《西说 FreeBSD》

西 门

二零一九年五月一日

西门？何许人也？

西门，本名范辉，西门课堂创始人，基础平台架构师，Linux 专家，一万小时程序员，一线大厂资深后端，区块链拓荒者，Rust 语言布道者 ··· 好吧，说人话，十年老码农，技术狂，热爱开源，乐于分享。

欢迎来到西门课堂，听西门老师说 FreeBSD！

FreeBSD 是什么？

FreeBSD 是 BSD[①]类操作系统的一个核心分支，在世界范围内都有广泛的应用，至今已有 30 多年的历史。关于 BSD，不得不提的是：

- TCP/IP 协议族的基石-sockets[②]，是由 BSD 发明的
- Linux 诞生与发展的过程中，大量借鉴了 BSD 的设计
- 苹果公司的手机操作系统 IOS 是基于 FreeBSD 开发的
- 苹果公司的电脑操作系统 Mac OS X 是基于 FreeBSD 开发的
- 思科公司的网络设备嵌入式操作系统 IOS，是基于 FreeBSD 开发的

本书风格是提纲式的解说，力求简单明了，需要详细步骤演示的同学，请结合视频教程一起学习，西门课堂的 B 站主页是：

space.bilibili.com/393582752

扫码加微信，欢迎技术交流

[①]BSD, Berkeley Software Distribution，最早的 UNIX 衍生系统，1977 至 1995 年间由加州大学伯克利分校开发

[②]Berkeley sockets，伯克利套接字，详情参见维基百科

目录

Chapter 1

基础篇

1.1 系统安装

1.1.1 准备虚拟机环境

可选 Qemu、VirtualBox 、Vmware 等虚拟方案，挑自己熟悉的即可。本书使用的是 Linux 平台上的 Qemu 方案，启动脚本参见第12页的附录.1。

1.1.2 获取系统盘并安装

> **NOTE**
> 官方提供了现成的多种格式的虚拟机镜像*，下载†完成后，将镜像导入虚拟机，就可以跳过安装环节，直接学习后续内容。
>
> *不同的虚拟机需要的镜像格式不同，Qemu 选择后缀名 qcow2，Vmware 或 VirtualBox 选择后缀名 vmdk
> †下载地址：mirrors.ustc.edu.cn/freebsd/releases/VM-IMAGES/12.0-RELEASE/amd64/Latest/

国内访问官网比较慢，建议从中科大镜像站下载系统安装盘。

FreeBSD 的安装过程非常简洁，按照向导一步步操作即可，初次操作可以全部使用默认选项。如有不解，可登陆西门课堂的 B 站主页观看视频教程，或与西门老师微信交流。

1.2 用户管理

1.2.1 交互式

增删用户

```
# 这两个命令会一项一项提示需要填写或选择的内容
# 最后还会弹出一个结果预览界面，以供确认是否执行
adduser
rmuser
```

修改用户属性

```
# 如果不指定用户名，默认修改当前用户自己的信息
# 这个命令会弹出一个文本编辑界面，保存退出后会批量应用更改的内容
# 默认启动的编辑器是vim
chpass [username]
```

1.2.2 命令式

pw 是 FreeBSD 下用户管理的高级通用工具[①]，提供了各种细化的配置选项，接下来给出几个常用功能的示例。

[①]功能相当于 Linux 下 useradd + userdel + usermod 三者的综合

添加用户或组

```
# -n 指定用户名，-u 指定 UID，-c 指定备注信息，-s 指定登陆 SHELL
# -w 表示初始密码设定策略，可选值有 yes(密码与用户名相同)、random(密码随机)等
# -G 将新用户加入 wheel、sshd 两个用户组，-m 表示创建家目录
pw useradd [-n] zhangsan -u 20000 -c 张三 -s /bin/sh -w random -G wheel,sshd -m

# -M 指定组成员
pw groupadd [-n] mygrp -g 20000 -M zhangsan,lisi,wangwu
```

查看用户或组信息

```
# -n 选项接受用户名或 UID为参数，用于标识要操作的用户，并且是可以省略的
# 后续命令的 -n 选项含义，均与此相同
# -P 以人类宜读的形式打印信息
# -a 显示所有用户的信息
pw usershow [-n] zhangsan -P
pw usershow -a

# -n 指定组名或 GID
pw groupshow [-n] wheel -P
pw groupshow -a
```

删除用户或组

```
# -r 表示同时删除用户家目录
pw userdel zhangsan -r
pw userdel 20000 -r

pw groupdel video
```

更改用户或组的属性

```
# 除 -n 外，其它选项都是用于指定要更改的内容，含义大多与添加用户时是一样的
# 比较特别是 -l 选项，用于指定新的用户名
pw usermod zhangsan -u 30000 -d /tmp/lisi -g sshd -G video,audio -s /bin/csh
pw usermod 20000 -l lisi -c 李四

# -g 指定新的 GID，-l 指定新的组名，-d 指定要删除的组成员
pw groupmod video -g 30000 -l VIDEO -d zhangsan,lisi
```

锁定与解锁用户

```
# 锁定之后无法登陆，解锁之后恢复登陆
pw lock zhangsan
pw unlock zhangsan
```

1.3 软件管理

1.3.1 启用国内软件源

顺序执行如下命令，启用中科大软件源：

```
# pkg 源
mkdir -p /usr/local/etc/pkg/repos
cd !$
cat<<!>FreeBSD.conf
FreeBSD: { url: "pkg+http://mirrors.ustc.edu.cn/freebsd-pkg/${ABI}/quarterly" }
!

# port 源
cat<<!>/etc/make.conf
MASTER_SITE_OVERRIDE?=http://mirrors.ustc.edu.cn/freebsd-ports/distfiles/${DIST_SUBDIR}
!
```

1.3.2 pkg 方式

直接下载安装已经编译好的二进制包[②]，常用操作如下：

pkg install <pkg name>	安装
pkg delete <pkg name>	卸载
pkg autoremove	清理
pkg -N	统计已安装的非系统包数量
pkg info	列出所有已安装的非系统包
pkg info <pkg name>	显示指定包的详细信息
pkg which <file path>	查询指定文件来源于哪个包
pkg check -s -a|<pkg name>	检查包的完整性（checksum）
pkg check -d -a|<pkg name>	检查并自动安装缺失的依赖包
pkg audit	对所有软件包进行安全审计

1.3.3 port 方式

从源码编译安装[③]，常用操作如下：

portsnap fetch	下载最新的源码库快照
portsnap extract	展开快照，仅在首次同步快照时需要
portsnap update*	更新本地仓库快照
make config†	配置编译选项
make [-jN] install	[N 路并行] 编译安装
make clean‡	清理临时文件
make deinstall	卸载
make reinstall	重装

*通常合并执行：portsnap fetch [extract] update

†执行任何 make 命令之前，需要首先切换到目标软件的源码路径

‡通常合并执行：make [-j5] install clean

[②]类似于 Ubuntu Linux 的 apt

[③]类似于 Gentoo Linux 的 emerge

1.3.4 系统自身更新

小版本更新

使用 GENERIC 内核的情况下，更新系统非常简单，执行 `freebsd-update fetch install` 即可；使用自定义内核的情况下，需要在更新完毕后重新编译内核。

大版本更新

生产环境中极少在既有系统之上进行操作系统的大版本更新，此处就不做无谓的论述了，有兴趣的同学可以参看官方文档。

1.4 服务管理

1.4.1 配置文件

服务管理的配置文件有三个：

/etc/rc.conf.local	优先级最高
/etc/rc.conf	优先级中等
/etc/default/rc.conf	优先级最低

在其中以 `<服务名称>_enable="YES"` 的格式写入，即表示开机启动某服务。

1.4.2 手动启停

已设置随机启动的服务

```
service <服务名称> start
service <服务名称> restart
service <服务名称> stop
```

未设置随机启动的服务

```
# 临时服务，即非随机启动的服务
# 其所有的子命令都需在标准子命令前加 one 前缀
service <服务名称> onestart
service <服务名称> onerestart
service <服务名称> onestop
```

1.4.3 自定义服务

为非系统服务设置开机启动，通常有两种方式：

- 在 /etc/rc.local 中追加指定服务的启动命令[4]
- 在 /usr/local/etc/rc.d 中放置自定义的服务管理脚本

[4] 已废弃但目前仍然可用，不推荐

第一种方式是几乎所有类 UNIX 系统都支持或曾经支持的传统启动方式，目前在 FreeBSD 和大多数 Linux 发行版中都处于“已废弃但仍然可用”的状态；这里重点讲一下第二种方式中提到的服务管理脚本的书写格式，样板示例[5]如下：

```
#!/bin/sh

######## 注意!!! 以下两行内容不是注释 ########
# PROVIDE: <服务名称>
# REQUIRE: <必须在这之前启动的服务列表，逗号分割>

# 服务名称，如 "sshd"
name="<服务名称>"

# 指定用于 /etc/rc.conf.local 等配置文件中的开机启动語法
# 如：此处 $name 设置为 sshd，则自启语法就是 sshd_enable="YES"
rcvar=${name}_enable

# 如： /usr/local/bin/sshd
command="<可执行文件的路径>"

# 可选：指定服务的 pid 文件存储路径，方便管理
# pidfile="<pid 路径>"

# 除 start/restart/onestart/onrestart/stop 等系统预置的子命令外，
# 在此列出用户自定义的其它子命令名称，以空格分割
extra_commands="<自定义子命令-1> <自定义子命令-2>"

# 用户自定义的子命令的具体实现，有两种方式：
# - 比较简单的直接在参数中写内容
# - 相对复杂的在参数中写自定义的函数的名称，并在之后实现该函数
<自定义子命令-1>_cmd="echo Hello World"
<自定义子命令-2>_cmd="do_<自定义子命令-2>"

do_<自定义子命令-2>() {
    echo "Hello World Again"
}

# 以下三项为固定格式，用于设置系统预定义的环境
. /etc/rc.subr
load_rc_config $name
run_rc_command "$1"
```

1.5 网络配置

1.5.1 地址与路由

手动管理

[5] 具体到某个服务的实际启动脚本，可以到 /etc/rc.d/ 路径下查看

```
# 查看已建立的网络连接与服务端口
sockstat -c
sockstat -4 # IPV4
sockstat -6 # IPV6

# 设置 IP
ifconfig <网卡名称> 192.168.1.99 netmask 255.255.225.0

# 配置路由
route show 172.16.10.0                      # 显示指定网络的路由信息
route add -net 172.16.10.0/24 172.16.1.1    # 为特定网络设定静态路由
route add -net 0.0.0.0/0 192.168.1.1        # 设置默认路由
route add default 192.168.1.1               # 设置默认路由，简短语法
route change -net 172.16.10.0/24 172.16.1.2 # 更改静态路由
route delete -net 172.16.10.0/24 172.16.1.2 # 删除网络的指定路由
route flush                                 # 删除本机所有路由信息
```

配置文件

也可以写在 rc.conf.local 等配置文件中，具体写法man rc.conf(5)[6]。

1.5.2 FTP

ftpd 是 FreeBSD 自带的一个精简实用的 ftp 服务器[7]。

```
# 黑名单
echo "root" >> /etc/ftpusers

# 将所有用户锁定在指定目录(/home/ftp)下，禁止查看外部目录結构
echo "@ /home/ftp" >> /etc/ftpchroot

# 开机自启
echo "ftpd_enable="YES"" >> /etc/rc.conf
```

1.5.3 NTP

nfpd 是 FreeBSD 自带的时间同步服务器。

```
# /etc/rc.conf
ntpd_enable="YES"

# /etc/ntp.conf: 用于陈列上游 NTP 服务器地址
server    ntp1.nl.net
```

[6]快速定位至网络配置，在手册中搜索 network_interfaces

[7]如果名称为 ftp 的用户存在，且不在黑名单中，则任意用户可使用 ftp 匿名登陆服务器，可见范围被限制在 ftp 的家目录下

1.6 桌面环境

FreeBSD 总体来说不适合用作通用的桌面环境，其对新硬件的支持速度远落后于 Windows、Linux 等系统，桌面软件的数量也较少。

但如果需要的仅仅是一个极简的高效开发环境，那么前面所说的缺点，反而会成为优点，因为太多花里胡哨的东西，只会对你造成干扰。

以下是 Intel 平台安装 xfce 桌面的简单示例：

```
# 安装基本环境
pkg install xorg xfce

# 确保开机加载声卡与显卡驱动
cat<<!>>/boot/loader.conf
snd_hda_load="YES"
i915kms_load="YES"
!

# 不安装窗口管理器，直接使用 startxfce4 启动桌面
echo ". /usr/local/etc/xdg/xfce4/xinitrc" > ~/.xinitrc

# 中文字体
mkdir -p /usr/local/share/fonts/extra_fonts_dir
cd !$
cp -R <你的字体文件存储路径>/* ./
mkfontdir && mkfontscale && fc-cache -fv

# 安装你需要的应用软件
pkg install ibus ibus-table firefox-esr cmake vim ...

# 使用桌面环境的用户需要加入 video 组
pw groupmod video -m <你的用户名>

# 从命令行终端启动桌面
startx
```

Chapter 2

进阶篇

鉴于近期事务繁杂，时间精力有限，进阶篇相关内容，请直接参看官方 HandBook。

Appendices

.1 Qemu/KVM 启动脚本

```
#!/usr/bin/env bash
ifname="enp5s0"             # 宿主机端口名称
br_name="br0"               # 虚拟网桥名称
br_addr="192.168.1.100/24"  # 给虚拟网桥配置的 IP
br_rtaddr="192.168.1.1"     # 虚拟网桥的网关 IP

iso_path="/tmp/FreeBSD.iso" # 安装盘存放路径
vm_path="/tmp/qemu"         # 虚拟机路径
vm_disk="disk.qcow2"        # 虚拟硬盘文件名

# 配置虚拟网桥
ip link del $br_name 2>/dev/null
ip link add $br_name type bridge || exit 1
ip link set $br_name up || exit 1
ip addr add $br_addr dev $br_name || exit 1
ip route replace default via $br_rtaddr dev $br_name || exit 1
ip addr flush dev $ifname || exit 1
ip route flush dev $ifname || exit 1
ip link set $ifname master $br_name || exit 1

# 按需创建虚拟机路径并进入
mkdir -p $vm_path || exit 1
cd $vm_path || exit 1

# tap 形式联网需要一个回调脚本
echo "#!/usr/bin/env bash
      ip link set \$1 up && sleep 0.1s;
      ip link set \$1 master $br_name" > tap.sh
chmod +x tap.sh

# 按需创建虚拟硬盘
if [[ 0 -eq `find . -name $vm_disk -type f | wc -l` ]]; then
    qemu-img create -f qcow2 -o size=20G disk.qcow2 || exit 1
fi

# 启动虚拟机，参数含义 man qemu-system-x86_64(1)
qemu-system-x86_64 -smbios type=0,uefi=on -enable-kvm \
    -machine q35,accel=kvm -device intel-iommu \
    -cpu host -smp 4,sockets=4,cores=1,threads=1 \
    -m 4096 \
    -netdev tap,ifname=tap0,script=tap.sh,id=vmNic -device virtio-net-pci,netdev=vmNic \
    -drive file=${vm_path}/${vm_disk},if=none,cache=writeback,id=vmDisk -device virtio-
        blk-pci,drive=vmDisk \
    -drive file=${iso_path},readonly=on,media=cdrom \
    -boot order=cd \
    -name vmFreeBSD \
    -display curses
```