一、环境准备

还原快照（xshell完成），开启虚拟机A与虚拟机B

二、服务器之间传递数据

•安全复制工具 scp（基于ssh远程管理）

–scp  [-r]  用户名@服务器:路径  本地路径

–scp  [-r]  本地路径  用户名@服务器:路径

虚拟机A：

[root@svr7 ~]# scp /etc/passwd root@192.168.4.207:/root/

[root@svr7 ~]# scp -r /home/ root@192.168.4.207:/opt/

[root@svr7 ~]# scp root@192.168.4.207:/etc/yum.repos.d/mydvd.repo /root

[root@svr7 ~]# ls /root/

虚拟机B：

[root@pc207 ~]# ls /root

[root@pc207 ~]# ls /opt

三、网络管理的工具

•查看IP地址

[root@svr7 ~]# ip address show

[root@svr7 ~]# ip a s #支持命令的缩写

2: eth0:

inet 192.168.4.7/24

•临时为一张网卡添加多个IP地址

[root@svr7 ~]# ip address add 192.168.8.1/24 dev eth0

[root@svr7 ~]# ip address show

•ping 命令，测网络连接，选项 -c 包个数

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

四、自定义Yum仓库

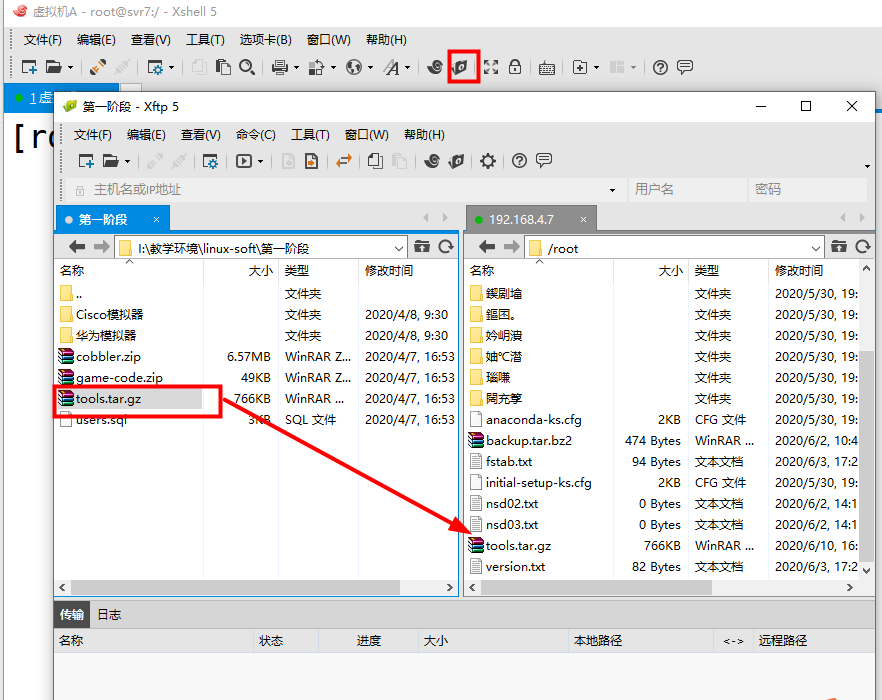
•将自己下载的RPM包构建为仓库

•下载 第一阶段 tools.tar.gz 软件资料：

链接：https://pan.baidu.com/s/1WK9orwEWh1R\_WVQgP0KWvA

提取码：yn45

•由真机将tools.tar.gz传递到虚拟机A的/root目录下



[root@svr7 ~]# ls /root

[root@svr7 ~]# tar -xf /root/tools.tar.gz -C /

[root@svr7 ~]# ls /

[root@svr7 ~]# ls /tools/

[root@svr7 ~]# ls /tools/other/

[root@svr7 ~]# createrepo /tools/other/ #生成仓库数据文件

[root@svr7 ~]# ls /tools/other/

[root@svr7 ~]# vim /etc/yum.repos.d/mydvd.repo

[mydvd]

name=centos7

baseurl=file:///mydvd

enabled=1

gpgcheck=0

[rpm] #唯一标识

name=myrpm

baseurl=file:///tools/other #指定Yum仓库的路径

enabled=1

gpgcheck=0

[root@svr7 ~]# yum repolist

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

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

五、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：实时跟踪日志消息

•users、who、w 命令

–查看已登录的用户信息，详细度不同

pts：图形命令行终端

[root@svr7 ~]# users

[root@svr7 ~]# who

[root@svr7 ~]# w

•last、lastb 命令

–查看最近登录成功/失败的用户信息

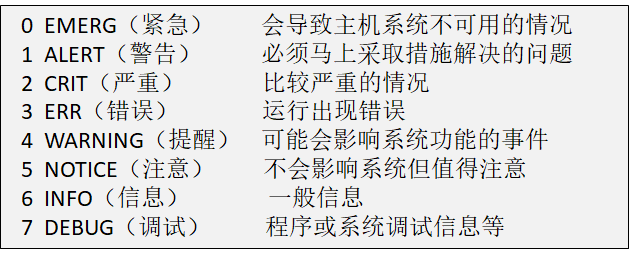
[root@svr7 ~]# last -2 #最近登录成功两条信息

[root@svr7 ~]# lastb -2 #最近登录失败两条信息

•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



•提取由 systemd-journal 服务搜集的日志

–主要包括内核/系统日志、服务日志

•常见用法

–journalctl  |  grep  关键词

–journalctl  -u  服务名  [-p  优先级]

–journalctl  -n  消息条数

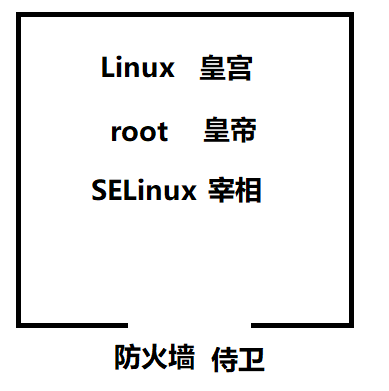
六、SELinux系统防护

•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）

任何默认变成disabled（彻底禁用）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 #每次开机读取模式文件

虚拟机A：

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

SELINUX=permissive

[root@svr7 ~]# getenforce #查看SELinux运行模式

Enforcing

[root@svr7 ~]# setenforce 0 #修改当前SELinux运行模式

[root@svr7 ~]# getenforce

Permissive

虚拟机B：同上

七、遗忘root用户密码（破解Linux系统root的密码）

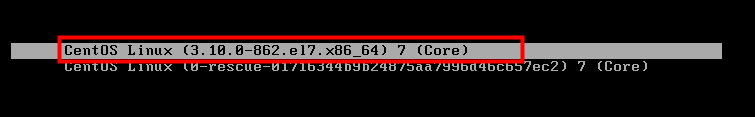
前提：必须是服务器的管理者，涉及重启服务器

破解密码思路

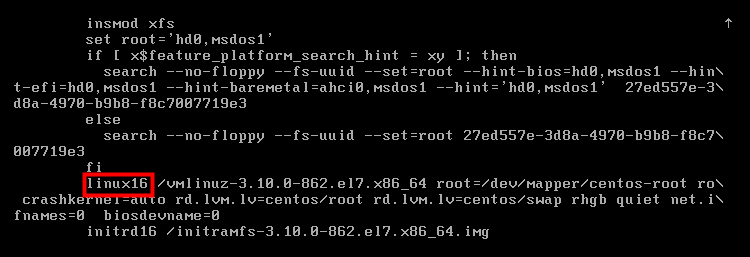
1)**重启系统**,进入 恢复模式

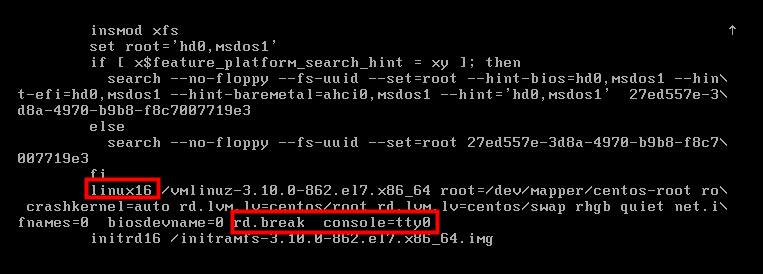
[root@A ~]# reboot

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

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

sh-4.4# 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-4.4# 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-4.4# vim /etc/selinux/config #查看SELinux开机的运行模式

sh-4.4# touch  /.autorelabel #让SELinux失忆

5)强制重启系统完成修复

sh-4.4# reboot -f

八、构建基本的Web服务

Web服务：提供页面内容

Web服务器：提供页面内容的机器

http协议：超文本传输协议

https协议：安全的超文本传输协议

虚拟机A：

1.安装可以提供Web服务功能的软件（httpd、Nginx、Tomcat）

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

[root@svr7 ~]# rpm -q httpd

httpd-2.4.6-80.el7.centos.x86\_64

[root@svr7 ~]#

2.运行httpd程序

[root@svr7 ~]# vim /etc/resolv.conf #清空文件所有内容

[root@svr7 ~]# /usr/sbin/httpd #运行程序

[root@svr7 ~]# killall httpd #停止程序

[root@svr7 ~]# /usr/sbin/httpd #以绝对路径方式运行程序

[root@svr7 ~]# pstree | grep httpd #查看进程信息

|-httpd---5\*[httpd]

3.本机测试（书写自己的页面）

]# vim /var/www/html/index.html #默认存放网页文件的路径

人在塔在！王者归来！

]# curl http://192.168.4.7 #curl为非图形的浏览器

人在塔在！王者归来！

九、防火墙策略管理

作用：隔离 ，严格过滤入站，放行出站

硬件防火墙：保护一个网络中所有的机器

软件防火墙：保护主机本身

•系统服务：firewalld（Linux防火墙软件）

•管理工具：firewall-cmd（命令）、firewall-config（图形）

•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等服务，其他都拒绝

–trusted：允许任何访问

–block：拒绝任何来访请求，会回应客户端

–drop：丢弃任何来访的数据包，不会回应客户端

•防火墙判断进入区域的原则

1.查看客户端请求中源IP地址，然后查看所有区域中规则，那个区域有该源IP地址的规则，则进入该区域

2.进入默认区域（默认情况下为public）

•防火墙默认区域的修改

虚拟机A

]# killall firewalld

]# pstree | grep firewalld #查看防火墙进程信息

|-firewalld---{firewalld}

]# /usr/sbin/firewalld #绝对路径运行

]# firewall-cmd --get-default-zone #查看默认区域

虚拟机B

]# curl http://192.168.4.7 #访问失败

虚拟机A

]# firewall-cmd --set-default-zone=trusted #修改默认区域

]# firewall-cmd --get-default-zone

虚拟机B

]# curl http://192.168.4.7 #访问成功

•防火墙区域中添加规则

虚拟机A：

]# firewall-cmd --set-default-zone=public

]# firewall-cmd --get-default-zone

虚拟机B：

]# curl http://192.168.4.7 #访问失败

虚拟机A：

]# firewall-cmd --zone=public --add-service=http #添加允许协议

]# firewall-cmd --zone=public --list-all #查看区域规则

虚拟机B：

]# curl http://192.168.4.7 #访问成功

•防火墙区域中添加规则，实现永久规则

–命令的选项永久（--permanent）

虚拟机A

]# firewall-cmd --zone=public --list-all

]# firewall-cmd --zone=public --remove-service=http #删除

]# firewall-cmd --zone=public --list-all

]# firewall-cmd --permanent --zone=public --add-service=http

]# firewall-cmd --zone=public --list-all

]# firewall-cmd --reload #重新加载所有永久规则，实现当前生效

•防火墙单独拒绝虚拟机B所有访问，其他机器可以访问（了解）

]# firewall-cmd --zone=block --add-source=192.168.4.207

]# firewall-cmd --zone=block --list-all

课后习题：

案例1：设置SELinux保护

为虚拟机A、虚拟机B 配置SELinux

1）确保 SELinux 处于宽松模式（permissive）

2）在每次重新开机后，此设置必须仍然有效

案例2：实现虚拟机A 的Web服务

1）利用httpd软件搭建Web服务，页面显示内容为 小蝌蚪找妈妈

案例3：实现虚拟机A 的防火墙配置

1）修改虚拟机A防火墙配置，明确拒绝所有客户端访问（默认区域修改为block）

2）在虚拟机B上,测试能否访问虚拟机A 的Web服务

3）在虚拟机B上,测试能否 ping通 虚拟机A

案例4：实现虚拟机A 的防火墙配置

1）修改虚拟机A防火墙配置，将默认区域修改为public

2）在虚拟机B上,测试能否访问虚拟机A 的Web服务

3）在虚拟机B上,测试能否 ping通虚拟机A

案例5：实现虚拟机A的防火墙配置

1）修改虚拟机A防火墙配置，将默认区域修改为public

2）修改虚拟机A永久的防火墙配置，在public区域中添加http协议

3）在虚拟机B上,测试能否访问虚拟机A的Web服务