Tedu.cn
达内教育

云计算应用管理

NSD ENGINEER DAY02

内容

上午	09:00 ~ 09:30	作业讲解和回顾
	09:30 ~ 10:20	系统安全保护
	10:30 ~ 11:20	配置用户环境
	11:30 ~ 12:00	防火墙策略管理
下午	14:00 ~ 14:50	
	15:00 ~ 15:50	
	16:10 ~ 17:00	
	17:10 ~ 18:00	总结和答疑

系统安全保护

SELinux安全机制

SELinux概述

知识讲解

- 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运行模式的切换

知识讲解

- SELinux的运行模式
  - enforcing（强制）、permissive（宽松）
  - disabled（彻底禁用）
- 切换运行模式
  - 临时切换：setenforce 1|0
  - 固定配置：/etc/selinux/config 文件

```
[root@server0 ~]# getenforce                    //查看当前模式
Disabled
[root@server0 ~]# vim  /etc/selinux/config
SELINUX=enforcing                               //设置为强制启用
.. ..
[root@server0 ~]# reboot                        //重启系统以切换模式
```

案例1：启用SELinux保护

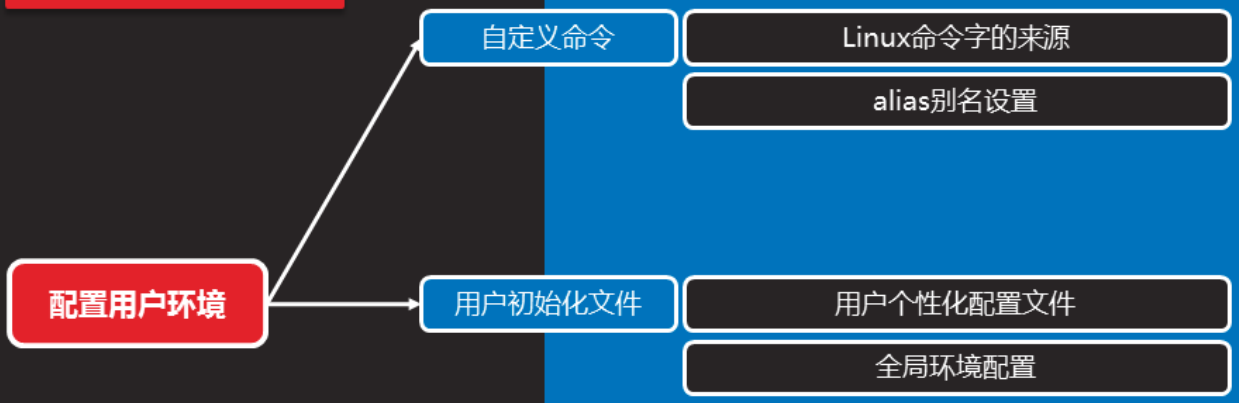
课堂练习

为虚拟机 server0、desktop0 配置SELinux

1）确保 SELinux 处于强制启用模式

2）在每次重新开机后，此设置必须仍然有效

配置用户环境



Tedu.cn
达内教育

自定义命令

Linux命令字的来源

Tedu.cn 达内教育

知识讲解

- 如何指定命令字
  - 可执行程序的路径
- 什么是别名
  - 在用户环境中，为一个复杂的、需要经常使用的命令行所起的短名称
  - 可用来替换普通命令，更加方便

alias别名设置

Tedu.cn 达内教育

知识讲解

- 查看已设置的别名
  - alias [别名名称]
- 定义新的别名
  - alias 别名名称= '实际执行的命令行'
- 取消已设置的别名
  - unalias [别名名称]

```
[root@server0 ~]# alias  qstat='/bin/ps -Ao pid,tt,user,fname,rsz'
[root@server0 ~]# qstat
.. ..
```

Tedu.cn 达内教育

用户初始化文件

Tedu.cn 达内教育

用户个性化配置文件

- 影响指定用户的 bash 解释环境
  - ~/.bashrc，每次开启 bash 终端时生效

知识讲解

```
[root@server0 ~]# vim  ~student/.bashrc
.. ..
alias  ld='ls -lhd --color=auto'

[root@server0 ~]# su  -  student              //仅对 student 用户有效
[student@server0 ~]$ alias  ld
alias ld='ls -lhd --color=auto'
```

全局环境配置

Tedu.cn 达内教育

知识讲解

- 影响所有用户的 bash 解释环境
  - /etc/bashrc，每次开启 bash 终端时生效

```
[root@server0 ~]# vim  /etc/bashrc
.. ..
alias  qstat='/bin/ps -Ao pid,tt,user,fname,rsz'

[root@server0 ~]# su  -  root                    //对所有用户有效
[root@server0 ~]# qstat
.. ..
```

案例2：自定义用户环境

Tedu.cn 达内教育

课堂练习

为系统 server0 和 desktop0 创建自定义命令

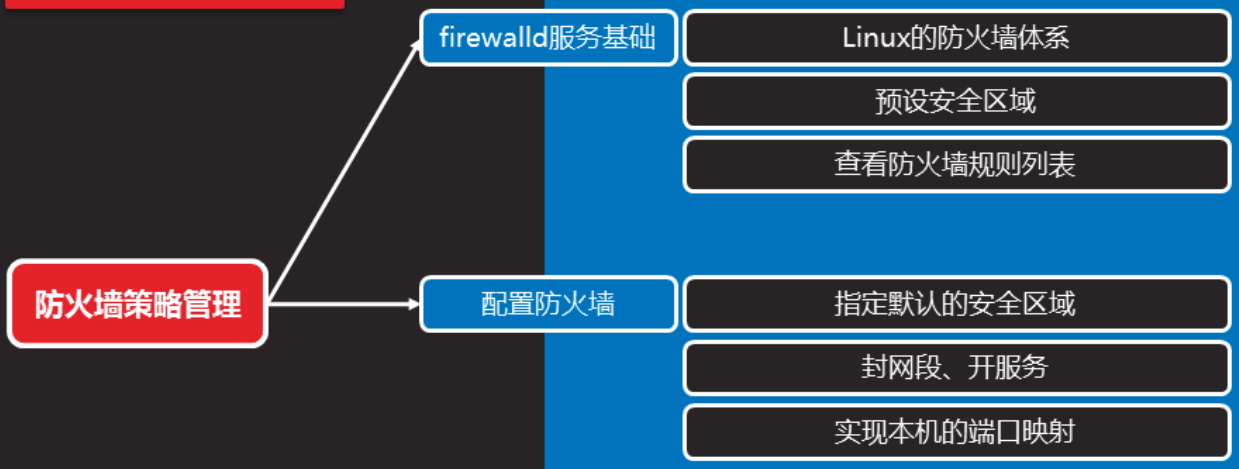
1）自定义命令的名称为 qstat

2）此自定义命令将执行以下操作：

/bin/ps -Ao pid,tt,user,fname,rsz

3）此自定义命令对系统中的所有用户都有效

防火墙策略管理



Tedu.cn
达内教育

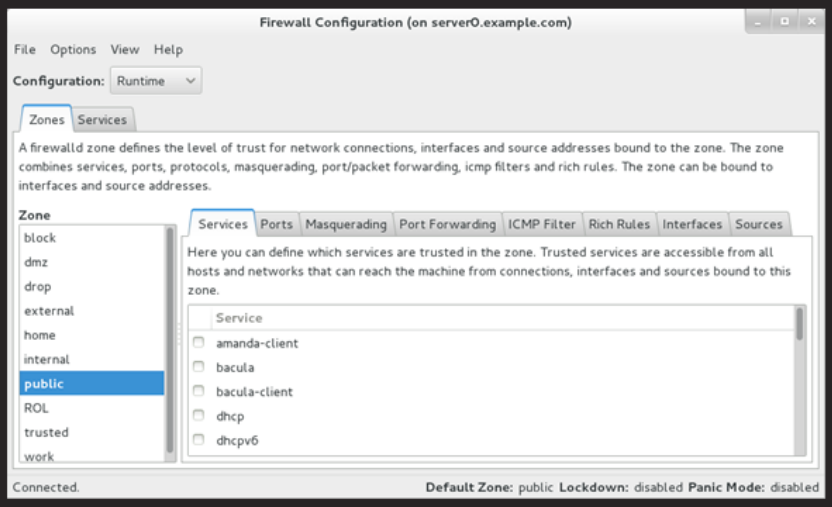
firewalld服务基础

Linux的防火墙体系

知识讲解

- 系统服务：firewalld
- 管理工具：firewall-cmd、firewall-config

```
[root@server0 ~]# systemctl  restart  firewalld
[root@server0 ~]# firewall-config  &
```



预设安全区域

知识讲解

- 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sshd等少数几个服务
  - trusted：允许任何访问
  - block：阻塞任何来访请求
  - drop：丢弃任何来访的数据包
  - ……
- 配置规则的位置
  - 运行时（runtime）
  - 永久（permanent）

查看防火墙规则列表

Tedu.cn 达内教育

知识讲解

- 列表查看操作
  - firewall-cmd --list-all [--zone=区域名]
  - firewall-cmd --list-all-zones
  - firewall-cmd --get-zones
  - firewall-cmd --get-services
  - firewall-cmd --get-default-zone

Tedu.cn 达内教育

配置防火墙

指定默认的安全区域

知识讲解

- 使用 --set-default-zone=区域名
  - 默认为 public ，限制较严格
  - 对于开放式环境，建议将默认区域修改为 trusted
  - 针对“运行时/永久配置”均有效

```
[root@server0 ~]# firewall-cmd  --get-default-zone      //修改前
public
[root@server0 ~]# firewall-cmd  --set-default-zone=trusted

[root@server0 ~]# firewall-cmd  --get-default-zone     //修改之后
trusted
```

封网段、开服务

知识讲解

- 若针对“永久配置” ，需添加 --permanent
  - 使用 --add-source=网段地址
  - 使用 --add-service=服务名

```
[root@server0 ~]# firewall-cmd  --permanent  --zone=block  --
add-source=172.34.0.0/24

[root@server0 ~]# firewall-cmd  --permanent  --zone=public  --
add-service=http
[root@server0 ~]# firewall-cmd  --permanent  --zone=public  --
add-service=ftp

[root@server0 ~]# firewall-cmd  --reload          //重载配置
```

实现本机的端口映射

Tedu.cn 达内教育

知识讲解

- 本地应用的端口重定向（端口1 --> 端口2）
  - 从客户机访问 端口1 的请求，自动映射到本机 端口2
  - 比如，访问以下两个地址可以看到相同的页面：
    http://server0.example.com:5423/
    http://server0.example.com/

```
[root@server0 ~]# firewall-cmd  --permanent --zone=trusted  --
add-forward-port=port=5423:proto=tcp:toport=80

[root@server0 ~]# firewall-cmd  --reload          //重载配置
```

案例3：配置firewalld防火墙

Tedu.cn 达内教育

课堂练习

为你的两个虚拟机配置防火墙策略

- 允许从 172.25.0.0/24 网段的客户机访问 server0、desktop0 的任何服务
- 在172.25.0.0/24网络中的系统，访问 server0 的本地端口5423将被转发到80
- 上述设置必须永久有效

Tedu.cn
达内教育

总结和答疑