a pop-up ("toast") message when the installation completes:



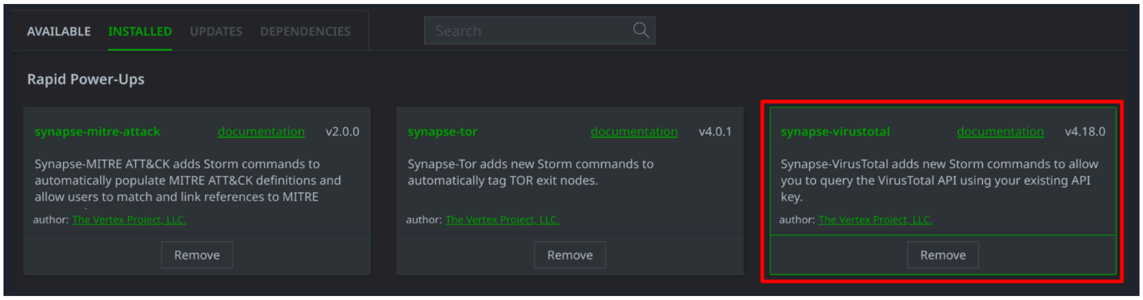
success

Added synapse-virustotal

- Click the **INSTALLED** tab:



- Confirm that the **synapse-virustotal** Power-Up appears on the tab:



Rapid Power-Ups

synapse-mitre-attack documentation v2.0.0

Synapse-MITRE ATT&CK adds Storm commands to automatically populate MITRE ATT&CK definitions and allow users to match and link references to MITRE

author: The Vertex Project, LLC

Remove

synapse-tor documentation v4.0.1

Synapse-Tor adds new Storm commands to automatically tag TOR exit nodes.

author: The Vertex Project, LLC

Remove

synapse-virustotal documentation v4.18.0

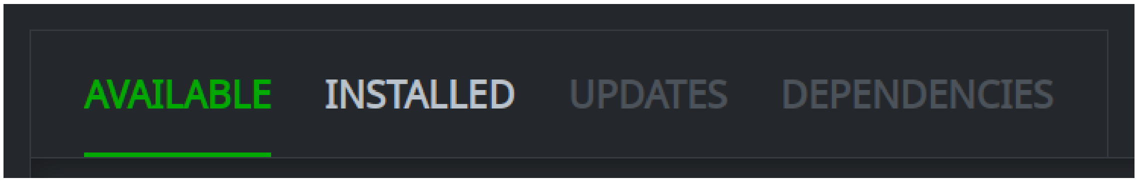
Synapse-VirusTotal adds new Storm commands to allow you to query the VirusTotal API using your existing API key.

author: The Vertex Project, LLC

Remove

Install additional Power-Ups.

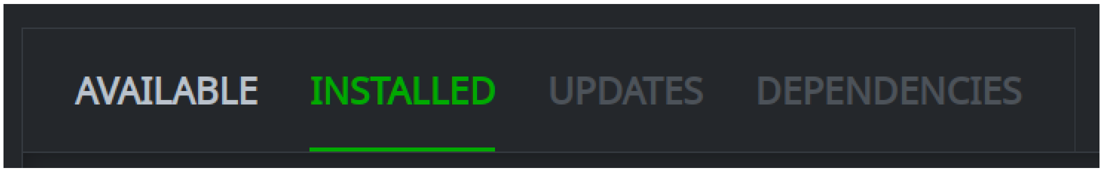
- Click the **AVAILABLE** tab:



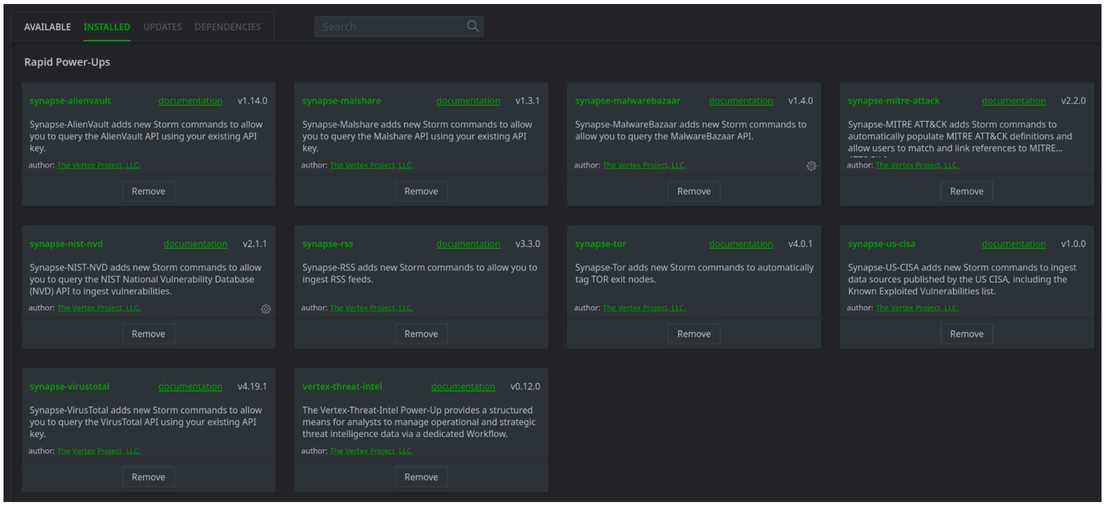
- **Repeat** the previous steps to install the following Power-Ups:
  - **synapse-alienvault** (AlienVault OTX / LevelBlue)
  - **synapse-malshare** (MalShare)
  - **synapse-malwarebazaar** (Abuse.ch MalwareBazaar)
  - **synapse-nist-nvd** (NIST National Vulnerability Database)
  - **synapse-rss** (Synapse RSS feed ingester)

  - **synapse-us-cisa** (US CISA Known Exploited Vulnerabilities)
  - **vertex-threat-intel** (Vertex Threat Intel Workflow)

- When you finish, click the **INSTALLED** tab:



- Confirm the Power-Ups have been installed:



Rapid Power-Ups

synapse-alienvault documentation v1.14.0
Synapse-AlienVault adds new Storm commands to allow you to query the AlienVault API using your existing API key.
author: The Vertex Project, LLC.

synapse-malshare documentation v1.3.1
Synapse-Malshare adds new Storm commands to allow you to query the Malshare API using your existing API key.
author: The Vertex Project, LLC.

synapse-malwarebazaar documentation v1.4.0
Synapse-MalwareBazaar adds new Storm commands to allow you to query the MalwareBazaar API.
author: The Vertex Project, LLC.

synapse-mitre-attack documentation v2.2.0
Synapse-MITRE ATT&CK adds Storm commands to automatically populate MITRE ATT&CK definitions and allow users to match and link references to MITRE...
author: The Vertex Project, LLC.

synapse-nist-nvd documentation v2.1.1
Synapse-NIST-NVD adds new Storm commands to allow you to query the NIST National Vulnerability Database (NVD) API to ingest vulnerabilities.
author: The Vertex Project, LLC.

synapse-rss documentation v3.3.0
Synapse-RSS adds new Storm commands to allow you to ingest RSS feeds.
author: The Vertex Project, LLC.

synapse-tor documentation v4.0.1
Synapse-Tor adds new Storm commands to automatically tag TOR exit nodes.
author: The Vertex Project, LLC.

synapse-us-cisa documentation v1.0.0
Synapse-US-CISA adds new Storm commands to ingest data sources published by the US CISA, including the Known Exploited Vulnerabilities list.
author: The Vertex Project, LLC.

synapse-virustotal documentation v4.19.1
Synapse-VirusTotal adds new Storm commands to allow you to query the VirusTotal API using your existing API key.
author: The Vertex Project, LLC.

vertex-threat-intel documentation v0.12.0
The Vertex-Threat-Intel Power-Up provides a structured means for analysts to manage operational and strategic threat intelligence data via a dedicated Workflow.
author: The Vertex Project, LLC.

There should be **ten Rapid Power-Ups** installed (including **synapse-mitre-attack** and **synapse-tor,** which were already loaded).

Note: Use the **UPDATES** tab to install any updates when they are released. Demo instances are updated weekly (usually between Monday evening and Tuesday morning) with any new releases.

You do not need any other Power-Ups for the Synapse Bootcamp course.

You can install any other Power-Ups on the **AVAILABLE** tab if you want to test them. Some Power-Ups may require API keys (free or paid) and additional setup; refer to the Power-Up documentation for details.

Configuring Power-Ups

NOTE: For this exercise, you will need the set of API keys / secrets / tokens that you registered for prior to the start of this course. If you did not register for these API keys, refer to the **Pre-Course Setup** document for instructions on how to register and obtain keys.

Exercise 2

Objective:

- **Understand how to configure Power-Ups (specifically, how to set API keys for Power-Ups that may require them).**

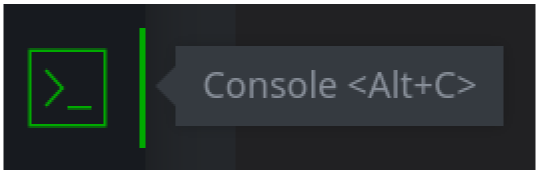
This exercise configures the API keys for the Power-Ups that require them.

Where the commands below specify *<your_api_key_here>*, paste in the value of your **API key** (without the greater than / less than signs).

If a different value is required (i.e., a **secret** or a **bearer token**) it will be noted in the command; paste in that value instead.

Configure Synapse-VirusTotal

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



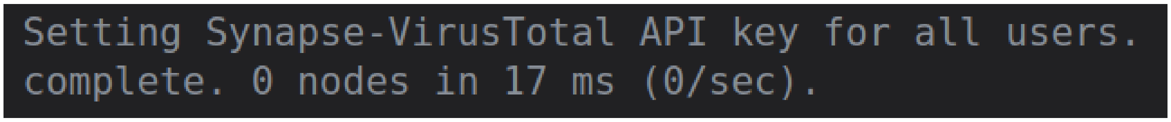
- In the **Console Tool,** enter the following command in the **Storm Query Bar** to set your **VirusTotal** API key.

  Paste your VirusTotal API key where it says *<your_api_key_here>*.

  Press **Enter** to run the command:

```
virustotal.setup.apikey <your_api_key_here>
```

- You should receive a message similar to the following indicating that you have configured a **global** key (i.e., for all users):



```
Setting Synapse-VirusTotal API key for all users.
complete. 0 nodes in 17 ms (0/sec).
```

> **Note:** Most Power-Ups allow you to configure either a **global** key (available to all users of the Power-Up) or a **personal** key (available to you; requires the `--self` option).
>
> We use global keys for Synapse Bootcamp for simplicity. In a production environment, global keys are typically installed and managed by your DevOps team. Whether you can install a personal key on your production system may depend on your organization's policies and / or Synapse permissions.

Configure Synapse-AlienVault

- In the **Console Tool,** enter the following command in the **Storm Query Bar** to set your **AlienVault** API key.

  Paste your AlienVault OTX API key where it says *`<your_api_key_here>`*.

  Press **Enter** to run the command:

```
alienvault.setup.apikey <your_api_key_here>
```

Configure Synapse-MalShare

- In the **Console Tool,** enter the following command in the **Storm Query Bar** to set your **MalShare** API key.

  Paste your MalShare API key where it says *`<your_api_key_here>`*.

  Press **Enter** to run the command:

```
malshare.setup.apikey <your_api_key_here>
```

Configure Synapse-MalwareBazaar

Note: The Synapse-MalwareBazaar Power-Up allows you to set and manage different **profiles** (configurations or "configs") for use with the Power-Up. Profiles allow you to optionally set additional configuration options besides your API key. These other settings are generally not needed for Synapse Bootcamp.

- In the **Console Tool,** enter the following command in the **Storm Query Bar** to set your **MalwareBazaar** profile name and API key.

  Specify a profile name where it says *<your_profile_name>*.

  Paste your MalwareBazaar API key where it says *<your_api_key_here>*.

  Press **Enter** to run the command:

  ```
  malwarebazaar.config.add <your_profile_name> <your_api_key_here>
  ```

Note: The remaining Power-Ups that we installed do not require API keys (or do not require them for the features used in this class).

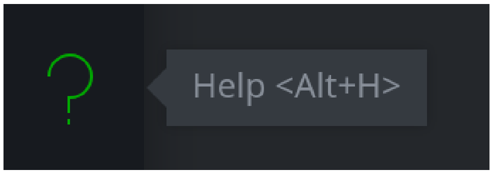
Power-Up Node Actions

Exercise 3

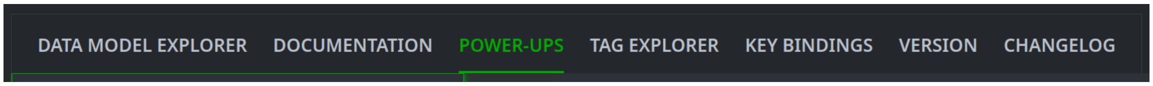
Objectives:

- **Understand the relationship between Power-Up commands and Node Actions.**
- **Know how to find information on installed Node Actions and the types of nodes that can be enriched by a Power-Up.**

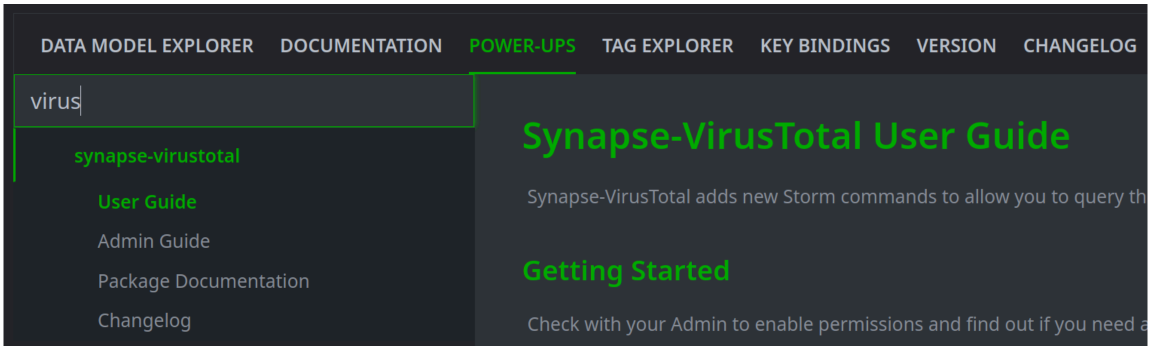
- From your **Toolbar,** select the **Help Tool:**



- In the **Help Tool,** click the **Power-Ups** tab:



- From the list view, locate the **synapse-virustotal** Power-Up:



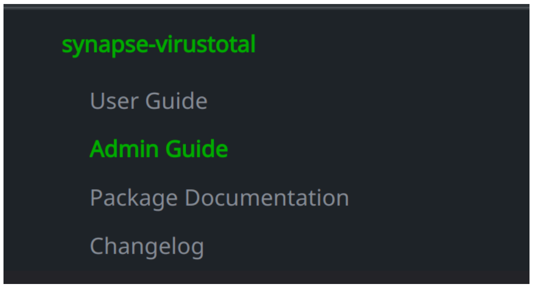
Synapse-VirusTotal User Guide

Synapse-VirusTotal adds new Storm commands to allow you to query th

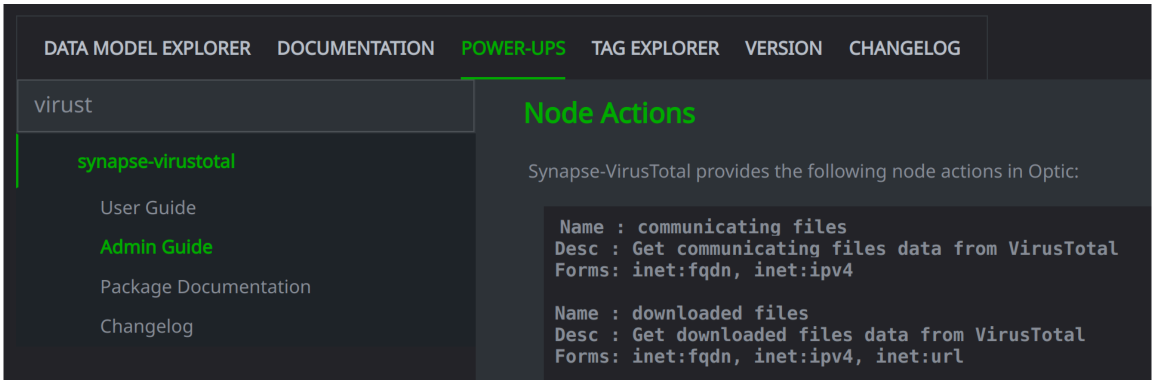
Getting Started

Check with your Admin to enable permissions and find out if you need a

- In the list view, click the synapse-virustotal **Admin Guide:**



- In the **Admin Guide, scroll** down until you see the **Node Actions** section:



Node Actions

Synapse-VirusTotal provides the following node actions in Optic:

```
 Name : communicating files
Desc : Get communicating files data from VirusTotal
Forms: inet:fqdn, inet:ipv4

Name : downloaded files
Desc : Get downloaded files data from VirusTotal
Forms: inet:fqdn, inet:ipv4, inet:url
```

Question 1: How many Node Actions are installed by the **synapse-virustotal** Power-Up?

Question 2: What kinds of data (nodes) can be enriched using this Power-Up?

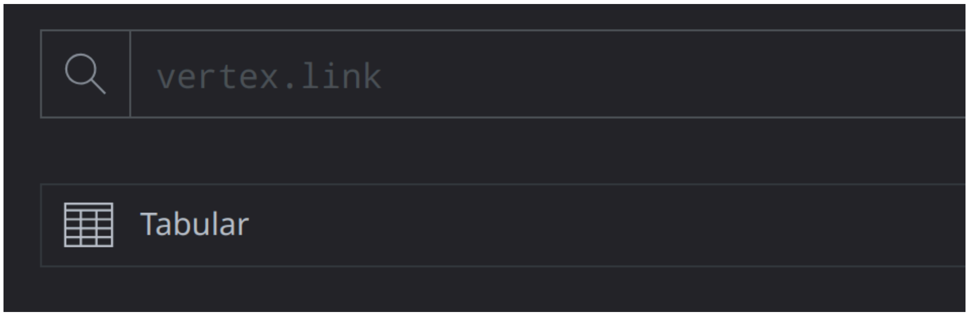
Enriching Data with Power-Ups

Exercise 4

Objectives:

- **Know how to run Power-Up Node Actions to enrich nodes.**
- **Understand changes that are made when enrichment occurs.**

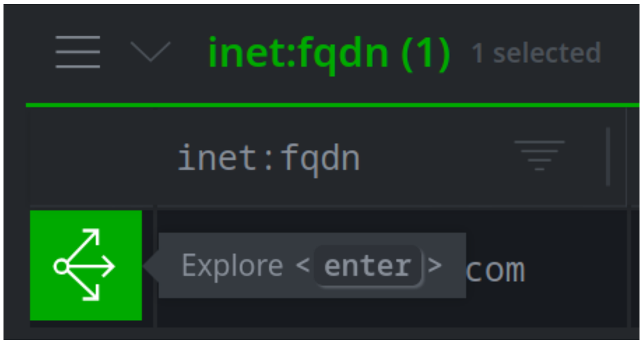
- In the **Research Tool,** ensure you are in **Tabular mode** and your **Storm Query Bar** is in **Lookup** mode:



- Enter the following in the **Storm Query Bar** and press **Enter** to run the query:

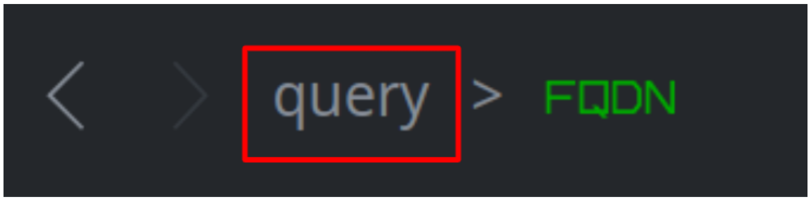
```
www.energym63.com
aa121762eb34d32c7d831d7abcec34f5a4241af9e669e5cc43a49a071bd6e894
91.214.124.143
```

- In the **Results Panel,** select the node for the FQDN (`www.energym63.com`). Click the **Explore** button to display adjacent nodes:

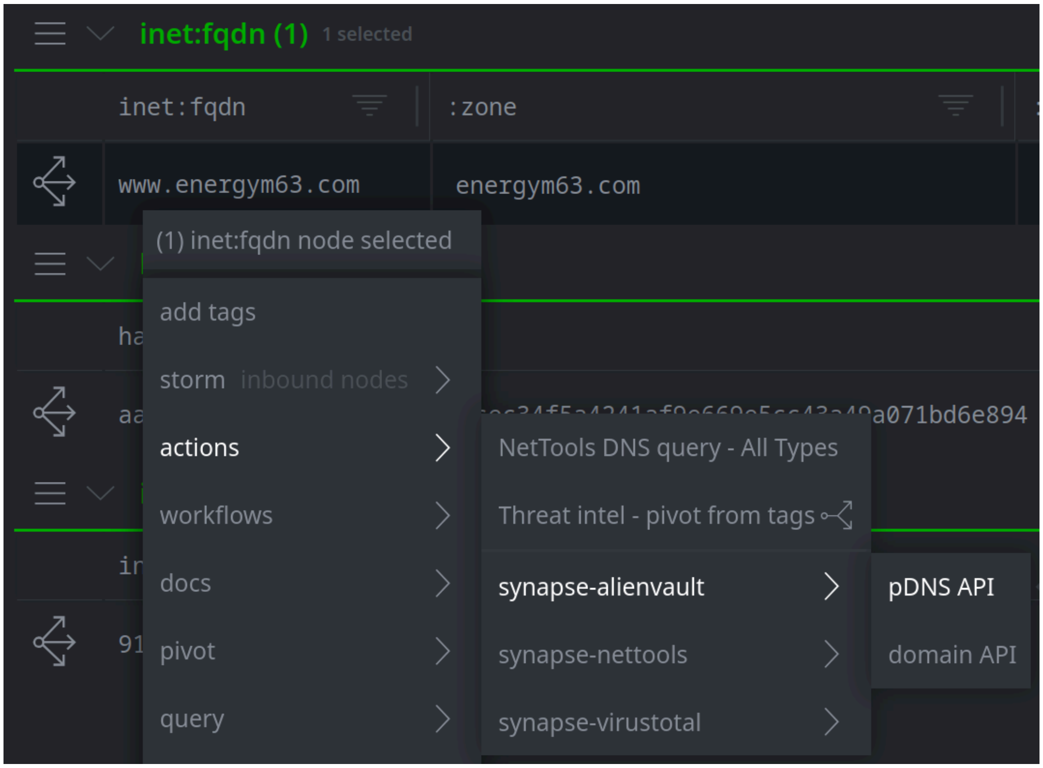


Question 1: What nodes (if any) are present in your results when you Explore from the FQDN **`www.energym63.com`**?

- In your **breadcrumbs,** click **query** to return to your original query:

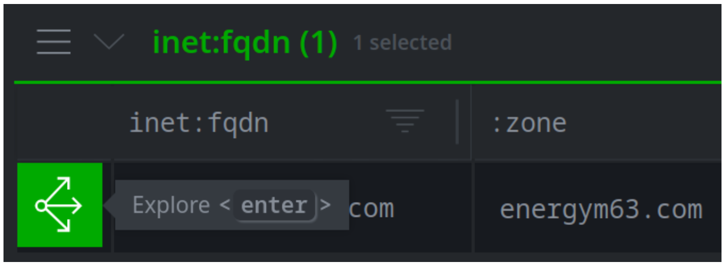


- In the **Results Panel,** right-click the FQDN **`www.energym63.com`** and choose **actions > synapse-alienvault > pDNS API** to run the Node Action:


inet:fqdn (1) 1 selected

inet:fqdn	:zone
www.energym63.com	energym63.com

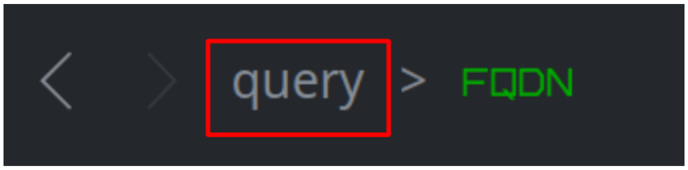
- When the Node Action completes, click the **Explore** button next to the FQDN again to display adjacent nodes:


inet:fqdn (1) 1 selected

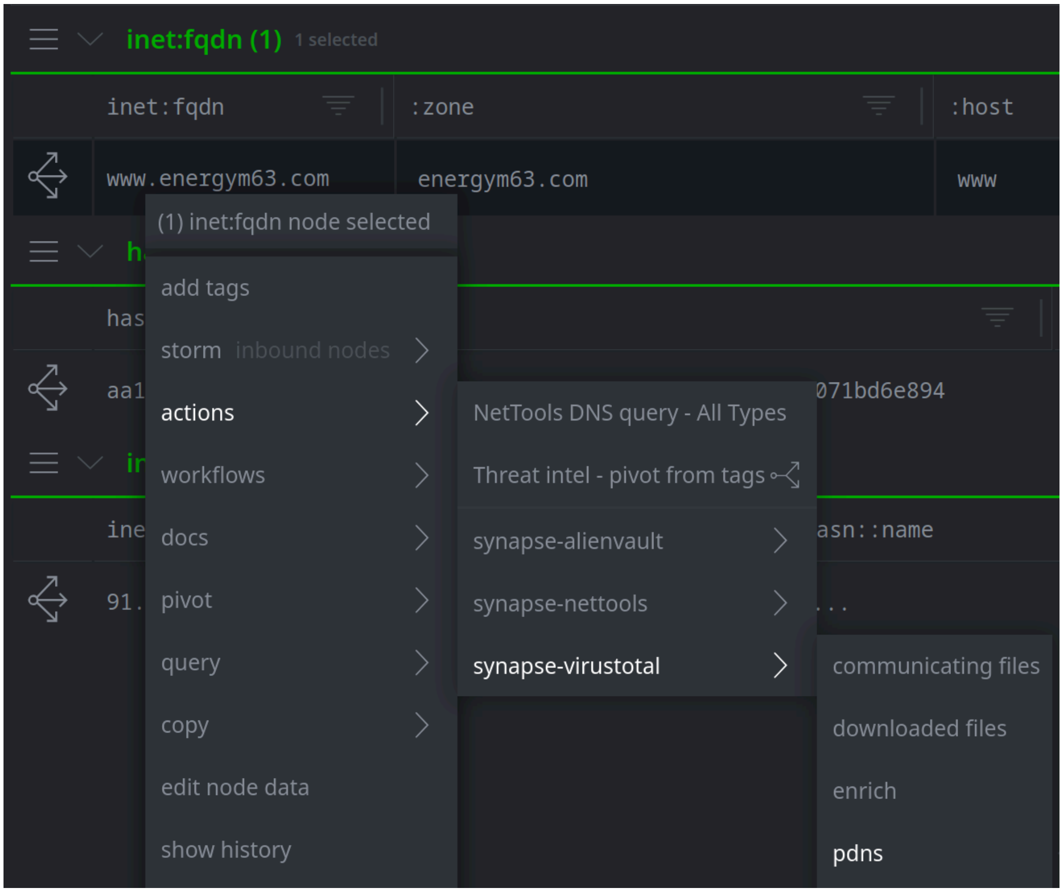
inet:fqdn	:zone
com	energym63.com

Question 2: What new data (if any) is present after you run the AlienVault PDNS Node Action?

- In your **breadcrumbs,** click **query** to return to your original query:

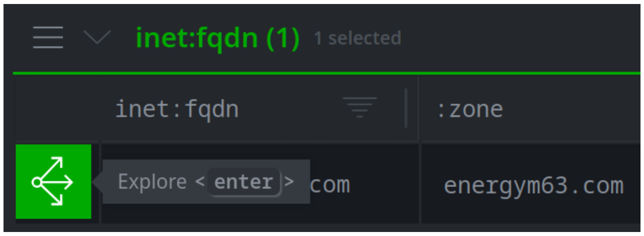


- In the **Results Panel, right-click** the FQDN and run the **actions > synapse-virustotal > pdns** Node Action:



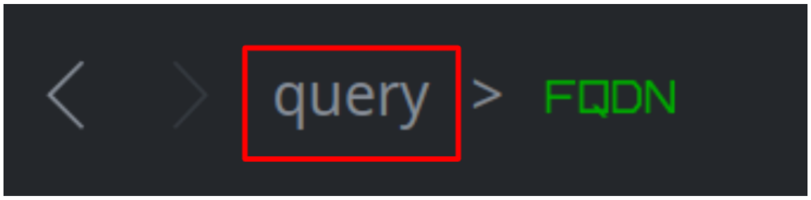
inet:fqdn	:zone	:host
www.energym63.com	energym63.com	www

- When the Node Action completes, click the **Explore** button next to the FQDN again to display adjacent nodes:

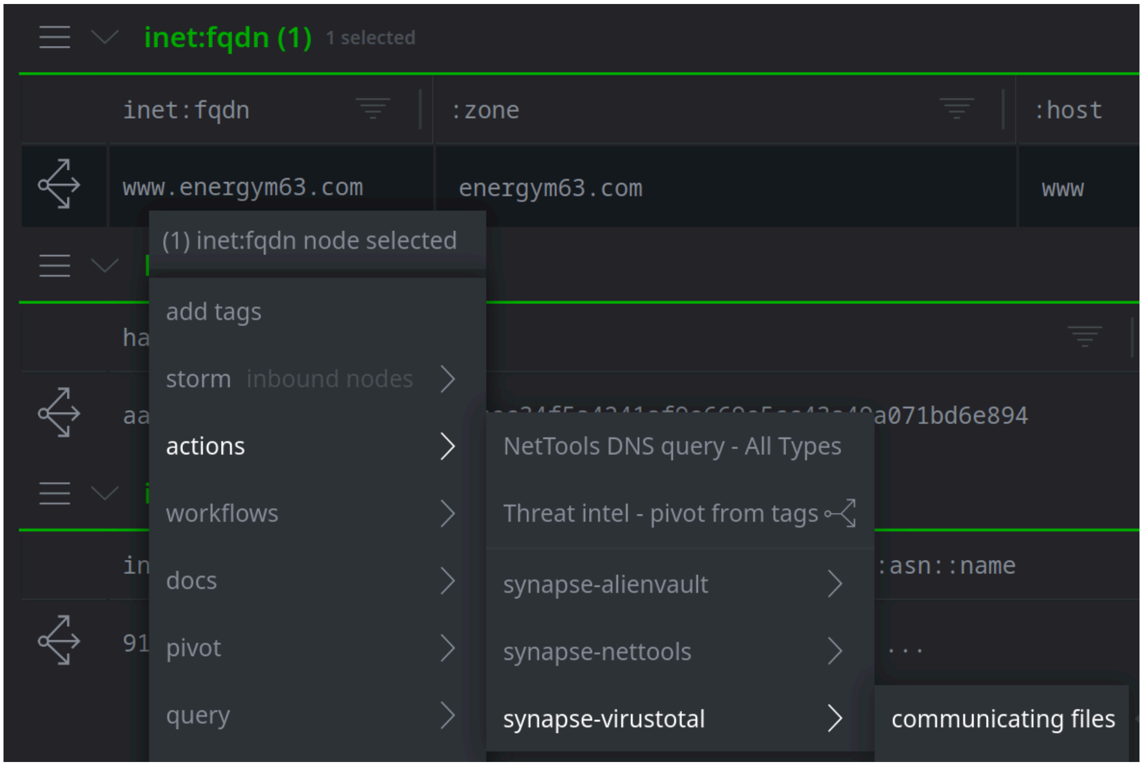


Question 3: What new data (if any) is present after you run the VirusTotal PDNS Node Action?

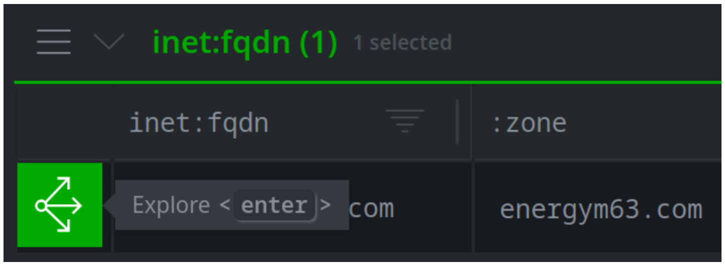
- In your **breadcrumbs,** click **query** to return to your original query once more:



- In the **Results Panel,** right-click the FQDN and run the **actions > synapse-virustotal > communicating files** Node Action:



- When the Node Action completes,click the **Explore** button next to the FQDN again to display adjacent nodes:



inet:fqdn (1) 1 selected

inet:fqdn	:zone
com	energym63.com

Question 4: What new data (if any) is present after you run the VirusTotal Communicating Files Node Action?

- **If time allows,** return to your original query and practice running some of the Node Actions available for the **`hash:sha256`** and the **`inet:ipv4`** nodes.
