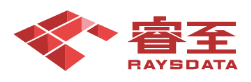
WebLogic日志模板参照说明



北京睿至大数据有限公司2017年10月31日

目录

说明 3

1.1 WebLogic Access日志样例 3

1.2 WebLogic Access日志字段映射列表 3

1.3 WebLogic Access日志源格式配置 4

1.4 WebLogic Access日志解析方式 4

2 WebLogic …… 4

2.1 其它 4

2.2 略 4

# 说明

WebLogic主要是 Access 日志

## WebLogic Access日志样例

192.168.1.1 - - [17/Mar/2012:16:23:05 +0800] "GET /JSLibrary/educational\_text.js HTTP/1.1" 200 39124

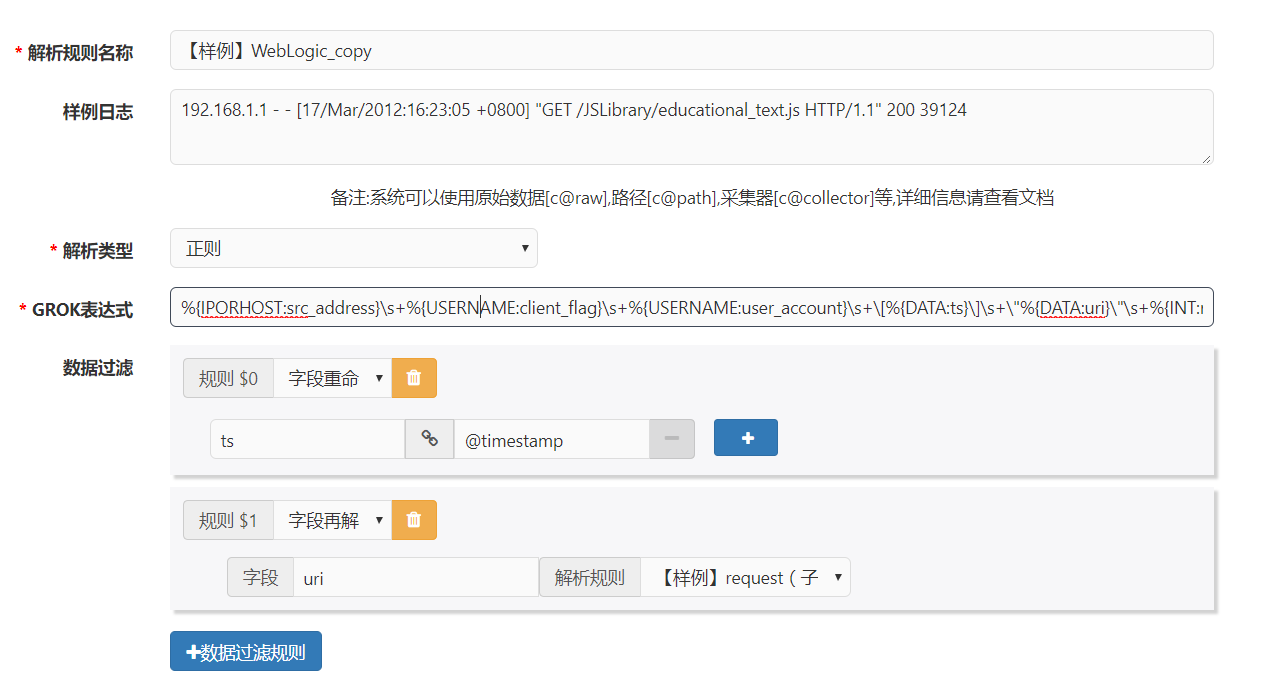
## WebLogic Access日志字段映射列表

|  |  |  |
| --- | --- | --- |
| **字段名** | **类型** | **内容** |
| @timestamp | Date | 17/Mar/2012:16:23:05 +0800 |
| request | Text | /JSLibrary/educational\_text.js |
| src\_address | Text | 192.168.1.1 |
| response\_code | Text | 200 |
| client\_flag | Text | - |
| protocol | Text | HTTP |
| protocol\_version | Text | 1.1 |
| request\_method | Text | GET |
| user\_account | Text | - |
| bytes\_sent | Number | 39124 |

## WebLogic Access日志源格式配置

|  |  |
| --- | --- |
| **WebLogic\_access\_default\_log\_format** | **zeta\_log\_fields** |
| %s %cf %u [%t] &quot;%G %req %H/%Hv&quot; %res %b |  |
| %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 |

## WebLogic Access日志解析方式



**GROK表达式：**

%{IPORHOST:src\_address}\s+%{USERNAME:client\_flag}\s+%{USERNAME:user\_account}\s+\[%{DATA:ts}\]\s+\"%{DATA:uri}\"\s+%{INT:response\_code}\s+%{INT:bytes\_sent}



**GROK表达式：**

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

# WebLogic ……

## 其它

## 略