牛犇

学习资料链接地址：

正式课程笔记：码云

https://gitee.com/niubenlinux/nsd2010

**一、环境准备**

还原快照网络配置完成，开启虚拟机A与虚拟机B

**二、常用的网络工具**

* **ip命令**

1.查看IP地址

]# ip address show

]# ip a s

2.添加IP地址

]# ip address add 192.168.10.1/24 dev eth0

]# ip a s

]# ip address add 192.168.20.1/24 dev eth0

]# ip a s

* **ping 命令，测网络连接**
  + 选项 -c 包个数

[root@svr7 ~]# ping -c 2 192.168.4.7

[root@svr7 ~]# ping -c 3 192.168.4.207

三、源码编译安装

RPM包：rpm -ivh yum install

源码包---开发工具--->可以执行的程序--->运行安装

* 主要优点
  + 获得软件的最新版，及时修复bug
  + **软件功能可按需选择/定制**，有更多软件可供选择
  + 源码包适用各种平台
  + ……
* **将真机的tools.tar.gz传递数据到虚拟机A**



[root@svr7 ~]# ls /root

**tools.tar.gz**  下载

公共 音乐

[root@svr7 ~]#

源码编译安装步骤：

步骤一:安装开发工具

]# yum -y install make

]# yum -y install gcc

]# rpm -q gcc #检测是否安装成功

]# rpm -q make #检测是否安装成功

步骤二:进行tar解包

]# tar -xf /root/tools.tar.gz -C /usr/local/

]# ls /usr/local/

]# ls /usr/local/tools/

]# tar -xf /usr/local/tools/inotify-tools-3.13.tar.gz -C /usr/local/

]# ls /usr/local/

步骤三：运行configure脚本进行配置

作用1：检测系统是否安装gcc

作用2：可以指定安装位置及功能

]# cd /usr/local/inotify-tools-3.13/

]# ./configure --prefix=/opt/myrpm #**指定安装位置**

常见错误：没有安装gcc

checking for gcc... no

checking for cc... no

checking for cl.exe... no

configure: error: no acceptable C compiler found in $PATH

See `config.log' for more details.

步骤四：make进行编译，产生可以执行的程序

]# cd /usr/local/inotify-tools-3.13/

]# **make**

步骤五：make install进行安装

]# cd /usr/local/inotify-tools-3.13/

]# **make install**

]# ls /opt/

]# ls /opt/myrpm/

]# ls /opt/myrpm/bin/

**四、日志管理**

* 系统和程序的“日记本”
  + 记录系统、程序运行中发生的各种事件
  + 通过查看日志，了解及排除故障
  + 信息安全控制的“依据”
* 由系统服务rsyslog统一记录/管理
  + 日志消息采用文本格式
  + 主要记录事件发生的时间、主机、进程、内容
* 常见的日志文件

|  |  |
| --- | --- |
| **日志文件** | **主要用途** |
| /var/log/messages | 记录内核消息、各种服务的公共消息 |
| /var/log/dmesg | 记录系统启动过程的各种消息 |
| /var/log/cron | 记录与cron计划任务相关的消息 |
| /var/log/maillog | 记录邮件收发相关的消息 |
| /var/log/secure | 记录与访问限制相关的安全消息 |

* 通用分析工具
  + tail、tailf、less、grep等文本浏览/检索命令
  + awk、sed等格式化过滤工具

tailf：实时跟踪

[root@svr7 /]# echo 123456 > /opt/1.txt

[root@svr7 /]# tailf /opt/1.txt

* users、who、w 命令
  + 查看已登录的用户信息，详细度不同
* last、lastb 命令
  + 查看最近登录成功/失败的用户信息

[root@svr7 /]# users

[root@svr7 /]# who

pts：图形命令行终端

[root@svr7 /]# last #登录成功的用户

[root@svr7 /]# lastb #登录失败的用户

* Linux内核定义的事件紧急程度
  + **分为 0~7 共8种优先级别**
  + **其数值越小**，表示对应事件越紧急/重要

0 EMERG（紧急） 会导致主机系统不可用的情况

1 ALERT（警告） 必须马上采取措施解决的问题

2 CRIT（严重） 比较严重的情况

3 ERR（错误） 运行出现错误

4 WARNING（提醒） 可能会影响系统功能的事件

5 NOTICE（注意） 不会影响系统但值得注意

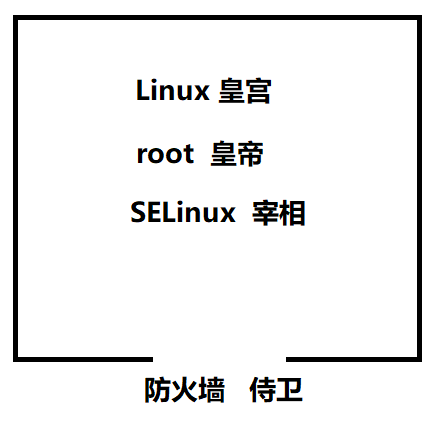
6 INFO（信息） 一般信息

7 DEBUG（调试） 程序或系统调试信息等

**五、系统安全保护**

**SELinux概述**

* Security-Enhanced Linux
  + 美国NSA国家安全局主导开发，一套增强Linux系统安全的强制访问控制体系
  + 集成到Linux内核（2.6及以上）中运行
  + RHEL7基于SELinux体系针对用户、进程、目录和文件提供了预设的保护策略，以及管理工具



* SELinux的运行模式
  + enforcing（强制）、permissive（宽松）
  + disabled（彻底禁用）

任何模式变成disabled模式，都要经历重启系统

* 切换运行模式
  + 临时切换：setenforce 1或0
  + 固定配置：/etc/selinux/config 文件

虚拟机A

[root@svr7 /]# getenforce #查看当前运行模式

Enforcing

[root@svr7 /]# setenforce 0 #修改当前运行模式

[root@svr7 /]# getenforce

Permissive

[root@svr7 /]# vim /etc/selinux/config

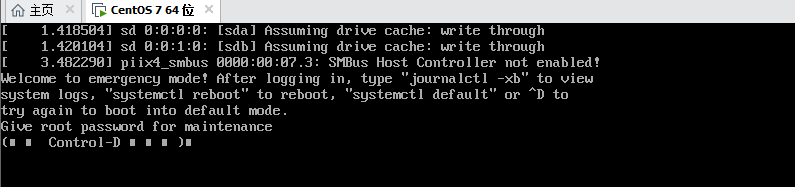
SELINUX=permissive

虚拟机B：同上

**六、系统故障修复**

* **如果/etc/fstab文件有误：修复办法**

1.输入root的密码



2.修改/etc/fstab文件内容

C:\Users\Python\AppData\Local\YNote\data\niubenlinux@163.com\09244c1a8bf449adaa13909084ae7e78\clipboard.png

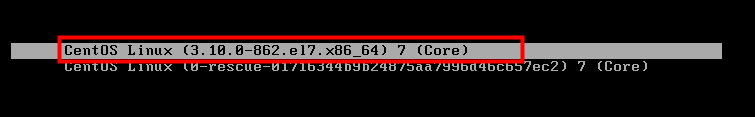
* **破解密码思路**

前提：必须是服务器的管理者，涉及重启服务器

1)**重启系统**,进入 恢复模式

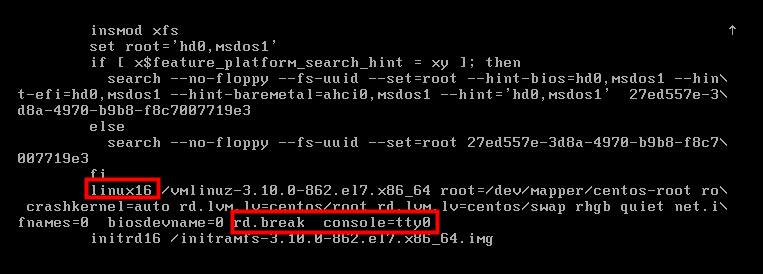
[root@A ~]# reboot

开启虚拟机A，在此界面按e键



找到linux16该行

在linux16该行的最后，空格输入 **rd.break console=tty0**



按 **ctrl + x** 启动，会看到switch\_root#

2)以可写方式重新挂载 /,并切换到此环境

# **chroot  /sysroot** #切换环境，切换到硬盘操作系统的环境

# **mount  -o  remount,rw   /**  #让根目录下所有数据，可以读也可以写入

3)重新设置root的密码

sh-4.2# **echo 1 | passwd --stdin  root**

4)如果SELinux是强制模式，才需要重设SELinux策略（其他模式不需要做此操作）

sh-4.2# vim /etc/selinux/config #查看SELinux开机的运行模式

sh-4.2# touch  /.autorelabel #让SELinux失忆

5)强制重启系统完成修复

sh-4.2# reboot -f

**七、构建基本服务**

* **构建Web服务**

Web服务：提供一个页面内容的服务

提供Web服务的软件：httpd、Nginx、tomcat

http协议：超文本传输协议

daemon

英 [ˈdiːmən] 美 [ˈdiːmən]

n.(古希腊神话中的)半神半人精灵

虚拟机A：

1.安装软件包

[root@svr7 ~]# yum -y install httpd

2.运行提供Web服务程序

]# > /etc/resolv.conf #清空此文件内容

]# /usr/sbin/httpd #绝对路径运行程序

]# pgrep -l httpd #查看进程信息

4.书写一个页面文件

[root@svr7 ~]# vim /var/www/html/index.html

NSD2010哈哈徐徐阳光明媚

5.浏览器访问测试

[root@svr7 ~]# firefox & #放入后台运行

[root@svr7 ~]# curl http://192.168.4.7

NSD2010哈哈徐徐阳光明媚

* **构建FTP服务**

FTP：文本传输协议

实习FTP服务功能的软件：vsftpd

默认共享数据的主目录：/var/ftp/

虚拟机A

1.安装软件包

[root@svr7 ~]# yum -y install vsftpd

2.运行程序

[root@svr7 ~]# /usr/sbin/vsftpd

3.访问测试

[root@svr7 ~]# curl ftp://192.168.4.7

**八、防火墙的策略管理**

作用：隔离，严格过滤入站，放行出站

硬件防火墙

软件防火墙

* 系统服务：firewalld
* 管理工具：firewall-cmd、firewall-config
* 根据所在的网络场所区分，预设保护规则集
  + public：仅允许访问本机的ssh、dhcp、ping服务
  + trusted：允许任何访问
  + block：拒绝任何来访请求，明确拒绝客户端
  + drop：丢弃任何来访的数据包，不给任何回应

课间休息：17:15上课