

设备审计不到日志时查看后台进程状态提示audit_server状态异常

设备审计不到日志，进入/home/audit目录下，使用./AutoCheckSystemTest命令查看系统关键进程状态，提示如下图

```
78.44.16.235 (1) x
[root@localhost audit]# ./AutoCheckSystemTest
[2017-05-18 15:12:25]: *****
[2017-05-18 15:12:25]: Start to check System environment Now.....
[2017-05-18 15:12:25]: *****
[2017-05-18 15:12:26]: *****
[2017-05-18 15:12:26]: Start to Check Process environment.....
[2017-05-18 15:12:27]: Start check the network bridge .....
[2017-05-18 15:12:27]: [br0] create the network bridge is success. [OK]
[2017-05-18 15:12:27]: *****
[2017-05-18 15:12:28]: Start to check the MySQL environment.....
[2017-05-18 15:12:29]: [Mysql] MySQL is normal running now.... [OK]
[2017-05-18 15:12:29]: *****
[2017-05-18 15:12:30]: Start to check the Tomcat service status.....
[2017-05-18 15:12:30]: [Tomcat]Tomcat is running OK now.. [OK]
[2017-05-18 15:12:30]: *****
[2017-05-18 15:12:31]: Start to check the audit_engine running status.....
[2017-05-18 15:12:31]: check the audit_engine. [OK]
[2017-05-18 15:12:31]: Starting audit_engine.. [OK]
[2017-05-18 15:12:31]: [audit_engine]the environment of the audit_engine is normal.....
[2017-05-18 15:12:31]: ***** [OK]
[2017-05-18 15:12:32]: Start to check the act_engine running status.....
[2017-05-18 15:12:32]: check the act_engine. [OK]
[2017-05-18 15:12:32]: Starting act_engine... [OK]
[2017-05-18 15:12:32]: [act_engine]the act_engine is normal running.... [OK]
[2017-05-18 15:12:33]: Start to check the connect module status.....
[2017-05-18 15:12:33]: Check the monitor. [OK]
[2017-05-18 15:12:33]: Starting monitor... [OK]
[2017-05-18 15:12:33]: [monitor]the network connected is ok..... [OK]
[2017-05-18 15:12:33]: *****
[2017-05-18 15:12:34]: Start to check the drives of the capture packet.....
[2017-05-18 15:12:34]: Check the myhook. [OK]
[2017-05-18 15:12:34]: Starting myhook... [OK]
[2017-05-18 15:12:34]: [myhook]the capture packet module start sucess. [OK]
[2017-05-18 15:12:34]: *****
[2017-05-18 15:12:35]: Start to check the audit_server environment.....
[2017-05-18 15:12:35]: [audit_server]audit_server is exception!! you may restart it now.... [FAILED]
[2017-05-18 15:12:35]: *****
[2017-05-18 15:12:35]: chcek the [audit_server]exception, please recheck ..
[root@localhost audit]#
```

截图表明audit_server进程有问题，输入./audit_server命令运行此进程查看报错信息如下

```
[root@localhost audit]# ./audit_server -p
./audit_server: error while loading shared libraries: libsybdb.so.5: cannot open shared object file: No such file or directory
[root@localhost audit]#
```

系统提示找不到libstbdb. so. 5文件，无法启动进程，找到缺失文件，上传到/usr/lib目录下；

在/home/audit/目录下输入sh kill. sh和sh audit. sh，清除缓存重启进程，再次输入./audit_server查看状态为running，使用./AutoCheckSystemTest命令查看系统关键进程状态是否正常。