

Linux高级运维

NSD OPERATION

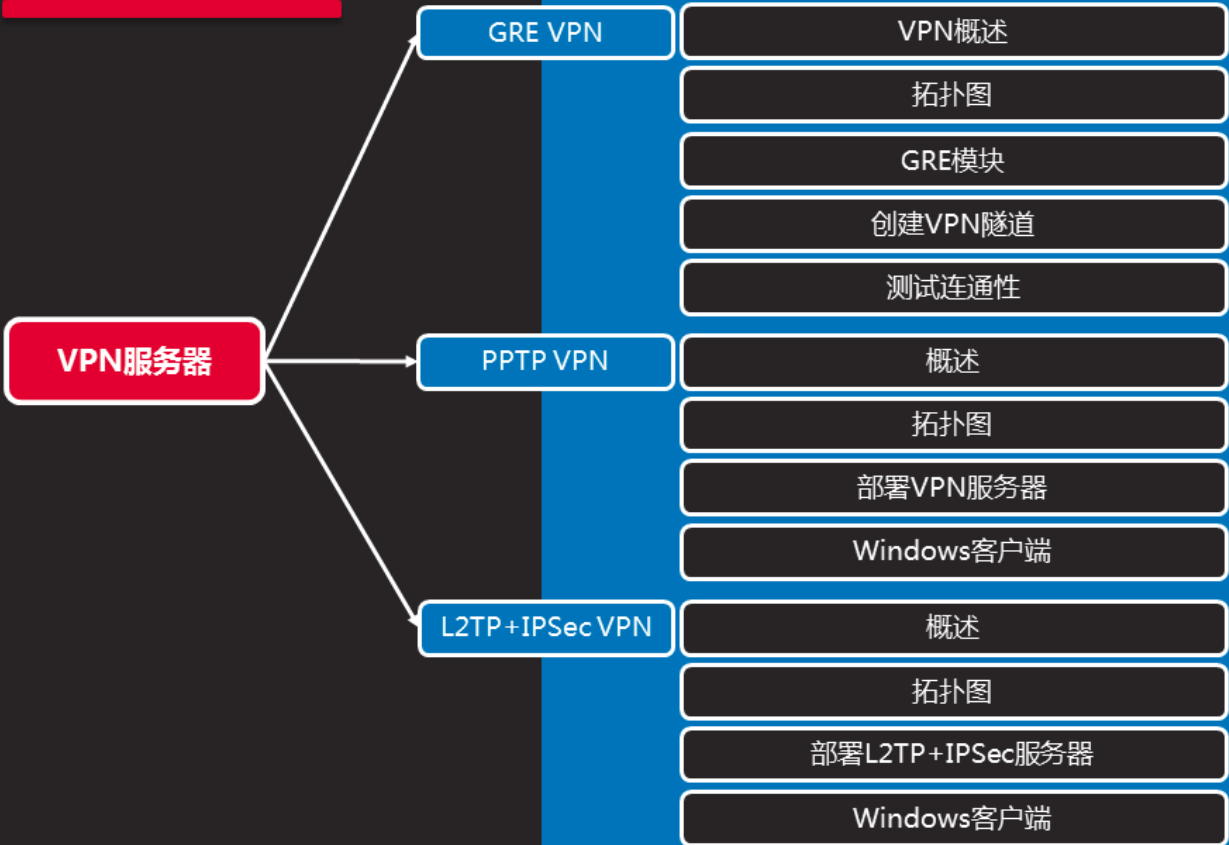
DAY07

内容

上午	09:00 ~ 09:30	作业讲解和回顾
	09:30 ~ 10:20	VPN服务器
	10:30 ~ 11:20	
	11:30 ~ 12:20	
下午	14:00 ~ 14:50	
	15:00 ~ 15:50	NTP时间同步
	16:00 ~ 16:50	PSSH远程工具
	17:00 ~ 17:30	总结和答疑



VPN服务器



GRE VPN

VPN概述

知识讲解

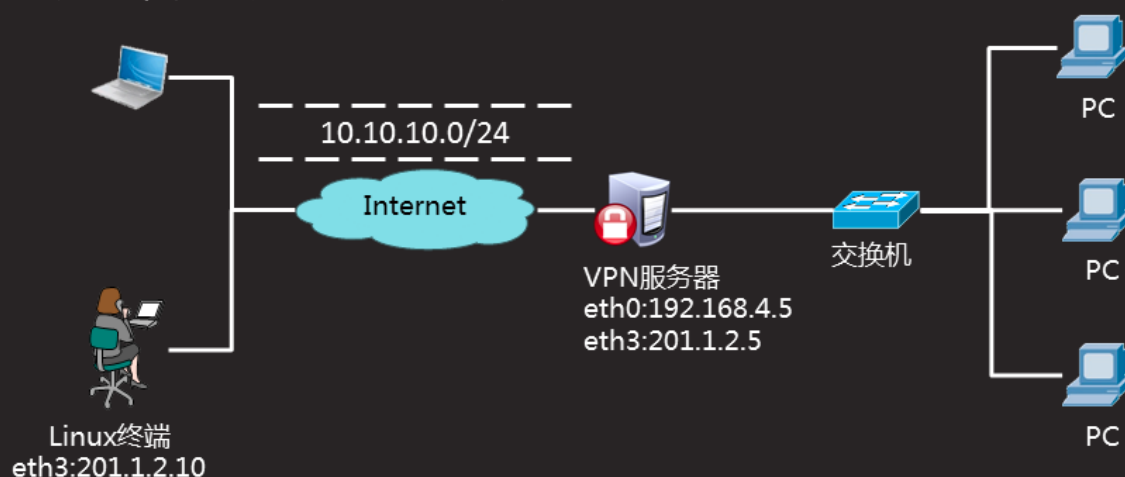
- Virtual Private Network (虚拟专用网络)
 - 在公用网络上建立专用私有网络，进行加密通讯
 - 多用于为集团公司的各地子公司建立连接
 - 连接完成后，各个地区的子公司可以像局域网一样通讯
 - 在企业网络中有广泛应用
 - 偶尔可以用于翻墙
 - 目前主流的VPN技术 (GRE , PPTP , L2TP+IPSec , SSL)



拓扑图

- 出差在外，连接公司的服务器
- 或者，分公司之间的连接

知识讲解



GRE模块

- Linux内核模块
 - ip_gre
- 加载模块
 - `lsmod | grep ip_gre` //显示模块列表
 - `modprobe ip_gre` //加载模板
 - `modinfo ip_gre` //查看模块信息
- 缺点：缺少加密机制

知识讲解



创建VPN隧道

- Client

```
[root@clinet ~]# modprobe ip_gre
[root@client ~]# ip tunnel add tun0 mode gre \
> remote 201.1.2.5 local 201.1.2.10
[root@client ~]# ip link set tun0 up
[root@client ~]# ip addr add 10.10.10.10/24 peer 10.10.10.5/24 \
> dev tun0
[root@client ~]# firewall-cmd --set-default-zone=trusted
```

知识讲解



创建VPN隧道（续1）

- VPN服务器

```
[root@proxy ~]# modprobe ip_gre
[root@proxy ~]# ip tunnel add tun0 mode gre \
> remote 201.1.2.10 local 201.1.2.5
[root@proxy ~]# ip link set tun0 up
[root@proxy ~]# ip addr add 10.10.10.5/24 peer 10.10.10.10/24 \
> dev tun0
[root@proxy ~]# echo "1" > /proc/sys/net/ipv4/ip_forward
[root@proxy ~]# firewall-cmd --set-default-zone=trusted
```

知识讲解



测试连通性

知识讲解

- Client

```
[root@client ~]# ping 10.10.10.5
```

```
[root@client ~]# ping 192.168.4.5
```

- Proxy

```
[root@proxy ~]# ping 10.10.10.10
```



案例1：配置GRE VPN

课堂练习

- 启用内核模块ip_gre
- 创建一个虚拟VPN隧道(10.10.10.0/24)
- 实现两台主机点到点的隧道通讯



PPTP VPN



概述

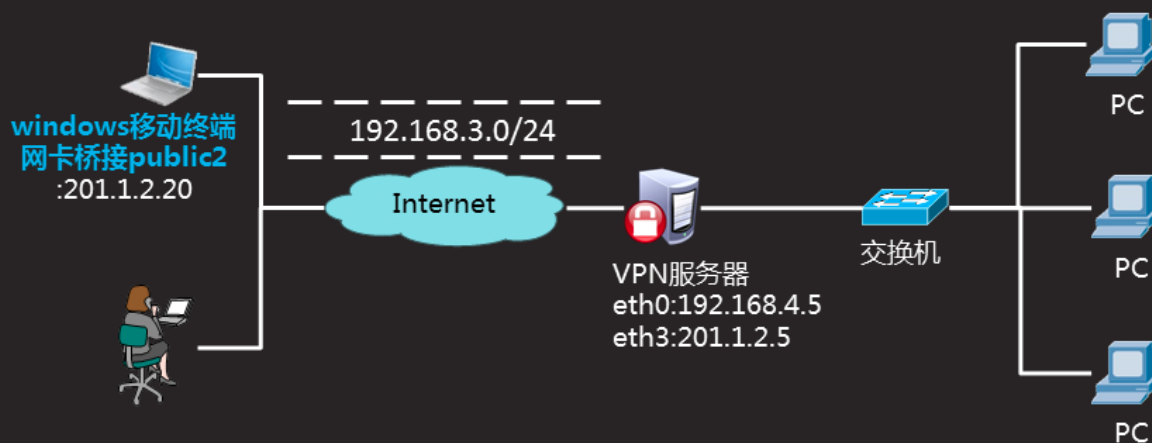
- PPTP (Point to Point Tunneling Protocol)
- 支持密码身份验证
- 支持MPPE(Microsoft Point-to-Point Encryption)加密



拓扑图

知识讲解

- 拓扑图沿用之前实验的拓扑结构
- 使用一台Windows主机做为客户端
- Windows IP地址为:201.1.2.20/24



部署VPN服务器

- 安装软件

知识讲解

```
[root@proxy ~]# yum localinstall pptpd-1.4.0-2.el7.x86_64.rpm
[root@proxy ~]# rpm -qc pptpd
/etc/ppp/options.pptpd
/etc/pptpd.conf
/etc/sysconfig/pptpd
```



部署VPN服务器（续1）

- 修改配置文件

```
[root@proxy ~]# vim /etc/pptpd.conf
localip 201.1.2.5           //服务器本地IP
remoteip 192.168.3.1-50    //分配给客户端的IP池
```

```
[root@proxy ~]# vim /etc/ppp/options.pptpd
require-mppe-128           //使用MPPE加密数据
ms-dns 8.8.8.8             //DNS服务器
```

```
[root@proxy ~]# vim /etc/ppp/chap-secrets
jacob      *      123456      *
//用户名   服务器标记  密码    客户端
```

```
[root@proxy ~]# echo "1" > /proc/sys/net/ipv4/ip_forward
```

知识讲解



部署VPN服务器（续2）

- 启动服务

```
[root@proxy ~]# systemctl start pptpd
[root@proxy ~]# firewall-cmd --set-default-zone=trusted
```

- 翻墙设置

```
[root@proxy ~]# iptables -t nat -A POSTROUTING -s 192.168.3.0/24 \
> -j SNAT --to-source 201.1.2.5
```

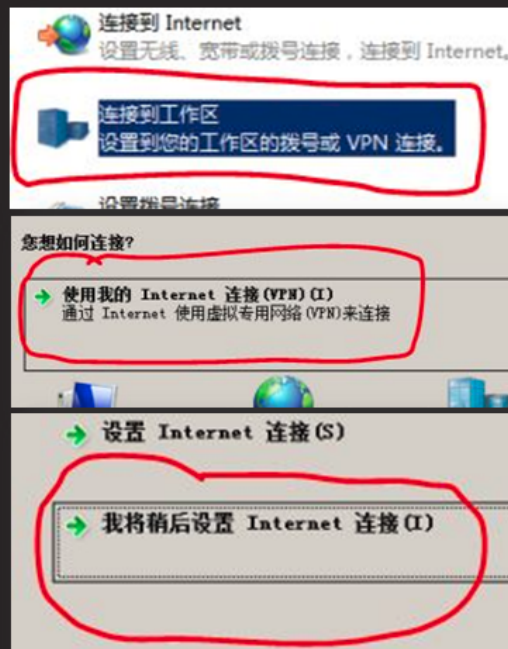
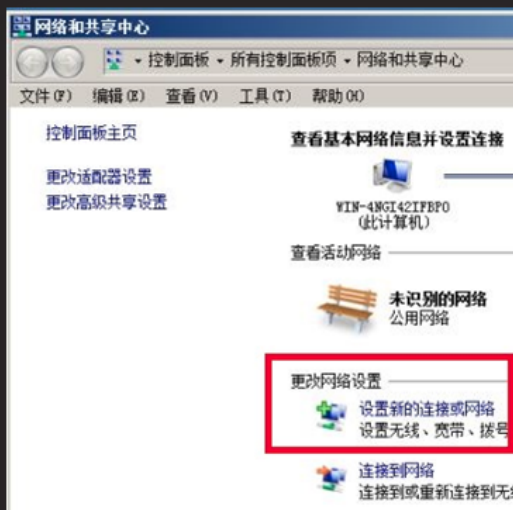
知识讲解



Windows客户端

- 配置IP地址：201.1.2.20
- 建立VPN连接

知识讲解



Windows客户端（续1）

- 测试

知识讲解



```
C:\Users\Jacob>ping 201.1.2.5
```

```
C:\Users\Jacob>ping 192.168.4.5
```



案例2：创建PPTP VPN

课堂练习

- 使用PPTP协议创建一个支持身份验证的隧道连接
- 使用MPPE对数据进行加密
- 为客户端分配192.168.3.0/24的地址池
- 客户端连接的用户名为jacob，密码为123456



L2TP+IPSec VPN

概述

知识讲解

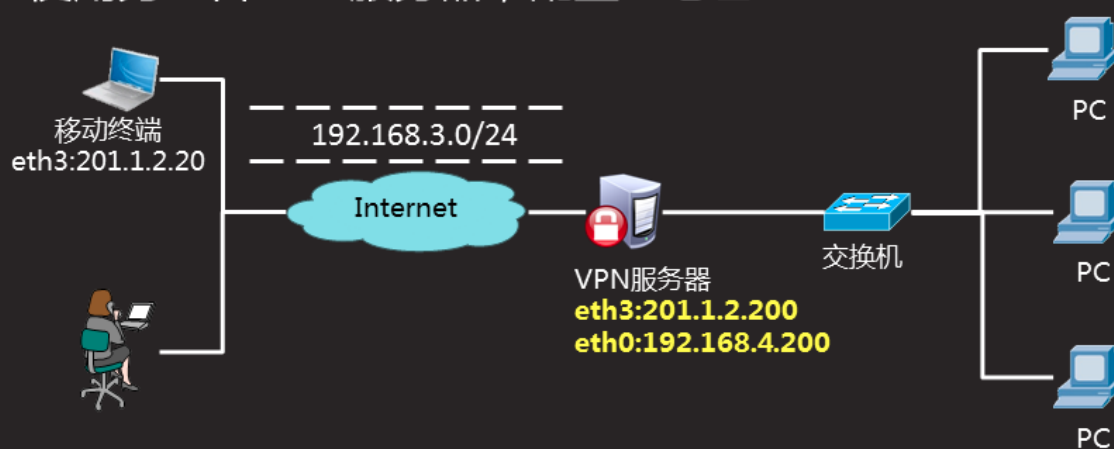
- Layer Two Tunneling Protocol (L2TP)
- L2TP建立主机之间的VPN隧道，压缩、验证
- IPSec提供数据加密、数据校验、访问控制的功能



拓扑图

- 沿用之前实验的拓扑结构
- 使用另一台VPN服务器，配置IP地址

知识讲解



部署L2TP+IPSec服务器

- 安装软件

```
[root@vpn ~]# yum -y install libreswan  
[root@vpn ~]# yum localinstall xl2tpd-1.3.8-2.el7.x86_64.rpm
```

知识讲解



部署L2TP+IPSec服务器（续1）

- 创建IPSec加密配置文件

```
[root@vpn ~]# vim /etc/ipsec.d/myipsec.conf //新建文件  
conn IDC-PSK-NAT  
    rightsubnet=vhost:%priv //允许的VPN虚拟网络  
    also=IDC-PSK-noNAT  
  
conn IDC-PSK-noNAT  
    authby=secret //加密认证  
    ike=3des-sha1;modp1024 //算法  
    phase2alg=aes256-sha1;modp2048 //算法  
    pfs=no  
    auto=add  
    keyingtries=3  
    rekey=no  
    ikelifetime=8h  
    keylife=3h  
    type=transport  
    left=201.1.2.200 //重要，服务器本机的外网IP  
    leftprotoport=17/1701  
    right=%any //允许任何客户端连接  
    rightprotoport=17/%any
```

知识讲解



部署L2TP+IPSec服务器（续2）

- 新建IPSec预定义共享密钥

```
[root@vpn ~]# cat /etc/ipsec.secrets  
include /etc/ipsec.d/*.secrets
```

//不要修改该文件

```
[root@vpn ~]# vim /etc/ipsec.d/mypass.secrets  
201.1.2.200 %any: PSK "randpass"
```

//新建文件

//randpass为密钥

知识讲解



部署L2TP+IPSec服务器（续3）

- 启动IPSec服务

```
[root@vpn ~]# systemctl start ipsec
```

```
[root@vpn ~]# netstat -ntulp | grep pluto
```

知识讲解



部署L2TP+IPSec服务器 (续4)

- 修改xl2tp配置文件

知识讲解

```
[root@vpn ~]# vim /etc/xl2tpd/xl2tpd.conf
```

```
[global]
```

```
[ins default]
```

```
ip range = 192.168.3.128-192.168.3.254
```

//分配给客户端的IP池

```
local ip = 201.1.2.200
```

//服务IP地址

```
[root@vpn ~]# vim /etc/ppp/options.xl2tpd
```

```
require-mschap-v2
```

//添加一行

```
#crtsts
```

//注释或删除该行

```
#lock
```

//注释或删除该行

```
root@vpn ~]# vim /etc/ppp/chap-secrets
```

//修改密码文件

```
jacob * 123456 *
```



部署L2TP+IPSec服务器 (续5)

- 启动XL2TP服务

知识讲解

```
[root@vpn ~]# systemctl start xl2tpd
```

```
root@vpn ~]# netstat -ntulp |grep xl2tpd
```

```
udp      0      0 0.0.0.0:1701      0.0.0.0:*
```

3580/xl2tpd

```
[root@vpn ~]# echo "1" > /proc/sys/net/ipv4/ip_forward
```

```
[root@vpn ~]# firewall-cmd --set-default-zone=trusted
```

- 翻墙

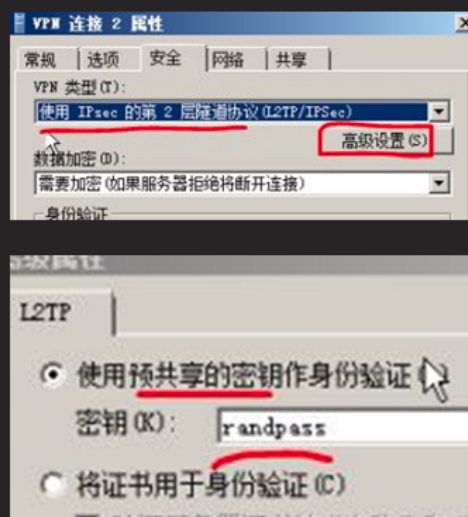
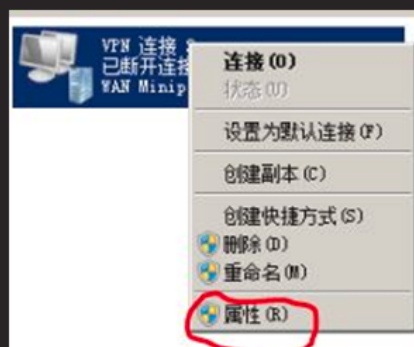
```
[root@proxy ~]# iptables -t nat -A POSTROUTING -s 192.168.3.0/24 \
> -j SNAT --to-source 201.1.2.200
```



Windows客户端

- 配置IP地址：201.1.2.20
- 建立VPN连接（与之前的实验一致）

知识讲解



Windows客户端（续1）

- 默认拨号会报错：789，需要做如下设置：
 - 单击"开始"，单击"运行"，键入"regedit"，然后单击"确定"
 - 找到下面的注册表子项，然后单击它：
 - HKEY_LOCAL_MACHINE\
 - System\CurrentControlSet\Services\Rasman\Parameters
 - 在"编辑"菜单上，单击"新建" -> "DWORD值"
 - 在"名称"框中，键入"ProhibitIpSec"
 - 在"数值数据"框中，键入"1"，然后单击"确定"
 - 退出注册表编辑器，然后重新启动计算机

知识讲解



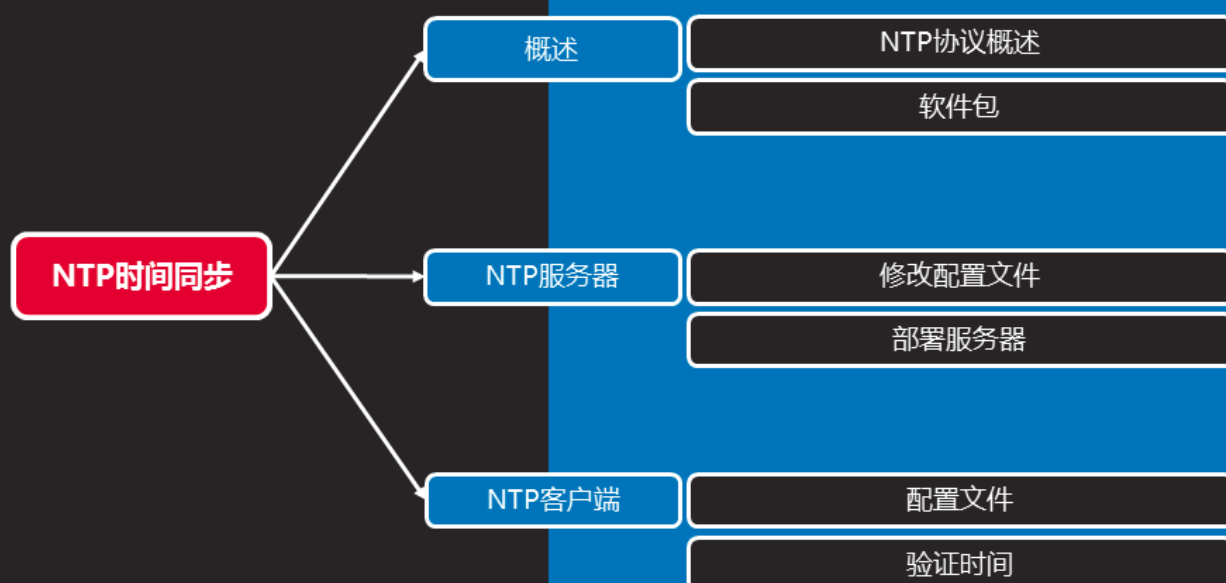
案例3：创建L2TP+IPSec VPN

课堂练习

- 使用L2TP协议创建一个支持身份验证与加密的隧道连接
- 使用IPSec对数据进行加密
- 为客户端分配192.168.3.0/24的地址池
- 客户端连接的用户名为：jacob，密码为：123456
- 预共享密钥为：randpass



NTP时间同步

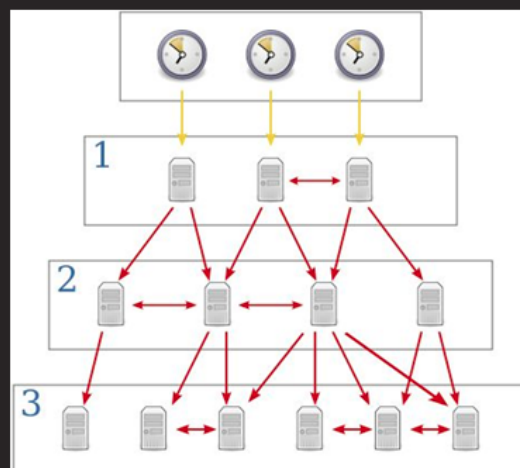


概述

NTP协议概述

- Network Time Protocol (网络时间协议)
- 它用来同步网络中各个计算机的时间的协议
- 210.72.145.39 (国家授时中心服务器IP地址)
- Stratum (分层设计)
- Stratum层的总数限制在15以内 (包括15)

知识讲解



软件包

- ntp和chrony

知识讲解

```
[root@proxy ~]# yum -y install chrony  
[root@proxy ~]# rpm -qc chrony  
/etc/chrony.conf  
/etc/chrony.keys  
.. ..
```

//查看配置文件



NTP服务器

修改配置文件

- 主配置文件/etc/chrony.conf

```
[root@proxy ~]# cat /etc/chrony.conf
```

```
server 0.centos.pool.ntp.org iburst
```

```
allow 192.168.4.0/24
```

```
deny 192.168.4.1
```

```
local stratum 10
```

```
.. ..
```

//server用户客户端指向上层NTP服务器

//允许那个IP或网络访问NTP

//拒绝那个IP或网络访问NTP

//设置NTP服务器的层数量

知识讲解



部署服务器

- 启动服务器

```
[root@proxy ~]# systemctl restart chronyd
```

```
[root@proxy ~]# systemctl enable chronyd
```

- 防火墙设置

```
[root@proxy ~]# firewall-cmd --set-default-zone=trusted
```

知识讲解



NTP客户端

配置文件

- 主配置文件/etc/chrony.conf

```
[root@proxy ~]# cat /etc/chrony.conf
```

```
server 192.168.4.5 iburst
```

//设置与哪台服务器同步数据

//iburst参数设置重启服务后尽快同步时间



验证时间

知识讲解

- 客户端将时间修改错误

```
[root@client ~]# date -s "hour:minute" //调整时间  
[root@client ~]# date //查看时间
```

- 重启服务

```
[root@client ~]# systemctl restart chronyd
```

- 验证时间是否同步

```
[root@client ~]# date //多执行几次查看
```



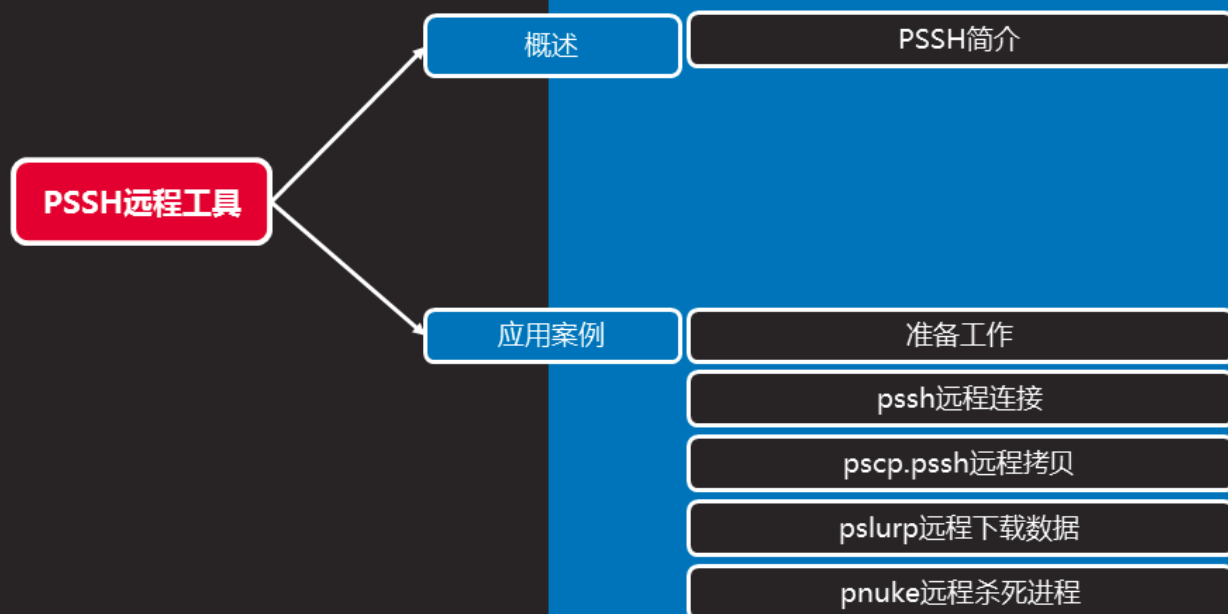
案例4：NTP时间同步

课堂练习

- 部署一台NTP时间服务器
 - 设置时间服务器上层与0.centos.pool.ntp.org同步
 - 设置本地服务器层级数量为10
 - 允许192.168.4.0/24网络的主机同步时间
- 客户端验证时间是否同步



PSSH远程工具



概述

PSSH简介

知识讲解

- PSSH提供了一套并发openssh工具
 - PSSH provides parallel versions of the openssh tools
- PSSH使用Python编写
- 计算机需要安装有Python2.4或更新版本才可以使用



应用案例

准备工作

知识讲解

- 安装软件

```
[root@proxy ~]# rpm -ivh pssh-2.3.1-5.el7.noarch.rpm
```

- 设置本地域名解析方便远程

```
[root@proxy ~]# cat /etc/hosts
```

```
... ..
```

```
192.168.2.100 host1
```

```
192.168.2.200 host2
```

```
192.168.4.100 host3
```

```
... ..
```

- 创建主机列表文件

```
[root@proxy ~]# cat /root/host.txt
```

//每行一个用户名、IP或域名

```
... ..
```

```
root@host1
```

```
host2
```

```
host3
```

```
... ..
```



pssh远程连接

知识讲解

- pssh提供并发远程连接功能

- -A 使用密码远程其他主机（默认使用密钥）
- -i 将输出显示在屏幕
- -H 设置需要连接的主机
- -h 设置主机列表文件
- -p 设置并发数量
- -t 设置超时时间
- -o dir 设置标准输出信息保存的目录
- -e dir 设置错误输出信息保存的目录
- -x 传递参数给ssh



pssh远程连接（续1）

- 案例

```
[root@proxy ~]# pssh -i -A -H 'host1 host2 host3' \  
> -x '-o StrictHostKeyChecking=no' echo hello
```

//使用密码远程多台主机执行命令，屏幕显示标准和错误输出信息

```
[root@proxy ~]# pssh -A -h host.txt \  
> -x '-o StrictHostKeyChecking=no' echo hello
```

//使用密码远程多台主机执行命令，不显示标准和错误输出信息
//通过读取host.txt读取主机信息

知识讲解



pssh远程连接（续2）

- 案例

```
[root@proxy ~]# ssh-keygen -N "" -f /root/.ssh/id_rsa //非交互生成密钥文件  
[root@proxy ~]# ssh-copy-id -i /root/.ssh/id_rsa.pub host1  
[root@proxy ~]# ssh-copy-id -i /root/.ssh/id_rsa.pub host2  
[root@proxy ~]# ssh-copy-id -i /root/.ssh/id_rsa.pub host3
```

```
[root@proxy ~]# pssh -h host.txt -x '-o StrictHostKeyChecking=no' echo hello  
//使用密钥远程其他主机
```

```
[root@proxy ~]# pssh -h host.txt -o /tmp/ -x '-o StrictHostKeyChecking=no' echo hello  
//使用密钥远程其他主机，将标准输出信息写入到/tmp目录
```

知识讲解



pscp.pssh远程拷贝

知识讲解

- pscp.pssh提供并发拷贝文件功能

- -r 递归拷贝目录
- 其他选项基本与pssh一致

```
[root@proxy ~]# pscp.pssh -h host.txt -x '-o StrictHostKeyChecking=no' etc.tar.gz /  
//将本地的etc.tar.gz拷贝到远程主机的根目录下
```

```
[root@proxy ~]# pscp.pssh -r -h host.txt \  
> -x '-o StrictHostKeyChecking=no' /etc /tmp  
//递归将本地的/etc目录拷贝到远程主机的/tmp目录下
```



pslurp远程下载数据

知识讲解

- pslurp提供远程下载功能
- 选项与pscp.pssh基本一致

```
[root@proxy ~]# pslurp -r -h host.txt -x '-o StrictHostKeyChecking=no' /etc /tmp  
//将远程主机的/etc/目录，拷贝到当前目录下，存放在对应IP下的tmp目录
```

```
[root@proxy ~]# pslurp -r -h host.txt -x '-o StrictHostKeyChecking=no' \  
> -L /media /etc /tmp  
//将远程主机的/etc/目录，拷贝到media下，存放在对应IP下的tmp目录
```



pnuke远程杀死进程

知识讲解

- pnuke提供远程杀死进程的功能
 - 选项与pssh基本一致

```
[root@proxy ~]# pnuke -h host.txt -x '-o StrictHostKeyChecking=no' sleep  
//将远程主机上的sleep进程杀死
```

```
[root@proxy ~]# pnuke -h host.txt -x '-o StrictHostKeyChecking=no' test  
//将远程主机上的test相关脚本都杀死（如：test1,testtt,test2等等）
```

```
[root@proxy ~]# pnuke -h host.txt -x '-o StrictHostKeyChecking=no' test.sh  
//将远程主机上的test.sh脚本杀死
```



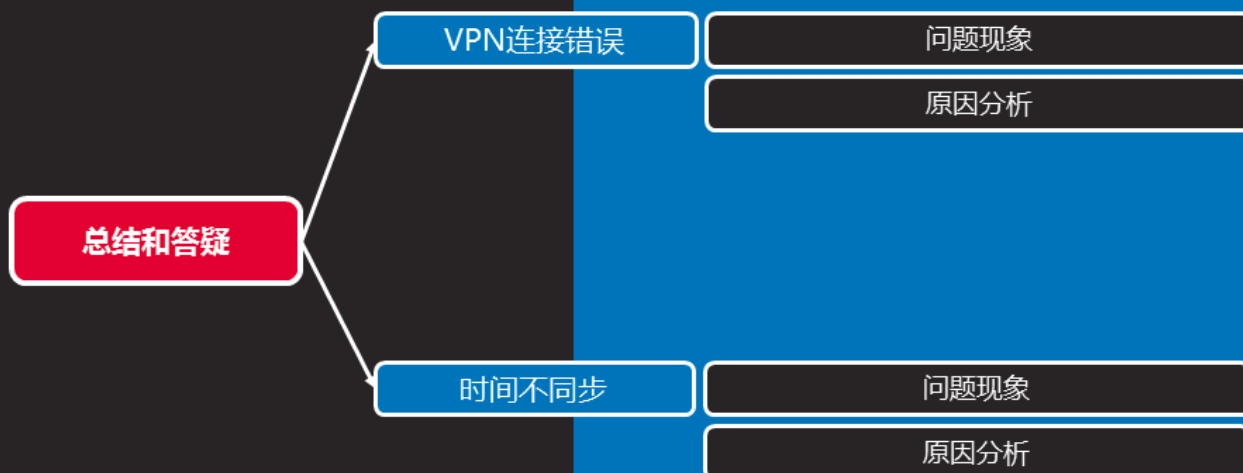
案例5：pssh远程套件工具

课堂练习

- 使用pssh套件工具实现如下功能
 - 使用密钥批量、多并发远程其他主机
 - 使用密钥批量、多并发远程其他主机
 - 批量、多并发拷贝数据到其他主机
 - 批量、多并发从其他主机下载数据到本机
 - 批量、多并发杀死其他主机的进程



总结和答疑



VPN连接错误

问题现象

- 故障错误信息
 - Windows某些版本的系统连接VPN时，报错789

知识讲解



原因分析

- 分析故障信息
 - 连接错误代码：789
- 分析故障原因
 - 需要修改注册表，并且重新启动计算机

知识讲解



时间不同步



问题现象

- 故障错误信息
 - 重启chronyd后时间不变

知识讲解



原因分析

- 分析故障信息
 - 重启服务后时间不同步
- 分析故障原因
 - 服务器防火墙是否关闭
 - 服务器是否配置了正确的allow与deny规则
 - 服务器是否已经启动了服务

知识讲解

