

# MISP - GALAXY 2.0

METHOD FOR SHARING THREAT INTELLIGENCE

TEAM CIRCL

INFO@CIRCL.LU

APRIL 15, 2024



2024-04-15

MISP - Galaxy 2.0

MISP - GALAXY 2.0

METHOD FOR SHARING THREAT INTELLIGENCE

TEAM CIRCL

INFO@CIRCL.LU

APRIL 15, 2024



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

### └ 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

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

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

## Default *Galaxy cluster*

- Coming from the `misp-galaxy` repository<sup>1</sup>
- 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

<sup>1</sup><https://github.com/MISP/misp-galaxy>

## └─ Default Galaxy clusters

**Default Galaxy cluster**

- Coming from the `misp-galaxy` repository<sup>1</sup>
- 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

<sup>1</sup><https://github.com/MISP/misp-galaxy>

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

2024-04-15

## └─ 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

- *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 blacklist

### └─ 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 blacklist

- 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: CRUD

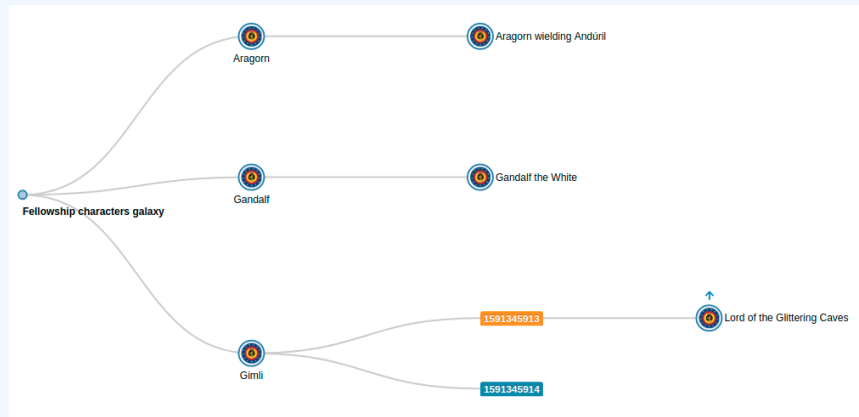
- Standard CRUD
- Soft and Hard deletion
- Publishing
- Update forked cluster to keep it synchronized with its parent
- ACL on the Cluster itself, not on its tag
  - ▶ `misp-galaxy:galaxy-type="cluster UUID"`
  - ▶ `misp-galaxy:mitre-attack-pattern="e4932f21-4867-4de6-849a-1b11e48e2682"`

# FEATURES IN DEPTH: VISUALIZATION

## Advertising

- Online Advertising
- Postal Advertising

## Tree view of forked Clusters



2024-04-15

## MISP - Galaxy 2.0

## Features in depth: Visualization

- Advertising
  - Online Advertising
  - Postal Advertising

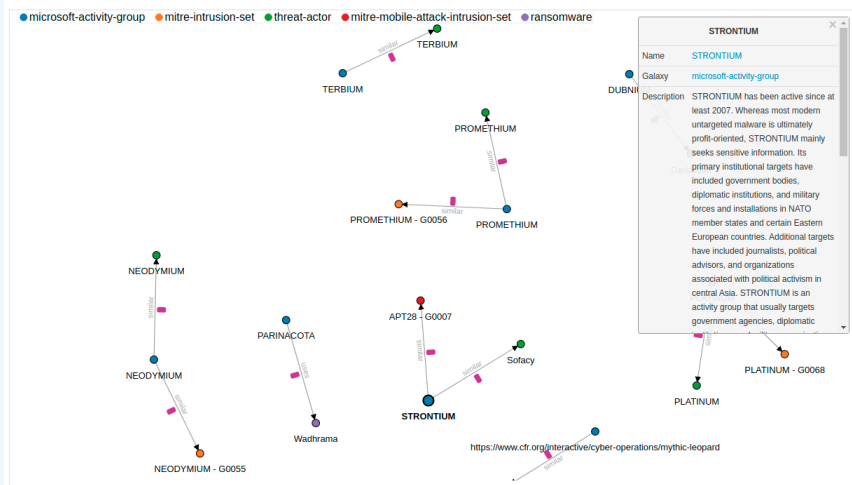
### Tree view of forked Clusters





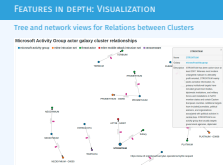
## Tree and network views for Relations between Clusters

### Microsoft Activity Group actor galaxy cluster relationships



2024-04-15

## Features in depth: Visualization



# FEATURES IN DEPTH: VISUALIZATION

## Tree and network views for Relations between Clusters

Source UUID: 8ed81090-f098-4878-b87e-2d801  
Relationship type: dropped  
Target UUID:  Picker  
Distribution: All communities

Tags:  Picker

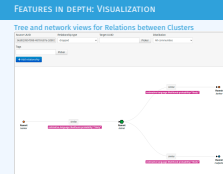
[+ Add relationship](#)

```
graph LR; RB1((Ramnit banker)) --- similar[similar] --- RB2((Ramnit banker)); RB2 --- similar[similar] --- RB3((Ramnit banker)); RB3 --- similar[similar] --- RB4((Ramnit malpedia)); RB4 --- similar[similar] --- RB5((Ramnit botnet)); RB5 --- similar[similar] --- RB6((Ramnit banker));
```

2024-04-15

MISP - Galaxy 2.0

└─ Features in depth: Visualization



Hasn't been touched: Still a key-value stored. But new feature have been added<sup>2</sup>

## Tabular view

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

« previous 1 2 3 next » last »

Tabular view JSON view

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	🗑️

<sup>2</sup>Will be included in next release

### └─ Galaxy cluster elements

Hasn't been touched: Still a key-value stored. But new feature have been added<sup>2</sup>

#### Tabular view

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

« previous 1 2 3 next » last »

Tabular view JSON view

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	🗑️

<sup>2</sup>Will be included in next release

## 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

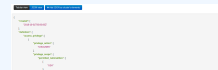
Tabular view JSON view + Add JSON as cluster's elements

```
{
  "created": [
    "2018-10-01T00:00:00Z"
  ],
  "definition": {
    "access_privilege": [
      {
        "privilege_action": [
          "CISAUSES"
        ],
        "privilege_scope": {
          "permitted_nationalities": [
            "USA"
          ]
        }
      }
    ]
  }
}
```

2024-04-15

## 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



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

2024-04-15

MISP - Galaxy 2.0

## └ 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