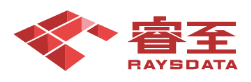
Tomcat 日志模板参照说明



北京睿至大数据有限公司2017年10月31日

目录

说明 3

1.1 Tomcat Catalina日志样例 3

1.2 Tomcat Catalina日志字段映射列表 4

1.3 Tomcat Catalina日志源格式配置 4

1.4 Tomcat Catalina日志解析方式 4

2 Tomcat 主机日志 5

2.1 Tomcat 主机日志样例 5

2.2 Tomcat 主机日志字段映射列表 5

2.3 Tomcat 主机日志源格式配置 8

2.4 Tomcat 主机日志解析方式 8

3 Tomcat 主机Access日志 8

3.1 Tomcat 主机Access日志样例 8

3.2 Tomcat 主机Access日志字段映射列表 8

3.3 Tomcat 主机Access日志源格式配置 9

3.4 Tomcat 主机Access日志解析方式 9

# 说明

Tomcat 相关日志包含以下几种：

1. Tomcat Catalina
2. Tomcat 主机
3. Tomcat 主机 Access

## Tomcat Catalina日志样例

03-Jul-2017 11:17:05.322 WARNING [ContainerBackgroundProcessor[StandardEngine[Catalina]]] org.apache.catalina.loader.WebappClassLoaderBase.clearReferencesThreads The web application [ELK-Web] appears to have started a thread named [qbScheduler-1] but has failed to stop it. This is very likely to create a memory leak. Stack trace of thread: sun.misc.Unsafe.park(Native Method) java.util.concurrent.locks.LockSupport.parkNanos(LockSupport.java:215) java.util.concurrent.locks.AbstractQueuedSynchronizer$ConditionObject.awaitNanos(AbstractQueuedSynchronizer.java:207 8) java.util.concurrent.ScheduledThreadPoolExecutor$DelayedWorkQueue.take(ScheduledThreadPoolExecutor.java:1093) java.util.concurrent.ScheduledThreadPoolExecutor$DelayedWorkQueue.take(ScheduledThreadPoolExecutor.java:809) java.util.concurrent.ThreadPoolExecutor.getTask(ThreadPoolExecutor.java:1067) java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1127) java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:617) java.lang.Thread.run(Thread.java:745)

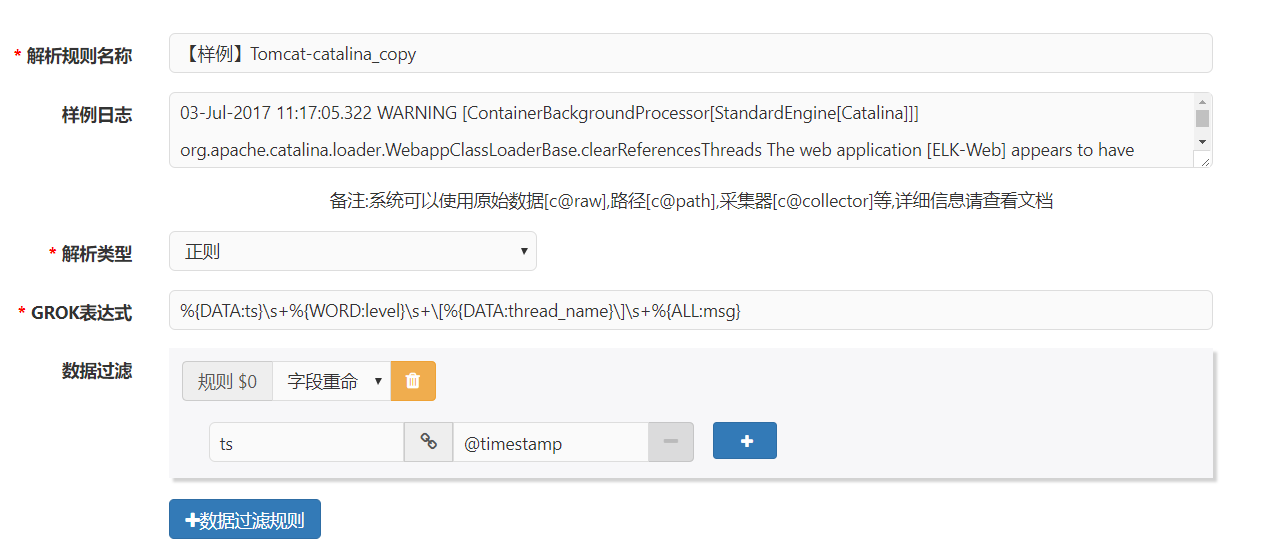
## Tomcat Catalina日志字段映射列表

|  |  |  |
| --- | --- | --- |
| **字段名** | **类型** | **内容** |
| @timestamp | Date | Mon Jul 03 11:17:05 CST 2017 |
| msg | Text | org.apache.catalina.loader.WebappClassLoaderBase.clearReferencesThreads The web application [ELK-Web] appears to have started a thread n java.util.concurrent.locks.LockSupport.parkNanos(LockSupport.java:215) java.util.concurrent.locks.AbstractQueuedSynchronizer DelayedWorkQueue.take(ScheduledThreadPoolExecutor.java:1093) java.util.concurrent.ScheduledThreadPoolExecutor  Worker.run(ThreadPoolExecutor.java:617) java.lang.Thread.run(Thread.java:745) |
| level | Text | WARNING |
| thread\_name | Text | ContainerBackgroundProcessor[StandardEngine[Catalina]] |

## Tomcat Catalina日志源格式配置

|  |  |
| --- | --- |
| **tomcat\_catalina\_default\_log\_format** | **zeta\_log\_fields** |
| %t %l %tn %m |  |
| %t | @timestamp |
| %l | thread\_name |
| %tn | function |
| %m | msg |

## Tomcat Catalina日志解析方式



**GROK表达式：**

%{DATA:ts}\s+%{WORD:level}\s+\[%{DATA:thread\_name}\]\s+%{ALL:msg}

# Tomcat 主机日志

## Tomcat 主机日志样例

13-Jul-2017 10:00:03.237 SEVERE [http-nio-8082-exec-3] org.apache.catalina.core.StandardWrapperValve.invoke Servlet.service() for servlet [springServlet] in context with path [/opt-web-api] threw exception [Request processing failed; nested exception is java.lang.NumberFormatException: For input string: ""] with root cause

java.lang.NumberFormatException: For input string: ""

at java.lang.NumberFormatException.forInputString(NumberFormatException.java:65)

at java.lang.Integer.parseInt(Integer.java:592)

at java.lang.Integer.parseInt(Integer.java:615)

……

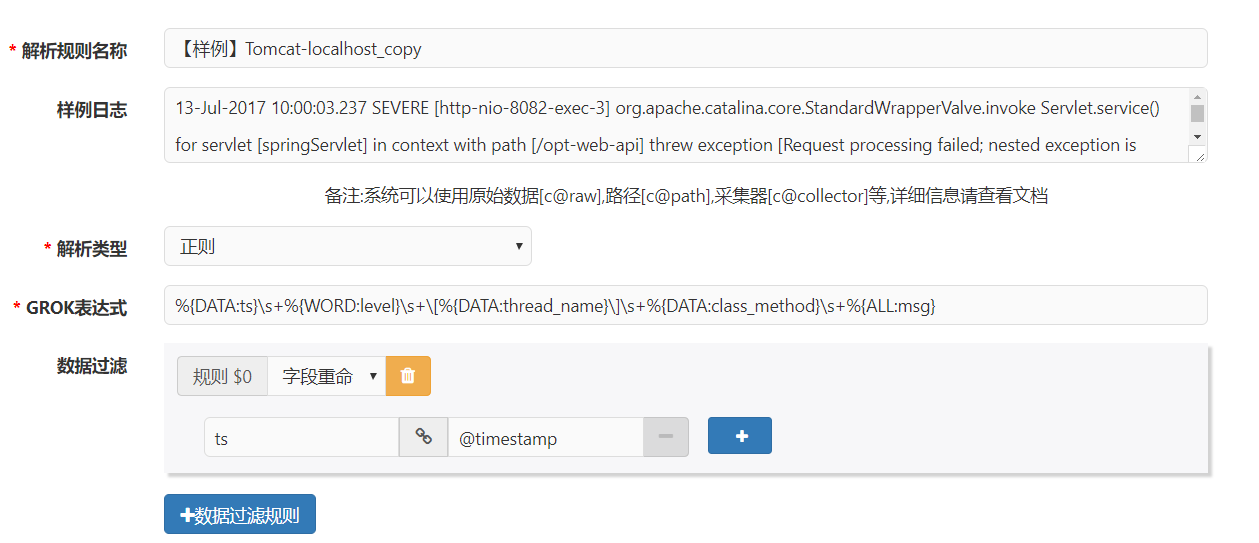
## Tomcat 主机日志字段映射列表

|  |  |  |
| --- | --- | --- |
| **字段名** | **类型** | **内容** |
| @timestamp | Date | Mon Jul 03 11:17:05 CST 2017 |
| class\_method | Text | org.apache.catalina.core.StandardWrapperValve.invoke |
| msg | Text | Servlet.service() for servlet [springServlet] in context with path [/opt-web-api] threw exception [Request processing failed; nested exception is java.lang.NumberFormatException: For input string: ""] with root cause java.lang.NumberFormatException: For input string: "" at java.lang.NumberFormatException.forInputString(NumberFormatException.java:65) at java.lang.Integer.parseInt(Integer.java:592) at java.lang.Integer.parseInt(Integer.java:615) …… |
| level | Text | WARNING |
| thread\_name | Text | ContainerBackgroundProcessor[StandardEngine[Catalina]] |

## Tomcat 主机日志源格式配置

|  |  |
| --- | --- |
| **tomcat\_localhost\_default\_log\_format** | **zeta\_log\_fields** |
| %t %l [%tn] %cm %m |  |
| %t | @timestamp |
| %l | thread\_name |
| %tn | function |
| %cm | class\_method |
| %m | msg |

## Tomcat 主机日志解析方式



**GROK表达式：**

%{DATA:ts}\s+%{WORD:level}\s+\[%{DATA:thread\_name}\]\s+%{DATA:class\_method}\s+%{ALL:msg}

# Tomcat 主机Access日志

## Tomcat 主机Access日志样例

127.0.0.1 - - [09/Oct/2017:10:34:55 +0800] "POST /opt-web-api/v1/cli-20170814/database/\_search HTTP/1.0" 404 992

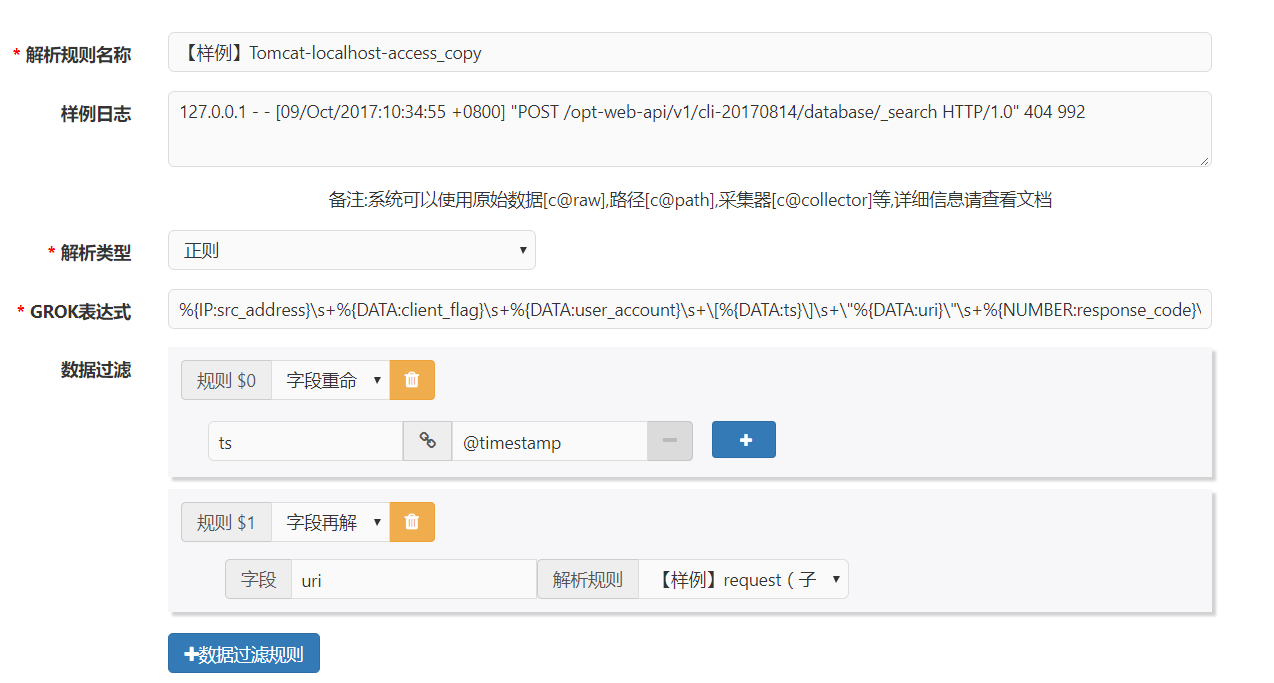
## Tomcat 主机Access日志字段映射列表

|  |  |  |
| --- | --- | --- |
| **字段名** | **类型** | **内容** |
| @timestamp | Date | 09/Oct/2017:10:34:55 +0800 |
| request | Text | /opt-web-api/v1/cli-20170814/database/\_search |
| src\_address | Text | 127.0.0.1 |
| response\_code | Text | 404 |
| client\_flag | Text | - |
| https | Text | HTTP/1.0 |
| request\_method | Text | POST |
| user\_account | Text | - |
| bytes\_sent | Number | 992 |

## Tomcat 主机Access日志源格式配置

|  |  |
| --- | --- |
| **tomcat\_localhost\_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 |

## Tomcat 主机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}



**GROK表达式：**

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