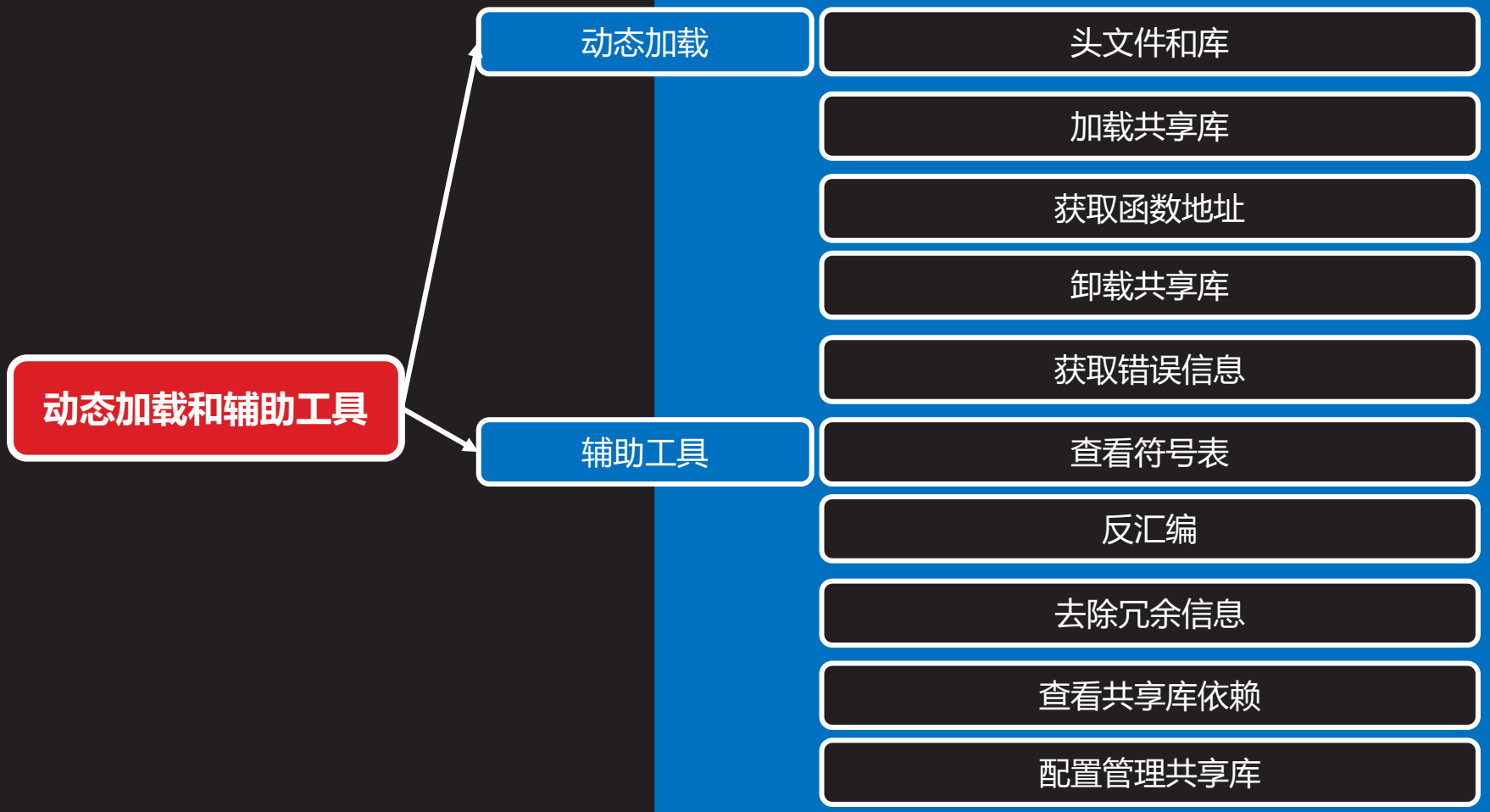
Technology Tarena 达内科技

Unix系统高级编程

动态加载和辅助工具 Unit03

动态加载和辅助工具


动态加载和辅助工具
动态加载
辅助工具
头文件和库
加载共享库
获取函数地址
卸载共享库
获取错误信息
查看符号表
反汇编
去除冗余信息
查看共享库依赖
配置管理共享库

Technology Tarena 达内科技

动态加载

头文件和库

- 在程序中动态加载共享库需要调用一组特殊的函数，它们被声明于一个专门的头文件，并在一个独立的库中予以实现。使用这组函数需要包含此头文件，并链接该库
  - #include <dlfcn.h>
  - -ldl

知识讲解

加载共享库

- 将共享库载入内存并获得其访问句柄

void* dlopen (const char* *filename*, int *flag*);

成功返回共享库句柄，失败返回NULL

  - ***filename***：共享库路径，若只给文件名，则根据LD_LIBRARY_PATH环境变量搜索
  - ***flag***：加载方式，可取以下值

    `RTLD_LAZY` - 延迟加载，使用共享库中的符号(如调用库中的函数)时才加载

    `RTLD_NOW` - 立即加载

- 共享库访问句柄唯一地标识了系统内核所维护的共享库对象，将作为后续函数调用的参数

知识讲解

加载共享库（续1）

- 例如
  - void* handle = dlopen ("libmath.so", RTLD_NOW);
    if (! handle) {
    fprintf (stderr, "加载共享库失败！\n");
    exit (EXIT_FAILURE);
    }

知识讲解

获取函数地址

- 从指定共享库中获取与给定函数名对应的函数入口地址

void* dlsym (void* *handle*, const char* *symbol*);

成功返回函数地址，失败返回NULL

  - ***handle***：共享库访问句柄
  - ***symbol***：函数名
- 所返回的函数指针是void*类型，需要造型为实际函数指针类型才能调用

知识讲解

获取函数地址（续1）

- 例如
  - int (*add) (int, int) = (int (*) (int, int))dlsym (
    handle, "add");
    if (! add) {
    fprintf (stderr, "获取函数地址失败！\n");
    exit (EXIT_FAILURE);
    }
  - int sum = add (30, 20);

知识讲解

卸载共享库

- 从内存中卸载共享库

int dlclose (void* *handle*);

成功返回0，失败返回非零

  - ***handle***：共享库访问句柄
- 所卸载的共享库未必真的会从内存中立即消失，因为其它程序可能还需要使用该库
- 只有所有使用该库的程序都显式或隐式地卸载了该库，该库所占用的内存空间才会真正得到释放
- 无论所卸载的共享库是否真正被释放，传递给dlclose函数的句柄参数都会在该函数成功返回后立即失效

知识讲解

卸载共享库（续1）

- 例如
  - if (dlclose (handle)) {
    fprintf (stderr, "卸载共享库失败！\n");
    exit (EXIT_FAILURE);
    }

获取错误信息

- 获取在加载、使用和卸载共享库过程中所发生的错误

char* dlerror (void);

有错误则返回指向错误信息字符串的指针，否则返回NULL

- 例如
  - void* handle = dlopen ("libmath.so", RTLD_NOW);
    if (! handle) {
    fprintf (stderr, "dlopen: %s\n", dlerror ());
    exit (EXIT_FAILURE);
    }

知识讲解

动态加载

【参见：load.c】

课堂练习

- 动态加载

Technology Tarena 达内科技

辅助工具

查看符号表

- 列出目标文件、可执行文件、静态库或共享库中的符号

```
$ nm libmath.a
```

```
calc.o:
00000000 T add
0000000d T sub
show.o:
00000000 T show
```

知识讲解

反汇编

- 显示二进制模块的反汇编信息

```
$ objdump -S a.out
```

```
8048514:    55                              push %ebp
8048515:    89 e5                           mov  %esp,%ebp
8048517:    83 e4 f0                        and  $0xfffffff0,%esp
804851a:    83 ec 20                        sub  $0x20,%esp
804851d:    c7 44 24 04 02 00 00    movl $0x2,0x4(%esp)
```

知识讲解

去除冗余信息

- 去除目标文件、可执行文件、静态库和共享库中的符号表、调试信息等

```
$ strip a.out
```

知识讲解

查看共享库依赖

- 查看可执行文件或共享库所依赖的共享库文件

```
$ ldd a.out
```

```
linux-gate.so.1 =>  (0xb7760000)
libmath.so (0xb775c000)
libc.so.6 => /lib/i386-linux-gnu/libc.so.6 (0xb7599000)
/lib/ld-linux.so.2 (0xb7761000)
```

知识讲解

配置管理共享库

Technology Tarena 达内科技

- 用专门的配置文件管理共享库的搜索路径
  - 事先将共享库的路径信息写入/etc/ld.so.conf配置文件中
  - 执行ldconfig命令，将/etc/ld.so.conf配置文件转换为/etc/ld.so.cache缓冲文件，并将后者加载到系统内存中，借以提高共享库的搜索和加载速度

```
$ ldconfig
```

  - 每次系统启动时都会自动执行ldconfig命令
  - 如果修改了共享库配置文件/etc/ld.so.conf，则需要手动执行ldconfig命令，更新缓冲文件并重新加载到系统内存

知识讲解

Technology Tarena 达内科技

总结和答疑