

Tree View

By Steven

介紹

Grafana 的插件之一。適用於有層級關係的資料型態，顯示由數據來源提供的記錄。官方推薦使用此插件時使用 JSON API。

設定&操作

1. 資料格式概況

範例資料包含來源 IP、目標 IP、Port、傳輸行為等。

```
Forti.csv - 記事本
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明
"timx", "sourceAddress", "sourcePort", "destinationAddress", "destinationPort", "action", "bytes"
2022-03-15 00:19:32,10.191.101.91,54896,162.247.243.146,443,accept,4704
2022-03-15 00:19:32,10.191.101.91,53352,162.247.243.146,443,accept,2047
2022-03-15 00:19:32,10.191.200.83,61661,101.32.104.4,443,accept,5911
2022-03-15 00:19:30,10.191.101.234,58215,104.18.17.184,443,accept,12263
2022-03-15 00:19:32,10.191.100.183,55223,142.251.43.10,443,accept,2114
2022-03-15 00:19:32,10.191.101.91,59942,172.217.163.42,443,accept,279
2022-03-15 00:19:32,10.191.101.231,55321,76.223.31.44,443,accept,1036
2022-03-15 00:19:32,10.191.200.168,52765,64.233.189.188,443,accept,279
2022-03-15 00:19:32,10.191.100.9,49710,142.251.43.10,443,accept,6770
```

2. plugin 設定概況

Tree View Configuration:

- Tree root name: 1 line, Root
- Field template engine: Simple
- Tree level definitions: Separated by newline. Use Series variable name in order to take difference several series.
 - Action: \${action.keyword}
 - 來源IP: \${sourceAddress.keyword}
 - 目標IP: \${destinationAddress.keyword}
 - 數量: \${Count}
- Series column name: Series name added as a new column. The value is unspecified in Table view. Example for usage in Tree level definitions: \${seriesColumn} or {seriesColumn}
- Expanded levels: Number of levels expanded by default. Applied after save and apply (page refresh). 1
- Show item count: ☒
- Order in each level: Ascendent

Tree View Data:

- Root (2971)
 - Action : accept (671)
 - 來源IP : 10.1.250.41 (1)
 - 目標IP : 52.179.219.14 (1)
 - 數量 : 3
 - 來源IP : 10.103.2.1 (1)
 - 來源IP : 10.103.2.2 (1)
 - 來源IP : 10.103.254.251 (1)

Query Configuration:

- Data source: fort2
- Query options: MD = auto = 1488 Interval = 3h
- Query: Lucene Query
- Metric (3): Count
- Group By: Terms, destinationAddress.keyword, Min Doc Count: 1, Order by: Term value (desc)
- Then By: Terms, sourceAddress.keyword, Min Doc Count: 1, Order by: Term value (desc)
- Then By: Terms, action.keyword, Min Doc Count: 1, Order by: Term value (desc)

*Tree root name 根名稱

*Field template engine 字段模板(選 Simple 即可)

*Tree level definitions 主要定義處

語法如下：

`${欄位名稱}`

換行即進入下一層

`${欄位名稱}`

前面+字即顯會顯示在圖表上

範例：

Tree level definitions

Separated by endline. Use Serie variable name in order to take difference several series

```
Action : ${action.keyword}
來源IP : ${sourceAddress.keyword}
目標IP : ${destinationAddress.keyword}
數量 : ${Count}
```

*Serie column name 欄目名稱(尚不清楚此功能作用)

*Expanded levels 展開級別(尚不清楚此功能作用)

*Show item count 是否顯示下方圖片中括弧中的數量

```
▼ Root (2971)
  ▼ Action : accept (671)
```

*Order in each level 排序方式