Zabbix监控日志文件

Zabbix监控日志文件

操作环境CenOS6.8，软件版本zabbix3.0
前提条件：Zabbix-Agent必须运行，且工作模式为主动模式。

监控日志Key

首先要了解 key

```
log[ file  ,<regexp>,<encoding>,<maxlines>,<mode>,<output>]
```

file ：文件名，写绝对路径
regexp： 要匹配内容的正则表达式，或者直接写你要检索的内容也可以，例如我想检索带 session 关键词的记录
encoding： 编码相关，留空即可
maxlines ：一次性最多提交多少行，这个参数覆盖配置文件 zabbxi_agentd.conf 中的 MaxLinesPerSecond ，我们也可以留空
mode： 默认是all，也可以是skip，skip会跳过老数据
output： 输出给 zabbix server 的数据。可以是\1、\2一直\9，\1表示第一个正则表达式匹配出得内容，\2表示第二个正则表达式匹配错的内容。

备注：推荐大家使用第二个参数，指定监控的具体内容来监控。如果不加指定内容监控，就会监控所有信息，这样会给服务器端带来很大负担。

访问日志文件权限配置

给日志文件加上读取权限

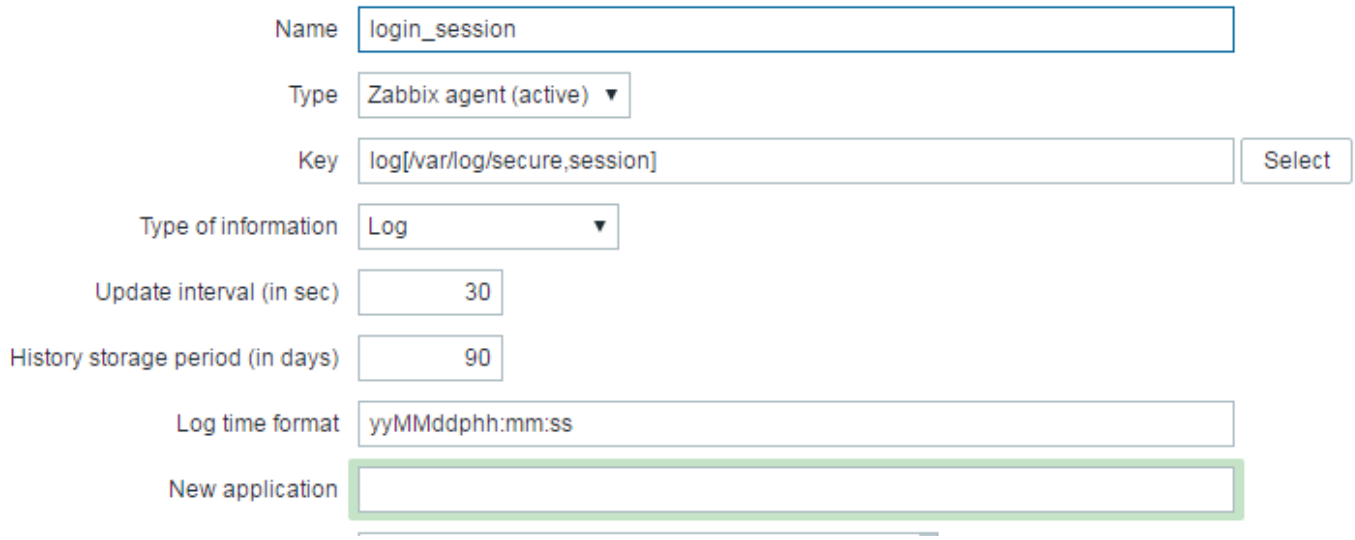
```
$ chown zabbix.root /var/log/secure
$ ll /var/log/secure
-rw------- 1 zabbix root 5273 Jun 22 12:14 /var/log/secure
```

如果权限给的不到位， zabbix agent 日志有类似如下报错：

```
58014:20170622:121346.662 using configuration file: /etc/zabbix/zabbix_agentd.conf
58014:20170622:121346.709 agent #0 started [main process]
58015:20170622:121346.711 agent #1 started [collector]
58016:20170622:121346.712 agent #2 started [active checks #1]
58016:20170622:121446.038 active check "log[/var/log/secure,session]" is not supported: Cannot open file
"/var/log/secure": [13] Permission denied
```

Zabbix配置

Host >>目标主机>> item >> create item ，如图：



zabbix日志监控
说明：

1. type 必须选择 zabbix agent（active），因为数据是 zabbix 被监控的主动提交给 server
2. log time format：yyMMddphh:mm:ss ，y表示年、M表示月、d表示日、p和:一个占位符，h表示小时，m表示分钟，s表示秒。

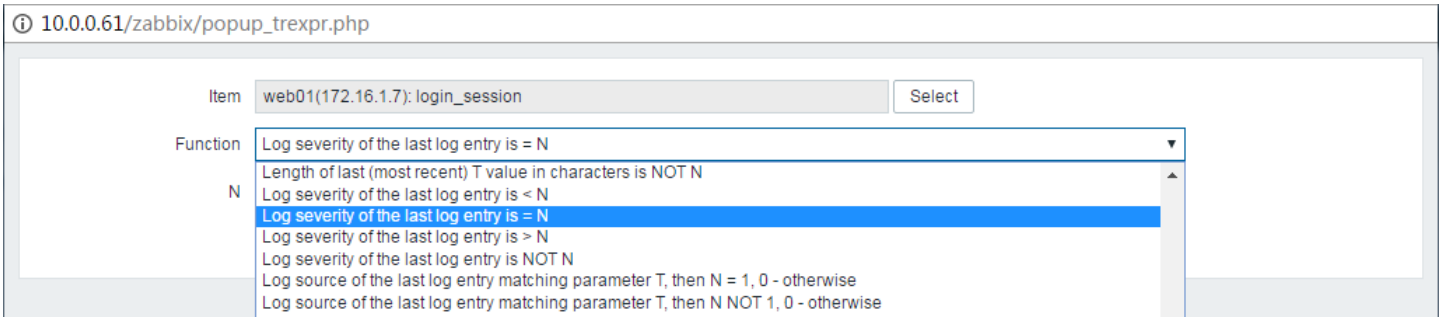
Zabbix监控日志查看

Monitoring >> lastest Data ,找到我们刚刚建立的这个 item ，点击右侧的 history ，就可以看到这样的内容了。

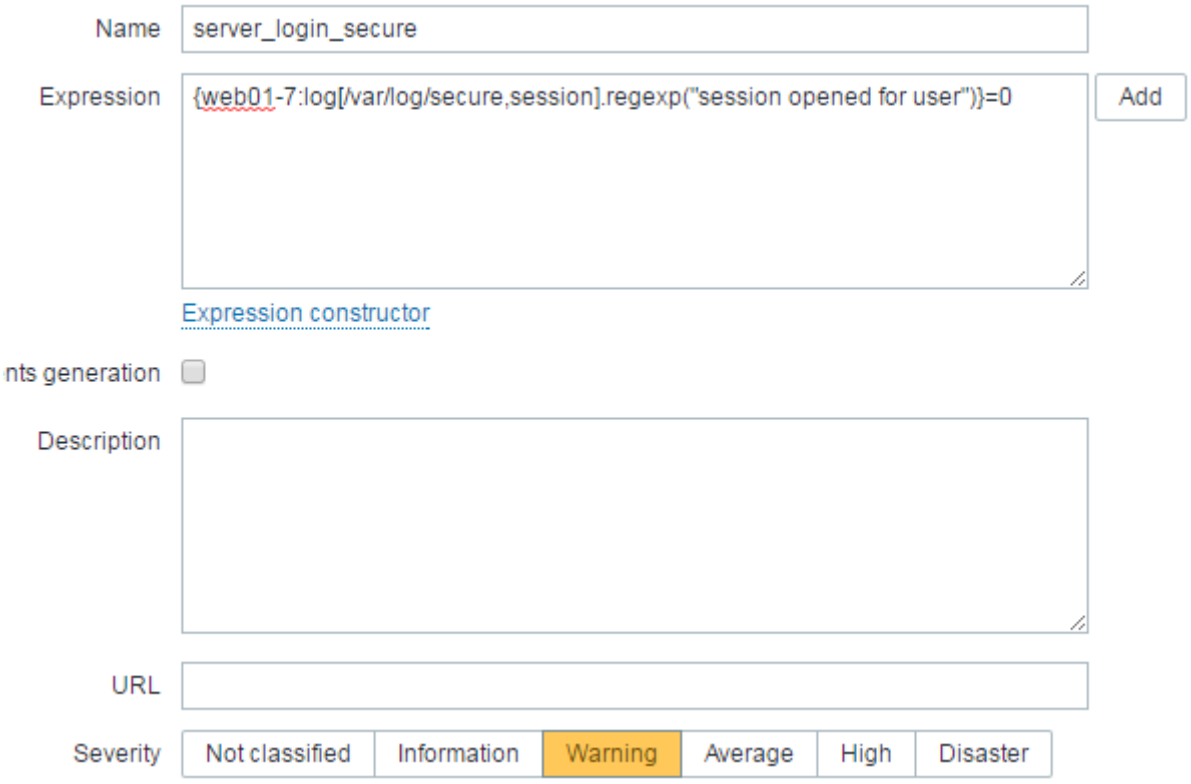
Timestamp	Local time	Value
2017-06-27 22:44:06		Jun 22 12:26:57 web01-7 sshd[58183]: pam_unix(sshd:session): session opened for user root by (uid=0)
2017-06-27 22:43:06		Jun 22 12:25:46 web01-7 sshd[58163]: pam_unix(sshd:session): session opened for user root by (uid=0)
2017-06-27 22:42:36		Jun 22 12:25:31 web01-7 sshd[58092]: pam_unix(sshd:session): session closed for user root
2017-06-27 22:42:36		Jun 22 12:25:30 web01-7 sshd[58021]: pam_unix(sshd:session): session closed for user root

日志监控触发器的设置

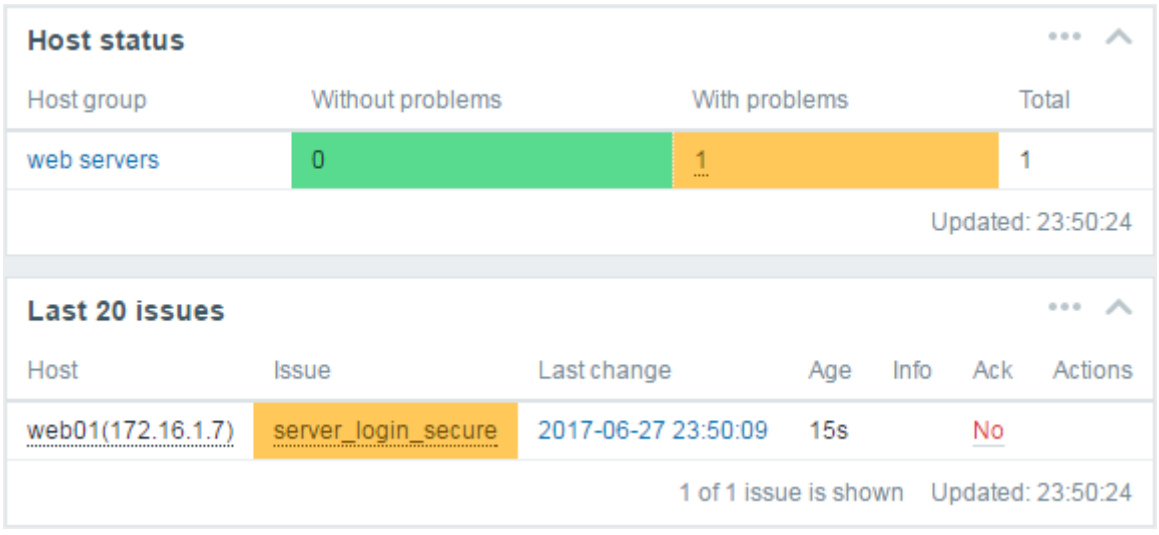
选择日志的 Item ,如图：



配置 Trigger 的值，如图：



如果日志中出现”session opened for user”字符串，将会触发 `Trigger` ，从而发生告警。如图：



Log与Logrt区别

```
key:
log[file,<regexp>,<encoding>,<maxlines>,<mode>,<output>]
logrt[file_regexp,<regexp>,<encoding>,<maxlines>,<mode>,<output>]
```

`log` 与 `logrt` 区别在于第一个参数不一样， `logrt` 的第一个参数可以使用正则表达式。针对日志回滚用得，例如我们每天都切割 `nginx` 日志，日志名位 `www.etiantian.org_2017-01-01.log、www.etiantian.ort_2017-01-02.log` 等等，使用 `log` 肯定不合适，如果文件名使用正则，那么新增的日志文件会立即加入监控。
备注：不管新日志、老日志，只要他们有变更，zabbix都会监控。