

某局点CAS CVM出现“主机日志分区5分钟内增长超过1MB，实际增长11MB”告警的经验案例

李树兵 2019-09-17 发表

组网及说明

略。

问题描述

某局点使用CAS配合OneStor存储的融合部署环境，主机多次收到“主机日志5分钟内增长超过1MB，实际增长10MB”的告警信息。



告警	主机名称	告警内容	告警时间	清除时间
告警	主机A	主机日志分区5分钟内增长超过1MB，实际增长11MB。	2019-08-29 15:35:39	2019-08-29 15:35:39
告警	主机A	主机日志分区5分钟内增长超过1MB，实际增长11MB。	2019-08-29 15:15:15	2019-08-29 15:15:08
告警	主机A	主机日志分区5分钟内增长超过1MB，实际增长11MB。	2019-08-29 15:09:10	2019-08-29 15:09:12
告警	主机A	主机日志分区5分钟内增长超过1MB，实际增长11MB。	2019-08-29 15:08:41	2019-08-29 15:08:40
告警	主机A	主机日志分区5分钟内增长超过1MB，实际增长11MB。	2019-08-29 15:07:40	2019-08-29 15:03:40
告警	主机A	主机日志分区5分钟内增长超过1MB，实际增长11MB。	2019-08-29 14:36:38	2019-08-29 14:32:44
告警	主机A	主机日志分区5分钟内增长超过1MB，实际增长11MB。	2019-08-29 14:31:44	2019-08-29 14:27:40
告警	主机A	主机日志分区5分钟内增长超过1MB，实际增长11MB。	2019-08-29 14:28:09	2019-08-29 14:24:07
告警	主机A	主机日志分区5分钟内增长超过1MB，实际增长11MB。	2019-08-29 14:25:09	2019-08-29 14:21:12
告警	主机A	主机日志分区5分钟内增长超过1MB，实际增长11MB。	2019-08-29 14:05:38	2019-08-29 14:01:39

过程分析

CAS中默认会监测系统日志的增长速度，如果增长速率比较高的话就会产生此告警，那么具体是哪些日志增长过快，这些日志增长是否正常，系统并没有记录，需要手动去收集这些信息。

当频繁出现这种告警的时候可以通过如下方法查看：

第一步：将附件下载下来解压，解压出来是一个python脚本文件，此脚本的作用是创建一个mnt/logininfo的目录，每隔300S（即5分钟）获取当前系统的时间，以及df -Tm的信息，还有就是使用du -ah /var/log，获取/var/log目录下所有文件的大小信息，并将每一次获取的数据生成一个文件。可以选择使用winscp等sftp的客户端软件连接到CVM主机中，然后将此文件上传到云主机后台。

第二步：通过命令python logininfo20190917.py 来执行，之后系统会执行这个脚本文件，因为每隔5分钟执行一次，如果想要让此脚本在后台运行，可以在后面加一个“&”字符。这里配置在前台运行。

```
root@cvm:~# python logininfo20190917.py
这是第 1 次运行
```

第二步：如果需要其他的操作可以再新建一个会话连接，保持此会话不懂，待出现告警之后去收集和告警时间相近的这几个日志文件，文件不多的话可以将这个目录全部打包发过来。

```
root@cvm:~# cd /mnt/logininfo
root@cvm:/mnt/logininfo# ll
total 600
drwxr-xr-x 2 root root 4096 Sep 17 19:01 ./
drwxr-xr-x 6 root root 4096 Aug 29 21:45 ../
-rw-r--r-- 1 root root 20 Aug 29 21:41 20190829_214144_9771.log
-rw-r--r-- 1 root root 81098 Aug 30 10:59 20190830-10-59-11.log
-rw-r--r-- 1 root root 81098 Aug 30 10:59 20190830-10-59-12.log
-rw-r--r-- 1 root root 82862 Sep 17 18:57 20190917-18-57-26.log
-rw-r--r-- 1 root root 82862 Sep 17 18:58 20190917-18-58-36.log
-rw-r--r-- 1 root root 82862 Sep 17 19:00 20190917-19-00-05.log
-rw-r--r-- 1 root root 82862 Sep 17 19:00 20190917-19-00-54.log
-rw-r--r-- 1 root root 82862 Sep 17 19:01 20190917-19-01-48.log
-rw-r--r-- 1 root root 40 Aug 29 21:44 .log
-rw-r--r-- 1 root root 1772 Aug 29 21:44 -logininfo.txt
root@cvm:/mnt/logininfo# ls -lh
total 588K
-rw-r--r-- 1 root root 20 Aug 29 21:41 20190829_214144_9771.log
-rw-r--r-- 1 root root 80K Aug 30 10:59 20190830-10-59-11.log
-rw-r--r-- 1 root root 80K Aug 30 10:59 20190830-10-59-12.log
-rw-r--r-- 1 root root 81K Sep 17 18:57 20190917-18-57-26.log
-rw-r--r-- 1 root root 81K Sep 17 18:58 20190917-18-58-36.log
-rw-r--r-- 1 root root 81K Sep 17 19:00 20190917-19-00-05.log
-rw-r--r-- 1 root root 81K Sep 17 19:00 20190917-19-00-54.log
-rw-r--r-- 1 root root 81K Sep 17 19:01 20190917-19-01-48.log
-rw-r--r-- 1 root root 1.8K Aug 29 21:44 -logininfo.txt
root@cvm:/mnt/logininfo#
```

第三步：找和出现告警相近的这两个日志文件，然后通过Beyond Compare软件对比两个文件的区别（Beyond Compare软件需自己到网上搜索下载安装），通过这个软件就可以对比这5分钟内哪些文件的大小变化，以及变化多少，找那些相差比较大的即是日志增长比较多的文件。

2019/09/17 10:01:40 62.062 字节 警告 - 已 + 添加 + 删除					2019/09/17 10:01:40 62.062 字节 警告 - 已 + 添加 + 删除				
1	log	log	12 10:01:40 537 2019	7 10:01	1	log	log	12 10:01:40 537 2019	7 10:01
2	fileinfo	err	1877036 1341361	438801 708 /usr/	2	fileinfo	err	1877036 1341361	438801 708 /usr/
3	fileinfo	usr/bin/can_hu/typs_auditd.log		1 10:01	3	fileinfo	usr/bin/can_hu/typs_auditd.log		1 10:01
4	3.10	usr/bin/can_hu		1 10:01	4	3.10	usr/bin/can_hu		1 10:01
5	3.10	usr/bin/canlog/can_device_config.log		1 10:01	5	3.10	usr/bin/canlog/can_device_config.log		1 10:01
6	300K	usr/bin/canlog/can_device1.log		1 10:01	6	300K	usr/bin/canlog/can_device1.log		1 10:01

第四步：查看具体的日志文件，看日志内容是否正常，如果正常的话可以忽略此告警。

解决方法

判断增长日志是否正常，如果正常可以选择屏蔽此告警。

类别	增长状态	告警来源	类型	告警信息	最新告警时间	上次告警时间	屏蔽次数
重要	未确认	主机cshoads7192.168.127.65	主机资源告警	主机磁盘分区"/usr/bin/can_hu/typs_auditd.log"当前使用量为71%...	2019-08-30 11:51:43	2019-08-29 11:31:52	34886
次要	未确认	主机com7192.168.127.65	其他部署告警	主机磁盘分区"/usr/bin/can_hu/typs_auditd.log"当前使用量为71%...	2019-08-30 11:51:17	2019-08-30 11:47:47	16
重要	未确认	主机com7192.168.127.65	其他部署告警	主机磁盘分区"/usr/bin/can_hu/typs_auditd.log"当前使用量为71%...	2019-08-30 11:51:12	2019-08-28 08:20:45	2772
次要	未确认	主机com7192.168.127.65	其他部署告警	主机磁盘分区"/usr/bin/can_hu/typs_auditd.log"当前使用量为71%...	2019-08-30 11:50:53	2019-08-30 01:42:48	1219
重要	未确认	主机com7192.168.127.65	主机资源告警	主机磁盘分区"/usr/bin/can_hu/typs_auditd.log"当前使用量为71%...	2019-08-30 11:50:47	2019-07-07 18:55:11	28638
重要	未确认	主机com7192.168.127.65	主机资源告警	主机磁盘分区"/usr/bin/can_hu/typs_auditd.log"当前使用量为71%...	2019-08-30 11:50:47	2019-08-03 21:43:40	48982
次要	未确认	主机com7192.168.127.65	其他部署告警	主机磁盘分区"/usr/bin/can_hu/typs_auditd.log"当前使用量为71%...	2019-08-30 11:50:02	2019-08-30 10:48:30	56
重要	未确认	主机com7192.168.127.65	其他部署告警	主机磁盘分区"/usr/bin/can_hu/typs_auditd.log"当前使用量为71%...	2019-08-30 11:49:47	2019-07-25 18:54:39	48128
重要	未确认	主机com7192.168.127.65	其他部署告警	主机磁盘分区"/usr/bin/can_hu/typs_auditd.log"当前使用量为71%...	2019-08-30 11:49:33	2019-08-30 10:20:56	11286
重要	未确认	主机com7192.168.127.65	其他部署告警	主机磁盘分区"/usr/bin/can_hu/typs_auditd.log"当前使用量为71%...	2019-08-30 11:48:43	2019-08-30 11:47:03	79144
重要	未确认	主机com7192.168.127.65	其他部署告警	主机磁盘分区"/usr/bin/can_hu/typs_auditd.log"当前使用量为71%...	2019-08-30 11:47:03	2019-07-24 18:24:48	20514
重要	未确认	主机com7192.168.127.65	其他部署告警	主机磁盘分区"/usr/bin/can_hu/typs_auditd.log"当前使用量为71%...	2019-08-30 11:46:33	2019-08-21 20:26:17	4879
重要	已确认	主机com7192.168.127.65	其他部署告警	主机磁盘分区"/usr/bin/can_hu/typs_auditd.log"当前使用量为71%...	2019-08-30 11:45:17	2019-08-30 11:41:57	18
次要	已确认	主机com7192.168.127.65	其他部署告警	主机磁盘分区"/usr/bin/can_hu/typs_auditd.log"当前使用量为71%...	2019-08-30 11:36:47	2019-08-30 11:32:47	18
次要	已确认	主机com7192.168.127.65	其他部署告警	主机磁盘分区"/usr/bin/can_hu/typs_auditd.log"当前使用量为71%...	2019-08-30 11:27:17	2019-08-30 11:23:17	18
次要	已确认	主机com7192.168.127.65	其他部署告警	主机磁盘分区"/usr/bin/can_hu/typs_auditd.log"当前使用量为71%...	2019-08-30 11:21:16	2019-08-30 11:17:17	18
次要	已确认	主机com7192.168.127.65	其他部署告警	主机磁盘分区"/usr/bin/can_hu/typs_auditd.log"当前使用量为71%...	2019-08-30 11:11:47	2019-08-30 11:07:47	18
次要	已确认	主机com7192.168.127.65	其他部署告警	主机磁盘分区"/usr/bin/can_hu/typs_auditd.log"当前使用量为71%...	2019-08-30 11:05:17	2019-08-30 11:01:17	18
次要	已确认	主机com7192.168.127.65	其他部署告警	主机磁盘分区"/usr/bin/can_hu/typs_auditd.log"当前使用量为71%...	2019-08-30 11:04:01	2019-08-30 11:00:01	18
次要	已确认	主机com7192.168.127.65	其他部署告警	主机磁盘分区"/usr/bin/can_hu/typs_auditd.log"当前使用量为71%...	2019-08-30 10:56:47	2019-08-30 10:52:47	18
次要	已确认	主机com7192.168.127.65	其他部署告警	主机磁盘分区"/usr/bin/can_hu/typs_auditd.log"当前使用量为71%...	2019-08-30 10:47:17	2019-08-30 10:43:16	18
次要	已确认	主机com7192.168.127.65	其他部署告警	主机磁盘分区"/usr/bin/can_hu/typs_auditd.log"当前使用量为71%...	2019-08-30 10:41:16	2019-08-30 10:37:16	18
提示	未确认	C:\Program Files\...	其他部署告警	C:\Program Files\...	2019-08-30 10:33:01	2019-08-07 10:31:40	4880

附件下载：loginfo20190917.rar