Vertex

Synapse Bootcamp - Module 8

Intro to Storm - Answer Key

© 2024 The Vertex Project, LLC

Answer Key

Basic Lifts

Exercise 1 Answer

Objective:
- **Use Storm to perform basic lift operations.**

Part 1

Question 1: How would you **lift** each of these nodes using **Storm?**

- The nodes can be lifted with the following Storm queries:

```
inet:ipv4=50.2.160.146
```

```
hash:md5=d41d8cd98f00b204e9800998ecf8427e
```

```
inet:email=mfa.cdep@mfa.gov.lv
```

```
inet:url=https://45.154.14.235/2023/PotPlayer.exe
```

  You can easily lift these indicators by adding the **form name** before the value you are interested in. All of the indicators are simple forms, where the "thing" you're lifting is the primary property of the node.

  (For you Storm nerds, this is called a **lift by primary property**.)

  You will need to "re-fang" any defanged indicators. Lookup mode was specifically designed to make your life easy by dealing with defanging for you.

  Some characters used for defanging (such as square brackets) have a specific meaning in Storm. Storm doesn't expect to find them in the middle of an email address (for example), so will generate a syntax error.

© 2024 The Vertex Project, LLC

Part 2

Question 2: Using Storm, how can you lift the **`inet:dns:a`** nodes for IPv4 **`46.37.164.184`**?

- You can lift the nodes with the following Storm:

```
inet:dns:a:ipv4=46.37.164.184
```

  You are telling Synapse that you want to see the DNS A records (**`inet:dns:a`** nodes) whose **`:ipv4`** property value is the IP we're interested in (**`46.37.164.184`**).

  We can lift a set of nodes that **share** a particular property value.

  (In Storm, this is a **lift by secondary property value**).

Part 3

Question 3: How can you use Storm to lift **all** of the network whois data (**`inet:whois:iprec`** nodes) in Synapse?

- You can lift all the network whois data with the following Storm:

```
inet:whois:iprec
```

  You are telling Synapse that you want to see **all** nodes of the form **`inet:whois:iprec`** that exist.

  (This is called a **lift by form**).

  A "network whois record" is not something that **Lookup mode** recognizes. You cannot look up or lift an **`inet:whois:iprec`** node directly without using Storm.

  > The number of **`inet:whois:rec`** nodes in your demo instance is small, so it is easy to ask to see all of them.
  >
  > For some forms, a "lift by form" would not make sense. In a production system (that may contain millions of nodes), you would not want to ask for **all** the **`inet:ipv4`** nodes!

© 2024 The Vertex Project, LLC

Part 4

Question 4: How can you use Storm to lift all of the nodes that Microsoft says are associated with Brass Typhoon?

- You can lift all the nodes with the following Storm:

```
#rep.microsoft.brass_typhoon
```

  You're telling Synapse you want to lift **all** nodes that have the **tag rep.microsoft.brass_typhoon.**

  (This is called a **lift by tag**).

  Because we are using Storm, we need to add a hashtag (**#**) before the tag name so that Synapse knows this is a tag.

Question 5: How can you **modify** your Storm query to only lift the **domains** Microsoft says are associated with Brass Typhoon?

- You can lift **only** the domains with the following Storm:

```
inet:fqdn#rep.microsoft.brass_typhoon
```

  Now you are telling Synapse you only want to lift any **`inet:fqdn`** nodes that have the specified tag.

  (This is called a **lift form by tag**).

  Notice that there is **no space** between the form name (**`inet:fqdn`**) and the hashtag (**`#`**).

  If you put a space between them, Synapse would interpret that Storm as **two** separate lifts:
  - All the **`inet:fqdn`** nodes, and
  - All the nodes tagged **`rep.microsoft.brass_typhoon`**

© 2024 The Vertex Project, LLC

Lifts with Mathematical Operators

Exercise 2 Answer

Objective:
- **Use mathematical operators to perform lifts with Storm.**

Question 1: How can you use Storm to lift all of the files (**`file:bytes`** nodes) whose size is larger than 5 MB? (**Note:** use **5000000** bytes as an approximation for 5 MB.)

- You can lift the files with the following Storm:

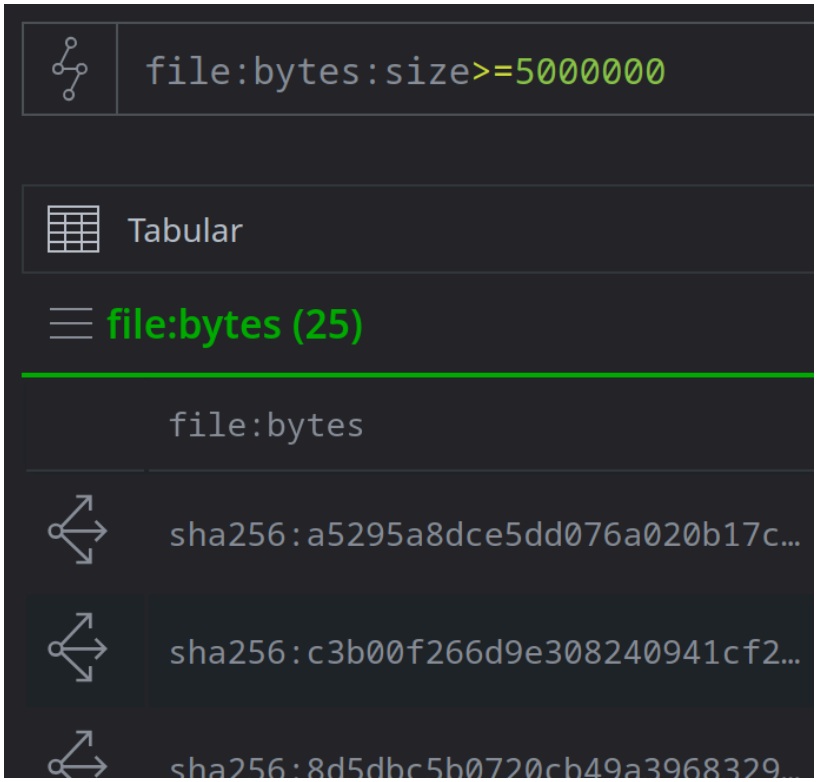
```
file:bytes:size>=5000000
```

> "Simple" lifts use the equals sign (=) to **exactly match** the value you're interested in.
>
> You can use other mathematical operators ("equal to" is a mathematical operator!) such as "less than" (**<**) or "greater than or equal to" (**>=**) in lift operations!

Question 2: How many files are there?

© 2024 The Vertex Project, LLC

- There are **25** files:



> **Note:** This answer is based on the baseline Synapse demo instance. Your answer may vary depending on the data that has been added to your demo instance so far in this course.

Lifts with Extended Operators

Exercise 3 Answer

> **Objective:**
> - **Use Storm's extended operators to perform custom lifts.**

Part 1

Question 1: How can you use Storm to lift all of the IPv4 nodes whose **:loc** property **starts with** 'kr'?

- You can lift the IPv4 addresses with the following Storm:

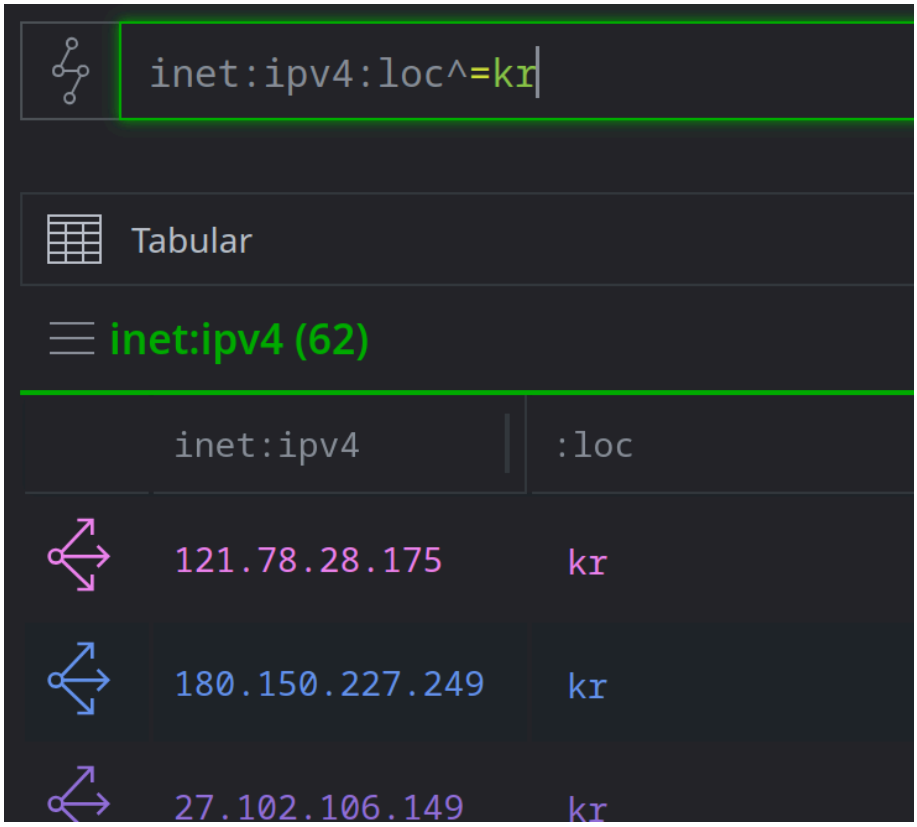
```
inet:ipv4:loc^=kr
```

Storm's **prefix** comparison operator (**^=**) allows you to lift nodes by matching the **beginning** of a string value.

If you used the equals operator (`inet:ipv4:loc=kr`), you would only get those IPv4 addresses whose `:loc` string **exactly** matches '**kr**'.

Question 2: How many IPv4 addresses are there?

- There are **62** IPv4 addresses geolocated in South Korea:



Note: This answer is based on the baseline Synapse demo instance. Your answer may vary depending on the data that has been added to your demo instance so far in this course.

© 2024 The Vertex Project, LLC

Part 2

Question 3: How can you use Storm to lift all of the files (**`file:bytes`**) nodes whose compile time (**`:mime:pe:compiled`**) is between those two dates (e.g., **2020/03/01** and **2020/03/31**)?

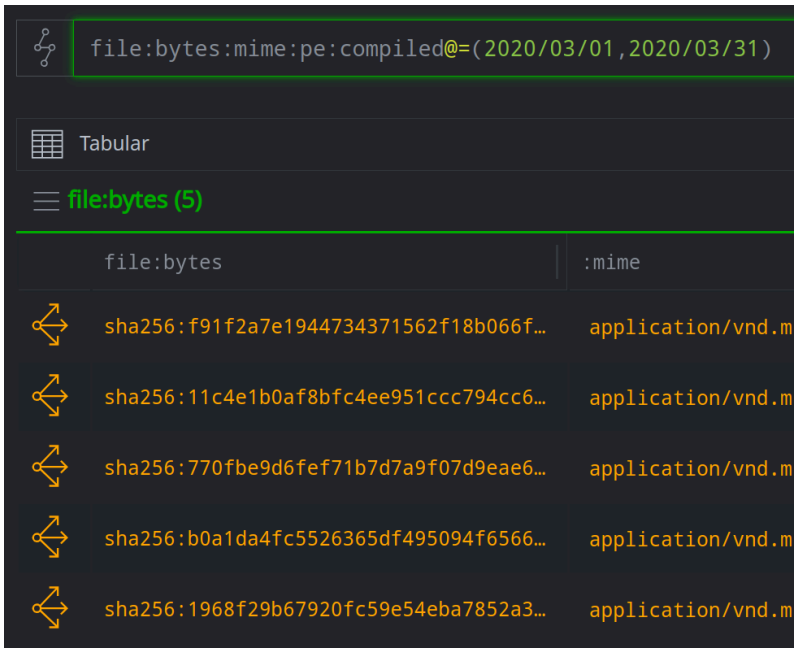
- You can lift the files with the following Storm:

```
file:bytes:mime:pe:compiled@=(2020/03/01,2020/03/31)
```

  Storm's **interval** comparison operator (**@=**) allows you to lift nodes by matching a date/time interval.

Question 4: How many files are there?

- There are **5** files:



> **Note:** This answer is based on the baseline Synapse demo instance. Your answer may vary depending on the data that has been added to your demo instance so far in this course.

© 2024 The Vertex Project, LLC

Tip: You do not need to include the forward slashes (/) within the date strings. (We use them for clarity.) In Storm, Synapse knows to expect a date and will interpret numeric strings as YYYYMMDDhhmmss. The following query will also work:

```
file:bytes:mime:pe:compiled@=(20200301,20200331)
```

Storm also allows you to use a wildcard (*) to partially match a date/time string. The file:bytes:mime:pe:compiled property is a single date/time value. We used the @= operator above to specify a **range** of dates between March 1 and March 31, 2020. We could also use a wildcard to represent "any date/time in March 2020":

```
file:bytes:mime:pe:compiled=2020/03*
```

© 2024 The Vertex Project, LLC