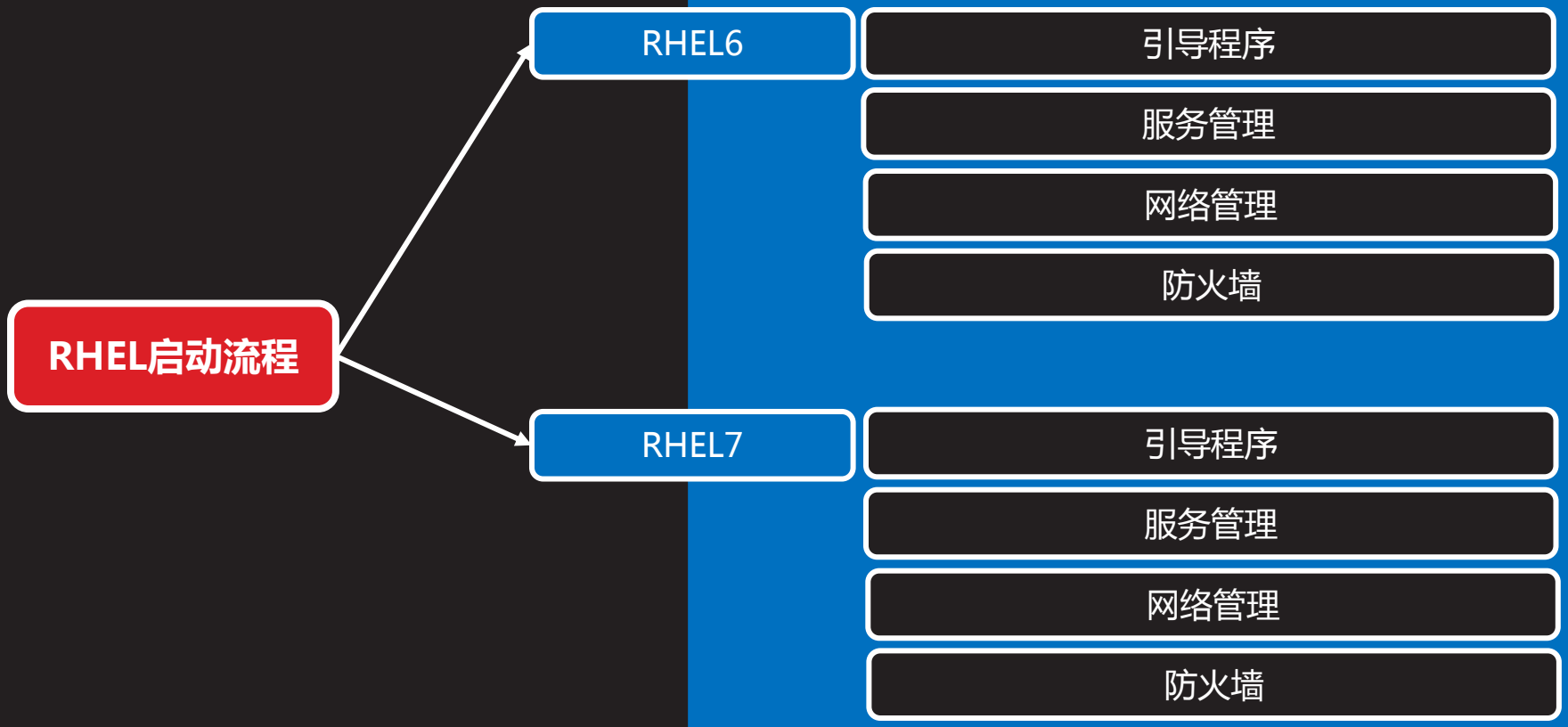
Linux 拓展

Redhat 6 vs 7

内容

上午	09:00 ~ 09:30	概述
	09:30 ~ 10:20	Init/systemd
	10:30 ~ 11:20	
	11:30 ~ 12:20	网络及防火墙
下午	14:00 ~ 14:50	
	15:00 ~ 15:50	服务管理
	16:00 ~ 16:50	
	17:00 ~ 17:30	总结和答疑

概述



Tedu.cn
达内教育

引导程序

引导程序

- RHEL6 使用 grub 引导程序
- RHEL7 使用 grub2
  - GRUB 2比之前的GRUB更强大
  - GRUB 2支持BIOS，EFI和OpenFiremware
  - GRUB 2支持MBR分区表和GPT分区表
  - GRUB 2甚至支持非Linux文件系统，如NTFS等
  - GRUB 2 的配置也更加复杂，学习成本也更高

知识讲解

Tedu.cn
达内教育

配置文件

简介

- GNU GRUB
  - 是一个来自GNU项目的启动引导程序，它允许用户可以在计算机内同时拥有多个操作系统，并在计算机启动时选择希望运行的操作系统
- GRUB版本
  - 目前GRUB分成GRUB legacy和GRUB 2，版本号是0.9x以及之前的版本都称为GRUB Legacy ，从 1.x 开始的就称为GRUB 2

知识讲解

主配置文件

- GRUB默认配置文件
  - /boot/grub2/grub.conf
- 更行GRUB配置文件
  - grub2-mkconfig -o /boot/grub2/grub.cfg
- 重新安装GRUB
  - grub2-install /dev/sda

知识讲解

手动引导

知识讲解

- grub> set root=(hd0,msdos1)

  //设置根目录为第一硬盘的第一个分区

- grub> linux /boot/vmlinuz

  //设置内核文件

- grub> initrd /boot/initrd

  //设置initrd文件，也有可能用软连接

- grub> boot 从硬盘启动

  //boot从硬盘启动

Tedu.cn
达内教育

引导启动参数

救援模式

- 系统启动时按下e键编辑菜单
  - Ctrl+a定位光标到行首
  - Ctrl+e定位光标到行尾
  - Esc退出，不保存
- 救援模式主要用来修改系统
  - 加载本地文件系统
  - 启动重要的服务
  - 不加载网络
  - 不允许其他用户登录
  - 参数：systemd.unit=rescue.target

知识讲解

急救模式

- 急救模式仅提供最小的系统环境
  - 仅挂载根文件系统
  - 不加载网络
  - 启动少数必须的服务
  - 参数：systemd.unit=emergency.target

知识讲解

图形模式

- 图形模式提供完整的图形系统环境
  - 挂载所有文件系统
  - 加载网络
  - 启动所有被设置为开机启动的服务
  - 参数：systemd.unit=graphical.target

知识讲解

引导参数

- GRUB2与GRUB的区别：
  - grub 的引导菜单是通过 menu.1st 配置的
  - GRUB2 引导菜单启动项是使用命令自动生成的
  - 分区编号发生变化：第一个分区现在是1而不是0，但第一个设备仍然以0开始计数，如hd0
- 例如关闭 selinux
  - 编辑内核参数 selinux=0
  - grub-mkconfig -o /boot/grub/grub.cfg

知识讲解

恢复root密码

知识讲解

- 重启计算机
- 中断启动引导
  - 参数：rd_break console=tty0
- 修改密码
  - mount –o remount,rw /sysroot
  - chroot /sysroot/
  - passwd
- 重置SELinux标签
  - touch /.autorelabel

课堂练习

- 练习 1
- 编辑 RHEL6 的 grub 禁用 selinux
- 编辑 RHEL7 的 网卡命名

- 练习 2
- 破解 RHEL6 的 ROOT 密码
- 破解 RHEL7 的 ROOT 密码

Tedu.cn
达内教育

RHEL6 服务管理

服务分类

- 系统服务
  - 独立监听的、响应速度快、持续占用系统资源
- 临时服务
  - 响应较慢、有访问时启用、更节省资源
- 路径
  - 系统服务（脚本）：/etc/rc.d/init.d/*
  - 临时服务（配置文件）： /etc/xinetd.d/*

知识讲解

查看所有服务

- 列出所有的系统服务（脚本名）

```
[root@svr5 ~]# ls  /etc/init.d/
acpid     hidd              netconsole        rpcidmapd
anacron           ip6tables         netfs             rpcsvcgssd
.. ..
```

- 列出所有的临时服务（配置文件名）

```
[root@svr5 ~]# ls  /etc/xinetd.d/
eklogin     gssftp   krb5-telnet  rmcp    ekrb5-telnet  klogin  kshell
rsync
```

知识讲解

系统服务控制

- 基本方法
  - service 服务名称 控制参数

  或者：/etc/init.d/服务名称 控制参数
- 主要控制参数
  - start：启动
  - stop：停止
  - status：查看服务的当前状态
  - restart：重新启动
  - reload：重新加载配置

系统服务脚本的存放位置

知识讲解

系统服务控制（续1）

知识讲解

```
[root@svr5 ~]# service  autofs  status          //查看状态
automount (pid  3894) 正在运行...

[root@svr5 ~]# service  autofs                  //用法提示
unknown, invalid or excess argument(s)
Usage: /etc/init.d/autofs
{start|forcestart|stop|status|restart|forcerestart|reload|condrestar
t|force-reload|try-restart|usage}

[root@svr5 ~]# service  autofs  restart         //重启服务
停止 automount：                                [确定]
启动 automount：                                [确定]
```

Xinetd 超级服务器

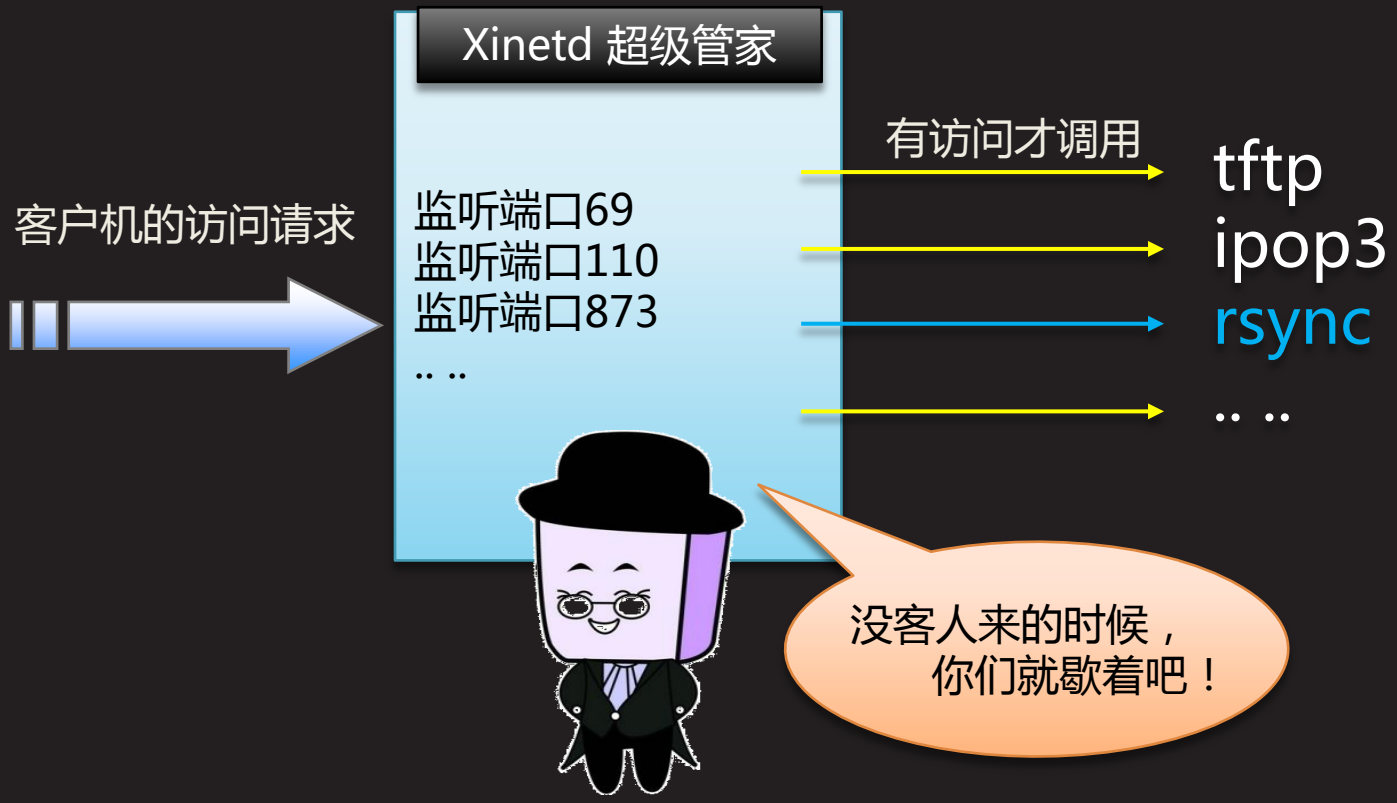
- eXtended InterNET services daemon
  - 超级守护进程、超级服务器
  - 统一管理多个TCP/UDP服务、控制访问权限

```
[root@svr5 ~]# rpm  -qi  xinetd
.. ..
Description :
.. .. Xinetd 让您把指定的服务绑定到您的主机上的指定 IP 编号。每个服
务都有它自己指定的 Xinetd 配置文件，这些文件
位于 /etc/xinetd.d 目录中。
```

知识讲解

Xinetd 超级服务器（续1）

知识讲解



Xinetd 典型配置解析

知识讲解

```
[root@svr5 ~]# vim  /etc/xinetd.d/rsync
service rsync                                   //定义服务名
{
        disable = yes                           //是否禁用
        socket_type     = stream                //套接字类型
        wait            = no                    //yes单线程，no多线程
        user            = root                  //服务的运行身份
        server          = /usr/bin/rsync        //可执行程序路径
        server_args     = --daemon              //执行选项/参数
        log_on_failure  += USERID               //失败时日志补充
}
```

临时服务控制

- 使用 chkconfig 工具
  - 格式：chkconfig 服务名 on|off
  - 相当于改配置文件的 disable 项

```
[root@svr5 ~]# chkconfig  rsync  on              //打开rsync服务
[root@svr5 ~]# chkconfig  --list                  //查看服务开关状态
.. ..
基于 xinetd 的服务：
        rsync:          关闭
        tftp:           关闭

[root@svr5 ~]# service  xinetd  reload          //重载配置
重新载入配置：                                  [确定]
```

知识讲解

临时服务控制（续1）

- 使用 /etc/init.d/xinetd 脚本
  - 若xinetd服务未运行，
  - 则/etc/xinetd.d/下的各配置文件均不生效

```
[root@svr5 ~]# service  xinetd  start
启动 xinetd：                                [确定]
```

知识讲解

服务的自启

设置服务自启状态

- chkconfig 命令行工具
  - 格式：chkconfig --list [服务名]
    chkconfig [--level 级别列表] 服务名 on
    chkconfig [--level 级别列表] 服务名 off

设置单个系统服务时，效率比较高

知识讲解

设置服务自启状态（续1）

- 列出所有服务的自启状态

```
[root@svr5 ~]# chkconfig  --list
acpid          0:off   1:off   2:on    3:on    4:on    5:on    6:off
anacron        0:off   1:off   2:on    3:on    4:on    5:on    6:off
.. ..
```

- 将 iptables 服务的自启设为关闭

```
[root@svr5 ~]# chkconfig  iptables  off
[root@svr5 ~]# chkconfig  --list  iptables
iptables       0:off   1:off   2:off   3:off   4:off   5:off   6:off
```

知识讲解

RHEL 7 特性

文件系统

- 默认使用的文件系统为XFS
  - XFS是一个高性能的大文件系统
  - XFS支持在线调整大小
  - RHEL6 默认 ext4

知识讲解

服务管理

- systemd
  - systemd是linux系统和服务的管理程序
  - systemd用来替代SysV和Upstart
  - systemd兼容于Sysv和基本init脚本
  - systemd提供了并行处理的能力

知识讲解

网络管理

知识讲解

- NetworkManager
  - 支持基本网络配置、虚拟VLAN、bonds、IPv6等功能
  - 可以通过命令行设置
  - 可以通过图形设置
  - 可以通过TUI设置
- network
  - 传统网络管理服务

防火墙

- firewalld
  - 支持zone及动态管理的防火墙守护进程
  - firewall-config：一个图形化管理工具
  - firewall-cmd：一个命令行工具
  - 防火墙规则以XML格式存储在/usr/lib/firewalld

知识讲解

systemd

init程序的作用

- Linux系统和服务管理器
  - 是内核引导之后加载的第一个初始化进程（PID=1）
  - 负责掌控整个Linux的运行/服务资源组合
- 传统的 init 程序风格
  - system v：顺序加载，RHEL6系列采用

知识讲解

systemd

- 一个更高效的系统&服务管理器
  - 开机服务并行启动，各系统服务间的精确依赖
  - 配置目录：/etc/systemd/system/
  - 服务目录：/lib/systemd/system/
  - 主要管理工具：systemctl

```
[root@svr7 ~]# ls  -l  /sbin/init
lrwxrwxrwx. 1 root root 22 12月  7 09:34 /sbin/init ->
 ../lib/systemd/systemd
```

知识讲解

unit配置单元

- 不同的unit决定了一组相关的启动任务
  - service：后台独立服务
  - socket：套接字，类似于xinetd管理的临时服务
  - target：一套配置单元的组合，类似于传统“运行级别”
  - device：对应udev规则标记的某个设备
  - mount、automount：挂载点、触发挂载点
  - .. ..

知识讲解

列出服务

- 列出活动的系统服务
  - systemctl -t service
- 列出所有系统服务（包括不活动的）
  - systemctl -t service --all

```
[root@svr7 ~]# systemctl -t service --all
  UNIT                    LOAD      ACTIVE   SUB     DESCRIPTION
  abrt-ccpp.service       loaded    active   exited  Install ABRT
coredump hoo
  .. ..
  abrt-vmcore.service  loaded    inactive dead    Harvest vmcores
for ABRT
.. ..
```

知识讲解

Tedu.cn
达内教育

管理运行级别

切换级别

- 列出可用运行级别
  - systemctl -t target
- 切换到文本/图形模式
  - systemctl isolate multi-user.target
  - systemctl isolate graphical.target

```
[root@svr7 ~]# systemctl isolate multi-user.target
.. ..
[root@svr7 ~]# runlevel                    //确认结果
5 3                                        //旧级别 当前级别
```

知识讲解

设置默认级别

- 查看默认级别
  - systemctl get-default
- 设置默认级别
  - systemctl set-default multi-user.target
  - systemctl set-default graphical.target

```
[root@svr7 ~]# systemctl set-default multi-user.target
Removed symlink /etc/systemd/system/default.target.
Created symlink from /etc/systemd/system/default.target to
/usr/lib/systemd/system/multi-user.target.

[root@svr7 ~]# systemctl get-default
multi-user.target
```

知识讲解

案例8：使用systemctl工具

通过 systemctl 完成下列任务

1）重启 httpd、crond、bluetooth 服务，查看状态

2）禁止 bluetooth 服务开机自启，并停用此服务

3）设置默认级别为 multi-user.target 并确认

课堂练习

兼容性

- systemd 引入了新的配置方式
- 很多程序并没有来得及为systemd做相应的改变
- systemd提供了和sysvinit兼容的特性
  - 系统中已经存在的服务和进程无需修改
  - 降低了系统向 systemd 迁移的成本
  - 使得systemd替换现有初始化系统成为可能

知识讲解

启动速度

- systemd的设计目标
  - 尽可能启动更少的进程
  - 尽可能将更多进程并行启动
  - 可以实现按需启动

知识讲解

单元的概念

- 启动后台服务、挂载文件系统等都被systemd抽象为一个配置单元，即Unit
- 可以认为一个服务是一个配置单元；一个挂载点是一个配置单元；一个交换分区的配置是一个配置单元

知识讲解

单元的概念（续1）

- 可用的配置单元类型如下
  - service
    代表一个后台服务
  - socket
    代表一个套接字
  - device
    代表一个设备
  - mount
    代表一个挂载点
  - automount
    代表一个自挂载点

知识讲解

单元的概念（续2）

- 可用的配置单元类型如下
  - swap

    交换配置单元用来管理交换分区
  - target

    此类配置单元为其他配置单元进行逻辑组合，它们本身实际上并不做什么，只是引用其他配置单元而已
  - timer

    定时器配置单元用来定时触发用户定义的操作，这类配置单元取代了atd、crond 等传统的定时服务
  - snapshot

    与target配置单元相似，快照是一组配置单元，它保存了系统当前的运行状态

知识讲解

Tedu.cn
达内教育

管理单元

服务管理工具对比

- RHEL6与RHEL7命令对比

知识讲解

传统工具	新工具	描述
service name start	systemctl start name.service	启动服务
service name stop	systemctl stop name.service	关闭服务
service name restart	systemctl restart name.service	重启服务
service name reload	systemctl reload name.service	重新加载配置文件
service name status	systemctl status name.service	查看状态
service --status-all	systemctl list-unit --type service --all	查看所有服务状态

服务管理工具对比（续1）

- RHEL6与RHEL7命令对比

传统工具	新工具	描述
chkconfig name on	systemctl enable name.service	开机启动
chkconfig name off	systemctl disable name.service	开机禁止
chkconfig --list name	systemctl status name.service systemctl is-enabled name.service	查看状态
chkconfig --list	systemctl list-units --type service	列出所有服务状态

知识讲解

开机运行级别

- RHEL7取消了运行级别的概念
- 与而代之的是Target Units
- Target是其他systemd单元的逻辑集合

知识讲解

RHEL6级别	RHEL7 Target Units	描述
0	poweroff.target	关机
1	rescue.target	救援模式
2	multi-user.garget	多用户模式
3	multi-user.garget	多用户模式
4	multi-user.garget	多用户模式
5	graphical.target	图形模式
6	reboot.target	重启

切换运行级别

- RHEL6与RHEL7对比

知识讲解

RHEL6	RHEL7	描述
runlevel	systemctl list-units --type target	查看当前加载的单元
telinit N	systemctl isolate name.target	切换Target Unit
	systemctl get-default	查看默认Target Unit
	systemctl set-default name.target	修改默认Target Unit

Tedu.cn
达内教育

更多操作

其他模式

- 救援模式
  - systemctl rescue
- 应急模式
  - systemctl emergency

知识讲解

电源管理

- RHEL6与RHEL7对比

RHEL6	RHEL7	描述
halt	systemctl halt	关机
reboot	systemctl reboot	重启
pm-suspend	systemctl suspend	暂停系统（保持系统状态到内存）
pm-hibernate	systemctl hibernate	系统休眠（保持系统状态到硬盘）

知识讲解

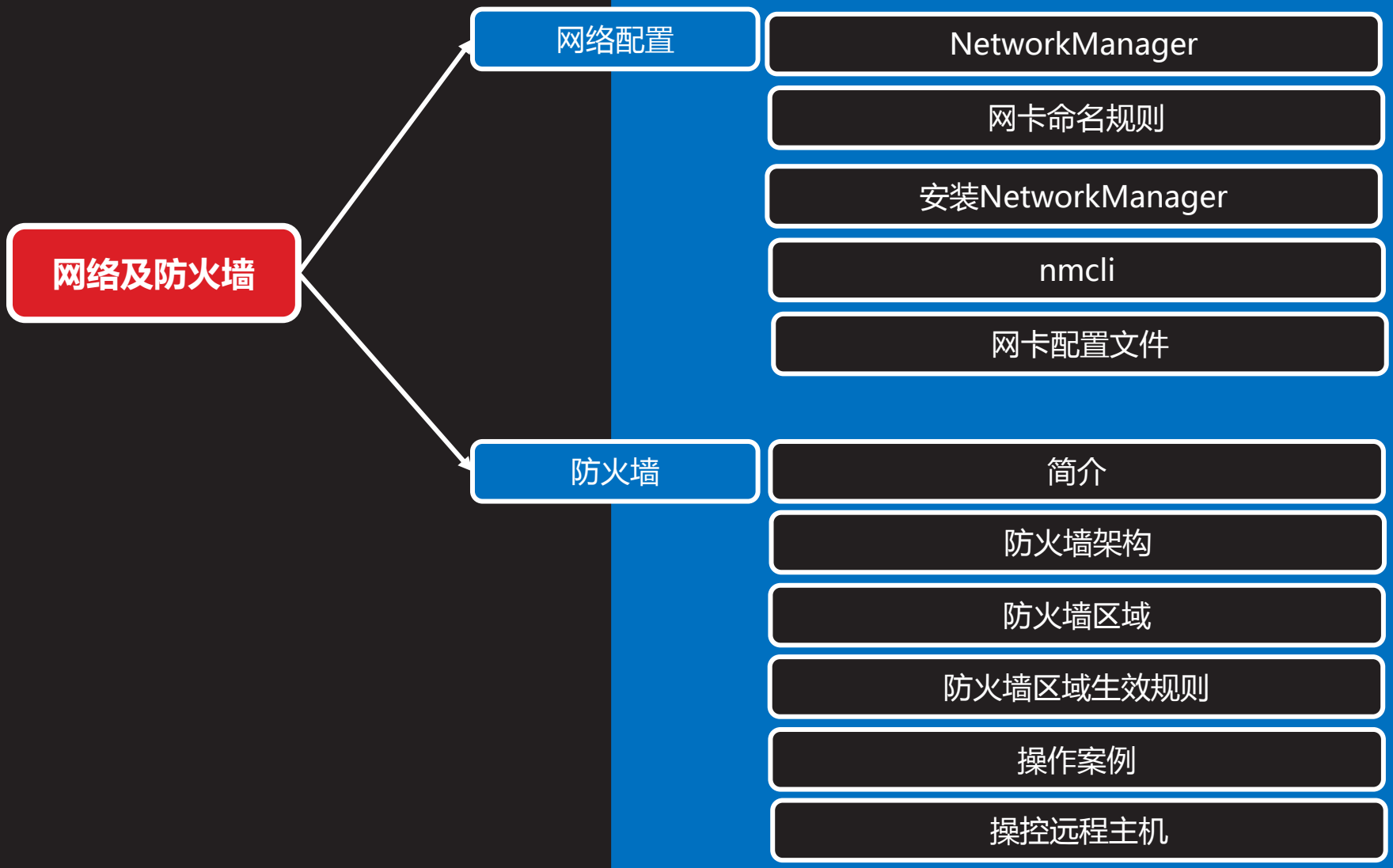
操控远程主机

- systemctl工具支持远程控制
  - 该功能依赖于SSH协议
  - systemctl -H user@hostname command

[root@rhel7 ~]# systemctl -H root@server status httpd.service

知识讲解

网络及防火墙


网络及防火墙
网络配置
NetworkManager
网卡命名规则
安装NetworkManager
nmcli
网卡配置文件
防火墙
简介
防火墙架构
防火墙区域
防火墙区域生效规则
操作案例
操控远程主机

Tedu.cn
达内教育

网络配置

网卡命名规则

- RHEL7采用新的网卡命名规则
  - 集成在主板上的设备，使用BIOS提供的索引编号，如eno1
  - 使用PCI-E的slot编号，如ens1
  - 使用硬件连接器的物理位置，如enp2s0
  - 使用mac地址，如enx78e7d1ea46da
  - 使用传统的方式，如eth0

知识讲解

网卡命名规则（续1）

- 网卡名称的含义：
  - 前两个字母代表网络类型
    - en表示以太网
    - wl表示无线局域网
    - ww表示无线广域网
  - 第三个字符表示设备类型
    - o表示主板设备
    - s表示插槽编号
    - p表示物理位置

知识讲解

NetworkManager

- RHEL7默认网络管理服务为NetworkManager
- 传统的ifcfg类型的配置文件依然被支持
- 新版网络管理工具如下
  - NetworkManager（默认网络服务进程）
  - nmtui（NetworkManager-TUI）
  - nmcli（ NetworkManager命令行工具）
  - control-center（GNOME控制中心）
  - nm-connection-editor（图形化配置工具）

知识讲解

安装NetworkManager

知识讲解

```
[root@rhel7 ~]# yum -y install NetworkManager
[root@rhel7 ~]# systemctl status NetworkManager
[root@rhel7 ~]# systemctl enable NetworkManager
[root@rhel7 ~]# yum -y install NetworkManager-tui
[root@rhel7 ~]# nmtui
```

nmcli

- 语法格式
  - nmcli 选项 OBJECT {命令}
  - OBJECT
    general，networkiing，connection，device
  - nmcli general help

知识讲解

nmcli（续1）

- 案例

```
[root@rhel7 ~]# nmcli connection show                    //查看网络连接
[root@rhel7 ~]# nmcli con show
[root@rhel7 ~]# nmcli connection show   --active
[root@rhel7 ~]# nmcli device status                      //查看设备状态
[root@rhel7 ~]# nmcli con mod my-eth ipv4.dns “8.8.8.8 8.8.4.4”
//设置DNS服务器
[root@rhel7 ~]# nmcli con modify "System eth0" ipv4.addresses \
>192.168.0.200/24
[root@rhel7 ~]# nmcli con up “my-eth1”
[root@rhel7 ~]# nmtui
```

知识讲解

网卡配置文件

- /etc/sysconfig/network-scripts/ifcfg-eth0

```
[root@rhel7 ~]# cat /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE=eth0
BOOTPROTO=none
ONBOOT=yes
NETMASK=255. 255. 255. 0
IPADDR=10. 0. 1. 27
```

知识讲解

Tedu.cn
达内教育

防火墙

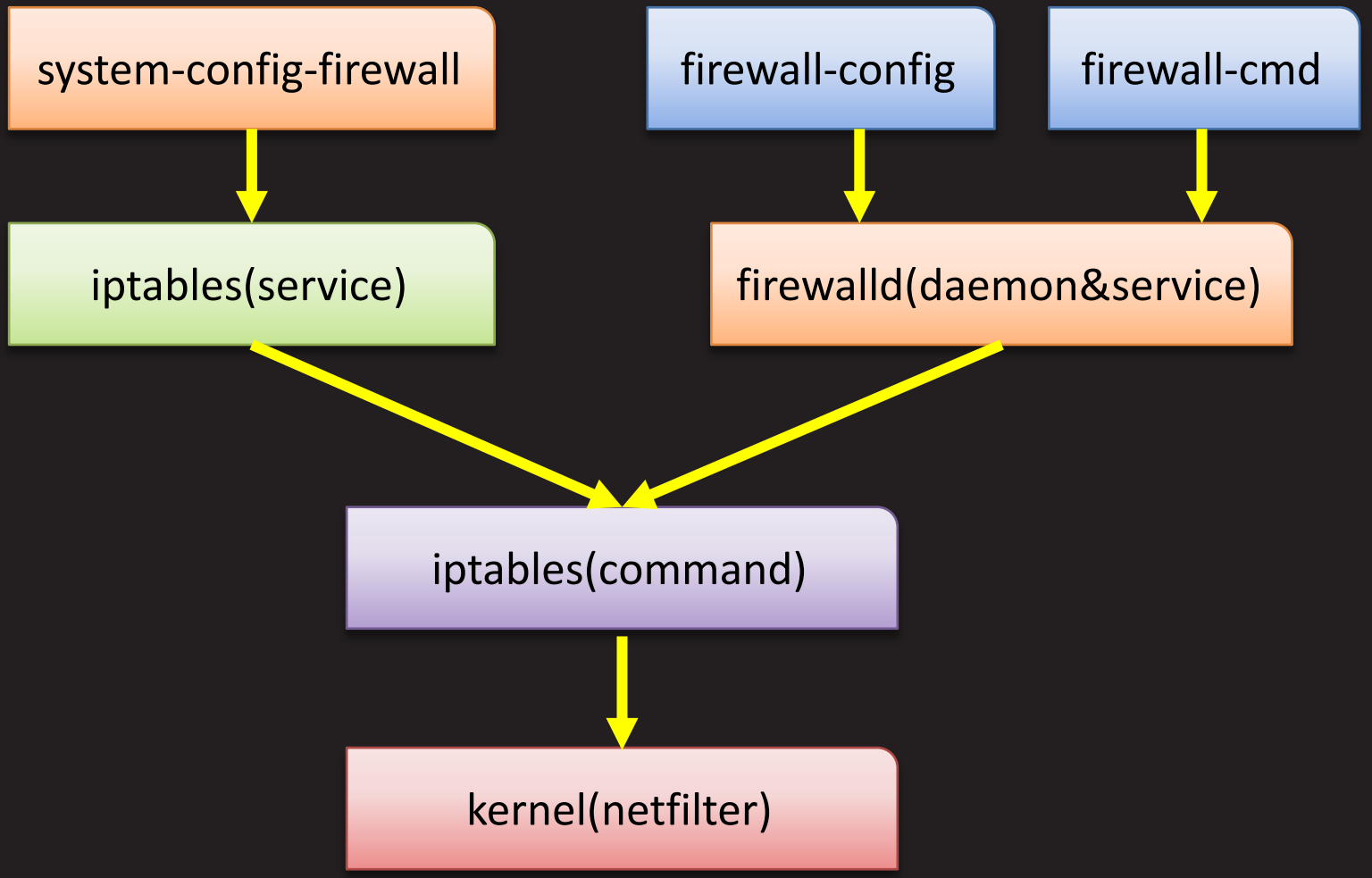
简介

- **firewalld是一个支持域的动态防火墙管理服务**
- **firewalld支持ipv4及ipv6网络**
- 支持图形和命令行两种配置方式
  - **firewall-config、firewall-cmd**
- 配置文件存放路径为：
  - /usr/lib/firewalld和/etc/firewalld

知识讲解

防火墙架构

知识讲解



防火墙区域

- firewalld根据网络区域过滤数据，默认区域如下：
  - drop、block、public、external、dmz、work、home、internal、trusted
- **我应该选用哪个区域?**
  - 例如，公共的WIFI连接应该主要为不受信任的，家庭的有线网络应该是相当可信任的。根据与你使用的网络最符合的区域进行选择

```
[root@rhel7 ~]# firewall-cmd --get-default-zone        //查看默认区域
[root@rhel7 ~]# firewall-cmd --set-default-zone dmz //设置默认区域
```

知识讲解

防火墙区域（续1）

- drop
  - 任何流入网络的包都被丢弃，不作出任何响应
- block
  - 任何进入的网络连接都被拒绝
- public
  - 用以可以公开的部分，只允许选中的服务通过
- external
  - 只允许选中的服务通过
- trusted
  - 允许所有网络连接

知识讲解

防火墙区域（续2）

- dmz
  - 用以允许隔离区（dmz）中的电脑有限地被外界网络访问
- home
  - 用在家庭网络。你信任网络中的大多数计算机不会影响你的计算机，只允许选中的服务通过
- work
  - 用在工作网络。你信任网络中的大多数计算机不会影响你的计算机，只允许选中的服务通过
- internal
  - 用在内部网络

知识讲解

防火墙区域生效规则

- 根据客户机IP地址，决定数据包进入哪个区域进行检查
- 根据进入的端口，决定数据包进入哪个区域检查
- 如果上述两个条件都不满足，则进入默区域检查

知识讲解

操作案例

知识讲解

```
[root@rhel7 ~]# yum -y install firewalld firewall- config
[root@rhel7 ~]# firewall-cmd --state                    //查看状态
[root@rhel7 ~]# firewall-cmd --list-all-zone            //列出所有区域
[root@rhel7 ~]# firewall-cmd --get-zone-of-interface=vnet1
//查看接口属于哪个区域
[root@rhel7 ~]# firewall-cmd --zone=trusted --add-interface=ens20055
//将网络接口加入到网络区域
[root@rhel7 ~]# firewall-cmd --zone=trusted --change-interface=virbr0
//修改接口所属区域
[root@rhel7 ~]# firewall-cmd trusted --remove-interface=virbr0
//从区域中将接口删除
[root@rhel7 ~]# firewall-cmd  --zone=public --list-services
//显示网络区域中的所有服务
```

操作案例（续1）

[root@rhel7 ~]# firewall-cmd --add-service=http
//将服务加入默认区域
[root@rhel7 ~]# firewall-cmd –zone=public--remove-service=http
//在区域中删除服务
[root@rhel7 ~]# firewall-cmd --add-port=<port>[-<port>]/<protocol> [--timeout=<seconds>]
//激活端口及协议组合规则
[root@rhel7 ~]# firewall-cmd --permanent [--zone=<zone>] --add-service=<service>
//永久生效规则
[root@rhel7 ~]# firewall- cmd - - zone=external \
>--add-forwardport=port=22:proto=tcp:toport=3753
//实现端口转发
[root@rhel7 ~]# firewall- cmd - - zone=external \
>--add-forwardport=port=22:proto=tcp:toaddr=192.0.2.55

知识讲解

Tedu.cn
达内教育

总结和答疑