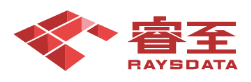
Nginx日志模板参照说明



北京睿至大数据有限公司2017年10月31日

目录

说明 2

1.1 Nginx Access日志样例 2

1.2 Nginx Access日志字段映射列表 3

1.3 Nginx Access日志源格式配置 3

1.4 Nginx Access日志解析方式 4

# 说明

Nginx主要指 Nginx 的 Access 日志

## Nginx Access日志样例

10.20.50.137 - guwei [01/Sep/2017:16:44:47 +0800] "POST /api/v1/requirement/list HTTP/1.1" 200 532 "http://test.raysdata- lab.com" "Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36" "-"

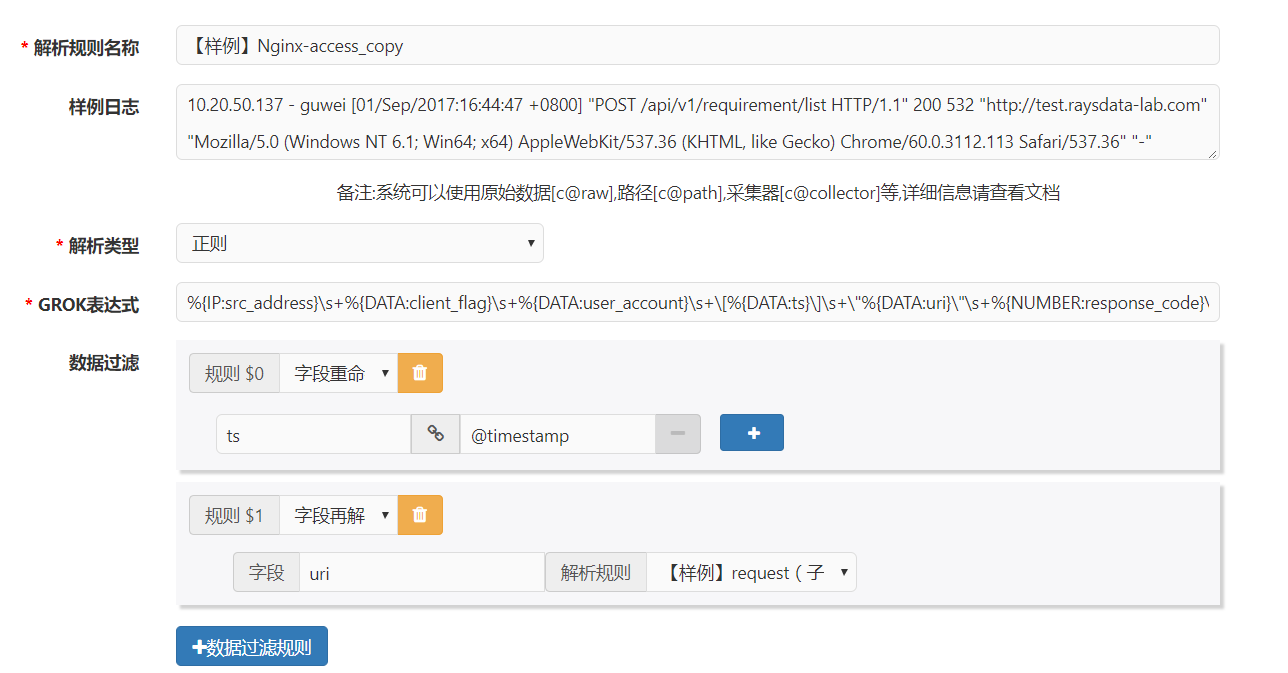
## Nginx Access日志字段映射列表

|  |  |  |
| --- | --- | --- |
| **字段名** | **类型** | **内容** |
| @timestamp | Date | 01/Sep/2017:16:44:47 +0800 |
| src\_address | Text | 10.20.50.137 |
| request | Text | /api/v1/requirement/list |
| bytes\_sent | Number | 532 |
| user\_agent | Text | Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36 |
| user\_account | Text | guwei |
| protocol | Text | HTTP |
| protocol\_version | Text | 1.1 |
| forwarded\_for | Text | - |
| response\_code | Text | 200 |
| client\_flag | Text | - |
| request\_method | Text | POST |
| http\_referer | Text | http://test.raysdata-lab.com |

## Nginx Access日志源格式配置

|  |  |
| --- | --- |
| **nginx\_access\_default\_log\_format** | **zeta\_log\_fields** |
| %s %cf %u [%t] &quot;%G %req %H/%Hv&quot; %res %b &quot;%hr&quot; &quot;%ua&quot; &quot;%f&quot; |  |
| %s | src\_address |
| %u | user\_account |
| %cf | client\_flag |
| %t | @timestamp |
| &quot; | " |
| %G | request\_method |
| %req | request |
| %H | protocol |
| %Hv | protocol\_version |
| &quot; | " |
| %res | response\_code |
| %b | bytes\_sent |
| &quot; | " |
| %hr; | http\_referer |
| &quot; | " |
| &quot; | " |
| %ua | user\_agent |
| &quot; | " |
| &quot; | " |
| %f | forwarded\_for |
| &quot; | " |

## Nginx Access日志解析方式



**GROK表达式：**

%{IP:src\_address}\s+%{DATA:client\_flag}\s+%{DATA:user\_account}\s+\[%{DATA:ts}\]\s+\"%{DATA:uri}\"\s+%{NUMBER:response\_code}\s+%{NUMBER:bytes\_sent}\s+\"%{DATA:http\_referer}\"\s+\"%{DATA:user\_agent}\"\s+\"%{DATA:forwarded\_for}\"



**GROK表达式：**

%{WORD:request\_method}\s+%{DATA:request}\s+%{WORD:protocol}\/%{ALL:protocol\_version}