asan

GCC 4.8以上版本使用ASAN时不需要安装第三方库，通过在编译时指定编译CFLAGS即可打开开关

Gcc编译选项

1.在CFLAGS和CXXFLAGS中加入以下

- -fsanitize=address：开启内存越界检测
- -fsanitize-recover=address：一般后台程序为保证稳定性，不能遇到错误就简单退出，而是继续运行，采用该选项支持内存出错之后程序继续运行，需要叠加设置ASAN_OPTIONS=halt_on_error=0才会生效；若未设置此选项，则内存出错即报错退出
- -fno-omit-frame-pointer：去使能栈溢出保护

2.在LDFLAGS中加入-lasan

删除tcmalloc和jcmalloc

CONFIGS('baidu/third-party/tcmalloc@tcmalloc_V2.7.0.7_GCC820_4U3_K3_GEN_PD_BL@git_tag', Libraries(“”))

编译

直接编译就行

ASAN_OPTIONS设置

需要在环境中export如下声明

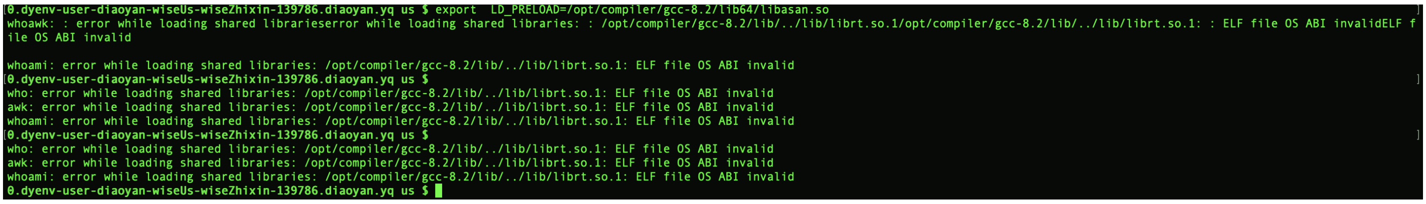
export ASAN_OPTIONS=halt_on_error=0:use_sigaltstack=0:detect_leaks=1:malloc_context_size=15:log_path=/home/xos/asan.log:suppressions=$SUPP_FILE

- ASAN_OPTIONS是Address-Sanitizier的运行选项环境变量。
- # halt_on_error=0：检测内存错误后继续运行
- # detect_leaks=1:使能内存泄露检测
- # malloc_context_size=15：内存错误发生时，显示的调用栈层数为15
- # log_path=/home/xos/asan.log:内存检查问题日志存放文件路径
- # suppressions=$SUPP_FILE:屏蔽打印某些内存错误

运行

LD_PRELOAD=/opt/compiler/gcc-8.2/lib64/libasan.so /home/work/search/us/bin//us -d /home/work/search/us/ -f /conf/us.conf -f /conf/server.conf -f/conf/us_left_stgy.conf -f /conf/us_zhixin.conf -f/conf/us_right_stgy.conf &

其实默认应该export LD_PRELOAD=/opt/compiler/gcc-8.2/lib64/libasan.so ,然后正常启动us就可以,但是我直接export,环境报错,应该是系统库版本太低



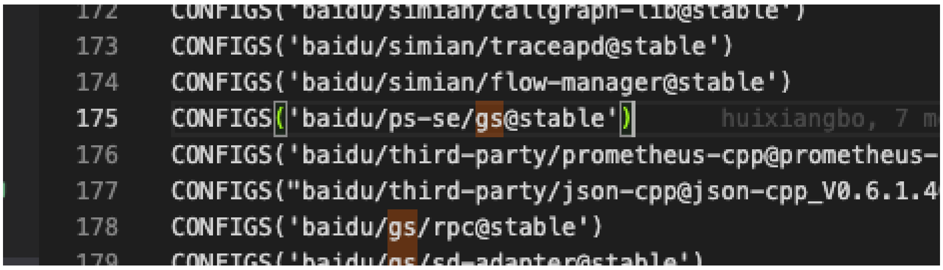
```
0.dyenv-user-diaoyan-wiseUs-wiseZhixin-139786.diaoyan.yq us $ export  LD_PRELOAD=/opt/compiler/gcc-8.2/lib64/libasan.so
whoawk: : error while loading shared librarieserror while loading shared libraries: : /opt/compiler/gcc-8.2/lib/../lib/librt.so.1/opt/compiler/gcc-8.2/lib/../lib/librt.so.1: : ELF file OS ABI invalidELF f
ile OS ABI invalid

whoami: error while loading shared libraries: /opt/compiler/gcc-8.2/lib/../lib/librt.so.1: ELF file OS ABI invalid
0.dyenv-user-diaoyan-wiseUs-wiseZhixin-139786.diaoyan.yq us $
who: error while loading shared libraries: /opt/compiler/gcc-8.2/lib/../lib/librt.so.1: ELF file OS ABI invalid
awk: error while loading shared libraries: /opt/compiler/gcc-8.2/lib/../lib/librt.so.1: ELF file OS ABI invalid
whoami: error while loading shared libraries: /opt/compiler/gcc-8.2/lib/../lib/librt.so.1: ELF file OS ABI invalid
0.dyenv-user-diaoyan-wiseUs-wiseZhixin-139786.diaoyan.yq us $
who: error while loading shared libraries: /opt/compiler/gcc-8.2/lib/../lib/librt.so.1: ELF file OS ABI invalid
awk: error while loading shared libraries: /opt/compiler/gcc-8.2/lib/../lib/librt.so.1: ELF file OS ABI invalid
whoami: error while loading shared libraries: /opt/compiler/gcc-8.2/lib/../lib/librt.so.1: ELF file OS ABI invalid
0.dyenv-user-diaoyan-wiseUs-wiseZhixin-139786.diaoyan.yq us $
```

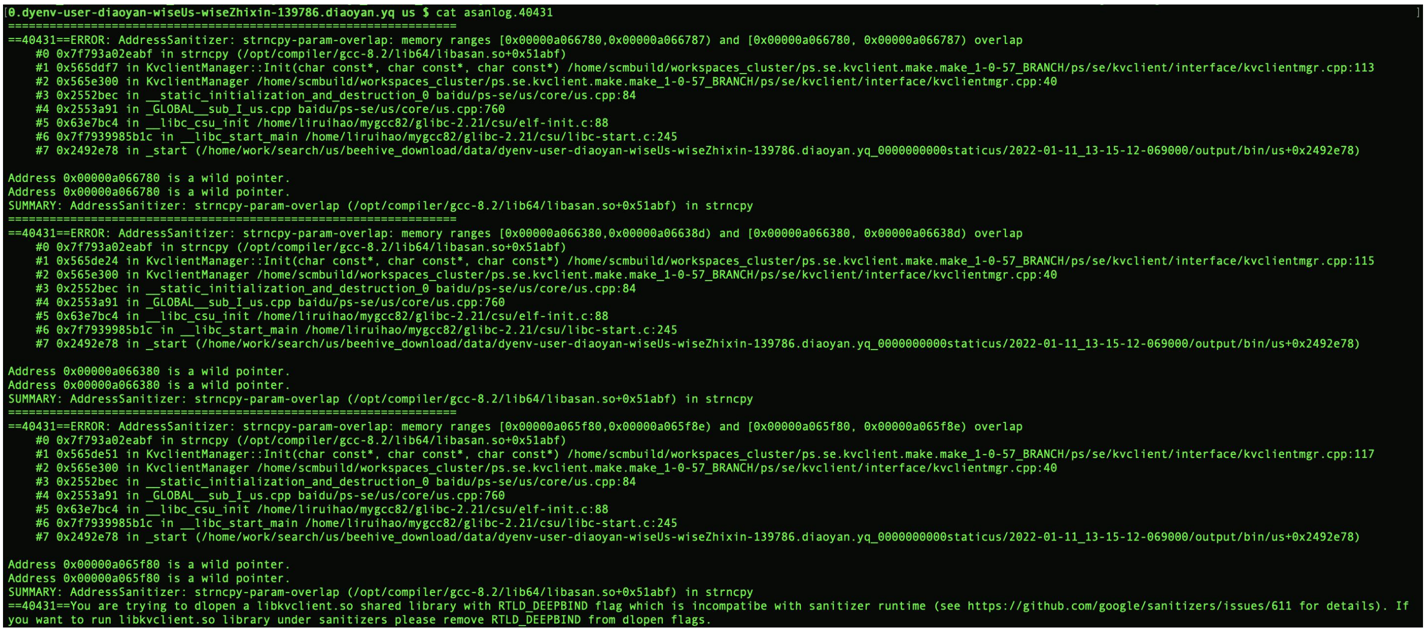
结果

如果检测出问题,会将结果输出到log文件中,结果如下,感觉检查的不太准,另外asan不兼容dlopen的RTLD_DEEPBIND字段,需要修改一下对应的库,修改完库后通过如下命令连接本地库

bcloud build --no-ut --no-release.bcloud --with-patch-list="baidu/ps-se/gs" > 001.txt 2>&1



```
CONFIGS('baidu/simian/callgraph-lib@stable')
CONFIGS('baidu/simian/traceapd@stable')
CONFIGS('baidu/simian/flow-manager@stable')
CONFIGS('baidu/ps-se/gs@stable')        huixiangbo, 7 m
CONFIGS('baidu/third-party/prometheus-cpp@prometheus-
CONFIGS("baidu/third-party/json-cpp@json-cpp_V0.6.1.4
CONFIGS('baidu/gs/rpc@stable')
CONFIGS('baidu/gs/sd-adapter@stable')
```



```
0.dyenv-user-diaoyan-wiseUs-wiseZhixin-139786.diaoyan.yq us $ cat asanlog.40431
=================================================================
==40431==ERROR: AddressSanitizer: strncpy-param-overlap: memory ranges [0x00000a066780,0x00000a066787) and [0x00000a066780, 0x00000a066787) overlap
    #0 0x7f793a02eabf in strncpy (/opt/compiler/gcc-8.2/lib64/libasan.so+0x51abf)
    #1 0x565ddf7 in KvclientManager::Init(char const*, char const*, char const*) /home/scmbuild/workspaces_cluster/ps.se.kvclient.make.make_1-0-57_BRANCH/ps/se/kvclient/interface/kvclientmgr.cpp:113
    #2 0x565e300 in KvclientManager /home/scmbuild/workspaces_cluster/ps.se.kvclient.make.make_1-0-57_BRANCH/ps/se/kvclient/interface/kvclientmgr.cpp:40
    #3 0x2552bec in __static_initialization_and_destruction_0 baidu/ps-se/us/core/us.cpp:84
    #4 0x2553a91 in _GLOBAL__sub_I_us.cpp baidu/ps-se/us/core/us.cpp:760
    #5 0x63e7bc4 in __libc_csu_init /home/liruihao/mygcc82/glibc-2.21/csu/elf-init.c:88
    #6 0x7f7939985b1c in __libc_start_main /home/liruihao/mygcc82/glibc-2.21/csu/libc-start.c:245
    #7 0x2492e78 in _start (/home/work/search/us/beehive_download/data/dyenv-user-diaoyan-wiseUs-wiseZhixin-139786.diaoyan.yq_0000000000staticus/2022-01-11_13-15-12-069000/output/bin/us+0x2492e78)

Address 0x00000a066780 is a wild pointer.
Address 0x00000a066780 is a wild pointer.
SUMMARY: AddressSanitizer: strncpy-param-overlap (/opt/compiler/gcc-8.2/lib64/libasan.so+0x51abf) in strncpy
=================================================================
==40431==ERROR: AddressSanitizer: strncpy-param-overlap: memory ranges [0x00000a066380,0x00000a06638d) and [0x00000a066380, 0x00000a06638d) overlap
    #0 0x7f793a02eabf in strncpy (/opt/compiler/gcc-8.2/lib64/libasan.so+0x51abf)
    #1 0x565de24 in KvclientManager::Init(char const*, char const*, char const*) /home/scmbuild/workspaces_cluster/ps.se.kvclient.make.make_1-0-57_BRANCH/ps/se/kvclient/interface/kvclientmgr.cpp:115
    #2 0x565e300 in KvclientManager /home/scmbuild/workspaces_cluster/ps.se.kvclient.make.make_1-0-57_BRANCH/ps/se/kvclient/interface/kvclientmgr.cpp:40
    #3 0x2552bec in __static_initialization_and_destruction_0 baidu/ps-se/us/core/us.cpp:84
    #4 0x2553a91 in _GLOBAL__sub_I_us.cpp baidu/ps-se/us/core/us.cpp:760
    #5 0x63e7bc4 in __libc_csu_init /home/liruihao/mygcc82/glibc-2.21/csu/elf-init.c:88
    #6 0x7f7939985b1c in __libc_start_main /home/liruihao/mygcc82/glibc-2.21/csu/libc-start.c:245
    #7 0x2492e78 in _start (/home/work/search/us/beehive_download/data/dyenv-user-diaoyan-wiseUs-wiseZhixin-139786.diaoyan.yq_0000000000staticus/2022-01-11_13-15-12-069000/output/bin/us+0x2492e78)

Address 0x00000a066380 is a wild pointer.
Address 0x00000a066380 is a wild pointer.
SUMMARY: AddressSanitizer: strncpy-param-overlap (/opt/compiler/gcc-8.2/lib64/libasan.so+0x51abf) in strncpy
=================================================================
==40431==ERROR: AddressSanitizer: strncpy-param-overlap: memory ranges [0x00000a065f80,0x00000a065f8e) and [0x00000a065f80, 0x00000a065f8e) overlap
    #0 0x7f793a02eabf in strncpy (/opt/compiler/gcc-8.2/lib64/libasan.so+0x51abf)
    #1 0x565de51 in KvclientManager::Init(char const*, char const*, char const*) /home/scmbuild/workspaces_cluster/ps.se.kvclient.make.make_1-0-57_BRANCH/ps/se/kvclient/interface/kvclientmgr.cpp:117
    #2 0x565e300 in KvclientManager /home/scmbuild/workspaces_cluster/ps.se.kvclient.make.make_1-0-57_BRANCH/ps/se/kvclient/interface/kvclientmgr.cpp:40
    #3 0x2552bec in __static_initialization_and_destruction_0 baidu/ps-se/us/core/us.cpp:84
    #4 0x2553a91 in _GLOBAL__sub_I_us.cpp baidu/ps-se/us/core/us.cpp:760
    #5 0x63e7bc4 in __libc_csu_init /home/liruihao/mygcc82/glibc-2.21/csu/elf-init.c:88
    #6 0x7f7939985b1c in __libc_start_main /home/liruihao/mygcc82/glibc-2.21/csu/libc-start.c:245
    #7 0x2492e78 in _start (/home/work/search/us/beehive_download/data/dyenv-user-diaoyan-wiseUs-wiseZhixin-139786.diaoyan.yq_0000000000staticus/2022-01-11_13-15-12-069000/output/bin/us+0x2492e78)

Address 0x00000a065f80 is a wild pointer.
Address 0x00000a065f80 is a wild pointer.
SUMMARY: AddressSanitizer: strncpy-param-overlap (/opt/compiler/gcc-8.2/lib64/libasan.so+0x51abf) in strncpy
==40431==You are trying to dlopen a libkvclient.so shared library with RTLD_DEEPBIND flag which is incompatibe with sanitizer runtime (see https://github.com/google/sanitizers/issues/611 for details). If
you want to run libkvclient.so library under sanitizers please remove RTLD_DEEPBIND from dlopen flags.
```

参数说明：

-fsanitize=address 表示编译和链接程序，是最常用的问题发现方式（选用此种问题发现方式）

-fsanitize=leak 表示开启内存泄漏检查功能

-fsanitize=thread 可以用来发现一些多线程竞争访问带来的bug，不能跟-fsanitize=address 和 -fsanitize=leak一起开启

-fno-omit-frame-pointer 可以得出更清晰的调用栈信息，得到更容易理解的stack trace

-fsanitize-recover=address 是为了解决asan输出一个错误后就退出的问题，需要和启动参数ASAN_OPTIONS=halt_on_error=false搭配使用。