Q1一次问题的复盘
关于PHP的问题

什么问题
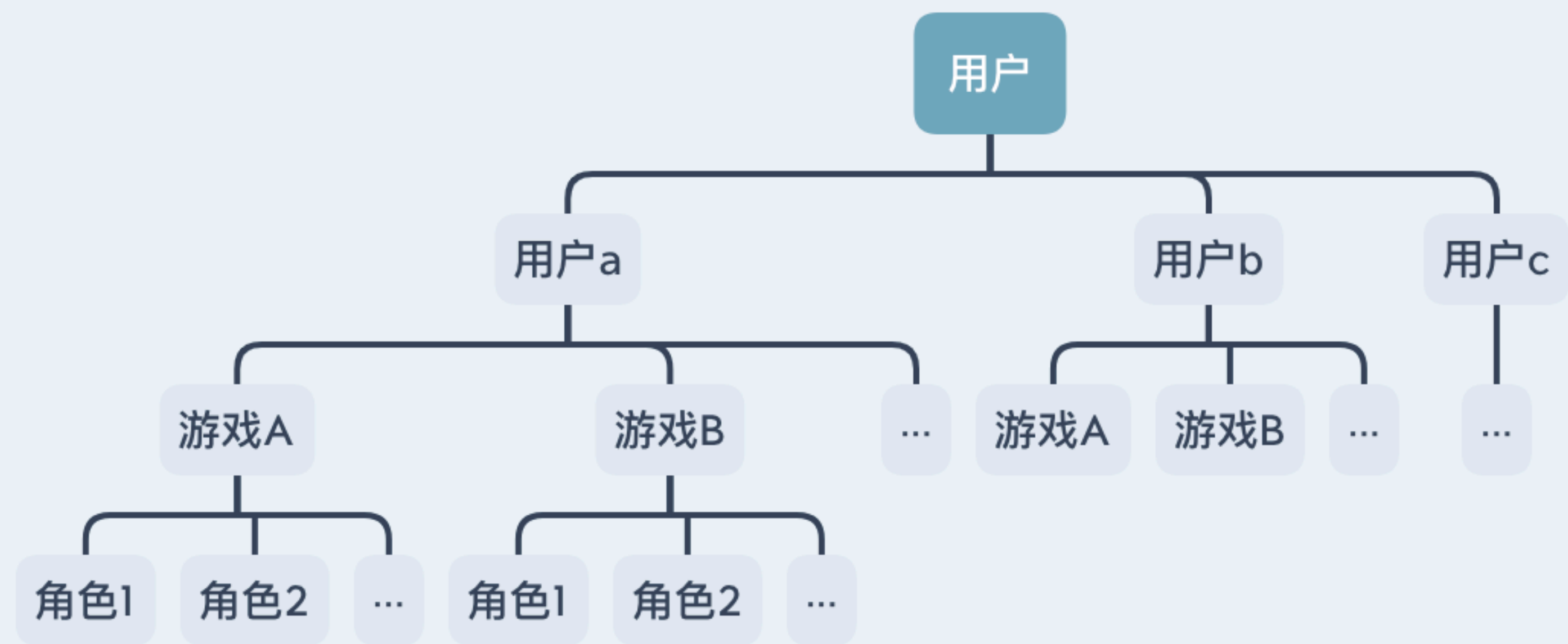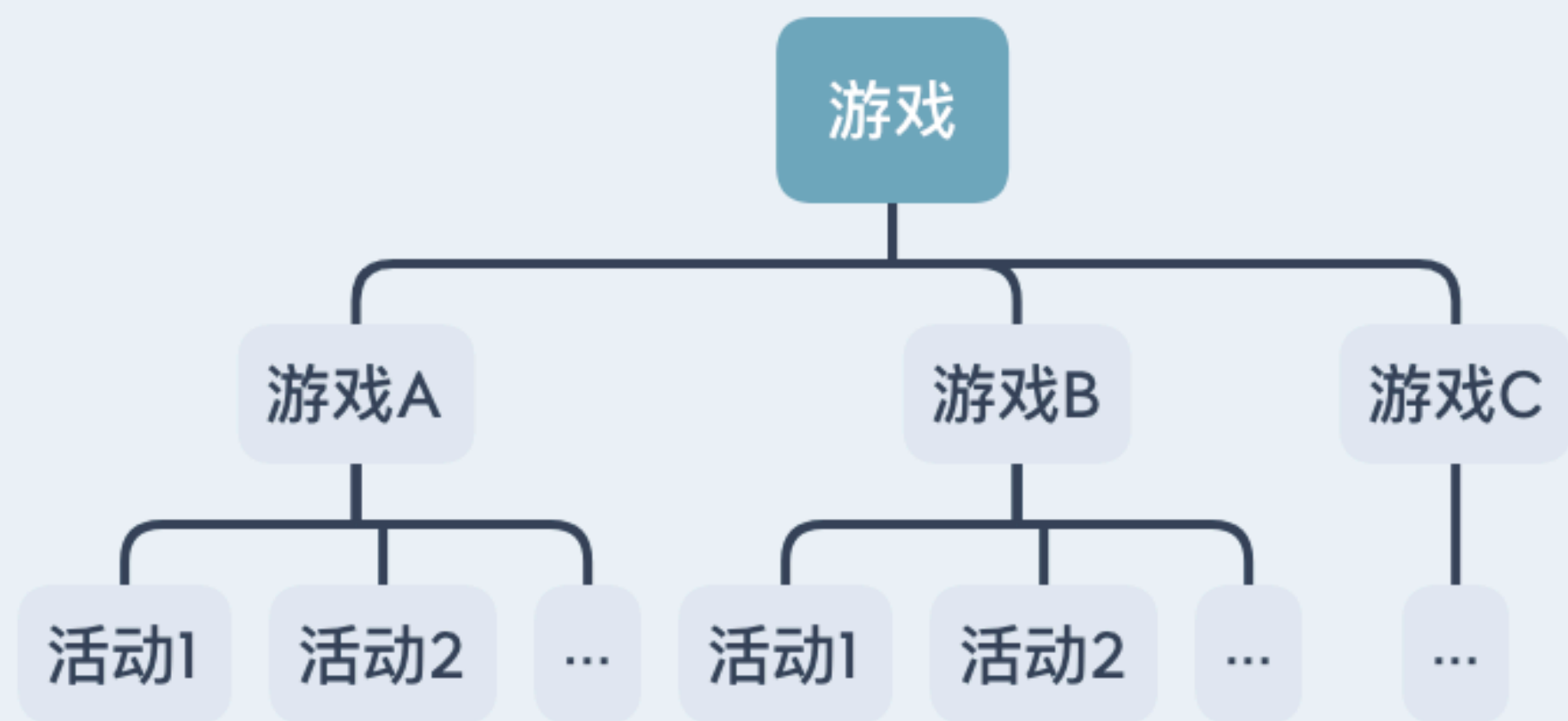
什么原因

怎么解决
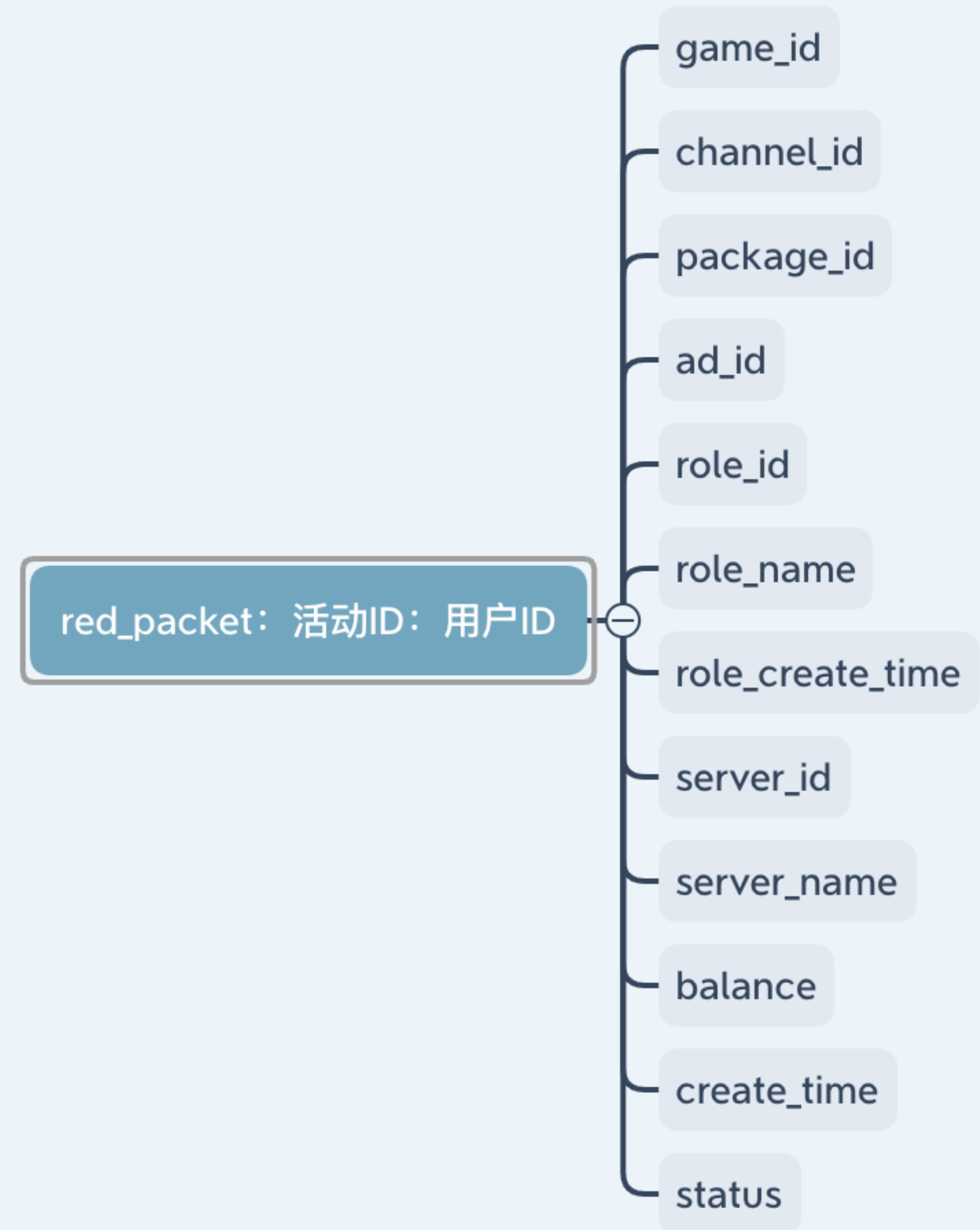
关于复盘

- 做一个红包活动
- 规则：同用户同游戏下有且仅有一个角色可以参与

- 选用redis
- string：set/get?
- hash：hset/hget?

- string 结构存储：

  - {red_packet:活动ID:用户ID} - 序列化后的对象
    - 并发加锁
    - 序列化反序列化的开销

  - {red_packet:活动ID:用户ID:game_id} - game_id
    - 整体上看key是有冗余

- hash 结构存储

red_packet：活动ID：用户ID
- game_id
- channel_id
- package_id
- ad_id
- role_id
- role_name
- role_create_time
- server_id
- server_name
- balance
- create_time
- status

```php
$redis = new \Redis();

$redis->connect('127.0.0.1', '6379');

$redis->hGetAll('bug');
```
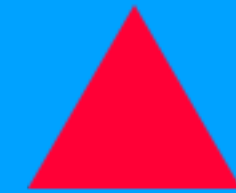
- 这是个锻炼机会：定位问题以及决策

  - 能不能快速定位问题（这是个什么问题？）

  - 有没有评估解决问题所需要的时间（解决需要多久？）

  - 有没有考虑项目交付的时间（看下deadline）

  - 有没有想过用其他方式解决（是不是一定要解决这个问题不可？）

  - 有没有求助其他人解决（集体的智慧）

- 这也是个考验能力的机会：

  - 代码设计是否合理

  - 直接影响修改成本

  - 是否追根溯源

  - 做个实践派

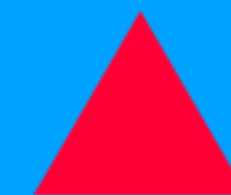- 我在项目交付的时间之前，虽然碰到了bug了，但是我通过自己的努力，并且解决了问题

问题排查

数据

知识

工具

事故现场

事故现场

- 系统内日志
- 系统外监控
- 保留运行状态
- 代码

```
[24-Mar-2020 20:16:23] WARNING: [pool www] child 24664 exited on signal 11 (SIGSEGV - core dumped) after 1252.346439 seconds from start
[24-Mar-2020 20:16:23] NOTICE: [pool www] child 31797 started
[24-Mar-2020 20:19:10] WARNING: [pool www] child 24679 exited on signal 11 (SIGSEGV - core dumped) after 1420.278015 seconds from start
[24-Mar-2020 20:19:10] NOTICE: [pool www] child 311 started
[24-Mar-2020 20:26:44] WARNING: [pool www] child 24686 exited on signal 11 (SIGSEGV - core dumped) after 1873.611088 seconds from start
[24-Mar-2020 20:26:44] NOTICE: [pool www] child 2684 started
[24-Mar-2020 21:16:25] WARNING: [pool www] child 24687 exited on signal 11 (SIGSEGV - core dumped) after 4854.674116 seconds from start
[24-Mar-2020 21:16:25] NOTICE: [pool www] child 22175 started
[24-Mar-2020 21:16:45] WARNING: [pool www] child 24678 exited on signal 11 (SIGSEGV - core dumped) after 4874.762470 seconds from start
[24-Mar-2020 21:16:45] NOTICE: [pool www] child 22179 started
[24-Mar-2020 21:16:46] WARNING: [pool www] child 24683 exited on signal 11 (SIGSEGV - core dumped) after 4875.729839 seconds from start
[24-Mar-2020 21:16:46] NOTICE: [pool www] child 22180 started
[24-Mar-2020 21:16:47] WARNING: [pool www] child 24680 exited on signal 11 (SIGSEGV - core dumped) after 4876.482671 seconds from start
[24-Mar-2020 21:16:47] NOTICE: [pool www] child 22181 started
[24-Mar-2020 21:16:47] WARNING: [pool www] child 24690 exited on signal 11 (SIGSEGV - core dumped) after 4877.070737 seconds from start
[24-Mar-2020 21:16:47] NOTICE: [pool www] child 22182 started
[24-Mar-2020 21:17:56] WARNING: [pool www] child 24599 exited on signal 11 (SIGSEGV - core dumped) after 4945.708840 seconds from start
[24-Mar-2020 21:17:56] NOTICE: [pool www] child 22520 started
[24-Mar-2020 21:17:57] WARNING: [pool www] child 24606 exited on signal 11 (SIGSEGV - core dumped) after 4946.923099 seconds from start
[24-Mar-2020 21:17:57] NOTICE: [pool www] child 22527 started
[24-Mar-2020 21:24:00] WARNING: [pool www] child 24573 exited on signal 11 (SIGSEGV - core dumped) after 5309.879935 seconds from start
[24-Mar-2020 21:24:00] NOTICE: [pool www] child 24678 started
[24-Mar-2020 21:24:42] WARNING: [pool www] child 24576 exited on signal 11 (SIGSEGV - core dumped) after 5351.993185 seconds from start
[24-Mar-2020 21:24:42] NOTICE: [pool www] child 25008 started
[24-Mar-2020 21:24:43] WARNING: [pool www] child 24574 exited on signal 11 (SIGSEGV - core dumped) after 5353.045784 seconds from start
[24-Mar-2020 21:24:43] NOTICE: [pool www] child 25010 started
```

- 1) SIGHUP   2) SIGINT   3) SIGQUIT 4) SIGILL   5) SIGTRAP
- 6) SIGABRT   7) SIGBUS 8) SIGFPE   9) SIGKILL 10) SIGUSR1
- **11) SIGSEGV** 12) SIGUSR2   13) SIGPIPE   14) SIGALRM   15) SIGTERM
- 16) SIGSTKFLT   17) SIGCHLD   18) SIGCONT   19) SIGSTOP   20) SIGTSTP
- 21) SIGTTIN   22) SIGTTOU   23) SIGURG   24) SIGXCPU   25) SIGXFSZ
- 26) SIGVTALRM   27) SIGPROF   28) SIGWINCH 29) SIGIO   30) SIGPWR
- 31) SIGSYS   34) SIGRTMIN   35) SIGRTMIN+1   36) SIGRTMIN+2   37) SIGRTMIN+3
- 38) SIGRTMIN+4 39) SIGRTMIN+5   40) SIGRTMIN+6   41) SIGRTMIN+7   42) SIGRTMIN+8
- 43) SIGRTMIN+9 44) SIGRTMIN+10   45) SIGRTMIN+11   46) SIGRTMIN+12   47) SIGRTMIN+13
- 48) SIGRTMIN+1449) SIGRTMIN+15   50) SIGRTMAX-14   51) SIGRTMAX-13 52) SIGRTMAX-12
- 53) SIGRTMAX-11   54) SIGRTMAX-10   55) SIGRTMAX-9   56) SIGRTMAX-8   57) SIGRTMAX-7
- 58) SIGRTMAX-6 59) SIGRTMAX-5   60) SIGRTMAX-4   61) SIGRTMAX-3   62) SIGRTMAX-2
- 63) SIGRTMAX-1 64) SIGRTMAX

- **SIGSEGV 11 无效的内存引用**

- **终止进程并进行内核映像转储（dump core），内核映像转储是指将进程数据在内存的映像和进程在内核结构中的部分内容以一定格式转储到文件系统，并且进程退出执行，这样做的好处是为程序员提供了方便，使得他们可以得到进程当时执行时的数据值，允许他们确定转储的原因，并且可以调试他们的程序**

- **程序自己都捕捉不了的死前快照**

- **ulimit -c**
- **ulimit -c unlimited**

- **/proc/sys/kernel/core_pattern**

- **%p所dump进程的进程ID**
- **%u所dump进程的实际用户ID**
- **%g所dump进程的实际组ID**
- **%s导致本次core dump的信号**
- **%t core dump的时间%h主机名**
- **%e程序文件名**

```php
$redis = new \Redis();

$redis->connect('127.0.0.1', '6379');

$redis->hGetAll('bug');
```

如何复现?

- 环境一致性原则：
  - 应用版本：**PHP、Redis、PHP扩展····**
  - 系统版本：**CentOS**

- 复现问题**PoC：**
  - 定位
  - 简化代码
  - 分析猜测可能的原因
  - 验证想法

初步排查

- 尝试下范围：版本影响

- 开发：我本地没有问题

- 开发：我本地PHP版本是7.2.X，线上版本是7.0.11

- **PHP的Redis扩展版本问题?**

- **Redis版本问题?**

- **PHP版本问题?**

- **系统的问题?**

- **PHP的Redis扩展版本问题？**

- **直接线上checkout 测试环境的PHPRedis的更高级版本，重新编译**

初步排查

- **Redis版本问题?**

- **sudo tcpdump -i lo -w /tmp/redis_php.cap**

- **sudo tcpdump -i lo -w /tmp/redis_cli.cap**

初步排查

	8	0.000194	127.0.0.1	127.0.0.1	TCP	90	37356 → 6379	[PSH, ACK] Seq=43 A
	9	0.000228	127.0.0.1	127.0.0.1	TCP	162	6379 → 37356	[PSH, ACK] Seq=5 Ac
	10	0.000342	127.0.0.1	127.0.0.1	TCP	66	37356 → 6379	[FIN, ACK] Seq=67 A
	11	0.000375	127.0.0.1	127.0.0.1	TCP	66	6379 → 37356	[FIN, ACK] Seq=101
	12	0.000380	127.0.0.1	127.0.0.1	TCP	66	37356 → 6379	[ACK] Seq=68 Ack=10
	13	4.114796	127.0.0.1	127.0.0.1	TCP	74	37536 → 1988	[SYN] Seq=0 Win=436
	14	-2091320396.163553	127.0.0.1	127.0.0.1	TCP	74	1988 → 37536	[SYN, ACK] Seq=0 Ac
	15	4.114833	127.0.0.1	127.0.0.1	TCP	66	37536 → 1988	[ACK] Seq=1 Ack=1 W
	16	4.114914	127.0.0.1	127.0.0.1	HTTP	456	POST /v1/push HTTP/1.1	(applica
	17	4.114921	127.0.0.1	127.0.0.1	TCP	66	1988 → 37536	[ACK] Seq=1 Ack=391

TCP payload (96 bytes)

```
0000   00 00 00 00 00 00 00 00   00 00 00 00 08 00 45 00   ........ ......E.
0010   00 94 b6 28 40 00 40 06   86 39 7f 00 00 01 7f 00   ...(@.@. .9......
0020   00 01 18 eb 91 ec 07 e4   a1 be 4c b5 03 8e 80 18   ........ ..L.....
0030   01 56 fe 88 00 00 01 01   08 0a 81 d3 17 9c 81 d3   .V...... ........
0040   17 9c 2a 31 32 0d 0a 24   31 0d 0a 61 0d 0a 24 31   ..*12..$ 1..a..$1
0050   0d 0a 78 0d 0a 24 31 0d   0a 62 0d 0a 24 31 0d 0a   ..x..$1. .b..$1..
0060   79 0d 0a 24 31 0d 0a 63   0d 0a 24 31 0d 0a 7a 0d   y..$1..c ..$1..z.
0070   0a 24 31 0d 0a 64 0d 0a   24 31 0d 0a 74 0d 0a 24   .$1..d.. $1..t..$
0080   31 0d 0a 65 0d 0a 24 31   0d 0a 69 0d 0a 24 34 0d   1..e..$1 ..i..$4.
0090   0a 6b 65 79 31 0d 0a 24   35 0d 0a 68 65 6c 6c 6f   .key1..$ 5..hello
00a0   0d 0a                                               ..
```

|					
105 5.004261	127.0.0.1	127.0.0.1	TCP	66 6379 → 37768 [ACK] Seq=1 Ack=25 W
106 5.004323	127.0.0.1	127.0.0.1	TCP	162 6379 → 37768 [PSH, ACK] Seq=1 Ack
107 5.004355	127.0.0.1	127.0.0.1	TCP	66 37768 → 6379 [ACK] Seq=25 Ack=97
108 10.521085	127.0.0.1	127.0.0.1	TCP	90 37768 → 6379 [PSH, ACK] Seq=25 Ac

▶ [SEQ/ACK analysis]
　 TCP payload (96 bytes)
▼ Data (96 bytes)
　　Data: 2a31320d0a24310d0a610d0a24310d0a780d0a24310d0a62...

```
0000   00 00 00 00 00 00 00 00   00 00 00 00 08 00 45 00   ........ ......E.
0010   00 94 a2 a4 40 00 40 06   99 bd 7f 00 00 01 7f 00   ....@.@. ........
0020   00 01 18 eb 93 88 11 a8   0d 31 24 c7 28 4d 80 18   ........ .1$.(M..
0030   01 56 fe 88 00 00 01 01   08 0a 81 d8 b7 5d 81 d8   .V...... .....]..
0040   b7 5d 2a 31 32 0d 0a 24   31 0d 0a 61 0d 0a 24 31   .]*12..$ 1..a..$1
0050   0d 0a 78 0d 0a 24 31 0d   0a 62 0d 0a 24 31 0d 0a   ..x..$1. .b..$1..
0060   79 0d 0a 24 31 0d 0a 63   0d 0a 24 31 0d 0a 7a 0d   y..$1..c ..$1.z.
0070   0a 24 31 0d 0a 64 0d 0a   24 31 0d 0a 74 0d 0a 24   .$1..d.. $1..t..$
0080   31 0d 0a 65 0d 0a 24 31   0d 0a 69 0d 0a 24 34 0d   1..e..$1 ..i..$4.
0090   0a 6b 65 79 31 0d 0a 24   35 0d 0a 68 65 6c 6c 6f   .key1..$ 5..hello
00a0   0d 0a                                              ..
```

- **PHP版本的问题?**
- **系统问题?**

- **7.0.12**
- **php的docker官方版**
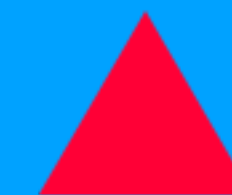
环境准备

- **Docker**
- **系统Centos：7.2.1511**
- **编译安装PHP**
- **Redis扩展**
- **Redis**


```
COPY redis-2.8.17.tar.gz /work/src/

RUN cd /work/src/;\
    tar -zxvf /work/src/redis-2.8.17.tar.gz;\
    cd /work/src/redis-2.8.17;\
    make PREFIX=/work/servers/redis install;\
    make install

COPY php-7.0.11 /work/src/php-7.0.11

RUN cd /work/src/;\
    cd /work/src/php-7.0.11;\
    make clean;\
    ./configure --prefix=/work/servers/php --enable-mbstring --with-mysql --with-mysqli
    --with-mysql-sock --with-gd  --enable-pdo --with-pdo-mysql --enable-sockets
    --enable-bcmath --enable-xml --enable-zip --with-openssl=/work/lib/openssl --with-zlib
    --with-curl --enable-opcache --with-mcrypt;\
    make -j4;\
    make install

RUN cd /work/src/;\
    rm -rf phpredis;\
    git clone https://github.com/phpredis/phpredis.git;\
    cd phpredis;\
    git checkout 3.1.3;\
    make clean;\
    /work/servers/php/bin/phpize;\
    ./configure --with-php-config=/work/servers/php/bin/php-config;\
    make -j4;\
    make install;
```

```
[24-Mar-2020 20:16:23] WARNING: [pool www] child 24664 exited on signal 11 (SIGSEGV - core dumped) after 1252.346439 seconds from start
[24-Mar-2020 20:16:23] NOTICE: [pool www] child 31797 started
[24-Mar-2020 20:19:10] WARNING: [pool www] child 24679 exited on signal 11 (SIGSEGV - core dumped) after 1420.278015 seconds from start
[24-Mar-2020 20:19:10] NOTICE: [pool www] child 311 started
[24-Mar-2020 20:26:44] WARNING: [pool www] child 24686 exited on signal 11 (SIGSEGV - core dumped) after 1873.611088 seconds from start
[24-Mar-2020 20:26:44] NOTICE: [pool www] child 2684 started
[24-Mar-2020 21:16:25] WARNING: [pool www] child 24687 exited on signal 11 (SIGSEGV - core dumped) after 4854.674116 seconds from start
[24-Mar-2020 21:16:25] NOTICE: [pool www] child 22175 started
[24-Mar-2020 21:16:45] WARNING: [pool www] child 24678 exited on signal 11 (SIGSEGV - core dumped) after 4874.762470 seconds from start
[24-Mar-2020 21:16:45] NOTICE: [pool www] child 22179 started
[24-Mar-2020 21:16:46] WARNING: [pool www] child 24683 exited on signal 11 (SIGSEGV - core dumped) after 4875.729839 seconds from start
[24-Mar-2020 21:16:46] NOTICE: [pool www] child 22180 started
[24-Mar-2020 21:16:47] WARNING: [pool www] child 24680 exited on signal 11 (SIGSEGV - core dumped) after 4876.482671 seconds from start
[24-Mar-2020 21:16:47] NOTICE: [pool www] child 22181 started
[24-Mar-2020 21:16:47] WARNING: [pool www] child 24690 exited on signal 11 (SIGSEGV - core dumped) after 4877.070737 seconds from start
[24-Mar-2020 21:16:47] NOTICE: [pool www] child 22182 started
[24-Mar-2020 21:17:56] WARNING: [pool www] child 24599 exited on signal 11 (SIGSEGV - core dumped) after 4945.708840 seconds from start
[24-Mar-2020 21:17:56] NOTICE: [pool www] child 22520 started
[24-Mar-2020 21:17:57] WARNING: [pool www] child 24606 exited on signal 11 (SIGSEGV - core dumped) after 4946.923099 seconds from start
[24-Mar-2020 21:17:57] NOTICE: [pool www] child 22527 started
[24-Mar-2020 21:24:00] WARNING: [pool www] child 24573 exited on signal 11 (SIGSEGV - core dumped) after 5309.879935 seconds from start
[24-Mar-2020 21:24:00] NOTICE: [pool www] child 24678 started
[24-Mar-2020 21:24:42] WARNING: [pool www] child 24576 exited on signal 11 (SIGSEGV - core dumped) after 5351.993185 seconds from start
[24-Mar-2020 21:24:42] NOTICE: [pool www] child 25008 started
[24-Mar-2020 21:24:43] WARNING: [pool www] child 24574 exited on signal 11 (SIGSEGV - core dumped) after 5353.045784 seconds from start
[24-Mar-2020 21:24:43] NOTICE: [pool www] child 25010 started
```

```yaml
version: "2"
services:
  php-worker:
    image: zhengzijian/bug/phpredis/7.0.11-try-fix:latest
    privileged: true
    ulimits:
      core: -1
      nproc: 65535
      nofile:
        soft: 20000
        hard: 40000
```

- echo "/tmp/core-%e-%p-%t" > /proc/sys/kernel/core_pattern

```php
<?php

$redis = new \Redis();
$redis->connect('redis','6379');
$redis->hSet('bug', 'a', 'A');
$redis->hSet('bug', 'b', 'B');
$redis->hSet('bug', 'c', 'C');
$redis->hSet('bug', 'd', 'D');
$redis->hSet('bug', 'e', 'E');
$redis->hSet('bug', 'f', 'F');
$bug = $redis->hGetAll('bug');
foreach($bug as $k => $v) {
    //遍历到f的时候一定概率coredump
    echo "k:{$k} v:{$v}\n";
    var_dump($v);
}
//有一定概率找不到，NULL
var_dump($bug['f']);

var_export($bug);
//echo json_encode($b);
```

```
[root@92094df03810 tmp]# /work/servers/php/bin/p
array (
  'a' => 'A',
  'b' => 'B',
  'c' => 'C',
  'd' => 'D',
  'e' => 'E',
  'E' => 'E',
)k:a v:A
string(1) "A"
k:b v:B
string(1) "B"
k:c v:C
string(1) "C"
k:d v:D
string(1) "D"
k:e v:E
string(1) "E"
Segmentation fault (core dumped)
```

```php
<?php

function main(){
    $redis = new \Redis();
    $redis->connect('127.0.0.1','6379');
    $bug = $redis->hGetAll('bug');

    foreach($bug as $k => $v) {

    }

    $_bug = [
        'a'=>'A',
        'b'=>'B',
        'c'=>'C' ,
        'd'=>'D',
        'e' => 'E',
        'f' => 'shit'
    ];

    var_export($bug);
    var_export($_bug);
}

main();
```

```
[root@92094df03810 php-scripts]# /work/se
array (
  'a' => 'A',
  'b' => 'B',
  'c' => 'C',
  'd' => 'D',
  'e' => 'E',
  'f' => 'shit',
)array (
  'a' => 'A',
  'b' => 'B',
  'c' => 'C',
  'd' => 'D',
  'e' => 'E',
  'f' => 'shit',
)[root@92094df03810 php-scripts]# 
```

```php
<?php

$redis = new \Redis();
$redis->connect('127.0.0.1','6379');
$bug = $redis->hGetAll('bug');
var_export($bug);
foreach($bug as $k => $v) {
    echo($v);
}
var_export($bug);
```

```
)[root@92094df03810 php-scripts]# /work/servers/php/bin/php
array (
  'a' => 'A',
  'b' => 'B',
  'c' => 'C',
  'd' => 'D',
  'e' => 'E',
  'E' => 'E',
)ABCDEEarray (
  'a' => 'A',
  'b' => 'B',
  'c' => 'C',
  'd' => 'D',
  '' . "\0" . 'D' . "\0" . 'harset$@# ' . "\0" . '' . "\0"
'' . "\0" . '' . "\0" . '' . "\0" . '' . "\0" . '' . "\0" .
. "\0" . '' . "\0" . '' . "\0" . '' . "\0" . '' . "\0" . '
\0" . '' . "\0" . '       @' . "\0" . '' . "\0" . '' . "\0"
. '# ' . "\0" . '' . "\0" . '@#@# ' . "\0" . '' . "\0" . '@
. "\0" . 'a' . "\0" . 'g' . "\0" . '# ' . "\0" . '' . "\0"
\0" . '' . "\0" . '' . "\0" . '' . "\0" . '' . "\0" . ''
. '' . "\0" . '' . "\0" . '' . "\0" . '' . "\0" . '' . "\0"
0" . '' . "\0" . ' #@# ' . "\0" . '' . "\0" . '@' . "\0"
b' . "\0" . '79' . "\0" . ' ' . "\0" . '' . "\0" . '@#@# '
"\0" . '' . "\0" . '' . "\0" . '' . "\0" . '' => NULL,
```

- 一定是内存管理出现了问题（空指针）
- 一定是和内存回收有关

- 一定是内存管理出现了问题（空指针）
- 一定是和内存回收有关

- gdb /work/servers/php/bin/php -c core-php-343-1589424760

```
(gdb) bt
#0  zend_mm_gc (heap=0x7ff8ba000040) at /work/src/php-7.0.11/Zend/zend_alloc.c:1899
#1  0x00000000007b6ab7 in zend_mm_alloc_huge (heap=0x7ff8ba000040, size=4047968968097232008) at /work/src/php-7.0.11/Zend/zend_alloc.c
#2  0x000000000081c6f8 in zend_string_alloc (persistent=0, len=4047968968097231980) at /work/src/php-7.0.11/Zend/zend_string.h:121
#3  ZEND_ROPE_END_SPEC_TMP_CONST_HANDLER () at /work/src/php-7.0.11/Zend/zend_vm_execute.h:12911
#4  0x000000000081705b in execute_ex (ex=<optimized out>) at /work/src/php-7.0.11/Zend/zend_vm_execute.h:414
#5  0x0000000000860517 in zend_execute (op_array=0x7ff8ba07f000, op_array@entry=0x7ff8b2d3eaa0, return_value=return_value@entry=0x7ff8
    at /work/src/php-7.0.11/Zend/zend_vm_execute.h:458
#6  0x0000000007dac34 in zend_execute_scripts (type=type@entry=8, retval=0x7ff8ba013030, retval@entry=0x0, file_count=file_count@entr
#7  0x000000000077f050 in php_execute_script (primary_file=primary_file@entry=0x7ffcd2989170) at /work/src/php-7.0.11/main/main.c:2494
#8  0x000000000086209f in do_cli (argc=4, argv=0x1c68840) at /work/src/php-7.0.11/sapi/cli/php_cli.c:974
#9  0x0000000000468d8f in main (argc=4, argv=0x1c68840) at /work/src/php-7.0.11/sapi/cli/php_cli.c:1344
```

- **export USE_ZEND_ALLOC=0**
- **是不是和zend的内存管理有关?**

```
[root@92094df03810 tmp]# /work/servers/php/bin/php -c /wor
array (
  'a' => 'A',
  'b' => 'B',
  'c' => 'C',
  'd' => 'D',
  'e' => 'E',
  'E' . "\0" . '' . "\0" . '' . "\0" . '' => 'E',
)k:a v:A
string(1) "A"
k:b v:B
string(1) "B"
k:c v:C
string(1) "C"
k:d v:D
string(1) "D"
k:e v:E
string(1) "E"
Bus error (core dumped)
```

```
(gdb) zbacktrace
[0x7f22c7801180] sleep(60) [internal function]
[0x7f22c78010e0] x(array(6)[0x7f22c7801140], array(1)[0x7f22c7801150]) /work/php-scripts/sleep.php:16
[0x7f22c7801040] (main) /work/php-scripts/sleep.php:13
(gdb) p ((zval *)0x7f22c7801140)
$1 = (zval *) 0x7f22c7801140
(gdb) p ((zval *)0x7f22c7801150)
$2 = (zval *) 0x7f22c7801150
(gdb) printzv $1
[0x7f22c7801140] (refcount=34360289) array:       Hash(6)[0x20c4bb0]: {
      [0] a => [0x20c4dd0] (refcount=34360128) string: A
      [1] b => [0x20c4df0] (refcount=34360352) string: B
      [2] c => [0x20c4e10] (refcount=34361040) string: C
      [3] d => [0x20c4e30] (refcount=34361712) string: D
      [4] e => [0x20c4e50] (refcount=34361760) string: E
      [5] f => [0x20c4e70] (refcount=34361808) string: F
}


(gdb) printzv $
[0x7f22c7801150] (refcount=2) array:       Hash(1)[0x7f22baa31678]: {
      [0] zhengzijian => [0x7f22baa316d0] (refcount=1) string: zhengzijian
}


(gdb) printzv $2
[0x7f22c7801150] (refcount=2) array:       Hash(1)[0x7f22baa31678]: {
      [0] zhengzijian => [0x7f22baa316d0] (refcount=1) string: zhengzijian
}
```

```
(gdb) p ((zval *)0x7f6ecac14130)
$1 = (zval *) 0x7f6ecac14130
(gdb) printzv $1
[0x7f6ecac14130] (refcount=-893033431) array:       Hash(6)[0x7f6ecac56460]: {
        [0] a => [0x7f6ecac5c7a0] (refcount=-893372960) string: A
        [1] b => [0x7f6ecac5c7c0] (refcount=-893373024) string: B
        [2] c => [0x7f6ecac5c7e0] (refcount=-893373088) string: C
        [3] d => [0x7f6ecac5c800] (refcount=-893373120) string: D
        [4] e => [0x7f6ecac5c820] (refcount=-893372224) string: E
        [5]   => [0x7f6ecac5c840] (refcount=-893373184) string: E
}
```

```
(gdb) p ((zval *)0x7f6ecac14130).value.arr.nNumUsed
$4 = 6
(gdb) p ((zval *)0x7f6ecac14130).value.arr.arData[6].val.value.str
$5 = (zend_string *) 0x0
(gdb) p ((zval *)0x7f6ecac14130).value.arr.arData[6].val.value.str.val
Cannot access memory at address 0x18
(gdb) p ((zval *)0x7f6ecac14130).value.arr.arData[0].val.value.str.val
$6 = "A"
(gdb) p ((zval *)0x7f6ecac14130).value.arr.arData[5].val.value.str.val
$7 = "E"
(gdb) p ((zval *)0x7f6ecac14130).value.arr.arData[6].val.value.str.val
Cannot access memory at address 0x18
(gdb)
```

```c
MAKE_STD_ZVAL(z_multi_result);
array_init(z_multi_result); /* pre-allocate array for multi's results. */

redis_sock_read_multibulk_reply_loop(INTERNAL_FUNCTION_PARAM_PASSTHRU,
                    redis_sock, z_multi_result, numElems, 1, flag ? UNSERIALIZE_ALL : l

array_zip_values_and_scores(redis_sock, z_multi_result, 0 TSRMLS_CC);

IF_MULTI_OR_PIPELINE() {
    add_next_index_zval(z_tab, z_multi_result);
} else {
    *return_value = *z_multi_result;
    zval_copy_ctor(return_value);
    zval_dtor(z_multi_result);
    efree(z_multi_result);
}
```
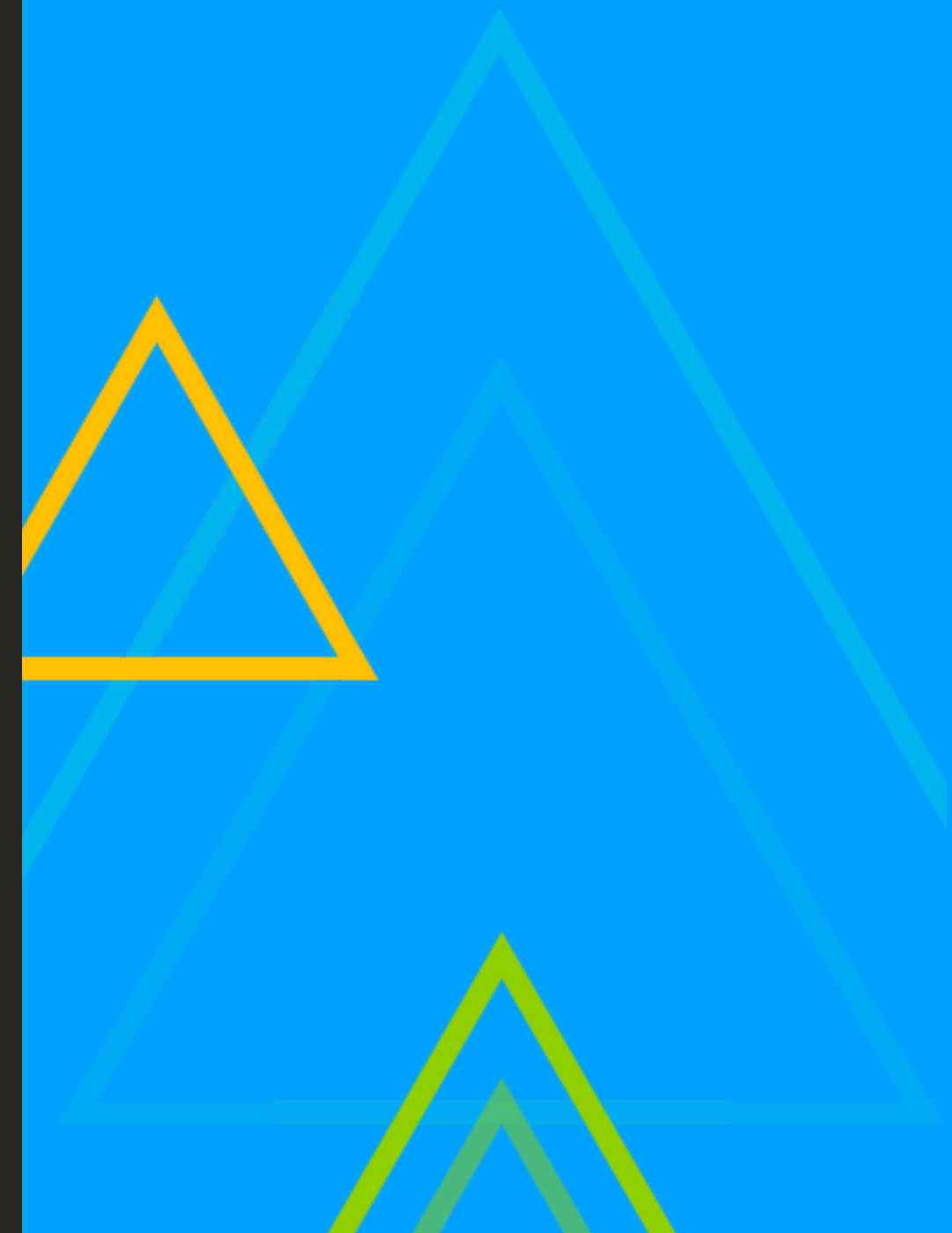
```c
ZEND_API void ZEND_FASTCALL _zval_dtor_func(zend_refcounted *p ZEND_FILE_LINE_DC)
{
    if (--GC_REFCOUNT(p)) {
        return;
    }

    switch (GC_TYPE(p)) {
        case IS_STRING:
        case IS_CONSTANT: {
                zend_string *str = (zend_string*)p;
                CHECK_ZVAL_STRING_REL(str);
                zend_string_release(str);
                break;
            }
        case IS_ARRAY: {
                zend_array *arr = (zend_array*)p;
                ZEND_ASSERT(GC_REFCOUNT(arr) <= 1);
                zend_array_destroy(arr);
                break;
            }
        case IS_CONSTANT_AST: {
                zend_ast_ref *ast = (zend_ast_ref*)p;

                zend_ast_destroy_and_free(ast->ast);
                efree_size(ast, sizeof(zend_ast_ref));
                break;
            }
        case IS_OBJECT: {
                zend_object *obj = (zend_object*)p;

                OBJ_RELEASE(obj);
                break;
```
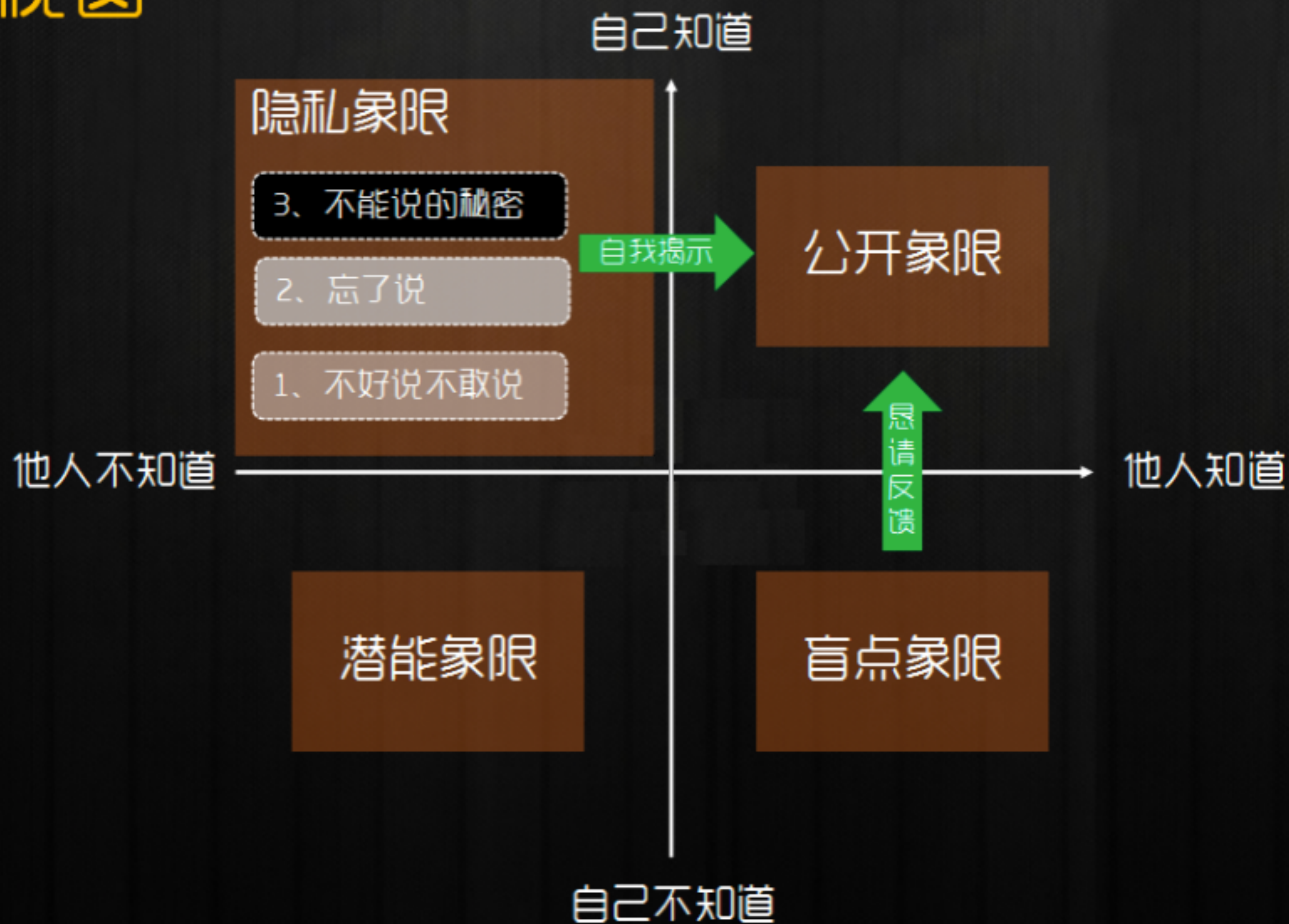
求知

对比

实践

谦虚

THANKS!