

31. GIẢI PHÁP-TESTING - Task #1360

Task # 1211 (Closed): Cài đặt server log tập trung

Scripts lấy thông tin network bytes trên elasticsearch

02-12-2024 08:41 - Minh Pham

Trạng thái:	Closed	Bắt đầu:	25-11-2024
Mức ưu tiên:	Normal	Hết hạn:	08-12-2024
Phân công cho:	Minh Pham	Tiến độ:	0%
Chủ đề:		Thời gian ước lượng:	0:00 giờ
Phiên bản:		Thời gian:	0:00 giờ

Mô tả

Mục tiêu: Scripts lấy thông tin network bytes trên elasticsearch

Kết quả thực hiện :

Script lấy tổng bằng thông trong vòng 2 ngày trên elasticseach

```
History Settings Help 200 - OK 450 ms
1 POST /elastiflow-flow-ecs-*/_search
2 {
3   "_source": ["none"]
4 },
5 "query": {
6   "bool": {
7     "must": [
8       {
9         "range": {
10          "@timestamp": {
11            "gte": "now-2d/d",
12            "lte": "now/d"
13          }
14        },
15        {
16          "term": {
17            "client.domain": {
18              "value": "103.48.194.12"
19            }
20          }
21        }
22      ]
23    }
24  },
25  "aggs": {
26    "total_network_bytes": {
27      "sum": {
28        "field": "network.bytes"
29      }
30    }
31  }
32 }
33 }
34
52 {
53   "_index": "elastiflow-flow-ecs-1.7-1.5-rollover-000204",
54   "_type": "_doc",
55   "_id": "CHjwhJMBkIcmg_hiBhiy",
56   "_score": 12.21894,
57   "_source": { }
58 },
59
60 {
61   "_index": "elastiflow-flow-ecs-1.7-1.5-rollover-000204",
62   "_type": "_doc",
63   "_id": "x3frhJMBkIcmg_hiinF8",
64   "_score": 12.21894,
65   "_source": { }
66 },
67
68 {
69   "_index": "elastiflow-flow-ecs-1.7-1.5-rollover-000204",
70   "_type": "_doc",
71   "_id": "JHfghJMBkIcmg_hip1DC",
72   "_score": 12.21894,
73   "_source": { }
74 },
75
76 {
77   "_index": "elastiflow-flow-ecs-1.7-1.5-rollover-000204",
78   "_type": "_doc",
79   "_id": "O3fthJMBkIcmg_hiEKji",
80   "_score": 12.21894,
81   "_source": { }
82 },
83
84 {
85   "_index": "elastiflow-flow-ecs-1.7-1.5-rollover-000204",
86   "_type": "_doc",
87   "_id": "dXG_hJMBkIcmg_hiC0ei",
88   "_score": 12.21894,
89   "_source": { }
90 },
91
92 "aggregations": {
93   "total_network_bytes": {
94     "value": 1.6623712E9
95   }
96 }
```

```

Console Search Profiler Grok Debugger Painless Lab BETA
History Settings Help
1 POST /elastiflow-flow-ecs-*/_search
2 {
3   "_source": ["none"]
4 },
5   "query": {
6     "bool": {
7       "must": [
8         {
9           "range": {
10            "@timestamp": {
11              "gte": "now-2d/d",
12              "lte": "now/d"
13            }
14          }
15        },
16        {
17          "term": {
18            "server.domain": {
19              "value": "103.48.194.12"
20            }
21          }
22        }
23      ]
24    }
25  },
26  "aggs": {
27    "total_network_bytes": {
28      "sum": {
29        "field": "network.bytes"
30      }
31    }
32  }
33 }
34
52 {
53   "_index": "elastiflow-flow-ecs-1.7-1.5-rollover-000204",
54   "_type": "doc",
55   "_id": "EXn7hJMBkIcmg_hivtyx",
56   "_score": 10.563283,
57   "_source": { }
58 },
59 {
60   "_index": "elastiflow-flow-ecs-1.7-1.5-rollover-000204",
61   "_type": "doc",
62   "_id": "3Xn7hJMBkIcmg_hiUctU",
63   "_score": 10.563283,
64   "_source": { }
65 },
66 {
67   "_index": "elastiflow-flow-ecs-1.7-1.5-rollover-000204",
68   "_type": "doc",
69   "_id": "DXn7hJMBkIcmg_hiWc0h",
70   "_score": 10.563283,
71   "_source": { }
72 },
73 {
74   "_index": "elastiflow-flow-ecs-1.7-1.5-rollover-000204",
75   "_type": "doc",
76   "_id": "M3n7hJMBkIcmg_hiaM_D",
77   "_score": 10.563283,
78   "_source": { }
79 },
80 {
81   "_index": "elastiflow-flow-ecs-1.7-1.5-rollover-000204",
82   "_type": "doc",
83   "_id": "_3n5hJMBkIcmg_hi4pAh",
84   "_score": 10.563283,
85   "_source": { }
86 },
87 }
88 },
89 "aggregations": {
90   "total_network_bytes": {
91     "value": 7.1735104E9
92   }
93 }
94 }
95

```

Convert từ Byte sang Mebibytes
<https://www.dataunitconverter.com/byte-to-mebibyte/7173510400>

Bytes to Mebibytes - 1662371200 Byte to MiB Conversion

DATA SIZE TRANSFER RATE

From: Byte (B) To: Mebibyte (MiB)

Byte --to--> Mebibyte (binary)

1662371200 Byte **→ CONVERT**

RESULT

Bytes(B) → Megabyte(MB) ✓ Bytes(B) → Mebibyte(MiB)

1,662,371,200 Byte
= 1,585.3607177734375 MiB
 (Equal to 1.5853607177734375E+3 MiB)

Calculated as → $1662371200 \div 1024^2$ **Show Steps**

Max Decimals in result: 40

