MISP

INTELLIGENCE SHARING

MISP - Galaxy 2.0

Method for sharing threat intelligence

Team CIRCL

info@circl.lu

November 4, 2026

Outline of the presentation

- Present the features available for Sharing *galaxy clusters*
- Look at the internals of what changed in the datamodel and MISP's behaviors

MISP Galaxy 2.0

Galaxy 2.0 introduces various new features for *Galaxies* and their *Clusters* allowing:

- Creation of **custom** *Clusters*
- **ACL** on *Clusters*
- **Connection** of *Clusters* via *Relations*
- **Synchronization** to connected instances.
- **Visualization** of forks and relationships

Default Galaxy clusters

Default *Galaxy cluster*

- Coming from the `misp-galaxy` repository[1]
- Cannot be edited
  - Only way to provide modification is to modify the stored JSON or to open a pull request
  - Are not synchronized
  - Source of trust
- Restrictions propagate to their children (`Galaxy cluster elements`, `Cluster relationships`)

Custom *Galaxy cluster*

- Can be created via the UI or API
- Belongs to an organisation
  - Fully editable
  - Are synchronized

[1] https://github.com/MISP/misp-galaxy

MISP Galaxy 2.0 - Comparison with prior version

Clusters and *Relations* can be edited.

- New *Clusters* fields
  - `distribution`, `sharing_group_id`
  - `org_id`, `orgc_id`
  - `locked`, `published`, `deleted`
  - `default`
    - *Clusters* coming from the `misp-galaxies` repository are marked as default
    - Not synchronized
    - Same purpose as *Event*'s `locked` field
  - `extends_uuid`
    - Point to the *Cluster* that has been forked
  - `extends_version`
    - Keep track of the *Cluster* version that has been forked

MISP Galaxy 2.0 - Others changes

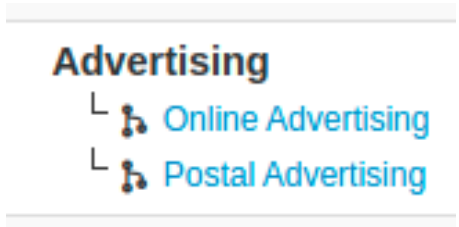
- *Role* `perm_galaxy_editor`
- Relations also have a `distribution` and can have *Tags*
- Synchronization servers have 2 new flags
  - `pull_galaxy_clusters`
  - `push_galaxy_clusters`
- Clusters `blocklist`

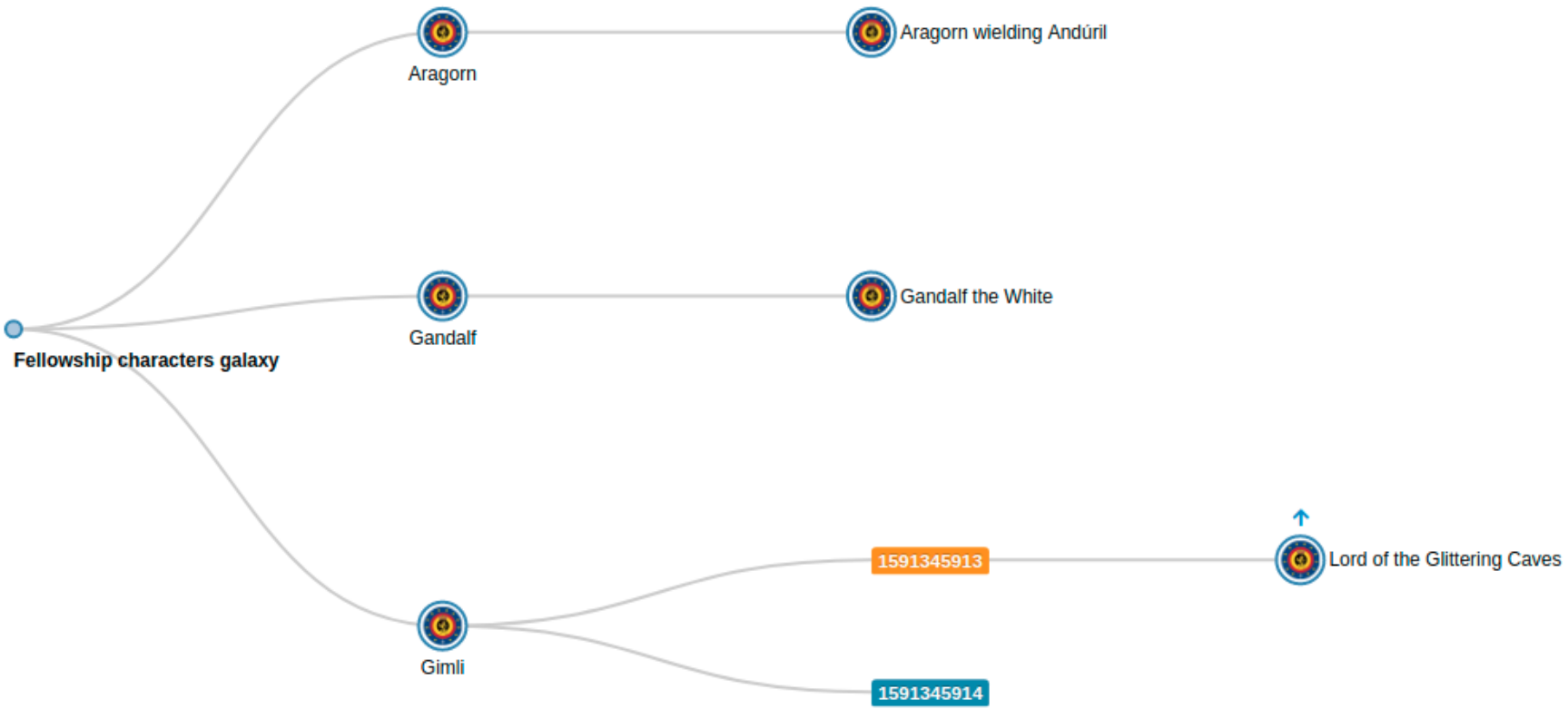
Features in depth: CRUD

- Standard CRUD
- Soft and Hard deletion
- Publishing
- Update forked cluster to keep it synchronized with its parent
- ACL on the *Cluster* itself, not on its tag
  - `misp-galaxy:galaxy-type="cluster UUID"`
  - `misp-galaxy:mitre-attack-pattern="e4932f21-4867-4de6-849a-1b11e48e2682"`

Features in depth: Visualization

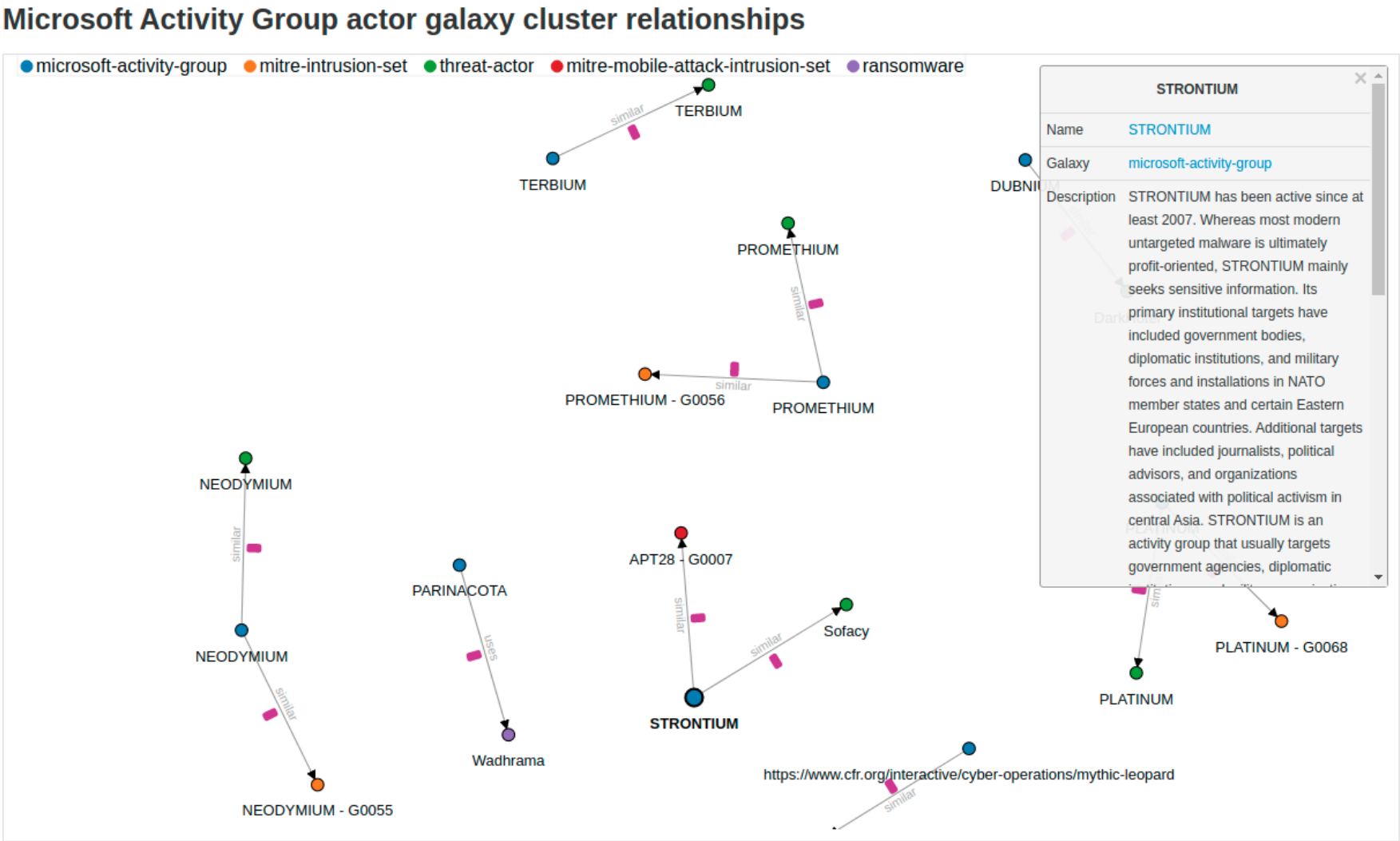
Tree view of forked Clusters





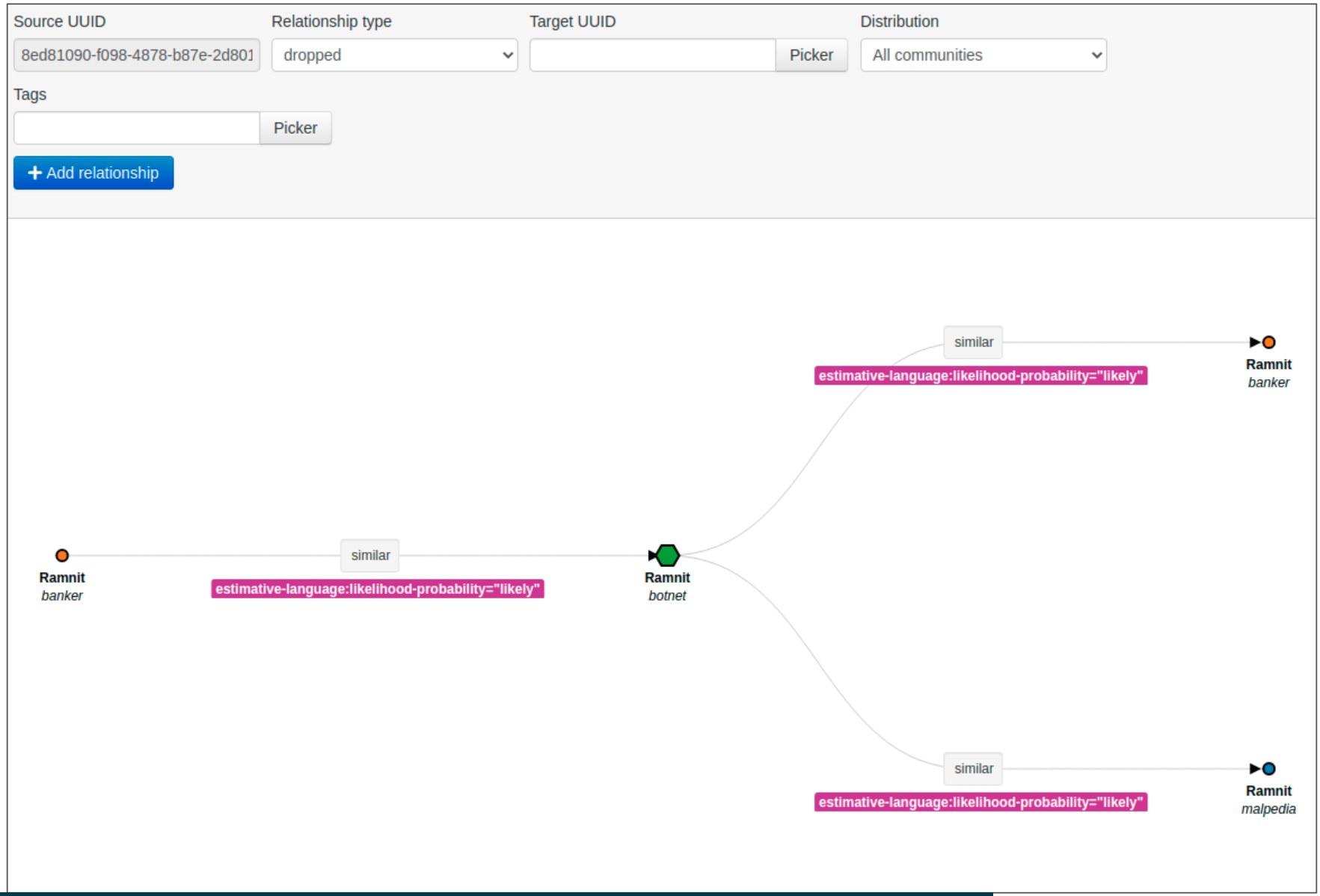
Features in depth: Visualization

Tree and network views for Relations between Clusters



Features in depth: Visualization

Tree and network views for Relations between Clusters

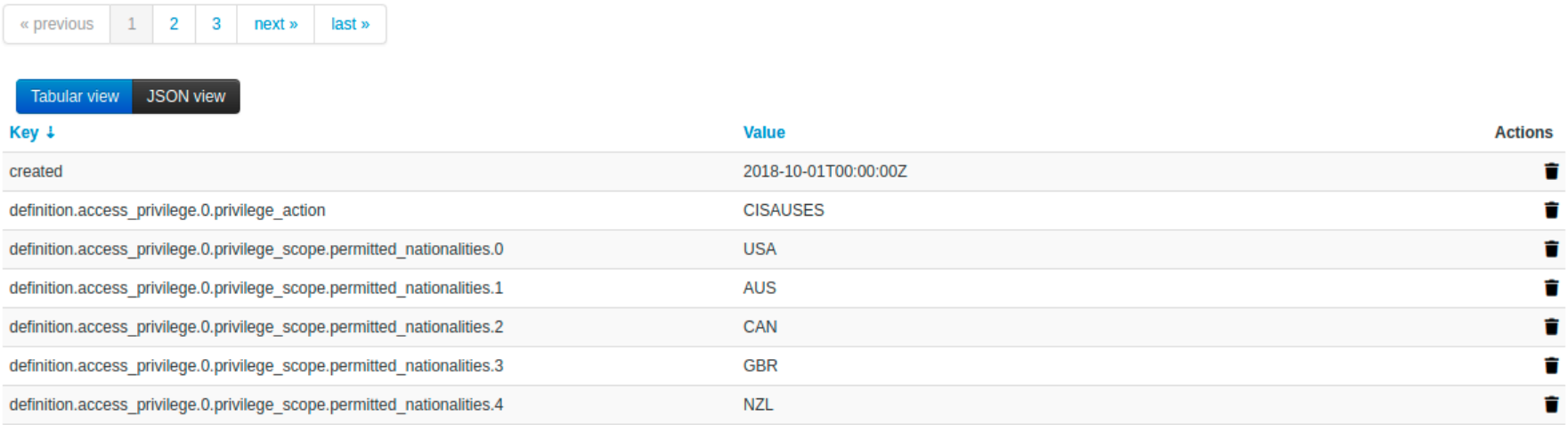


Galaxy cluster elements

Hasn’t been touched: Still a key-value stored. But new feature have been added[2]

Tabular view

- Allows you to browse **cluster elements** like before



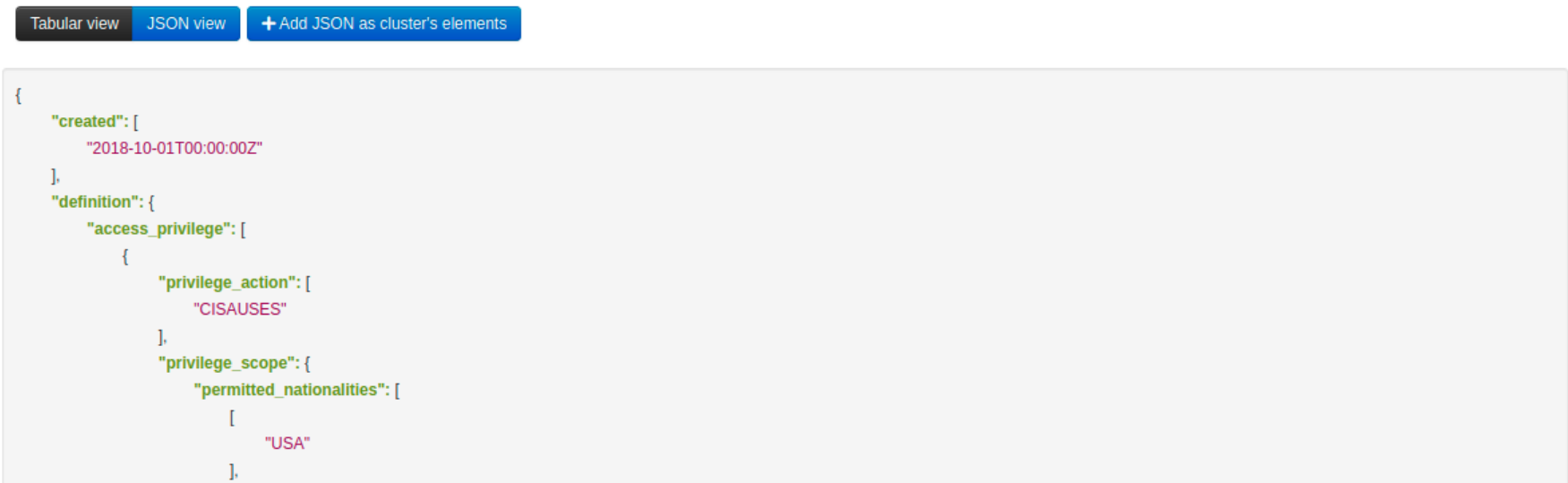
Key ↓	Value	Actions
created	2018-10-01T00:00:00Z	
definition.access_privilege.0.privilege_action	CISAUSES	
definition.access_privilege.0.privilege_scope.permitted_nationalities.0	USA	
definition.access_privilege.0.privilege_scope.permitted_nationalities.1	AUS	
definition.access_privilege.0.privilege_scope.permitted_nationalities.2	CAN	
definition.access_privilege.0.privilege_scope.permitted_nationalities.3	GBR	
definition.access_privilege.0.privilege_scope.permitted_nationalities.4	NZL	

[2]Will be included in next release

Galaxy cluster elements

JSON view

- Allows you to visualisation **cluster element** in a JSON structure
- Allows you to convert any JSON into **cluster elements** enabling searches and correlations



Synchronization in depth

Has its own synchronization mechanism which can be enabled with the `pull_galaxy_cluster` and `push_galaxy_cluster` flags

- **Pull All**: Pull all remote Clusters (similar to event's pull all)
- **Pull Update**: Update local Clusters (similar to event's pull update)
- **Pull Relevant**: Pull missing Clusters based on local Tags
- **Push**: Triggered whenever a Cluster is published or via standard push