Synapse Bootcamp - Module 5

## Power-Ups - Answer Key

Answer Key

Installing Power-Ups

Exercise 1 Answer

> **Objective:**
> ● **Understand how to view and install Power-Ups.**

● After completing the setup steps in this exercise, the following **Rapid Power-Ups** should be visible on the **Installed** tab of the **Power-Ups Tool** (some of these Power-Ups were already installed in your demo instance):

    ○ synapse-alienvault
    ○ synapse-malshare
    ○ synapse-malwarebazaar
    ○ synapse-mitre-attack
    ○ synapse-nist-nvd
    ○ synapse-rss
    ○ synapse-tor
    ○ synapse-us-cisa
    ○ synapse-virustotal
    ○ vertex-threat-intel
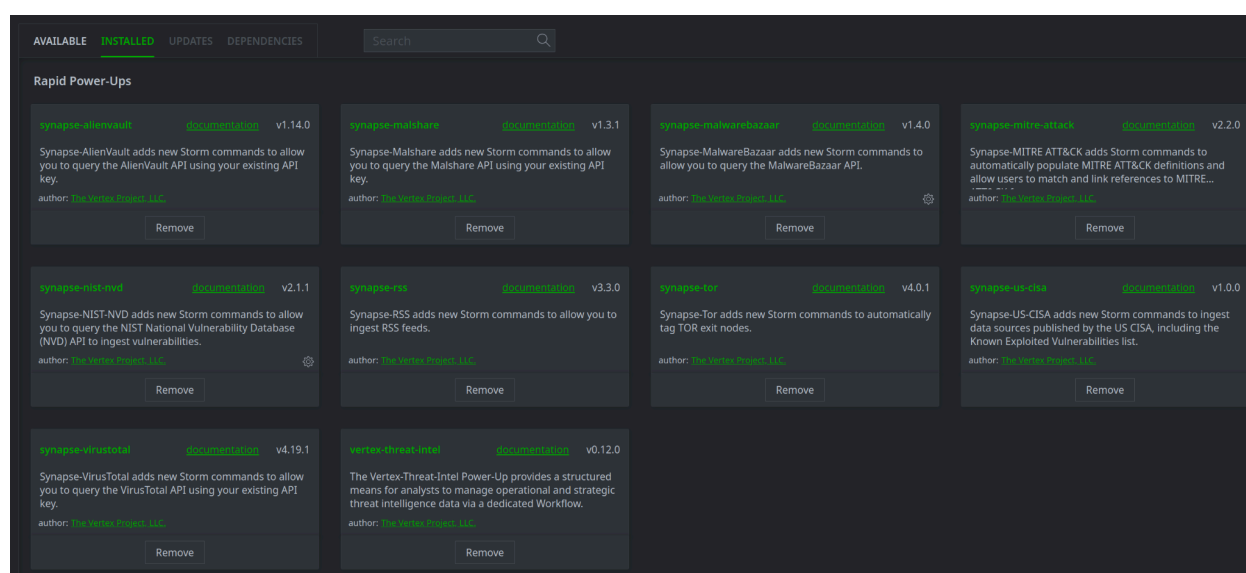
Configuring Power-Ups

Exercise 2 Answer

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

After completing the steps in this exercise, you should have configured the API keys and other information needed to access the vendors' services / API endpoints using your Synapse Power-Ups.

We encourage you to complete **Exercise 3** and **Exercise 4** at this point!

If time allows (or you want to perform the steps below after class) the following commands can be used to check your quotas and verify your keys are set correctly.

Synapse-VirusTotal

- In the **Console Tool,** in the **Storm Query Bar,** click **Storm Mode Selector** and choose **Storm** mode:
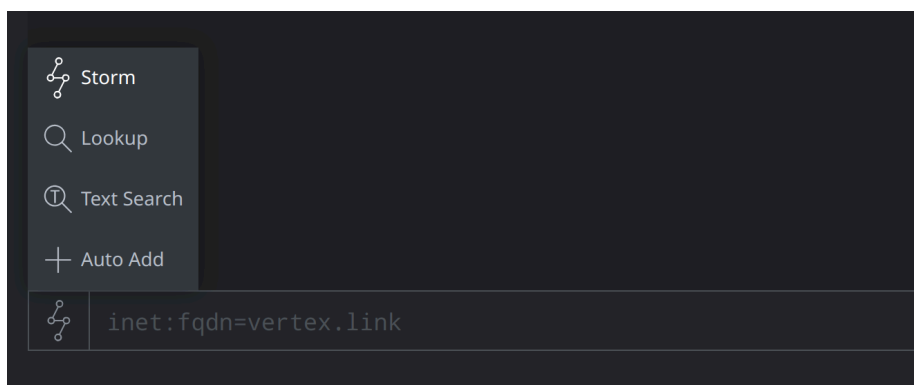
- Enter the following in the **Storm Query Bar** and press **Enter** to run the command:

  ```
  virustotal.info
  ```

- You'll see information about available privileges and quotas:

```
Optic Console Initialized
> virustotal.info
Privileges:
  downloads-tier-2: false
  downloads-tier-1: false
  intelligence: false
  private: false
  click_to_accept: false
  vtinsights: false
  file-feed-without-av-results: false
  url-feed: false
  sales-staff: false
  staff: false
  domain-feed: false
  file-feed: false
  ip-feed: false
  vtalerts: false
  creditcards: false
  monitor-partner: false
  file-behaviour-feed: false
  monitor: false
  oem_click_to_accept: false
  vtdiff-api: false
  vtdiff-ui: false
  intelligence-search-tier-2: false
  intelligence-search-tier-3: false
  intelligence-search-tier-1: false
  dogfooder: false
  retrohunt-tier-3: false
  retrohunt-tier-2: false
  retrohunt-tier-1: false

Quota                                  Used        Allowed
----------------------------------------------------------
private_scans_per_minute                 0              0
monitor_uploaded_files                   0              0
monitor_storage_files                    0              0
                                                Scroll to bottom  ∨

  ⌇    inet:fqdn=vertex.link
```

Synapse-AlienVault

- LevelBlue / AlienVault OTX does not have a 'quotas' endpoint and does not limit access to the free Open Threat Exchange (OTX) platform.

Synapse-MalShare

- In the **Console Tool,** enter the following in the **Storm Query Bar** and press **Enter** to run the command:

```
malshare.quota
```

Synapse-MalwareBazaar

- MalwareBazaar does not implement formal API quotas, but you can use the Power-Up commands to view your configuration settings / profile.

- In the **Console Tool,** enter the following in the **Storm Query Bar** and press **Enter** to run the command:

```
malwarebazaar.config.show
```

Power-Up Node Actions

Exercise 3 Answer

> **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.**

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

- The **synapse-virustotal** Power-Up adds **eleven** Node Actions to Synapse (as of v5.4.0 of the Power-Up):

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

Name : enrich
Desc : Get report data from VirusTotal
Forms: file:bytes, hash:md5, hash:sha1, hash:sha256, inet:fqdn, inet:ipv4, inet:url

Name : pdns
Desc : Get passive DNS information from VirusTotal
Forms: inet:fqdn, inet:ipv4

Name : urls
Desc : Get URLs data from VirusTotal
Forms: inet:fqdn, inet:ipv4

Name : file behavior
Desc : Get sandbox execution data from VirusTotal
Forms: file:bytes, hash:md5, hash:sha1, hash:sha256

Name : file download
Desc : Download file bytes from VirusTotal
Forms: file:bytes, hash:md5, hash:sha1, hash:sha256

Name : file report
Desc : Get file report data from VirusTotal
Forms: file:bytes, hash:md5, hash:sha1, hash:sha256

Name : in the wild URLs
Desc : Get "in the wild" URL data from VirusTotal
Forms: file:bytes, hash:md5, hash:sha1, hash:sha256

Name : ssl history
Desc : Get historical SSL certificate data from VirusTotal
Forms: inet:fqdn, inet:ipv4

Name : whois history
Desc : Get historical WHOIS records from VirusTotal
Forms: inet:fqdn, inet:ipv4
```

Power-Ups add **Storm commands** that implement the Power-Up's features. A **Node Action** is a right-click context menu option that makes it easy for you to run those Storm commands.

A Power-Up typically adds Node Actions for a **subset** of the Storm commands installed by the Power-Up. Storm commands that **operate on nodes** are installed as Node Actions.

Storm commands for other tasks - to set an API key or check your API quota - do not operate on nodes. These commands need to be run from the Storm Query Bar (e.g., in the Console Tool).

All of the Storm commands installed by a Power-Up can be found in the Power-Up's **Package Documentation.** We'll talk more about Power-Ups in a later module!

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

- Based on the **Admin Guide** documentation (**Node Action** section), the synapse-virustotal Power-Up can be used to enrich the following (for v5.4.0 of the Power-Up):
  - "Files", using either a `file:bytes` node or any of the common hash values (`hash:md5`, `hash:sha1`, `hash:sha256`)
  - Domains (`inet:fqdn` nodes)
  - IPv4 addresses (`inet:ipv4` nodes)
  - URLs (`inet:url` nodes)

Enriching Data with Power-Ups

Exercise 4 Answer

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

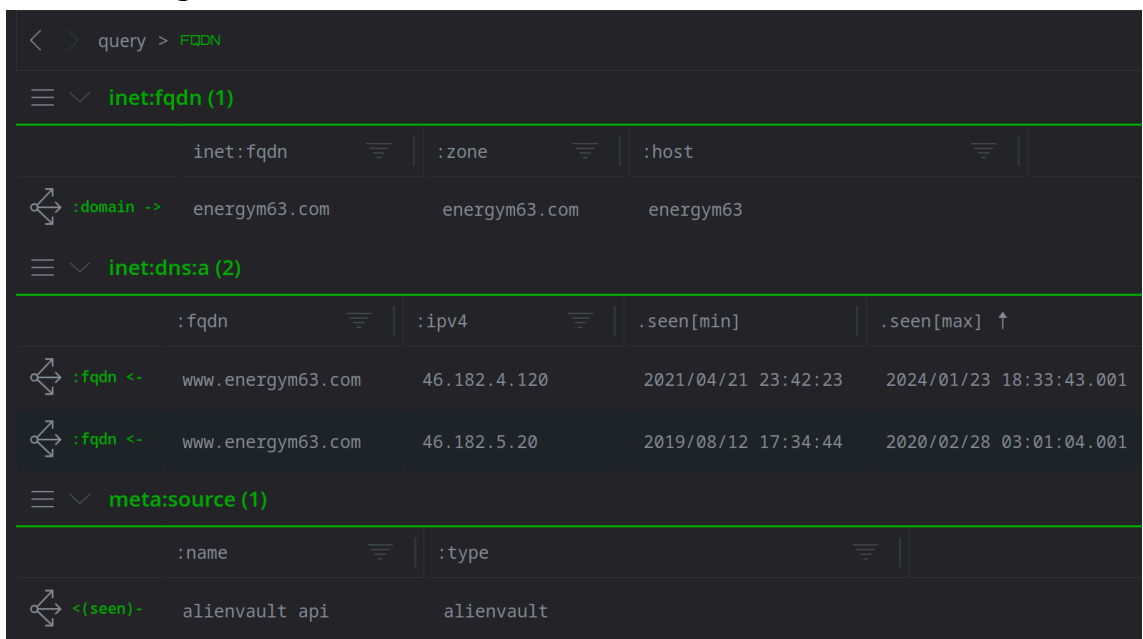**Question 1:** What nodes (if any) are present in your results when you Explore from the FQDN `www.energym63.com`?

- The only node adjacent to FQDN **www.energym63.com** is the domain's zone:

inet:fqdn		:zone
:domain -> energym63.com		energym63.com

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

- After running the AlienVault PDNS Node Action, two DNS A records (**inet:dns:a** nodes) are present for the FQDN, as well as a **meta:source** node for the AlienVault API (as of August 2025):

inet:fqdn (1)

inet:fqdn	:zone	:host
:domain -> energym63.com	energym63.com	energym63

inet:dns:a (2)

	:fqdn	:ipv4	.seen[min]	.seen[max] ↑
:fqdn <-	www.energym63.com	46.182.4.120	2021/04/21 23:42:23	2024/01/23 18:33:43.001
:fqdn <-	www.energym63.com	46.182.5.20	2019/08/12 17:34:44	2020/02/28 03:01:04.001

meta:source (1)

	:name	:type
<(seen)-	alienvault api	alienvault

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

- After running the VirusTotal PDNS Node Action, one additional DNS A record is present (as of August 2025):

	:fqdn	:ipv4	.seen[min]	.seen[max]
≡ ∨	**inet:dns:a (3)**			
:fqdn <-	www.energym63.com	46.182.5.20	2019/08/12 17:34:44	2020/02/28 03:01:04.001
:fqdn <-	www.energym63.com	217.16.10.2	2018/07/24 05:51:47	2018/07/24 05:51:47.001
:fqdn <-	www.energym63.com	46.182.4.120	2021/01/29 11:38:58	2024/01/23 18:33:43.001

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

- The FQDN `www.energym63.com` is now linked to five files (`file:bytes`) nodes (as of August 2025). These are the files that VirusTotal says "communicate with" the FQDN:

file:bytes
≡ ∨ **file:bytes (5)**
<(refs)-   sha256:80b4fe41d371bb70645aef35...
<(refs)-   sha256:a214c21389ebb839617f450a...
<(refs)-   sha256:b48421dd44297b34e574e65d...
<(refs)-   sha256:efa78d9ed272969fb2ac62b3...
<(refs)-   sha256:0219966745cb935fc69270c4...

> VirusTotal's "communicating files" API does not specify what the "communicating" relationship is. In Synapse, we can only show that the file (`file:bytes`) "references" ("communicates with") the FQDN.
>
> Running additional Node Actions may return more data. For example, using the **actions > synapse-virustotal > file behavior** Node Action may return sandbox execution data that shows the file made a DNS query (`inet:dns:request`) for the FQDN.