AnaTraf

网络流量分析仪

HTTPS API 使用手册

Version 1.1.0

文档说明

AnaTraf HTTPS API 接口是一套为第三方应用程序提供的与 AnaTraf 进行交互的接口。通过 API，用户的应用程序可以从 AnaTraf 获取网络流量的统计数据。

通过此文档，用户可以快速了解各个接口的功能、参数设置范围、返回值的含义和发生错误的具体位置。

AnaTraf HTTPS API 使用 JSON（JavaScript Object Notation）作为数据交换格式，因此，用户需要对 JSON 数据格式有所了解，以便轻松解析和使用 API。

使用说明

基础信息

- **基础 URL**：`https://<设备IP地址>`（例如：`https://192.168.1.234`）
- **请求头 Content-Type**：`application/json`
- **认证方式**：在请求头中添加 `authorization` 字段，值为登录接口返回的 `token`。

API 设计理念

一个接口，承载所有数据查询，从分析仪获取 2-7层的任何数据，都通过这个统一的接口： POST | /api/datasources/query。

无论您需要获取何种类型的数据（如指标、图表数据等），均需向该接口发送一份包含查询信息的 JSON 请求体，服务端将根据该查询返回相应的数据结果。

设备登录

接口类型	api	接口描述
POST	/api/user/login	用户登录接口，调用成功后返回包含 token 的响应。该 token 应放入后续请求的 `authorization` 请求头中。

请求头：

- `Content-Type: application/json`

请求 json 示例：

```
{
  "username": "your_username",                    // 用户名
  "password": "your_password"                     // 密码
}
```

成功响应 json 示例（200 OK）：

```
{
  "token": "AV8rk4KXFY1hnh8P",                    // 登录成功后的 token，直接使用此值作为后续请求的 authorization header
  "code": 0,                                      // 状态码，0 表示成功
  "message": "Success"                            // 响应信息
}
```

> **重要提示：**
>
> 1. 登录成功后获得的 `token` 需要直接作为 `authorization` 请求头的值。
> 2. 示例：如果 token 为 `AV8rk4KXFY1hnh8P`，则请求头应设置为：`authorization: AV8rk4KXFY1hnh8P`
> 3. Token 的有效期请参考设备配置，过期后需要重新登录获取新的 token。

L2 - L7 数据获取

列举可用的查询

接口类型	api	接口描述
GET	/api/datasources/metrics/find	列举可用的查询

> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

返回响应	格式	
成功响应（200 OK）	application/json	
字段名	**类型**	**描述**
code	int	状态码，0 表示成功
message	string	响应信息
data	array[object{3}]	响应信息

该接口将返回分析仪**所有统计字段**，响应的 json 内容庞大。为方便使用，将分析仪所有的统计字段按照 WEB 界面的分层逻辑列举在附录。

获取数据

接口类型	api	接口描述
POST	/api/datasources/query	从数据源获取数据

请求头：

- `Content-Type: application/json`
- `authorization: <登录获取的token>`

queries 数组中每个查询对象参数说明：

参数名	类型	必填	说明	示例值
count	int	是	查询数据条数	20
reverse	boolean	是	是否反向排序	true
sort_by	string	是	数据排序字段，使用字段ID（如 l3.ip_address.bytes）。字段ID可通过列举可用的查询接口获取	"l3.ip_address.bytes"
start	int	是	从第几条开始查询（分页起始位置）	0
expr	string	否	过滤表达式，用于筛选数据，空字符串表示不过滤	"" 或 "ip_address==192.168.1.1"
target	array	是	查询目标列表，包含要查询的字段	见下方示例

target 数组中每个字段对象参数说明：

参数名	类型	必填	说明	示例值
field	string	是	字段ID，可通过列举可用的查询接口获取	"l2.mac.mac_address"
format	string	是	呈现数据的方式：`table`（表格数据）或 `time_series`（时间序列数据）	"table"
group_id	string	条件必填	当 format 为 `time_series` 时必填，用于将多个字段打包在一个组中，相同 group_id 的字段会合并显示	"每秒流量(图表)"

请求 json 示例（查询 L3 IP 地址统计）：

以下示例展示了如何查询 L3 IP 地址的详细统计信息，包括基本信息、流量统计、TCP 性能指标等。

```
{
  "from": -60,                                          // 开始时间，相对时间，-60 表示60秒前
  "to": 0,                                              // 结束时间，相对时间，0 表示当前最新时间
  "queries": [                                          // 请求的数据源列表
    {
      "count": 20,                                      // 查询数据条数，返回前20条
      "expr": "",                                       // 过滤表达式，空字符串表示不过滤
      "reverse": true,                                  // 是否反向排序，true 表示降序
      "sort_by": "l3.ip_address.bytes",                 // 数据排序字段，按总字节数降序排列
```

```
      "start": 0,                                                    // 从第几条开始查询，0 表示从第一条开始
      "target": [                                                    // 查询目标列表，包含要查询的所有字段
        {
          "field": "l3.ip_address.ip_address",                       // IP地址
          "format": "table"
        },
        {
          "field": "l3.ip_address.ip_dhcp_name",                     // DHCP主机名
          "format": "table"
        },
        {
          "field": "l3.ip_address.dns_name",                         // DNS域名
          "format": "table"
        },
        {
          "field": "l3.ip_address.http_name",                        // HTTP主机名
          "format": "table"
        },
        {
          "field": "l3.ip_address.tls_name",                         // TLS主机名
          "format": "table"
        },
        {
          "field": "l3.ip_address.ip_os_name",                       // 操作系统
          "format": "table"
        },
        {
          "field": "l3.ip_address.ip_group_name",                    // IP组名
          "format": "table"
        },
        {
          "field": "l3.ip_address.region",                           // 国家/地区
          "format": "table"
        },
        {
          "field": "l3.ip_address.mac_address",                      // 最近的MAC地址
          "format": "table"
        },
        {
          "field": "l3.ip_address.tx_bytes",                         // 总发送字节数
          "format": "table"
        },
        {
          "field": "l3.ip_address.rx_bytes",                         // 总接收字节数
          "format": "table"
        },
        {
          "field": "l3.ip_address.peer_ip_count",                    // 对等IP数
          "format": "table"
        },
```

```
        {
          "field": "l3.ip_address.l7_protocol",                    // 应用层协议
          "format": "table"
        },
        {
          "field": "l3.ip_address.tx_bps",                         // 每秒发送流量（用于图表）
          "format": "time_series",
          "group_id": "每秒流量(图表)"                               // format为time_series
类型的情况下需要填写分组id
        },
        {
          "field": "l3.ip_address.rx_bps",                         // 每秒接收流量（用于图表）
          "format": "time_series",
          "group_id": "每秒流量(图表)"                               // 相同 group_id 的字段
的值将打包在一个组中
        }
      ]
    }
  ],
  "is_history": false,                                             // 是否查询历史数据
  "link_id": 0,                                                    // 虚拟链路ID，0表示所有链
路
  "is_persistence": false                                          // 是否持久化查询
}
```

> **说明：**
>
> - 以上示例仅展示了部分常用字段。实际查询时，您可以根据需要在 `target` 数组中添加更多字段。
> - 完整的可用字段列表请参考附录：各分析模块可用的查询字段。
> - 一个 `target` 数组中可以包含多个字段，但同一查询中的字段不能跨层（如不能同时包含 `l2.xxx` 和 `l3.xxx`）。

> **重要提示：**
>
> 1. 可以在一个数据获取请求（queries）中包含多次查询（query），即 queries array 中可以包含多个项。
> 2. 一个 target 中可以包含多个字段。
> 3. 在一个 query 的 target 中包含的字段**不能跨层**，如： target 中的 field 字段不能同时存在 l2.xxx.xxx 和 l3.xxx.xxx。如果需要在一个数据获取请求（queries）请求不同层的数据，需要拆分成不同的查询（query）。
> 4. `from` 和 `to` 参数使用相对时间（秒），负数表示过去的时间，0 表示当前时间。例如：`from: -60, to: 0` 表示查询过去60秒到当前的数据。
> 5. `expr` 参数支持过滤表达式，可用于筛选特定条件的数据。例如：`"expr": "ip_address==192.168.1.1"` 表示只查询IP地址为192.168.1.1的数据。

返回响应 json 示例：

响应数据结构说明：

字段路径	类型	说明
`code`	int	状态码，0 表示成功
`message`	string	响应消息
`data`	object	数据部分，包含查询结果
`data.from`	int	数据的时间范围开始时间（秒级时间戳）
`data.to`	int	数据的时间范围结束时间（秒级时间戳）
`data.start`	int	实际查询的时间范围开始时间（秒级时间戳）
`data.end`	int	实际查询的时间范围结束时间（秒级时间戳）
`data.granularity`	int	时间粒度（秒）
`data.result`	array	查询结果数组，每个元素对应一个查询（queries 中的一项）
`data.result[].refId`	string	查询引用ID（可选，某些情况下可能不存在）
`data.result[].data`	object	数据值对象
`data.result[].data.values`	array	数据值数组，每个元素对应一个字段，顺序与 `target` 数组中的字段顺序一致。每个 `values` 元素本身是一个数组，包含所有数据行在该字段上的值
`data.result[].info`	object	查询信息对象
`data.result[].info.total`	int	符合查询条件的总数据条数
`data.result[].schema`	object	字段定义对象
`data.result[].schema.fields`	array	字段定义数组，描述每个字段的类型和名称。对于 `time_series` 类型的字段，`schema.fields` 中会包含一个特殊的字段定义，其 `type` 为 `time_series`，内部包含 `fields` 数组，描述时间序列中的各个字段

```
{
    "code": 0,                                                    // 状态码，0 表示成功
    "data": {
        "end": 1765162850,                                        // 全部数据结束时间（秒级时间戳）
        "from": 1765162790,                                       // 全部数据开始时间（秒级时间戳）
        "granularity": 1,                                         // 当前数据的时间粒度（秒）
        "result": [                                               // 数据结果数组，每个元素对应
queries 中的一项查询
            {
                "refId": "A",                                     // 查询引用ID（可选，某些情况下可
能不存在）
                "data": {                                         // 数据值
                    "values": [
                        [                                         // 第1个字段：IP地址（对应
target[0]）
                            "192.168.1.139",
```

```
                        "192.168.1.234",
                        "192.168.1.119",
                        "192.168.1.245",
                        "192.168.1.246"
                        // ... 更多IP地址（共20个）
                    ],
                    [                                   // 第2个字段：DHCP主机名（对应
target[1])
                        null,                           // 第1个IP没有DHCP主机名
                        null,                           // 第2个IP没有DHCP主机名
                        null,
                        null,
                        null
                        // ... 更多值
                    ],
                    [                                   // 第3个字段：DNS域名（对应
target[2])
                        null,
                        null,
                        null,
                        null,
                        null
                        // ... 更多值
                    ],
                    [                                   // 第4个字段：HTTP主机名（对应
target[3])
                        null,
                        null,
                        null,
                        null,
                        null
                        // ... 更多值
                    ],
                    [                                   // 第5个字段：TLS主机名（对应
target[4])
                        null,
                        null,
                        null,
                        null,
                        null
                        // ... 更多值
                    ],
                    [                                   // 第6个字段：操作系统（对应
target[5])
                        ["Intel Mac OS X 10_15_7"],     // 数组类型，可能包含多个值
                        ["Windows 10"],
                        ["Linux x86_64"],
                        ["Windows 10"],
                        null
                        // ... 更多值
                    ],
```

```
                    [                                       // 第7个字段：IP组名（对应
target[6]）
                        ["test", "阿水淀粉"],               // 数组类型，一个IP可能属于多个组
                        ["test"],
                        ["test"],
                        ["test"],
                        null
                        // ... 更多值
                    ],
                    [                                       // 第8个字段：国家/地区（对应
target[7]）
                        "本地地址",
                        "本地地址",
                        "本地地址",
                        "本地地址",
                        "荷兰|Zuid-Holland"
                        // ... 更多值
                    ],
                    [                                       // 第9个字段：MAC地址（对应
target[8]）
                        "b6:56:21:58:37:e6",
                        "74:27:ea:d0:b7:72",
                        "8e:69:a4:ae:8d:0d",
                        "52:54:00:cc:8c:11",
                        "f4:6d:2f:ad:fd:9f"
                        // ... 更多值
                    ],
                    [                                       // 第10个字段：总发送字节数（对应
target[9]）
                        2571857,
                        197577470,
                        1482608,
                        31032938,
                        18933314
                        // ... 更多值
                    ],
                    [                                       // 第11个字段：总接收字节数（对应
target[10]）
                        228981146,
                        0,
                        71799478,
                        1920404,
                        169930
                        // ... 更多值
                    ],
                    [                                       // 第12个字段：对等IP数（对应
target[11]）
                        68,
                        4,
                        52,
                        1,
                        1
```

```
                            // ... 更多值
                        ],
                        [                                   // 第13个字段：应用层协议（对应
target[12]）
                            ["TLS", "QQ", "DNS", "GoogleServices", "SSH", "QUIC", "NTP",
"Alibaba"],
                            ["TLS", "NTP", "WireGuard"],
                            ["DNS", "MDNS", "Xiaomi", "TLS", "STUN", "LLMNR"],
                            ["TLS"],
                            ["TLS"]
                            // ... 更多值
                        ],
                        [                                   // 第14个字段：时间序列数据（对应
target[13] 和 target[14]）
                            [                               // 第1个IP的时间序列数据
                                [                           // 时间数组（秒级时间戳）
                                    1765162790, 1765162791, 1765162792, 1765162793,
1765162794,
                                    1765162795, 1765162796, 1765162797, 1765162798,
1765162799,
                                    1765162800, 1765162801, 1765162802, 1765162803,
1765162804,
                                    // ... 更多时间点（共61个，对应60秒的数据）
                                    1765162849, 1765162850
                                ],
                                [                           // 每秒发送流量数组（bps）
                                    100368, 483840, 47768, 585696, 69952,
                                    524704, 34960, 545752, 60872, 626040,
                                    // ... 更多值（与时间数组长度相同）
                                    269880
                                ],
                                [                           // 每秒接收流量数组（bps）
                                    12605024, 48252664, 12583768, 48753344, 10898656,
                                    51259720, 8180544, 51068600, 8466776, 50250832,
                                    // ... 更多值（与时间数组长度相同）
                                    27662536
                                ]
                            ],
                            [                               // 第2个IP的时间序列数据
                                [
                                    1765162790, 1765162791, 1765162792, 1765162793,
1765162794,
                                    // ... 更多时间点
                                    1765162849, 1765162850
                                ],
                                [
                                    10713424, 40853712, 10457384, 42322888, 8962280,
                                    // ... 更多值
                                    26024288
                                ],
                                [
                                    0, 0, 0, 0, 0,
```

```
                                    // ... 更多值（全为0，表示该IP没有接收流量）
                                    0
                                ]
                            ]
                            // ... 更多IP的时间序列数据（共20个IP）
                        ]
                    ]
                },
                "info": {
                    "total": 509                                    // 符合查询条件的总数据条数（实际
返回20条）
                },
                "schema": {                                         // 字段定义，描述每个字段的类型和
名称
                    "fields": [
                        {
                            "id": "l3.ip_address.ip_address",
                            "name": "IP地址",
                            "type": "ip"
                        },
                        {
                            "id": "l3.ip_address.ip_dhcp_name",
                            "name": "DHCP主机名",
                            "type": "array"
                        },
                        {
                            "id": "l3.ip_address.dns_name",
                            "name": "DNS域名",
                            "type": "array"
                        },
                        {
                            "id": "l3.ip_address.http_name",
                            "name": "HTTP主机名",
                            "type": "array"
                        },
                        {
                            "id": "l3.ip_address.tls_name",
                            "name": "TLS主机名",
                            "type": "array"
                        },
                        {
                            "id": "l3.ip_address.ip_os_name",
                            "name": "操作系统",
                            "type": "array"
                        },
                        {
                            "id": "l3.ip_address.ip_group_name",
                            "name": "组名",
                            "type": "array"
                        },
                        {
                            "id": "l3.ip_address.region",
```

```
                        "name": "国家/地区",
                        "type": "string"
                    },
                    {
                        "id": "l3.ip_address.mac_address",
                        "name": "最近的MAC",
                        "type": "mac"
                    },
                    {
                        "id": "l3.ip_address.tx_bytes",
                        "name": "总发送字节数",
                        "type": "bytes"
                    },
                    {
                        "id": "l3.ip_address.rx_bytes",
                        "name": "总接收字节数",
                        "type": "bytes"
                    },
                    {
                        "id": "l3.ip_address.peer_ip_count",
                        "name": "对等IP数",
                        "type": "number"
                    },
                    {
                        "id": "l3.ip_address.l7_protocol",
                        "name": "应用层协议",
                        "type": "array"
                    },
                    {
                        "fields": [                         // time_series 类型的字段定义
                            {
                                "name": "x",
                                "type": "time"
                            },
                            {
                                "name": "每秒发送流量",
                                "type": "bps"
                            },
                            {
                                "name": "每秒接收流量",
                                "type": "bps"
                            }
                        ],
                        "name": "每秒流量(图表)",
                        "type": "time_series"
                    }
                ]
            }
        }
    ],
    "start": 1765156896,                                    // 查询数据起始时间（秒级时间戳）
    "to": 1765162850                                        // 查询数据终止时间（秒级时间戳）
```

```
    },
    "message": "Success"
}
```

重要提示：

1. 数据对应关系

- `values` 数组中的每个元素按顺序对应 `target` 数组中的字段，同时也对应 `schema.fields` 中相应位置的字段定义。
- 例如：`values[0]` 对应 `target[0]` 和 `schema.fields[0]`，`values[1]` 对应 `target[1]` 和 `schema.fields[1]`，以此类推。
- 每个 `values` 元素本身是一个数组，包含所有数据行在该字段上的值。例如：`values[0] = ["192.168.1.139", "192.168.1.234", ...]` 表示所有IP地址。

2. 数据类型说明

- **`array` 类型**：返回值为字符串数组（如 `["value1", "value2"]`）或 `null`。某些字段可能包含多个值，如一个IP可能有多个DNS域名、多个应用层协议等。数组类型的字段在 `schema.fields` 中的 `type` 为 `"array"`。
- **`time` 类型**：返回值为纳秒级时间戳（19位数字，如 `1765156896000041162`）。注意：响应中的 `start`、`end`、`from`、`to` 以及时间序列中的时间数组为秒级时间戳（10位数字）。
- **`time_series` 类型**：返回值为嵌套数组结构：
  - 第一层数组：对应不同的数据行（如不同的IP地址），数组长度为返回的数据行数
  - 第二层数组：每个数据行的时间序列数据，包含：
    - 第一个子数组：时间点数组（秒级时间戳），长度为时间序列数据点数量
    - 后续子数组：对应 `schema.fields` 中 `time_series` 类型字段的 `fields` 数组定义的各个字段的值数组（与时间数组长度相同）
  - 例如：查询了 `tx_bps` 和 `rx_bps` 两个字段，且它们有相同的 `group_id`，则时间序列数据包含3个子数组：时间数组、tx_bps值数组、rx_bps值数组。

3. 数据行数说明

- `info.total` 表示符合查询条件的总数据条数（如总共有509个IP地址）。
- 实际返回的数据条数由 `count` 参数决定（如返回前20条）。
- 可以通过调整 `start` 和 `count` 参数实现分页查询。

4. null 值处理

- 某些字段可能返回 `null`，表示该字段在当前数据中无值。
- 例如：`ip_dhcp_name` 为 `null` 表示该IP地址没有DHCP主机名。
- 数组类型的字段可能为 `null` 或空数组 `[]`，都表示没有值。

5. 时间序列数据说明

- 时间数组的长度等于查询时间范围除以时间粒度。例如：查询60秒的数据，时间粒度为1秒，则时间数组包含61个时间点（从开始时间到结束时间，包含两端）。

- 值数组中的元素数量与时间数组中的元素数量相同，一一对应。

将数据导出 csv

使用 API 将分析仪各个分析模块的表格数据导出 csv 文件需要使用以下两个接口。

步骤1：创建CSV导出任务

接口类型	api	接口描述
POST	/api/datasources/csv	创建CSV导出任务，响应中将得到一个 csv_token

请求头：

- `Content-Type: application/json`
- `authorization: <登录获取的token>`

请求体： 与获取数据接口中的请求体格式完全一致，使用相同的 JSON 结构

请求 json 示例：

```
{
  "from": -60,
  "to": 0,
  "queries": [
    {
      "count": 20,
      "expr": "",
      "reverse": true,
      "sort_by": "l3.ip_address.bytes",
      "start": 0,
      "target": [
        {
          "field": "l3.ip_address.ip_address",
          "format": "table"
        }
      ]
    }
  ],
  "is_history": false,
  "link_id": 0
}
```

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "message": "Success",
  "data": {
    "csv_token": "abc123def456"
  }
}
```

步骤2：下载CSV文件

接口类型	api	接口描述
GET	/api/datasources/csv	使用步骤1中得到的 csv_token 作为请求参数，下载 csv 文件

请求头：

- `authorization: <登录获取的token>`

请求参数：

参数名	类型	必填	说明	示例值
csv_token	string	是	步骤1返回的 csv_token	"abc123def456"

请求示例：

```
GET /api/datasources/csv?csv_token=abc123def456
```

响应：

- 成功：返回 CSV 文件内容（Content-Type: text/csv）
- 失败：返回 JSON 错误信息

> **提示：**
>
> 1. 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。
> 2. 如果 csv_token 已过期或无效，将返回错误响应。

下载 PCAP 文件

接口类型	api	接口描述
GET	/api/download	下载某个时间范围内，符合特定条件的 pcap 文件

请求参数	类型	描述
from	int	开始时间戳（秒级，10 位数）
to	int	结束时间戳（秒级，10 位数）
filter	string	过滤表达式，如：ip_address==192.168.1.199

> **提示：**
> 1.需要将登录成功获得的 token 作为 header 中 authorization 参数的值。
> 2.当分析仪根据提供的时间段以及过滤表达式没有检索到符合条件的数据包时，该接口将返回一个空的 pcap 文件（大小为 24B）。

虚拟链路管理

获取虚拟链路列表

接口类型	api	接口描述
GET	/api/vlan/list	获取分析仪当前虚拟链路的配置列表

请求头：

- `authorization: <登录获取的token>`

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "message": "Success",
  "data": [
    {
      "id": 0,
      "name": "默认链路",
      "vlan_id": 0,
      "description": "默认虚拟链路"
    }
  ]
}
```

> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

添加虚拟链路

接口类型	api	接口描述
POST	/api/vlan/list	添加虚拟链路

请求头：

- `Content-Type: application/json`
- `authorization: <登录获取的token>`

请求 json 示例：

```
{
  "id": 1,
  "name": "VLAN 100",
  "vlan_id": 100,
  "description": "虚拟链路描述"
}
```

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "message": "Success"
}
```

> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

删除虚拟链路

接口类型	api	接口描述
DELETE	/api/vlan/list	删除虚拟链路

请求头：

- `Content-Type: application/json`
- `authorization: <登录获取的token>`

请求 json 示例：

```
{
  "link_id_list": [1, 2]
}
```

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "message": "Success"
}
```

> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

排序虚拟链路

接口类型	api	接口描述
PUT	/api/vlan/list	排序虚拟链路

请求头：

- `Content-Type: application/json`
- `authorization: <登录获取的token>`

请求 json 示例：

```
{
  "link_id_list": [3, 1, 2]
}
```

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "message": "Success"
}
```

> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

事件

获取事件列表

接口类型	api	接口描述
GET	/api/incident	获取分析仪当前的触发事件列表

请求头：

- `authorization: <登录获取的token>`

请求参数：

参数名	类型	必填	描述	示例值
count	int	否	表示获取多少项，默认值请参考API实现	20
start	int	否	从第几项开始获取（分页起始位置），默认 0	0
rule_id	int	否	按规则 id 过滤	1
level	int	否	按规则的严重等级过滤：1-低；2-中；3-高	2

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "message": "Success",
  "data": {
    "total": 100,
    "items": [
      {
        "id": 1,
        "rule_id": 1,
        "level": 2,
        "message": "事件描述",
        "timestamp": 1765156896,
        "details": {}
      }
    ]
  }
}
```

> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

获取事件规则

接口类型	api	接口描述
GET	/api/incident/rule	获取所有事件规则

请求头：

- `authorization: <登录获取的token>`

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "data": [
    {
      "id": 1,
      "name": "规则名称",
      "level": 2,
      "expr": "过滤表达式",
      "enabled": true
    }
  ],
  "message": "Success"
}
```

> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

创建事件规则

接口类型	api	接口描述
POST	/api/incident/rule	创建事件规则

请求头：

- `Content-Type: application/json`
- `authorization: <登录获取的token>`

请求参数说明：

参数名	类型	必填	说明	示例值
name	string	是	规则名称	"高流量告警"
level	int	是	严重等级：1-低；2-中；3-高	2
expr	string	是	过滤表达式	"bytes > 1000000"
enabled	boolean	否	是否启用	true

请求 json 示例：

```
{
  "name": "高流量告警",
  "level": 2,
  "expr": "bytes > 1000000",
  "enabled": true
}
```

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "message": "Success"
}
```

> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

更新事件规则

接口类型	api	接口描述
PUT	/api/incident/rule	更新事件规则

请求头：

- `Content-Type: application/json`
- `authorization: <登录获取的token>`

请求 json 示例：

```
{
  "id": 1,
  "name": "高流量告警",
  "level": 2,
  "expr": "bytes > 1000000",
  "enabled": true
}
```

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "message": "Success"
}
```

> 提示：
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

删除事件规则

接口类型	api	接口描述
DELETE	/api/incident/rule	删除事件规则

请求头：

- `authorization: <登录获取的token>`

请求参数：

参数名	类型	必填	说明	示例值
id	int	是	规则ID	1

请求示例：

```
DELETE /api/incident/rule?id=1
```

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "message": "Success"
}
```

> 提示：
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

删除事件

接口类型	api	接口描述
DELETE	/api/incident	删除事件

请求头：

- `authorization: <登录获取的token>`

请求参数：

参数名	类型	必填	说明	示例值
id	int	否	事件ID，不提供则删除所有事件	1

请求示例：

```
DELETE /api/incident?id=1
```

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "message": "Success"
}
```

> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

IP 组

获取 IP 组

接口类型	api	接口描述
GET	/api/ip_group	获取 ip 组配置

请求头：

- `authorization: <登录获取的token>`

成功响应 json 示例（200 OK）：


```
{
    "code": 0,
    "data": [
        {
            "desc": "",
            "id": 1,
            "members": [
                {
                    "ip": "192.168.1.1/16",
                    "remark": ""
                }
            ],
            "name": "test"
        },
        {
            "desc": "",
            "id": 2,
            "members": [
                {
                    "ip": "192.168.1.139",
                    "remark": ""
                }
            ],
            "name": "test2"
        }
    ],
    "message": "Success"
}
```


响应字段说明：

字段名	类型	说明	示例值
code	int	状态码，0 表示成功	0
message	string	响应信息	"Success"
data	array	IP 组列表	见下方说明
data[].id	int	IP 组 ID	1
data[].name	string	IP 组名称	"test"
data[].desc	string	IP 组描述，可能为空字符串	"" 或 "服务器IP组"
data[].members	array	IP 组成员列表	见下方说明
data[].members[].ip	string	IP 地址，支持单个 IP 或 CIDR 格式	"192.168.1.139" 或 "192.168.1.1/16"
data[].members[].remark	string	成员备注，可能为空字符串	"" 或 "Web服务器"

> **重要提示：**
>
> 1. **空值处理**：`desc` 和 `remark` 字段可能为空字符串 `""`，表示该字段未设置。
> 2. **成员数组**：一个 IP 组可以包含多个成员，每个成员可以是单个 IP 或 IP 段。

> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

添加 IP 组

接口类型	api	接口描述
POST	/api/ip_group	添加 ip 组

请求头：

- `Content-Type: application/json`
- `authorization: <登录获取的token>`

请求参数说明：

参数名	类型	必填	说明	示例值
name	string	是	IP组名称	"服务器组"
members	array	是	IP组成员列表	见下方示例
desc	string	否	IP组描述	"服务器IP组"

members 数组中每个成员对象参数说明：

参数名	类型	必填	说明	示例值
ip	string	是	IP地址	"192.168.1.100"
remark	string	否	备注	"Web服务器"

请求 json 示例：

```
{
  "name": "服务器组",
  "members": [
    {
      "ip": "192.168.1.100",
      "remark": "Web服务器"
    },
    {
      "ip": "192.168.1.101",
      "remark": "数据库服务器"
    }
  ],
  "desc": "服务器IP组"
}
```

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "message": "Success",
  "data": {
    "id": 1
  }
}
```

> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

删除 IP 组

接口类型	api	接口描述
DELETE	/api/ip_group	删除 ip 组

- **请求 json 示例：**

```
{
  "ids": [
    0
  ]
}
```

修改 IP 组

接口类型	api	接口描述
PUT	/api/ip_group	修改 ip 组

请求头：

- `Content-Type: application/json`
- `authorization: <登录获取的token>`

```
{
  "id": 0,
  "name": "string",
  "members": [
    {
      "ip": "string",
      "remark": "string"
    }
  ],
  "desc": "string"
}
```

上传 IP 组配置 csv

接口类型	api	接口描述
POST	/api/ip_group_upload	上传 IP 组配置 csv 文件

> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

导出 IP 组配置 csv

接口类型	api	接口描述
GET	/api/ip_group_download	导出 IP 组配置 csv 文件

> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

重启设备

接口类型	api	接口描述
POST	/api/reboot	重启设备。无需提交任何数据。

请求头：

- `authorization: <登录获取的token>`

请求体： 无（空请求体或 `{}`）

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "message": "Success"
}
```

> 警告：
>
> 1. 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。
> 2. 此操作将立即重启设备，请谨慎使用。
> 3. 重启后设备需要一段时间才能恢复服务，请确保有足够的等待时间。

恢复出厂设置

接口类型	api	接口描述
POST	/api/reset	恢复出厂设置。无需提交任何数据。

请求头：

- `authorization: <登录获取的token>`

请求体： 无（空请求体或 `{}`）

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "message": "Success"
}
```

> 警告：
>
> 1. 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。
> 2. **此操作将清除所有配置数据并恢复出厂设置，请谨慎使用！**
> 3. 恢复出厂设置后，设备将重启并恢复到初始状态。
> 4. 所有自定义配置（包括IP组、虚拟链路等）将被清除。

管理口网络设置

获取管理口网络设置

接口类型	api	接口描述
GET	/api/system/control_port	获取设备管理口网络设置信息

请求头：

- `authorization: <登录获取的token>`

成功响应 json 示例（200 OK）：

```
{
    "code": 0,
    "data": [
        {
            "broadcast": "192.168.1.255",
            "default": true,
            "dhcp": false,
            "dns": [
                "8.8.8.8"
            ],
            "eth": "enp3s0",
            "gateway": "192.168.1.1",
            "inet": "192.168.1.234",
            "mac": "74:27:ea:d0:b7:72",
            "netmask": "255.255.255.0"
        }
    ],
    "message": "获取成功"
}
```

> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

修改管理口网络设置

接口类型	api	接口描述
POST	/api/system/control_port	修改设备管理口网络设置信息

请求头：

- `Content-Type: application/json`
- `authorization: <登录获取的token>`

请求参数说明：

参数名	类型	必填	说明	示例值
dhcp	boolean	是	是否启用DHCP	false
gateway	string	否	网关地址	"192.168.1.1"
inet	string	否	IPv4地址	"192.168.1.208"
netmask	string	否	子网掩码	"255.255.255.0"
broadcast	string	否	广播地址	"192.168.1.255"
inet6	string	否	IPv6地址	"fe80::2ab1:33ff:fe03:7b8c"

请求 json 示例：

```
[
    {
        "eth": "enp3s0",
        "dhcp": false,
        "inet": "192.168.1.234",
        "netmask": "255.255.255.0",
        "gateway": "192.168.1.1",
        "dns": [
            "8.8.8.8"
        ]
    }
]
```

成功响应 json 示例（200 OK）：

```
{
    "code": 0,
    "message": "设置成功"
}
```

> **提示：**
> 1.需要将登录成功获得的 token 作为 header 中 authorization 参数的值。
> 2.该接口调用成功后，设备不会自动重启。新的管理口网络设置需要重启设备才生效。

用户管理

修改密码

接口类型	api	接口描述
POST	/api/user/change_password	修改用户密码

请求头：

- `Content-Type: application/json`
- `authorization: <登录获取的token>`

请求参数说明：

参数名	类型	必填	说明	示例值
username	string	是	用户名	"admin"
old_password	string	是	旧密码	"old_password"
new_password	string	是	新密码	"new_password"

请求 json 示例：

```
{
  "username": "admin",
  "old_password": "old_password",
  "new_password": "new_password"
}
```

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "message": "Success"
}
```

> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

邮件配置

获取邮件配置

接口类型	api	接口描述
GET	/api/system/email	获取邮件配置列表

请求头：

- `authorization: <登录获取的token>`

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "data": [
    {
      "id": 1,
      "recipient": "admin@example.com"
    }
  ],
  "message": "Success"
}
```

> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

添加邮件配置

接口类型	api	接口描述
POST	/api/system/email	添加邮件配置

请求头：

- `Content-Type: application/json`
- `authorization: <登录获取的token>`

请求参数说明：

参数名	类型	必填	说明	示例值
recipient	string	是	收件人邮箱地址	"admin@example.com"

请求 json 示例：

```
{
  "recipient": "admin@example.com"
}
```

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "message": "Success"
}
```

> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

删除邮件配置

接口类型	api	接口描述
DELETE	/api/system/email	删除邮件配置

请求头：

- `Content-Type: application/json`
- `authorization: <登录获取的token>`

请求 json 示例：

```
{
  "id": 1
}
```

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "message": "Success"
}
```

> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

测试邮件配置

接口类型	api	接口描述
POST	/api/system/email/test	测试邮件配置

请求头：

- `Content-Type: application/json`
- `authorization: <登录获取的token>`

请求 json 示例：

```
{
  "id": 1
}
```

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "message": "Success"
}
```

> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

自定义协议

获取自定义协议

接口类型	api	接口描述
GET	/api/custom	获取自定义协议列表

请求头：

- `authorization: <登录获取的token>`

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "data": [
    {
      "id": 1,
      "name": "协议名称",
      "port": 8080,
      "protocol": "TCP"
    }
  ],
  "message": "Success"
}
```

> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

添加自定义协议

接口类型	api	接口描述
POST	/api/custom	添加自定义协议

请求头：

- `Content-Type: application/json`
- `authorization: <登录获取的token>`

请求 json 示例：

```
{
  "name": "协议名称",
  "port": 8080,
  "protocol": "TCP"
}
```

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "message": "Success"
}
```

> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

修改自定义协议

接口类型	api	接口描述
PUT	/api/custom	修改自定义协议

请求头：

- `Content-Type: application/json`
- `authorization: <登录获取的token>`

请求 json 示例：

```
{
  "id": 1,
  "name": "更新后的协议名称",
  "port": 8080,
  "protocol": "TCP"
}
```

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "message": "Success"
}
```

> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

删除自定义协议

接口类型	api	接口描述
DELETE	/api/custom	删除自定义协议

请求头：

- `Content-Type: application/json`
- `authorization: <登录获取的token>`

请求 json 示例：

```
{
  "ids": [1, 2, 3]
}
```

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "message": "Success"
}
```

> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

自定义协议排序

接口类型	api	接口描述
POST	/api/custom_order	设置自定义协议排序

请求头：

- `Content-Type: application/json`
- `authorization: <登录获取的token>`

请求 json 示例：

```
{
  "order_list": [3, 1, 2]
}
```

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "message": "Success"
}
```

> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

系统信息与配置

获取系统信息

接口类型	api	接口描述
GET	/api/get_system_info	获取系统信息

请求头：

- `authorization: <登录获取的token>`

请求参数：

参数名	类型	必填	说明	示例值
link_id	int	否	虚拟链路ID	0

请求示例：

```
GET /api/get_system_info?link_id=0
```

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "data": {
    "version": "1.0.0",
    "uptime": 3600
  },
  "message": "Success"
}
```

> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

IP 白名单

获取 IP 白名单

接口类型	api	接口描述
GET	/api/system/network/ip_white_list	获取 IP 白名单列表

请求头：

- `authorization: <登录获取的token>`

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "data": [
    "192.168.1.100",
    "192.168.1.101"
  ],
  "message": "Success"
}
```

> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

设置 IP 白名单

接口类型	api	接口描述
POST	/api/system/network/ip_white_list	设置 IP 白名单

请求头：

- `Content-Type: application/json`
- `authorization: <登录获取的token>`

请求 json 示例：

```
[
  "192.168.1.100",
  "192.168.1.101"
]
```

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "message": "Success"
}
```

> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

系统时间

NTP 配置

接口类型	api	接口描述
POST	/api/system/time	配置 NTP 或关闭 NTP

请求头：

- `Content-Type: application/json`
- `authorization: <登录获取的token>`

启用 NTP 请求 json 示例：

```
{
  "ntp": true,
  "update_interval": 3600,
  "pool_server_name": "pool.ntp.org"
}
```

关闭 NTP 请求 json 示例：

```
{
  "ntp": false
}
```

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "message": "Success"
}
```

请求参数说明：

参数名	类型	必填	说明	示例值
ntp	boolean	是	是否启用 NTP	true
update_interval	int	否	更新间隔（秒），启用 NTP 时必填	3600
pool_server_name	string	否	NTP 服务器地址，启用 NTP 时必填	"pool.ntp.org"

> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

系统配置管理

重置系统配置

接口类型	api	接口描述
POST	/api/config/reset_sys_config	重置万用表系统配置

请求头：

- `authorization: <登录获取的token>`

请求体： 无（空请求体或 `{}`）

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "message": "Success"
}
```

> **警告：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。此操作将重置系统配置，请谨慎使用。

保存系统配置

接口类型	api	接口描述
POST	/api/config/save_cur_sys_config	保存当前系统配置到万用表

请求头：

- `authorization: <登录获取的token>`

请求体： 无（空请求体或 `{}`）

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "message": "Success"
}
```

> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

导出系统配置

接口类型	api	接口描述
GET	/api/config/export_sys_config	导出万用表系统配置

请求头：

- `authorization: <登录获取的token>`

响应：

- 成功：返回配置文件（zip 格式）
- 失败：返回 JSON 错误信息

> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

导入系统配置

接口类型	api	接口描述
POST	/api/config/import_sys_config	导入万用表系统配置

请求头：

- `Content-Type: application/octet-stream`
- `authorization: <登录获取的token>`

请求体： 配置文件（zip 格式）的二进制数据

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "message": "Success"
}
```

> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

日志管理

获取日志列表

接口类型	api	接口描述
GET	/api/log/list	获取设备日志文件列表

请求头：

- `authorization: <登录获取的token>`

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "data": [
    {
      "name": "system.log",
      "size": 1024000,
      "modified_time": 1765162850
    }
  ],
  "message": "Success"
}
```


> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

下载日志

接口类型	api	接口描述
GET	/api/log/download	下载日志文件

请求头：

- `authorization: <登录获取的token>`

请求参数：

参数名	类型	必填	说明	示例值
filename	string	否	日志文件名，不提供则下载所有日志	"system.log"

请求示例：

```
GET /api/log/download?filename=system.log
```

响应：

- 成功：返回日志文件内容或下载路径
- 失败：返回 JSON 错误信息

> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

日志配置

获取日志配置

接口类型	api	接口描述
GET	/api/log/config	获取 Logger 配置列表

请求头：

- `authorization: <登录获取的token>`

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "data": [
    {
      "logger_name": "syslog",
      "log_type": "syslog",
      "server_host": "192.168.1.100",
      "port": 514,
      "log_level": "info"
    }
  ],
  "message": "Success"
}
```

> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

添加日志配置

接口类型	api	接口描述
POST	/api/log/logger	添加 Logger 配置

请求头：

- `Content-Type: application/json`
- `authorization: <登录获取的token>`

请求参数说明：

参数名	类型	必填	说明	示例值
logger_name	string	是	Logger 名称	"syslog"
log_type	string	是	日志类型	"syslog"
server_host	string	是	服务器地址	"192.168.1.100"
port	int	是	端口号	514
log_level	string	否	日志级别	"info"
facility	int	否	设施代码	16
log_host_name	string	否	主机名	"device"
app_name	string	否	应用名称	"anatraf"
fm_style	string	否	格式样式	"rfc5424"

请求 json 示例：

```
{
  "logger_name": "syslog",
  "log_type": "syslog",
  "server_host": "192.168.1.100",
  "port": 514,
  "log_level": "info"
}
```

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "message": "Success"
}
```

> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

删除日志配置

接口类型	api	接口描述
DELETE	/api/log/logger	删除 Logger 配置

请求头：

- `Content-Type: application/json`
- `authorization: <登录获取的token>`

请求 json 示例：

```
{
  "logger_name": "syslog"
}
```

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "message": "Success"
}
```

> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

用户日志

获取用户日志列表

接口类型	api	接口描述
GET	/api/log/user/list	获取用户日志文件列表

请求头：

- `authorization: <登录获取的token>`

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "data": [
    {
      "name": "user.log",
      "size": 512000,
      "modified_time": 1765162850
    }
  ],
  "message": "Success"
}
```

> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

下载用户日志

接口类型	api	接口描述
GET	/api/log/user/download	下载用户日志文件

请求头：

- `authorization: <登录获取的token>`

请求参数：

参数名	类型	必填	说明	示例值
filename	string	否	日志文件名，不提供则下载所有用户日志	"user.log"

请求示例：

```
GET /api/log/user/download?filename=user.log
```

响应：

- 成功：返回日志文件内容或下载路径
- 失败：返回 JSON 错误信息

> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

获取用户日志内容

接口类型	api	接口描述
GET	/api/log/user/lines	获取用户日志最后50行内容

请求头：

- `authorization: <登录获取的token>`

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "data": [
    "2024-01-01 10:00:00 [INFO] User logged in",
    "2024-01-01 10:01:00 [INFO] User performed action"
  ],
  "total": 50,
  "message": "Success"
}
```

> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

用户日志配置

接口类型	api	接口描述
GET	/api/log/user/config	获取用户日志配置
PUT	/api/log/user/config	更新用户日志配置

请求头：

- `authorization: <登录获取的token>`（GET）
- `Content-Type: application/json`、`authorization: <登录获取的token>`（PUT）

获取配置成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "data": {
    "level": "info",
    "max_size": 10485760,
    "max_files": 10
  },
  "message": "Success"
}
```

更新配置请求 json 示例：

```
{
  "level": "debug",
  "max_size": 20971520,
  "max_files": 20
}
```

更新配置成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "message": "Success"
}
```

> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

存储管理

获取存储列表

接口类型	api	接口描述
GET	/api/storage/list	获取存储列表

请求头：

- `authorization: <登录获取的token>`

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "data": [
    {
      "id": 1,
      "name": "capture_001",
      "size": 1048576000,
      "start_time": 1765162790,
      "end_time": 1765162850
    }
  ],
  "message": "Success"
}
```

> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

删除存储

接口类型	api	接口描述
DELETE	/api/storage	删除存储

请求头：

- `Content-Type: application/json`
- `authorization: <登录获取的token>`

请求 json 示例：

```
{
  "capture_id_list": [1, 2, 3]
}
```

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "message": "Success"
}
```

> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

获取存储图表数据

接口类型	api	接口描述
POST	/api/storage/capture_graph	获取存储捕获的图表数据

请求头：

- `Content-Type: application/json`
- `authorization: <登录获取的token>`

请求参数说明：

参数名	类型	必填	说明	示例值
capture_id	array[int]	是	捕获ID列表	[1, 2]
range	object	否	时间范围	见下方示例
range.start_time	int	否	开始时间（秒级时间戳）	1765162790
range.end_time	int	否	结束时间（秒级时间戳）	1765162850

请求 json 示例：

```
{
  "capture_id": [1, 2],
  "range": {
    "start_time": 1765162790,
    "end_time": 1765162850
  }
}
```

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "data": {
    "len": 61,
    "bytes": [1000, 2000, 1500, null],
    "time": [1765162790, 1765162791, 1765162792],
    "granularity": 1
  },
  "message": "Success"
}
```


> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

VLAN 别名

获取 VLAN 别名

接口类型	api	接口描述
GET	/api/vlan_alias	获取 VLAN 别名列表

请求头：

- `authorization: <登录获取的token>`

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "data": [
    {
      "id": 100,
      "alias": "管理VLAN"
    }
  ],
  "message": "Success"
}
```

> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

添加 VLAN 别名

接口类型	api	接口描述
POST	/api/vlan_alias	添加 VLAN 别名

请求头：

- `Content-Type: application/json`
- `authorization: <登录获取的token>`

请求参数说明：

参数名	类型	必填	说明	示例值
id	int	是	VLAN ID	100
alias	string	是	别名	"管理VLAN"

请求 json 示例：

```
{
  "id": 100,
  "alias": "管理VLAN"
}
```

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "message": "Success"
}
```

> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

删除 VLAN 别名

接口类型	api	接口描述
DELETE	/api/vlan_alias	删除 VLAN 别名

请求头：

- `Content-Type: application/json`
- `authorization: <登录获取的token>`

请求 json 示例：

```
{
  "id": 100
}
```

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "message": "Success"
}
```

> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

导出 VLAN 别名 CSV

接口类型	api	接口描述
GET	/api/vlan_alias/download	导出 VLAN 别名配置 CSV 文件

请求头：

- `authorization: <登录获取的token>`

请求参数：

参数名	类型	必填	说明	示例值
token	string	是	登录获取的 token	"AV8rk4KXFY1hnh8P"

请求示例：

```
GET /api/vlan_alias/download?token=AV8rk4KXFY1hnh8P
```

响应：

- 成功：返回 CSV 文件内容
- 失败：返回 JSON 错误信息

> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

上传 VLAN 别名 CSV

接口类型	api	接口描述
POST	/api/vlan_alias/upload	上传 VLAN 别名配置 CSV 文件

请求头：

- `Content-Type: application/json`
- `authorization: <登录获取的token>`

请求体： CSV 文件的二进制数据

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "message": "Success"
}
```

> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

数据包回放

加载回放

接口类型	api	接口描述
POST	/api/replay/load	加载指定时间范围和过滤条件的数据包进行回放

请求头：

- `authorization: <登录获取的token>`

请求参数：

参数名	类型	必填	说明	示例值
from	int	是	开始时间戳（秒级，10 位数）	1765162790
to	int	是	结束时间戳（秒级，10 位数）	1765162850
filter	string	是	过滤表达式	"ip_address==192.168.1.1"

请求示例：

```
POST /api/replay/load?from=1765162790&to=1765162850&filter=ip_address==192.168.1.1
```

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "message": "Success"
}
```

> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

停止回放

接口类型	api	接口描述
POST	/api/replay/stop	停止数据包回放

请求头：

- `authorization: <登录获取的token>`

请求体： 无（空请求体或 `{}`）

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "message": "Success"
}
```

> 提示：
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

获取回放链路

接口类型	api	接口描述
GET	/api/replay/link	获取可用的回放链路列表

请求头：

- `authorization: <登录获取的token>`

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "data": [
    {
      "link_id": 0,
      "name": "默认链路"
    }
  ],
  "message": "Success"
}
```

> 提示：
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

获取回放状态

接口类型	api	接口描述
GET	/api/replay/state	获取当前回放状态

请求头：

- `authorization: <登录获取的token>`

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "data": {
    "status": "running",
    "progress": 50
  },
  "message": "Success"
}
```

> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

上传回放文件

接口类型	api	接口描述
POST	/api/replay/upload	上传 PCAP 文件用于回放

请求头：

- `Content-Type: application/json`
- `authorization: <登录获取的token>`

请求参数：

参数名	类型	必填	说明	示例值
token	string	是	登录获取的 token	"AV8rk4KXFY1hnh8P"
pcap_file_size	int	是	PCAP 文件大小（字节）	1048576

请求体： PCAP 文件的二进制数据

请求示例：

```
POST /api/replay/upload?token=AV8rk4KXFY1hnh8P&pcap_file_size=1048576
```

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "message": "Success"
}
```

> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

入口过滤

获取入口过滤

接口类型	api	接口描述
GET	/api/ingress_filter	获取入口过滤表达式

请求头：

- `authorization: <登录获取的token>`

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "data": {
    "ingress_filter_expr": "ip_address==192.168.1.1"
  },
  "message": "Success"
}
```

> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

设置入口过滤

接口类型	api	接口描述
POST	/api/ingress_filter	设置入口过滤表达式

请求头：

- `Content-Type: application/json`
- `authorization: <登录获取的token>`

请求参数说明：

参数名	类型	必填	说明	示例值
ingress_filter_expr	string	是	入口过滤表达式	"ip_address==192.168.1.1"

请求 json 示例：

```
{
  "ingress_filter_expr": "ip_address==192.168.1.1"
}
```

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "message": "Success"
}
```

> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

截断规则

获取截断规则

接口类型	api	接口描述
GET	/api/cut_rule/list	获取截断规则列表

请求头：

- `authorization: <登录获取的token>`

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "data": [
    {
      "id": 1,
      "name": "规则名称",
      "expr": "过滤表达式"
    }
  ],
  "message": "Success"
}
```

> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

设置截断规则

接口类型	api	接口描述
POST	/api/cut_rule/list	设置截断规则列表

请求头：

- `Content-Type: application/json`

- `authorization: <登录获取的token>`

请求 json 示例：

```
[
  {
    "id": 1,
    "name": "规则名称",
    "expr": "过滤表达式"
  }
]
```

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "message": "Success"
}
```

> **提示：**
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

分析开关

获取分析开关

接口类型	api	接口描述
GET	/api/analysis_switch	获取分析开关列表

请求头：

- `authorization: <登录获取的token>`

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "data": {
    "analysis_switch_list": [
      {
        "id": "l2",
        "name": "L2分析",
        "enabled": true
      }
    ]
  },
  "message": "Success"
}
```

> 提示：
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

设置分析开关

接口类型	api	接口描述
POST	/api/analysis_switch	设置分析开关

请求头：

- `Content-Type: application/json`
- `authorization: <登录获取的token>`

请求参数说明：

参数名	类型	必填	说明	示例值
analysis_switch_id_list	array[string]	是	启用的分析开关ID列表	["l2", "l3"]

请求 json 示例：

```
{
  "analysis_switch_id_list": ["l2", "l3"]
}
```

成功响应 json 示例（200 OK）：

```
{
  "code": 0,
  "message": "Success"
}
```

> 提示：
> 需要将登录成功获得的 token 作为 header 中 authorization 参数的值。

附录: 各分析模块可用的查询字段

网口统计

id/field	is_series	name	title	type
l1.port.interface	false	interface	网口号	number
l1.port.pkts	true	pkts	总包数	pkts
l1.port.bytes	true	bytes	总字节数	bytes
l1.port.pps	true	pps	每秒包数	pps
l1.port.bps	true	bps	每秒流量	bps
l1.port.io_drop_pkts	true	io_drop_pkts	IO总丢包数	pkts
l1.port.io_drop_pps	true	io_drop_pps	IO每秒丢包数	pps
l1.port.error_pkts	true	error_pkts	总错包数	pkts
l1.port.error_pps	true	error_pps	每秒错包数	pps
l1.port.analysis_drop_bytes	true	analysis_drop_bytes	分析丢包总字节数	bytes
l1.port.analysis_drop_bps	true	analysis_drop_bps	分析每秒丢包流量	bps
l1.port.analysis_drop_pkts	true	analysis_drop_pkts	分析总丢包数	pkts
l1.port.analysis_drop_pps	true	analysis_drop_pps	分析每秒丢包数	pps
l1.port.storage_drop_bytes	true	storage_drop_bytes	存储丢包总字节数	bytes
l1.port.storage_drop_bps	true	storage_drop_bps	存储每秒丢包流量	bps
l1.port.storage_drop_pkts	true	storage_drop_pkts	存储总丢包数	pkts
l1.port.storage_drop_pps	true	storage_drop_pps	存储每秒丢包数	pps
l1.port.link_speed	false	link_speed	连接速率	bps
l1.port.port_speed	false	port_speed	网口速率	bps
l1.port.utilization_pct	true	utilization_pct	利用率	permyriad
l1.port.utilization_pct_ge_0_lt_10	true	utilization_pct_ge_0_lt_10	利用率 0% ~ 10%	permyriad
l1.port.utilization_pct_ge_10_lt_50	true	utilization_pct_ge_10_lt_50	利用率 10% ~ 50%	permyriad
l1.port.utilization_pct_ge_50_lt_90	true	utilization_pct_ge_50_lt_90	利用率 50% ~ 90%	permyriad
l1.port.utilization_pct_ge_90_lt_95	true	utilization_pct_ge_90_lt_95	利用率 90% ~ 95%	permyriad
l1.port.utilization_pct_ge_95_lt_99	true	utilization_pct_ge_95_lt_99	利用率 95% ~ 99%	permyriad
l1.port.utilization_pct_ge_99_lt_100	true	utilization_pct_ge_99_lt_100	利用率 99% ~ 100%	permyriad
l1.port.utilization_pct_ge_100	true	utilization_pct_ge_100	利用率 >= 100%	permyriad

L2 MAC

id/field	is_series	name	title	type
l2.mac.mac_address	false	mac_address	MAC地址	mac
l2.mac.nic_vendor	false	nic_vendor	网卡供应商	string
l2.mac.mac_dhcp_name	false	mac_dhcp_name	DHCP主机名	array
l2.mac.mac_os_name	false	mac_os_name	操作系统	array
l2.mac.first_activity_time	false	first_activity_time	首次活动时间	time
l2.mac.last_activity_time	false	last_activity_time	上次活动时间	time
l2.mac.tx_pkts	true	tx_pkts	总发包数	pkts
l2.mac.rx_pkts	true	rx_pkts	总收包数	pkts
l2.mac.pkts	true	pkts	总包数	pkts
l2.mac.tx_bytes	true	tx_bytes	总发送字节数	bytes
l2.mac.rx_bytes	true	rx_bytes	总接收字节数	bytes
l2.mac.bytes	true	bytes	总字节数	bytes
l2.mac.tx_pps	true	tx_pps	每秒发包数	pps
l2.mac.rx_pps	true	rx_pps	每秒收包数	pps
l2.mac.pps	true	pps	每秒包数	pps
l2.mac.tx_bps	true	tx_bps	每秒发送流量	bps
l2.mac.rx_bps	true	rx_bps	每秒接收流量	bps
l2.mac.bps	true	bps	每秒流量	bps
l2.mac.peer_mac_count	true	peer_mac_count	对等MAC数	number
l2.mac.peer_ip_count	true	peer_ip_count	活跃IP数	number
l2.mac.peer_flow_count	true	peer_flow_count	活跃连接数	number
l2.mac.l7_protocol	false	l7_protocol	应用层协议	array

L2 MAC Pairs

id/field	is_series	name	title	type
l2.mac_pairs.mac_address	false	mac_address	MAC地址	mac
l2.mac_pairs.mac_peer_address	false	mac_peer_address	对等MAC	mac
l2.mac_pairs.nic_vendor	false	nic_vendor	网卡供应商	string
l2.mac_pairs.mac_dhcp_name	false	mac_dhcp_name	DHCP主机名	array
l2.mac_pairs.mac_os_name	false	mac_os_name	操作系统	array
l2.mac_pairs.peer_nic_vendor	false	peer_nic_vendor	对等网卡供应商	string
l2.mac_pairs.peer_dhcp_name	false	peer_dhcp_name	对等DHCP主机名	array
l2.mac_pairs.peer_os_name	false	peer_os_name	对等操作系统	array
l2.mac_pairs.first_activity_time	false	first_activity_time	首次活动时间	time
l2.mac_pairs.last_activity_time	false	last_activity_time	上次活动时间	time
l2.mac_pairs.tx_pkts	true	tx_pkts	MAC地址到对等MAC总包数	pkts
l2.mac_pairs.rx_pkts	true	rx_pkts	对等MAC到MAC地址总包数	pkts
l2.mac_pairs.pkts	true	pkts	总包数	pkts
l2.mac_pairs.tx_bytes	true	tx_bytes	MAC地址到对等MAC总字节数	bytes
l2.mac_pairs.rx_bytes	true	rx_bytes	对等MAC到MAC地址总字节数	bytes
l2.mac_pairs.bytes	true	bytes	总字节数	bytes
l2.mac_pairs.tx_pps	true	tx_pps	MAC地址到对等MAC每秒包数	pps
l2.mac_pairs.rx_pps	true	rx_pps	对等MAC到MAC地址每秒包数	pps
l2.mac_pairs.pps	true	pps	每秒包数	pps
l2.mac_pairs.tx_bps	true	tx_bps	MAC地址到对等MAC每秒流量	bps
l2.mac_pairs.rx_bps	true	rx_bps	对等MAC到MAC地址每秒流量	bps
l2.mac_pairs.bps	true	bps	每秒流量	bps

L2 ARP

L2 ARP Overview

id/field	is_series	name	title	type
l2.arp.overview.request_count	true	request_count	ARP请求总数	number
l2.arp.overview.response_count	true	response_count	ARP响应总数	number
l2.arp.overview.request_per_sec_count	true	request_per_sec_count	ARP每秒请求数	number
l2.arp.overview.response_per_sec_count	true	response_per_sec_count	ARP每秒响应数	number

L2 ARP-MAC

id/field	is_series	name	title	type
l2.arp.mac.mac_address	false	mac_address	MAC地址	mac
l2.arp.mac.mac_dhcp_name	false	mac_dhcp_name	MAC的DHCP主机名	array
l2.arp.mac.mac_os_name	false	mac_os_name	MAC的操作系统	array
l2.arp.mac.nic_vendor	false	nic_vendor	网卡供应商	string
l2.arp.mac.request_count	true	request_count	ARP请求数量	number
l2.arp.mac.response_count	true	response_count	ARP回复数量	number
l2.arp.mac.ip_address	false	ip_address	最近宣告IP	ip
l2.arp.mac.ip_dhcp_name	false	ip_dhcp_name	IP的DHCP主机名	array
l2.arp.mac.ip_os_name	false	ip_os_name	IP的操作系统名	array
l2.arp.mac.different_ips	false	different_ips	使用过的IP	array

L2 ARP-IP

id/field	is_series	name	title	type
l2.arp.ip.ip_address	false	ip_address	IP地址	ip
l2.arp.ip.ip_dhcp_name	false	ip_dhcp_name	IP的DHCP主机名	array
l2.arp.ip.ip_os_name	false	ip_os_name	IP的操作系统名	array
l2.arp.ip.request_count	true	request_count	ARP请求数量	number
l2.arp.ip.response_count	true	response_count	ARP回复数量	number
l2.arp.ip.mac_address	false	mac_address	最近使用的MAC	mac
l2.arp.ip.mac_dhcp_name	false	mac_dhcp_name	MAC的DHCP主机名	array
l2.arp.ip.mac_os_name	false	mac_os_name	MAC的操作系统	array
l2.arp.ip.nic_vendor	false	nic_vendor	网卡供应商	string
l2.arp.ip.different_macs	false	different_macs	使用过的MAC	array
l2.arp.ip.peer_mac_count	false	peer_mac_count	使用过的MAC数量	number

L2 VLAN

L2 VLAN Outer

id/field	is_series	name	title	type
l2.vlan.outer.vlan_id	false	vlan_id	VLAN id	number
l2.vlan.outer.alias	false	alias	备注	string
l2.vlan.outer.pkts	true	pkts	数据包数	pkts
l2.vlan.outer.bytes	true	bytes	总字节数	bytes
l2.vlan.outer.pps	true	pps	每秒数据包数	pps
l2.vlan.outer.bps	true	bps	每秒流量	bps

L2 VLAN-MAC

id/field	is_series	name	title	type
l2.vlan.mac.vlan_id	false	vlan_id	VLAN id	number
l2.vlan.mac.mac_address	false	mac_address	MAC地址	mac
l2.vlan.mac.mac_dhcp_name	false	mac_dhcp_name	MAC的DHCP主机名	array
l2.vlan.mac.mac_os_name	false	mac_os_name	MAC的操作系统	array
l2.vlan.mac.nic_vendor	false	nic_vendor	网卡供应商	string
l2.vlan.mac.tx_pkts	true	tx_pkts	上行总包数	pkts
l2.vlan.mac.rx_pkts	true	rx_pkts	下行总包数	pkts
l2.vlan.mac.pkts	true	pkts	总包数	pkts
l2.vlan.mac.tx_bytes	true	tx_bytes	上行总字节数	bytes
l2.vlan.mac.rx_bytes	true	rx_bytes	下行总字节数	bytes
l2.vlan.mac.bytes	true	bytes	总字节数	bytes
l2.vlan.mac.tx_pps	true	tx_pps	上行每秒包数	pps
l2.vlan.mac.rx_pps	true	rx_pps	下行每秒包数	pps
l2.vlan.mac.pps	true	pps	每秒包数	pps
l2.vlan.mac.tx_bps	true	tx_bps	上行每秒流量	bps
l2.vlan.mac.rx_bps	true	rx_bps	下行每秒流量	bps
l2.vlan.mac.bps	true	bps	每秒流量	bps

L2 QoS

id/field	is_series	name	title	type
l2.qos.vlan_qos	false	vlan_qos	VLAN QoS	string
l2.qos.pkts	true	pkts	总包数	pkts
l2.qos.bytes	true	bytes	总字节数	bytes
l2.qos.pps	true	pps	每秒包数	pps
l2.qos.bps	true	bps	每秒流量	bps

L2 数据包大小统计

L2 全局数据包大小统计

id/field	is_series	name	title	type
l2.packet_size.global_avg_size.avg	true	avg	平均数据包大小	number
l2.packet_size.global_avg_size.min	true	min	最小数据包大小	number
l2.packet_size.global_avg_size.max	true	max	最大数据包大小	number
l2.packet_size.global.bytes	true	bytes	数据包大小	string
l2.packet_size.global.pkts	true	pkts	数据包数量	pkts
l2.packet_size.global.pps	true	pps	每秒数据包数量	pps

L2 TCP 数据包大小统计

id/field	is_series	name	title	type
l2.packet_size.tcp_avg_size.avg	true	avg	平均数据包大小	number
l2.packet_size.tcp_avg_size.min	true	min	最小数据包大小	number
l2.packet_size.tcp_avg_size.max	true	max	最大数据包大小	number
l2.packet_size.tcp.bytes	true	bytes	数据包大小	string
l2.packet_size.tcp.pkts	true	pkts	数据包数量	pkts
l2.packet_size.tcp.pps	true	pps	每秒数据包数量	pps

L2 UDP 数据包大小统计

id/field	is_series	name	title	type
l2.packet_size.udp_avg_size.avg	true	avg	平均数据包大小	number
l2.packet_size.udp_avg_size.min	true	min	最小数据包大小	number
l2.packet_size.udp_avg_size.max	true	max	最大数据包大小	number
l2.packet_size.udp.bytes	true	bytes	数据包大小	string
l2.packet_size.udp.pkts	true	pkts	数据包数量	pkts
l2.packet_size.udp.pps	true	pps	每秒数据包数量	pps

L3 IP

id/field	is_series	name	title	type
l3.ip_address.ip_address	false	ip_address	IP地址	ip
l3.ip_address.ip_dhcp_name	false	ip_dhcp_name	DHCP主机名	array
l3.ip_address.dns_name	false	dns_name	DNS域名	array
l3.ip_address.http_name	false	http_name	HTTP主机名	array
l3.ip_address.tls_name	false	tls_name	TLS主机名	array
l3.ip_address.ip_os_name	false	ip_os_name	操作系统	array
l3.ip_address.ip_group_name	false	ip_group_name	组名	array
l3.ip_address.ip_remark_name	false	ip_remark_name	备注名	array
l3.ip_address.region	false	region	国家/地区	string
l3.ip_address.mac_address	false	mac_address	最近的MAC	mac
l3.ip_address.nic_vendor	false	nic_vendor	网卡供应商	string
l3.ip_address.mac_dhcp_name	false	mac_dhcp_name	最近MAC的DHCP主机名	array
l3.ip_address.mac_os_name	false	mac_os_name	最近MAC的操作系统	array
l3.ip_address.first_activity_time	false	first_activity_time	首次活动时间	time
l3.ip_address.last_activity_time	false	last_activity_time	上次活动时间	time
l3.ip_address.tx_pkts	true	tx_pkts	总发包数	pkts
l3.ip_address.rx_pkts	true	rx_pkts	总收包数	pkts
l3.ip_address.pkts	true	pkts	总包数	pkts
l3.ip_address.tx_bytes	true	tx_bytes	总发送字节数	bytes
l3.ip_address.rx_bytes	true	rx_bytes	总接收字节数	bytes
l3.ip_address.bytes	true	bytes	总字节数	bytes
l3.ip_address.tx_pps	true	tx_pps	每秒发包数	pps
l3.ip_address.rx_pps	true	rx_pps	每秒收包数	pps
l3.ip_address.pps	true	pps	每秒包数	pps
l3.ip_address.tx_bps	true	tx_bps	每秒发送流量	bps
l3.ip_address.rx_bps	true	rx_bps	每秒接收流量	bps
l3.ip_address.bps	true	bps	每秒流量	bps
l3.ip_address.peer_ip_count	true	peer_ip_count	对等IP数	number
l3.ip_address.tx_handshake_count	true	tx_handshake_count	客户端握手次数	number
l3.ip_address.rx_handshake_count	true	rx_handshake_count	服务器握手次数	number
l3.ip_address.handshake_count	true	handshake_count	握手次数	number
l3.ip_address.tx_avg_handshake_time	true	tx_avg_handshake_time	客户端握手平均时延	ns
l3.ip_address.rx_avg_handshake_time	true	rx_avg_handshake_time	服务器握手平均时延	ns
l3.ip_address.avg_handshake_time	true	avg_handshake_time	握手平均时延	ns
l3.ip_address.tx_max_handshake_time	true	tx_max_handshake_time	客户端握手最大时延	ns
l3.ip_address.rx_max_handshake_time	true	rx_max_handshake_time	服务器握手最大时延	ns
l3.ip_address.max_handshake_time	true	max_handshake_time	握手最大时延	ns
l3.ip_address.tx_min_handshake_time	true	tx_min_handshake_time	客户端握手最小时延	ns
l3.ip_address.rx_min_handshake_time	true	rx_min_handshake_time	服务器握手最小时延	ns

l3.ip_address.min_handshake_time	true	min_handshake_time	握手最小时延	ns
l3.ip_address.response_count	true	response_count	响应次数	number
l3.ip_address.avg_response_time	true	avg_response_time	平均响应时延	ns
l3.ip_address.max_response_time	true	max_response_time	最大响应时延	ns
l3.ip_address.min_response_time	true	min_response_time	最小响应时延	ns
l3.ip_address.interface	false	interface	网口	array

L3 IP Group

id/field	is_series	name	title	type
l3.ip_groups.ip_group_name	false	ip_group_name	IP组	string
l3.ip_groups.ip_group_members	false	ip_group_members	IP组成员	array
l3.ip_groups.ip_group_desc	false	ip_group_desc	IP组描述	string
l3.ip_groups.first_activity_time	false	first_activity_time	首次活动时间	time
l3.ip_groups.last_activity_time	false	last_activity_time	上次活动时间	time
l3.ip_groups.tx_pkts	true	tx_pkts	总发包数	pkts
l3.ip_groups.rx_pkts	true	rx_pkts	总收包数	pkts
l3.ip_groups.pkts	true	pkts	总包数	pkts
l3.ip_groups.tx_bytes	true	tx_bytes	总发送字节数	bytes
l3.ip_groups.rx_bytes	true	rx_bytes	总接收字节数	bytes
l3.ip_groups.bytes	true	bytes	总字节数	bytes
l3.ip_groups.tx_pps	true	tx_pps	每秒发包数	pps
l3.ip_groups.rx_pps	true	rx_pps	每秒收包数	pps
l3.ip_groups.pps	true	pps	每秒包数	pps
l3.ip_groups.tx_bps	true	tx_bps	每秒发送流量	bps
l3.ip_groups.rx_bps	true	rx_bps	每秒接收流量	bps
l3.ip_groups.bps	true	bps	每秒流量	bps
l3.ip_groups.tx_mtu	true	tx_mtu	上行MTU	bytes
l3.ip_groups.rx_mtu	true	rx_mtu	下行MTU	bytes
l3.ip_groups.mtu	true	mtu	MTU	bytes
l3.ip_groups.tcp_count	true	tcp_count	TCP数据包数量	pkts
l3.ip_groups.udp_count	true	udp_count	UDP数据包数量	pkts
l3.ip_groups.tx_tcp_payload	true	tx_tcp_payload	发送TCP载荷	bytes
l3.ip_groups.rx_tcp_payload	true	rx_tcp_payload	接收TCP载荷	bytes
l3.ip_groups.tcp_payload	true	tcp_payload	TCP载荷	bytes
l3.ip_groups.tx_retransmit_bytes	true	tx_retransmit_bytes	发送TCP重传流量	bytes
l3.ip_groups.rx_retransmit_bytes	true	rx_retransmit_bytes	接收TCP重传流量	bytes
l3.ip_groups.retransmit_bytes	true	retransmit_bytes	TCP重传流量	bytes
l3.ip_groups.tx_retransmit_rate	true	tx_retransmit_rate	发送TCP重传率	permyriad
l3.ip_groups.rx_retransmit_rate	true	rx_retransmit_rate	接收TCP重传率	permyriad
l3.ip_groups.retransmit_rate	true	retransmit_rate	TCP重传率	permyriad
l3.ip_groups.tx_syn_count	true	tx_syn_count	发送SYN包数量	pkts
l3.ip_groups.rx_syn_count	true	rx_syn_count	接收SYN包数量	pkts
l3.ip_groups.syn_count	true	syn_count	SYN包数量	pkts
l3.ip_groups.tx_syn_ack_count	true	tx_syn_ack_count	发送SYN-ACK包数量	pkts
l3.ip_groups.rx_syn_ack_count	true	rx_syn_ack_count	接收SYN-ACK包数量	pkts
l3.ip_groups.syn_ack_count	true	syn_ack_count	SYN-ACK包数量	pkts
l3.ip_groups.tx_fin_count	true	tx_fin_count	发送FIN包数量	pkts
l3.ip_groups.rx_fin_count	true	rx_fin_count	接收FIN包数量	pkts

l3.ip_groups.fin_count	true	fin_count	FIN包数量	pkts
l3.ip_groups.tx_rst_count	true	tx_rst_count	发送RST包数量	pkts
l3.ip_groups.rx_rst_count	true	rx_rst_count	接收RST包数量	pkts
l3.ip_groups.rst_count	true	rst_count	RST包数量	pkts
l3.ip_groups.tx_dup_ack_count	true	tx_dup_ack_count	发送重复ACK包数量	pkts
l3.ip_groups.rx_dup_ack_count	true	rx_dup_ack_count	接收重复ACK包数量	pkts
l3.ip_groups.dup_ack_count	true	dup_ack_count	重复ACK包数量	pkts
l3.ip_groups.tx_zero_window_count	true	tx_zero_window_count	发送TCP零窗口包数量	pkts
l3.ip_groups.rx_zero_window_count	true	rx_zero_window_count	接收TCP零窗口包数量	pkts
l3.ip_groups.zero_window_count	true	zero_window_count	TCP零窗口包数量	pkts
l3.ip_groups.peer_flow_count	true	peer_flow_count	活跃连接数	number
l3.ip_groups.l7_protocol	false	l7_protocol	应用层协议	array
l3.ip_groups.tx_handshake_count	true	tx_handshake_count	客户端握手次数	number
l3.ip_groups.rx_handshake_count	true	rx_handshake_count	服务器握手次数	number
l3.ip_groups.handshake_count	true	handshake_count	握手次数	number
l3.ip_groups.tx_avg_handshake_time	true	tx_avg_handshake_time	客户端握手平均时延	ns
l3.ip_groups.rx_avg_handshake_time	true	rx_avg_handshake_time	服务器握手平均时延	ns
l3.ip_groups.avg_handshake_time	true	avg_handshake_time	握手平均时延	ns
l3.ip_groups.tx_max_handshake_time	true	tx_max_handshake_time	客户端握手最大时延	ns
l3.ip_groups.rx_max_handshake_time	true	rx_max_handshake_time	服务器握手最大时延	ns
l3.ip_groups.max_handshake_time	true	max_handshake_time	握手最大时延	ns
l3.ip_groups.tx_min_handshake_time	true	tx_min_handshake_time	客户端握手最小时延	ns
l3.ip_groups.rx_min_handshake_time	true	rx_min_handshake_time	服务器握手最小时延	ns
l3.ip_groups.min_handshake_time	true	min_handshake_time	握手最小时延	ns
l3.ip_groups.response_count	true	response_count	响应次数	number
l3.ip_groups.avg_response_time	true	avg_response_time	平均响应时延	ns
l3.ip_groups.max_response_time	true	max_response_time	最大响应时延	ns
l3.ip_groups.min_response_time	true	min_response_time	最小响应时延	ns
l3.ip_groups.interface	false	interface	网口	array

L3 IP Pair

id/field	is_series	name	title	type
l3.ip_pairs.ip_address	false	ip_address	IP地址	ip
l3.ip_pairs.ip_dhcp_name	false	ip_dhcp_name	DHCP主机名	array
l3.ip_pairs.dns_name	false	dns_name	DNS域名	array
l3.ip_pairs.http_name	false	http_name	HTTP主机名	array
l3.ip_pairs.tls_name	false	tls_name	TLS主机名	array
l3.ip_pairs.ip_os_name	false	ip_os_name	操作系统	array
l3.ip_pairs.ip_remark_name	false	ip_remark_name	备注名	array
l3.ip_pairs.region	false	region	国家/地区	string
l3.ip_pairs.ip_peer_address	false	ip_peer_address	对等IP	ip
l3.ip_pairs.peer_dhcp_name	false	peer_dhcp_name	对等DHCP主机名	array
l3.ip_pairs.peer_dns_name	false	peer_dns_name	对等DNS域名	array
l3.ip_pairs.peer_http_name	false	peer_http_name	对等HTTP主机名	array
l3.ip_pairs.peer_tls_name	false	peer_tls_name	对等TLS主机名	array
l3.ip_pairs.peer_os_name	false	peer_os_name	对等操作系统	array
l3.ip_pairs.peer_remark_name	false	peer_remark_name	对等备注名	array
l3.ip_pairs.peer_region	false	peer_region	对等国家/地区	string
l3.ip_pairs.first_activity_time	false	first_activity_time	首次活动时间	time
l3.ip_pairs.last_activity_time	false	last_activity_time	上次活动时间	time
l3.ip_pairs.tx_pkts	true	tx_pkts	IP地址到对等IP总包数	pkts
l3.ip_pairs.rx_pkts	true	rx_pkts	对等IP到IP地址总包数	pkts
l3.ip_pairs.pkts	true	pkts	总包数	pkts
l3.ip_pairs.tx_bytes	true	tx_bytes	IP地址到对等IP总字节数	bytes
l3.ip_pairs.rx_bytes	true	rx_bytes	对等IP到IP地址总字节数	bytes
l3.ip_pairs.bytes	true	bytes	总字节数	bytes
l3.ip_pairs.tx_pps	true	tx_pps	IP地址到对等IP每秒包数	pps
l3.ip_pairs.rx_pps	true	rx_pps	对等IP到IP地址每秒包数	pps
l3.ip_pairs.pps	true	pps	每秒包数	pps
l3.ip_pairs.tx_bps	true	tx_bps	IP地址到对等IP每秒流量	bps
l3.ip_pairs.rx_bps	true	rx_bps	对等IP到IP地址每秒流量	bps
l3.ip_pairs.bps	true	bps	每秒流量	bps
l3.ip_pairs.retransmit_bytes	true	retransmit_bytes	TCP重传流量	bytes
l3.ip_pairs.syn_count	true	syn_count	SYN包数量	pkts
l3.ip_pairs.syn_ack_count	true	syn_ack_count	SYN-ACK包数量	pkts
l3.ip_pairs.fin_count	true	fin_count	FIN包数量	pkts
l3.ip_pairs.rst_count	true	rst_count	RST包数量	pkts

L3 IP Group Pairs

id/field	is_series	name	title	type
l3.ip_group_pairs.ip_group_name	false	ip_group_name	IP组	string
l3.ip_group_pairs.ip_group_members	false	ip_group_members	IP组成员	array
l3.ip_group_pairs.ip_group_desc	false	ip_group_desc	IP组描述	string
l3.ip_group_pairs.ip_group_peer_name	false	ip_group_peer_name	对等IP组	string
l3.ip_group_pairs.ip_group_peer_members	false	ip_group_peer_members	对等IP组成员	array
l3.ip_group_pairs.ip_group_peer_desc	false	ip_group_peer_desc	对等IP组描述	string
l3.ip_group_pairs.first_activity_time	false	first_activity_time	首次活动时间	time
l3.ip_group_pairs.last_activity_time	false	last_activity_time	上次活动时间	time
l3.ip_group_pairs.tx_pkts	true	tx_pkts	IP地址到对等IP总包数	pkts
l3.ip_group_pairs.rx_pkts	true	rx_pkts	对等IP到IP地址总包数	pkts
l3.ip_group_pairs.pkts	true	pkts	总包数	pkts
l3.ip_group_pairs.tx_bytes	true	tx_bytes	IP地址到对等IP总字节数	bytes
l3.ip_group_pairs.rx_bytes	true	rx_bytes	对等IP到IP地址总字节数	bytes
l3.ip_group_pairs.bytes	true	bytes	总字节数	bytes
l3.ip_group_pairs.tx_pps	true	tx_pps	IP地址到对等IP每秒包数	pps
l3.ip_group_pairs.rx_pps	true	rx_pps	对等IP到IP地址每秒包数	pps
l3.ip_group_pairs.pps	true	pps	每秒包数	pps
l3.ip_group_pairs.tx_bps	true	tx_bps	IP地址到对等IP每秒流量	bps
l3.ip_group_pairs.rx_bps	true	rx_bps	对等IP到IP地址每秒流量	bps
l3.ip_group_pairs.bps	true	bps	每秒流量	bps
l3.ip_group_pairs.retransmit_bytes	true	retransmit_bytes	TCP重传流量	bytes
l3.ip_group_pairs.syn_count	true	syn_count	SYN包数量	pkts
l3.ip_group_pairs.syn_ack_count	true	syn_ack_count	SYN-ACK包数量	pkts
l3.ip_group_pairs.fin_count	true	fin_count	FIN包数量	pkts
l3.ip_group_pairs.rst_count	true	rst_count	RST包数量	pkts

L3 IP-MACs

id/field	is_series	name	title	type
l3.mac_ips.mac_address	false	mac_address	MAC地址	mac
l3.mac_ips.ip_address	false	ip_address	IP地址	ip
l3.mac_ips.mac_dhcp_name	false	mac_dhcp_name	MAC的DHCP主机名	array
l3.mac_ips.mac_os_name	false	mac_os_name	MAC的操作系统	array
l3.mac_ips.nic_vendor	false	nic_vendor	网卡供应商	string
l3.mac_ips.ip_dhcp_name	false	ip_dhcp_name	DHCP主机名	array
l3.mac_ips.dns_name	false	dns_name	DNS域名	array
l3.mac_ips.http_name	false	http_name	HTTP主机名	array
l3.mac_ips.tls_name	false	tls_name	TLS主机名	array
l3.mac_ips.ip_os_name	false	ip_os_name	操作系统	array
l3.mac_ips.region	false	region	国家/地区	string
l3.mac_ips.first_activity_time	false	first_activity_time	首次活动时间	time
l3.mac_ips.last_activity_time	false	last_activity_time	上次活动时间	time
l3.mac_ips.tx_pkts	true	tx_pkts	上行总包数	pkts
l3.mac_ips.rx_pkts	true	rx_pkts	下行总包数	pkts
l3.mac_ips.pkts	true	pkts	总包数	pkts
l3.mac_ips.tx_bytes	true	tx_bytes	上行总字节数	bytes
l3.mac_ips.rx_bytes	true	rx_bytes	下行总字节数	bytes
l3.mac_ips.bytes	true	bytes	总字节数	bytes
l3.mac_ips.tx_pps	true	tx_pps	上行每秒包数	pps
l3.mac_ips.rx_pps	true	rx_pps	下行每秒包数	pps
l3.mac_ips.pps	true	pps	每秒包数	pps
l3.mac_ips.tx_bps	true	tx_bps	上行每秒流量	bps
l3.mac_ips.rx_bps	true	rx_bps	下行每秒流量	bps
l3.mac_ips.bps	true	bps	每秒流量	bps

L3 IP Geo

id/field	is_series	name	title	type
l3.ip_region.region	false	region	国家/地区	string
l3.ip_region.tx_pkts	true	tx_pkts	总发包数	pkts
l3.ip_region.rx_pkts	true	rx_pkts	总收包数	pkts
l3.ip_region.pkts	true	pkts	总包数	pkts
l3.ip_region.tx_bytes	true	tx_bytes	总发送字节数	bytes
l3.ip_region.rx_bytes	true	rx_bytes	总接收字节数	bytes
l3.ip_region.bytes	true	bytes	总字节数	bytes
l3.ip_region.tx_pps	true	tx_pps	每秒发包数	pps
l3.ip_region.rx_pps	true	rx_pps	每秒收包数	pps
l3.ip_region.pps	true	pps	每秒包数	pps
l3.ip_region.tx_bps	true	tx_bps	每秒发送流量	bps
l3.ip_region.rx_bps	true	rx_bps	每秒接收流量	bps
l3.ip_region.bps	true	bps	每秒流量	bps

L3 IP ICMP

L3 IP ICMP Overview

id/field	is_series	name	title	type
l3.icmp.overview.pkts	true	pkts	总包数	pkts
l3.icmp.overview.bytes	true	bytes	总字节数	bytes
l3.icmp.overview.pps	true	pps	每秒包数	pps
l3.icmp.overview.bps	true	bps	每秒流量	bps

L3 IP ICMP 常见类型

id/field	is_series	name	title	type
l3.icmp.common_types.title	false	title	常见ICMP类型	string
l3.icmp.common_types.pkts	true	pkts	总包数	pkts
l3.icmp.common_types.bytes	true	bytes	总字节数	bytes
l3.icmp.common_types.pps	true	pps	每秒包数	pps
l3.icmp.common_types.bps	true	bps	每秒流量	bps

L3 IP ICMP Ping

id/field	is_series	name	title	type
l3.icmp.ping_time.tx_ip	false	tx_ip	ping来自	ip
l3.icmp.ping_time.tx_dhcp_name	false	tx_dhcp_name	ping来自DHCP主机名	array
l3.icmp.ping_time.tx_os_name	false	tx_os_name	ping来自操作系统名	array
l3.icmp.ping_time.tx_dns_name	false	tx_dns_name	ping来自DNS域名	array
l3.icmp.ping_time.tx_http_name	false	tx_http_name	ping来自HTTP主机名	array
l3.icmp.ping_time.tx_tls_name	false	tx_tls_name	ping来自TLS主机名	array
l3.icmp.ping_time.tx_region	false	tx_region	ping来自国家/地区	string
l3.icmp.ping_time.last_req_time	false	last_req_time	最新请求时间	time
l3.icmp.ping_time.rx_ip	false	rx_ip	ping目标	ip
l3.icmp.ping_time.rx_dhcp_name	false	rx_dhcp_name	ping目标DHCP主机名	array
l3.icmp.ping_time.rx_os_name	false	rx_os_name	ping目标操作系统名	array
l3.icmp.ping_time.rx_dns_name	false	rx_dns_name	ping目标DNS域名	array
l3.icmp.ping_time.rx_http_name	false	rx_http_name	ping目标HTTP主机名	array
l3.icmp.ping_time.rx_tls_name	false	rx_tls_name	ping目标TLS主机名	array
l3.icmp.ping_time.rx_region	false	rx_region	ping目标国家/地区	string
l3.icmp.ping_time.last_resp_time	false	last_resp_time	最新应答时间	time
l3.icmp.ping_time.min	true	min	ping最小响应	ns
l3.icmp.ping_time.avg	true	avg	ping平均响应	ns
l3.icmp.ping_time.max	true	max	ping最大响应	ns
l3.icmp.ping_time.request_count	true	request_count	ping请求数量	number
l3.icmp.ping_time.response_count	true	response_count	ping应答数量	number

L3 QoS

id/field	is_series	name	title	type
l3.qos.ip.ip_qos	false	ip_qos	IP QoS	string
l3.qos.ip.pkts	true	pkts	总包数	pkts
l3.qos.ip.bytes	true	bytes	总字节数	bytes
l3.qos.ip.pps	true	pps	每秒包数	pps
l3.qos.ip.bps	true	bps	每秒流量	bps
l3.qos.ip	false	ip	IP-Qos	
l3.qos.ip_dscp.ip_address	false	ip_address	IP地址	ip
l3.qos.ip_dscp.ip_dhcp_name	false	ip_dhcp_name	DHCP主机名	array
l3.qos.ip_dscp.dns_name	false	dns_name	DNS域名	array
l3.qos.ip_dscp.http_name	false	http_name	HTTP主机名	array
l3.qos.ip_dscp.tls_name	false	tls_name	TLS主机名	array
l3.qos.ip_dscp.ip_os_name	false	ip_os_name	操作系统	array
l3.qos.ip_dscp.region	false	region	国家/地区	string
l3.qos.ip_dscp.ip_qos	false	ip_qos	QoS	string
l3.qos.ip_dscp.tx_pkts	true	tx_pkts	总发包数	pkts
l3.qos.ip_dscp.rx_pkts	true	rx_pkts	总收包数	pkts
l3.qos.ip_dscp.pkts	true	pkts	总包数	pkts
l3.qos.ip_dscp.tx_bytes	true	tx_bytes	总发送字节数	bytes
l3.qos.ip_dscp.rx_bytes	true	rx_bytes	总接收字节数	bytes
l3.qos.ip_dscp.bytes	true	bytes	总字节数	bytes
l3.qos.ip_dscp.tx_pps	true	tx_pps	每秒发包数	pps
l3.qos.ip_dscp.rx_pps	true	rx_pps	每秒收包数	pps
l3.qos.ip_dscp.pps	true	pps	每秒包数	pps
l3.qos.ip_dscp.tx_bps	true	tx_bps	每秒发送流量	bps
l3.qos.ip_dscp.rx_bps	true	rx_bps	每秒接收流量	bps
l3.qos.ip_dscp.bps	true	bps	每秒流量	bps

L4 连接

id/field	is_series	name	title	type
l4.flow.tx_ip	false	tx_ip	客户端IP	ip
l4.flow.tx_port	false	tx_port	客户端端口	number
l4.flow.tx_dhcp_name	false	tx_dhcp_name	客户端DHCP主机名	array
l4.flow.tx_dns_name	false	tx_dns_name	客户端DNS域名	array
l4.flow.tx_http_name	false	tx_http_name	客户端HTTP主机名	array
l4.flow.tx_tls_name	false	tx_tls_name	客户端TLS主机名	array
l4.flow.tx_os_name	false	tx_os_name	客户端操作系统	array
l4.flow.tx_region	false	tx_region	客户端国家/地区	string
l4.flow.rx_ip	false	rx_ip	服务器IP	ip
l4.flow.rx_port	false	rx_port	服务器端口	number
l4.flow.rx_dhcp_name	false	rx_dhcp_name	服务器DHCP主机名	array
l4.flow.rx_dns_name	false	rx_dns_name	服务器DNS域名	array
l4.flow.rx_http_name	false	rx_http_name	服务器HTTP主机名	array
l4.flow.rx_tls_name	false	rx_tls_name	服务器TLS主机名	array
l4.flow.rx_os_name	false	rx_os_name	服务器操作系统	array
l4.flow.rx_region	false	rx_region	服务器国家/地区	string
l4.flow.l4_protocol	false	l4_protocol	L4协议	string
l4.flow.first_activity_time	false	first_activity_time	首次活动时间	time
l4.flow.last_activity_time	false	last_activity_time	上次活动时间	time
l4.flow.tx_pkts	true	tx_pkts	客户端总发包数	pkts
l4.flow.rx_pkts	true	rx_pkts	服务器总发包数	pkts
l4.flow.pkts	true	pkts	总包数	pkts
l4.flow.tx_bytes	true	tx_bytes	客户端总发送字节数	bytes
l4.flow.rx_bytes	true	rx_bytes	服务器总发送字节数	bytes
l4.flow.bytes	true	bytes	总字节数	bytes
l4.flow.tx_pps	true	tx_pps	客户端每秒发包数	pps
l4.flow.rx_pps	true	rx_pps	服务器每秒发包数	pps
l4.flow.pps	true	pps	每秒包数	pps
l4.flow.tx_bps	true	tx_bps	客户端每秒发送流量	bps
l4.flow.rx_bps	true	rx_bps	服务器每秒发送流量	bps
l4.flow.bps	true	bps	每秒流量	bps
l4.flow.tx_l4_payload_bytes	true	tx_l4_payload_bytes	客户端l4字节	bytes
l4.flow.rx_l4_payload_bytes	true	rx_l4_payload_bytes	服务器l4字节	bytes
l4.flow.l4_payload_bytes	true	l4_payload_bytes	l4字节	bytes
l4.flow.tx_retransmit_bytes	true	tx_retransmit_bytes	客户端重传字节	bytes
l4.flow.rx_retransmit_bytes	true	rx_retransmit_bytes	服务器重传字节	bytes
l4.flow.retransmit_bytes	true	retransmit_bytes	重传字节	bytes
l4.flow.tx_retransmit_rate	true	tx_retransmit_rate	客户端重传率	permyriad
l4.flow.rx_retransmit_rate	true	rx_retransmit_rate	服务器重传率	permyriad
l4.flow.retransmit_rate	true	retransmit_rate	重传率	permyriad

l4.flow.tx_retransmit_pkts	true	tx_retransmit_pkts	客户端重传包	pkts
l4.flow.rx_retransmit_pkts	true	rx_retransmit_pkts	服务器重传包	pkts
l4.flow.retransmit_pkts	true	retransmit_pkts	重传包	pkts
l4.flow.tx_out_of_order_pkts	true	tx_out_of_order_pkts	客户端乱序包	pkts
l4.flow.rx_out_of_order_pkts	true	rx_out_of_order_pkts	服务器乱序包	pkts
l4.flow.out_of_order_pkts	true	out_of_order_pkts	乱序包	pkts
l4.flow.syn_count	true	syn_count	SYN包数量	pkts
l4.flow.syn_ack_count	true	syn_ack_count	SYN-ACK包数量	pkts
l4.flow.fin_count	true	fin_count	FIN包数量	pkts
l4.flow.rst_count	true	rst_count	RST包数量	pkts
l4.flow.tx_handshake_count	true	tx_handshake_count	客户端握手次数	number
l4.flow.rx_handshake_count	true	rx_handshake_count	服务器握手次数	number
l4.flow.handshake_count	true	handshake_count	握手次数	number
l4.flow.tx_avg_handshake_time	true	tx_avg_handshake_time	客户端握手平均时延	ns
l4.flow.rx_avg_handshake_time	true	rx_avg_handshake_time	服务器握手平均时延	ns
l4.flow.avg_handshake_time	true	avg_handshake_time	握手平均时延	ns
l4.flow.tx_max_handshake_time	true	tx_max_handshake_time	客户端握手最大时延	ns
l4.flow.rx_max_handshake_time	true	rx_max_handshake_time	服务器握手最大时延	ns
l4.flow.max_handshake_time	true	max_handshake_time	握手最大时延	ns
l4.flow.tx_min_handshake_time	true	tx_min_handshake_time	客户端握手最小时延	ns
l4.flow.rx_min_handshake_time	true	rx_min_handshake_time	服务器握手最小时延	ns
l4.flow.min_handshake_time	true	min_handshake_time	握手最小时延	ns
l4.flow.close_time	true	close_time	流关闭时间	time
l4.flow.tx_dup_ack_count	true	tx_dup_ack_count	客户端重复ACK的TCP包	pkts
l4.flow.rx_dup_ack_count	true	rx_dup_ack_count	服务器重复ACK的TCP包	pkts
l4.flow.dup_ack_count	true	dup_ack_count	重复ACK的TCP包	pkts
l4.flow.close_reason	true	close_reason	会话状态	string
l4.flow.tx_mss	true	tx_mss	客户端MSS	bytes
l4.flow.rx_mss	true	rx_mss	服务器MSS	bytes
l4.flow.mss	true	mss	MSS	bytes
l4.flow.tx_window_scale	true	tx_window_scale	客户端窗口缩放	number
l4.flow.rx_window_scale	true	rx_window_scale	服务器窗口缩放	number
l4.flow.window_scale	true	window_scale	窗口缩放	number
l4.flow.tx_zero_window_count	true	tx_zero_window_count	客户端零窗口	pkts
l4.flow.rx_zero_window_count	true	rx_zero_window_count	服务器零窗口	pkts
l4.flow.zero_window_count	true	zero_window_count	零窗口	pkts
l4.flow.tx_max_window	true	tx_max_window	客户端最大窗口	bytes
l4.flow.rx_max_window	true	rx_max_window	服务器最大窗口	bytes
l4.flow.max_window	true	max_window	最大窗口	bytes
l4.flow.tx_max_flight	true	tx_max_flight	客户端最大未确认传输	bytes
l4.flow.rx_max_flight	true	rx_max_flight	服务器最大未确认传输	bytes
l4.flow.max_flight	true	max_flight	最大未确认传输	bytes
l4.flow.tx_mtu	true	tx_mtu	客户端MTU	bytes
l4.flow.rx_mtu	true	rx_mtu	服务器MTU	bytes

l4.flow.mtu	true	mtu	MTU	bytes
l4.flow.l7_protocol	false	l7_protocol	应用层协议	string
l4.flow.flow_info	false	flow_info	流信息	string
l4.flow.tx_response_count	true	tx_response_count	客户端响应次数	number
l4.flow.rx_response_count	true	rx_response_count	服务器响应次数	number
l4.flow.response_count	true	response_count	响应次数	number
l4.flow.tx_avg_response_time	true	tx_avg_response_time	客户端平均响应时延	ns
l4.flow.rx_avg_response_time	true	rx_avg_response_time	服务器平均响应时延	ns
l4.flow.avg_response_time	true	avg_response_time	平均响应时延	ns
l4.flow.tx_max_response_time	true	tx_max_response_time	客户端最大响应时延	ns
l4.flow.rx_max_response_time	true	rx_max_response_time	服务器最大响应时延	ns
l4.flow.max_response_time	true	max_response_time	最大响应时延	ns
l4.flow.tx_min_response_time	true	tx_min_response_time	客户端最小响应时延	ns
l4.flow.rx_min_response_time	true	rx_min_response_time	服务器最小响应时延	ns
l4.flow.min_response_time	true	min_response_time	最小响应时延	ns
l4.flow.avg_l7_response_time	true	avg_l7_response_time	应用层平均响应时延	ns
l4.flow.max_l7_response_time	true	max_l7_response_time	应用层最大响应时延	ns
l4.flow.min_l7_response_time	true	min_l7_response_time	应用层最小响应时延	ns
l4.flow.interface	false	interface	网口	array
l4.flow.application_latency	true	application_latency	应用时延	ns
l4.flow.tls_hello_avg_handshake_time	true	tls_hello_avg_handshake_time	TLS Hello平均握手时延	ns
l4.flow.tls_hello_max_handshake_time	true	tls_hello_max_handshake_time	TLS Hello最大握手时延	ns
l4.flow.tls_hello_min_handshake_time	true	tls_hello_min_handshake_time	TLS Hello最小握手时延	ns
l4.flow.tls_hello_handshake_count	true	tls_hello_handshake_count	TLS Hello握手次数	number
l4.flow.tls_data_avg_response_time	true	tls_data_avg_response_time	TLS第一次数据响应平均时延	ns
l4.flow.tls_data_max_response_time	true	tls_data_max_response_time	TLS第一次数据响应最大时延	ns
l4.flow.tls_data_min_response_time	true	tls_data_min_response_time	TLS第一次数据响应最小时延	ns
l4.flow.tls_data_response_count	true	tls_data_response_count	TLS第一次数据响应次数	number
l4.flow.tls_cipher	false	tls_cipher	TLS协商的加密算法	string
l4.flow.tls_version	false	tls_version	TLS版本	string
l4.flow.validity	false	validity	有效性	string

L4 TCP

id/field	is_series	name	title	type
l4.tcp.pkts	true	pkts	数据包数	pkts
l4.tcp.bytes	true	bytes	总字节数	bytes
l4.tcp.pps	true	pps	每秒数据包数	pps
l4.tcp.bps	true	bps	每秒流量	bps
l4.tcp.l4_payload_bytes	true	l4_payload_bytes	4层载荷	bps
l4.tcp.tx_handshake_count	true	tx_handshake_count	客户端握手次数	number
l4.tcp.rx_handshake_count	true	rx_handshake_count	服务器握手次数	number
l4.tcp.handshake_count	true	handshake_count	握手次数	number
l4.tcp.tx_avg_handshake_time	true	tx_avg_handshake_time	客户端平均握手时延	ns
l4.tcp.rx_avg_handshake_time	true	rx_avg_handshake_time	服务器平均握手时延	ns
l4.tcp.avg_handshake_time	true	avg_handshake_time	平均握手时延	ns
l4.tcp.tx_max_handshake_time	true	tx_max_handshake_time	客户端最大握手时延	ns
l4.tcp.rx_max_handshake_time	true	rx_max_handshake_time	服务器最大握手时延	ns
l4.tcp.max_handshake_time	true	max_handshake_time	最大握手时延	ns
l4.tcp.tx_min_handshake_time	true	tx_min_handshake_time	客户端最小握手时延	ns
l4.tcp.rx_min_handshake_time	true	rx_min_handshake_time	服务器最小握手时延	ns
l4.tcp.min_handshake_time	true	min_handshake_time	最小握手时延	ns
l4.tcp.tx_avg_response_time	true	tx_avg_response_time	客户端平均响应时延	ns
l4.tcp.rx_avg_response_time	true	rx_avg_response_time	服务器平均响应时延	ns
l4.tcp.avg_response_time	true	avg_response_time	平均响应时延	ns
l4.tcp.tx_max_response_time	true	tx_max_response_time	客户端最大响应时延	ns
l4.tcp.rx_max_response_time	true	rx_max_response_time	服务器最大响应时延	ns
l4.tcp.max_response_time	true	max_response_time	最大响应时延	ns
l4.tcp.tx_min_response_time	true	tx_min_response_time	客户端最小响应时延	ns
l4.tcp.rx_min_response_time	true	rx_min_response_time	服务器最小响应时延	ns
l4.tcp.min_response_time	true	min_response_time	最小响应时延	ns
l4.tcp.retransmit_bytes	true	retransmit_bytes	重传字节	bytes
l4.tcp.retransmit_rate	true	retransmit_rate	重传率	permyriad
l4.tcp.syn_count	true	syn_count	SYN包数量	number
l4.tcp.syn_ack_count	true	syn_ack_count	SYN-ACK包数量	number
l4.tcp.fin_count	true	fin_count	FIN包数量	number
l4.tcp.rst_count	true	rst_count	RST包数量	number
l4.tcp.dup_ack_count	true	dup_ack_count	重复ACK包数量	number
l4.tcp.zero_window_count	true	zero_window_count	零窗口包数量	number
l4.tcp.out_of_order_pkts	true	out_of_order_pkts	乱序包数量	number

L7 DHCP

L7 DHCP Overview

id/field	is_series	name	title	type
l7.dhcp.global_response_times.response_count	false	response_count	响应的数量	number
l7.dhcp.global_response_times.min	true	min	最小响应耗时	ns
l7.dhcp.global_response_times.avg	true	avg	平均响应耗时	ns
l7.dhcp.global_response_times.max	true	max	最大响应耗时	ns
l7.dhcp.global_response_times	false	global_response_times	全局响应耗时	
l7.dhcp.overview.ip_address	false	ip_address	IP地址	ip
l7.dhcp.overview.ip_os_name	false	ip_os_name	操作系统名	array
l7.dhcp.overview.hostname	false	hostname	主机名称	string
l7.dhcp.overview.mac_address	false	mac_address	MAC地址	mac
l7.dhcp.overview.mac_os_name	false	mac_os_name	MAC操作系统名	array
l7.dhcp.overview.nic_vendor	false	nic_vendor	网卡供应商	array
l7.dhcp.overview.subnet_mask	false	subnet_mask	子网掩码	string
l7.dhcp.overview.rx_ip	false	rx_ip	DHCP服务器IP地址	ip
l7.dhcp.overview.update_time	false	update_time	分配时间	time
l7.dhcp.overview.lease_time	false	lease_time	租期	s
l7.dhcp.message_types.message_unknown_type_count	true	message_unknown_type_count	unknown	number
l7.dhcp.message_types.message_discover_type_count	true	message_discover_type_count	discover	number
l7.dhcp.message_types.message_offer_type_count	true	message_offer_type_count	offer	number
l7.dhcp.message_types.message_request_type_count	true	message_request_type_count	request	number
l7.dhcp.message_types.message_decline_type_count	true	message_decline_type_count	decline	number
l7.dhcp.message_types.message_ack_type_count	true	message_ack_type_count	ack	number
l7.dhcp.message_types.message_nack_type_count	true	message_nack_type_count	nack	number
l7.dhcp.message_types.message_release_type_count	true	message_release_type_count	release	number
l7.dhcp.message_types.message_inform_type_count	true	message_inform_type_count	inform	number

L7 DHCP 服务器

id/field	is_series	name	title	type
l7.dhcp.server.ip_address	false	ip_address	IP地址	ip
l7.dhcp.server.hostname	false	hostname	主机名称	string
l7.dhcp.server.last_activity_time	false	last_activity_time	最近更新时间	time
l7.dhcp.server.succeed_request_count	true	succeed_request_count	成功请求数量	number
l7.dhcp.server.different_ips	true	different_ips	分配IP数量	number

L7 DNS

L7 DNS 服务器

id/field	is_series	name	title	type
l7.dns.server.ip_address	false	ip_address	IP地址	ip
l7.dns.server.ip_dhcp_name	false	ip_dhcp_name	DHCP主机名	array
l7.dns.server.dns_name	false	dns_name	DNS域名	array
l7.dns.server.http_name	false	http_name	HTTP主机名	array
l7.dns.server.tls_name	false	tls_name	TLS主机名	array
l7.dns.server.ip_os_name	false	ip_os_name	操作系统	array
l7.dns.server.region	false	region	国家/地区	string
l7.dns.server.request_count	true	request_count	请求数量	number
l7.dns.server.response_count	true	response_count	响应数量	number
l7.dns.server.request_per_sec_count	true	request_per_sec_count	每秒请求数量	number
l7.dns.server.response_per_sec_count	true	response_per_sec_count	每秒响应数量	number
l7.dns.server.min	true	min	最小响应耗时	ns
l7.dns.server.avg	true	avg	平均响应耗时	ns
l7.dns.server.max	true	max	最大响应耗时	ns
l7.dns.server.succeed_request_count	true	succeed_request_count	成功响应数量	number
l7.dns.server.error_request_count	true	error_request_count	错误请求数量	number
l7.dns.server.format_error_count	true	format_error_count	格式错误请求数量	number
l7.dns.server.server_error_count	true	server_error_count	服务器错误请求数量	number
l7.dns.server.not_exist_count	true	not_exist_count	查询不存在错误数量	number
l7.dns.server.other_error_count	true	other_error_count	其他错误数量	number

L7 DNS 解析

id/field	is_series	name	title	type
l7.dns.resolved_names.domain_name	false	domain_name	请求域名	string
l7.dns.resolved_names.resolved_ip	false	resolved_ip	解析结果(IP)	array
l7.dns.resolved_names.update_time	false	update_time	更新时间	time
l7.dns.resolved_names.expire_time	false	expire_time	过期时间	time
l7.dns.resolved_names.rx_ip	false	rx_ip	服务器IP	ip

L7 DNS 服务器响应时间

id/field	is_series	name	title	type
l7.dns.global_response_times.min	true	min	最小响应耗时	ns
l7.dns.global_response_times.avg	true	avg	平均响应耗时	ns
l7.dns.global_response_times.max	true	max	最大响应耗时	ns

L7 DNS 服务器响应代码

id/field	is_series	name	title	type
l7.dns.global_reply_codes.request_count	true	request_count	请求数量	number
l7.dns.global_reply_codes.response_count	true	response_count	响应数量	number
l7.dns.global_reply_codes.succeed_request_count	true	succeed_request_count	成功响应数量	number
l7.dns.global_reply_codes.error_request_count	true	error_request_count	错误请求数量	number
l7.dns.global_reply_codes.format_error_count	true	format_error_count	格式错误请求数量	number
l7.dns.global_reply_codes.server_error_count	true	server_error_count	服务器错误请求数量	number
l7.dns.global_reply_codes.not_exist_count	true	not_exist_count	查询不存在错误数量	number
l7.dns.global_reply_codes.other_error_count	true	other_error_count	其他错误数量	number

L7 DNS 记录类型

id/field	is_series	name	title	type
l7.dns.global_record_types.packet_a_record_type_count	true	packet_a_record_type_count	A记录类型包数量	number
l7.dns.global_record_types.packet_aaaa_record_type_count	true	packet_aaaa_record_type_count	AAAA记录类型包数量	number
l7.dns.global_record_types.packet_cname_record_type_count	true	packet_cname_record_type_count	CNAME记录类型包数量	number
l7.dns.global_record_types.packet_mx_record_type_count	true	packet_mx_record_type_count	MX记录类型包数量	number
l7.dns.global_record_types.packet_srv_record_type_count	true	packet_srv_record_type_count	SRV记录类型包数量	number
l7.dns.global_record_types.packet_other_record_type_count	true	packet_other_record_type_count	其它记录类型包数量	number
l7.dns.global_record_types	false	global_record_types	记录类型计数总数	
l7.dns.record_types.title	false	title	类型	string
l7.dns.record_types.pps	true	pps	每秒包数量	pps
l7.dns.record_types.bps	true	bps	每秒流量	bps

L7 HTTP

L7 HTTP 服务器

id/field	is_series	name	title	type
l7.http.server.ip_address	false	ip_address	IP地址	ip
l7.http.server.hostname	false	hostname	主机名	array
l7.http.server.http_name	false	http_name	HTTP主机名	array
l7.http.server.ip_dhcp_name	false	ip_dhcp_name	DHCP主机名	array
l7.http.server.tls_name	false	tls_name	TLS主机名	array
l7.http.server.dns_name	false	dns_name	DNS域名	array
l7.http.server.ip_os_name	false	ip_os_name	操作系统	array
l7.http.server.region	false	region	国家/地区	string
l7.http.server.request_count	false	request_count	请求数量	number
l7.http.server.min	true	min	最小响应耗时	ns
l7.http.server.avg	true	avg	平均响应耗时	ns
l7.http.server.max	true	max	最大响应耗时	ns
l7.http.server.response_count	true	response_count	响应数量	number
l7.http.server.http_response_1xx_type_count	true	http_response_1xx_type_count	1xx(信息)响应数量	number
l7.http.server.http_response_2xx_type_count	true	http_response_2xx_type_count	2xx(成功)响应数量	number
l7.http.server.http_response_3xx_type_count	true	http_response_3xx_type_count	3xx(重定向)响应数量	number
l7.http.server.http_response_4xx_type_count	true	http_response_4xx_type_count	4xx(客户端错误)响应数量	number
l7.http.server.http_response_5xx_type_count	true	http_response_5xx_type_count	5xx(服务器错误)响应数量	number
l7.http.server.http_response_other_type_count	true	http_response_other_type_count	(其他)响应数量	number

L7 HTTP 响应时间

id/field	is_series	name	title	type
l7.http.global_response_times.request_count	false	request_count	请求数量	number
l7.http.global_response_times.min	true	min	最小响应耗时	ns
l7.http.global_response_times.avg	true	avg	平均响应耗时	ns
l7.http.global_response_times.max	true	max	最大响应耗时	ns

L7 HTTP 响应代码

id/field	is_series	name	title	type
l7.http.global_reply_codes.response_count	true	response_count	响应数量	number
l7.http.global_reply_codes.http_response_1xx_type_count	true	http_response_1xx_type_count	1xx(信息)响应数量	number
l7.http.global_reply_codes.http_response_2xx_type_count	true	http_response_2xx_type_count	2xx(成功)响应数量	number
l7.http.global_reply_codes.http_response_3xx_type_count	true	http_response_3xx_type_count	3xx(重定向)响应数量	number
l7.http.global_reply_codes.http_response_4xx_type_count	true	http_response_4xx_type_count	4xx(客户端错误)响应数量	number
l7.http.global_reply_codes.http_response_5xx_type_count	true	http_response_5xx_type_count	5xx(服务器错误)响应数量	number
l7.http.global_reply_codes.http_response_other_type_count	true	http_response_other_type_count	(其他)响应数量	number

L7 TLS

L7 TLS 服务器

id/field	is_series	name	title	type
l7.tls.server.ip_address	false	ip_address	IP地址	ip
l7.tls.server.hostname	false	hostname	主机名	array
l7.tls.server.tls_name	false	tls_name	TLS主机名	array
l7.tls.server.http_name	false	http_name	HTTP主机名	array
l7.tls.server.ip_dhcp_name	false	ip_dhcp_name	DHCP主机名	array
l7.tls.server.dns_name	false	dns_name	DNS域名	array
l7.tls.server.ip_os_name	false	ip_os_name	操作系统	array
l7.tls.server.region	false	region	国家/地区	string
l7.tls.server.tls_hello_avg_handshake_time	true	tls_hello_avg_handshake_time	Hello平均握手时延	ns
l7.tls.server.tls_hello_max_handshake_time	true	tls_hello_max_handshake_time	Hello最大握手时延	ns
l7.tls.server.tls_hello_min_handshake_time	true	tls_hello_min_handshake_time	Hello最小握手时延	ns
l7.tls.server.tls_hello_handshake_count	true	tls_hello_handshake_count	Hello握手次数	number
l7.tls.server.tls_data_avg_response_time	true	tls_data_avg_response_time	第一次数据响应平均时延	ns
l7.tls.server.tls_data_max_response_time	true	tls_data_max_response_time	第一次数据响应最大时延	ns
l7.tls.server.tls_data_min_response_time	true	tls_data_min_response_time	第一次数据响应最小时延	ns
l7.tls.server.tls_data_response_count	true	tls_data_response_count	第一次数据响应次数	number
l7.tls.server.tls_cipher	false	tls_cipher	协商的加密算法	string
l7.tls.server.tls_version	false	tls_version	TLS版本	string
l7.tls.server.tls_cert_server_names	false	tls_cert_server_names	证书中服务器名称	array
l7.tls.server.tls_cert_issuer_dn	false	tls_cert_issuer_dn	证书发布者名称	array
l7.tls.server.tls_cert_subject_dn	false	tls_cert_subject_dn	证书主体名称	array
l7.tls.server.tls_cert_not_before	false	tls_cert_not_before	证书有效期从	time
l7.tls.server.tls_cert_not_after	false	tls_cert_not_after	证书有效期到	time

L7 TLS 响应时延

id/field	is_series	name	title	type
l7.tls.global.tls_hello_avg_handshake_time	true	tls_hello_avg_handshake_time	Hello平均握手时延	ns
l7.tls.global.tls_hello_max_handshake_time	true	tls_hello_max_handshake_time	Hello最大握手时延	ns
l7.tls.global.tls_hello_min_handshake_time	true	tls_hello_min_handshake_time	Hello最小握手时延	ns
l7.tls.global.tls_hello_handshake_count	true	tls_hello_handshake_count	Hello握手次数	number
l7.tls.global.tls_data_avg_response_time	true	tls_data_avg_response_time	第一次数据响应平均时延	ns
l7.tls.global.tls_data_max_response_time	true	tls_data_max_response_time	第一次数据响应最大时延	ns
l7.tls.global.tls_data_min_response_time	true	tls_data_min_response_time	第一次数据响应最小时延	ns
l7.tls.global.tls_data_response_count	true	tls_data_response_count	第一次数据响应次数	number

L7 应用层协议

id/field	is_series	name	title	type
l7.L7_proto.l7_protocol	false	l7_protocol	协议(应用)名	string
l7.L7_proto.l7_proto_desc	false	l7_proto_desc	协议(应用)描述	string
l7.L7_proto.first_activity_time	false	first_activity_time	首次活动时间	time
l7.L7_proto.last_activity_time	false	last_activity_time	上次活动时间	time
l7.L7_proto.pkts	true	pkts	总包数	pkts
l7.L7_proto.bytes	true	bytes	总字节数	bytes
l7.L7_proto.pps	true	pps	每秒包数	pps
l7.L7_proto.bps	true	bps	每秒流量	bps

L7 应用层协议-MACs

id/field	is_series	name	title	type
l7.mac_L7_proto.mac_address	false	mac_address	MAC地址	mac
l7.mac_L7_proto.mac_dhcp_name	false	mac_dhcp_name	MAC的DHCP主机名	string
l7.mac_L7_proto.mac_os_name	false	mac_os_name	MAC的操作系统	string
l7.mac_L7_proto.nic_vendor	false	nic_vendor	网卡供应商	string
l7.mac_L7_proto.l7_protocol	false	l7_protocol	协议(应用)名	string
l7.mac_L7_proto.first_activity_time	false	first_activity_time	首次活动时间	time
l7.mac_L7_proto.last_activity_time	false	last_activity_time	上次活动时间	time
l7.mac_L7_proto.tx_pkts	true	tx_pkts	上行总包数	pkts
l7.mac_L7_proto.rx_pkts	true	rx_pkts	下行总包数	pkts
l7.mac_L7_proto.pkts	true	pkts	总包数	pkts
l7.mac_L7_proto.tx_bytes	true	tx_bytes	上行总字节数	bytes
l7.mac_L7_proto.rx_bytes	true	rx_bytes	下行总字节数	bytes
l7.mac_L7_proto.bytes	true	bytes	总字节数	bytes
l7.mac_L7_proto.tx_pps	true	tx_pps	上行每秒包数	pps
l7.mac_L7_proto.rx_pps	true	rx_pps	下行每秒包数	pps
l7.mac_L7_proto.pps	true	pps	每秒包数	pps
l7.mac_L7_proto.tx_bps	true	tx_bps	上行每秒流量	bps
l7.mac_L7_proto.rx_bps	true	rx_bps	下行每秒流量	bps
l7.mac_L7_proto.bps	true	bps	每秒流量	bps

L7 应用层协议-IPs

id/field	is_series	name	title	type
l7.ip_L7_proto.ip_address	false	ip_address	IP地址	ip
l7.ip_L7_proto.l7_protocol	false	l7_protocol	协议(应用)名	string
l7.ip_L7_proto.ip_dhcp_name	false	ip_dhcp_name	DHCP主机名	string
l7.ip_L7_proto.dns_name	false	dns_name	DNS域名	string
l7.ip_L7_proto.http_name	false	http_name	HTTP主机名	string
l7.ip_L7_proto.tls_name	false	tls_name	TLS主机名	string
l7.ip_L7_proto.ip_os_name	false	ip_os_name	操作系统	string
l7.ip_L7_proto.first_activity_time	false	first_activity_time	首次活动时间	time
l7.ip_L7_proto.last_activity_time	false	last_activity_time	上次活动时间	time
l7.ip_L7_proto.tx_pkts	true	tx_pkts	上行总包数	pkts
l7.ip_L7_proto.rx_pkts	true	rx_pkts	下行总包数	pkts
l7.ip_L7_proto.pkts	true	pkts	总包数	pkts
l7.ip_L7_proto.tx_bytes	true	tx_bytes	上行总字节数	bytes
l7.ip_L7_proto.rx_bytes	true	rx_bytes	下行总字节数	bytes
l7.ip_L7_proto.bytes	true	bytes	总字节数	bytes
l7.ip_L7_proto.tx_pps	true	tx_pps	上行每秒包数	pps
l7.ip_L7_proto.rx_pps	true	rx_pps	下行每秒包数	pps
l7.ip_L7_proto.pps	true	pps	每秒包数	pps
l7.ip_L7_proto.tx_bps	true	tx_bps	上行每秒流量	bps
l7.ip_L7_proto.rx_bps	true	rx_bps	下行每秒流量	bps
l7.ip_L7_proto.bps	true	bps	每秒流量	bps

- 江门市云争科技有限公司
- www.anatraf.com