

Storm Quick Reference - Example Edits (Data Modification)

Note: Storm queries act as a pipeline, with operations (lift, filter, pivot, edit...) chained together and executing in sequence from left to right. Edit operations will therefore operate on **any / all** nodes currently in the pipeline, not "just" what is inside the edit brackets.

Edit Brackets - Nodes and Properties

Create a node	<code>[inet:fqdn=vertex.link]</code>	Create the FQDN vertex.link
Create multiple nodes	<code>[inet:fqdn=vertex.link inet:ipv4=1.2.3.4]</code>	Create the FQDN vertex.link and the IPv4 1.2.3.4
Create a node and set properties	<code>[ou:org=* :name=vertex :url=https://vertex.link]</code>	Create an organization node for The Vertex Project and set the name and url properties
Create multiple nodes and set a property for all of them	<code>[inet:ipv4=120.132.81.0/24 :loc=cn]</code>	Create the 256 IPv4 addresses in the specified CIDR block and set all of their location properties to CN (China)
Set /modify a property	<code>inet:ipv4=1.2.3.4 [:loc=au]</code>	Set the location property for IPv4 1.2.3.4 to AU (Australia)
Set a property for multiple nodes	<code>inet:ipv4=1.2.3.4 inet:ipv4=5.6.7.8 [:asn=6805]</code>	Set the AS property for IPv4 1.2.3.4 and IP 5.6.7.8 to AS 6805
Remove a property	<code>inet:ipv4=1.2.3.4 [-:loc]</code>	Remove the location property from IPv4 1.2.3.4
Remove a property from multiple nodes	<code>inet:ipv4=1.2.3.4 inet:ipv4=5.6.7.8 [-:latlong]</code>	Remove the geolocation (latitude / longitude) property from IPv4 1.2.3.4 and IPv4 5.6.7.8
Set / modify an array property	<code>ou:org:alias=vertex [:names=('the vertex project',)]</code>	Set the 'names' array property for The Vertex Project
Add a value to an array	<code>ou:org:alias=vertex [:names+=vertex]</code>	Add the name 'vertex' to the names array property for The Vertex Project
Remove a value from an array	<code>ou:org:alias=vertex [:names-=vertex]</code>	Remove the name 'vertex' from the names array property for The Vertex Project

Edit Brackets - Tags		
Add a tag	<code>inet:fqdn=evil.com [+#rep.eset.sednit]</code>	Add the tag #rep.eset.sednit ("ESET reports this indicator as Sednit") to the FQDN evil.com
Remove a base tag	<code>inet:fqdn=evil.com [-#rep.eset.sednit]</code>	Remove the tag #rep.eset.sednit from evil.com (leaves the tag #rep.eset)
Remove a full tag	<code>inet:fqdn=evil.com [-#rep]</code>	Remove any / all tags starting with #rep from evil.com
Add a tag with timestamp	<code>inet:ipv4=1.1.1.1 [+#cno.infra.anon.tor=2022/09/01]</code>	Add a tag to show the IP was a TOR node on Sept 1, 2022
Add a tag with time range	<code>inet:ipv4=1.1.1.1 [+#cno.infra.anon.tor=(2022/09/01, 2022/09/18)]</code>	Add a tag to show the IP was a TOR node between Sept 1 and Sept 18, 2022

Edit Brackets with Edit Parentheses		
Parentheses can be used inside of edit brackets to isolate specific edit operations and prevent them from being applied to other nodes in the pipeline.		
Create multiple nodes with different properties	<code>[(inet:ipv4=4.4.4.4 :loc=us) (inet:ipv4=111.111.111.111 :loc=jp)]</code>	Create IPv4 4.4.4.4 with location US and IPv4 111.111.111.111 with location JP

Edit Try Operator		
The edit try operator (?=) attempts to create a node or set a property with the specified value. Edit try allows Synapse to "fail silently" and continue (vs. error and halting) if the value is invalid for the property.		
Use edit try to create a node	<code>[inet:fqdn?=info@vertex.link]</code>	Try to create an FQDN with the value 'info@vertex.link'
Use edit try to set a property	<code>inet:ipv4=1.2.3.4 [:asn?=amazon]</code>	Try to set the ASN property of IPv4 1.2.3.4 to 'amazon'
Use edit try to set an array property	<code>ps:contact:name=visi [:emails?+=visi@vtx.lk]</code>	Try to add an email to the emails array of the contact for 'visi'

For a complete list of Storm edit operations and additional examples, see the [Data Modification](#) section of the [Storm Reference Guide](#).