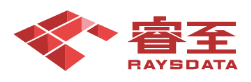
Apache日志模板 参照说明



北京睿至大数据有限公司2017年10月18日

目录

1 说明 3

1.1 Apache Access日志样例 3

1.2 Apache Access日志字段映射列表 3

1.3 Apache Access日志源格式配置 4

1.4 日志解析方式 4

2 其它 4

2.1 其它 4

2.2 略 4

# 说明

Apache 日志只包含 Apache Access 日志。

## Apache Access日志样例

218.19.140.242 - - [10/Dec/2010:09:31:17 +0800] \"GET /query/trendxml/district/todayreturn/month/2009-12-14/2010-12- 09/haizhu\_tianhe.xml HTTP/1.1\" 200 1933 \"-\" \"Mozilla/5.0 (Windows; U; Windows NT 5.1; zh-CN; rv:1.9.2.8) Gecko/20100722 Firefox/3.6.8 (.NET CLR 3.5.30729)\"

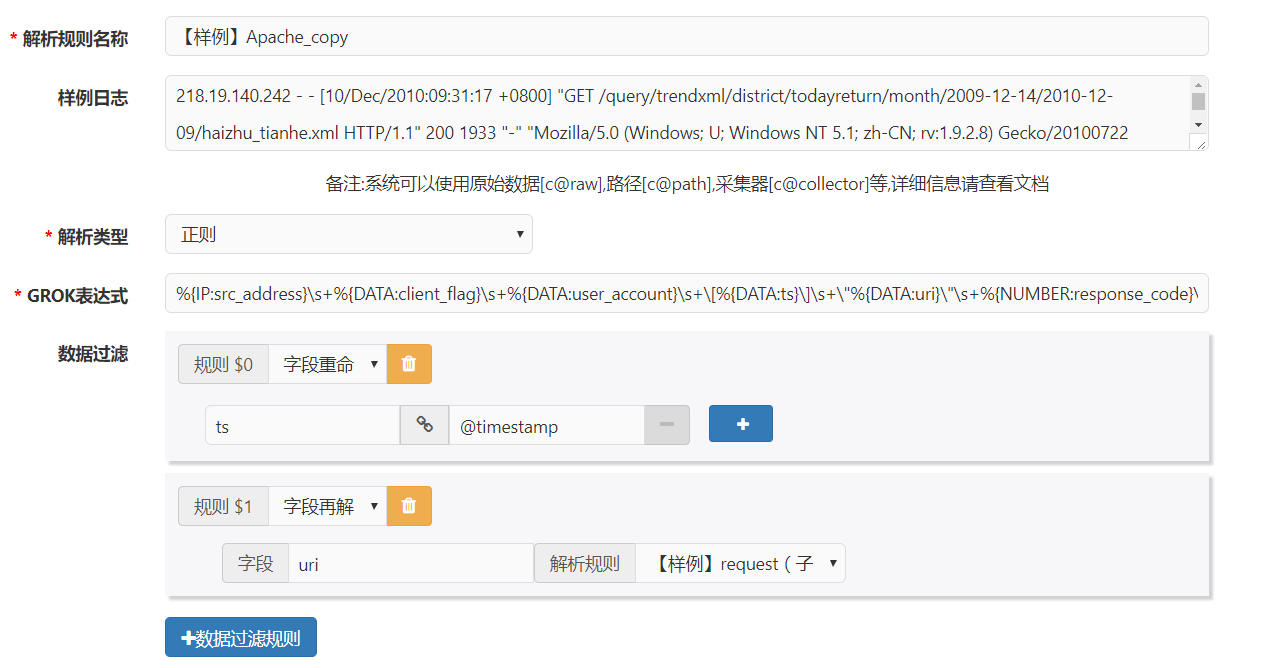
## Apache Access日志字段映射列表

|  |  |  |
| --- | --- | --- |
| **字段名** | **类型** | **内容** |
| @timestamp | Date | 10/Dec/2010:09:31:17 +0800 |
| client\_flag | Text | - |
| user\_account | Text | - |
| http\_referer | Text | - |
| request | Text | /query/trendxml/district/todayreturn/month/2009-12-14/2010-12-09/haizhu\_tianhe.xml |
| request\_method | Text | GET |
| protocol | Text | HTTP |
| protocol\_version | Text | 1.1 |
| user\_agent | Text | Mozilla/5.0 (Windows; U; Windows NT 5.1; zh-CN; rv:1.9.2.8) Gecko/20100722 Firefox/3.6.8 (.NET CLR3.5.30729) |
| response\_code | Text | 200 |
| src\_address | Text | 218.19.140.242 |
| bytes\_sent | Number | 1933 |

## Apache Access日志源格式配置

|  |  |
| --- | --- |
| **apache\_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; |  |
| %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 | response\_code |
| &quot; | " |

## 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}\"



**GROK表达式：**

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

# 其它

## 其它

## 略