



Vertex

Synapse Bootcamp

Module 12

Modifying Data with Storm

v0.4 - May 2024



Objectives

- Understand how to use edit brackets in Storm
- Know how the Storm pipeline affects edit operations
- Understand how edit parentheses can be used to scope edits
- Use Storm edit operations to:
 - Create nodes
 - Set, modify, and remove properties
 - Add and remove tags



Modifying Data in Storm



Storm Operations

Operation	Meaning	Common Storm Operator	UI Equivalent
Lift	Select data (nodes) from Synapse	Query bar - Storm	Query bar - Lookup / Text Search query and copy menu options
Pivot	Move between nodes that share the same property value	-> or <- *	Explore button pivot menu option
Traverse	Move between nodes that are linked by an edge	-(*)> or <(*)-	Explore button
Filter	Include / exclude a subset of nodes	+ or -	n/a (column filters; query / select menu options)
Run	Execute a Storm command	<command>	Node Action
Modify / Edit	Modify or delete properties Add or remove tags Add nodes	[] or [()]	Inline property edit; delete menu option Add / remove tags menu options Lookup or Auto Add / Add Node



Edit Brackets

- Storm uses square brackets (**[]**) to enclose **edit** operations
 - Also known as "data modification"
- "Edit" means any change:
 - Add / create nodes
 - Set, modify, or delete properties
 - Add or remove tags or tag timestamps
 - Add or remove light edges
- A set of brackets represents a single **edit operation**
 - The brackets can enclose multiple changes



Adding / Modifying Data



Adding Nodes

- When creating a node, the only thing **required** is the **primary property**
 - Other properties are optional / can be set later
- Creating a node requires:
 - **Edit brackets**
 - The **form** name
 - The **equals** sign (=)
 - The primary property **value**

```
[ inet:email = info@vertex.link ]
```
- If the node already exists, Synapse simply **lifts** the node
 - Synapse checks (deconflicts) based on the primary property



Adding Nodes

- Add simple node

```
[ inet:fqdn = vertex.link ]
```

- Add composite node

```
[ inet:dns:a = (vertex.link, 137.184.16.9) ]
```

- Add guid node

```
[ ou:org = * ]
```

- Using an asterisk (*) will generate an **arbitrary** guid

Storm gen.* commands can be used to **deconflict** and **create** some guid forms.



Adding Multiple Nodes

- Edit brackets can be used to make multiple changes
 - No need to place individual changes in separate brackets
- These two queries perform the **same** actions:

```
[ inet:fqdn=vertex.link ] [ inet:dns:a=(vertex.link,137.184.16.9) ] [ ps:contact=* ]
```

```
[ inet:fqdn=vertex.link inet:dns:a=(vertex.link,137.184.16.9) ps:contact=* ]
```

- In each case we provide the node's **primary property** to create it



Setting Properties

- Set or modify the same way
- Requires:
 - The node(s) whose property you want to set
 - Edit brackets
 - The **relative** property name
 - The **value** of the property

```
inet:ipv4=8.8.8.8 [ :loc='us.ca.mountain view' ]
```

Node

Relative
property
name

Value



Setting Properties

- Add node and set property

```
[ ou:org=* :name='The Vertex Project' ]
```

- Set property on existing node

```
ou:org:name='The Vertex Project' [ :loc=us.va.reston ]
```

- Set multiple properties on existing node

```
ou:org:name='The Vertex Project' [ :loc=us.va.reston :founded=2016 ]
```



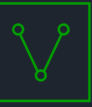
Removing Properties

- Removing a property **deletes** it entirely
 - Delete in the layer where it resides
- Requires:
 - The node(s) whose property you want to remove
 - Edit brackets
 - The **minus** sign (-)
 - The **relative** property name

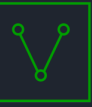
```
inet:ipv4=8.8.8.8 [ -:loc ]
```

Node

Relative
property
name (with
minus)



Adding / Modifying Data - Demo



Applying / Removing Tags



Applying Tags

- Requires:
 - The node(s) you want to apply the tag to
 - Edit brackets
 - The **plus** sign (+)
 - The **hashtag** sign (#)
 - The **tag name**

```
inet:ipv4=8.8.8.8 [ +#cno.infra.dns.google ]
```

- Synapse automatically creates the syn:tag node(s) if they don't exist



Applying Tags

- With node creation

```
[ inet:ipv4=47.56.228.89 +#rep.secureworks.shadowpad ]
```

- To existing node

```
inet:ipv4=47.56.228.89 [ +#rep.secureworks.shadowpad ]
```

- Add multiple tags to existing node

```
inet:ipv4=47.56.228.89 [ +#rep.secureworks.shadowpad  
    +#rep.secureworks.bronze_university ]
```




Applying Tags with Timestamps

- Requires:
 - The **equals** sign and a **single** date/time, **or**
 - The **equals** sign and a **pair** of date/times in **parentheses**
- Can **modify** a timestamp the same way as adding
 - Subject to interval (ival) behavior

```
ou:org:name=vertex [ +#super.cool.company=2016/06/01 ]
```

```
ou:org:name=vertex [ +#super.cool.company=(2016/06/01, now) ]
```



Removing Tags / Tag Timestamps

- Requires:

- The node(s) you want to remove the tag from
- The **minus** sign (-)
- The **hashtag** sign (#)
- The **tag name**

```
inet:ipv4=8.8.8.8 [ -#cno.infra.dns.google ]
```

- Synapse removes the tag you specify
 - "From here down"
- To remove a **tag timestamp**, remove the **tag** element associated with the timestamp



Removing Tags

- For a node with the tag `#cno.infra.dns.google`
 - Remove the **base** tag ('google'):

```
inet:ipv4=8.8.8.8 [ -#cno.infra.dns.google ]
```

Remaining tag: `#cno.infra.dns`

- Remove the **full** tag:

```
inet:ipv4=8.8.8.8 [ -#cno ]
```

Remaining tag: none



Removing Tag Timestamps

- IPv4 with `#cno.infra.dns.google=(2022/01/15, 2022/04/07)`

- Remove timestamp by removing base tag (leaves tag `#cno.infra.dns`):

```
inet:ipv4=8.8.8.8 [ -#cno.infra.dns.google ]
```

- We now have:

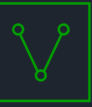
```
inet:ipv4=8.8.8.8 with #cno.infra.dns
```

- If the node should still have the tag (without timestamps), re-add it:

```
inet:ipv4=8.8.8.8 [ +#cno.infra.dns.google ]
```

- To **shrink** the time window, re-add the tag with the new dates:

```
inet:ipv4=8.8.8.8 [ +#cno.infra.dns.google=(2022/02/15, 2022/04/07) ]
```



Applying / Removing Tags - Demo



Adding / Removing Light Edges



Adding Light Edges

– Requires:

- The node(s) you want to link via the edge
- Edit brackets
- The **plus** sign (+)
- The **edge name** in parentheses (e.g., (refs))
- The **edge direction** arrow (> or <)
- The node(s) you want to link enclosed in **curly braces** ({ })

```
hash:sha1#rep.eset.sednit [ <(refs)+ { media:news:title='en route with sednit' } ]
```

```
media:news:title='en route with sednit' [ +(refs)> { hash:sha1#rep.eset.sednit } ]
```

For many common use cases, Synapse creates light edges for you!



Removing Light Edges

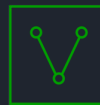
– Requires:

- The node(s) you want to link via the edge
- Edit brackets
- The **minus** sign (-)
- The **edge name** in parentheses ((refs))
- The **edge direction** arrow (> or <)
- The node(s) you want to unlink enclosed in **curly braces** ({ })

```
hash:sha1#rep.eset.sednit [ <(refs)- { media:news:title='en route with sednit' } ]
```

```
media:news:title='en route with sednit' [ -(refs)> { hash:sha1#rep.eset.sednit } ]
```


Add Edges Dialog



hash:md5

↔	9b39e1f72cf4acffd45f45f08483abf0
↔	4fe276edc21ec5f2540c2babd81c8653
↔	11511b3d69fbb6ccea1dd0278cbdfb
↔	f62dfc4999d624d01e94b89946ec1036
↔	05cf906b750eb335125695da42f4eafc
↔	748de2b2aa1fa23fa5996f287437af1b
↔	9912eb641eabd640a476720c51f5e3ad
↔	aa115f20472e78a068c1bbf739c443bf
↔	28c6f235946fd694d2634c7a2f24c1ba
↔	08f25a641e8361495a415c763fbb9b71

(1) hash:md5 node selected

add tags

storm inbound nodes >

actions >

docs >

query >

copy >

edit node data

show history

notes >

add edges

add node to story

Add Edges

source nodes

hash:md5 (1)

hash:md5

9b39e1f72cf4acffd45f45f08483abf0

reverse

☐ OFF

verb

refs

edge

hash:md5

+(refs)>

media:news

target nodes

media:news:publisher:name=anomali

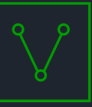
media:news (2) 1 selected

:publisher:name	:published	:title	:url
anomali	2019/10/07 00:00:00	china-based apt mustang panda targets minority group...	https://www.anomali.com/blog/china-t
anomali	2020/04/29 00:00:00	anomali suspects that china- backed apt pirate panda...	https://www.anomali.com/blog/anomali

+ Add All

+ Add Selected

Cancel



Adding Light Edges - Demo



Edits and the Storm Pipeline



Edits and the Storm Pipeline

- Storm operations are chained to form longer queries
 - The chain is a **pipeline** through which nodes pass
 - Any **edit operation** is also part of the pipeline
- Edit brackets **do not** separate or isolate changes
 - Applies `#cno.mal` to **both** FQDNs:

```
inet:fqdn=google.com [ inet:fqdn=evil.com +#cno.mal ]
```

- Sets `:loc=au` for 1.2.3.4, then sets `:loc=de` for **both** IPv4s:

```
[ inet:ipv4=1.2.3.4 :loc=au ] [ inet:ipv4=5.6.7.8 :loc=de ]
```



Edit Parentheses

- You can use **parentheses** inside edit brackets
 - Parentheses **isolate changes**

```
inet:fqdn=google.com [ ( inet:fqdn=evil.com +#cno.mal ) ]
```

```
[ ( inet:ipv4=1.2.3.4 :loc=au ) ( inet:ipv4=5.6.7.8 :loc=de ) ]
```

- **Nodes** remain in the pipeline
 - Edits **outside** parentheses apply to all nodes

```
[ ( inet:ipv4=1.2.3.4 :loc=au ) ( inet:ipv4=5.6.7.8 :loc=de ) +#woot ]
```



Edits and Bulk Changes

- An edit operation can be used like any other operation
 - Added to a Storm query / query pipeline
- The edit can operate on **any number** of inbound nodes
 - Make modifications at scale

```
[ inet:ipv4=213.24.76.0/24 ]
```

```
media:news [ -:author ]
```

```
file:bytes.created@=(now, '-1 day') +#rep [ +#thesilence.triage ]
```



Synapse UI and Storm

Synapse UI	Storm Editing
Multiple methods to add (Lookup mode, Add Node dialog)	Single method (edit brackets / parentheses)
Multiple methods to edit (inline, edit menu, add / remove tags)	Single method (edit brackets / parentheses)
Good for making changes to one or a small number of nodes	Good for making changes at scale



Summary

- In Storm **edit brackets** enclose operations that add or modify data
 - Add nodes
 - Set/modify/delete properties
 - Add/remove tags
 - Add/remove tag timestamps
 - Add/remove light edges
- An **edit operation** acts like any other operation in the Storm **pipeline**
 - One or more nodes are **inbound to** (or specified within) the edit brackets
 - The edit operation takes place on **all** inbound nodes
- **Edit parentheses** can be used to segregate specific edit operations
- Storm edit operations are convenient for making changes **at scale**