2015 年全国职业院校技能大赛

网络搭建与应用竞赛

（总分 1000 分）

赛题说明

一、竞赛内容分布

“网络搭建与应用”竞赛共分二个部分，其中：

第一部分：网络搭建及安全部署项目，占总分的比例为 45%；

第二部分：服务器配置及应用项目，占总分的比例为 55%；

二、竞赛注意事项

（1）禁止携带和使用移动存储设备、计算器、通信工具及参考资料。

（2）请根据大赛所提供的比赛环境，检查所列的硬件设备、软件清单、材料清单是否齐全，计算机设备是否能正常使用。

（3）本试卷共有两个部分。请选手仔细阅读比赛试卷，按照试卷要求完成各项操作。

（4）操作过程中，需要及时保存设备配置。比赛结束后，所有设备保持运行状态，不要拆、动硬件连接。

（5）比赛完成后，比赛设备、软件和赛题请保留在座位上，禁止将比赛所用的所有物品（包括试卷和草纸）带离赛场。

（6）所有需要提交的文档均放置在桌面的 PC1“比赛文档”文件夹中，禁止在纸质资料上填写与竞赛无关的标记，如违反规定，可视为 0 分。

（7）裁判以各参赛队提交的竞赛结果文档为主要评分依据。所有提交的文档

必须按照赛题所规定的命名规则命名，文档中有对应题目的小标题，截图有截图的简要说明，否则按无效内容处理。

（8）与比赛相关的工具软件放置在 D 盘的 tools 文件夹中。

项目简介：

某集团公司经过业务发展，总公司在北京市，在上海设置了分公司，为了实现快捷的信息交流和资源共享，需要构建统一网络，整合公司所有相关业务流程。采用单核心的网络架构的网络接入模式，采用路由器接入城域网专用链路来传输业务数据流。总公司为了安全管理每个部门的用户，使用 VLAN 技术将每个部门的用户划分到不同的 VLAN 中。分公司采用路由器接入互联网络和城域网专用网络，总公司的内网用户采用无线接入方式访问网络资源。

为了保障总公司与分公司业务数据流传输的高可用性，使用防火墙进行保证网络安全，采用 QOS 技术对公司重要的业务数据流进行保障。网络采用 OSPF 动态路由协议和 RIP 动态路由协议.

拓扑结构图

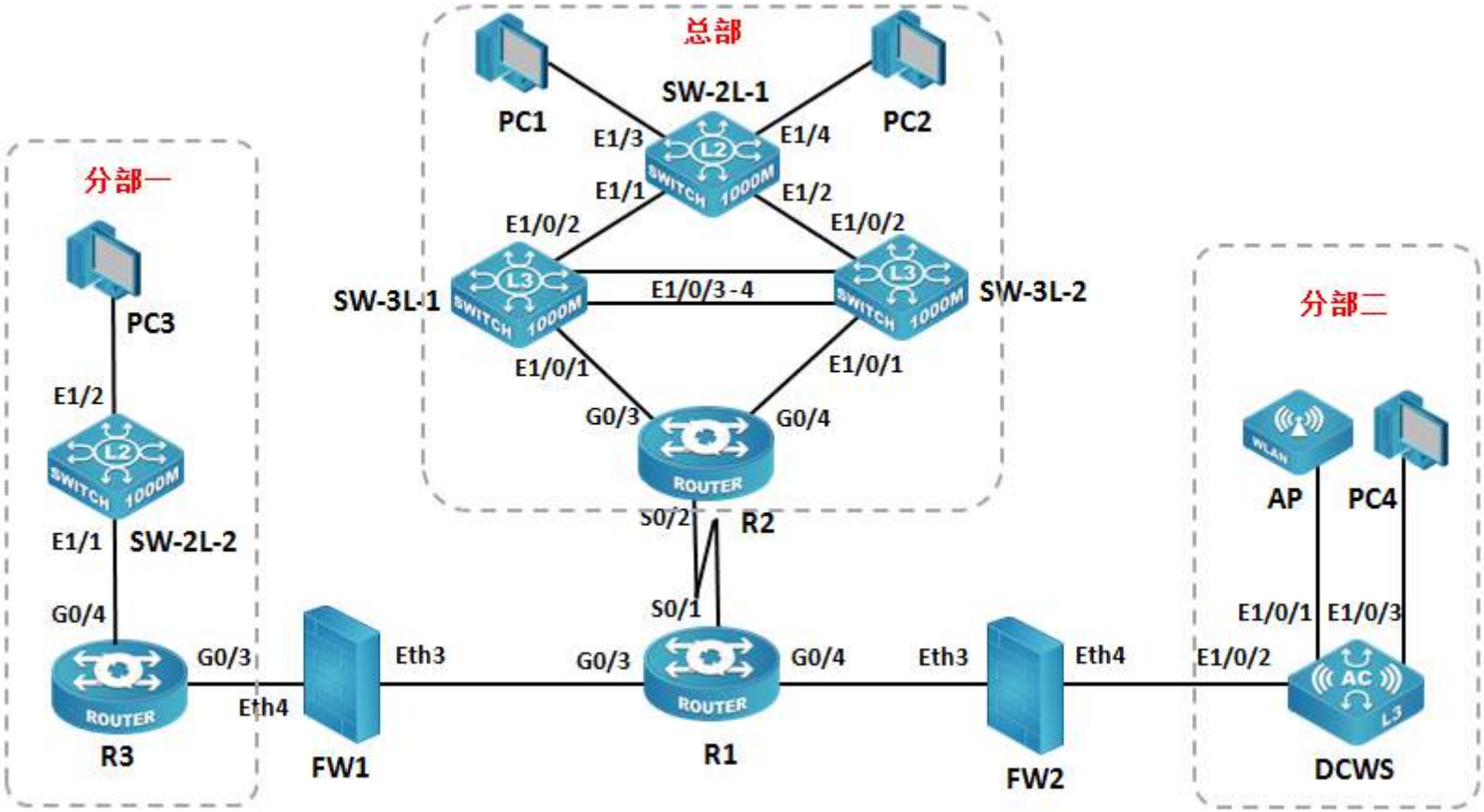

总部
PC1
PC2
SW-2L-1
E1/3
E1/4
E1/1
E1/2
E1/0/2
E1/0/2
SW-3L-1
E1/0/3-4
SW-3L-2
E1/0/1
E1/0/1
G0/3
G0/4
ROUTER
R2
S0/2
S0/1
分部一
PC3
E1/2
SW-2L-2
E1/1
G0/4
G0/3
ROUTER
R3
Eth4
FW1
Eth3
G0/3
G0/4
ROUTER
R1
Eth3
Eth4
FW2
分部二
AP
PC4
E1/0/1
E1/0/3
E1/0/2
AC
DCWS

表 1 网络设备连接表

A 设备连接至 B 设备			
设备名称	接口	设备名称	接口
R1	G 0/3	FW1	E0/3
R1	G 0/4	FW2	E0/3
R1	S 0/1	R2	S 0/2
R2	G 0/3	SW-3L-1	E 1/0/1
R2	G 0/4	SW-3L-2	E 1/0/1
R3	G 0/3	FW1	E0/4
R3	G 0/4	SW-2L-2	E 1/1
DCWS	E 1/0/2	FW2	E0/4
DCWS	E 1/0/1	AP	Lan
SW-3L-1	E 1/0/3	SW-3L-2	E 1/0/3
SW-3L-1	E 1/0/2	SW-2L-1	E 1/1
SW-3L-2	E 1/0/4	SW-3L-2	E 1/0/4
SW-3L-2	E 1/0/2	SW-2L-1	E 1/2
PC1	NIC	SW-2L-1	E 1/3
PC2	NIC	SW-2L-1	E 1/4
PC3	NIC	SW-2L-2	E 1/2
PC4	NIC	DCWS	E 1/0/3

表 2. 网络设备 IP 地址分配表

表 2 网络设备 IP 地址分配表

设备	设备名称	设备接口	IP 地址
路由器	R-1	G 0/3	200.200.1.1/30
		G 0/4	200.200.2.1/30
		S 0/1	200.200.3.1/30
		Loopback0	200.200.200.200/32
	R-2	G 0/3	10.10.10.1/30
		G 0/4	10.10.10.5/30
		S 0/2	200.200.3.2/30
	R-3	G 0/3	10.10.10.10/30
		G 0/4	————————
三层交换机	SW3-1	VLAN10 SVI	192.168.10.1/24
		VLAN20 SVI	192.168.20.1/24
		VLAN30 SVI	192.168.30.1/24
		VLAN40 SVI	192.168.40.1/24
		VLAN 1 SVI	10.10.10.2/30
	SW3-2	VLAN10 SVI	192.168.10.2/24
		VLAN20 SVI	192.168.20.2/24
		VLAN30 SVI	192.168.30.2/24
		VLAN40 SVI	192.168.40.2/24
		VLAN 1 SVI	10.10.10.6/30
防火墙 1	FW-1	Eth0/3	200.200.1.2/30
		Eth0/4	10.10.10.9/30
防火墙 2	FW-2	Eth0/3	200.200.2.2/30
		Eth0/4	10.10.100.0/24
无线控制器	DCWS	E1/0/24	10.10.100.200/24

表 3.服务器 IP 地址分配表

宿主机	虚拟主机名称	域名信息	服务角色	系统及版本信息	IPv4 地址信息
Server 1	Win2003-A1	dc.2015Network.com	域控制器 DNS 服务器 CA 证书服务器	Windows Server2003 R2	IP: 192.168.1.1
	Win2008-A1	dhcp.2015Network.com	DHCP 服务器	Windows Server 2008 R2	IP: 192.168.1.2
	Centos-A1	smb.jnds.net	SAMBA 共享服务器	Centos 6.5	IP: 192.168.1.3
Server 2	Win2008-B2	nps.2015Network.com	FTP 服务器 RADIUS 服务器	Windows Server 2008 R2	IP: 192.168.1.4
	Centos-B1	raid.jnds.net	逻辑卷及磁盘阵列服务	Centos 6.5	IP: 192.168.1.5
	Centos-B2	ftp.jnds.net ftp1.jnds.net ftp2.jnds.net	FTP 文件服务器	Centos 6.5	IP: 192.168.1.105 IP: 192.168.1.106 IP: 192.168.1.107
Server 3	Win2003-C1	tj.2015Network.com	子域控制器	Windows Server 2003 R2	IP:192.168.1.6
	Centos-C1	dns.jnds.net	BIND 域名服务器	Centos 6.5	IP: 192.168.1.109
Server 4(虚拟化)	Centos-D1	bbs.jnds.net	MySQL	Centos 6.5	IP: 192.168.1.161

竞赛题目

网络搭建部分（450 分）

【注意事项】

（1)设备 console 线有两条。交换机， AC，防火墙使用同一条 console 线，路由器使用另外一条 console 线。

（2)设备配置完毕后，保存最新的设备配置。保存文档方式分为两种：

交换机和路由器要把 show running-config 的配置保存在 PC1 桌面的相应文档中，文档命名规则为：设备名称.doc,例如：RT1 路由器文件命名为：RT1.doc，然后放入到 PC1 桌面上“比赛文档”文件夹中

防火墙等截图方式的设备，把截图的图片放到同一 word 文档中，文档命名规则为：设备名称.doc,例如：防火墙 FW1 文件命名为：FW1.doc, 保存后放入到 PC1 桌面上“比赛文档”文件夹中。

1、物理连接与 IP 地址划分

（1)按照网络拓扑图制作以太网网线，并连接设备。要求符合 T568A 和 T568B 的标准，其线缆长度适中。

（2)根据“拓扑结构图”和“表 2:网络设备 IP 地址分配表”所示，对网络中的所有设备接口配置 IP 地址。

2、交换机配置

（1)为交换机设备命名，命名规则参考为表 1 中的“设备名称”。

（2)在两台三层交换设备上开启 telnet 管理功能，同时要求每台网络设备只允许 5 条线路管理网络设备,管理设备使用 2015DCN 做为用户名,口令为 telnet123，enable 密码为 pwd@dcn。

（3)根据需求完成 vlan;

（4)总部的交换网络中,有 4 个 VLAN;财务部使用 VLAN10,名字为 CW,生产部使用 VLAN20,

名字为 SC，销售部使用 VLAN30，名字为 XS，技术部使用 VLAN40，名字 JS；

分部一的交换网络中，共 2 个 VLAN，分别为 VLAN100、VLAN200；

按下表要求将端口加入 VLAN：

设备名称	VLAN	端口
SW-2L-1	10	E 1/3
	20	E 1/4
	30	E 1/5 - 6
	40	E 1/7 - 8
SW-2L-2	100	E 1/2
	200	E 1/3

(5)使用端口汇聚技术，在 SW-3L-1 与 SW-3L-2 之间的链路启用端口汇聚，汇聚接口为动态方式，要求 SW-3L-1 为主动端，负载分担方式基于源、目地 MAC 及 IP 地址。

(6)配置生成树协议，要求启用 MSTP 协议，name 为 2015DCN，revision-level 1，实例 1 中包括 VLAN10、20；实例 2 中包括 VLAN30、40；要求 SW-3L-1 为实例 1 的主根，SW-3L-2 为实例 2 的主根，并互为备份根

(7)在三层交换机上启用路由功能，实现 VLAN 间互通。

(8)在三层交换之间启用 VRRP 协议，为 VLAN、10、20、30、40 实现网关备份，组地址为该 VLAN 中的最后一个可用 IP,SW-3L-1 为 VLAN10、20 的 master；SW-3L-2 为 30、40 的 master，且互为备份，开启抢占功能

(9)为 PC1 双向流量进行分析,网络分析仪将安装在 SW-2L-1 的 Ethernet1/20 接口下，请把相应流量映射给 Ethernet1/20 接口。

3、路由器配置与调试

(1)为路由设备命名，命名规则参考为表 1 中的“设备名称”。

(2)把下面的设备 RID 设置上，要求不能增加接口的相关信息。

设备名称	RID
R-2	2.2.2.2
SW-3L-1	5.5.5.5

SW-3L-2	6.6.6.6

(3)R2、SW-3L-1、SW-3L-2 三台设备运行 OSPF，实现内外互通，并在 R2 下发默认路由

(4)在 R3 配置单臂路由，实现 VLAN100、VLAN200 互通

(5)FW1、R3 之间运行 RIPv2 路由协议，并在 FW1 下发默认路由

(6)在 R3 连接 FW2 的端口上进行端口限速，限制速率上行 2000Kbps，下行 1000Kbps

4、广域网配置

(1)总部网络允许 VLAN10、VLAN20、VLAN30、VLAN40 的用户通过源 NAT 访问外网，类型为端口 NAT。

(2)分别在 FW1、FW2 上配置 NAT，实现内外访问外网。

(3)R-1 与 R-2 间并采用 PPP 封装，PAP 认证方式，R1 主认证方，用户名称为 DCN001 名称，密码：123456。

5、无线配置

(1)无线控制器建立 1 个 SSID,SSID 为 DCN01SSID 设置为隐藏，工作信道为自动；使用无线控制器提供 DHCP 服务，动态分配 IP 地址和网关，DNS 地址为：202.106.0.20，其分配的地址段为自行计算，需要排除网关，地址租约为 2 天。

(2)保障无线信息的覆盖性，无线 AP 的发射功率设置为 90%。

(3)为了控制带宽，保证正常使用，配置无线局域网用户上行速度为 2Mbps，下行速度为 5Mbps。

安全策略部分

1、防火墙配置

(1)把防火墙进行设备命名，命名规则参考为表 1 中的“设备名称”。

(2)FW1 禁止访问 www.taobao.com

(3)FW2 禁止访问 www.jd.com

(4)FW2 为了保证带宽的正常使用，限制 P2P 应用的下行带宽最高为 10M。

(5)FW1 限制 VALN100、200 的用户仅在工作日（周一到周五，9：00-18：00）允许访问网络。

(6)FW2 对关键字为“暴力”的网页内容进行过滤。

2、网络配置优化

（1)为了增加设备管理安全性，R2、R3 上开启 SSH 方式登录，SSH 登录用户分别为 R2SSH 和 R3SSH，密码为 Network2015（注意区分大小写）。

（2)限制 R2 的 SSH 登陆，仅允许 IP 地址为 192.168.10.10 的用户登录。

3、VPN 技术应用

（1)FW1 与 FW2 配置 IPSec VPN 的方式 进行互联。要求使用隧道模式，数据加密算法采用 3DES、认证算法采用 md5。

4、无线网络安全

（1)用户接入无线网络时需要输入密码，加密模式为 wpa-personal，其口令为：chinaskill。

（2)阻止 MAC 地址为 F0-DE-F1-F2-8C-CC 的主机连接的无线网络。

Windows 操作系统部分

【说明】

（1)题目中所涉及Windows操作系统的administrator管理员以及其他普通用户密码均为2015Netwlrk（注意区分大小写），若未按照要求设置密码，涉及到该操作的所有分值记为0分。

（2)虚拟主机的IP属性设置请按照网络拓扑结构图以及“表3:服务器IP地址分配表”的要求设定。

（3)除非作特殊说明，在同一主机下需要安装相同操作系统版本的虚拟机时，可采用Oracle VM VirtualBox软件自带的克隆系统功能实现。

（4)（所有系统镜像文件及试题所需的其它软件均存放在每台主机的 D:\soft 文件夹中，并将题目要求的截图内容以.jpg格式存储于桌面BACKUP文件夹中。

（5)题目要求的虚拟机均安装于每台主机的 D：\virtualPC 目录，即路径为 D：\virtualPC\虚拟主机名称。

（一）在 Server 1 上完成如下操作:

1、完成虚拟主机的创建

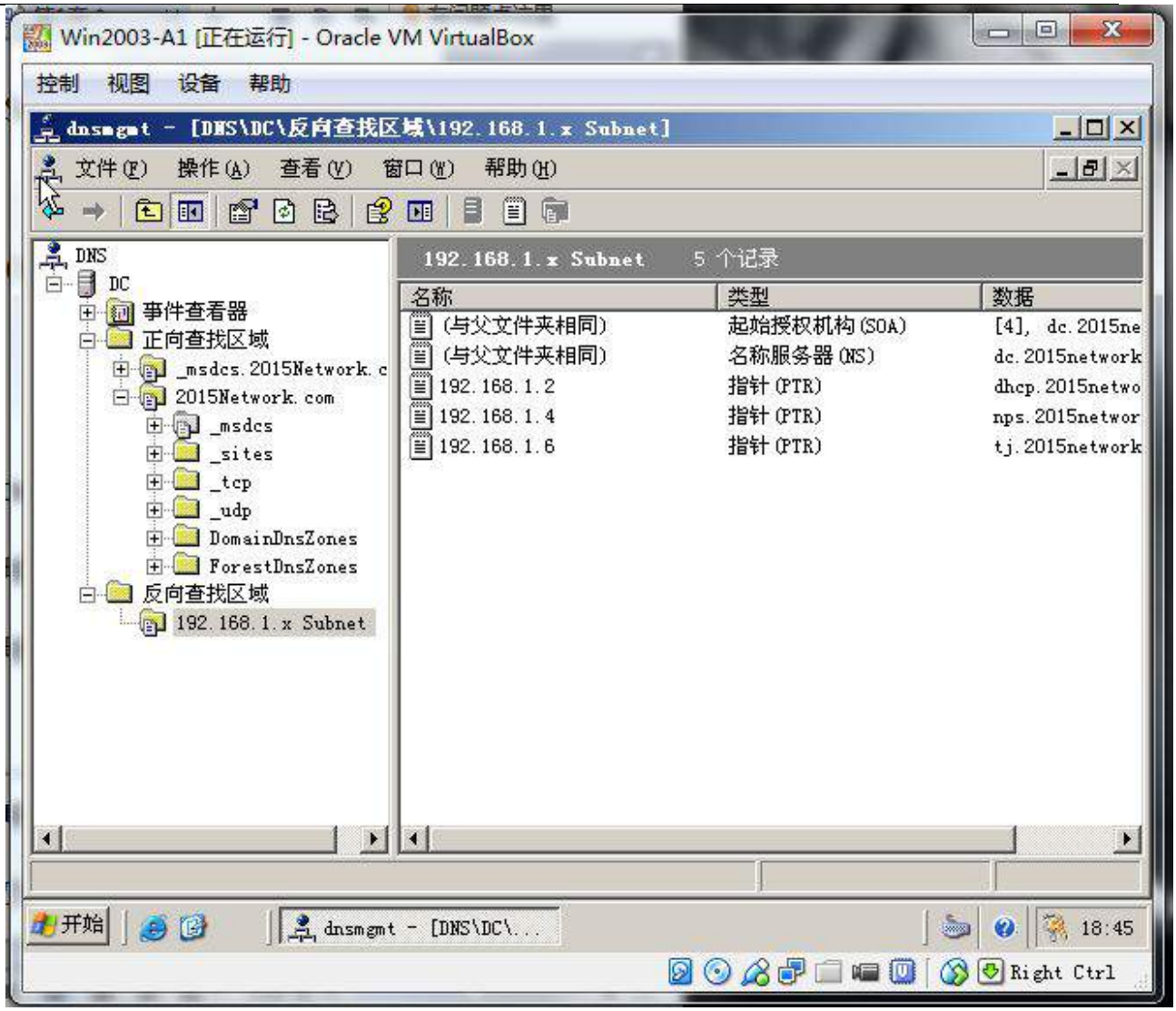
1）安装虚拟机“Win2003-A1”，具体要求为内存为512MB，硬盘20G,网卡为桥接模式；虚拟机分区分别为C、D、E；主分区一个，容量10G；扩展分区为10G，两个逻辑分区分别为5G。

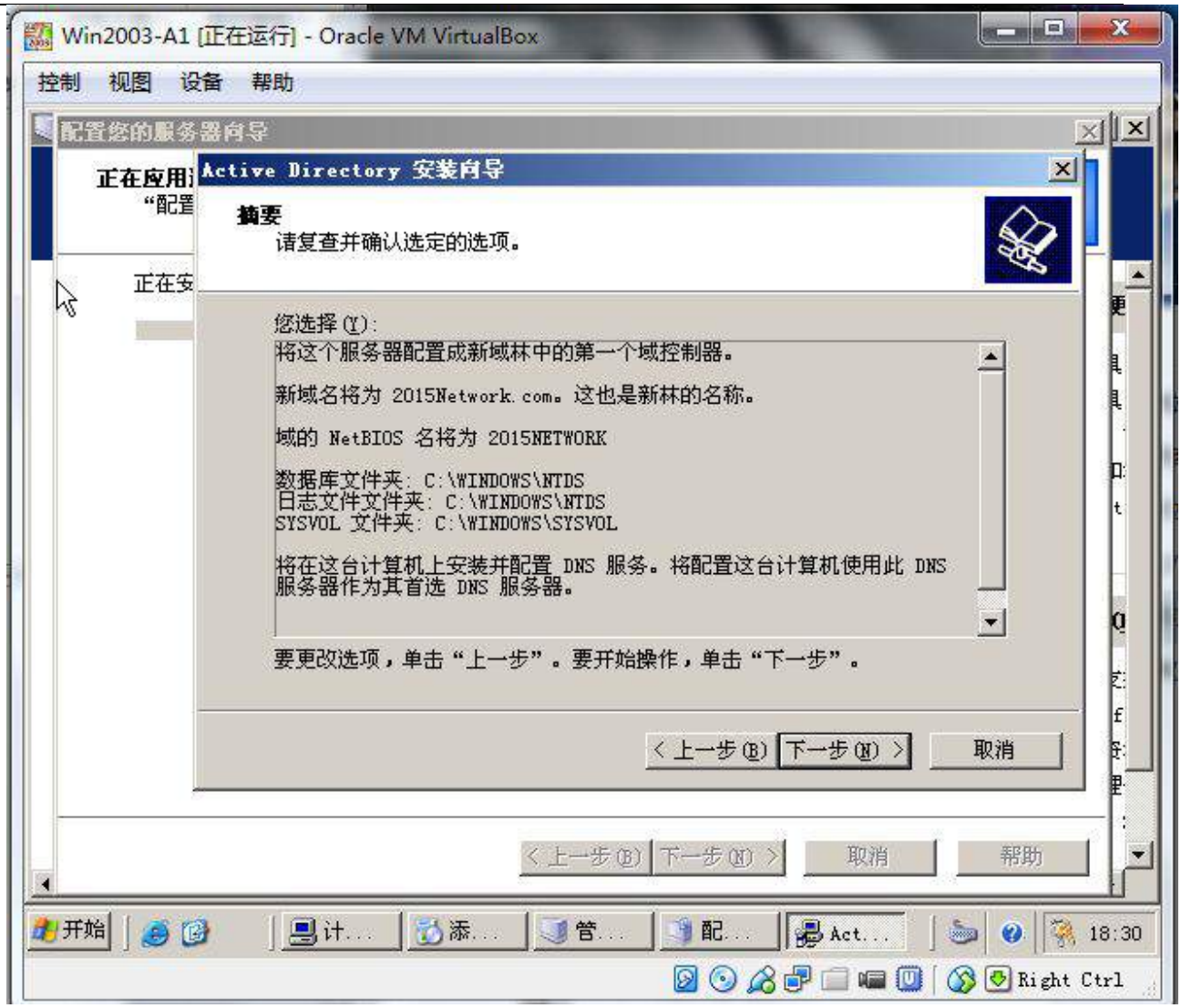
2）在虚拟机“Win2003-A1”中添加 SCSI 控制器，再添加三块 SCSI 虚拟硬盘，其每块硬盘的大小为 5G；制作成一个 RAID-5 卷，磁盘盘符为 F:\。

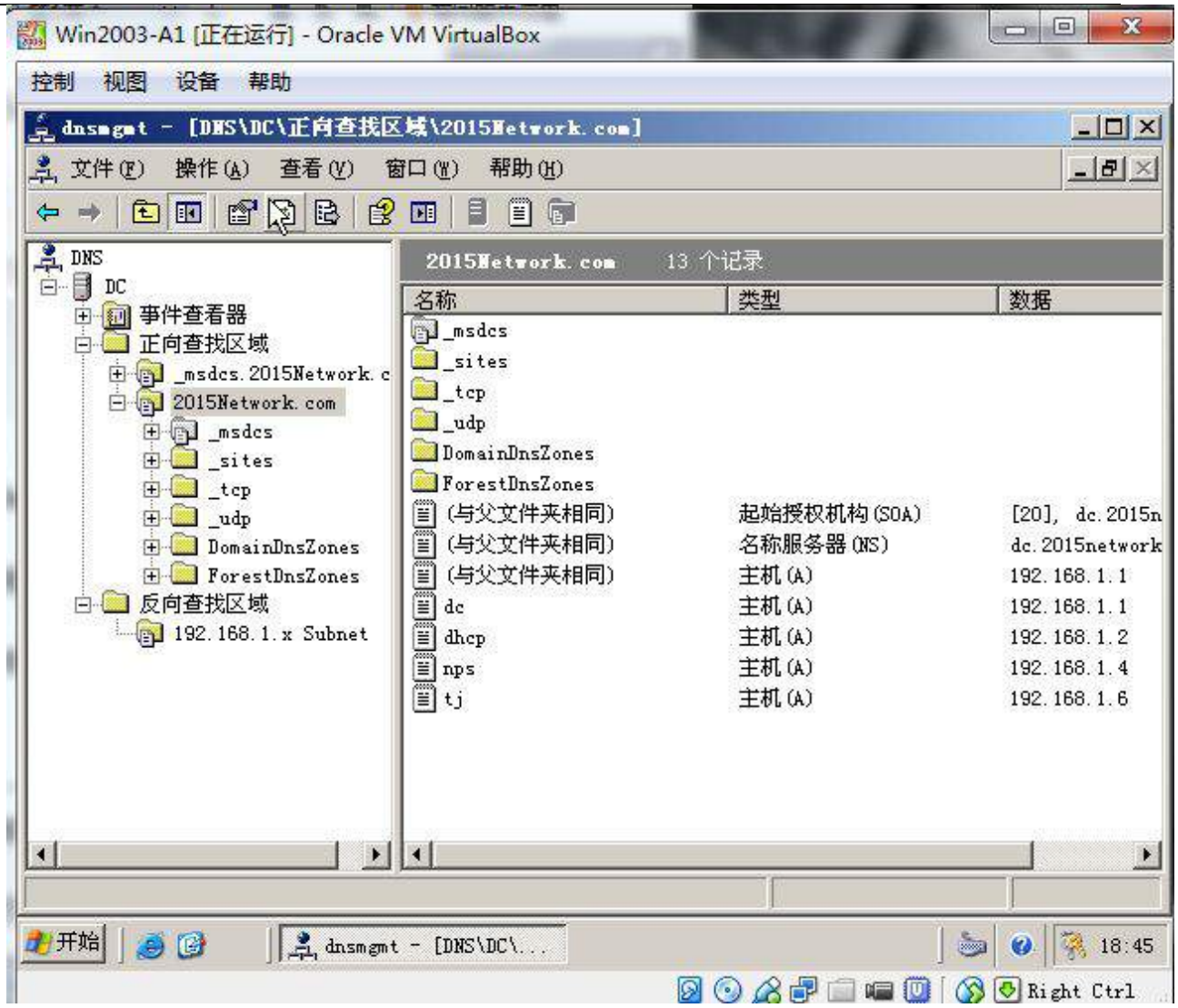
3）安装虚拟机“Win2008-A1”，具体要求为内存为 1G，硬盘 20G，并将该虚拟机加入到域中。

2、在主机 Win2003-A1 中完成域控制器的部署

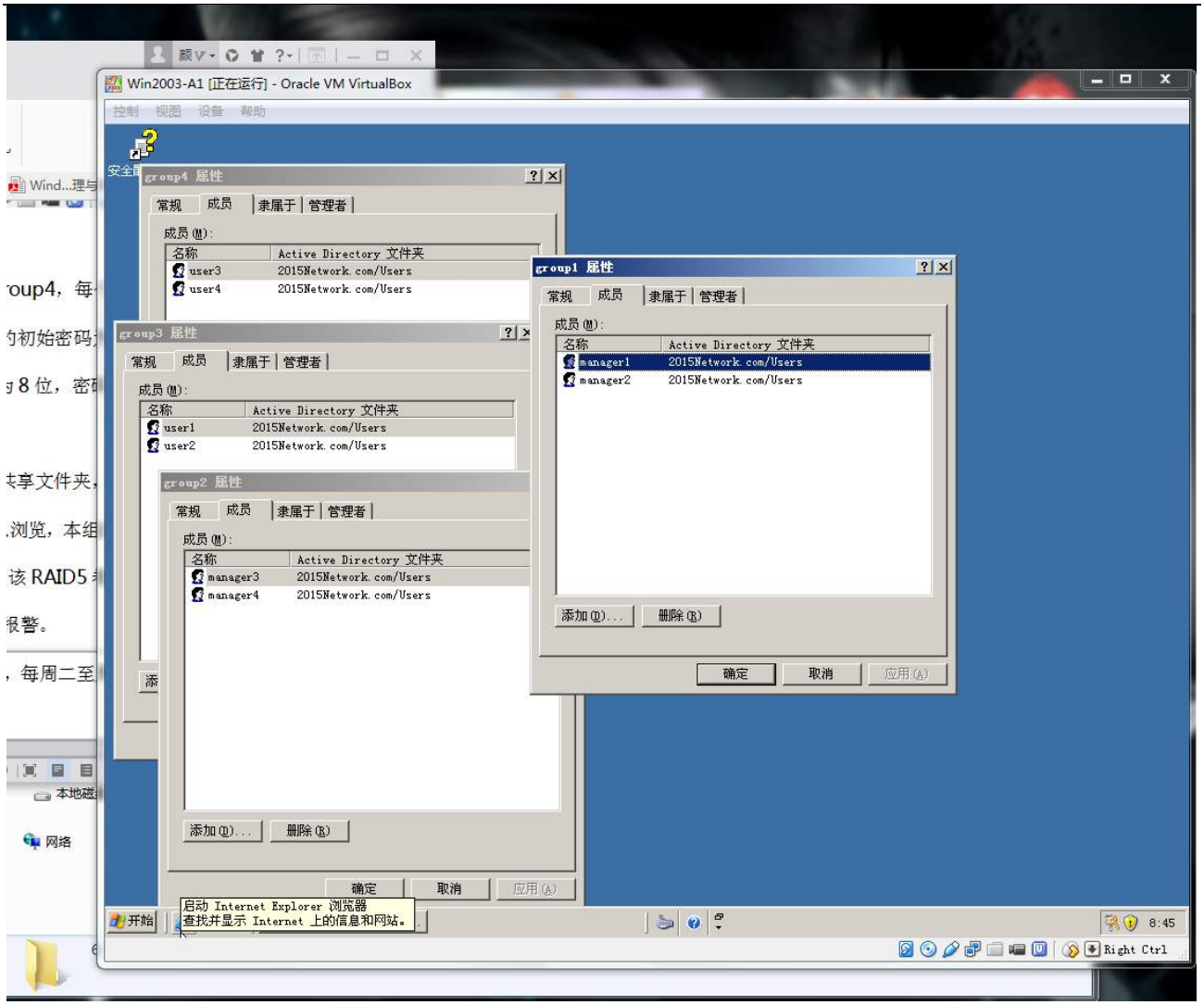
1）将在虚拟机“Win2003-A1”配置为主域控制器。域名为 2015Network.com，NetBIOS 域名为 2015Network，服务器的 FQDN 为 dc. 2015Network.com，域的功能级别为 2003 模式。同时，该服务器为 DNS 服务器，负责解析 2015Network.com 域名。实现 DNS 转发功能。

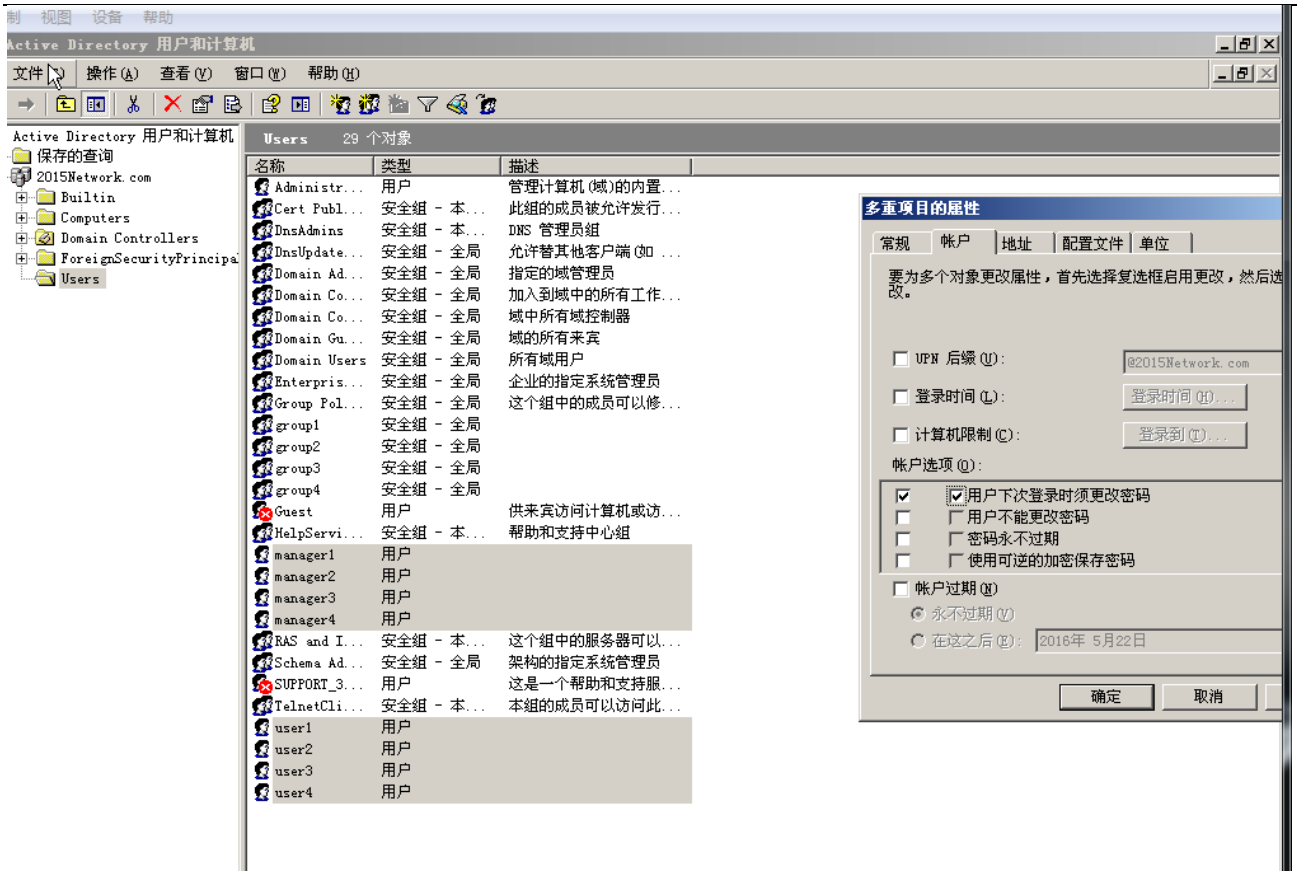

Win2003-A1 [正在运行] - Oracle VM VirtualBox
控制 视图 设备 帮助
dnsmgmt - [DNS\DC\反向查找区域\192.168.1.x Subnet]
文件(F) 操作(A) 查看(V) 窗口(W) 帮助(H)
DNS
DC
事件查看器
正向查找区域
_msdcs.2015Network.c
2015Network.com
_msdcs
_sites
_tcp
_udp
DomainDnsZones
ForestDnsZones
反向查找区域
192.168.1.x Subnet
192.168.1.x Subnet 5 个记录
名称 类型 数据
(与父文件夹相同) 起始授权机构(SOA) [4], dc.2015ne
(与父文件夹相同) 名称服务器(NS) dc.2015network
192.168.1.2 指针(PTR) dhcp.2015netwo
192.168.1.4 指针(PTR) nps.2015networ
192.168.1.6 指针(PTR) tj.2015network
开始
dnsmgmt - [DNS\DC\...
18:45
Right Ctrl


Win2003-A1 [正在运行] - Oracle VM VirtualBox
控制 视图 设备 帮助
配置您的服务器向导
正在应用
"配置
正在安
Active Directory 安装向导
摘要
请复查并确认选定的选项。
您选择(Y):
将这个服务器配置成新域林中的第一个域控制器。
新域名将为 2015Network.com。这也是新林的名称。
域的 NetBIOS 名将为 2015NETWORK
数据库文件夹: C:\WINDOWS\NTDS
日志文件文件夹: C:\WINDOWS\NTDS
SYSVOL 文件夹: C:\WINDOWS\SYSVOL
将在这台计算机上安装并配置 DNS 服务。将配置这台计算机使用此 DNS 服务器作为其首选 DNS 服务器。
要更改选项，单击"上一步"。要开始操作，单击"下一步"。
< 上一步(B)
下一步(N) >
取消
< 上一步(B)
下一步(N) >
取消
帮助
开始
计...
添...
管...
配...
Act...
18:30
Right Ctrl

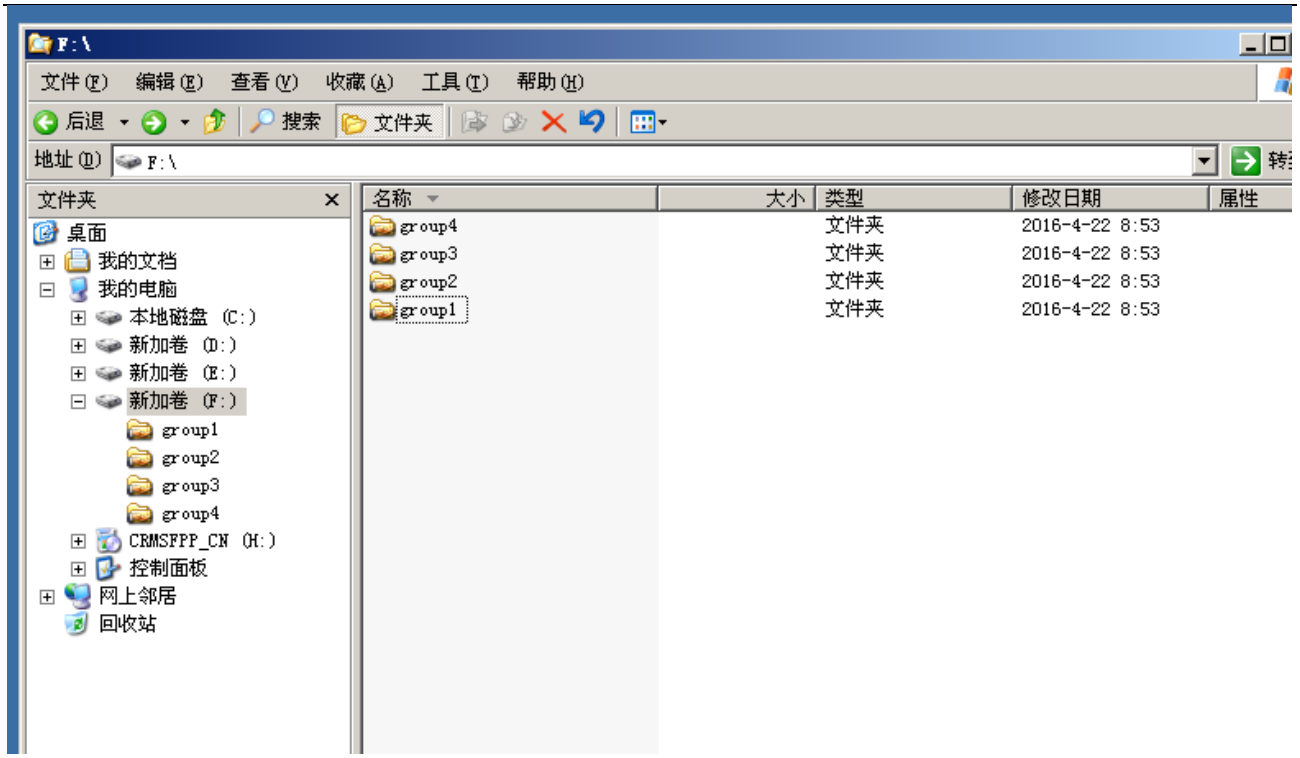


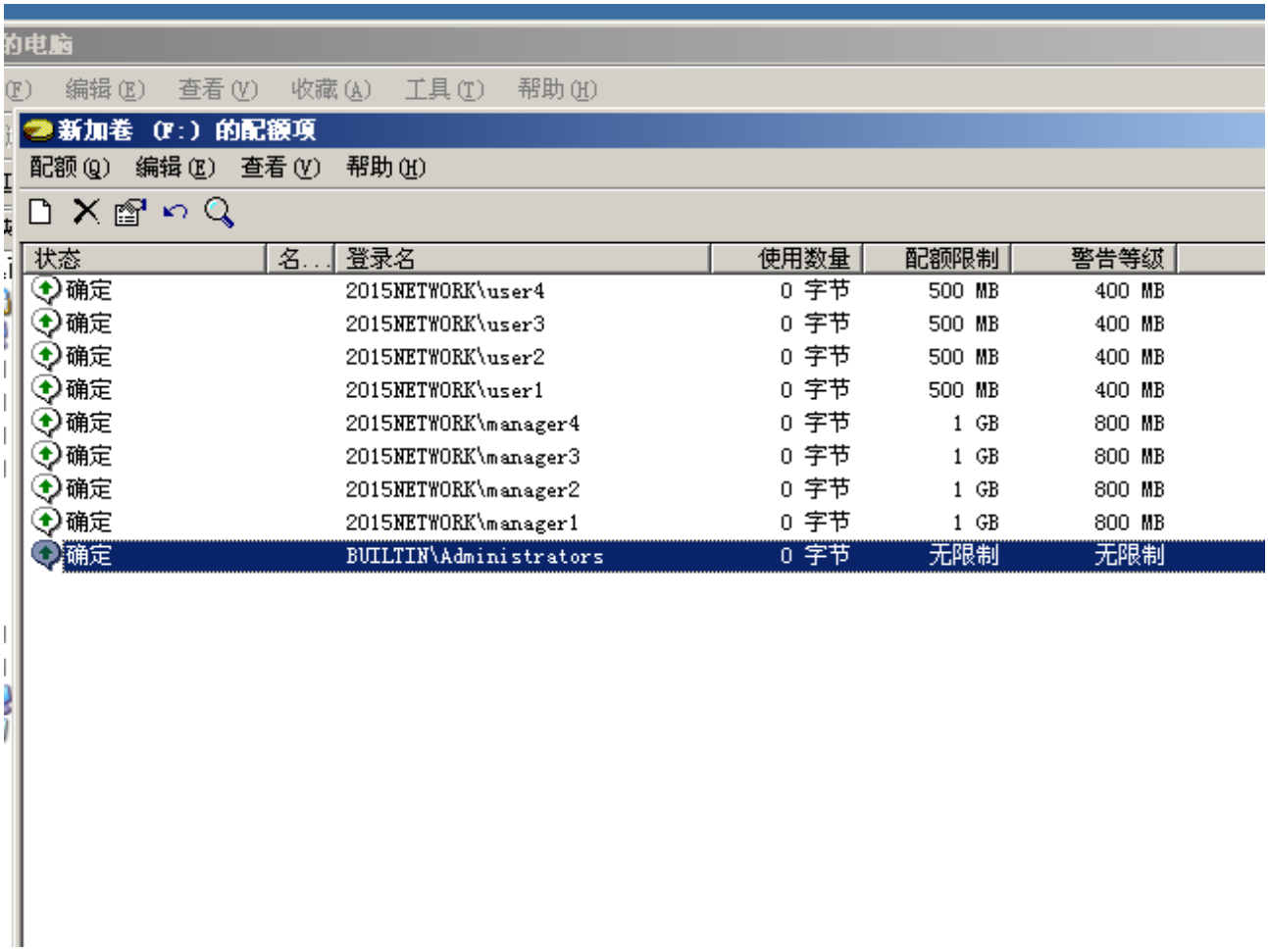
2）创建 4 个全局组，分别为 group1，group2，group3，group4，每个组都创建 2 个用户，依次分别为 manager1-manager4 和 user1-user4，用户的初始密码为“用户名＋1”，用户首次登录时须更改密码。采用复杂密码，密码长度最小为 8 位，密码最长存留其为 15 天，帐户锁定阈值为 2 次，如果到过阈值需要锁定 15 分钟。


Win2003-A1 [正在运行] - Oracle VM VirtualBox
控制 视图 设备 帮助
group4 属性
group3 属性
group2 属性
group1 属性
常规 成员 隶属于 管理者
成员(M):
名称 Active Directory 文件夹
user3 2015Network.com/Users
user4 2015Network.com/Users
user1 2015Network.com/Users
user2 2015Network.com/Users
manager3 2015Network.com/Users
manager4 2015Network.com/Users
manager1 2015Network.com/Users
manager2 2015Network.com/Users
添加(D)... 删除(R)
确定 取消 应用(A)
启动 Internet Explorer 浏览器
查找并显示 Internet 上的信息和网站。
开始
8:45
Right Ctrl

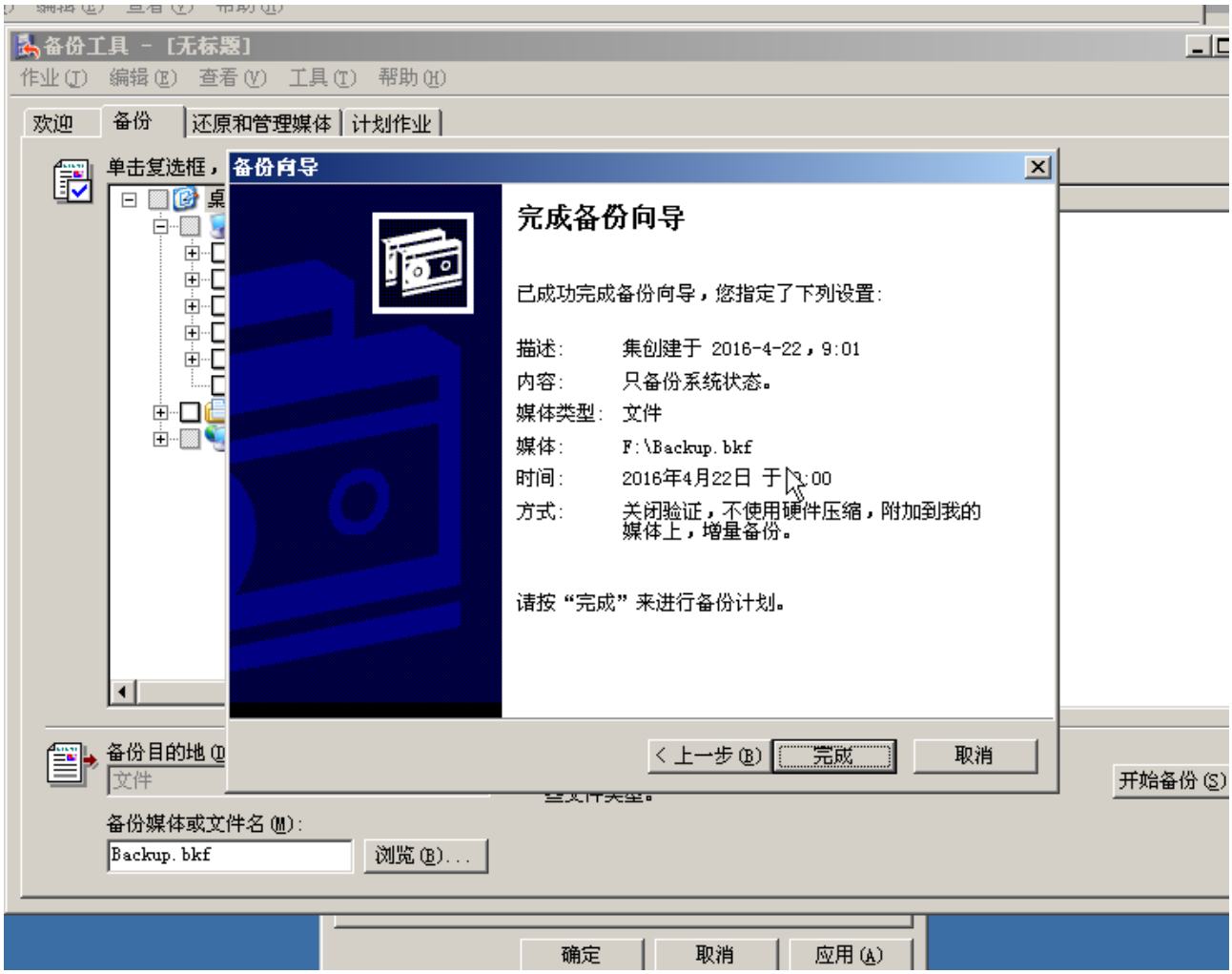


3）设置文件服务器，根据组的不同，在 RAID5 卷中建立 4 个共享文件夹，文件夹的名字分别为 group1- group4，共享权限设置为：其他组的成员仅可以浏览，本组的 user 可以上传文件，本组的 manager 具有完全控制权。所有的 manager 在该 RAID5 卷中的使用空间为 1G，超过 800M 报警；user 使用空间为 500M，超过 400M 报警。

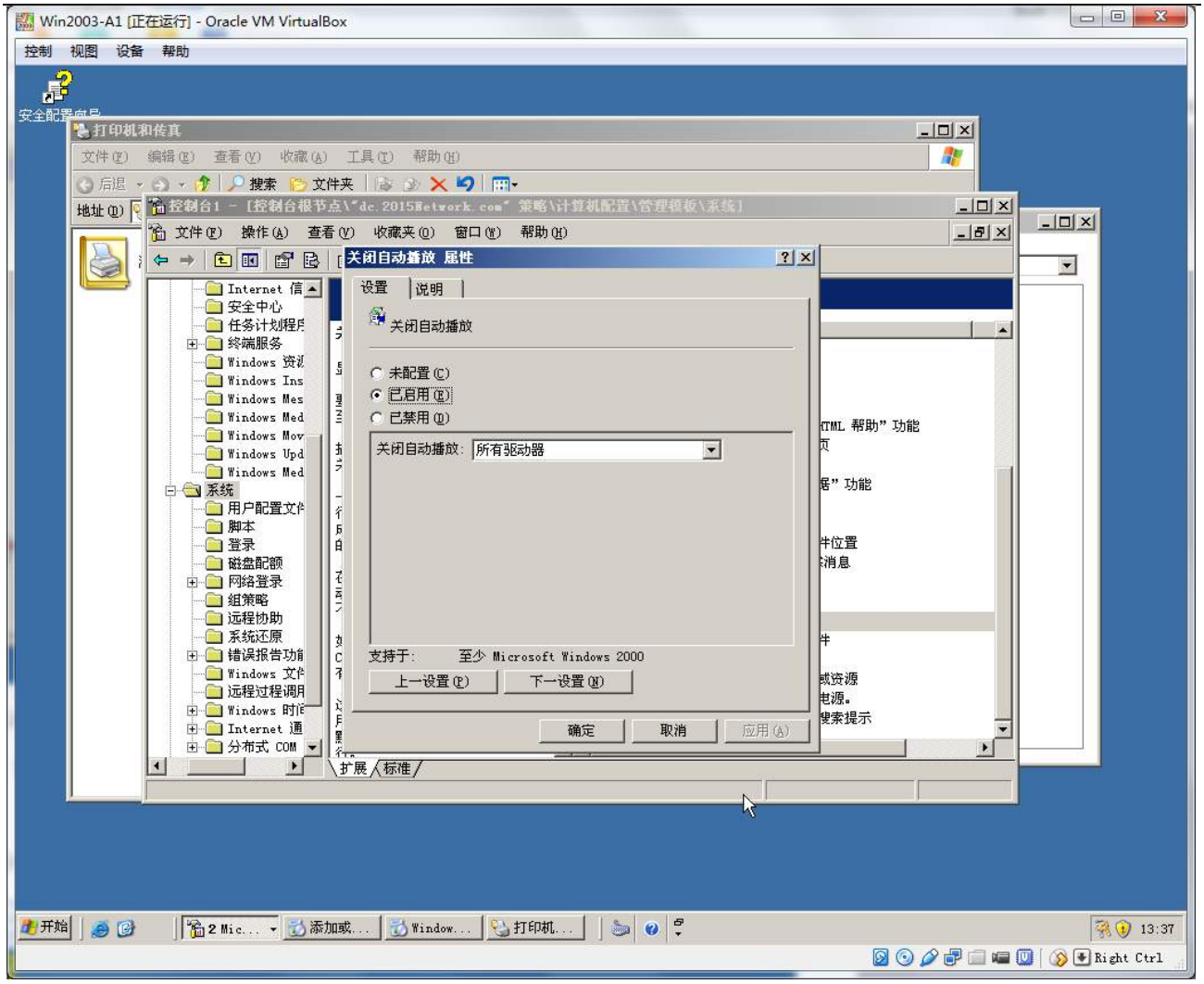

F:\
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
后退 搜索 文件夹
地址(D) F:\
文件夹
桌面
我的文档
我的电脑
本地磁盘 (C:)
新加卷 (D:)
新加卷 (E:)
新加卷 (F:)
group1
group2
group3
group4
CRMSFPP_CN (H:)
控制面板
网上邻居
回收站
名称 大小 类型 修改日期 属性
group4 文件夹 2016-4-22 8:53
group3 文件夹 2016-4-22 8:53
group2 文件夹 2016-4-22 8:53
group1 文件夹 2016-4-22 8:53


的电脑
(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
新加卷 (F:) 的配额项
配额(Q) 编辑(E) 查看(V) 帮助(H)
状态 名... 登录名 使用数量 配额限制 警告等级
确定 2015NETWORK\user4 0 字节 500 MB 400 MB
确定 2015NETWORK\user3 0 字节 500 MB 400 MB
确定 2015NETWORK\user2 0 字节 500 MB 400 MB
确定 2015NETWORK\user1 0 字节 500 MB 400 MB
确定 2015NETWORK\manager4 0 字节 1 GB 800 MB
确定 2015NETWORK\manager3 0 字节 1 GB 800 MB
确定 2015NETWORK\manager2 0 字节 1 GB 800 MB
确定 2015NETWORK\manager1 0 字节 1 GB 800 MB
确定 BUILTIN\Administrators 0 字节 无限制 无限制

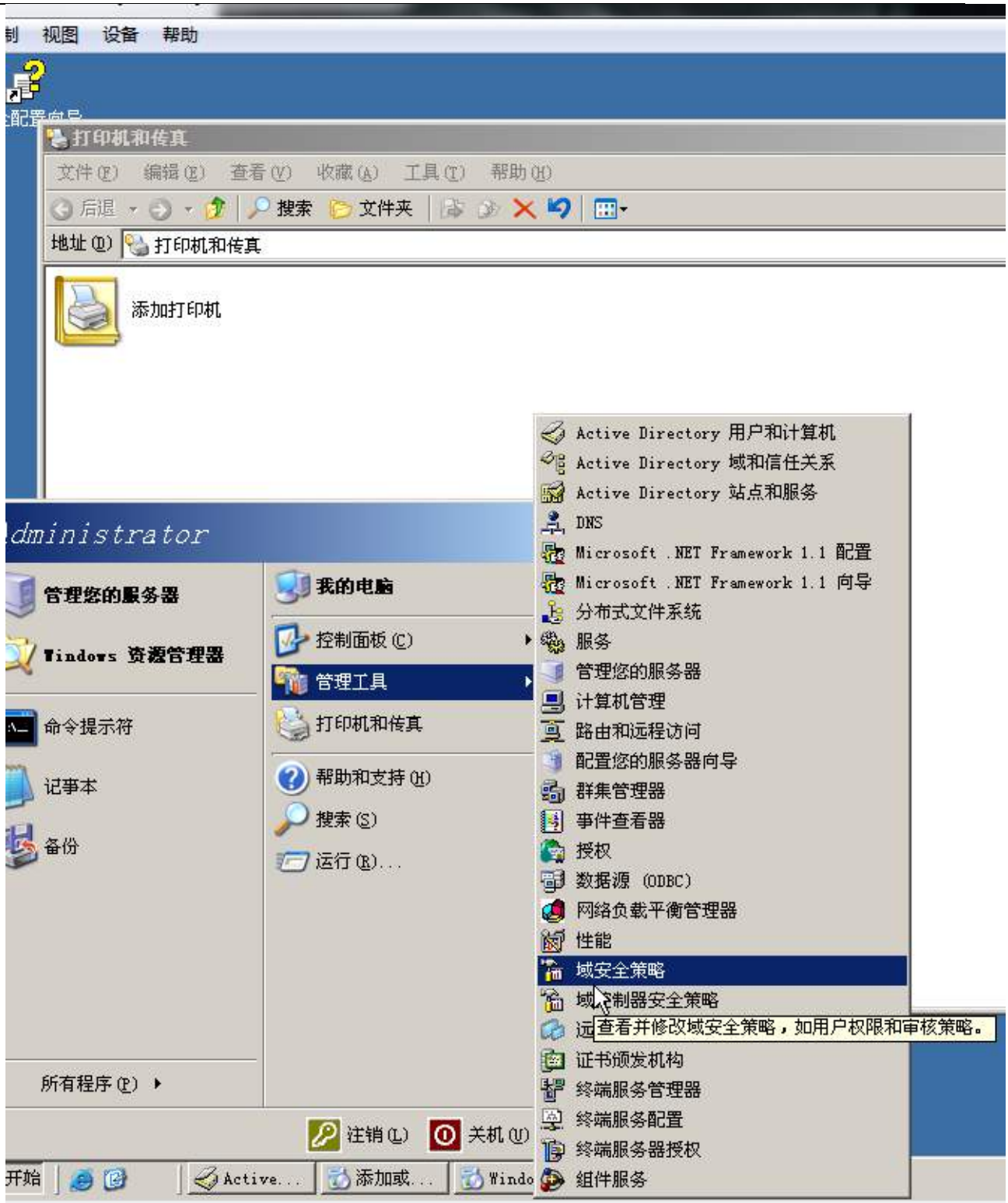
4）制定备份计划，每周一的午夜 0 点对活动目录进行正常备份，每周二至周五的午夜 0 点对活动目录进行增量备份，并将备份放置在 RAID5 卷中。



5）配置组策略，要求所有域内计算机“关闭自动播放”，所有用户不能使用 media player 软件，而部门经理和总经理除外。



6）在此域控制器上安装证书 CA 服务，并要求能够通过 WEB 申请证书。



3、在主机 Win2008-A1 中完成 DHCP 服务器的部署

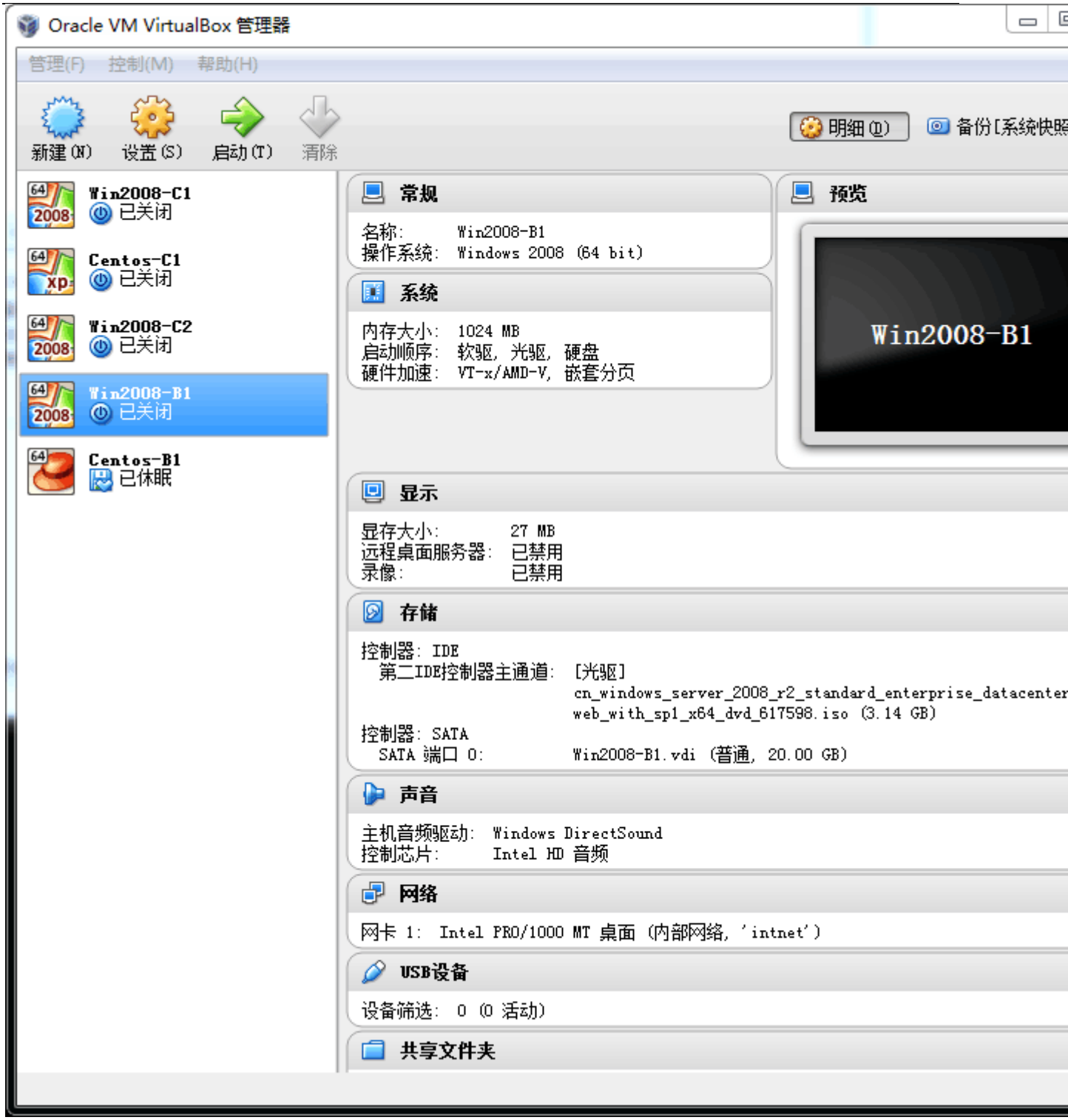
安装 DHCP 服务，为内网的用户主机动态分配 IPv4 地址，建立作用域，作用域的名称采用对应 VLAN 的名称，超级作用域的名称为 DHCPSERVER，为用户分配网关、DNS 服务

器及域名；此后将 DHCP 服务管理器有关超级作用域内容展开并截图存储为 dhcp.jpg；(20 分)

（二）在 Server 2 上完成如下操作:

1、完成虚拟主机的创建

1）安装虚拟机“Win2008-B1”，其内存为 1G，硬盘 20G，将服务器加入至 Windows 域中；



2、在主机 Win2008-B1 中完成 RADIUS 服务器的部署

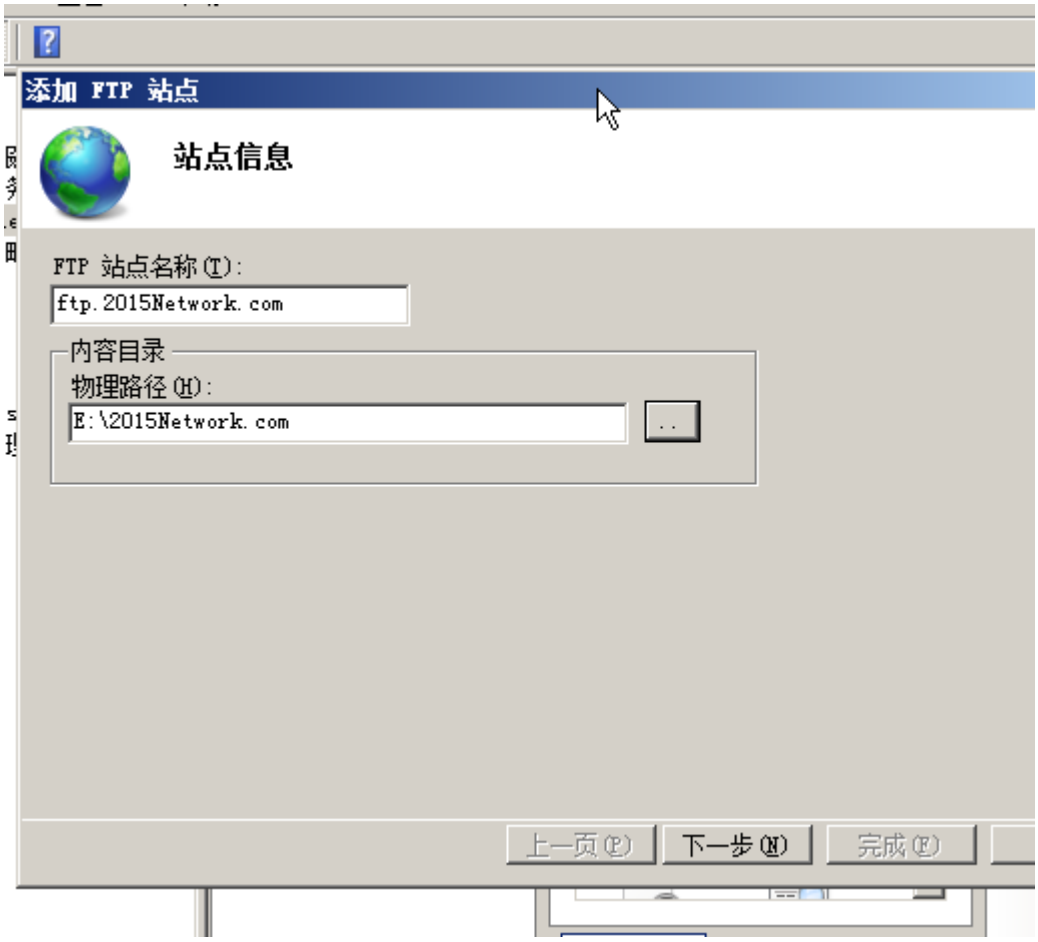
1）安装 RADIUS 服务，配置此服务器为 RADIUS 服务器，为网络提供 RADIUS 认证；

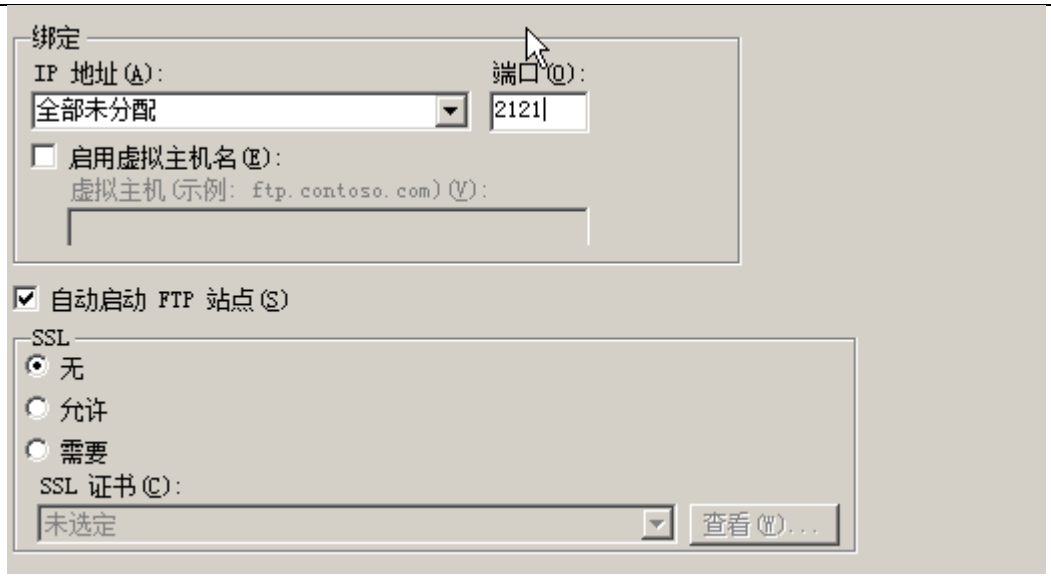
2）为了保障安全策略数据传送的安全性，需要对 RADIUS 服务器与域控制器服务器之

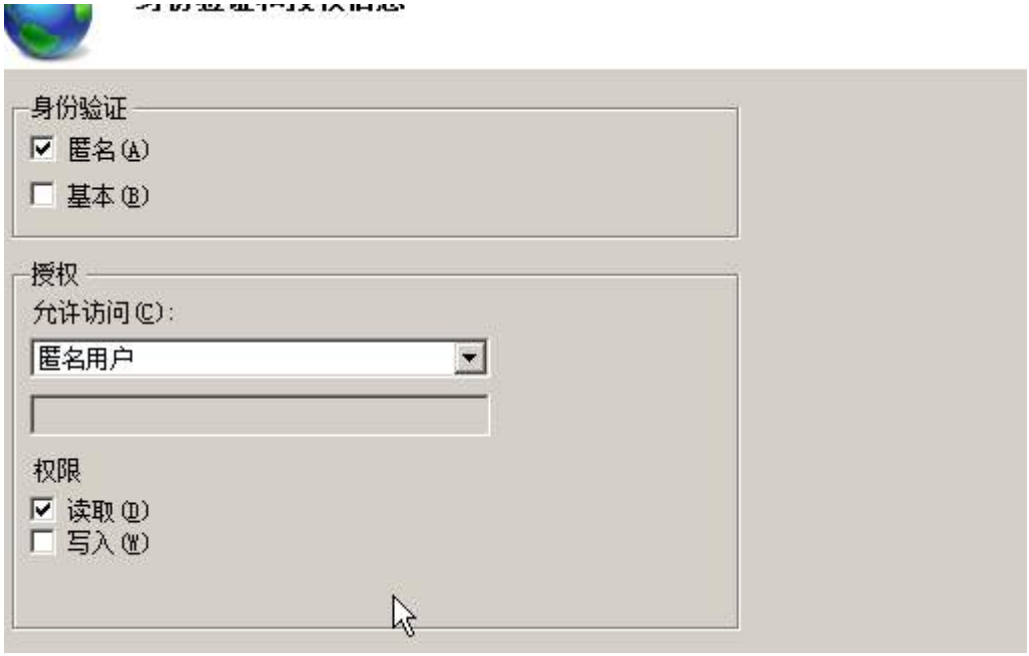
间的数据传输采用 IPSec 方式加密；并在命令提示符中键入 netsh ipsec static show policy all(后将输出截图并存储为 ipsec.jpg；

3、在主机 Win2008-B1 中完成 FTP 服务器的部署

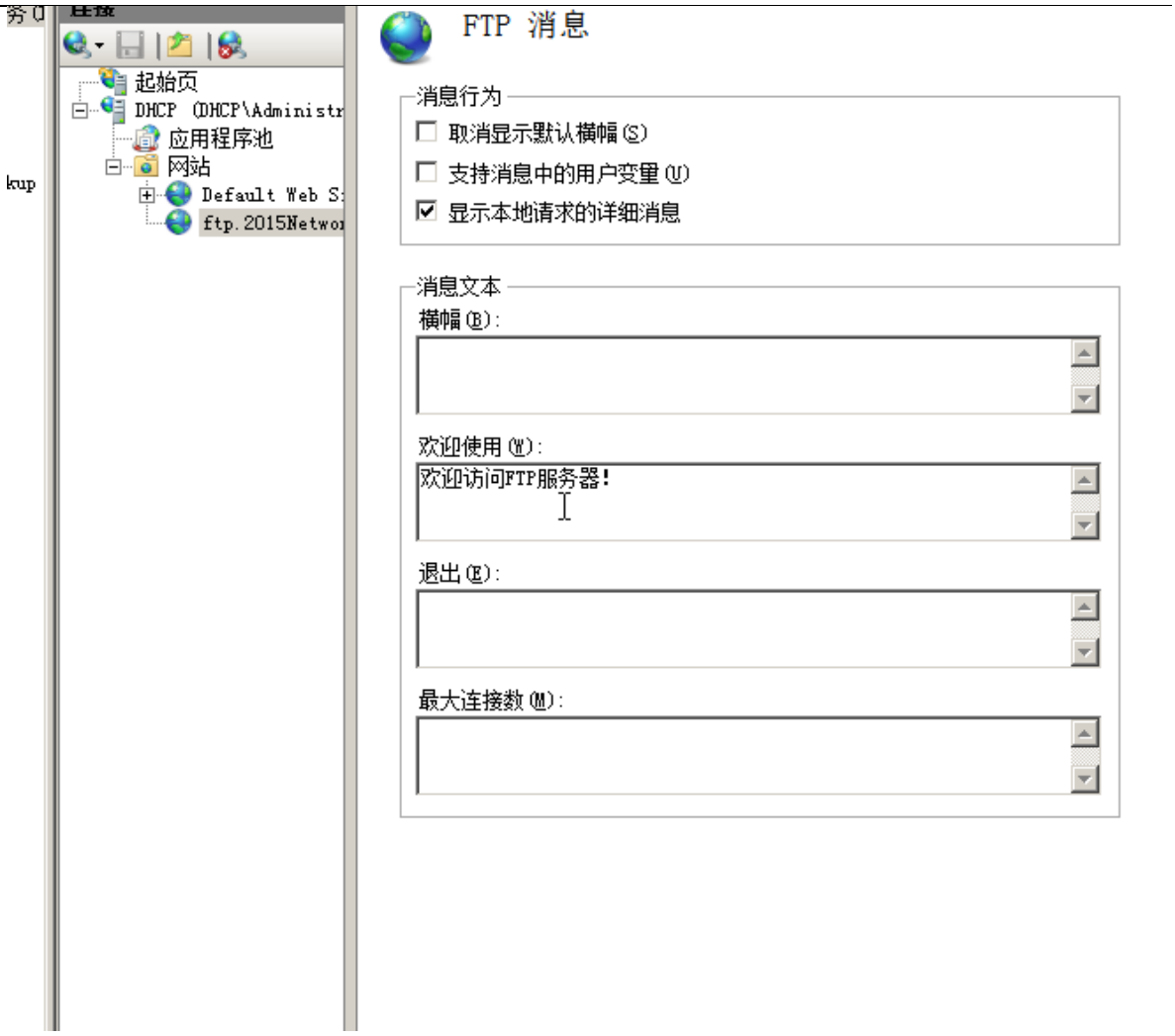
1）域名为 ftp.2015Network.com，端口号为 2121，只有内网用户才能访问 FTP 站点。要求站点主目录为 e:\ 2015Network.com，允许匿名登录，只能下载文件；使用 FTP 命令登录时，FTP 站点欢迎消息为：“欢迎访问 FTP 服务器！”,日志文件记录到 c:\ftproot\LogFiles 目录下。




绑定
IP 地址(A):
端口(O):
全部未分配
2121
启用虚拟主机名(E):
虚拟主机(示例: ftp.contoso.com)(V):
自动启动 FTP 站点(S)
SSL
无
允许
需要
SSL 证书(C):
未选定
查看(W)...


身份验证
匿名(A)
基本(B)
授权
允许访问(C):
匿名用户
权限
读取(D)
写入(W)


Internet 信息服务(IIS)管理器
DHCP ▸ 网站 ▸ ftp.2015Network.com ▸
连接
起始页
DHCP (DHCP\Administr
应用程序池
网站
Default Web S
ftp.2015Networ
FTP 日志
一个日志文件/每(O):
站点
日志文件
选择 W3C 字段(S)...
目录(Y):
C:\ftproot\LogFiles
浏览(B)...
编码(E):
UTF8
日志文件滚动更新
选择 FTP 用于创建新日志文件的方法。
计划(C):
每天
最大文件大小(字节)(Z):
不创建新的日志文件(N)
使用本地时间进行文件命名和滚动更新(U)



（三）在 Server 3 上完成如下操作:

1、完成虚拟主机的创建

1）在虚拟机“Win2003-C1”，其内存为 1G，硬盘 20G，并将服务器加入到 Windows 域环境；

2、在主机 Win2003-C1 中完成子域控制器的部署

1)配置此服务器为 2015Network.com 域的子域控制器，子域名 tj.2015Network.com，为并要求与父域建立双向的信任关系；

2）为了保障域数据传送的安全性，需要对父域控制器服务器与子域控制器服务器之间传输数据时，采用 IPSec 加密的方式进行传输；

Linux 操作系统和集群部分

【说明】

1、所有 Linux 操作系统的 root 用户的密码为 123456，若未按要求设置密码，涉及到该操作系统下的所有分值记为 0 分。

2、虚拟主机的 IP 属性设置请按照网络拓扑结构图以及“表 3：服务器 IP 地址分配表”的要求设定。

3、除有特别规定外，其他未明确规定用户密码均与用户名相同。

4、所有操作系统镜像文件及试题所需的其他软件均存放于每台计算机的/根目录下。

5、题目要求的虚拟机均安装于每台主机的 D：\virtualPC 目录，即路径为 D：\virtualPC\虚拟主机名称。

一、在 Server 1 上完成如下操作:

（一）完成虚拟主机的创建

1、安装虚拟机“Centos-A1”,具体要求为内存 512MB,硬盘 20GB；分区大小为：SWAP 分区大小为 1024M；/boot 分区大小为 500M，文件类型为 ext4；/根分区大小为 8G，文件类型为 ext4；/home 分区大小为 3G，文件类型为 ext4。

（二）在主机 Centos-A1 中完成 Samba 共享服务器的部署

1、在此服务器中安装配置 Samba 服务，创建四个用户 user1, user2, user3, manager，user1 和 user2 属于 finance 组，user3 属于 sales 组，manager 属于 manager 组。

```
[root@localhost samba]# useradd user1
[root@localhost samba]# useradd user2
[root@localhost samba]# useradd user3
[root@localhost samba]# useradd manager
```

```
[root@localhost samba]# smbpasswd -a user1
New SMB password:
Retype new SMB password:
Added user user1.
[root@localhost samba]# smbpasswd -a user2
New SMB password:
Retype new SMB password:
^[[AAdded user user2.
[root@localhost samba]# smbpasswd -a user3
New SMB password:
Retype new SMB password:
Added user user3.
[root@localhost samba]# smbpasswd -a manager
New SMB password:
Retype new SMB password:
Added user manager.
```

```
[root@localhost samba]# id user1
uid=500(user1) gid=500(finance) groups=500(finance)
[root@localhost samba]# id user2
uid=501(user2) gid=500(finance) groups=500(finance)
[root@localhost samba]# id user3
uid=502(user3) gid=501(sales) groups=501(sales)
[root@localhost samba]# id manager
uid=503(manager) gid=505(manager) groups=505(manager)
```

2、建立共享目录/opt/finance_share, /opt/sales_share, /opt/public_share。

```
[root@localhost opt]# mkdir /opt/finance_share
[root@localhost opt]# mkdir /opt/sales_share
[root@localhost opt]# mkdir /opt/public_share
[root@localhost opt]# chmod 777 /opt/finance_share/
[root@localhost opt]# chmod 777 /opt/sales_share/
[root@localhost opt]# chmod 777 /opt/public_share/
```

3、finance 组的用户对目录 finance 共享有读写权限。sales 组的用户对目录 sales_share 共享有读写权限，目录 public_share 允许所有人只读权限。manger 对所有目录均有读写权限。要求新建立的文件的权限是用户本身有完全权限，其它所有用户只有读取权。在 linux 系统和 WINDOWS 中能用 SAMBA 的共享打印机。

```
[root@localhost samba]# setfacl -R -m g:finance:rw /opt/finance_share/
[root@localhost samba]# setfacl -R -m g:sales:rw /opt/sales_share/
[root@localhost samba]# setfacl -R -m u::r /opt/public_share/
[root@localhost samba]# setfacl -R -m u:manager:rw /opt/finance_share/
[root@localhost samba]# setfacl -R -m u:manager:rw /opt/sales_share/
[root@localhost samba]# setfacl -R -m u:manager:rw /opt/public_share/
```

```
[root@localhost opt]# setfacl -R -m u:user1:rwx /opt/finance_share/
[root@localhost opt]# setfacl -R -m u:user2:rwx /opt/finance_share/
[root@localhost opt]# setfacl -R -m o::r /opt/finance_share/
[root@localhost opt]# setfacl -R -m u:user3:rwx /opt/sales_share/
[root@localhost opt]# setfacl -R -m o::r /opt/sales_share/
```

```
[printers]
        comment = All Printers
        path = /var/spool/samba
        browseable = no
        guest ok = yes
        writable = yes
        printable = yes
```

4、，将目录/opt/public_share 共享，共享名为 share，创建用户 Tonny，此用户不具有登陆系统功能，允许所有用户访问 public_share，具有读取和写入权限，无论是什么用户登录这个共享目录，在共享目录中建立的文件都是 Tonny 的。

```
[share]
path = /ope/sales_share
public =yes
write enable=yes
read only =yes
```

```
[root@localhost samba]# useradd -s /sbin/nologin Tonny
```

5、能够共享 samba 的计算机必须在 192.168.1.0/24 网段中。开机自启动 samba，并且在每周 2、5 的零点重启 samba 服务。

```
hosts allow=192.168.1.0/24
```

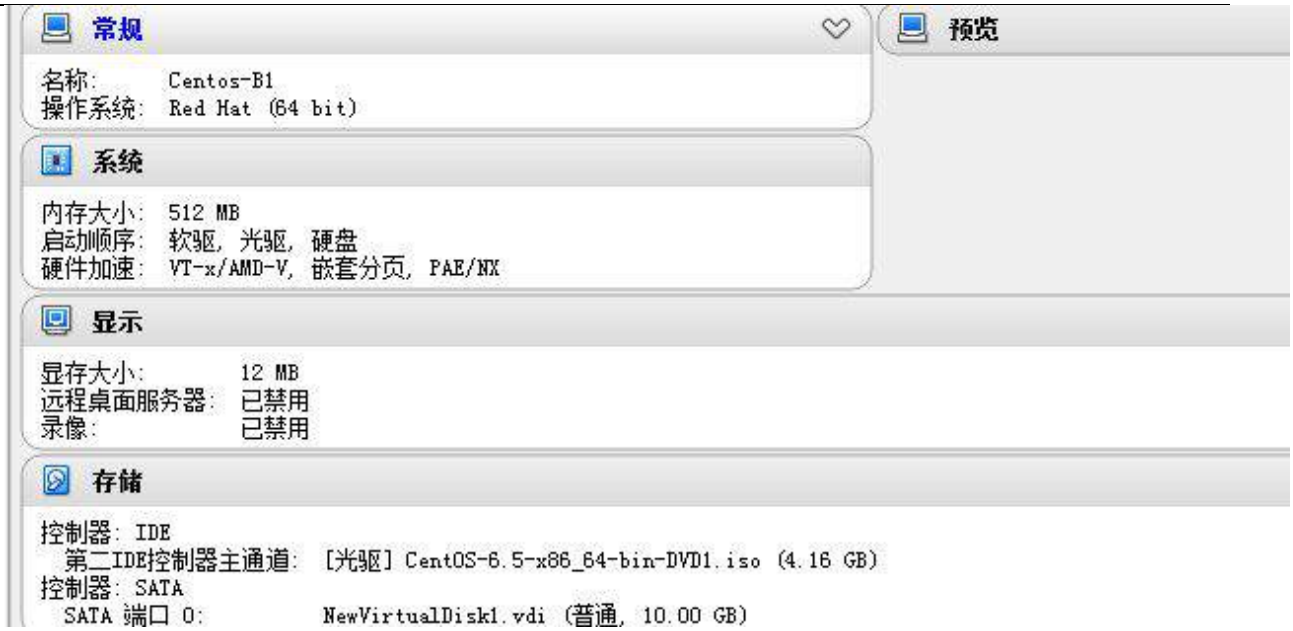
```
[root@localhost samba]# chkconfig smb on
```

```
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root
HOME=/

# For details see man 4 crontabs

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,f
ri,sat
# |  |  |  |  |
# *  *  *  *  * user-name command to be executed
  *  *  *  *  2 root service smb restart
  *  *  *  *  5 root service smb restart
```

二、在 Server 2 上完成如下操作：

（一）完成虚拟主机的创建

1、安装虚拟机“Centos-B1”,具体要求为内存 512MB，硬盘 10GB；



2、安装虚拟机“Centos-B2”，具体要求为内存 512MB，硬盘 10GB；

（二）在主机 Centos-B1 中完成磁盘管理的部署

1、在“Centos-B1”中额外添加

5 块硬盘，容量分别为 2G；

2、此操作需要 3 块硬盘，以前两块硬盘为基础建立冗余阵列 RAID1；要求每周 5 晚 24 点系统自动将第三块硬盘作为热备盘加入到 RAID1 中实现阶段性数据备份；

```
[root@localhost ~]# mdadm -C /dev/md0 -l 1 -n 2 /dev/sdb /dev/sdc
```

3、此操作需要 1 块硬盘，通过格式化建立两个主分区以及一个逻辑分区，利用这三个分区建立条带卷，要求条带容量为 16K，条带卷容量为 300M，并挂载到本地系统根目录下自建的 disk1 文件夹，且要求实现开机自动挂载；

```
Disk /dev/sde: 2147 MB, 2147483648 bytes
255 heads, 63 sectors/track, 261 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x200f71fe

   Device Boot      Start         End      Blocks   Id  System
/dev/sde1               1          65      522081   8e  Linux LVM
/dev/sde2              66         130      522112+  8e  Linux LVM
/dev/sde3             131         261     1052257+   5  Extended
/dev/sde5             131         261     1052226   8e  Linux LVM
```

```
[root@localhost etc]# lvcreate -i 3 -I 16 -L 300M -n LV1 VG1
  Logical volume "LV1" created
[root@localhost etc]# mkdir /disk1
[root@localhost etc]# mount /dev/VG1/LV1 /disk1/
```

```
#
# /etc/fstab
# Created by anaconda on Fri Apr 22 08:06:56 2016
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
UUID=cca060ab-bf2c-4dd2-9a24-43adda5f1bda /                       ext4    defaul
ts        1 1
UUID=f3cdcd41-bdd2-42bc-9217-d09b288e5850 /boot                   ext4    defaul
ts        1 2
UUID=dbc7ed21-67ee-4fc0-90b6-3588561fffcc /home                   ext4    defaul
ts        1 2
UUID=5a2d6bb3-a467-4dd1-9077-62e21e209d7a swap                    swap    defaul
ts        0 0
tmpfs                   /dev/shm                tmpfs   defaults        0 0
devpts                  /dev/pts                devpts  gid=5,mode=620  0 0
sysfs                   /sys                    sysfs   defaults        0 0
proc                    /proc                   proc    defaults        0 0
/dev/VG1/LV1            /disk1                  ext3    defaults        0 0_
```

4、此操作需要 1 块硬盘，通过格式化建立两个主分区以及一个逻辑分区，创建一个逻辑卷。逻辑卷命名为 engineering，属于卷组 vol，且大小为 10 个扩展；在卷组 vol 的逻辑卷每个扩展的大小为 32MiB；使用 vfat 格式化这个新的逻辑卷，此逻辑卷在系统启动的时候应该能自动挂在到/mnt/engineering.

```
Disk /dev/sdf: 2147 MB, 2147483648 bytes
255 heads, 63 sectors/track, 261 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0xa4e269c1

   Device Boot      Start         End      Blocks   Id  System
/dev/sdf1               1          65      522081   8e  Linux LVM
/dev/sdf2              66         130      522112+  8e  Linux LVM
/dev/sdf3             131         261     1052257+   5  Extended
/dev/sdf5             131         261     1052226   8e  Linux LVM
```

（三）在主机 Centos-B2 中完成 FTP 服务器的部署

1、Linux 服务器提供网站服务，现采用提供虚拟主机基于域名 ftp.jnds.net 的 FTP 服务，实现对网站 www.jnds.com 维护的功能。

```
write_enable=YES
```

2、为网站管理员创建一个 FTP 帐户 webmaster，将其加入到 ftp 组中，其登录的主目录为 WEB 站点的主目录/var/www/jnds.net，设置其为系统帐户，但却没有登录系统的权限，备注该用户为“FTP User。

```
[root@localhost vsftpd]# useradd -g ftp -d /var/www/jnds.net -r -s /sbin/nologin
 -c "FTP User" webmaster
```

3、利用该帐户登录后，可对 WEB 站点根目录及其子目录下的文件进行上传、下载、创建子目录、更名和删除操作，用户只能对自己的 WEB 站点根目录及其下面的目录文件操作，不允许切换到上级目录，不允许匿名用户登录和访问。

```
#anonymous_enable=YES
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
chroot_local_user=YES
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
local_umask=022
```

三、在 Server 3 上完成如下操作：

（一）完成虚拟主机的创建

1、安装名为“Centos-C1”的虚拟机，具体要求为硬盘大小为 12GB，内存为 512MB，系统为 Centos6.5。分区大小为：SWAP 分区大小为 1024M；/boot 分区大小为 500M，文件类型为 ext4；其余为/分区，文件类型为 ext4；

（二）在主机 Centos-C1 中完成 BIND 域名服务器及系统基本配置。

1、在此服务器中安装配置 bind 服务，负责区域“jnds.net”内主机解析，五台主机分别为 dns.jnds.net 、www.jnds.net、bbs.jnds.net、smb.jnds.net、ftp.jnds.net 以及 mail.jnds.net,做好正反向 DNS 服务解析，对访问 2015Network.com 域的解析转发给 win2003_A1 ；

```
$TTL 1D
@       IN SOA  ns.jnds.net.    root.jnds.net. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
ns      IN      A       192.168.1.109
@       IN      NS      ns.jnds.net.
dns     IN      A       192.168.1.109
smb     IN      A       192.168.1.3
bbs     IN      A       192.168.1.161
ftp     IN      A       192.168.1.105
```

```
$TTL 3H
@       IN SOA  ns.jnds.net.    root.jnds.net. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
@       IN      NS      ns.jnds.net.
109     IN      PTR     ns.jnds.net.
109     IN      PTR     dns.jnds.net.
3       IN      PTR     smb.jnds.net.
161     IN      PTR     bbs.jnds.net.
105     IN      PTR     ftp.jnds.net._
```

```
options {
        listen-on port 53 { any; };
        listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        allow-query     { any; };
        recursion yes;
        forwarders{192.168.1.1;};_
```

2、为用户提供域名解析禁止 ip 为 192.168.1.161 的机器解析。

```
        blackhole{192.168.161;};_
```

3、新建目录/tmp/jnds，配置该目录的权限。复制文件/etc/fstab 到/tmp/jnds。配置

/tmp/jnds/fstab 权限。文件/var/tmp/fstab 所有者是 root，属于 root 组，文件/var/tmp/fstab 不能被任何用户执行，用户 sunny 可读和可写/tmp/jnds/fstab，用户 mike 既不能读也不能写/tmp/jnds/fstab，所有其他用户对/tmp/jnds/fstab 目录有只读权限。

```
[root@localhost etc]# mkdir /tmp/jnds
[root@localhost etc]# cp -p /etc/fstab /tmp/jnds/
[root@localhost etc]# cp -p /etc/fstab /var/tmp/
[root@localhost etc]# chown root:root /var/tmp/fstab
[root@localhost etc]# chmod 666 /var/tmp/fstab
[root@localhost etc]# useradd sunny
[root@localhost etc]# useradd mike
[root@localhost etc]# setfacl -R -m u:sunny:rw /tmp/jnds/fstab
[root@localhost etc]# setfacl -R -m u:mike:x /tmp/jnds/fstab
[root@localhost etc]# setfacl -R -m o::r /tmp/jnds/fstab
```

四、在 Server 4 上完成如下操作：

（一）完成虚拟主机的创建

1、Server4 主机系统为 CentOS6.5，需要在此 Linux 平台上采用 KVM 方式安装虚拟机“Centos-D1”，具体要求为硬盘大小为 12GB，内存为 768MB，系统为 CentOs6.5；（小提示：如无法正确安装虚拟机 Centos-D1，下述题目中所涉及的虚拟机题目可在 Server4 真实主机中完成）

（二）在主机 Centos-D1 中完成 MySQL 数据库服务器的部署

1、采用 MySQL 数据库作为认证来源，创建用户认证数据库为 www，建立保存用户名及密码的表名为 users，建立 web1 以及 web2 两个用户，将其密码均设置为 6666，并对密码采用 password 函数加密，表结构如下；

字段名	数据类型	主键	自增
ID	int	是	是
name	varchar(10)	否	否
birthday	datetime	否	否
sex	char(1)	否	否
Password	Char（8）	否	否

```
mysql> create database www;
Query OK, 1 row affected (0.00 sec)

mysql> use www
Database changed
mysql> create table users(
    -> ID int primary key auto_increment,
    -> name varchar(10),
    -> birthday datetime,
    -> sex char(1),
    -> Password char(8));
Query OK, 0 rows affected (0.05 sec)
```

```
mysql> desc users;
+----------+-------------+------+-----+---------+----------------+
| Field    | Type        | Null | Key | Default | Extra          |
+----------+-------------+------+-----+---------+----------------+
| ID       | int(11)     | NO   | PRI | NULL    | auto_increment |
| name     | varchar(10) | YES  |     | NULL    |                |
| birthday | datetime    | YES  |     | NULL    |                |
| sex      | char(1)     | YES  |     | NULL    |                |
| Password | char(8)     | YES  |     | NULL    |                |
+----------+-------------+------+-----+---------+----------------+
5 rows in set (0.00 sec)
```

```
mysql> insert into users(name,Password)value("web1",password("6666"));
Query OK, 1 row affected, 1 warning (0.00 sec)

mysql> insert into users(name,Password)value("web2",password("6666"));
Query OK, 1 row affected, 1 warning (0.00 sec)

mysql> select * from users;
+----+------+----------+------+----------+
| ID | name | birthday | sex  | Password |
+----+------+----------+------+----------+
|  1 | web1 | NULL     | NULL | *1C73826 |
|  2 | web2 | NULL     | NULL | *1C73826 |
+----+------+----------+------+----------+
2 rows in set (0.00 sec)
```

2015 年全国职业院校技能大赛

网络搭建与应用竞赛

（总分 1000 分）

赛题说明

一、竞赛内容分布

“网络搭建与应用”竞赛共分二个部分，其中：

第一部分：网络搭建及安全部署项目，占总分的比例为 45%；

第二部分：服务器配置及应用项目，占总分的比例为 55%；

二、竞赛注意事项

（1）禁止携带和使用移动存储设备、计算器、通信工具及参考资料。

（2）请根据大赛所提供的比赛环境，检查所列的硬件设备、软件清单、材料清单是否齐全，计算机设备是否能正常使用。

（3）本试卷共有两个部分。请选手仔细阅读比赛试卷，按照试卷要求完成各项操作。

（4）操作过程中，需要及时保存设备配置。比赛结束后，所有设备保持运行状态，不要拆、动硬件连接。

（5）比赛完成后，比赛设备、软件和赛题请保留在座位上，禁止将比赛所用的所有物品（包括试卷和草纸）带离赛场。

（6）所有需要提交的文档均放置在桌面的 PC1“比赛文档”文件夹中，禁止在纸质资料上填写与竞赛无关的标记，如违反规定，可视为 0 分。

（7）裁判以各参赛队提交的竞赛结果文档为主要评分依据。所有提交的文档

必须按照赛题所规定的命名规则命名，文档中有对应题目的小标题，截图有截图的简要说明，否则按无效内容处理。

（8）与比赛相关的工具软件放置在 D 盘的 tools 文件夹中。

项目简介

某集团公司经过业务发展，总公司在北京市，在上海设置了分公司，为了实现快捷的信息交流和资源共享，需要构建统一网络，整合公司所有相关业务流程。采用单核心的网络架构的网络接入模式，采用路由器接入城域网专用链路来传输业务数据流。总公司为了安全管理每个部门的用户，使用 VLAN 技术将每个部门的用户划分到不同的 VLAN 中。分公司采用路由器接入互联网络和城域网专用网络，总公司的内网用户采用无线接入方式访问网络资源。

为了保障总公司与分公司业务数据流传输的高可用性，使用防火墙进行保证网络安全，采用 QOS 技术对公司重要的业务数据流进行保障。网络采用 OSPF 动态路由协议和 RIP 动态路由协议。

拓扑结构

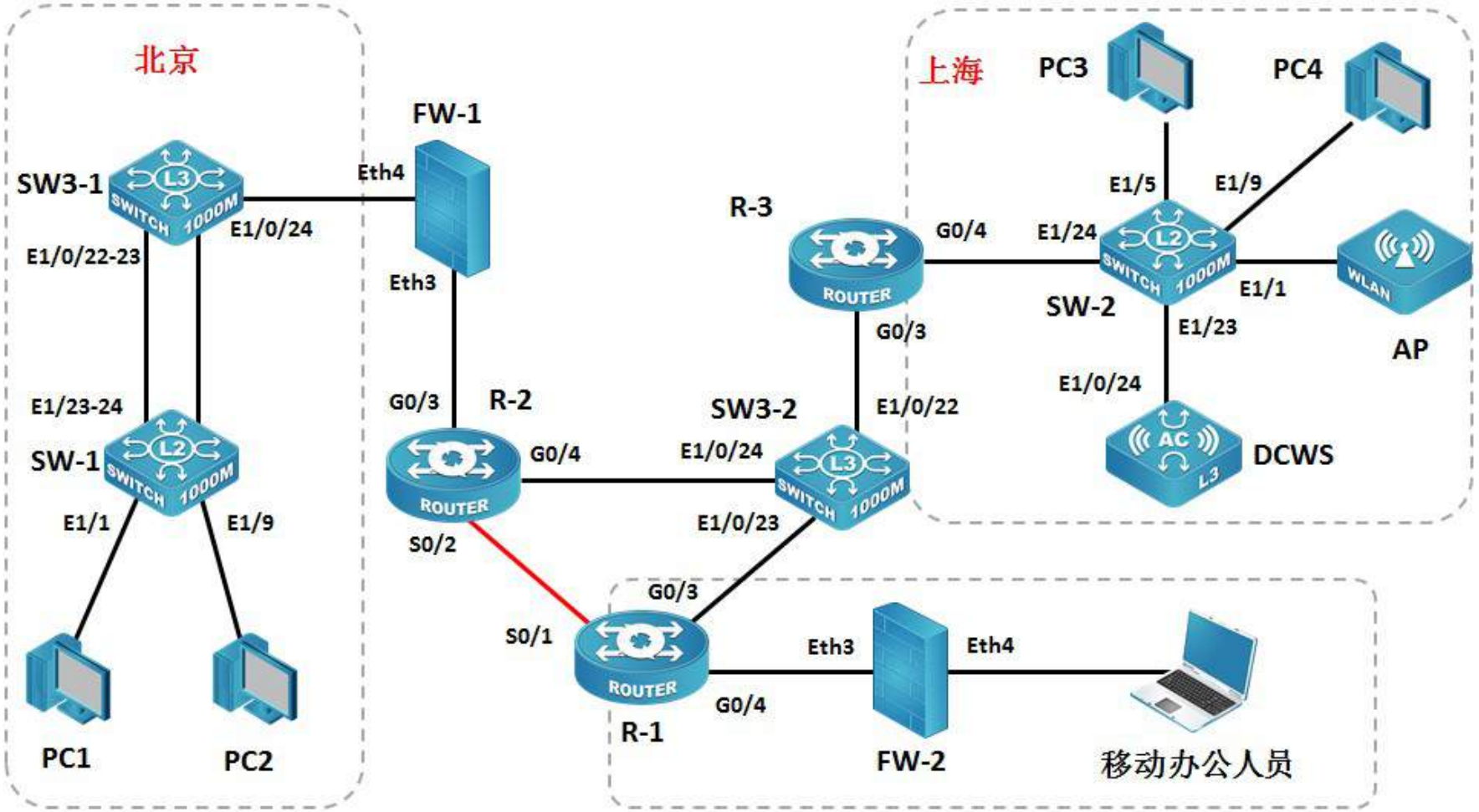

北京
上海
FW-1
SW3-1
Eth4
E1/0/24
E1/0/22-23
Eth3
R-3
G0/4
E1/24
PC3
PC4
E1/5
E1/9
SW-2
E1/1
WLAN
AP
G0/3
E1/23
E1/0/24
E1/23-24
G0/3
R-2
SW3-2
E1/0/22
SW-1
G0/4
E1/0/24
AC
DCWS
E1/1
E1/9
S0/2
E1/0/23
G0/3
S0/1
Eth3
Eth4
G0/4
R-1
FW-2
移动办公人员
PC1
PC2

表 1 网络设备连接表

A 设备连接至 B 设备			
设备名称	接口	设备名称	接口
R-1	G 0/4	FW-2	E0/3
R-1	G 0/3	SW3-2	E 1/0/23
R-1	S 0/1	R-2	S 0/1
R-2	G 0/3	FW-2	E0/3
R-2	G 0/4	SW3-2	E 1/0/24
SW3-2	E 1/0/22	R-3	G 0/3
R-3	G 0/4	SW-2	E 1/24
SW-2	E 1/1	AP	
SW-2	E 1/23	DCWS	E 1/0/24
FW-2	E0/4	移动办公	
FW-1	E0/4	SW3-1	E 1/0/24
SW3-1	E 1/0/22-23	SW-1	E 1/23-24
PC1	NIC	SW-1	E 1/1
PC2	NIC	SW-1	E 1/9
PC3	NIC	SW-2	E 1/5
PC4	NIC	SW-2	E 1/9

表 2. 网络设备 IP 地址分配表

设备	设备名称	设备接口	IP 地址
路由器	R-1	S0/1	202.90.1.1/30
		G0/3	202.80.1.1/30
		G0/4	202.100.1.1/24
	R-2	S0/2	202.90.1.2/30
		G0/3	202.50.1.1/30
		G0/4	202.70.1.1/30
	R-3	G0/4	
		G0/3	202.200.1.2/24
三层交换机	SW3-1	Vlan 10	
		Vlan 20	
		Vlan 30	
		Vlan 40	
		Vlan 100	
		Vlan 200	172.16.1.254/24
	SW3-2	Vlan 10	202.80.1.2/30 (E 1/0/23)
		Vlan 20	202.70.1.2/30 (E 1/0/24)
		Vlan 30	202.200.1.1/24 (E 1/0/22)
防火墙	FW-1	Eth0/3	202.50.1.254/24
		Eth0/4	
	FW-2	Eth0/3	202.100.1.254/24

		Eth0/4	10.1.1.254/24
无线控制器	DCWS	Vlan 10	
		Vlan 20	
		Vlan 100	
		Vlan 200	192.168.1.254/24
计算机	PC1	NIC	172.16.1.253 (SW-1 E1/1)
	PC2	NIC	172.16.1.252 (SW-1 E1/9)
	PC3	NIC	192.168.1.253 (SW-2 E1/5)
	PC4	NIC	192.168.1.252 (SW-2 E1/9)

表 3.服务器 IP 地址分配表

宿主机	虚拟主机名称	域名信息	服务角色	系统及版本信息	IPv4 地址信息
Server 1	Win2003-A1	DC1.2015Network.com	域控制器 DNS 服务器 CA 证书服务器	Windows Server 2003 R2	IP：192.168.1.1
	Win2008-A1	dhcp.2015Network.com	DHCP 服务器	Windows Server 2008 R2	IP：192.168.1.2
	Centos-A1	smb.jnds.net	SAMBA 共享服务器	Centos 6.5	IP：192.168.1.3
Server 2	Win2008-B1	www.2015Network.com www2.2015Network.com	WWW 服务器 邮件服务器	Windows Server 2008 R2	IP：192.168.1.4
	Centos-B1	raid.jnds.net	逻辑卷及磁盘阵列服务	Centos 6.5	IP：192.168.1.5
	Centos-B2	ftp.jnds.net ftp1.jnds.net ftp2.jnds.net	文件服务器	Centos 6.5	IP：192.168.1.105 IP：192.168.1.106 IP：192.168.1.107
Server 3	Win2003-C1	bdns.2015Network.com	备份 DNS	Windows Server 2003 R2	IP：192.168.1.6
	Centos-C1	dns.jnds.net	BIND 域名服务器 Squid 代理服务器	Centos 6.5	IP：192.168.1.109

Server 4（Linux 虚拟化主机）	Centos-D1	www.jnds.com www.jnds.lab.com	Apache web 服务器	Centos 6.5	IP：192.168.1.161

竞赛题目

网络搭建部分（450 分）

【注意事项】

(1) 设备 console 线有两条。交换机， AC，防火墙使用同一条 console 线，路由器使用另外一条 console 线。

(2) 设备配置完毕后，保存最新的设备配置。保存文档方式分为两种：

交换机和路由器要把 show running-config 的配置保存在 PC1 桌面的相应文档中，文档命名规则为：设备名称.doc,例如：RT1 路由器文件命名为：RT1.doc，然后放入到 PC1 桌面上“比赛文档”文件夹中

防火墙等截图方式的设备，把截图的图片放到同一 word 文档中，文档命名规则为：设备名称.doc,例如：防火墙 FW1 文件命名为：FW1.doc, 保存后放入到 PC1 桌面上“比赛文档”文件夹中。

1.物理连接与 IP 地址划分

(3) 按照网络拓扑图制作以太网网线，并连接设备。要求符合 T568A 和 T568B 的标准，其线缆长度适中。

(4) 根据”拓扑结构图”和”网络设备 IP 地址分配表”所示，对网络中所有设备接口配置 IP 地址。

北京使用 172.16.0.0/16 的地址段，上海使用 192.168.0.0/16 的地址段，为了节省 IP 资源，做到合理分配，设备间互联地址使用 30 位掩码。

北京区域服务器区（VLAN200）使用 192.168.1.1/24 位地址段，上海区域服务器区（VLAN200）使用 172.16.1.1/24 位地址段。北京区域设有财务部（Vlan10）有 30 名员工、工程部（Vlan20）不少于 90 名员工、

软件部（Vlan30）和系统集成部（Vlan40）两个部门都有 120 名员工，需要根据需要做出 IP 地址划分；上海区域有行政部（Vlan10）最少 90 台主机，销售部（Vlan20）最少有 300 台主机。把 IP 地址填入上面网络设备 IP 地址分配表中的空白处。

注意：

- 网关地址为网段最后一个可用地址。

2.交换机调试与配置

(1) 为交换机设备命名，命名规则参考为表 1 中的设备名称。

(2) 依据拓扑结构图和下表，把相应端口加入到 Vlan 中；

设备	VLAN 名称	VLANID	接口
SW3-1	CU	10	E 1/0/22-23
	GC	20	E 1/0/22-23
	RJ	30	E 1/0/22-23
	JC	40	E 1/0/22-23
	Server	200	E 1/0/22-23
DCWS	XZ	10	E1/0/23
	XS	20	E1/0/23
	Server	200	E 1/0/23
SW-1	Link-to-SW3-1 (端口命名)	Trunk	E1/23-24
	Link-to-PC1 (端口命名)	200	E1/1
	Link-to-PC2 (端口命名)	200	E1/9
SW-2	Link-to-PC3 (端口命名)	200	E1/5

	Link-to-PC4 (端口命名)	200	E1/9

(3) 为了统一管理，所有交换机开启 Telnet 功能，用户名为 user1，密码为 PWD@123，用户级别为 15 级，Enable 密码为 DCN（注意密码大小写）。

(4) 使用端口汇聚技术，将 SW3-1 的 E1/0/22-23 和二层交换机 SW-1 的 E1/23-24 配置为端口汇聚，汇聚接口为动态方式。SW-1 负载分担方式基于源、目地 MAC

(5) 在 SW3-1 连接 FW-1 的端口进行端口限速，将 SW3-1 的 E1/0/24 端口双向限速为 20M。

(6) 上海办公区为了加强内网防护等级，计划后续增加流量分析服务器，本次首先将 PC1、PC2 所连端口的双向流量镜象到端口 E1/20，以便后续增加的流量分析服务器分析内网服务器的流量。

3.路由器调试与配置

(1) 为路由设备命名，命名规则参考为表 1 中的“设备名称”。

(2) FW-1 与 R-2 间运行 RIPv2 路由协议；R-2 与 R-1 间运行 OSPF 路由协议区域为 Area0，R-2 与 SW3-2 间运行 OSPF 路由协议，区域为 Area0；R-1 与 SW3-2 和 SW3-2 与 R-3 之间运行 RIPv2 路由协议，北京、上海内部使用静态路由。

(3) 根据下表，配置设备的 RouterID，要求不能增加接口的相关信息。

设备名称	Router-ID
R-1	1.1.1.1
R-2	2.2.2.2
SW3-2	3.3.3.3

(4) 在 R-1，R-2 及 SW3-2 中通过路由重发布确保网络互联互通

(5) R-2 不参与 SW3-2 之间 OSPF 的 DR、BDR 选举；

(6) 在 R-2 上使用 QoS 进行流量整形，使 R-2 到 SW3-2 间的流量限制 CIR 为 40000，Exces Burst Size 为 1000，Burst Size 为 2000，超额流量不需要处理。

(7) R-2 配置策略路由，限制北京区域访问上海区域时，通过 R-1 与 SW3-2 之间的链路转发。

4.广域网配置

(1) R-1 与 R-2 之间的串口配置为 PPP 链路，启用双向 Chap 认证。对端设备名称做为用户名，密码为 PWDchap；

(2) 北京、上海区域用户在互相访问时，由各区域的出口设备负责 NAT 转换工作，转换方式为端口 NAT；FW2 使用端口 NAT

5.无线网调试与配置

(1) 为无线控制器进行设备命名，命名规则参考表 1 中的“设备名称”。

(2) 无线控制器建立 2 个 SSID，SSID 分别为 BJ1 和 BJ2。BJ1 的 SSID 设置为隐藏，工作信道为 11；BJ1 工作信道为自动。使用无线控制器的 DHCP 服务，使 BJ1、BJ2 这 2 个 SSID 下的用户分别获得 VLAN50/60 的 IP 地址，每个网段最少保证 50 个用户接入。通过无线方式接入的用户获取 DHCP 方式分配的 IP 地址，DNS 地址为 8.8.8.8，租期 1 天；

(3) 限制无线发射功率为 90%。

6、路由器、交换机和 AP 上部署安全策略

(1) 北京办公区的SW-1限制端口E1/3的端口MAC地址学习规则，指定E1/3端口最多可以学习 3 个 MAC 地址，对于学习到更多的 MAC 地址时直接丢弃。E1/4 端口绑定 MAC 地址为 00-33-33-33-33-33，其他 MAC 地址不再学习。

(2) 北京区域限制每周的工作日 9：00-18：00 的办公时间以外不允许访问外网。

(3) 激活无线网络的二层隔离，实现同一个 AP 下无线局域网内的用户不能互相访问

(4) 阻止 MAC 地址为 F0-11-22-33-44-55 的主机连接无线网络

(5) 限制通过无线方式接入的用户上行速度为 5Mbps，下行速度为 4Mbps。

(6) 用户接入无线网络时需要输入密码，加密方式为 WPA-Personal，口令为“chinaDCN”

(7) 在 SW3-2 上开启端口保护功能，防止 PC 机发出网关欺骗报文。

(8) 在 SW1 的 E1/2 接口上，限制源 MAC 为 00-11-22-33-44-55 的主机不允许访问 MAC 地址为 00-55-44-33-22-11 的主机。其余主机可以正常访问。

7、　防火墙安全策略

(1) 为防火墙设备命名，命名规则参考表 1 中的”设备名称“

(2) 上海办公区出口防火墙上配置 SSL 方式远程接入 VPN，允许远程办公的用户可以访问内部服务器资源，SSL 方式允许用户名为 vpn5、vpn6、vpn7、vpn8，密码与用户名相同，拨入的计算机获取的 IP 地址段为 172.16.0.40-50

(3) 北京办公区的 FW-1 禁止访问 www.taobao.com

(4) 北京办公区为了保证宽带的正常使用，限制 P2P 的应用下行带宽最高为 4M。

(5) 北京办公区限制用户访问含有“赌博”字段的网页。

服务器架设（550 分）

拓扑图中共有四台物理计算机，每台物理计算机使用 VirtualBox 安装虚拟计算机，按照地址规划中安装相应服务，具体要求如下所述：

Windows 操作系统部分

【说明】

（1）题目中所涉及 Windows 操作系统的 administrator 管理员以及其他普通用户密码均为 2015Netw1rk（注意区分大小写），若未按照要求设置密码，涉及到该操作的所有分值记为 0 分。

（2）虚拟主机的 IP 属性设置请按照网络拓扑结构图以及“表 3：服务器 IP 地址分配表”的要求设定。

（3）除非作特殊说明，在同一主机下需要安装相同操作系统版本的虚拟机时，可采用 Oracle VM VirtualBox 软件自带的克隆系统功能实现。

（4）所有系统镜像文件及试题所需的其它软件均存放在每台主机的 D:\soft 文件夹中，并将题目要求的截图内容以.jpg 格式存储于桌面 BACKUP 文件夹中。

（5）题目要求的虚拟机均安装于每台主机的 D：\virtualPC 目录，即路径为 D：\virtualPC\虚拟主机名称。

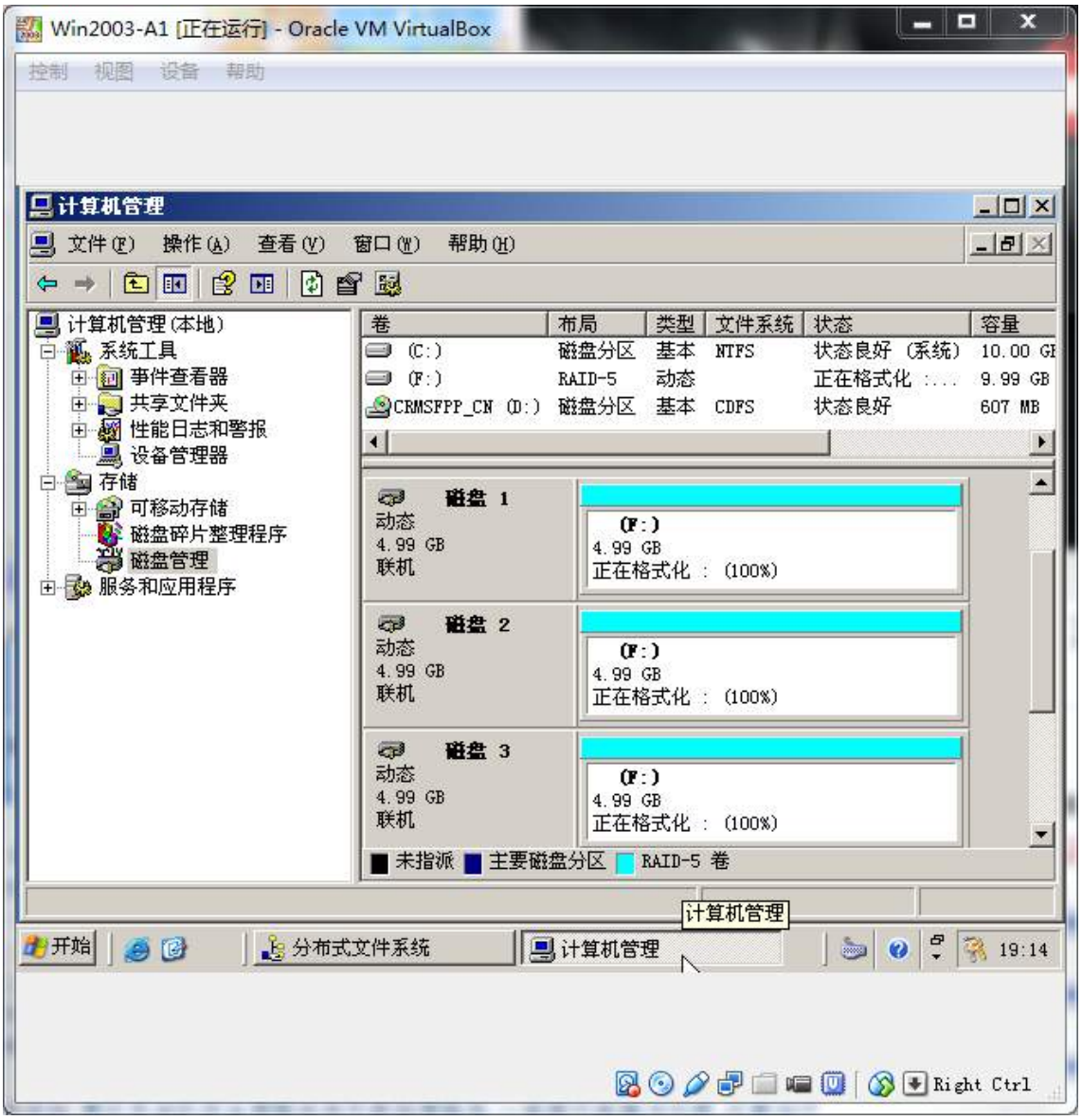
一、在 Server 1 上完成如下操作:

（一）完成虚拟主机的创建

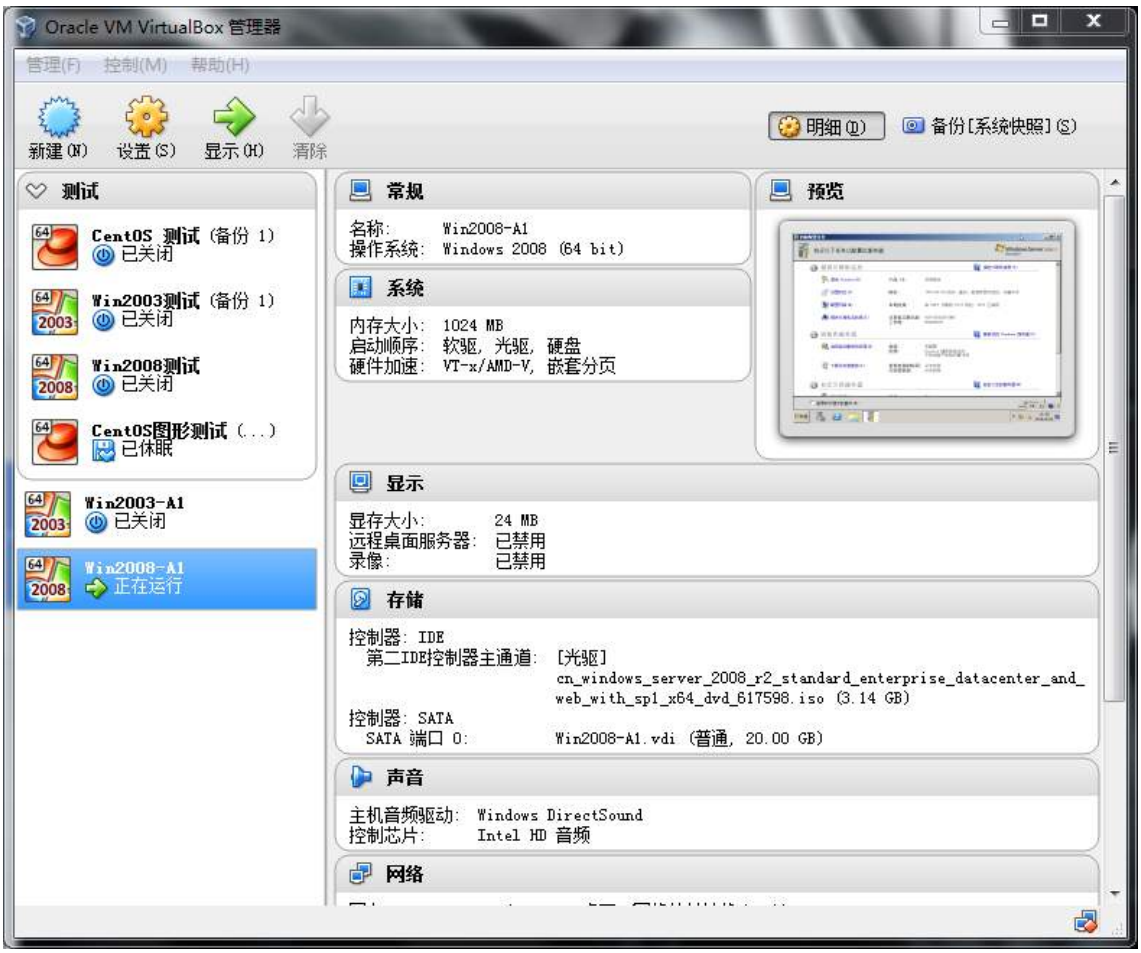
1、安装虚拟机“Win2003-A1”，具体要求为内存为 512M，硬盘 20G,网卡为桥接模式；虚拟机分区分别为 C、D、E；主分区一个，容量 10G；扩展分区为 10G，两个逻辑分区分别为 5G。

2、在虚拟机“Win2003-A1”中添加 SCSI 控制器，再添加三块 SCSI 虚拟硬

盘，其每块硬盘的大小为 5G；制作成一个 RAID-5 卷，磁盘盘符为 F:\。

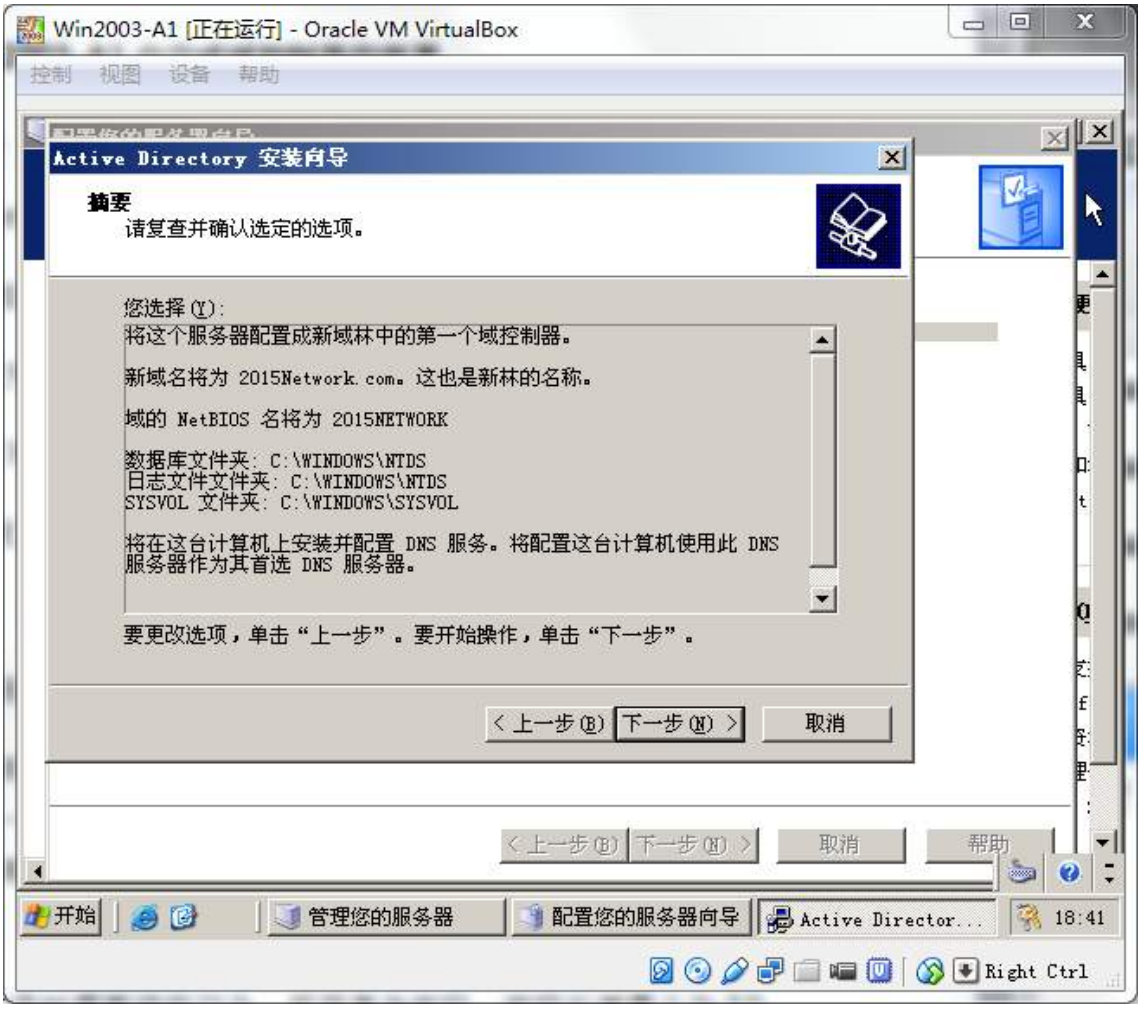


3、安装虚拟机“Win2008-A1”，具体要求为内存为 1G，硬盘 20G，并将该虚拟机加入到域中。

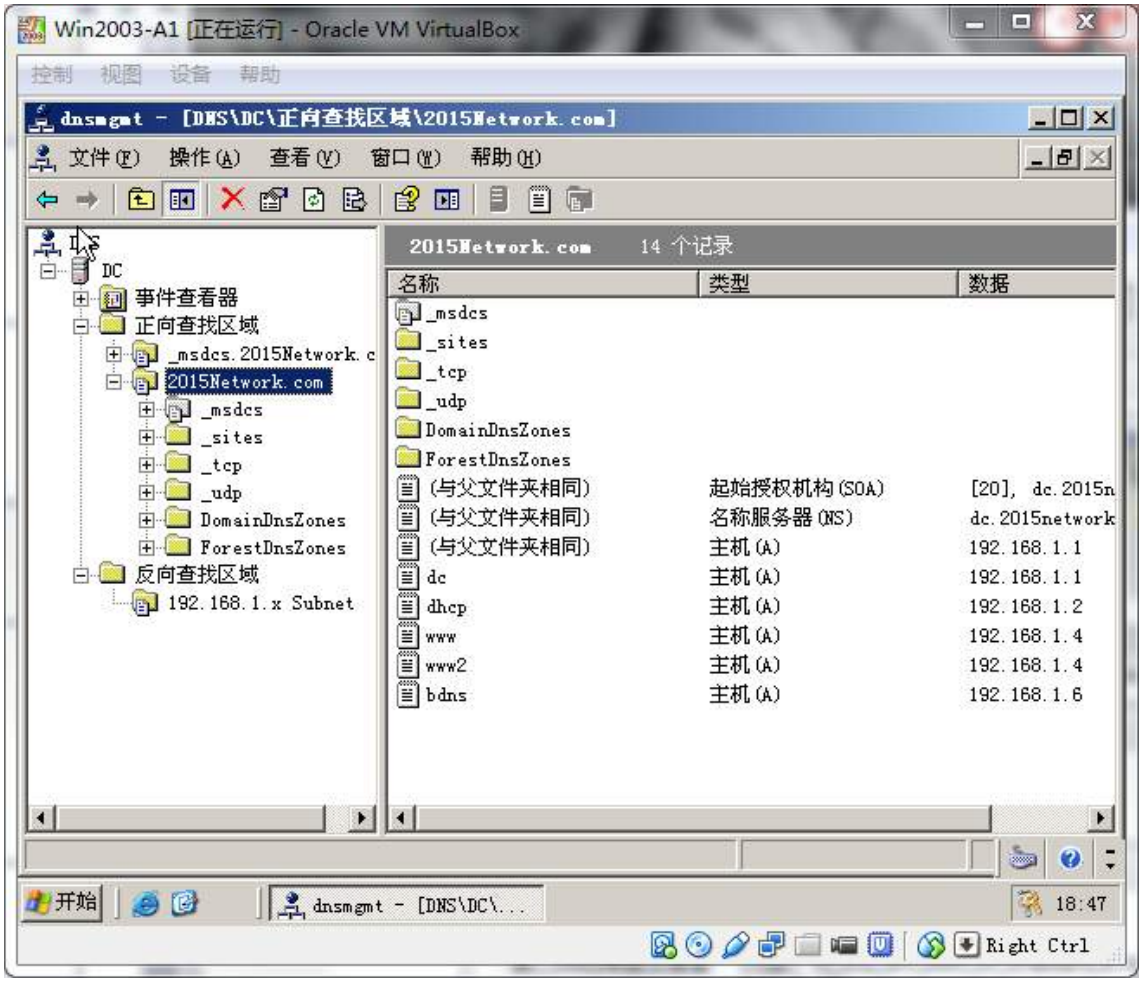
4、 

（二）在主机 Win2003-A1 中完成域控制器的部署

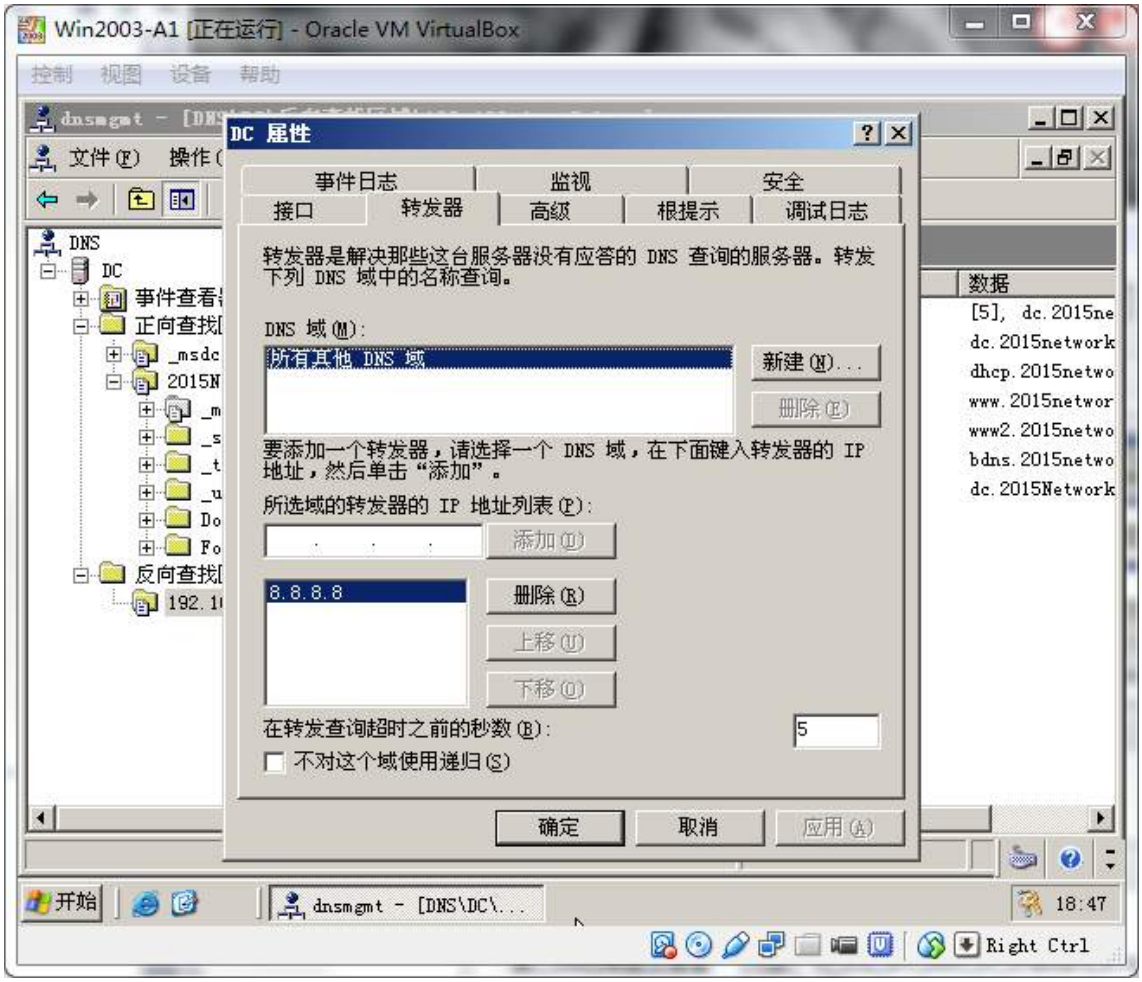
1、将在虚拟机“Win2003-A1”配置为主域控制器。域名为 2015Network.com，NetBIOS 域名为 2015Network，服务器的 FQDN 为 DC1.2015Network.com，域的功能级别为 2003 模式。



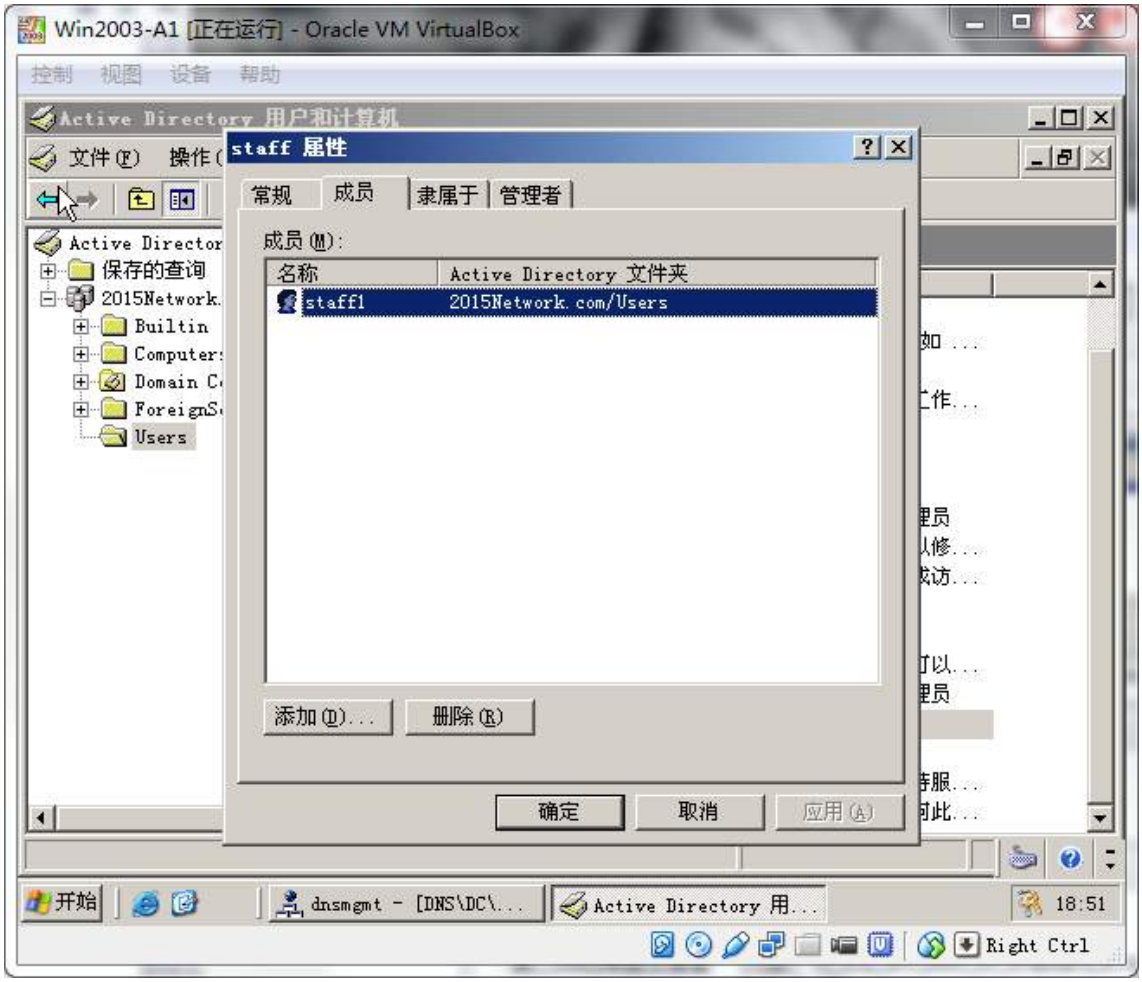
2、将此服务器配置为主 DNS 服务器，正确配置 2015Network.com 域名的正向区域与 IPV4 反向区域，能够正确解析网络中的所有服务器，当遇到无法解析的域名时，将其请求转发至 8.8.8.8 互联网域名服务器。

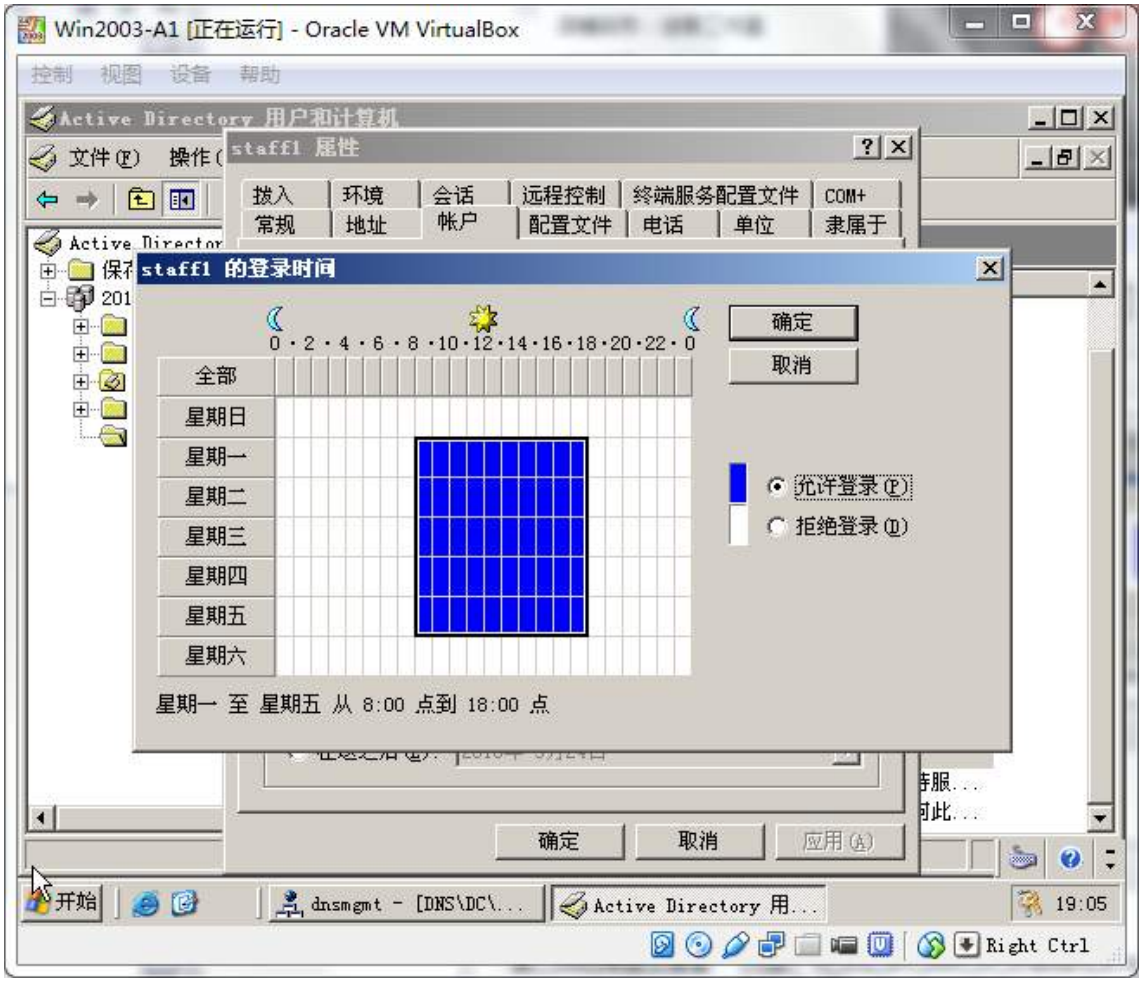

Win2003-A1 [正在运行] - Oracle VM VirtualBox
控制 视图 设备 帮助
dnsmgmt - [DNS\DC\正向查找区域\2015Network.com]
文件(F) 操作(A) 查看(V) 窗口(W) 帮助(H)
DC
事件查看器
正向查找区域
_msdcs.2015Network.c
2015Network.com
_msdcs
_sites
_tcp
_udp
DomainDnsZones
ForestDnsZones
反向查找区域
192.168.1.x Subnet
2015Network.com 14 个记录
名称 类型 数据
_msdcs
_sites
_tcp
_udp
DomainDnsZones
ForestDnsZones
(与父文件夹相同) 起始授权机构(SOA) [20], dc.2015n
(与父文件夹相同) 名称服务器(NS) dc.2015network
(与父文件夹相同) 主机(A) 192.168.1.1
dc 主机(A) 192.168.1.1
dhcp 主机(A) 192.168.1.2
www 主机(A) 192.168.1.4
www2 主机(A) 192.168.1.4
bdns 主机(A) 192.168.1.6
开始
dnsmgmt - [DNS\DC\...
18:47
Right Ctrl

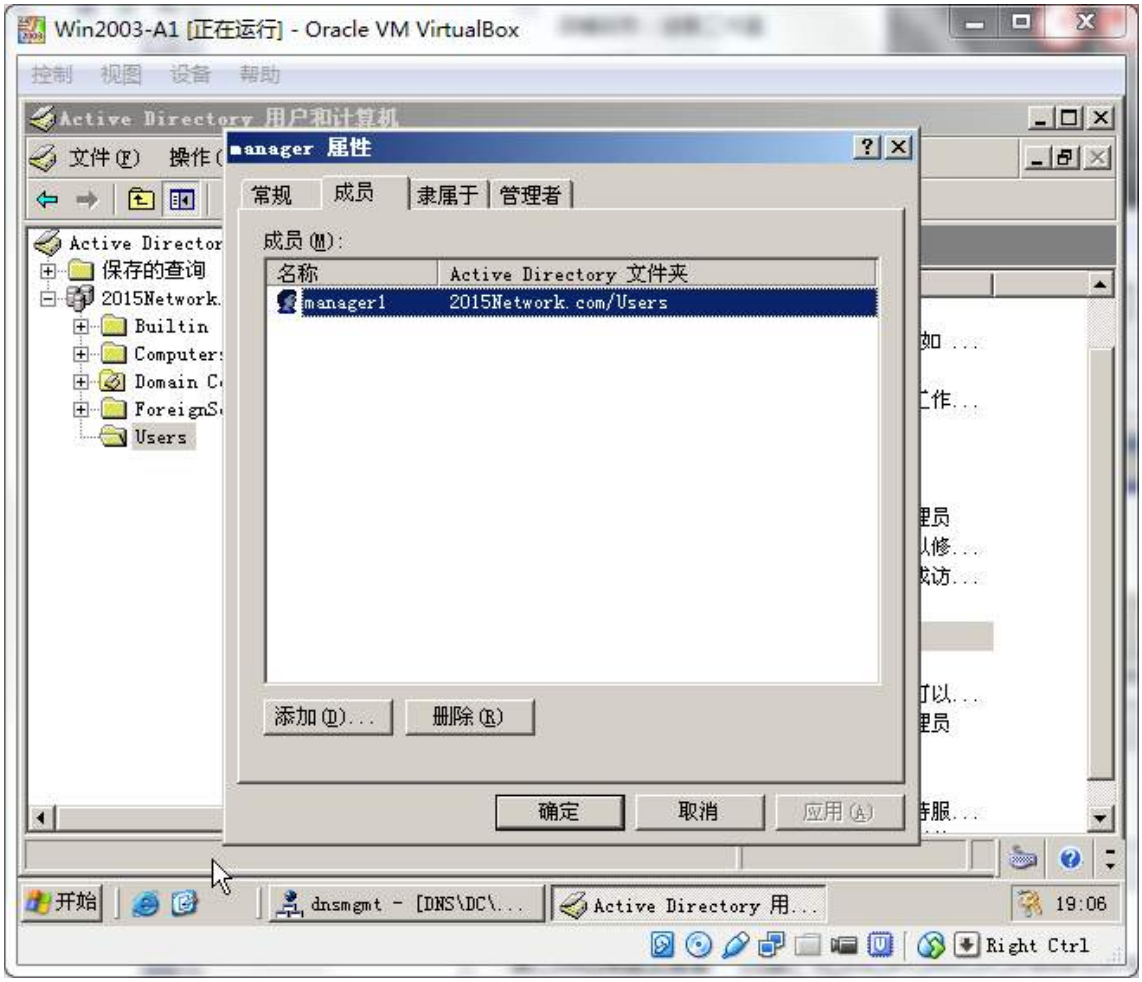

Win2003-A1 [正在运行] - Oracle VM VirtualBox
控制 视图 设备 帮助
dnsmgmt - [DNS\DC\反向查找区域\192.168.1.x Subnet]
文件(F) 操作(A) 查看(V) 窗口(W) 帮助(H)
DNS
DC
事件查看器
正向查找区域
_msdcs.2015Network.c
2015Network.com
_msdcs
_sites
_tcp
_udp
DomainDnsZones
ForestDnsZones
反向查找区域
192.168.1.x Subnet
192.168.1.x Subnet 7 个记录
名称 类型 数据
(与父文件夹相同) 起始授权机构(SOA) [5], dc.2015ne
(与父文件夹相同) 名称服务器(NS) dc.2015network
192.168.1.2 指针(PTR) dhcp.2015netwo
192.168.1.4 指针(PTR) www.2015networ
192.168.1.4 指针(PTR) www2.2015netwo
192.168.1.6 指针(PTR) bdns.2015netwo
192.168.1.1 指针(PTR) dc.2015Network
开始
dnsmgmt - [DNS\DC\...
18:47
Right Ctrl



3、创建两个 OU，名字分别为 manager 和 staff;创建全局组，名字分别 manager 和 staff;创建用户 staff1（隶属于 staff 组），对于 staff1，仅仅允许周一到周五的 8:00 到 18:00 登录到域,创建用户 manager1（隶属于 manager 组），允许 manager1 登录到域控并具有关闭域控的权利。网络管理员和 manager1 都可以远程登录到域。。

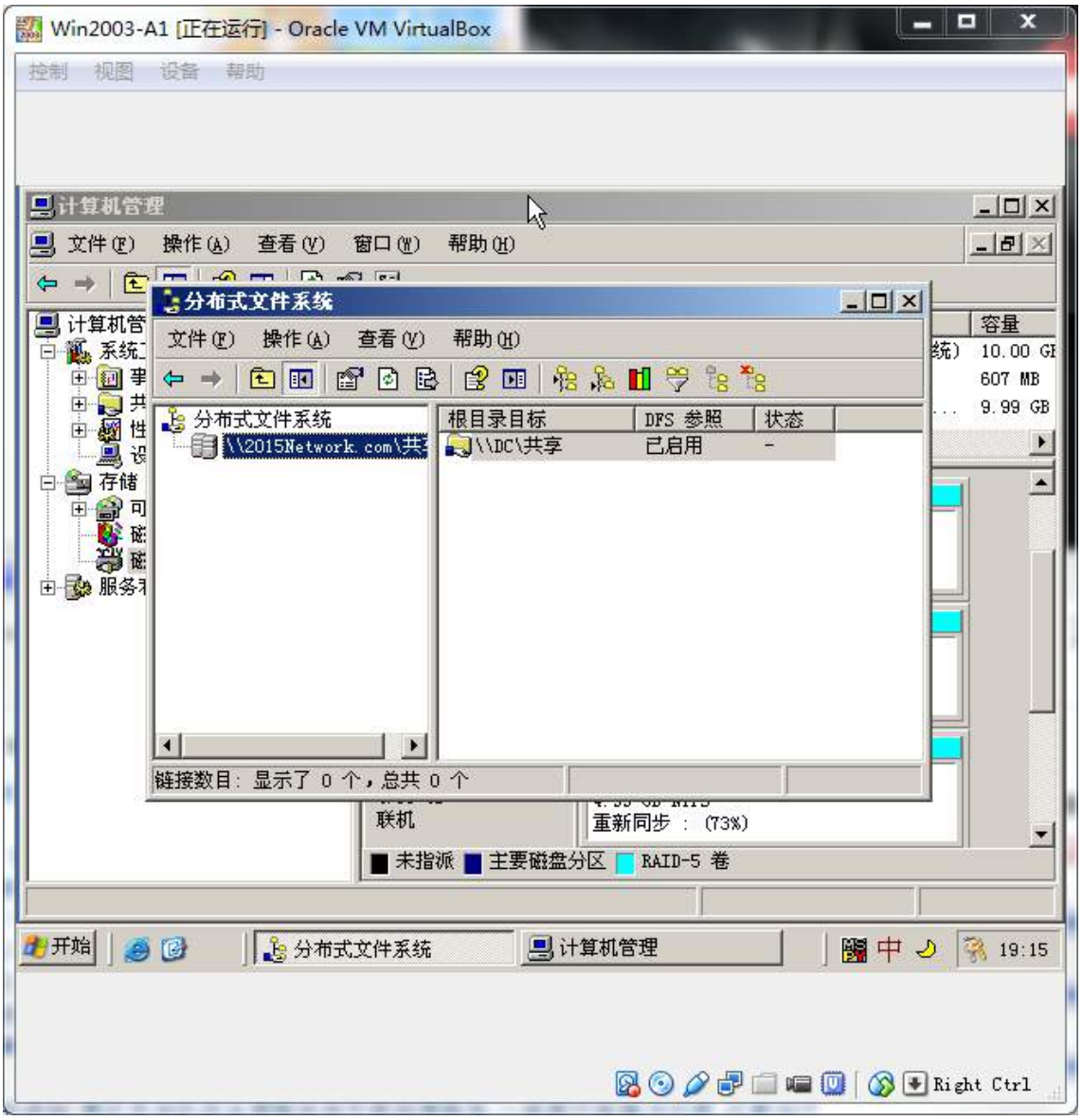

Win2003-A1 [正在运行] - Oracle VM VirtualBox
控制 视图 设备 帮助
Active Directory 用户和计算机
文件(F) 操作(
Active Director
保存的查询
2015Network.
Builtin
Computer
Domain C
ForeignS
Users
staff 属性
常规 成员 隶属于 管理者
成员(M):
名称 Active Directory 文件夹
staff1 2015Network.com/Users
添加(D)... 删除(R)
确定 取消 应用(A)
开始
dnsmgmt - [DNS\DC\...
Active Directory 用...
18:51
Right Ctrl

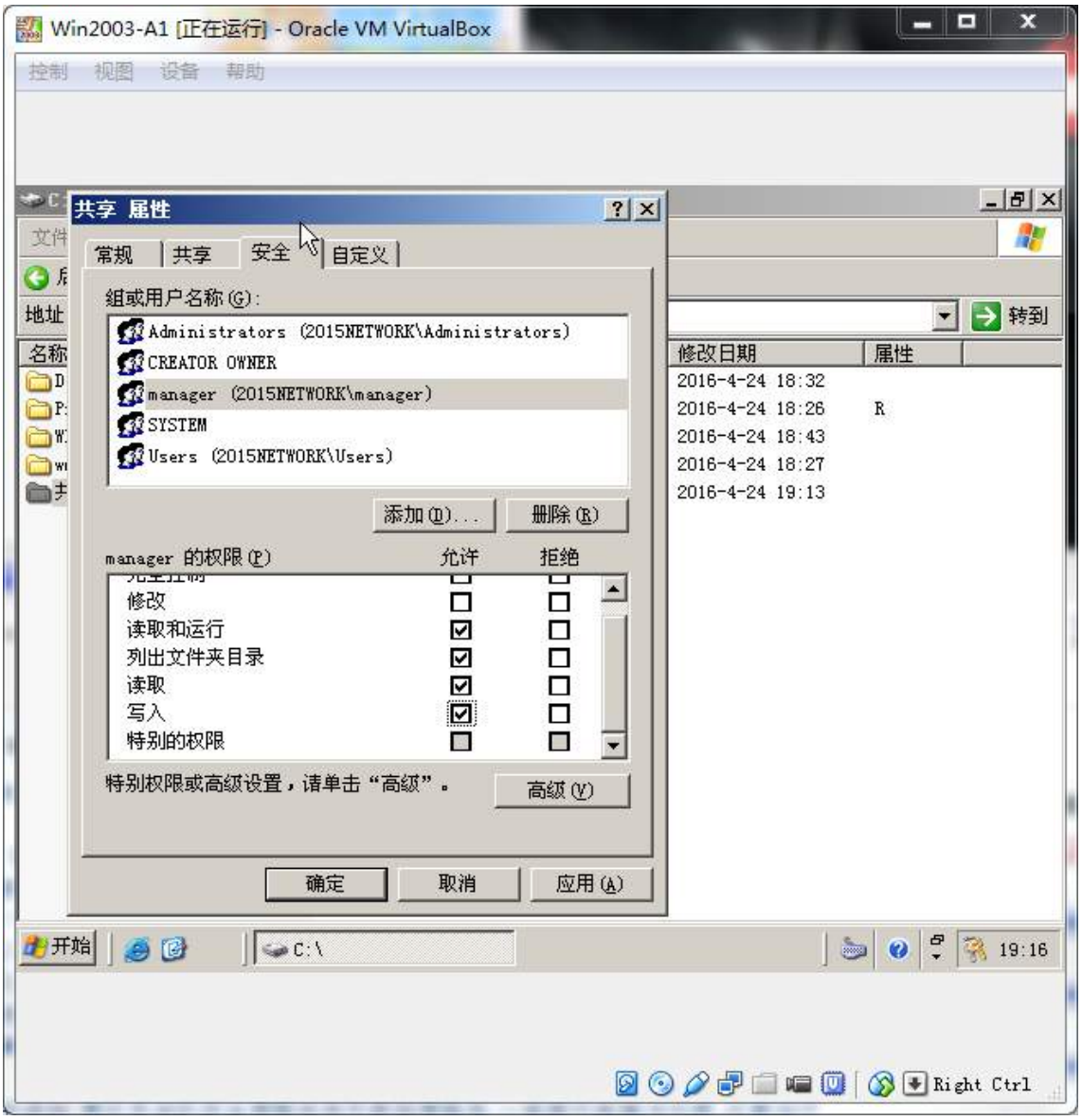

Win2003-A1 [正在运行] - Oracle VM VirtualBox
控制 视图 设备 帮助
Active Directory 用户和计算机
文件(F) 操作(
staff1 属性
拨入 环境 会话 远程控制 终端服务配置文件 COM+
常规 地址 帐户 配置文件 电话 单位 隶属于
staff1 的登录时间
0 · 2 · 4 · 6 · 8 · 10 · 12 · 14 · 16 · 18 · 20 · 22 · 0
全部
星期日
星期一
星期二
星期三
星期四
星期五
星期六
确定
取消
允许登录(P)
拒绝登录(D)
星期一 至 星期五 从 8:00 点到 18:00 点
确定 取消 应用(A)
开始
dnsmgmt - [DNS\DC\...
Active Directory 用...
19:05
Right Ctrl

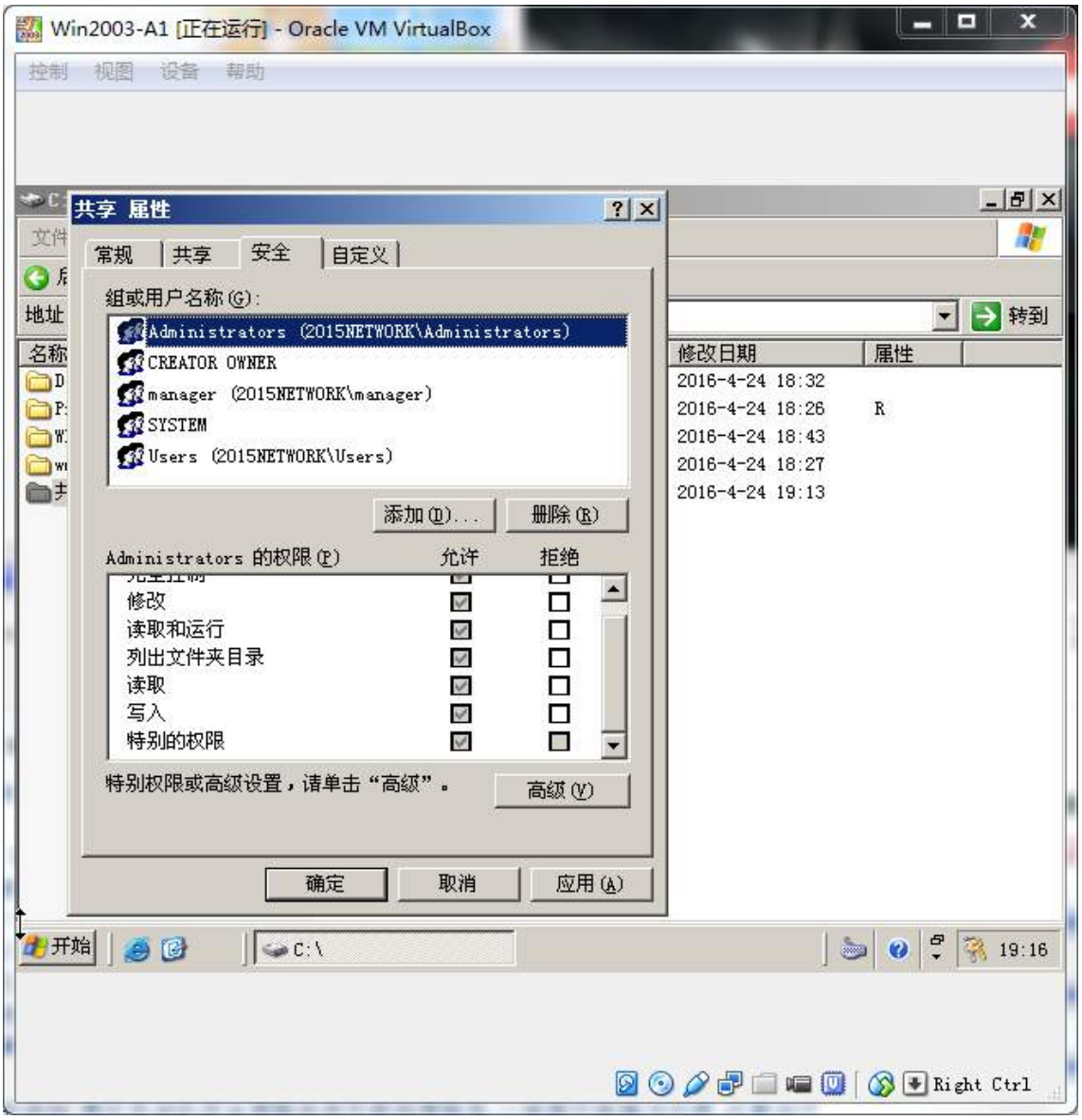


4、域用户在首次登录时需要修改口令，采用复杂密码，密码长度最小为 10 位，密码最长存留其为 30 天，帐户锁定阈值为 5 次，如果到过阈值需要锁定 45 分钟。

5、在此域控制器中发布一个共享文件夹，其名字为“共享”，设置访问该文件夹的权限为：管理员能下载、上传、删除共享文件夹中的资源；所有 manager 组成员既能读取、修改资源的内容、上传资源，但是不能删除资源，其他用户只能下载。

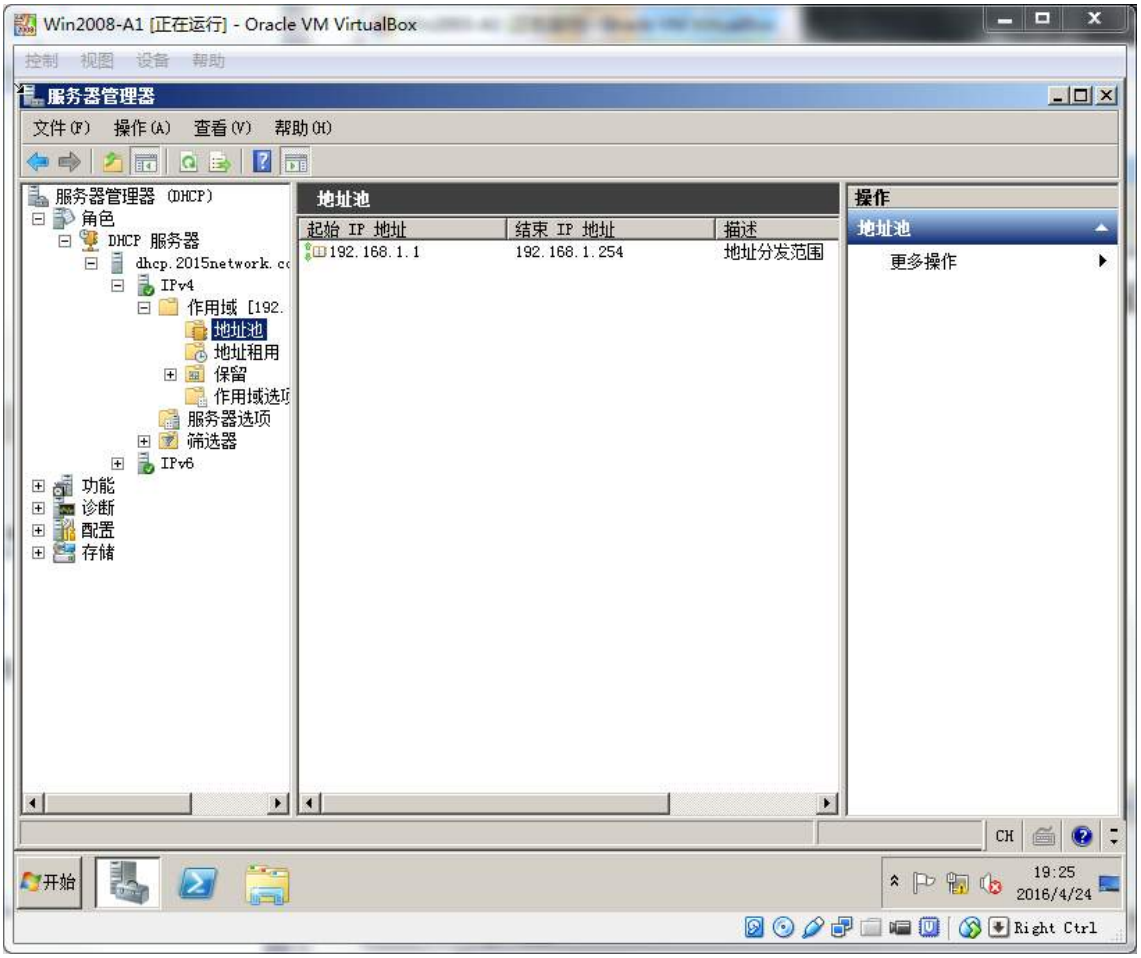

Win2003-A1 [正在运行] - Oracle VM VirtualBox
控制 视图 设备 帮助
计算机管理
文件(F) 操作(A) 查看(V) 窗口(W) 帮助(H)
分布式文件系统
文件(F) 操作(A) 查看(V) 帮助(H)
分布式文件系统
\\2015Network.com\共
根目录目标
DFS 参照
状态
\\DC\共享
已启用
链接数目：显示了 0 个，总共 0 个
容量
10.00 GB
607 MB
9.99 GB
联机
重新同步 : (73%)
未指派
主要磁盘分区
RAID-5 卷
开始
分布式文件系统
计算机管理
19:15
Right Ctrl


Win2003-A1 [正在运行] - Oracle VM VirtualBox
控制 视图 设备 帮助
共享 属性
常规 共享 安全 自定义
组或用户名称(G):
Administrators (2015NETWORK\Administrators)
CREATOR OWNER
manager (2015NETWORK\manager)
SYSTEM
Users (2015NETWORK\Users)
添加(D)... 删除(R)
manager 的权限(P) 允许 拒绝
修改
读取和运行
列出文件夹目录
读取
写入
特别的权限
特别权限或高级设置，请单击“高级”。
高级(V)
确定 取消 应用(A)
修改日期 属性
2016-4-24 18:32
2016-4-24 18:26 R
2016-4-24 18:43
2016-4-24 18:27
2016-4-24 19:13
转到
开始
C:\
19:16
Right Ctrl



（三）在主机 Win2008-A1 中完成 DHCP 服务器的部署

1、为总公司内网的所有 VLAN 网段的计算机提供 DHCP 服务，分配的 IP 段、子网掩码、网关及 DNS 服务器信息请根据题意说明确定。



二、在 Server 2 上完成如下操作:

（一）完成虚拟主机的创建

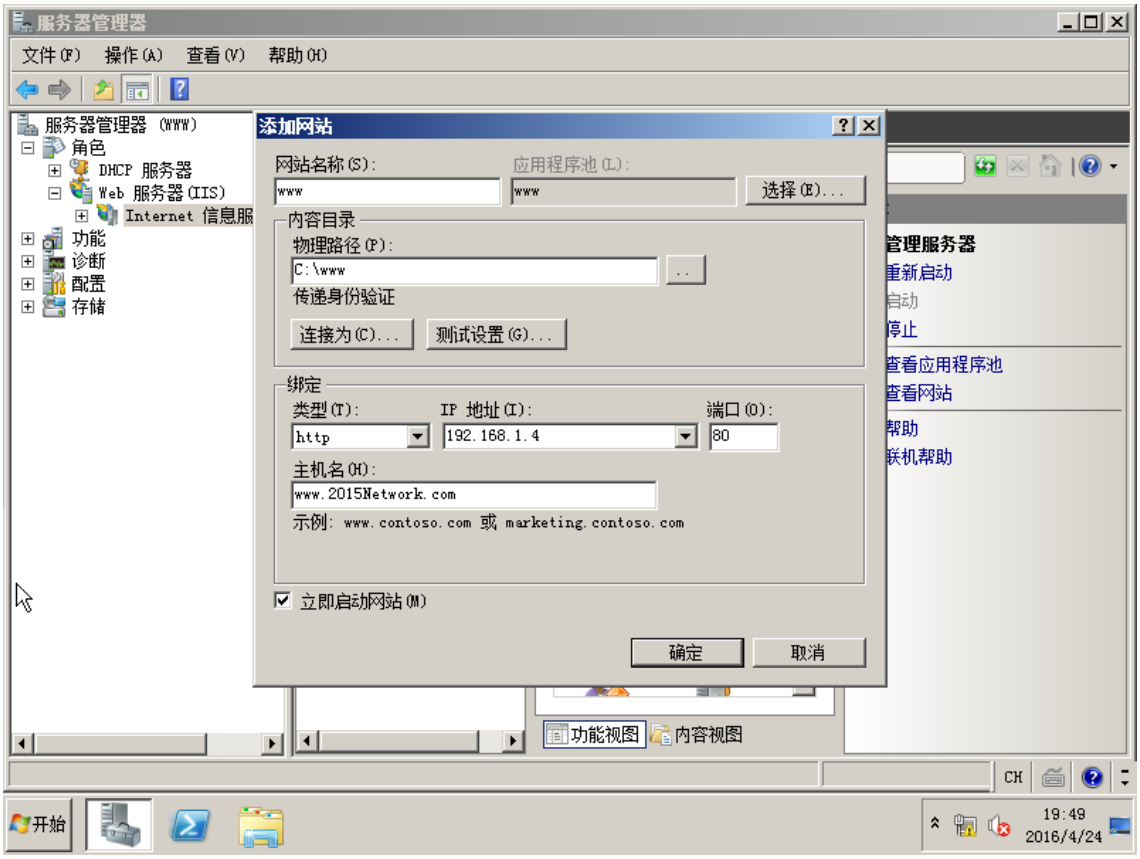
1、安装虚拟机“Win2008-B1”，其内存为 1G，硬盘 20G，将服务器加入至 Windows 域中；

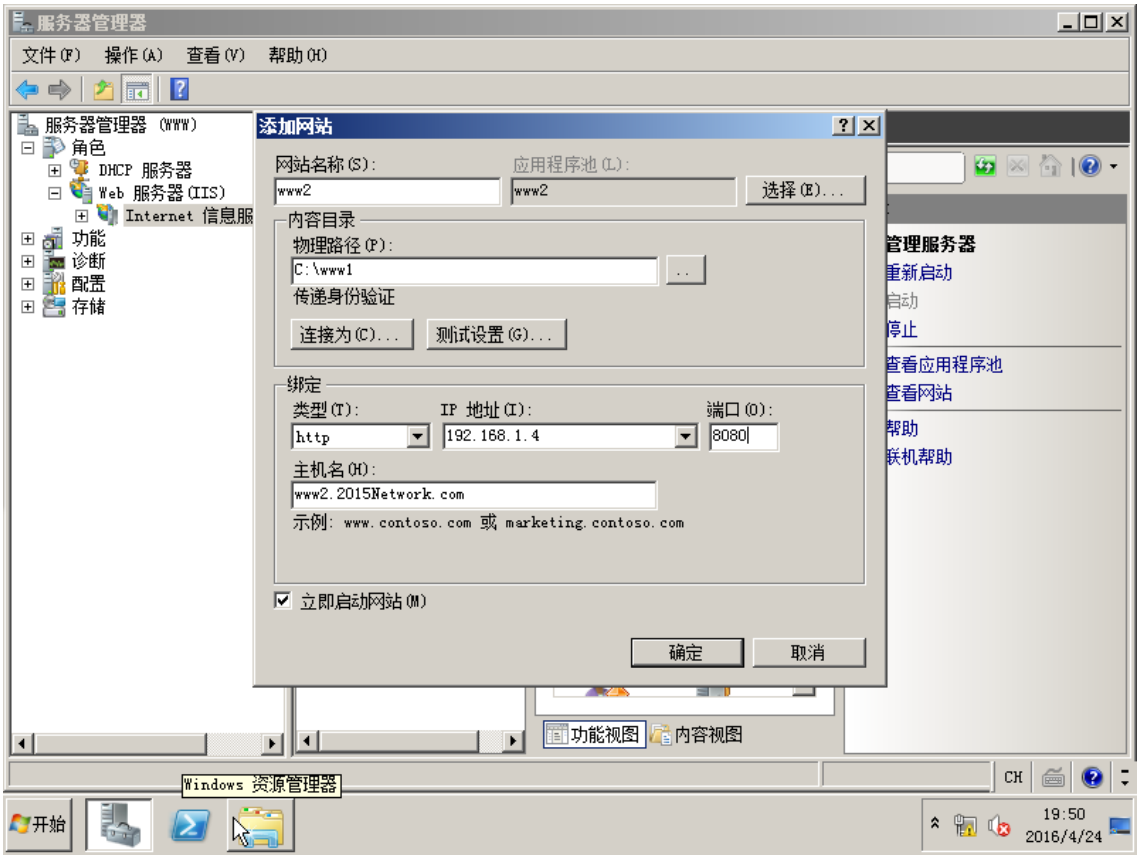
（二）在主机 Win2008-B1 中完成邮件服务器的部署

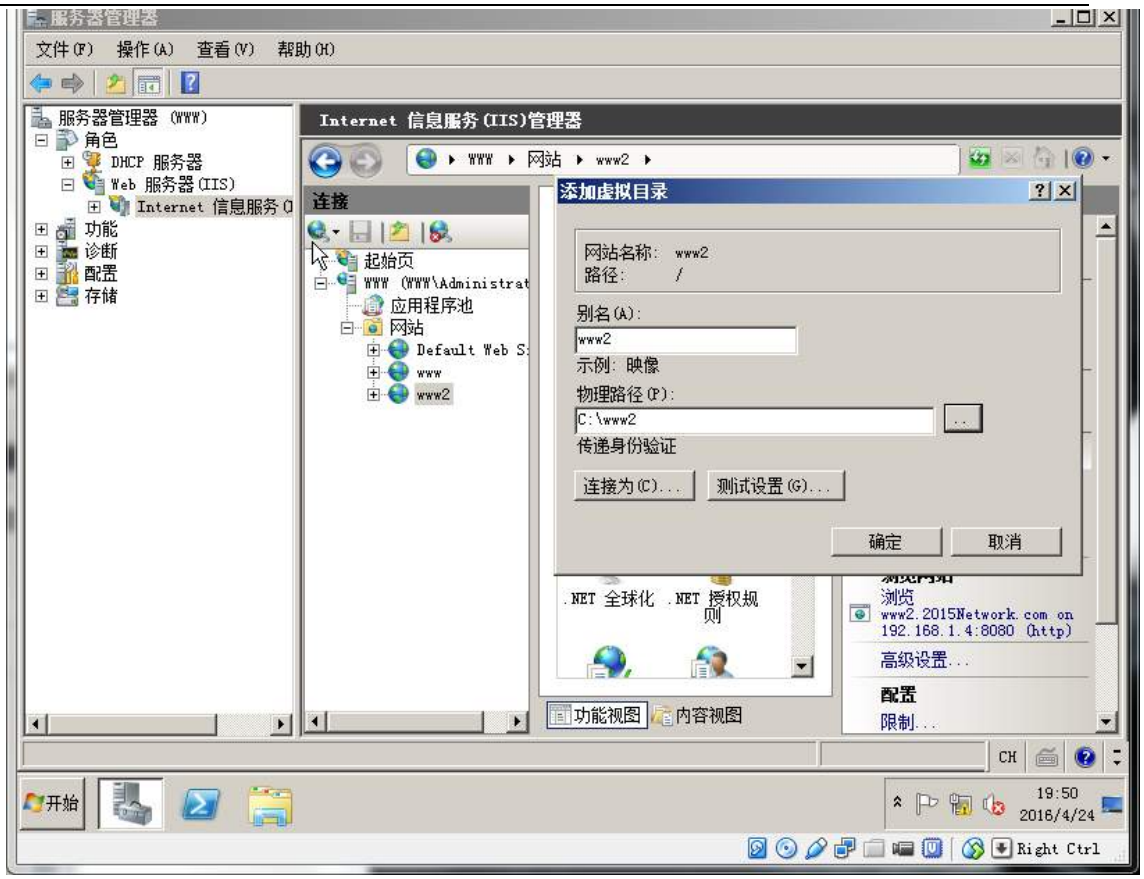
1、安装邮件服务器，要求域名为 2015Network.com 实现安全密码身份验证，实现 manager1 和 staff1 的邮件互发，并限制 staff1 的邮箱的容量为 50M，manager1 的邮箱为 100M,用 outlook 测试。将测试成功截图存为 email.jpg。

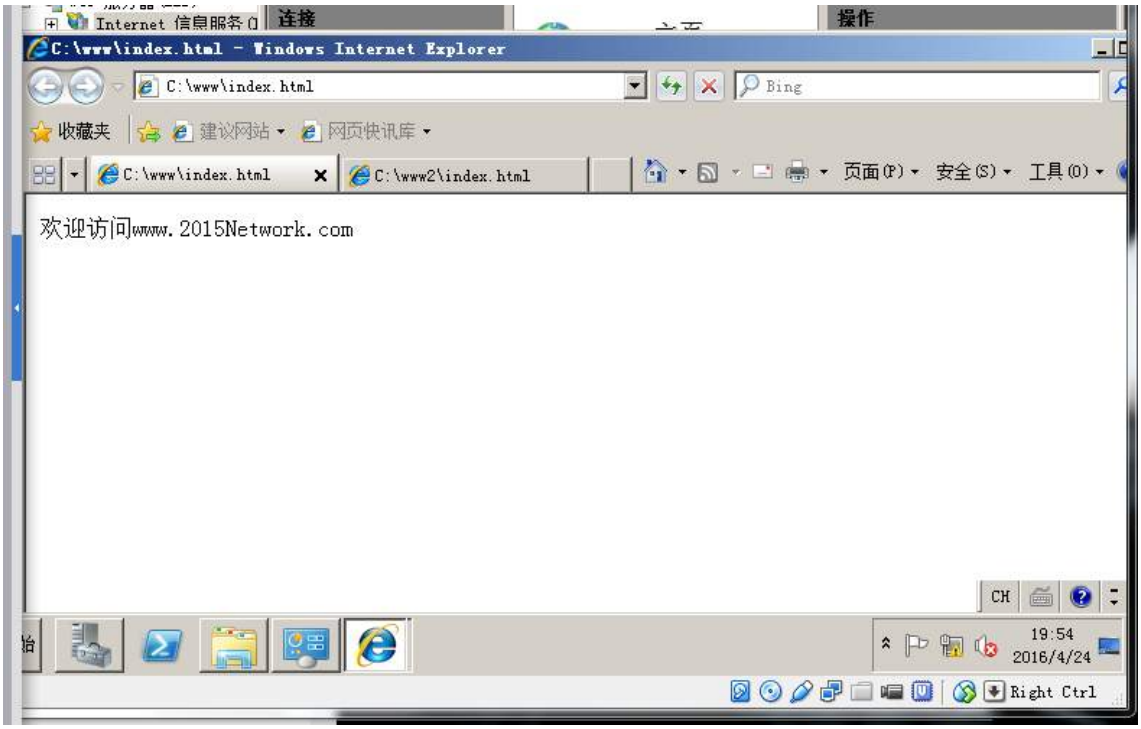
（三）在主机 Win2008-B1 中完成 WWW 服务器的部署

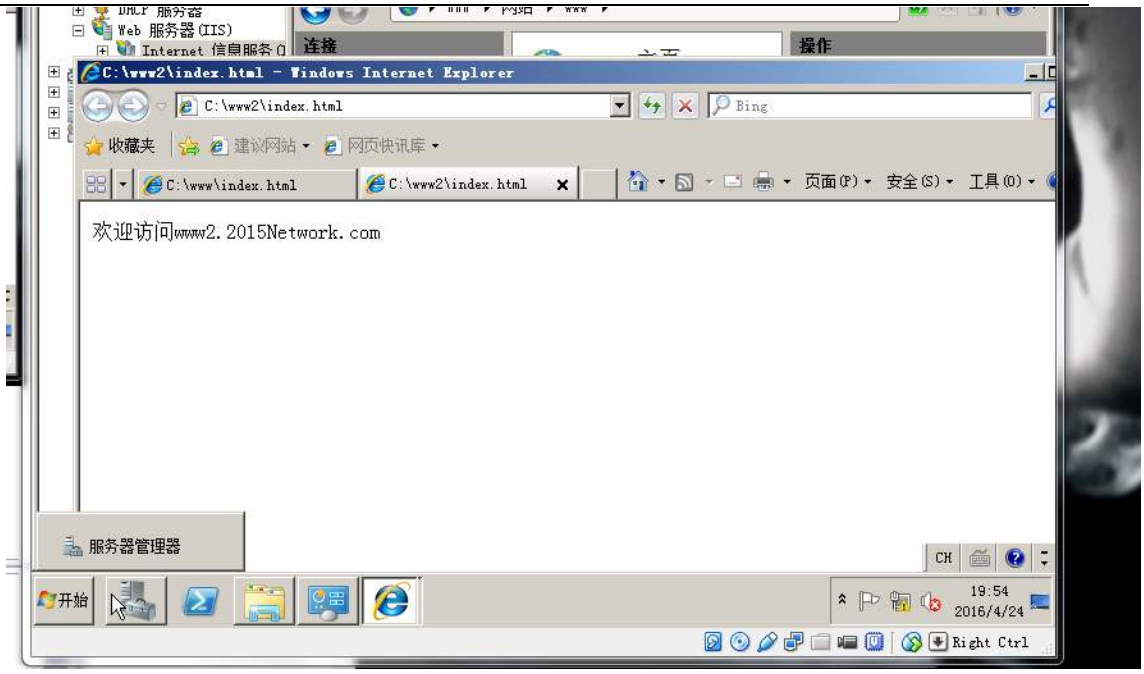
1、建立企业的外部 web 站点 www.2015Network.com 和内部站点 www2. 2015Network.com，其中内部站点的端口号为：8080，主页放置于虚拟目录中，虚拟目录为名为 www2。站点的主页内容分别为：“欢迎访问 www. 2015Network.com”和“欢迎访问 www2. 2015Network .com”。


服务器管理器
文件(F) 操作(A) 查看(V) 帮助(H)
服务器管理器 (WWW)
角色
DHCP 服务器
Web 服务器(IIS)
Internet 信息服
功能
诊断
配置
存储
添加网站
网站名称(S):
www
应用程序池(L):
www
选择(E)...
内容目录
物理路径(P):
C:\www
传递身份验证
连接为(C)...
测试设置(G)...
绑定
类型(T):
http
IP 地址(I):
192.168.1.4
端口(O):
80
主机名(H):
www.2015Network.com
示例: www.contoso.com 或 marketing.contoso.com
立即启动网站(M)
确定
取消
管理服务器
重新启动
启动
停止
查看应用程序池
查看网站
帮助
联机帮助
功能视图
内容视图
CH
开始
19:49
2016/4/24


服务器管理器
文件(F) 操作(A) 查看(V) 帮助(H)
服务器管理器 (WWW)
角色
DHCP 服务器
Web 服务器(IIS)
Internet 信息服
功能
诊断
配置
存储
添加网站
网站名称(S):
www2
应用程序池(L):
www2
选择(E)...
内容目录
物理路径(P):
C:\www1
传递身份验证
连接为(C)...
测试设置(G)...
绑定
类型(T):
http
IP 地址(I):
192.168.1.4
端口(O):
8080
主机名(H):
www2.2015Network.com
示例: www.contoso.com 或 marketing.contoso.com
立即启动网站(M)
确定
取消
管理服务器
重新启动
启动
停止
查看应用程序池
查看网站
帮助
联机帮助
功能视图
内容视图
CH
Windows 资源管理器
开始
19:50
2016/4/24


服务器管理器
文件(F) 操作(A) 查看(V) 帮助(H)
服务器管理器 (WWW)
角色
DHCP 服务器
Web 服务器(IIS)
Internet 信息服务(IIS)管理器
功能
诊断
配置
存储
连接
起始页
应用程序池
网站
Default Web S
www
www2
添加虚拟目录
网站名称: www2
路径: /
别名(A):
www2
示例: 映像
物理路径(P):
C:\www2
传递身份验证
连接为(C)...
测试设置(G)...
确定
取消
.NET 全球化
.NET 授权规则
浏览
www2.2015Network.com on 192.168.1.4:8080 (http)
高级设置...
配置
限制...
功能视图
内容视图
开始
19:50
2016/4/24
Right Ctrl


C:\www\index.html - Windows Internet Explorer
C:\www\index.html
Bing
收藏夹
建议网站
网页快讯库
C:\www\index.html
C:\www2\index.html
页面(P)
安全(S)
工具(O)
欢迎访问www.2015Network.com
19:54
2016/4/24
Right Ctrl

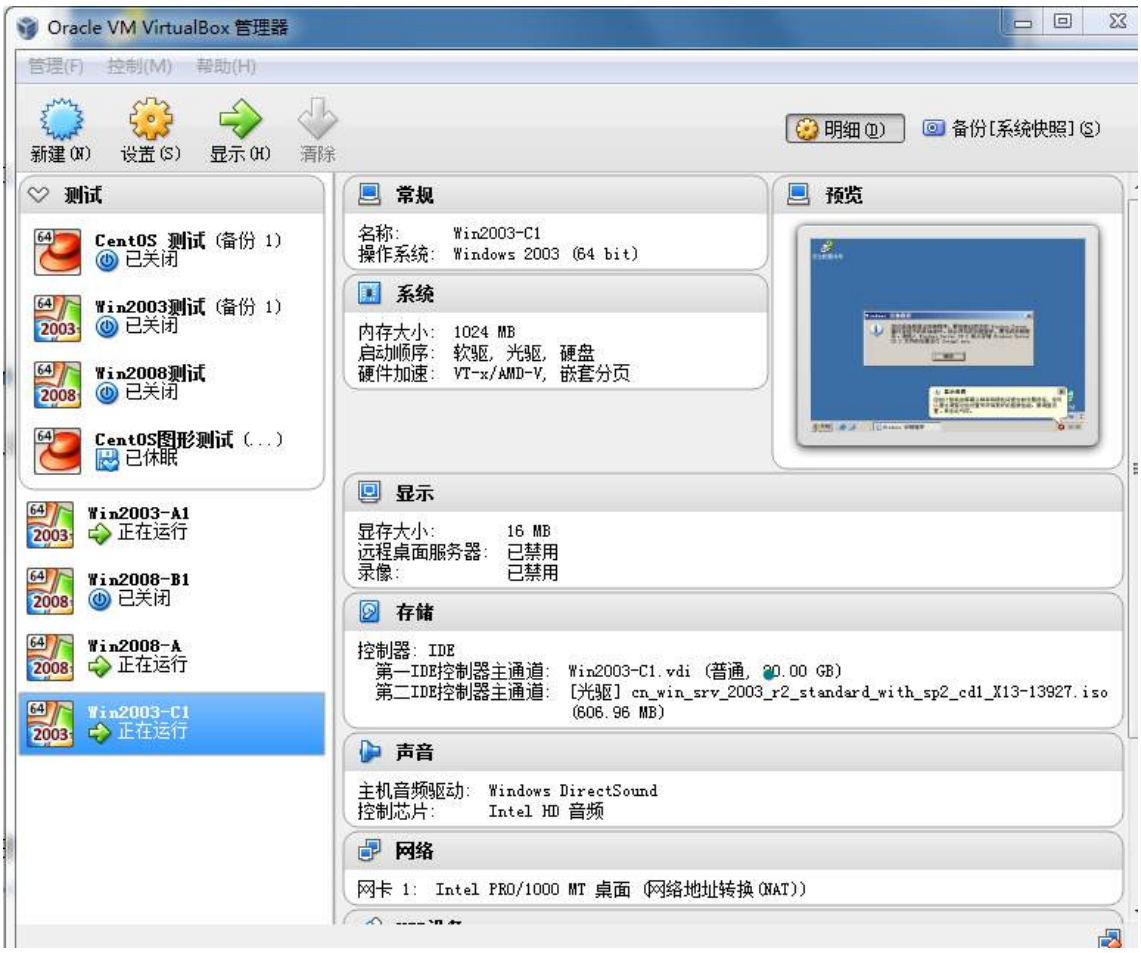


2、　申请证书，访问 www. 2015Network.com 时，不需要 SSL 加密；访问 www2. 2015Network.com 时必须使用 SSL 加密。

三、在 Server 3 上完成如下操作:

（一）完成虚拟主机的创建

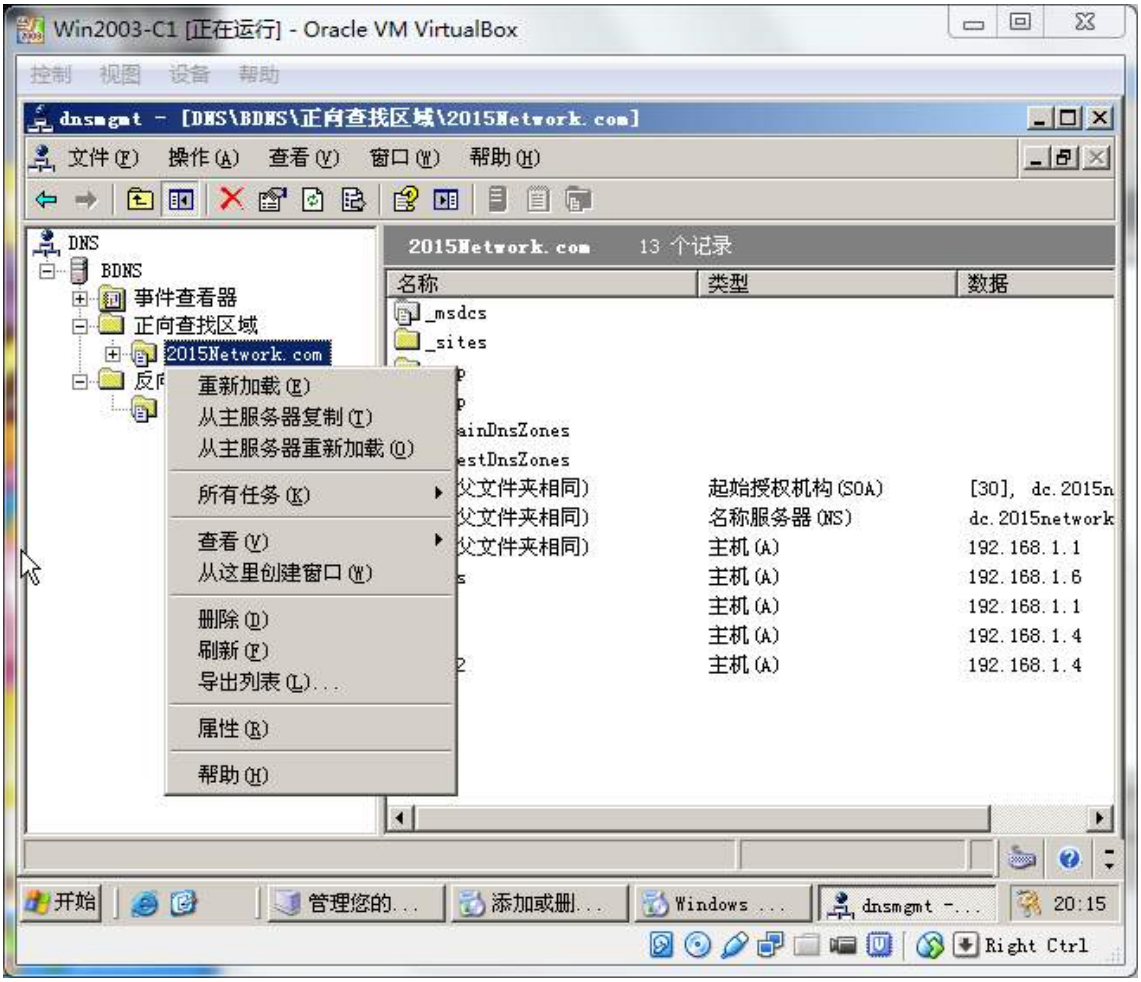
1、在虚拟机“Win2003-C1”，其内存为 1G，硬盘 20G，并将服务器加入到 Windows 域环境；

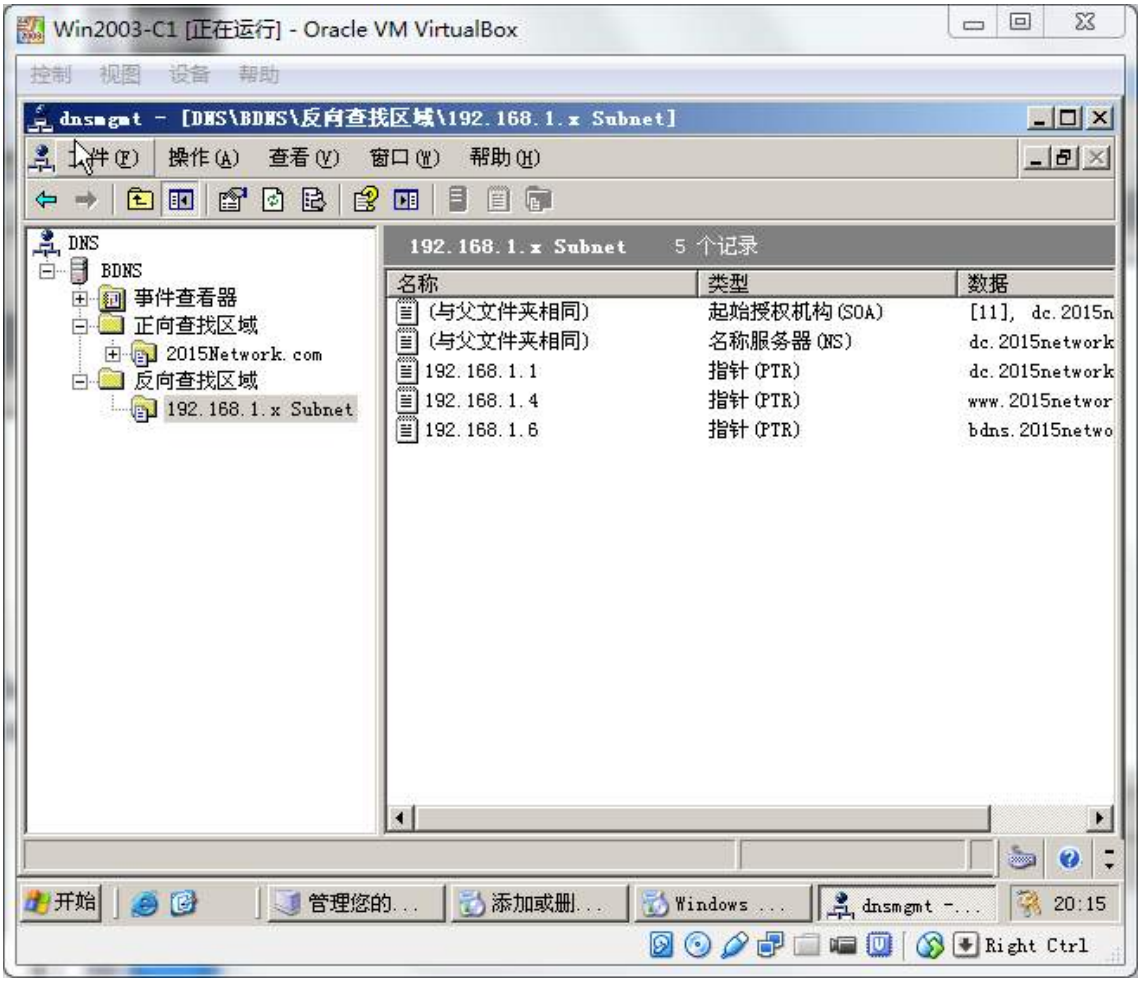


（二）在主机 Win2003-C1 中完成备份 DNS 的部署

1、配置此服务器为备份 DNS，其合法域名为 bdns.2015Network.com

2、将服务器加入到 windows 域中，将所有的主 DNS 的区域都复制到备份 DNS 服务器上


Win2003-C1 [正在运行] - Oracle VM VirtualBox
控制 视图 设备 帮助
dnsmgmt - [DNS\BDNS\正向查找区域\2015Network.com]
文件(F) 操作(A) 查看(V) 窗口(W) 帮助(H)
DNS
BDNS
事件查看器
正向查找区域
2015Network.com
2015Network.com 13 个记录
名称 类型 数据
_msdcs
_sites
重新加载(E)
从主服务器复制(T)
从主服务器重新加载(Q)
所有任务(K)
查看(V)
从这里创建窗口(W)
删除(D)
刷新(F)
导出列表(L)...
属性(R)
帮助(H)
起始授权机构(SOA)
名称服务器(NS)
主机(A)
192.168.1.1
192.168.1.6
192.168.1.4
开始
管理您的...
添加或删...
Windows ...
dnsmgmt -...
20:15
Right Ctrl



Linux 操作系统和集群部分

【说明】

1、所有 Linux 操作系统的 root 用户的密码为 123456，若未按要求设置密码，涉及到该操作系统下的所有分值记为 0 分。

2、虚拟主机的 IP 属性设置请按照网络拓扑结构图以及“表 3：服务器 IP 地址分配表”的要求设定。

3、除有特别规定外，其他未明确规定用户密码均与用户名相同。

4、所有操作系统镜像文件及试题所需的其他软件均存放于每台计算机的/根目录下。

5、题目要求的虚拟机均安装于每台主机的 D：\virtualPC 目录，即路径为 D：\virtualPC\虚拟主机名称。

一、在 Server 1 上完成如下操作：

（一）完成虚拟主机的创建

安装虚拟机“Centos-A1”，具体要求为内存 512MB，硬盘 10GB；

（二）在主机 Centos-A1 中完成 Samba 共享服务器的部署

1、在此服务器中安装配置 Samba 服务，公司有财务、工程、经理 3 个部门，每个部门对应一个用户组，设为 finance、engineer、manager；每个部门各有 2 个用户，用户分别为： finance01、finance02、engineer01、 engineer02 、manager01、manager02。

```
[root@localhost samba]# groupadd finance
[root@localhost samba]# groupadd engineer
[root@localhost samba]# groupadd manager
[root@localhost samba]# useradd -g finance finance01
[root@localhost samba]# useradd -g finance finance02
[root@localhost samba]# useradd -g engineer engineer01
[root@localhost samba]# useradd -g engineer engineer02
[root@localhost samba]# useradd -g manager manager01
[root@localhost samba]# useradd -g manager manager02
```

2、服务器采用用户验证的方式，每个用户可以访问自己的宿主目录，并且只能有该用户访问宿主目录，并且有完全的权限，而且他人不能看到你的宿主目录。

```
        security = user
        passdb backend = tdbsam
```

3、建立目录/opt/finance,希望 finance 组和 manager 组的人能看到，engineer02 也可以访问，但只有 finance 有写的权限。

```
[root@localhost samba]# mkdir /opt/finance
```

```
[finance]
path = /opt/finance
writable = yes
write list = @finance
valid user=engineer02
read list=@finance,@manager
```

4、建立一个/opt/manager 的目录，只有经理组的人可以访问，并读写，还有 engineer02 也可以访问，但外人看不到那个目录。

```
[root@localhost samba]# mkdir /opt/manager
```

```
[manager]
path = /opt/manager
writable = yes
write list = @manager
valid user=engineer02
browseable=no
```

5、建立一个文件交换目录 exchange，所有的人都能读写包括 guest 用户，但每个人不能删除别人的文件。

```
[exchange]
path = /opt/exchange
write enable=no
public=yes
```

6、阻止客户端上传含有特定关键字的文件或目录到 samba 共享资源，客户端不允许在目录/opt/finance 中上传可执行文件（.exe）及位图（.jpg）文件；客户端不允许在/opt/sales 目录中上传包含 root 关键字的文件或目录。

```
[finance]
path = /opt/finance
writable = yes
write list = @finance
valid user=engineer02
read list=@finance,@manager
veto files=/*.exe,*.jpg/
```

```
[sales]
path = /opt/sales
veto files=/*root*/
```

二、在 Server 2 上完成如下操作：

（一） 完成虚拟主机的创建

1、安装虚拟机“Centos-B1”,具体要求为内存 768MB，硬盘 20GB；分区大小为：SWAP 分区大小为 512M；/boot 分区大小为 500M，文件类型为 ext4；/home 分区大小为 2G，文件类型为 ext4， /分区为 10G，文件类型为 ext4；

2、安装虚拟机“Centos-B2”,具体要求为内存 512MB,硬盘 10GB；

（二） 在主机 Centos-B1 中完成磁盘管理的部署

1、在“Centos-B1”中额外添加 4 块硬盘，容量分别为 2G；

2、此操作需要 1 块硬盘，系统应该有 2GB 的交换空间。配置足够的交换空间，满足以下条件，不删除任何已经存在的 swap 分区，额外的 swap 空间应该均匀分布在两个硬盘上（同等大小），系统启动时，swap 分区应该自动挂载。

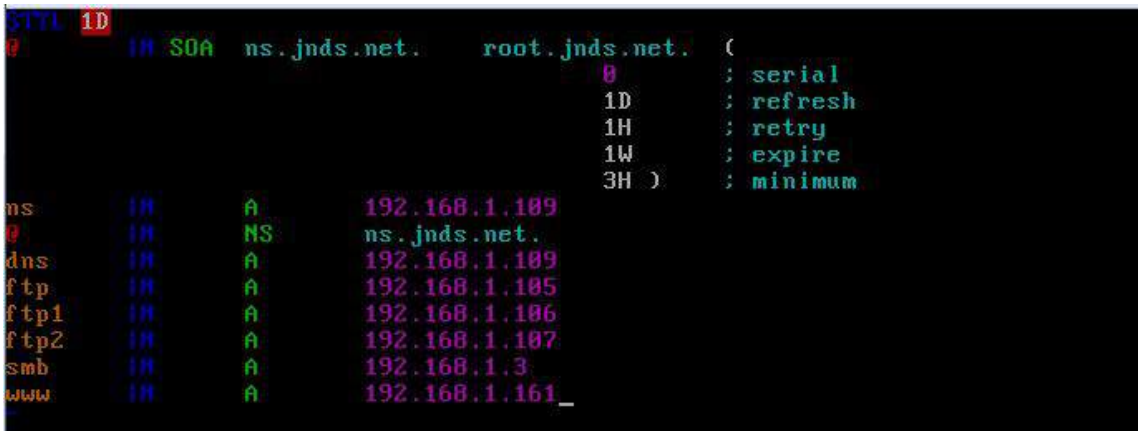
3、此操作需要 3 块硬盘，以前两块硬盘为基础建立冗余阵列 RAID1；要求每周 5 晚 24 点系统自动将第三块硬盘作为热备盘加入到 RAID1 中实现阶段性数据备份；

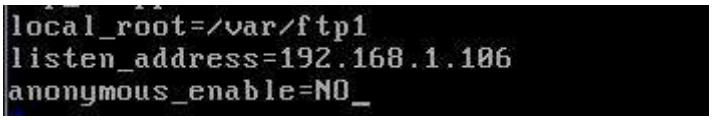
```
[root@localhost etc]# mdadm -C /dev/md0 -l 1 -n 2 /dev/sdc /dev/sdd
mdadm: Note: this array has metadata at the start and
    may not be suitable as a boot device.  If you plan to
    store '/boot' on this device please ensure that
    your boot-loader understands md/v1.x metadata, or use
    --metadata=0.90
Continue creating array?
Continue creating array? (y/n) y
mdadm: Defaulting to version 1.2 metadata
mdadm: array /dev/md0 started.
```

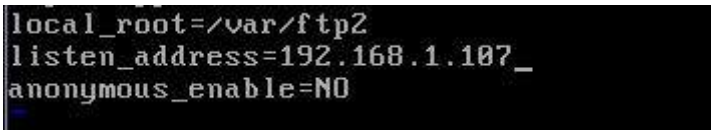
```
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root
HOME=/

# For details see man 4 crontabs

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,f
ri,sat
# |  |  |  |  |
# *  *  *  *  * user-name command to be executed
  *  0  *  *  5 root mdadm /dev/md0 -a /dev/sde
~
~
```

（三）在主机 Centos-B2 中完成 FTP 服务器的部署

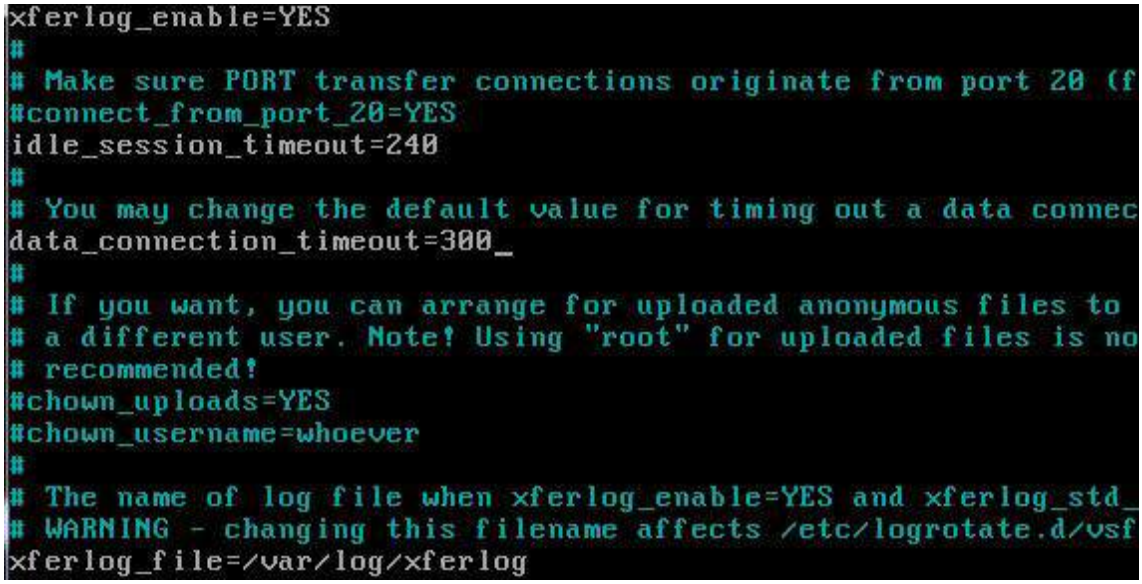
1、配置多站点 FTP 服务，创设三个 FTP 服务站点，域名分别为 ftp.jnds.net、ftp1.jnds.net 以及 ftp2.jnds.net，除站点 ftp.jnds.net 采用默认配置外，其余站点配置文件名分别为 vsftpd1.conf 以及 vsftpd2.conf，站点主目录分别为 /var/ftp1 以及/var/ftp2。为了保证公司的 ftp 服务器的安全性，所有用户都要有登录的账号和密码，匿名访问的用户（anonymous_enable）是不允许登录的；







2、开启 vsftp 的 log 日志功能（xferlog_file）设置，文件保存在 /var/log/xferlog 中。设置：无任何操作的超时时间为 4 分钟,数据连接的超时时间为 5 分钟。注意：主配置文件中的默认单位为秒。



3、为了保证 FTP 的访问速度，设置 FTP 服务器最大支持连接数为 1000 个。

考虑到公司内部某些员工可能会用迅雷、快车等多个 BT 下载工具同时下载文件，所以将同一 IP 地址的 FTP 客户机与 FTP 服务器建立的最大连接数不超过 2 个。

```
max_clients=1000
max_per_ip=2
```

4、在站点 vsftpd1 中，建立本地用户 ftpuser1 及 ftpuser2，两个用户共用同一个主目录，并在主目录中具备上传及下载权限。

```
[root@localhost ftpuser]# usermod -d /var/ftp1 ftpuser1
```

```
[root@localhost ftpuser]# usermod -d /var/ftp1 ftpuser2
```

```
listen_address=192.168.1.106
local_root=/var/ftp1
chroot_local_user=/var/ftp1
write_enble=YES
```

三、 在 Server 3 上完成如下操作：

（一）完成虚拟主机的创建

1、安装名为“Centos-C1”的虚拟机，具体要求为硬盘大小为 20GB，内存为 512MB；

（二）在主机 Centos-C1 中完成 BIND 域名服务器以及代理服务器的部

署

1、在此服务器中安装配置 bind 服务，负责区域“jnds.net”内主机解析，五台主机分别为 dns.jnds.net 、www.jnds.net、www.jnds.lab.com、smb.jnds.net、ftp.jnds.net、ftp1.jnds.net、ftp2.jnds.net,做好正反向 DNS 服务解析，对访问 chinaskills.com 域的解析转发给 win2003_A1；

```
zone "jnds.net" IN {
        type master;
        file "named.jnds.net";
        allow-update { none; };
};
zone "jnds.lab.com" IN {
        type master;
        file "named.jnds.lab.com";
        allow-update { none; };
};

zone "1.168.192.in-addr.arpa" IN {
        type master;
        file "named.empty";
        allow-update { none; };
};
```

```
$TTL 1D
@       IN SOA  ns.jnds.net.    root.jnds.net.  (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
ns      IN      A       192.168.1.109
@       IN      NS      ns.jnds.net.
dns     IN      A       192.168.1.109
ftp     IN      A       192.168.1.105
ftp1    IN      A       192.168.1.106
ftp2    IN      A       192.168.1.107
smb     IN      A       192.168.1.3
www     IN      A       192.168.1.161
```

```
$TTL 1D
@       IN SOA  ns.jnds.lab.com.        root.jnds.lab.com.      (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
ns      IN      A       192.168.1.109
@       IN      NS      ns.jnds.lab.com.
www     IN      A       192.168.1.161
```

```
$TTL 3H
@       IN SOA ns.jnds.net.     root.jnds.net. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
@       IN      NS      ns.jnds.net.
109     IN      PTR     ns.jnds.net.
@       IN      PTR     ns.jnds.lab.com.
109     IN      PTR     ns.jnds.lab.com.
109     IN      PTR     smb.jnds.net.
105     IN      PTR     ftp.jnds.net.
106     IN      PTR     ftp1.jnds.net.
107     IN      PTR     ftp2.jnds.net.
3       IN      PTR     smb.jnds.net.
161     IN      PTR     www.jnds.net.
161     IN      PTR     www.jnds.lab.com._
```

```
options {
        listen-on port 53 { any; };
        listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        allow-query     { any; };
        recursion yes;
        forwarders{192.168.1.1;};_
```

2、安装并完成代理服务器 squid 的初始配置，使用 8080 作为代理服务端口，指定 DNS 服务器 IP 地址信息，使得 squid 服务器能够解析域名；

```
http_port 8080
dns_nameservers 192.168.1.109
```

3、设置 squid 代理服务器采用 ufs 缓存机制，缓存目录设置为/cache,目录容量为 5GB，L1 及 L2 级目录数量分别为 16 及 256，定义高速缓存值为 512MB；

```
cache_dir ufs /cache 5120 16 256
cache_mem 512 MB
```

4、针对主机 192.168.1.0 /24 提供代理服务，为缓解请求队列忙碌，设置重定向器池进程数为 20，并将缓存日志存放于/var/squid/cache.log 中；

```
visible_hostname 192.168.1.0/24
redirect_children 20
cache_log /var/squid/cache.log_
```

四、在 **Server 4** 上完成如下操作：

（一）完成虚拟主机的创建

1、Server4 主机系统为 CentOS6.5，需要在此 Linux 平台上采用 KVM 方式安装虚拟机“Centos-D1”，具体要求为硬盘大小为 12GB，内存为 768MB，系统为 CentOs6.5；（小提示：如无法正确安装虚拟机 Centos-D1，下述题目中所涉及的虚拟机题目可在 Server4 真实主机中完成）

（二）在主机 **Centos-D1** 中完成 **Apache** 服务器服务器的部署

1、在此服务器中安装配置 WEB 服务，建立 web 站点：www.jnds.com 和 www.jnds.lab.com。

```
NameVirtualHost *:80
#
# NOTE:  NameVirtualHost cannot be used without a port specifier
# (e.g. :80) if mod_ssl is being used, due to the nature of the
# SSL protocol.
#

#
# VirtualHost example:
# Almost any Apache directive may go into a VirtualHost container.
# The first VirtualHost section is used for requests without a known
# server name.
#
<VirtualHost *:80>
    DocumentRoot /www/1
    ServerName www.jnds.net
</VirtualHost>
<VirtualHost *:80>
    DocumentRoot /www/2
    ServerName www.jnds.lab.com
</VirtualHost>
```

2、在站点 www.jnds.com 上建立两个虚拟目录 en 和 cn，其对应的物理路径分别是/data/CN 和/data/EN。配置 Web 服务器对虚拟目录/data/CN 启用用户认证，只允许 webadmin 用户访问。配置 Web 服务器对虚拟目录/data/EN 仅允许来自网络 jnds.com 域和 192.168.X.0/24 网段的客户机访问该虚拟目录。

```
[root@localhost conf]# mkdir -p /data/cn
[root@localhost conf]# mkdir -p /data/en
```

```
Alias en "/data/en"
Alias cn "/data/cn"
```

```
<Directory "/data/cn">
    Options Indexes MultiViews FollowSymLinks
    AllowOverride all
    authname "1"
    authtype basic
    authuserfile /etc/httpd/conf/htpasswd
    require user webadmin
    Order allow,deny
    Allow from all
</Directory>
<Directory "/data/en">
    Options Indexes MultiViews FollowSymLinks
    AllowOverride none
    Order allow,deny
    Allow from jnds.com 192.168.*.0/24
</Directory>
```

3、建立主页，要求如下：

www. jnds.com 主页内容为“jnds.com”；

www. jnds.lab.com 主页内容为“china.lab.com”；

www. jnds.com/en 主页内容为“en. jnds.com”；

www. jnds.com/cn 主页内容为“cn. jnds.com”

2015 年全国职业院校技能大赛

网络搭建与应用竞赛

（总分 1000 分）

赛题说明

一、竞赛内容分布

“网络搭建与应用”竞赛共分二个部分，其中：

第一部分：网络搭建及安全部署项目，占总分的比例为 45%；

第二部分：服务器配置及应用项目，占总分的比例为 55%；

二、竞赛注意事项

（1）禁止携带和使用移动存储设备、计算器、通信工具及参考资料。

（2）请根据大赛所提供的比赛环境，检查所列的硬件设备、软件清单、材料清单是否齐全，计算机设备是否能正常使用。

（3）本试卷共有两个部分。请选手仔细阅读比赛试卷，按照试卷要求完成各项操作。

（4）操作过程中，需要及时保存设备配置。比赛结束后，所有设备保持运行状态，不要拆、动硬件连接。

（5）比赛完成后，比赛设备、软件和赛题请保留在座位上，禁止将比赛所用的所有物品（包括试卷和草纸）带离赛场。

（6）所有需要提交的文档均放置在桌面的 PC1“比赛文档”文件夹中，禁止在纸质资料上填写与竞赛无关的标记，如违反规定，可视为 0 分。

（7）裁判以各参赛队提交的竞赛结果文档为主要评分依据。所有提交的文档必须按照赛题所规定的命名规则命名，文档中有对应题目的小标题，截图有截图的简要说明，否则按无效内容处理。

（8）与比赛相关的工具软件放置在 D 盘的 tools 文件夹中。

项目背景及网络拓扑

某天津集团公司在天津设置有总公司，总公司使用 ospf 技术,在上海设置分公司,分公司使用 RIPv1 技术，两地公司的网络一直未统一管理，现总公司提出网络整合。所以对网络进行改造。

改造主要的工作是租用 ISP 的专线链路，解决两地互联问题。网络管理员使用路由重发布技术进行两地互通。然后通过 Internet 采用基于 GRE-VPN 技术作为备份链路。以实现业务流量的高可用性。集团网络具体拓扑结构如图 1 所示。

总公司有四个部门，分别为财务部、工程部、软件部和系统集成部四个部门，上海分公司设有行政部和销售部。

请你帮助公司网络管理员进行网络调试与改造，完成相关任务。

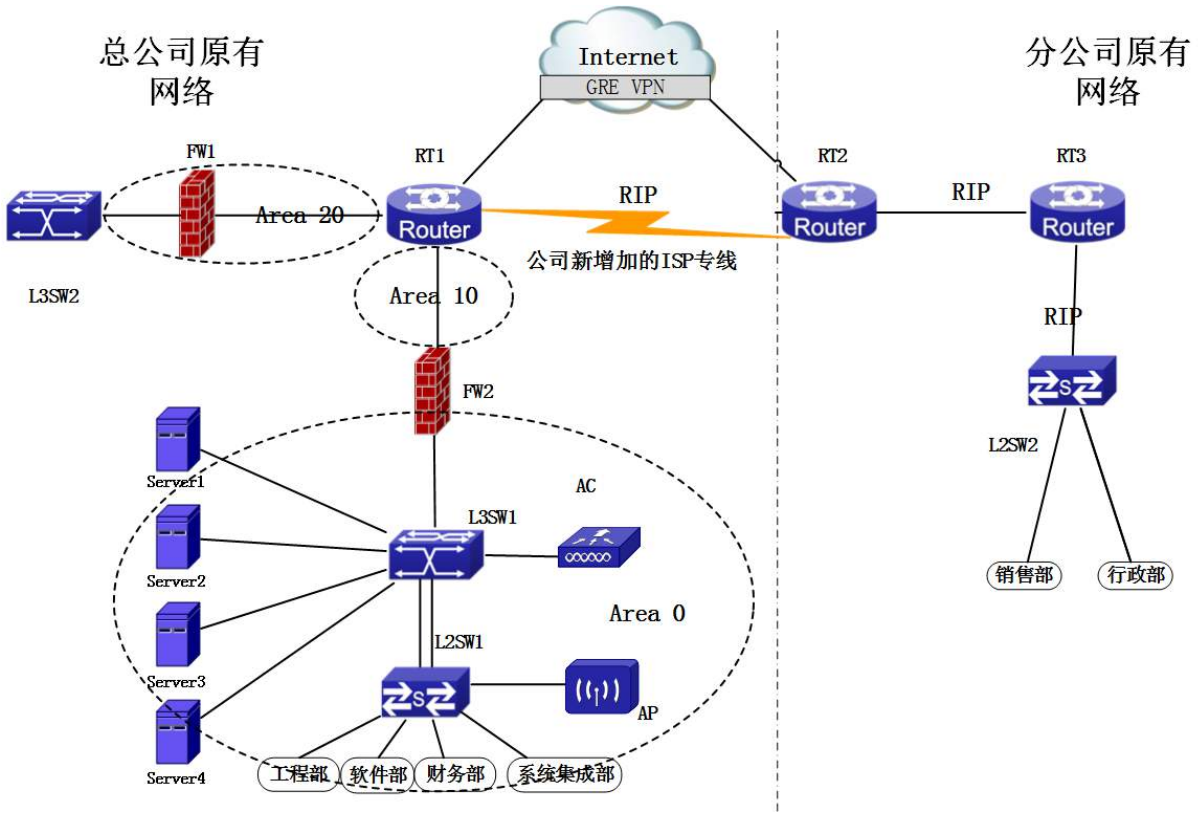

总公司原有
网络
Internet
GRE VPN
分公司原有
网络
FW1
RT1
RT2
RT3
RIP
RIP
Area 20
Router
Router
Router
公司新增加的ISP专线
L3SW2
Area 10
RIP
FW2
L2SW2
Server1
AC
L3SW1
Server2
Area 0
L2SW1
Server3
AP
Server4
工程部
软件部
财务部
系统集成部
销售部
行政部

表 1 网络设备连接表

设备一	设备一端口	设备一地址	设备二	设备二端口	设备二地址
RT1	Serial0/1		RT2	Serial0/2	
RT1	GE0/4		FW1	Ethernet0/3	
RT1	GE0/3		FW2	Ethernet0/3	
RT1	GE0/6	123.11.1.1/24	RT2	GE0/6	123.11.1.2/24
RT2	GE0/3		RT3	GE0/3	
RT2	Tunnel		RT3	Tunnel	
RT3	GE0/4		L2SW2	Ethernet1/24	----------
RT3	Loopback1	10.1.204.1/24	----------	----------	----------
FW1	Ethernet0/4		L3SW2	Ethernet1/0/24(VLAN100)	
FW1	Loopback1	10.1.104.1/24	------	----------	----------
FW2	Ethernet0/4		L3SW1	Ethernet1/0/22(VLAN100)	
L3SW1	Ethernet1/0/23	----------	L2SW1	Ethernet1/23	----------
L3SW1	Ethernet1/0/24	----------	L2SW1	Ethernet1/24	----------
L3SW1	Ethernet1/0/21	----------	AC	Ethernet1/0/24	----------
L2SW1	Ethernet1/20	----------	AP	lan	----------
L3SW1	Ethernet1/1	----------	Server A	NIC	
L3SW1	Ethernet1/2	----------	Server B	NIC	
L3SW1	Ethernet1/3	----------	Server C	NIC	
L3SW1	Ethernet1/4	----------	Server D	NIC	

表 2 网络设备 IP 地址分配表

	网关地址及掩码
VLAN10 SVI(工程部)	
VLAN20 SVI(软件部)	
VLAN30 SVI(财务部)	
VLAN40 SVI(系统集成部)	
VLAN50 SVI(服务器)	10.1.100.254/24

表 3：服务器 IP 地址分配表

宿主机	虚拟主机名称	域名信息	服务角色	系统及版本信息	IPv4地址信息

Server 1	Win2003-A1	dc.chinaskills.com	域控制器 DNS 服务器 CA 证书服务器	Windows Server 2003 R2	IP: 10.1.100.100
	Win2008-A1	dhcp.chinaskills.com	DHCP 服务器	Windows Server 2008 R2	IP: 10.1.100.101
	Centos-A1	target.jnds.net	iSCSI 远程存储服务端	Centos 6.5	IP: 10.1.100.102
Server 2	Win2008-B1	www1.chinaskills.com	WEB 服务器 NLB 集群服务	Windows Server 2008 R2	IP: 10.1.100.150
	Win2008-B2	bdns. chianskills.com	备份 DNS	Windows Server 2008 R2	IP: 10.1.100.103
	Centos-B1	ftp.jnds.net ftp1.jnds.net ftp2.jnds.net	iSCSI 远程存储客户端 FTP 文件服务器	Centos 6.5	IP: 10.1.100.104 IP: 10.1.100.105 IP: 10.1.100.106
Server 3	Win2008-C1	www2.chinaskills.com	WEB 服务器 NLB 集群服务	Windows Server 2008 R2	IP: 10.1.100.160
	Win2008-C2	ftp.chinaskills.com	FTP 服务器 备份域控制器	Windows Server 2008 R2	IP：10.1.100.107
	Centos-C1	dns.jnds.net	BIND 域名服务器 Squid 代理服务器	Centos 6.5	IP: 10.1.100.108
Server 4（Linux 虚拟化主机）	Centos-D1	www.jnds.net bbs.jnds.net	Apache web 服务器 MySQL 数据库服务器	Centos 6.5	IP: 10.1.100.109

一、 网络搭建部分（450 分）

【注意事项】

设备 console 线有两条，。交换机， AC，防火墙使用同一条 console 线，路由器使用另外一条 console 线。

设备配置完毕后，保存最新的设备配置。保存文档方式分为两种：

交换机和路由器要把 show running-config 的配置保存在 PC1 桌面的相应文档中，文档命名规则为：设备名称.doc,例如：RT1 路由器文件命名为：RT1.doc，然后放入到 PC1 桌面上“比赛文档”文件夹中

防火墙等截图方式的设备，把截图的图片放到同一 word 文档中，文档命名规则为：设备名称.doc,例如：防火墙 FW1 文件命名为：FW1.doc, 保存后放入到 PC1 桌面上“比赛文档”文件夹中。

1、 物理连接与 IP 地址划分

（1） 按照网络拓扑图制作以太网网线，并连接设备。要求符合 T568A 和 T568B 的标准，其线缆长度适中。

（2） 根据“拓扑结构图”和“网络设备 IP 地址分配表”所示，对网络中的所有设备接口配置 IP 地址,并填入表中。

分配地址时做到节省 IP 资源，合理分配(先划分大的地址块，再划分小的地址块，可以节省 IP 资源)。总公司中除服务器区所有主机规划使用 10.1.1.0/20 所在地址段。财务部有 12 台主机、工程部有 75 台主机、软件部和系统集成部两个部门都有 120 台主机，服务器的网段为 10.1.100.0/24。分公司使用 10.1.200.100/22 所在地址段。总公司与分公司所有设备互联地址使用 192.168.1.0/24 的掩码进行分配，并把地址填入上面网络设备 IP 地址分配表中的空白处。

本卷规定：

- 网关地址为每个网段的最后一个 IP 地址。

2、 交换机配置

（1） 为交换机设备命名，命名规则参考为表 1 中的“设备名称”。

（2） 用户为了维护方便，需要远程控制 L3SW1 和 L3SW2 交换机。通过 telnet 的技术使用。只允许 10.1.100.0/24 整个网段都可以进行登陆。用户名为:server, 密码 为 serverenable,用户特权密码为 enable,。

（3） 依据“拓扑结构图”和 VLAN 接口地址表，在交换机上完成 VLAN 配置和端口分配。

VLAN 接口地址表

设备	VLAN 名称	VLAN ID	接口
L2SW1	Link-to-CW	10	Ethernet1/1~ Ethernet1/4
	Link-to-RJ	20	Ethernet1/5~ Ethernet1/8
	Link-to-XTJC	30	Ethernet1/9~ Ethernet1/12
	Link-to-GC	40	Ethernet1/13~ Ethernet1/16
L3SW1	Link_to_Server	50	Ethernet1/0/1~ Ethernet1/0/4

（4） 总公司采用 DCHP 的方式 把地址动态分配给 vlan10,vlan20,vlan30,vlan40 的用户。DHCP 服务器的地址是 10.1.100.101。

（5） 总公司两个核心交换机 L2SW1 和 L3SW1 之间使用冗余线路连接，端口 23 和端口 24 配置端口聚合，方式为动态方式。

（6） 分公司的地址都在同一网段。但分为两个部门，销售部，行政部。现公司领导要求：销售部，行政部之间不能互相访问，公司内部来访人员的有 2 台电脑，这 2 台电脑之间不可以互相访问，也不可以访问销售部，行政部。无线相当于销售部或

行政部的功能。

Vlan 名称	部门	接口
10	销售部	Ethernet1/0/1~ Ethernet1/0/2
20	行政部	Ethernet1/0/3~ Ethernet1/0/4
30	无线	Ethernet1/0/5~ Ethernet1/0/6
40	来访人员	Ethernet1/0/7~ Ethernet1/0/8

(7) 总公司内部主机经常无法上网，网管在解决故障时发现，主机自动获取的地址是 192.168.100.1 网段地址，经过排障发现，由于很多人私自架设无线路由导致，请配置相关命令，防止非法的 DHCP Server 影响网络，公司的 DHCP 服务器在 L2SW1 上。

(8) 在改造过程中，网络管理员提出网络经常上网时断时续，有时完全断网，猜测有可能是 ARP 病毒引起网络故障，为了确认故障问题，在 L2SW1 上通过 22 端口进行双向流量的查看，请帮助管理员查找问题所在。

(9) 经过查看后发现是端口 10 的主机发出的 arp 网关欺骗报文，欺骗其它主机，除了对系统相应的杀毒处理后，为了避免相同故障再次发生，在交换机的端口 10 上进行 ARP 的保护。请配置相关命令。

(10) 通过这次流量查看发现，在 L2SW1 的交换机上在端口 19 端口 20 之间有异常流量，占用流量非常大，管理员决定把端口经行隔离，请配置相关命令。

(11) OSPF 区域 0 开启基于区域的认证。认证方式为 MD5 方式，密码为 123。

3、 路由器配置与调试

(1) 为路由设备命名，命名规则参考为表 1 中的“设备名称”。

(2) 根据网络拓扑图所示，为了保障 ISP 的租用专用线路的链路安全，需要在 RT1 与 RT2 之间连接的链路上配置 PPP 协议，采用双向 CHAP 的验证方式，用户名分别使用对方的用户名 RT1 和 RT2，密码均为 7654321。速率为 9600

(3) 总公司网络中采用的 OSPF 动态路由协议，根据“网络拓扑结构图”所示，配置动态路由协议，将设备接口分配到不同的区域中。分公司的采用 RIPv1 动态路由协议保障网络正常通信。RT 3loopback 口需要通告进 RIP。

(4) 下面的是网络设备 RID，防火墙使用 ROUTER-ID 的方式的设置相关信息。其它设备不能使用 ROUTER-ID 的方式的设置相关信息。

设备名称	RID
FW1	1.1.1.1
FW2	2.2.2.2
RT1	3.3.3.3
L3SW1	4.4.4.4
L3SW2	5.5.5.5

(5) 在总公司与分公司的互联网出口设备上，需要将去往互联网的默认路由引入到动态路由中。

(6) 总公司与分公司通过地址池方式进行NAT映射.保证总公司与分公司可以正常上网，要求两个公司只能从自己的出口进行上网访问。要求访问控制列表的名字为

nat,RT1 和 RT2 上使用地址池的方式，名称为 natpool，地址池的范围都是 123.11.1.1-123.11.1.253/24。

(7) 管理员把总公司去往外网的 TCP 流量整形成 cir 为 17000 bc8000 be8000QOS

(8) 为了保障总公司与分公司之间传输业务的高可用性，当总公司与分公司之间的 ISP 专线中断后，需要采用互联网链路做为备份链路，在集团公司与上海分公司的两端路由器上配置 GRE VPN

(9) 公司网络改造完成后，服务器的流量通过 ISP 的专线去往分公司，工程部通过 GREVPN 去往分公司

(10) 当分公司与总公司的网络按照网络管理员的思路改造完成时，改造后，网络管理员发现分公司到总公司的网络是不通的，请帮助网管员查找故障并解决。

4、 防火墙配置

(1) 把防火墙进行设备命名，命名规则参考为表 1 中的“设备名称”。

(2) 在总公司 FW2 上设置 URL 过滤，禁止内网访问 www.163.com，要求主要过程进行截图。

(3) 在总公司的 FW1 和 FW2 使用 OSPF 协议，根据与路由的相关配置，完成防火墙的配置，保证网络互通。FW1 通告进 OSPF

(4) 内网用户 10.1.100.50 在访问 www.baidu.com 和 www.google.com 已经将日志信息记录到了日志内存缓存中。，要求主要过程进行截图。

(5) 在总公司 FW2 上，要求内网用户不能登陆 MSN，要求主要过程进行截图

(6) 在总公司 FW2 上，为了保障网络资源合理使用，在总公司上配置禁止 VLAN10 和 VLAN30 网段所有 P2P 软件视频数据通过。每个用户的网络速率为上行最大 64K，下行最大 128K，要求主要过程进行截图。

(7) 当总公司 FW2 上有人用 console 登陆配置设备时，需要发送向 administrator@sina.com 地址发送邮件进行提醒记录。新浪邮箱发信(smtp)服务器的地址为：smtp.sina.com，新浪邮箱服务器的地址为：pop.sina.com，要求主要过程进行截图

5. 无线配置

(1) 总公司软件部经常移动办公,所以部分用户采用无线接入方式,其中 SSID 为 TJ+自己的组号，协议为 802.11b，信道为 1；地址池 10.1.1.128/25,网关为 10.1.1.254/25，DNS 地址为 8.8.8.8.用户接入无线网络时采用 WEP 认证方式，其口令为 012345678。

(2) 配置 AP 下可以连接的无线用户数是 20。

(3) 配置无线局域网用户上行速度为 512Kbps,下行速度为 2Mbps,突发速度为 4Mbps。

(4) 网络管理员发现 AP 的发射功率较小，客户端发送总是出现丢包的现象，通过手动触发调整功率。

(5) 假设 AP1 和 AP2 有着相同的信道，在 AC 上开启 radio 的自动信道调整功能，设置触发时间为每天的 8:00。

二 操作系统部分（550 分）

Windows 操作系统

【说 明】

（1）题目中所涉及 Windows 操作系统的 administrator 管理员以及其他普通用户密码均为 2015Netwlrk（注意区分大小写），若未按照要求设置密码，涉及到该操作的所有分值记为 0 分。

（2）虚拟主机的 IP 属性设置请按照网络拓扑结构图以及“表 3：服务器 IP 地址分配表”的要求设定。

（3）除非作特殊说明，在同一主机下需要安装相同操作系统版本的虚拟机时，可采用 Oracle VM VirtualBox 软件自带的克隆系统功能实现。

（4）所有系统镜像文件及试题所需的其它软件均存放在每台主机的 D:\soft 文件夹中，并将题目要求的截图内容以.jpg 格式存储于桌面 BACKUP 文件夹中。

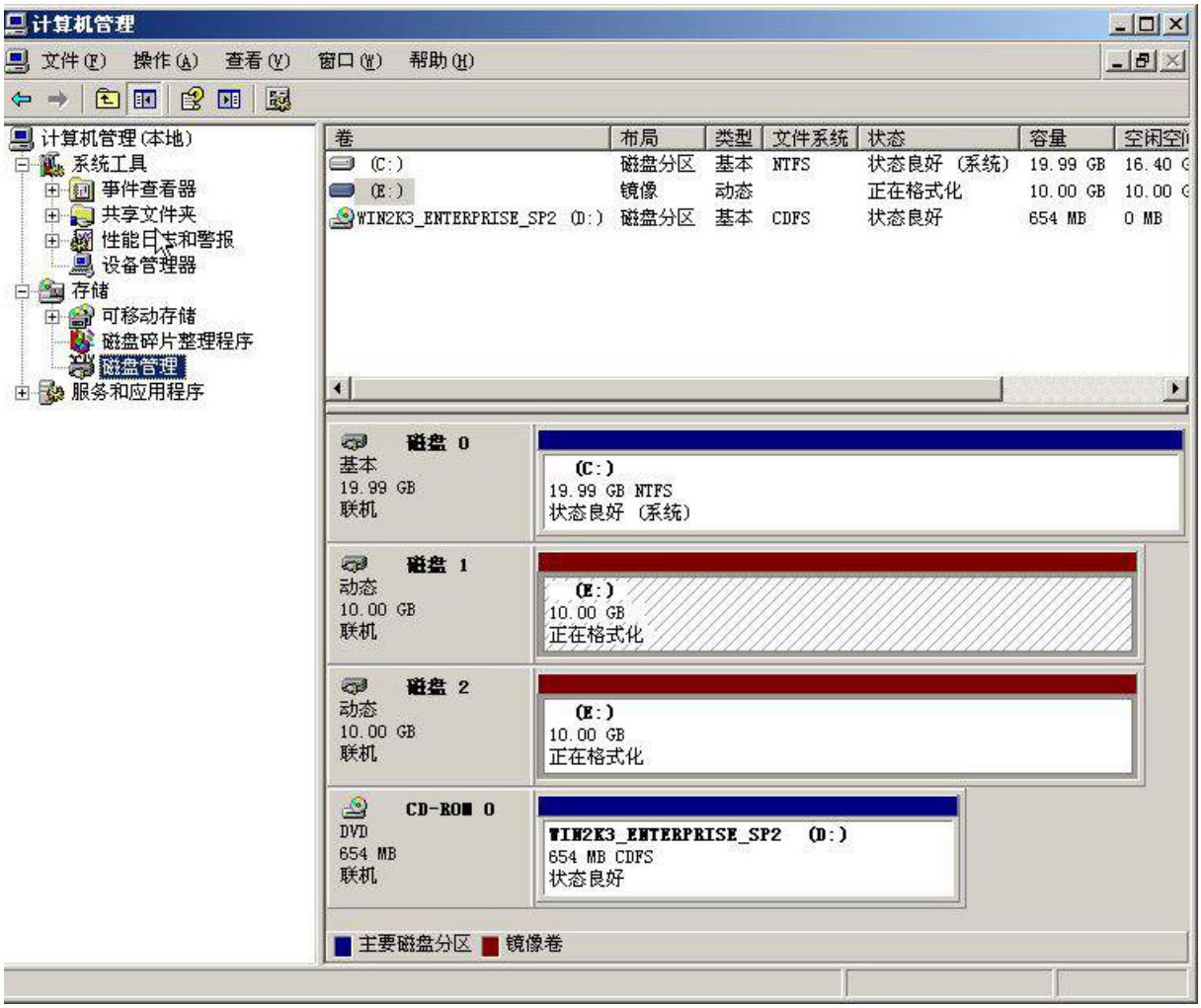
（5）题目要求的虚拟机均安装于每台主机的 D：\virtualPC 目录，即路径为 D：\virtualPC\虚拟主机名称。

一、在 Server 1 上完成如下操作：

（一）完成虚拟主机的创建

1、安装虚拟机“Win2003-A1”，具体要求为内存为 1G，硬盘 20G；

2、在虚拟机“Win2003-A1”中添加 SCSI 控制器，添加二块 SCSI 虚拟硬盘，其每块硬盘的大小为 10G；将二块硬盘制作成 RAID1，磁盘盘符为 e:\；



3、安装虚拟机“Win2008-A1”，具体要求为内存为 1G，硬盘 20G，并将服务器加入到 Windows 域环境；

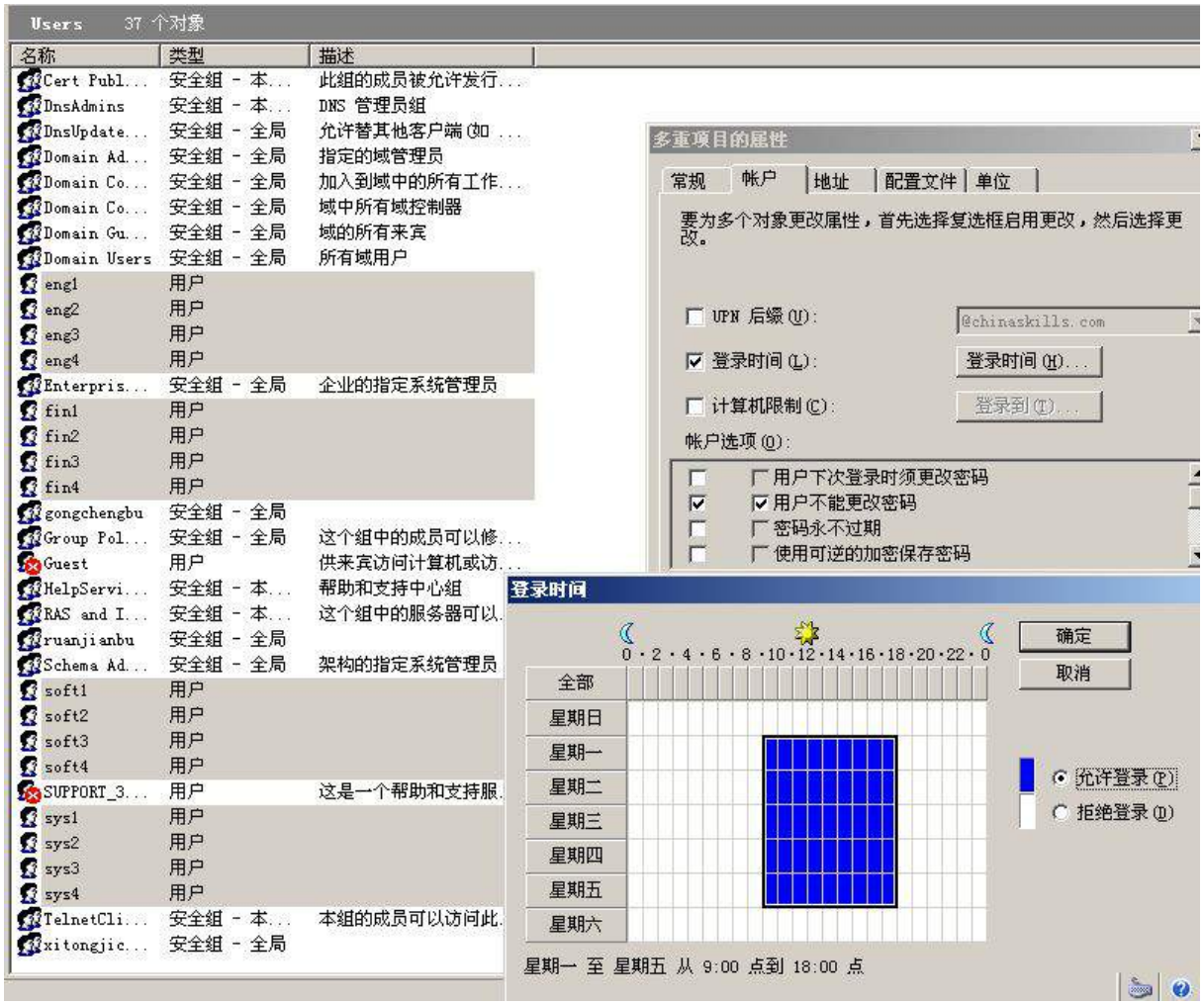
（二）在主机 Win2003-A1 中完成域控制器的部署

1、创建 4 个用户组，**组名采用对应部门名称的拼音来命名**，每个部门都创建 4 个

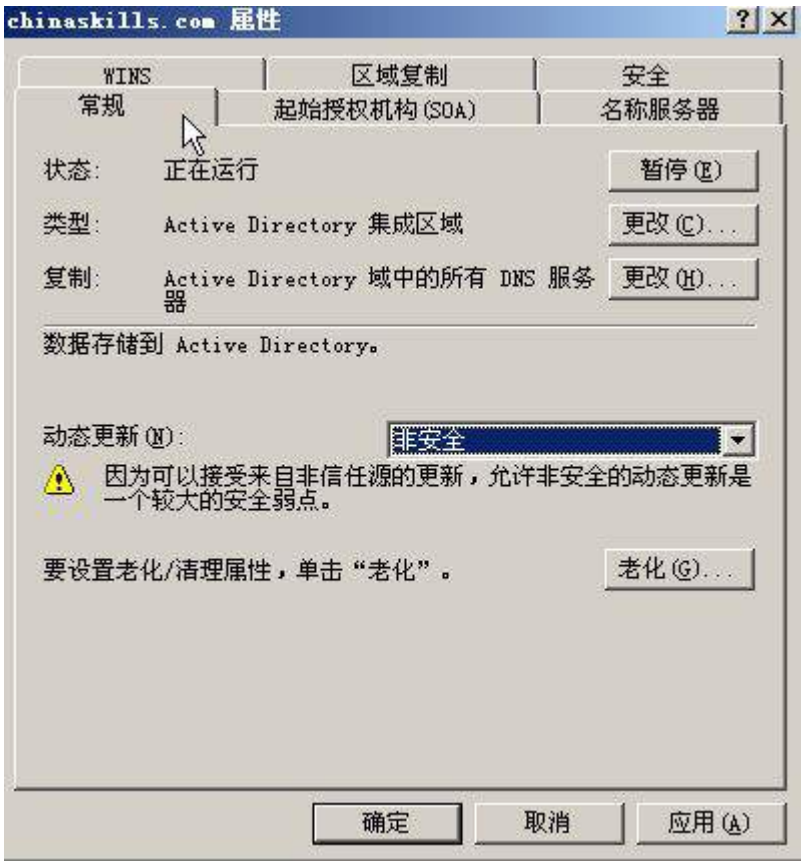
用户，财务部用户：fin1~fin4、工程部用户：eng1~eng4、软件部用户：soft1~soft4、系统集成部用户：sys1~sys4，所有用户不能修改其用户口令，具体口令为 2015Netw1rk，并要求用户只能在上班时间可以登录（每周工作日 9:00~18:00）；


ruanjianbu 属性
常规
成员
隶属于
管理者
成员(M):
名称
Active Directory 文件夹
soft1
chinaskills.com/Users
soft2
chinaskills.com/Users
soft3
chinaskills.com/Users
soft4
chinaskills.com/Users
添加(D)...
删除(R)
确定
取消
应用(A)


xitongjichengbu 属性
常规
成员
隶属于
管理者
成员(M):
名称
Active Directory 文件夹
sys1
chinaskills.com/Users
sys2
chinaskills.com/Users
sys3
chinaskills.com/Users
sys4
chinaskills.com/Users
添加(D)...
删除(R)
确定
取消
应用(A)



2、将此服务器配置为主 DNS 服务器，正确配置 chinaskills.com 域名的正向及反向解析区域，能够正确解析 chinaskills.com 域中的所有服务器；创建对应服务器主机记录,需要关闭网络掩码排序功能。设置DNS服务正向区域和反向区域与活动目录集成；要求动态更新设置为非安全；

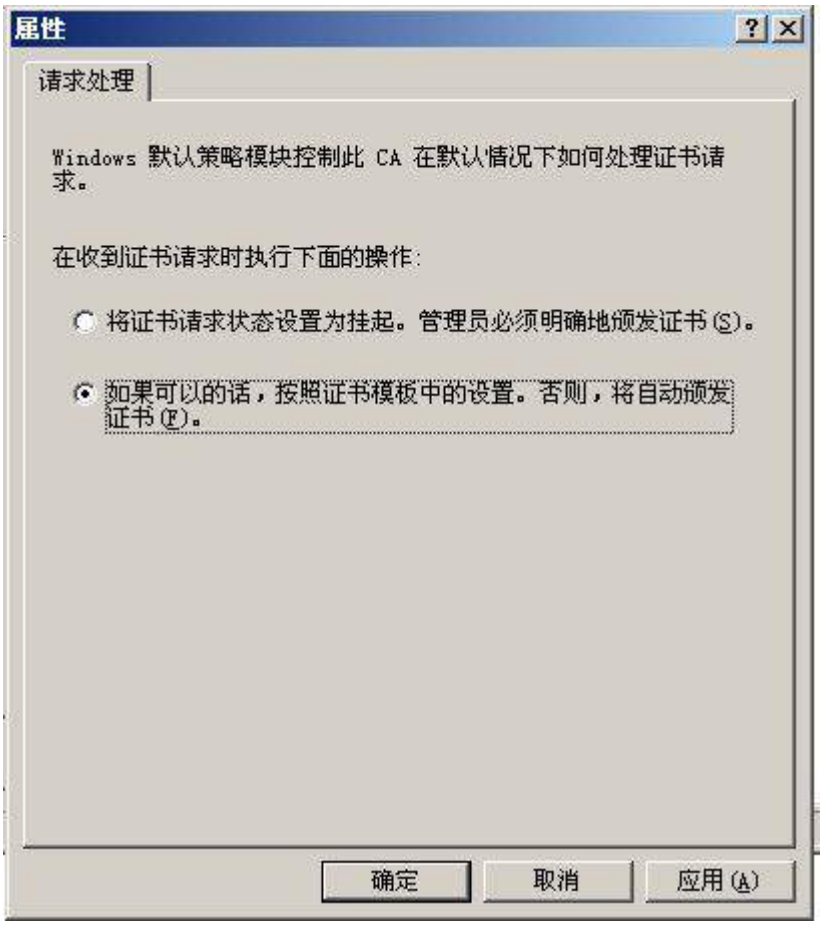

chinaskills.com 属性
WINS
区域复制
安全
常规
起始授权机构(SOA)
名称服务器
状态:
正在运行
暂停(P)
类型:
Active Directory 集成区域
更改(C)...
复制:
Active Directory 域中的所有 DNS 服务器
更改(H)...
数据存储到 Active Directory。
动态更新(N):
非安全
因为可以接受来自非信任源的更新，允许非安全的动态更新是一个较大的安全弱点。
要设置老化/清理属性，单击“老化”。
老化(G)...
确定
取消
应用(A)


DC 属性
事件日志
监视
安全
接口
转发器
高级
根提示
调试日志
服务器版本号(S):
5.2 3790 (0xece)
服务器选项(V):
禁用递归(也禁用转发器)
BIND 辅助区域
如果区域数据不正确，加载会失败
启用循环
启用网络掩码排序
保护缓存防止污染
名称检查(N):
多字节(UTF8)
启动时加载区域数据(L):
从 Active Directory 和注册表
启用过时记录自动清理(E)
清理周期(C):
0
天
重置成默认值(R)
确定
取消
应用(A)

3、将此服务器设置为域控制器，设置域和林的功能级别为 Windwos Server 2003；此外，安装证书服务，设置为企业根，有效期为 5 年，为企业内部自动回复证书申请；

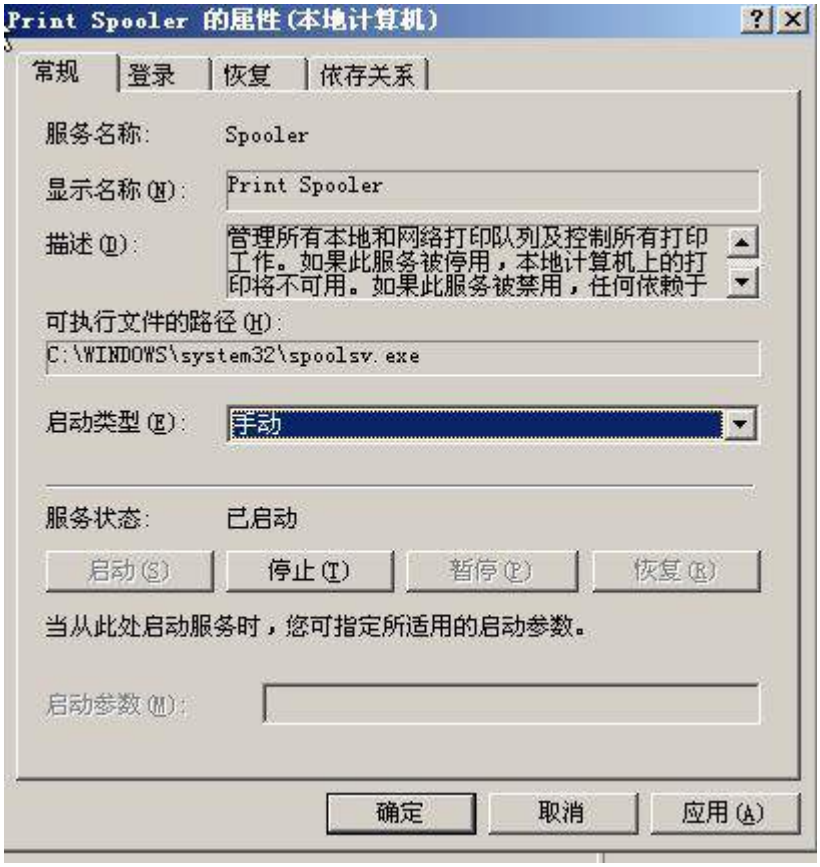

Windows 组件向导
CA 类型
选择您想设置的 CA 类型。
企业根 CA(E)
企业从属 CA(R)
独立根 CA(S)
独立从属 CA(T)
CA 类型的描述
企业中最受信任的 CA。应该在安装其他 CA 之前安装。
用自定义设置生成密钥对和 CA 证书(U)
< 上一步(B)
下一步(N) >
取消
帮助

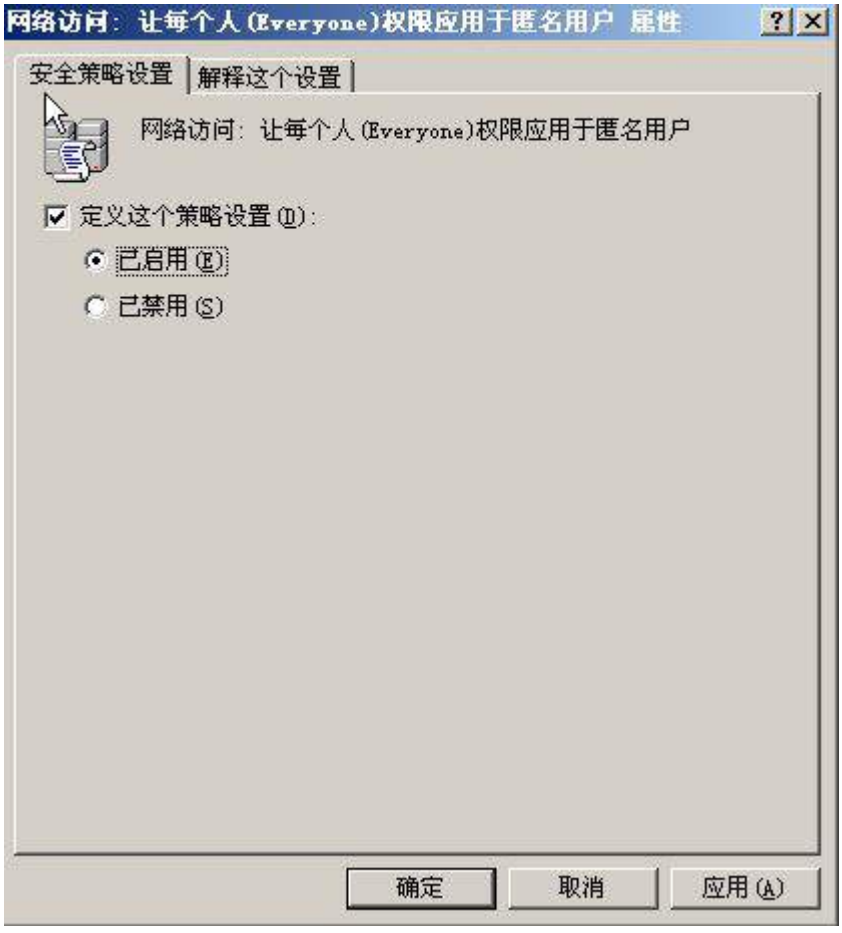

Windows 组件向导
CA 识别信息
输入识别该 CA 的信息。
此 CA 的公用名称(C):
CACACACACA
可分辨名称后缀(D):
DC=chinaskills, DC=com
可分辨名称的预览(P):
CN=CACACACACA, DC=chinaskills, DC=com
有效期限(V):
5
年
截止日期:
2021-5-4 19:26
< 上一步(B)
下一步(N) >
取消
帮助

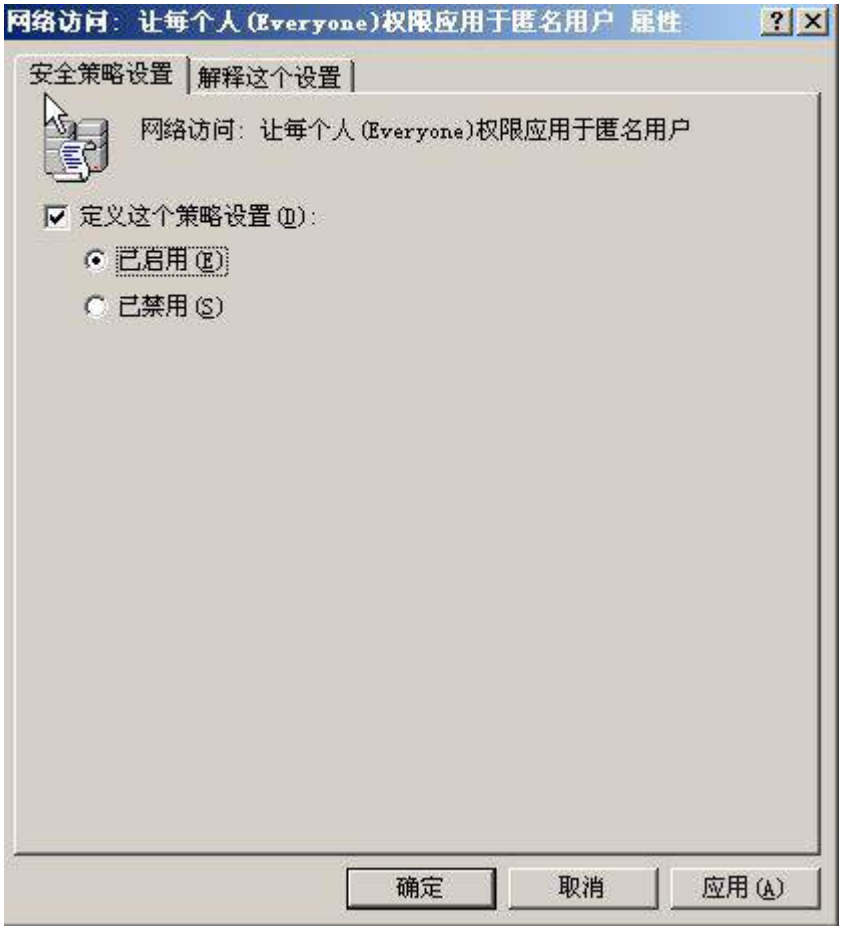


4、制订备份计划，每天的 0 点对“系统状态”进行备份，并采用 VSS 完整备份，备份至 e:\盘；

5、设置组策略把的“print spooler”服务改为手动启动；设置组策略对 “不显示上次登录名”选项已启用;设置组策略禁用“将everyone权限应用于匿名用户”；更改组策略密码策略为无复杂性要求；


Print Spooler 的属性(本地计算机)
常规
登录
恢复
依存关系
服务名称:
Spooler
显示名称(N):
Print Spooler
描述(D):
管理所有本地和网络打印队列及控制所有打印工作。如果此服务被停用，本地计算机上的打印将不可用。如果此服务被禁用，任何依赖于
可执行文件的路径(H):
C:\WINDOWS\system32\spoolsv.exe
启动类型(E):
手动
服务状态:
已启动
启动(S)
停止(T)
暂停(P)
恢复(R)
当从此处启动服务时，您可指定所适用的启动参数。
启动参数(M):
确定
取消
应用(A)


网络访问: 让每个人(Everyone)权限应用于匿名用户 属性
安全策略设置
解释这个设置
网络访问: 让每个人(Everyone)权限应用于匿名用户
定义这个策略设置(D):
已启用(E)
已禁用(S)
确定
取消
应用(A)



（三）在主机 Win2008-A1 中完成 DHCP 服务器的部署

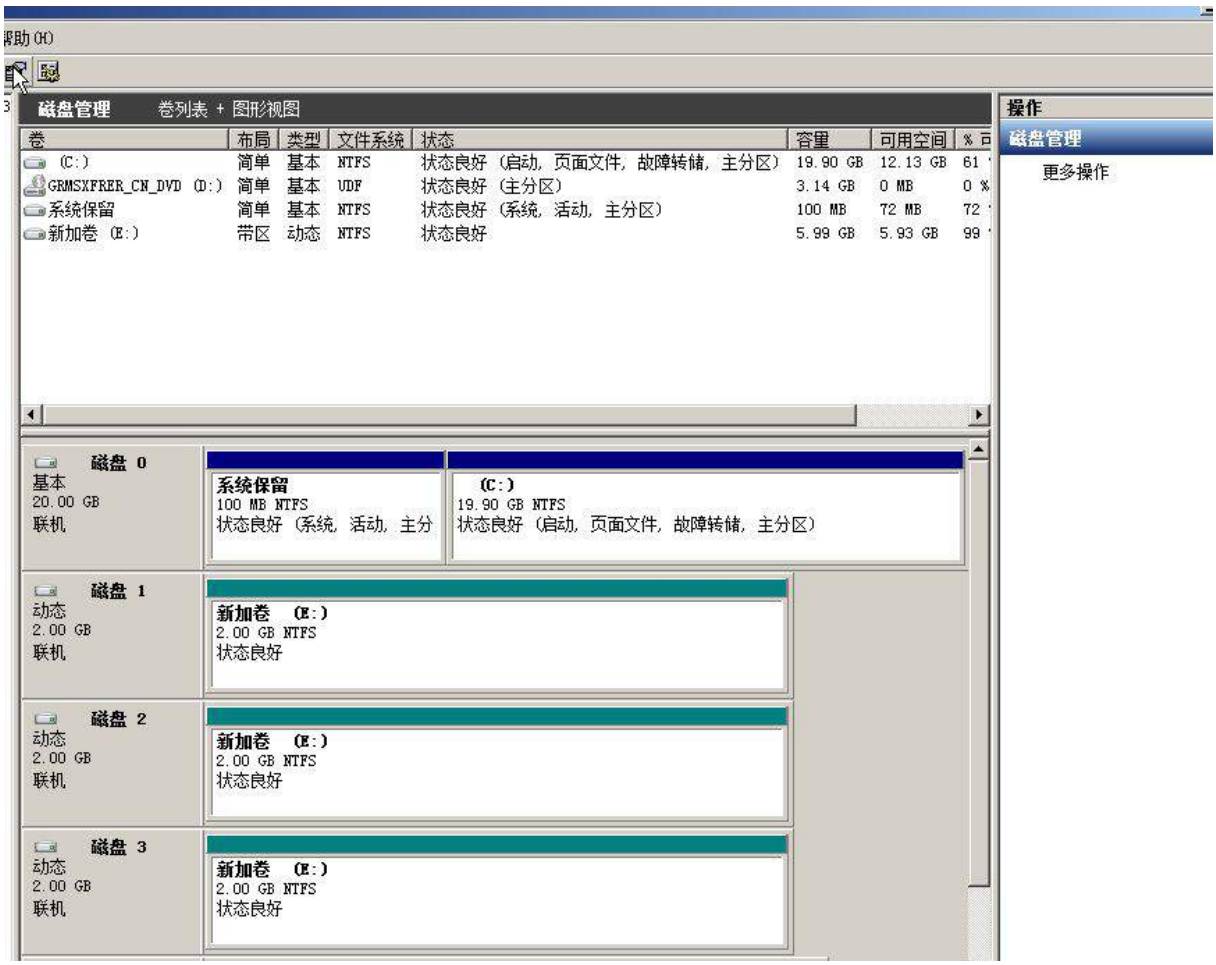
安装 DHCP 服务，为**内网财务部、工程部、软件部和系统集成部**的用户主机动态分配 IPv4 地址，建立作用域，作用域的名称采用对应部门名称的拼音，超级作用域的名称为 DHCPSERVER，为用户分配网关、DNS 服务器及域名；此后将 DHCP 服务管理器有关超级作用域内容展开并截图存储为 dhcp.jpg；

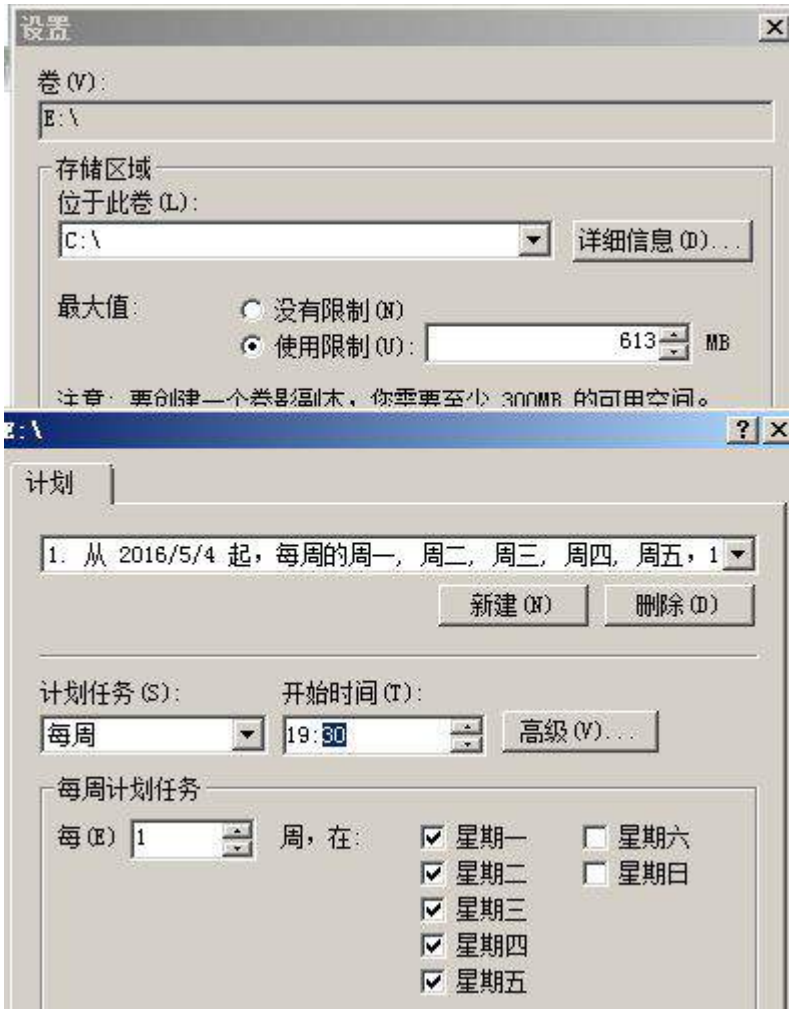
二、在 Server 2 上完成如下操作：

（一）完成虚拟主机的创建

1、安装虚拟机“Win2008-B1”，其内存为 1G，硬盘 20G，并将服务器加入到 Windows 域环境；

2、在虚拟机“Win2008-B1”中添加 SCSI 控制器，添加 3 块 SCSI 虚拟硬盘，其每块硬盘的大小为 2G。将三块硬盘配置为 RAID0，对应磁盘盘符为 e:\；同时需要在 e:\启用卷影副本功能，设置每周工作日的下午 19:30 创建卷影副本，将副本存储于 c:\；

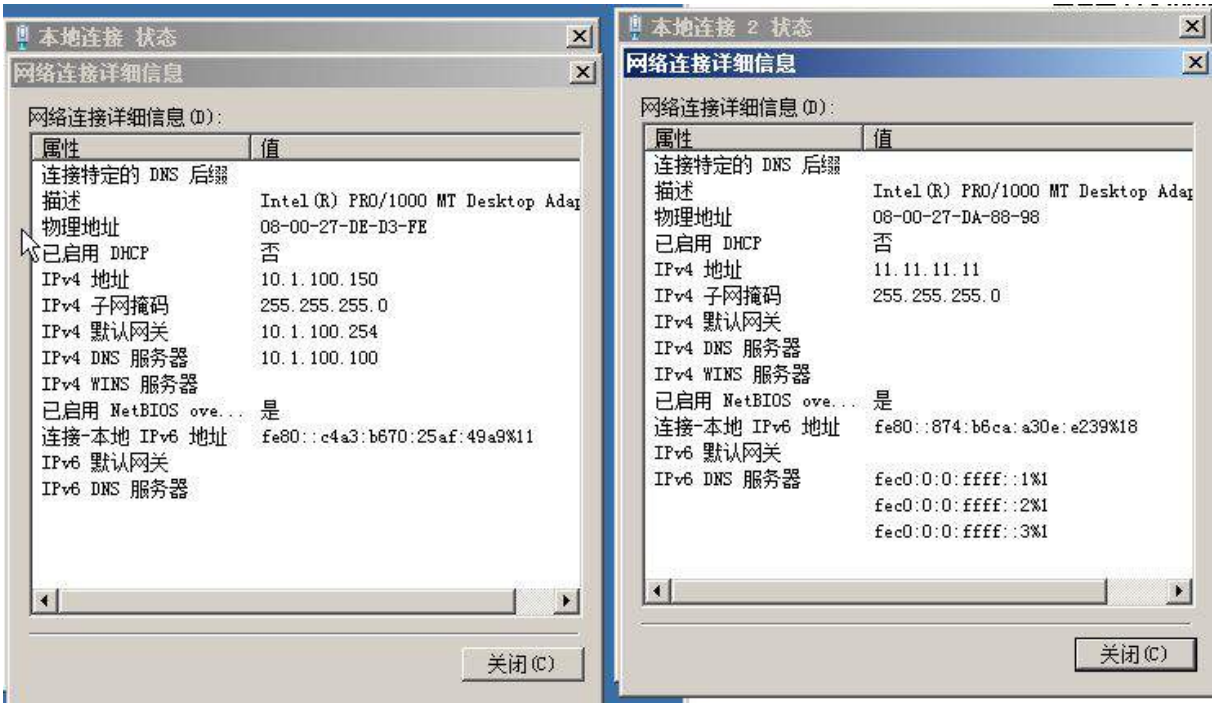

帮助(H)
磁盘管理
卷列表 + 图形视图
操作
磁盘管理
更多操作
卷 布局 类型 文件系统 状态 容量 可用空间 % 可
(C:) 简单 基本 NTFS 状态良好 (启动, 页面文件, 故障转储, 主分区) 19.90 GB 12.13 GB 61
GRMSXFRER_CN_DVD (D:) 简单 基本 UDF 状态良好 (主分区) 3.14 GB 0 MB 0 %
系统保留 简单 基本 NTFS 状态良好 (系统, 活动, 主分区) 100 MB 72 MB 72
新加卷 (E:) 带区 动态 NTFS 状态良好 5.99 GB 5.93 GB 99
磁盘 0
基本
20.00 GB
联机
系统保留
100 MB NTFS
状态良好 (系统, 活动, 主分
(C:)
19.90 GB NTFS
状态良好 (启动, 页面文件, 故障转储, 主分区)
磁盘 1
动态
2.00 GB
联机
新加卷 (E:)
2.00 GB NTFS
状态良好
磁盘 2
动态
2.00 GB
联机
新加卷 (E:)
2.00 GB NTFS
状态良好
磁盘 3
动态
2.00 GB
联机
新加卷 (E:)
2.00 GB NTFS
状态良好



3、安装虚拟机“Win2008-B2”， 其内存为 512M，硬盘 20G，将服务器加入至 Windows 域 中 ；

（二）在主机 Win2008-B1 中完成 WEB 服务器 1 的部署

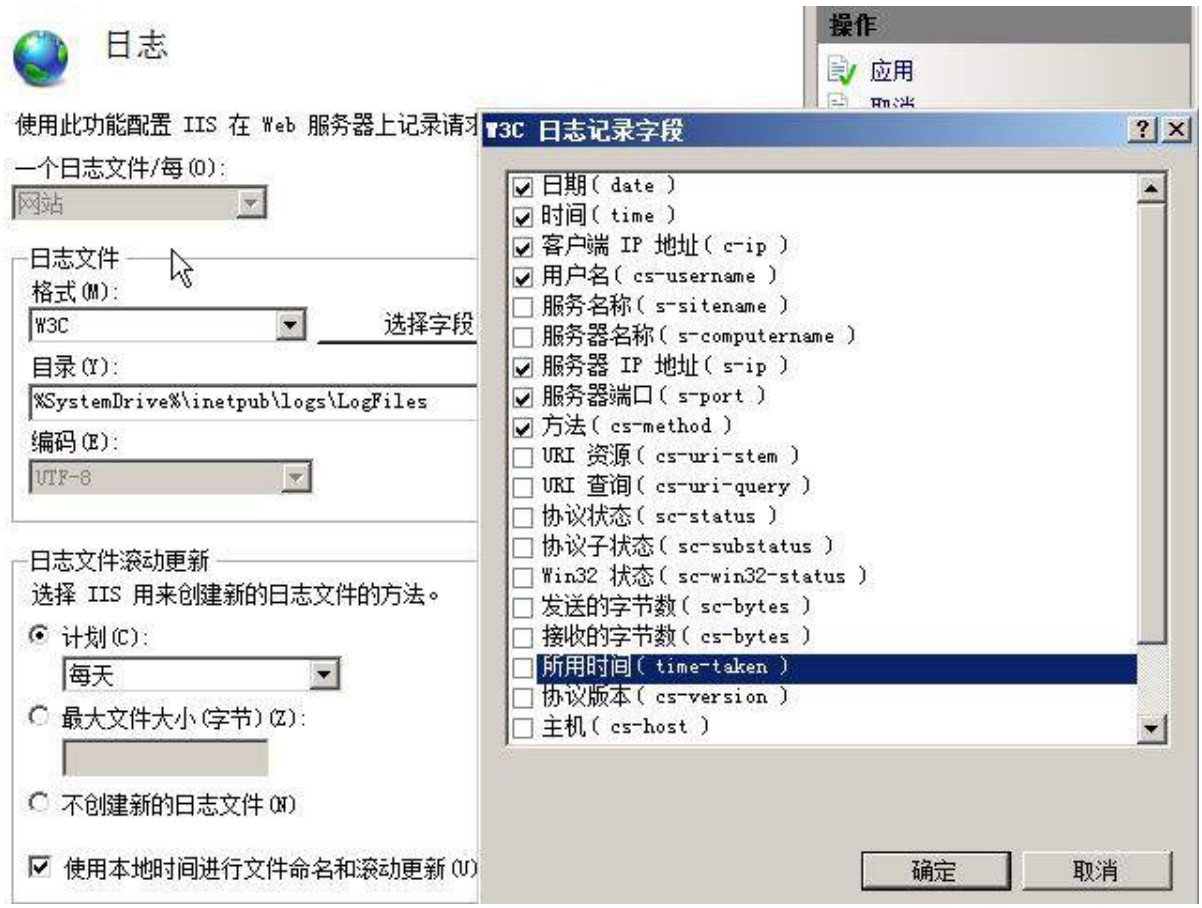
1、在 VirtualBox 中配置安装两块网卡，一块网卡提供网络服务，其 IPv4 地址为 10.1.100.150/24,另一块网卡为心跳线网卡，其 IPv4 地址为 11.11.11.11；



2、安装 IIS 组件，创建 www.chinaskills.com 站点，在挂载的磁盘 e:\下创建名称为 www 的目录，在 www 文件夹中创建名称为 chinaskills.html 的主页，其主页显示内容“热烈庆祝 2015 年全国职业技能竞赛开幕”，同时只允许使用 SSL 且只能通过域名方

式进行访问；

3、设置网站的最大连接数为 1000，网站连接超时为 60s，网站的带宽为 1000KB/S，使用 W3C 记录日志；禁用父路径；每天创建一个新的日志文件，使用当地时间作为日志文件名；日志只允许记录日期、时间、客户端 IP 地址、用户名、服务器 IP 地址、服务器端口号和方法；



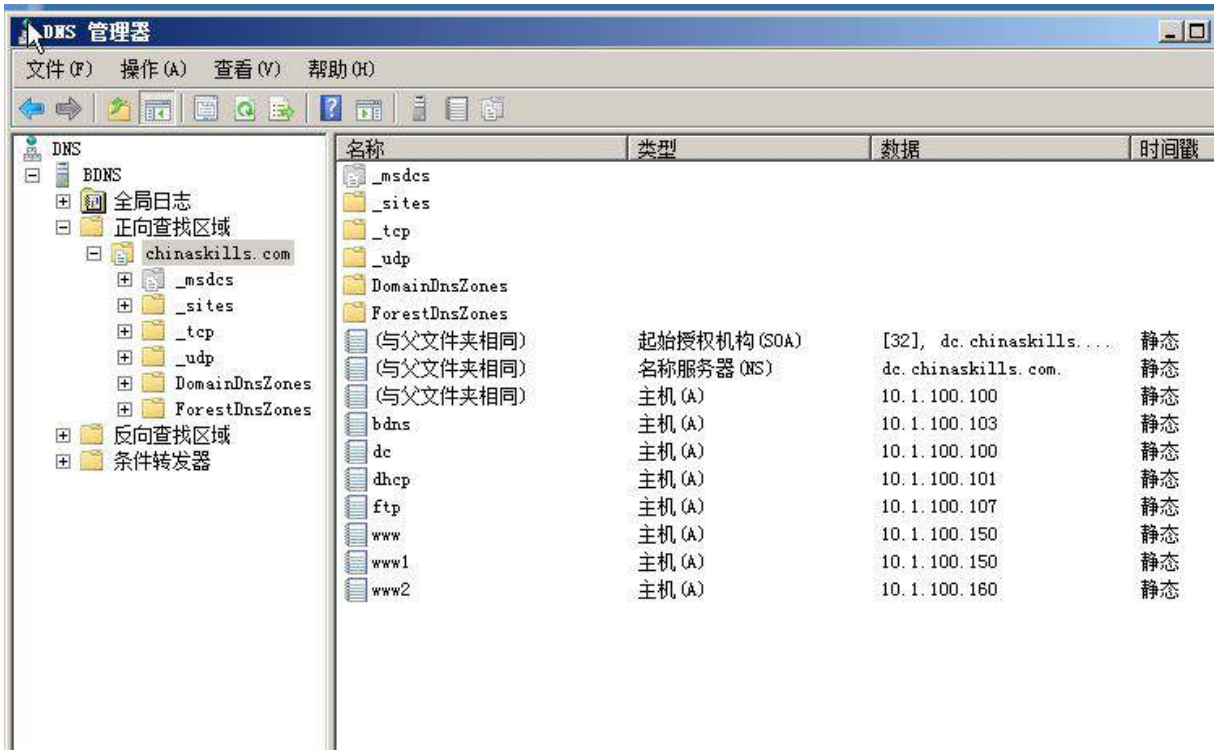
4、安装 NLB 负载平衡服务，其群集 IPv4 地址为 10.1.100.180/24，新建群集优先级为 2，群集名称为 www. chinaskills.com，采用多播方式；

5、配置 DFS 服务，实现两个服务器的网站主页内容保持同步，空间名称为 WEB，文件夹为 WWW，复制组为 www-backup,拓扑采用交错方式，设置复制在周六和周日带宽为完整，周一至周五带宽为 64M；

（三）在主机 Win2008-B2 中完成备份 DNS 的部署

1、配置此服务器为备份 DNS，其合法域名为 bdns. Chianskills.com

2、将服务器加入到 windows 域中，将所有的主 DNS 的区域都复制到备份 DNS 服务器 上



三、在 Server 3 上完成如下操作：

（一）完成虚拟主机的创建

1、安装虚拟机“Win2008-C1”，其内存为 1G，硬盘 20G，并将服务器加入到 Windows 域环境；

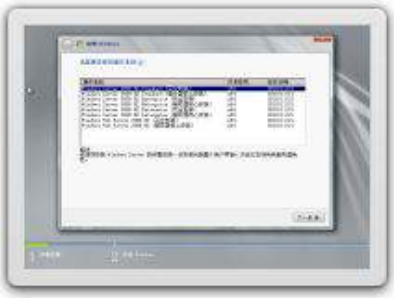
常规

名称: Win2008-C1
操作系统: Windows 2008 (64 bit)

系统

内存大小: 1024 MB
启动顺序: 软驱, 光驱, 硬盘
硬件加速: VT-x/AMD-V, 嵌套分页

预览



显示

显存大小: 27 MB
远程桌面服务器: 已禁用
录像: 已禁用

存储

控制器: IDE
第二IDE控制器主通道: [光驱] cn_windows_server_2008_r2_standard_enterprise_datacenter_and_web_with_sp1_x64_dvd_617598.iso (3.14 GB)
控制器: SATA
SATA 端口 0: Win2008-C1.vdi (普通, 20.00 GB)

声音

主机音频驱动: Windows DirectSound
控制芯片: Intel HD 音频

网络

网卡 1: Intel PRO/1000 MT 桌面 (桥接网络, Intel(R) Ethernet Connection I217-LM)

查看有关计算机的基本信息

Windows 版本

Windows Server 2008 R2 Standard
版权所有 © 2009 Microsoft Corporation。保留所有权利。
Service Pack 1

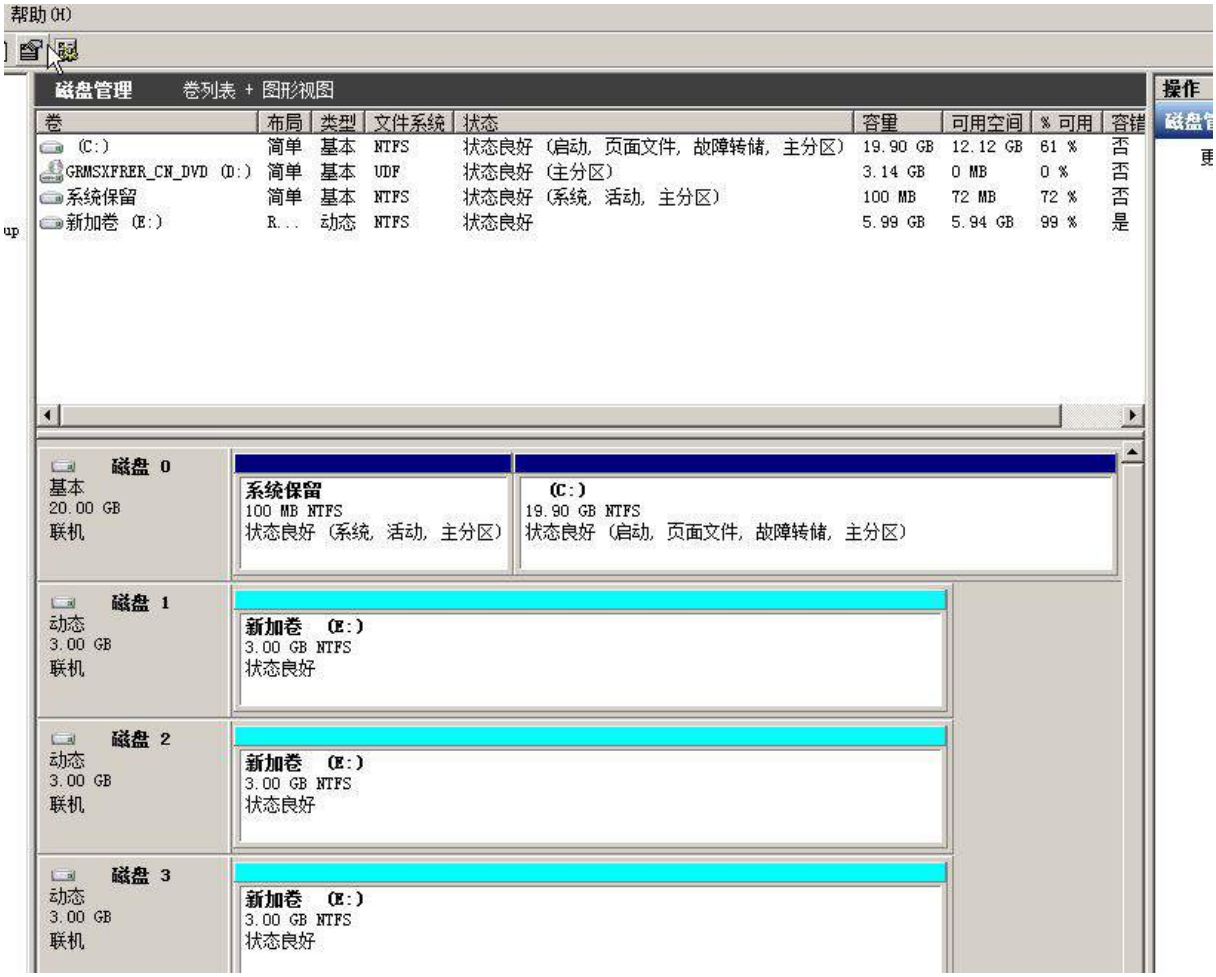
系统

处理器: Intel(R) Xeon(R) CPU E5-1620 v3 @ 3.50GHz 3.49 GHz
安装内存(RAM): 1.00 GB
系统类型: 64 位操作系统
笔和触摸: 没有可用于此显示器的笔或触控输入

计算机名称、域和工作组设置

计算机名: www2 更改设置
计算机全名: www2.chinaskills.com
计算机描述:
域: chinaskills.com

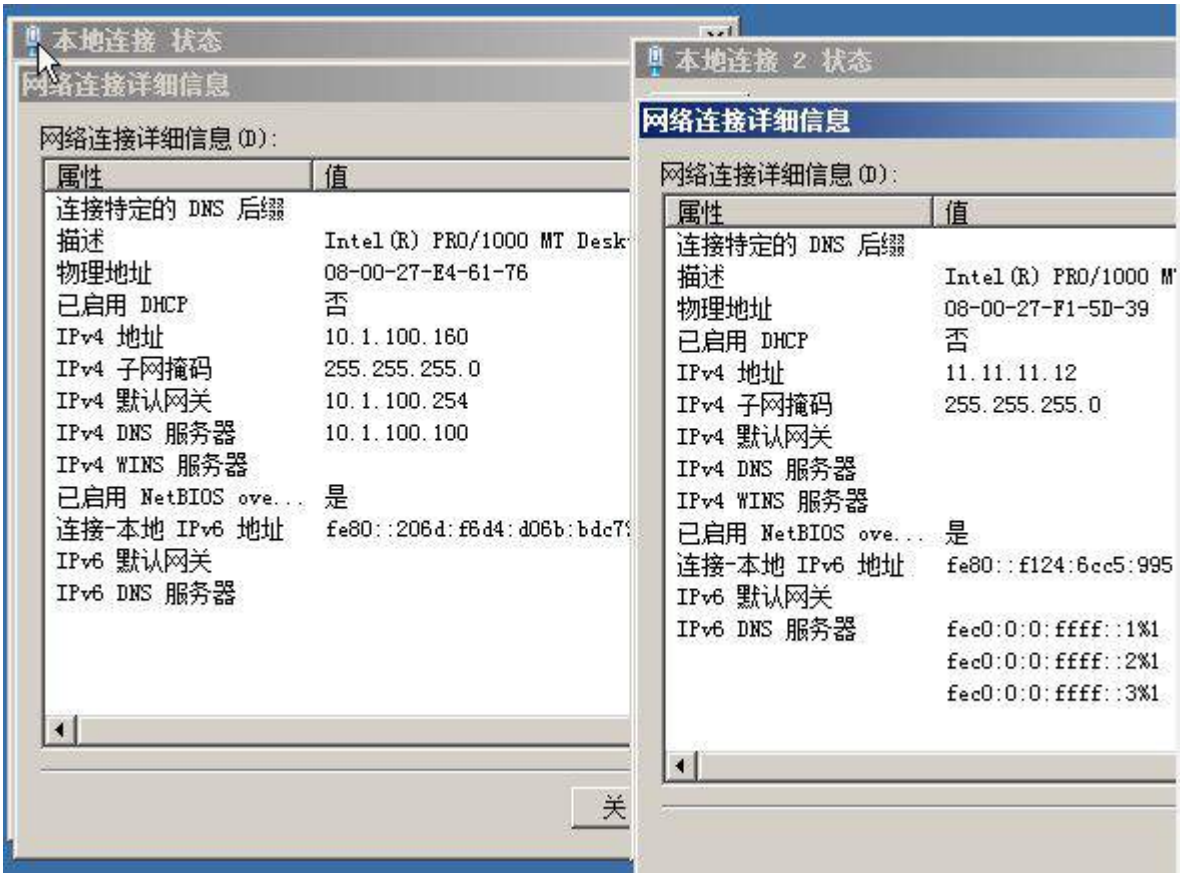
2、在虚拟机“Win2008-C1”中添加 SCSI 控制器，添加 3 块 SCSI 虚拟硬盘，其每块硬盘的大小为 3G，将三块硬盘配置为 RAID5，对应磁盘盘符为 e:\；



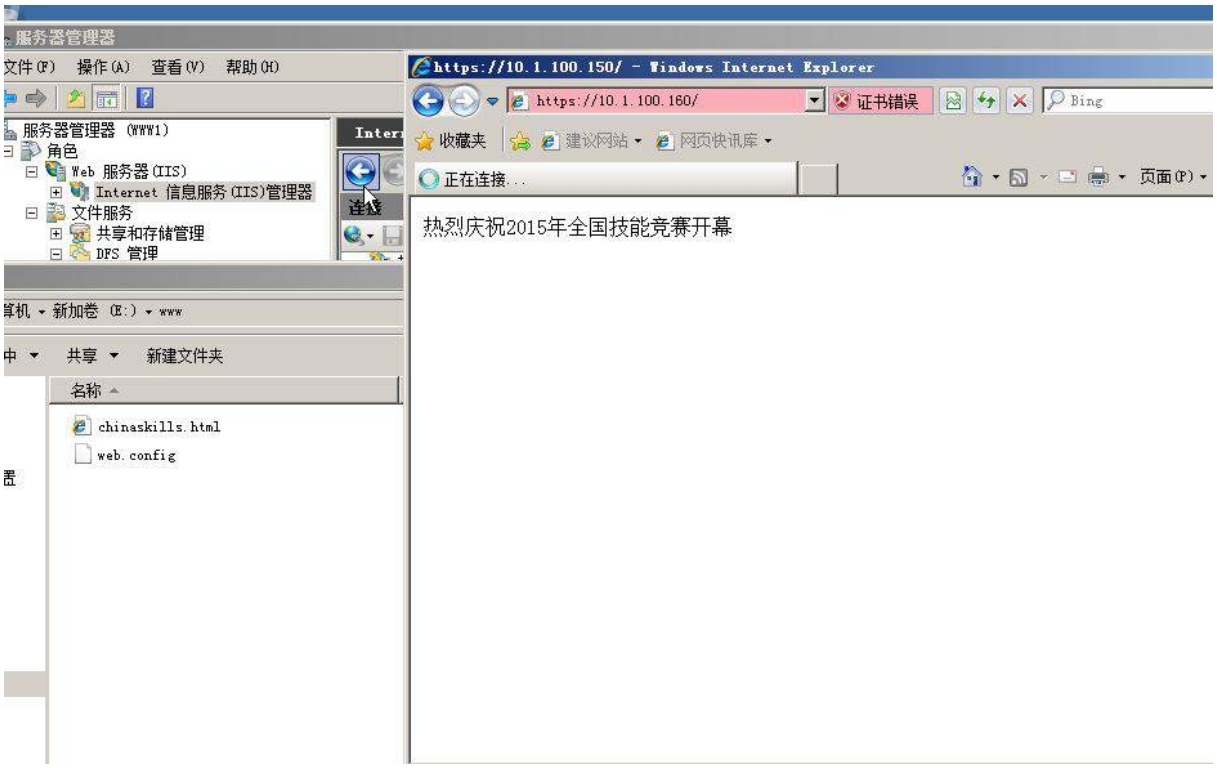
3、在虚拟机“Win2008-C2”其内存为 1G，硬盘 20G，并将服务器加入到 Windows 域环境；

（二）在主机 Win2008-C1 中完成 WEB 服务器 2 的部署

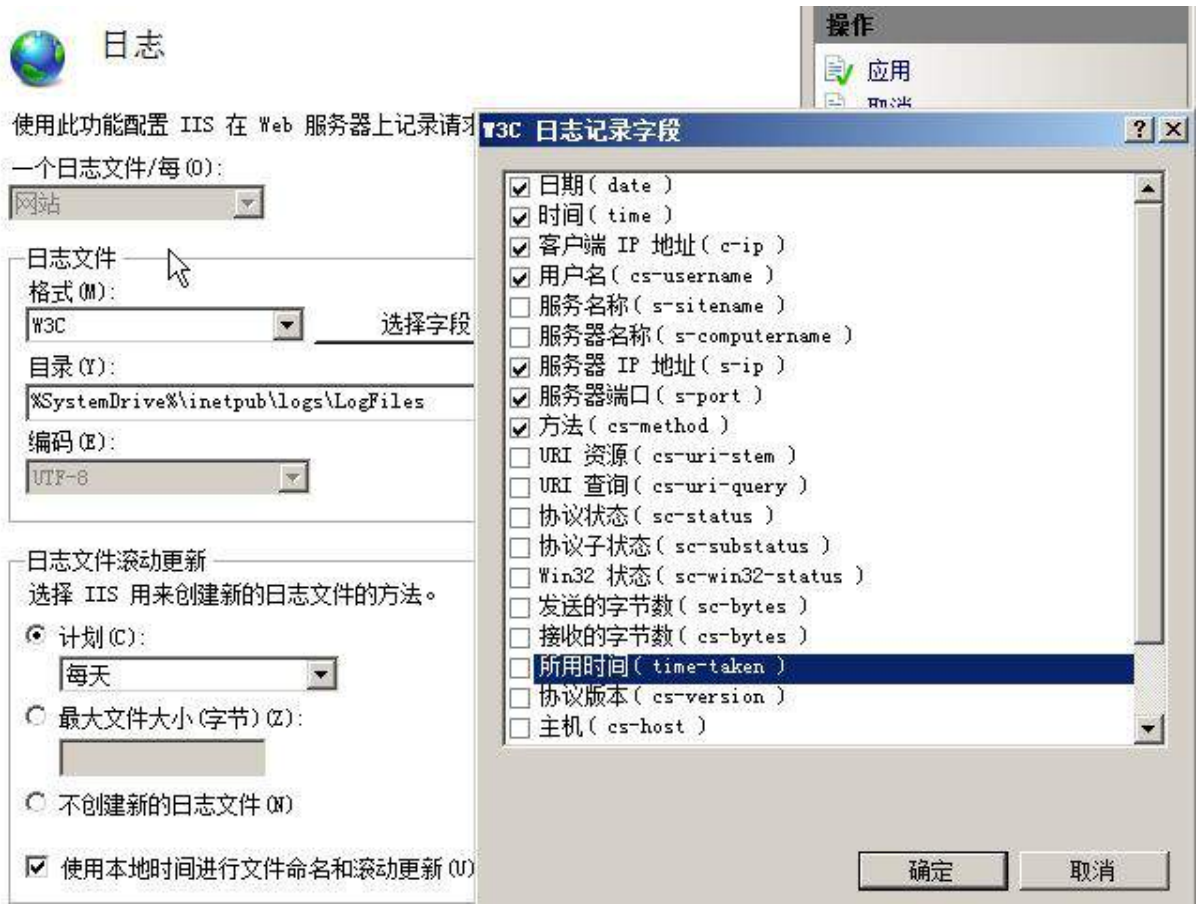
1、在 VirtualBox 上添加安装两块网卡，一块网卡提供网络服务，其 IPv4 地址为 10.1.100.160/24,，另一块网卡为心跳线网卡，其 IPv4 地址为 11.11.11.12；（15 分）



2、安装 IIS 组件，创建 www.chinaskills.com 站点，在挂载的磁盘 e:\下创建名称为 www 的文件，在 www 文件中创建名称为 chinaskills.html 的主页，主页显示内容“热烈庆祝 2015 年全国职业技能竞赛开幕”，同时只允许使用 SSL 且只能采用域名方式进行访问；



3、设置网站的最大连接数为 1000,网站连接超时为 60s,网站的带宽为 1000KB/S,使用 W3C 记录日志；每天创建一个新的日志文件，使用当地时间作为日志文件名；日志只允许记录日期、时间、客户端 IP 地址、用户名、服务器 IP 地址、服务器端口号和方法；



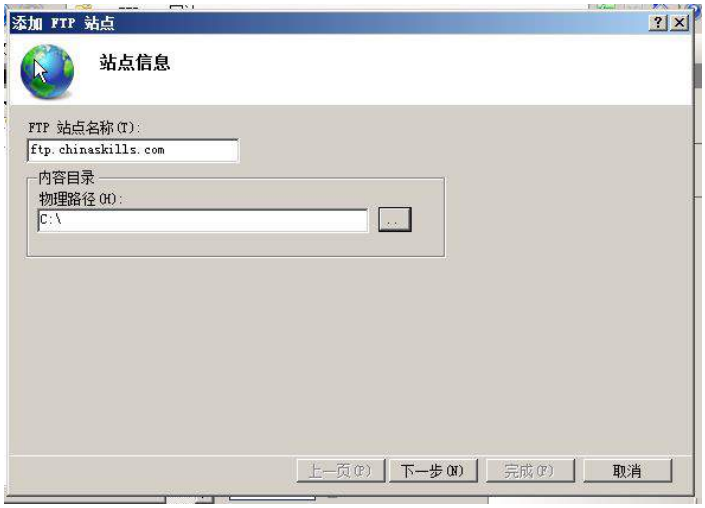
4、安装 NLB 负载平衡服务，其群集 IPv4 地址为 10.1.100.180/24，完整的 Internet 名称为 www.chinaskills.com，采用多播方式；

5、配置 DFS 服务，实现两个服务器的网站主页内容保持同步，空间名称为 WEB，文件夹为 WWW，复制组为 www-backup,拓扑采用交错方式，设置复制在周六和周日带宽为

完整，周一至周五带宽为 64M；在本机网卡的“本地连接 状体”选项框中点击“详细信息”并将此选项框截图存储为 nlb.jpg；

（三）在主机 Win2008-C2 中完成 FTP 服务器以及域控服务器角色迁移的部署

1、安装 IIS 组件的 FTP 组件，创建 FTP 站点，ftp.chinaskills.com 站点只允许软件部的用户都可以上传文件和下载文件，而其它及匿名用户只能下载文件，但不能上传文件，限制用户上传最大空间为 100M，超过 80M 预警，预警采用电子邮件和记录事务日志；



2、建立备份域控服务器，将主域控服务器操作主机角色、全局编录角色迁移至备份域控服务器上；

Linux 操作系统部分

【说 明】

1、所有 Linux 操作系统的 root 用户的密码为 123456，若未按要求设置密码，涉及到该操作系统下的所有分值记为 0 分。

2、虚拟主机的 IP 属性设置请按照网络拓扑结构图以及“表 3：服务器 IP 地址分配表”的要求设定。

3、除有特别规定外，其他未明确规定用户密码均与用户名相同。

4、所有操作系统镜像文件及试题所需的其他软件均存放于每台计算机的/根目录下。

5、题目要求的虚拟机均安装于每台主机的 D：\virtualPC 目录，即路径为 D：

\virtualPC\虚拟主机名称。

一、在 Server 1 上完成如下操作：

（一）完成虚拟主机的创建

1、安装虚拟机“Centos-A1”，具体要求为内存 512MB，硬盘 10GB；

（二）在主机 Centos-A1 中完成 iSCSI 服务器的部署

1、关闭虚拟机的前提下在“Centos-A1”中手动再添加两块硬盘（SCSI），容量均为 5G，分别将两块硬盘设置为一个主分区（2G 容量）和两个逻辑分区（分别 1G 容量），并完成 PV 物理卷的初始化操作；


```
Command (m for help): p

Disk /dev/sdb: 5368 MB, 5368709120 bytes
255 heads, 63 sectors/track, 652 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0xadbf7456

   Device Boot      Start         End      Blocks   Id  System
/dev/sdb1               1         262     2104483+  8e  Linux LVM
/dev/sdb2             263         524     2104515    5  Extended
/dev/sdb5             263         394     1060258+  8e  Linux LVM
/dev/sdb6             395         524     1044193+  8e  Linux LVM
```

```
Command (m for help): p

Disk /dev/sdc: 5368 MB, 5368709120 bytes
255 heads, 63 sectors/track, 652 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0xe31cd6b6

   Device Boot      Start         End      Blocks   Id  System
/dev/sdc1               1         262     2104483+  8e  Linux LVM
/dev/sdc2             263         524     2104515    5  Extended
/dev/sdc5             263         394     1060258+  8e  Linux LVM
/dev/sdc6             395         524     1044193+  8e  Linux LVM
```

```
[root@localhost ~]# pvcreate /dev/sdb1 /dev/sdb5 /dev/sdb6 /dev/sdc1 /dev/sdc5 /
dev/sdc6
  Physical volume "/dev/sdb1" successfully created
  Physical volume "/dev/sdb5" successfully created
  Physical volume "/dev/sdb6" successfully created
  Physical volume "/dev/sdc1" successfully created
  Physical volume "/dev/sdc5" successfully created
  Physical volume "/dev/sdc6" successfully created
```

2、将/dev/sdb1 及/dev/sdc2 加入到卷组 VG1 中，其显示的逻辑卷名称为 LV1，格式化为 ext3 文件系统，对应挂载目录为/volume；

```
[root@localhost ~]# vgcreate VG1 /dev/sdb1 /dev/sdc5
  Volume group "VG1" successfully created
[root@localhost ~]# lvcreate -L +3G -n LV1 VG1
  Logical volume "LV1" created
[root@localhost ~]# mkfs -t ext3 /dev/VG1/LV1
[root@localhost ~]# mkdir /volume
[root@localhost ~]# mount /dev/VG1/LV1 /volume/
```

3、将Centos-A1主机作为target服务器端进行设置，创建target设备，targetID为10，名称为iqn.2015-06.com.jnds:test，并绑定target端IP地址；

二、在 Server 2 上完成如下操作：

（一）完成虚拟主机的创建

1、安装虚拟机“Centos-B1”,具体要求为内存 512MB，硬盘 10GB；

（二）在主机 Centos-B1 中完成 iSCSI 客户端的部署

1、借助 YUM 源安装 iSCSI 客户端程序包，编辑 iSCSI 客户端配置文档将节点开启方式改为手动（manual）模式，之后启动 iSCSI 客户端进程以便发现 target 服务端；

2、将连接到的 target 端硬盘空间做磁盘初始化处理，要求建立 LVM 逻辑卷，卷组名称为 VG1，对应逻辑卷名称为 LV1，对应目录为/volume；

3、目录/volume 实现开机远程挂载；

（三）在主机 Centos-B1 中完成 FTP 服务器的部署

1、配置多站点 FTP 服务，创设三个 FTP 服务站点，域名分别为 ftp.jnds.net、ftp1.jnds.net 以及 ftp2.jnds.net，除站点 ftp.jnds.net 采用默认配置外，其余站点配置文件名分别为 vsftpd1.conf 以及 vsftpd2.conf，站点主目录分别为 /var/ftp1 以及/var/ftp2；

```
listen_address=10.1.100.105
local_root=/var/ftp1_
```

```
listen_address=10.1.100.106
local_root=/var/ftp2_
```

2、在站点 vsftpd 中，建立用户 ftpuser1 及 ftpuser2，使得两个用户登录后的主目录是各自家目录，并将两用户限制在监牢（chroot）中

```
[root@localhost vsftpd]# useradd ftpuser1
^[[A[root@localhost vsftpd]# useradd ftpuser2
```

```
chroot_local_user=YES
```

3、在站点 vsftpd1 中，建立本地用户 ftpuser3 及 ftpuser4，两个用户共用同一个主目录，并在主目录中具备上传及下载权限。

```
[root@localhost vuser]# useradd ftpuser3
[root@localhost vuser]# useradd ftpuser4
```

```
listen_address=10.1.100.105
local_root=/var/ftp1
write_enable=YES_
```

4、借助自签名证书完成 ftps 服务的配置，结合 ssl 实现安全传输，服务证书名为 vsftpd.pem，服务私钥名为 ftpssl.pem，证书有效期为 100 天；

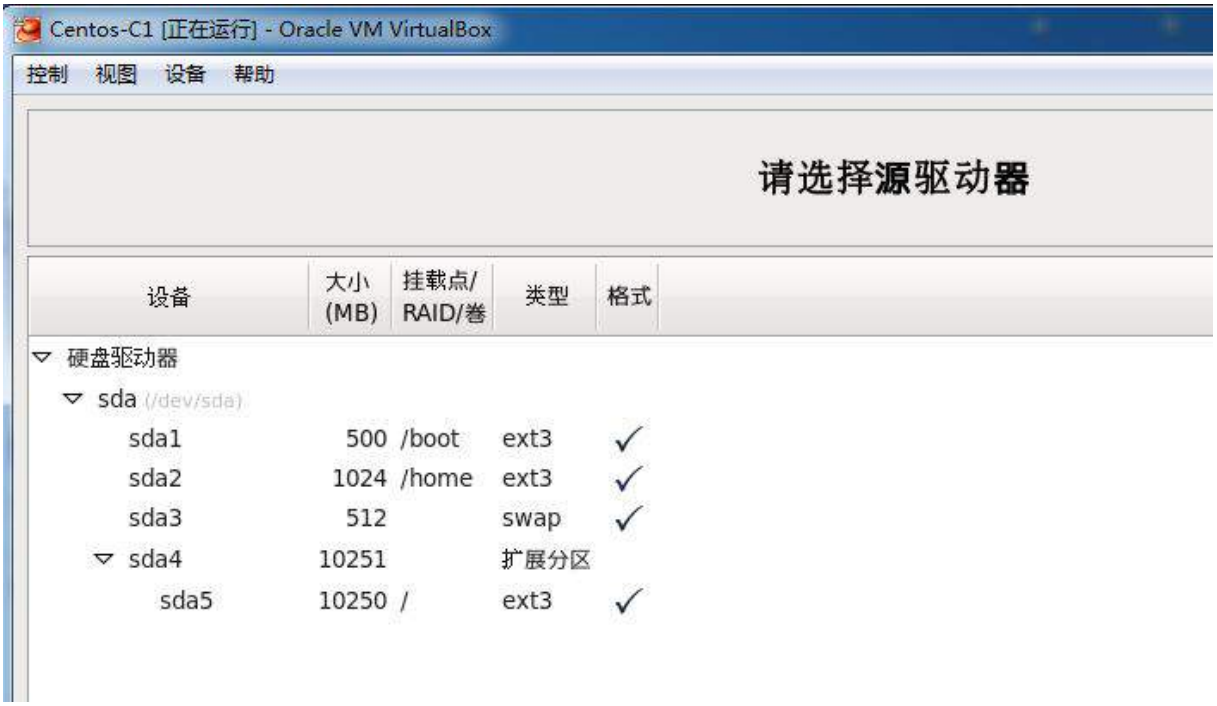
```
[root@localhost tls]# openssl genrsa -out ftpssl.pem 1024
Generating RSA private key, 1024 bit long modulus
...++++++
.........++++++
e is 65537 (0x10001)
```

```
[root@localhost tls]# openssl x509 -days 100 -req -in ftpssl.csr -signkey ftpssl
.pem -out vsftpd.pem
Signature ok
subject=/C=XX/L=Default City/O=Default Company Ltd
Getting Private key
```

三、在 Server 3 上完成如下操作：

（一）完成虚拟主机的创建

1、安装名为“Centos-C1”的虚拟机，具体要求为硬盘大小为 12GB，内存为 768MB，系统为 Centos6.5。分区大小为：SWAP 分区大小为 512M；/boot 分区大小为 500M，文件类型为 ext3；/home 分区大小为 1G，文件类型为 ext3，其余为/分区，文件类型为 ext3；（小提示：如无法正确安装虚拟机 Centos-D1，下述题目中所涉及的虚拟机题目可在 Server4 真实主机中完成）



（二）在主机 Centos-C1 中完成 BIND 域名服务器以及代理服务器的部署

1、在此服务器中安装配置 bind 服务，负责区域“jnds.net”内主机解析，五台主机分别为 dns.jnds.net 、www.jnds.net、bbs.jnds.net、pxe.jnds.net、ftp.jnds.net、ftp1.jnds.net、ftp2.jnds.net ，做好正反向 DNS 服务解析，对访问 chinaskills.com 域的解析转发给 win2003_A1；

```
$TTL 3H
@       IN SOA  ns.jnds.net.     root.jnds.net. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
@       IN      NS      ns.jnds.net.
108     IN      PTR     dns.jnds.net.
109     IN      PTR     www.jnds.net.
109     IN      PTR     bbs.jnds.net.
104     IN      PTR     ftp.jnds.net.
105     IN      PTR     ftp1.jnds.net.
106     IN      PTR     ftp2.jnds.net.
~
~
~
```

```
$TTL 1D
@       IN SOA  ns.jnds.net.     root.jnds.net. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
ns      IN      A       10.1.100.108
@       IN      NS      ns.jnds.net.
dns     IN      A       10.1.100.108
www     IN      A       10.1.100.109
bbs     IN      A       10.1.100.109
ftp     IN      A       10.1.100.104
ftp1    IN      A       10.1.100.105
ftp2    IN      A       10.1.100.106
~
```

```
    options {
            listen-on port 53 { any; };
            listen-on-v6 port 53 { any; };
            directory       "/var/named";
            dump-file       "/var/named/data/cache_dump.db";
            statistics-file "/var/named/data/named_stats.txt";
            memstatistics-file "/var/named/data/named_mem_stats.txt";
            allow-query     { any; };
            recursion yes;
            forwarde only;
            forwarders{10.1.100.100; };
```

2、安装并完成代理服务器 squid 的初始配置，使用 8080 作为代理服务端口，指定 DNS 服务器 IP 地址信息，使得 squid 服务器能够解析域名；

```
http_port 8080
dns_nameservers 10.1.100.108
```

3、设置 squid 代理服务器采用 ufs 缓存机制，缓存目录设置为/cache,目录容量为 5GB，L1 及 L2 级目录数量分别为 16 及 256，定义高速缓存值为 512MB；

```
cache_dir ufs /cache 5120 16 256
cache_mem 512 MB
```

4、针对主机 10.1.100.109/24 提供代理服务，为缓解请求队列忙碌，设置重定向器池进程数为 20，并将缓存日志存放于/var/squid/cache.log 中；

```
visible_hostname 10.1.100.109/24
redirect_children 20
cache_log /var/squid/cache.log
```

四、在 Server 4 上完成如下操作：

（一）完成虚拟主机的创建

1、Server4 主机系统为 CentOS6.5，需要在此 Linux 平台上采用 KVM 方式安装虚拟机“Centos-D1”，具体要求为硬盘大小为 12GB，内存为 768MB，系统为 CentOs6.5；

（二）在主机 Centos-D1 中完成 Apache 服务器以及 MySQL 数据库服务器的部署

1、在此服务器中安装 httpd 服务，建立站点 www.jnds.net，其网站主目录为/var/www/html，首页内容为“chinaskills’s website” ；

```
ServerName www.jnds.net:80

#
# UseCanonicalName: Determines how Apache constructs
# URLs and the SERVER_NAME and SERVER_PORT variables.
# When set "Off", Apache will use the Hostname and Po
# by the client. When set "On", Apache will use the
# ServerName directive.
#
UseCanonicalName Off

#
# DocumentRoot: The directory out of which you will s
# documents. By default, all requests are taken from
# symbolic links and aliases may be used to point to
#
DocumentRoot "/var/www/html"
```

2、使用 openssl 申请证书，创建自签名证书 server.crt 和私钥 server.key，要求只允许使用域名通过 SSL 加密访问；

```
[root@localhost tls]# openssl x509 -days 365 -req -in server.csr -signkey server
.key -out server.csr
Signature ok
subject=/C=XX/L=Default City/O=Default Company Ltd
Getting Private key
```

```
[root@localhost tls]# openssl genrsa -out server.key 1024
Generating RSA private key, 1024 bit long modulus
.................++++++
.............++++++
e is 65537 (0x10001)
[root@localhost tls]# openssl req -new -key server.key -out server.csr
```

3、将此服务器配置为 MYSQL 服务器，创建数据库为 userdatabase，在库中创建表为 username，在表中创建 5 个用户，分别为 myuser1、myuser2、myuser3、myuser4、myuser5，口令与用户名相同，需要对登录网站的用户进行身份验证，表结构如下；

字段名	数据类型	主键	自增
ID	int	是	是
name	varchar(10)	否	否
birthday	datetime	否	否
sex	char(1)	否	否
Password	Char（8）	否	否

```
mysql> create database userdatabase;
Query OK, 1 row affected (0.00 sec)
```

```
mysql> create table username( ID int primary key auto_increment, name varchar(10
), birthday datetime, sex char(1), Password char(8));
Query OK, 0 rows affected (0.02 sec)

mysql> desc username;
+----------+-------------+------+-----+---------+----------------+
| Field    | Type        | Null | Key | Default | Extra          |
+----------+-------------+------+-----+---------+----------------+
| ID       | int(11)     | NO   | PRI | NULL    | auto_increment |
| name     | varchar(10) | YES  |     | NULL    |                |
| birthday | datetime    | YES  |     | NULL    |                |
| sex      | char(1)     | YES  |     | NULL    |                |
| Password | char(8)     | YES  |     | NULL    |                |
+----------+-------------+------+-----+---------+----------------+
5 rows in set (0.00 sec)
```

```
mysql> insert into username(name,Password)value("myuser1","myuser1");
Query OK, 1 row affected (0.00 sec)

mysql> insert into username(name,Password)value("myuser2","myuser2");
Query OK, 1 row affected (0.00 sec)

mysql> insert into username(name,Password)value("myuser3","myuser3");
Query OK, 1 row affected (0.00 sec)

mysql> insert into username(name,Password)value("myuser4","myuser4");
Query OK, 1 row affected (0.00 sec)

mysql> select * from username;
+----+---------+----------+------+----------+
| ID | name    | birthday | sex  | Password |
+----+---------+----------+------+----------+
|  1 | myuser1 | NULL     | NULL | myuser1  |
|  2 | myuser2 | NULL     | NULL | myuser2  |
|  3 | myuser3 | NULL     | NULL | myuser3  |
|  4 | myuser4 | NULL     | NULL | myuser4  |
+----+---------+----------+------+----------+
4 rows in set (0.00 sec)
```

4.在服务器端使用 iptables 设置防火墙功能,只允许用户访问这台服务器的 WWW 服务，而服务器只能被动地接受连接请求，不能主动的发起连接；

```
[root@localhost conf]# iptables -P OUTPUT DROP
[root@localhost conf]# iptables -I OUTPUT 1 -p tcp -m state --state=RELATED,ESTA
BLISHED --sport 80 -j ACCEPT
```

2015 年全国职业院校技能大赛
网络搭建与应用竞赛
（总分 1000 分）

赛题说明

一、竞赛内容分布

“网络搭建与应用”竞赛共分二个部分，其中：

第一部分：网络搭建及安全部署项目，占总分的比例为 45%；

第二部分：服务器配置及应用项目，占总分的比例为 55%；

二、竞赛注意事项

（1）禁止携带和使用移动存储设备、计算器、通信工具及参考资料。

（2）请根据大赛所提供的比赛环境，检查所列的硬件设备、软件清单、材料清单是否齐全，计算机设备是否能正常使用。

（3）本试卷共有两个部分。请选手仔细阅读比赛试卷，按照试卷要求完成各项操作。

（4）操作过程中，需要及时保存设备配置。比赛结束后，所有设备保持运行状态，不要拆、动硬件连接。

（5）比赛完成后，比赛设备、软件和赛题请保留在座位上，禁止将比赛所用的所有物品（包括试卷和草纸）带离赛场。

（6）所有需要提交的文档均放置在桌面的 PC1 “比赛文档”文件夹中，禁止在纸质资料上填写与竞赛无关的标记，如违反规定，可视为 0 分。

（7）裁判以各参赛队提交的竞赛结果文档为主要评分依据。所有提交的文档必须按照赛题所规定的命名规则命名，文档中有对应题目的小标题，截图有截图的简要说明，否则按无效内容处理。

（8）与比赛相关的工具软件放置在 D 盘的 tools 文件夹中。

项目背景及网络拓扑

某天津集团公司在天津设置有总公司，总公司使用 ospf 技术,在上海设置分公司，分公司使用 RIPv1 技术，两地公司的网络一直未统一管理，现总公司提出网络整合。所以对网络进行改造。

改造主要的工作是租用 ISP 的专线链路，解决两地互联问题。网络管理员使用路由重发布技术进行两地互通。然后通过 Internet 采用基于 IPSEC-VPN 技术作为备份链路。以实现业务流量的高可用性。集团网络具体拓扑结构如图 1 所示。

总公司有四个部门，分别为财务部、工程部、软件部和系统集成部四个部门，上海分公司设有行政部和销售部。

请你帮助公司网络管理员进行网络调试与改造，完成相关任务。

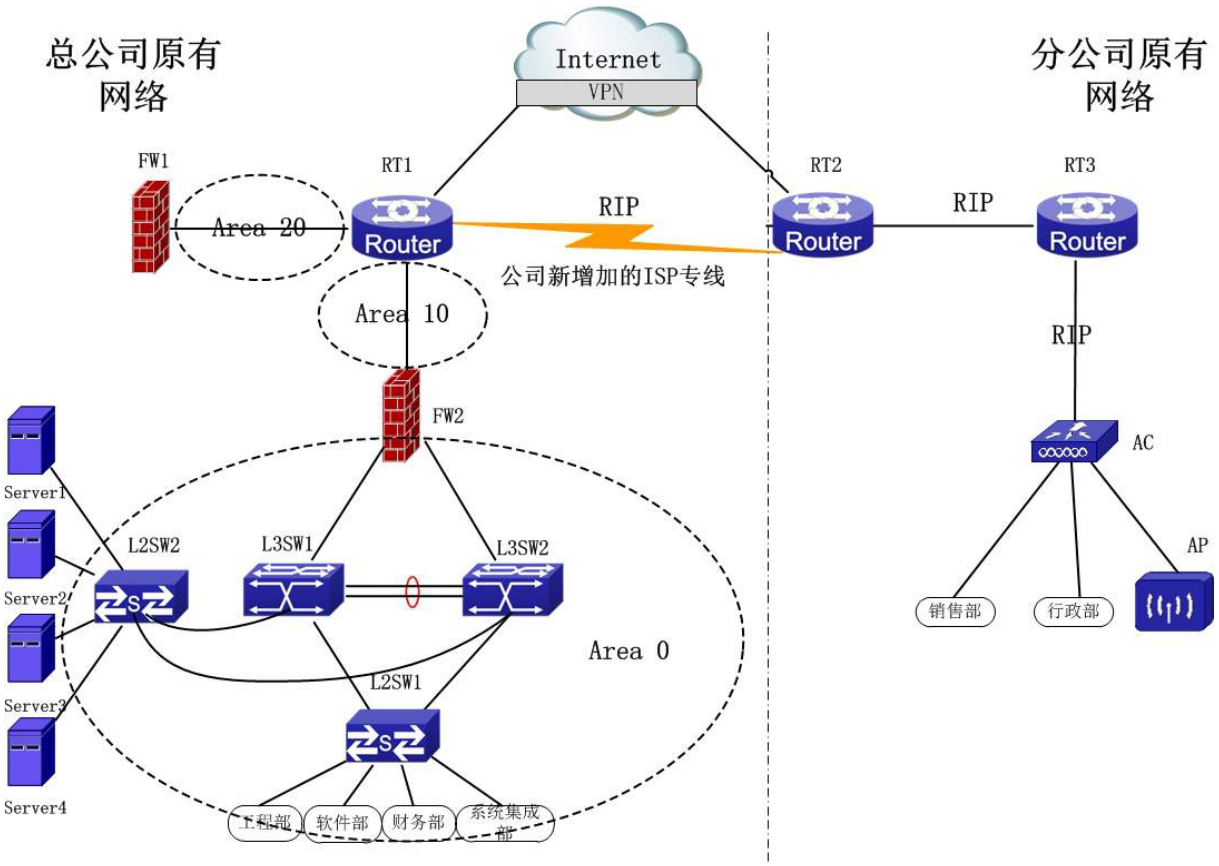


表 1 网络设备连接表

设备一	设备一端口	设备一地址	设备二	设备二端口	设备二地址
RT1	Serial0/1		RT2	Serial0/2	
RT1	GE0/4		FW1	Ethernet0/3	
RT1	GE0/3		FW2	Ethernet0/2	
RT1	GE0/6	123.1.12.1/24	RT2	GE0/6	123.1.12.2/24

RT2	GE0/3		RT3	GE0/3	
RT3	GE0/4		AC	Ethernet1/0/24（vlan100）	----------
RT3	Loopback 1	10.100.204.1/24	----------	----------	----------
AC	Ethernet1/0/7（vlan100）	----------	AP	LAN	----------
FW1	Loopback 1	10.100.104.1/24	----------	----------	----------
FW2	Ethernet0/3		L3SW1	Ethernet1/0/22 (vlan100)	
FW2	Ethernet0/4		L3SW2	Ethernet1/0/22 (vlan200)	
L3SW1	Ethernet1/0/23	----------	L3SW2	Ethernet1/0/23	----------
L3SW1	Ethernet1/0/24	----------	L3SW2	Ethernet1/0/24	----------
L3SW1	Ethernet1/0/21	----------	L2SW1	Ethernet1/23	----------
L3SW1	Ethernet1/0/20	----------	L2SW2	Ethernet1/23	----------
L3SW2	Ethernet1/0/20	----------	L2SW2	Ethernet1/24	----------
L3SW2	Ethernet1/0/21	----------	L2SW1	Ethernet1/24	----------
L2SW2	Ethernet1/1	----------	ServerA	NIC	----------
L2SW2	Ethernet1/2	----------	ServerB	NIC	----------
L2SW2	Ethernet1/3	----------	ServerC	NIC	----------
L2SW2	Ethernet1/4	----------	ServerD	NIC	----------

表 2 网络设备 IP 地址分配表

	网关地址及掩码
VLAN10 SVI(财务部)	
VLAN20 SVI(软件部)	
VLAN30 SVI (系统集成部)	
VLAN40 SVI(工程部)	
VLAN50 SVI(服务器)	10.100.100.254/24

表 3：服务器 IP 地址分配表

宿主机	虚拟主机名称	域名信息	服务角色	系统及版本信息	IPv4 地址信息
Server1	Win2003-A1	dc.chinaskills.com	域控制器 DNS 服务器 CA 证书服务器	Windows Server 2003 R2	IP: 10.100.100.100
	Win2008-A1	dhcp.chinaskills.com	DHCP 服务器	Windows Server 2008 R2	IP: 10.100.100.101
	Centos-A1	pxe.jnds.net	PXE 远程安装服务器	Centos 6.5	IP: 10.100.100.102
Server2	Win2008-B1	www1.chinaskills.com	WEB 服务器 NLB 集群服务	Windows Server 2008 R2	IP: 10.100.100.150
	Win2008-B2	bdns. chianskills.com	备份 DNS	Windows Server 2008 R2	IP: 10.100.100.103
	Centos-B1	ftp.jnds.net ftp1.jnds.net ftp2.jnds.net	逻辑卷磁盘容量服务 FTP 文件服务器	Centos 6.5	IP: 10.100.100.104 IP: 10.100.100.105 IP: 10.100.100.106
Server3	Win2008-C1	www2.chinaskills.com	WEB 服务器 NLB 集群服务	Windows Server 2008 R2	IP: 10.100.100.160
	Win2008-C2	ftp.chinaskills.com	FTP 服务器 备份域控制器	Windows Server 2008 R2	IP：10.100.100.107
	Centos-C1	dns.jnds.net	BIND 域名服务器 Squid 代理服务器	Centos 6.5	IP: 10.100.100.108
Server4（Linux 虚拟化主机）	Centos-D1	www.jnds.net bbs.jnds.net	Apache web 服务器 MySQL 数据库服务器	Centos 6.5	IP: 10.100.100.109

一、 网络搭建部分（450 分）

【注意事项】

1、设备 console 线有两条。交换机， AC，防火墙使用同一条 console 线，路由器使用另外一条 console 线。

2、设备配置完毕后，保存最新的设备配置。保存文档方式分为两种：

a) 交换机和路由器要把 show running-config 的配置保存在 PC1 桌面的相应文档中，文档命名规则为：设备名称.doc,例如：RT1 路由器文件命名为 RT1.doc，然后放入到 PC1 桌面“比赛文档”文件夹中

b) 防火墙要求截图的部分，把截图的图片放到 word 文档中，请标明题号。截图后文档命名规则为：设备名称.doc,例如：防火墙 FW1 文件命名为 FW1.doc, 保存后放入到 PC1 桌面“比赛文档”文件夹中。

1、 物理连接与 IP 地址划分

（1） 按照网络拓扑图制作以太网网线，并连接设备。要求符合 T568A 和 T568B 的标准，其线缆长度适中。

（2） 根据“拓扑结构图”和“网络设备 IP 地址分配表”所示，对网络中的所有设备接口配置 IP 地址,并填入表中。

分配地址时做到节省 IP 资源，合理分配(先划分大的地址块，再划分小的地址块，可以节省 IP 资源)。总公司中除服务器区（vlan 50）所有主机规划使用 10.100.30.0/20 所在地址段。财务部（vlan 10）有 15 台主机、工程部（vlan 40）有 60 台主机、软件部（vlan 20）和系统集成部（vlan 30）两个部门都有 124 台主机，服务器的网段为 10.100.100.0/24。分公司使用 10.100.200.100/22 所在地址段。总公司与分公司所有设备互联地址使用 192.168.1.0/24 进行分配，并把地址填入上面网络设备 IP 地址分配表中的空白处。

本卷规定：

- 网关地址为每个网段的最后一个 IP 地址。
- 如果有 VRRP，虚拟网关不能使用真实接口 IP 地址。

2、 交换机配置

（1） 为交换机设备命名，命名规则参考为表 1 中的“设备名称”。

（2） 用户为了维护方便，需要远程控制 L3SW1 和 L3SW2 交换机。同时还要考虑网络安全，选择安全性较高，对密码进行密文传输的技术使用。只允许 10.100.100.0/24 整个网段都可以进行登陆。用户名为：user1,密码 为 2015network。

(3) 依据“拓扑结构图”和 VLAN 接口地址表，在交换机上完成 VLAN 配置和端口分配。

VLAN 接口地址表

设备	VLAN 名称	VLAN ID	接口
L2SW1	Link-to-CW	10	Ethernet1/1~ Ethernet1/4
	Link-to-RJ	20	Ethernet1/5~ Ethernet1/8
	Link-to-XTJC	30	Ethernet1/9~ Ethernet1/12
	Link-to-GC	40	Ethernet1/13~ Ethernet1/16
L2SW2	Link_to_Server	50	Ethernet1/1~ Ethernet1/4

(4) 采用基于 VLAN 生成树协议，实现网络中的冗余备份，按需求设置 MST 根的优先级为 4096,非根优先级为 8192,MST 的 name 为 test。交换机创建两个实例：分别为 Instance 10 和 Instance 20， 其中 Instance 10 关联 VLAN 10 和 VLAN20，VLAN50,Instance 20 关联 VLAN 30 和 VLAN40。采用 VRRP 技术实现网络中三层冗余备份，L3SW1 为 Instance10 的主交换机， 为 Instance20 备份交换机；L3SW2 为 Instance20 主交换机，为 Instance10 的备份交换机。要求 VRRP 组分别为 10,20,30,40,50，并对应相关 vlan，VRRP 组高优先级设置为 120。

(5) 总公司采用 DCHP 的方式 把地址动态分配给 vlan10,vlan20,vlan30,vlan40 的用户。DHCP 服务器的地址是 10.100.100.101。

(6) 总公司两个核心交换机 L3SW1 和 L3SW2 之间使用冗余线路连接，端口 Ethernet1/0/23 和 Ethernet1/0/24 配置端口聚合，方式为动态方式。

(7) 分公司的地址都在同一网段。但分为两个部门，销售部，行政部。现公司领导要求：销售部，行政部之间不能互相访问，公司内部来访人员的有 2 台专用电脑，这 2 台电脑之间不可以互相访问，也不可以访问销售部，行政部。

Vlan 名称	部门	接口
10	销售部	Ethernet1/0/1~ Ethernet1/0/2
20	行政部	Ethernet1/0/3~ Ethernet1/0/4
30	来访人员	Ethernet1/0/5~ Ethernet1/0/6

(8) 在改造过程中，网络管理员提出网络经常上网时断时续，有时完全断网，猜测有可能是 ARP 病毒引起网络故障，为了确认故障问题，在 L2SW1 上通过 22 端口进

行双向流量的查看，请帮助管理员查找问题所在。

(9) 经过查看后发现是 L2SW1 端口 9 的主机发出的 arp 网关欺骗报文，欺骗其它主机，除了对系统相应的杀毒处理后，为了避免相同故障再次发生，在交换机的端口 9 上进行 ARP 的保护。请配置相关命令。

(10) 通过流量查看发现，在总公司的 L2SW1 上在端口 20 的计算机经常私自看电影下载电影，占用流量非常大，管理员决定把端口速度限制在下行为 8M，请配置相关命令。

(11) OSPF 区域 0 开启基于区域的认证。认证方式为 MD5 方式，密码为 123。

3、 路由器配置与调试

(1) 为路由设备命名，命名规则参考为表 1 中的“设备名称”。

(2) 根据网络拓扑图所示，为了保障 ISP 的租用专用线路的链路安全，需要在 RT1 与 RT2 之间连接的链路上配置 PPP 协议，采用双向 CHAP 的验证方式，用户名分别使用对方的用户名 RT1 和 RT2，密码均为 7654321。速率为 115200

(3) 总公司网络中采用的 OSPF 动态路由协议，根据“网络拓扑结构图”所示，配置动态路由协议，将设备接口分配到不同的区域中。分公司采用 RIPv1 动态路由协议保障网络正常通信。RT3 的 loopback 口通告进 RIP 中

(4) 下面的是网络设备 RID，防火墙通过 OSPF 进程下指定 ROUTER-ID 的方式设置。其它设备不能使用 OSPF 进程下指定 ROUTER-ID 的方式设置,请根据 ROUTER-ID 的选举规则进行配置。

设备名称	RID
FW1	1.1.1.1
RT1	2.2.2.2
FW2	3.3.3.3
L3SW1	4.4.4.4
L3SW2	5.5.5.5

(5) 在总公司与分公司的互联网出口设备上，需要将去往互联网的默认路由引入到动态路由中。

(6) 总公司与分公司通过地址池方式进行NAT映射.保证总公司与分公司可以正常上网，要求两个公司只能从自己的出口进行上网访问。要求访问控制列表的名字为nat,RT1 和 RT2 上使用地址池的方式，名称为 natpool，地址池的范围都是123.1.12.1-123.1.12.253/24。

(7) 在分公司 RT3 上做为 DHCP 服务器为分公司所有用户动态分配 IP 地址，地址10.100.201.100/22-10.100.201.200/22，网关为 10.100.203.254,DNS 地址为8.8.8.8。地址租约时长为1天。

(8) 在总公司的 RT1 通过 CQ 的方式把去往外网的流量分为三个队列，将源地址为10.100.31.0/29 放入第一队列，将源地址为 TCP 端口为 8000 放入第二队列，其他默认的流量放入第三队列，第一队列可传送最大字节数 200 字节，第二队列最大字节数 300 字节，第三队列最大字节数为 400 字节

(9) 为了保障总公司与分公司之间传输业务的高可用性，当总公司与分公司之间的ISP 专线中断后，需要采用互联网链路做为备份链路，在集团公司与上海分公司的两端路由器上配置 IPSEC VPN，保障分公司 10.100.200.0/24 到总公司10.100.100.0/24 之间的流量。ISA 策略，使用组 2，验证方式为预共享。isakmp key为 12345,传输集的名字为 tianjin,采用 esp-des esp-md5-hmac 的方式，crymap 的名称为 guosai。

(10) 网络改造完成后，RT1 通过 ACL 的配置，使总公司的 10.100.104.0/24 的网络随时可以访问分公司的 10.100.204.0/24 的网络。访问总公司服务器区10.100.100.0/24 的不进行任何限制，访问总公司的 10.100.70.0/24 的网络无论什么类型的流量，在每星期一至星期五 9：00~17:00 放行，其余时间不允许访问。要求 time-range 的名称为 time

(11) 当分公司与总公司的网络按照网络管理员的思路改造完成时，改造后，网络管理员发现分公司到总公司的网络是不通的，请帮助网管员查找故障并解决。

4、 防火墙配置

(1) 把防火墙进行设备命名，命名规则参考为表 1 中的“设备名称”。

(2) 在总公司的 FW1 和 FW2 使用 OSPF 协议，根据与路由的相关配置，完成防火墙的配置，保证网络互通。FW1 的 loopback 口通告进 ospf

(3) 在总公司 FW2 上设置关键词过滤，禁止办公室用户浏览在网页中出现“暴力”一词超过三次或三次以上的网站,并要求记录日志，要求主要过程进行截图。

(4) 在总公司 FW2 上，每周一到周五 9:00 到 17:30，禁止邮件中带有“反动”关键字的邮件进行发送，要求主要过程进行截图。

(5) 在总公司 FW2 上，出现 ICMP 大于 2048 的包开启大包攻击防护，使用丢弃来保证总公司的网络安全性。并开启其它的 DDOS 功能进行防护，要求主要过程进行截图

(6) 在总公司 FW2 上，为了保障网络资源合理使用，每个用户的网络速率为上行最大 64K，下行最大 128K，要求主要过程进行截图。

(7) 当总公司 FW2 上有人用 console 登陆配置设备时，需要发送向 administrator@sina.com 地址发送邮件进行提醒记录。新浪邮箱发信(smtp)服务器的地址为：smtp.sina.com，新浪邮箱服务器的地址为：pop.sina.com，要求主要过程进行截图

5. 无线配置

(1) 把 AC 进行设备命名，命名规则参考为表 1 中的“设备名称”。

(2) 分公司用户采用无线接入方式,其中 SSID 为 TJ+自己的组号,协议为 802.11bgn，信道为 1；用户接入无线网络时采用 wpa-personal 认证方式，其口令为 12345678。AC 的 vlan100 为管理 vlan,管理地址为 192.168.1.9/24,AP 管理地址为 192.168.1.10/24

(3) 客户端有 802.11G 和 802.11N，保证客户端的服务质量和网络整体吞吐量，不让高速无线客户端被低速客户端拖累，对无线的下行流量进行时空公平调度。

(4) 为了更好的发挥 AP 的性能 ，开启无线的 ARP 代理功能，限制 AP 的 ARP 广播。

(5) 网络管理员发现 AP 的发射功率不稳定，客户端总是出现丢包的现象，通过周期性的触发方式每隔一小时对发射功率进行一次调整。

(6) 假设 AP1 和 AP2 有着相同的信道，在 AC 上开启 radio 的自动信道调整功能，周期调整时间为 8 个小时。

操作系统部分（550 分）
Windows 操作系统

【说 明】

（1）题目中所涉及 Windows 操作系统的 administrator 管理员以及其他普通用户密码均为 2015Netw1rk（注意区分大小写），若未按照要求设置密码，涉及到该操作的所有分值记为 0 分。

（2）虚拟主机的 IP 属性设置请按照网络拓扑结构图以及“表 3：服务器 IP 地址分配表”的要求设定。

（3）除非作特殊说明，在同一主机下需要安装相同操作系统版本的虚拟机时，可采用 Oracle VM VirtualBox 软件自带的克隆系统功能实现。

（4）所有系统镜像文件及试题所需的其它软件均存放在每台主机的 D:\soft 文件夹中，并将题目要求的截图内容以.jpg 格式存储于桌面 BACKUP 文件夹中。

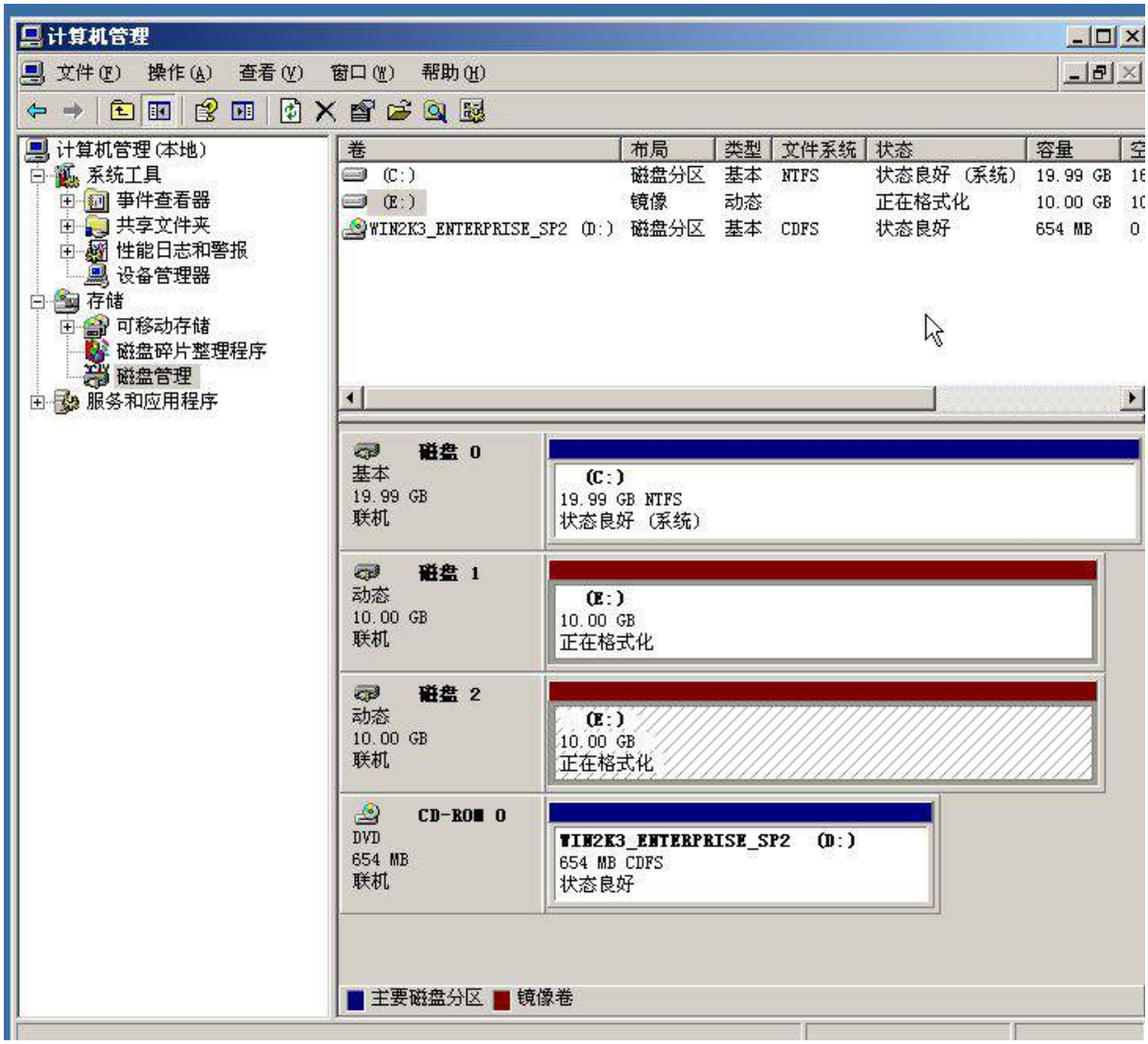
（5）题目要求的虚拟机均安装于每台主机的 D：\virtualPC 目录，即路径为 D：\virtualPC\虚拟主机名称。

一、在 Server 1 上完成如下操作:

（一）完成虚拟主机的创建

1、安装虚拟机“Win2003-A1”，具体要求为内存为 1G，硬盘 20G；

2、在虚拟机“Win2003-A1”中添加 SCSI 控制器，添加二块 SCSI 虚拟硬盘，其每块硬盘的大小为 10G；将二块硬盘制作成 RAID1，磁盘盘符为 e:\；



3、安装虚拟机“Win2008-A1”，具体要求为内存为 1G，硬盘 20G，并将服务器加入到 Windows 域环境；

（二）在主机 Win2003-A1 中完成域控制器的部署

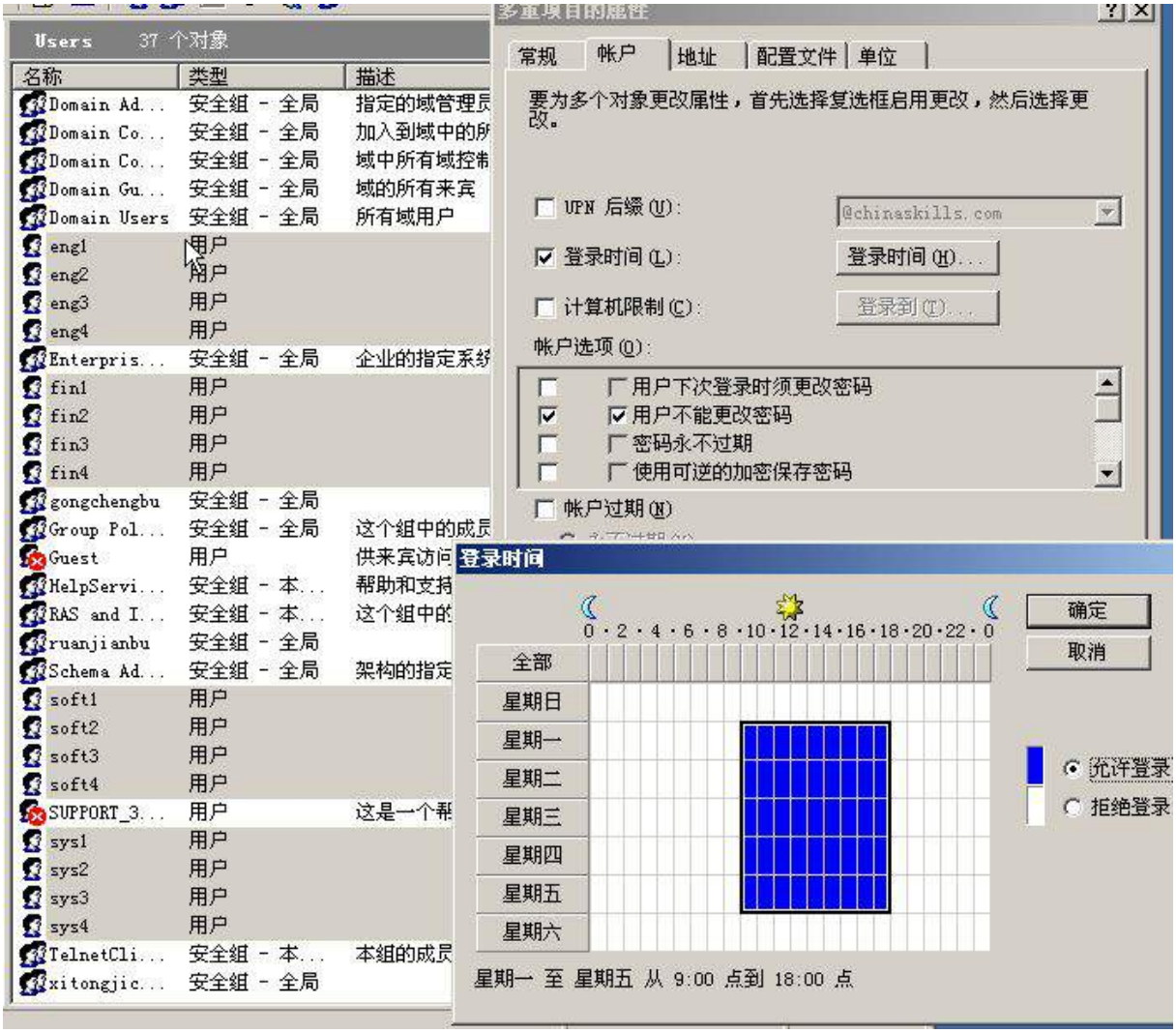
1、创建 4 个用户组，**组名采用对应部门名称的拼音来命名**，每个部门都创建 4 个

用户，财务部用户：fin1~fin4、工程部用户：eng1~eng4、软件部用户：soft1~soft4、系统集成部用户：sys1~sys4，所有用户不能修改其用户口令，具体口令为2015Netw1rk,并要求用户只能在上班时间可以登录（每周工作日 9:00~18:00）；

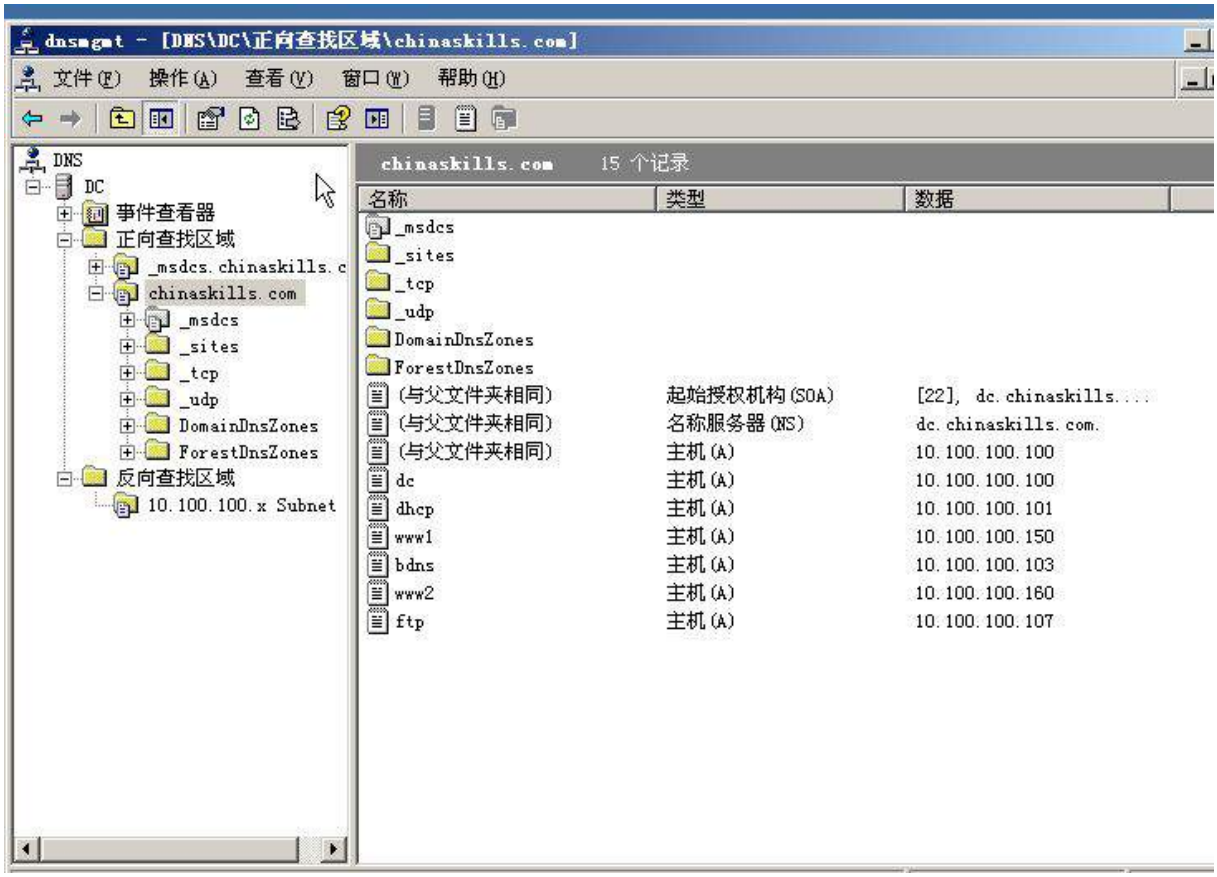

caiwubu 属性
常规
成员
隶属于
管理者
成员(M):
名称
Active Directory 文件夹
fin1 chinaskills.com/Users
fin2 chinaskills.com/Users
fin3 chinaskills.com/Users
fin4 chinaskills.com/Users
添加(D)...
删除(R)
确定
取消
应用(A)

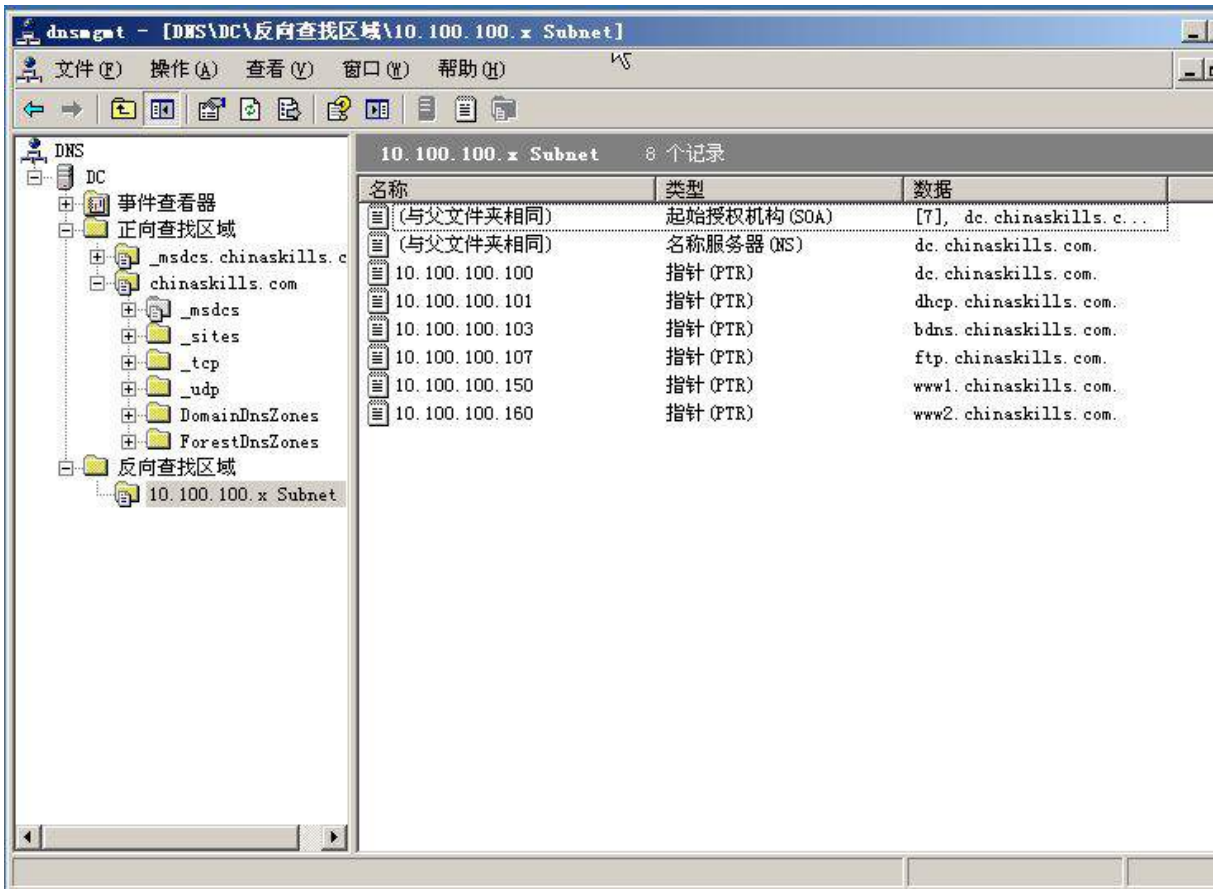

gongchengbu 属性
常规
成员
隶属于
管理者
成员(M):
名称
Active Directory 文件夹
eng1 chinaskills.com/Users
eng2 chinaskills.com/Users
eng3 chinaskills.com/Users
eng4 chinaskills.com/Users
添加(D)...
删除(R)
确定
取消
应用(A)

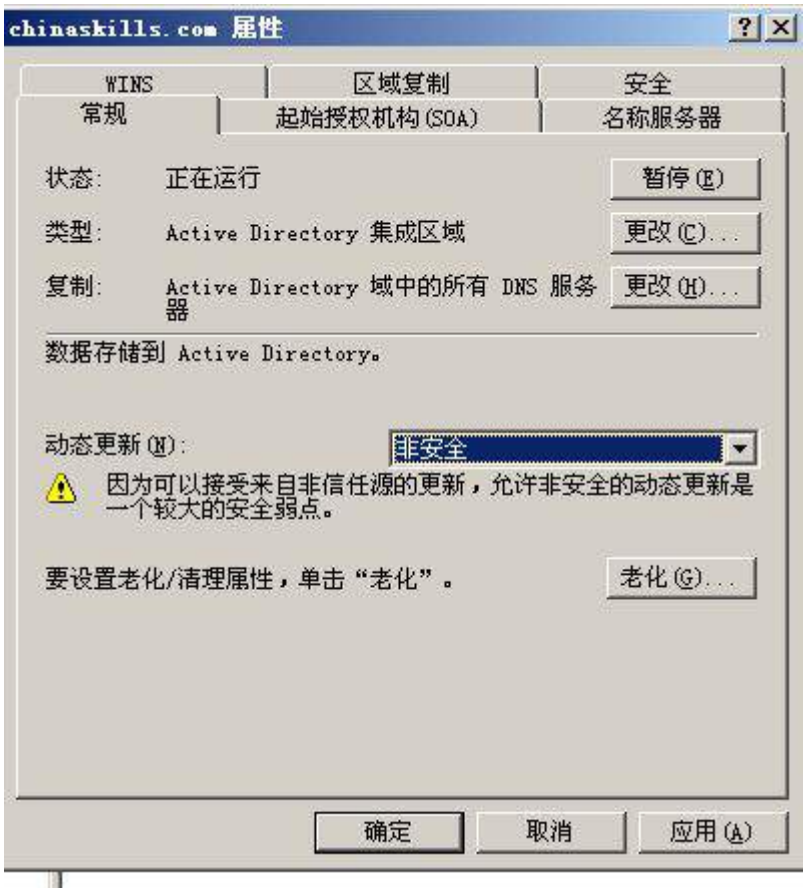

ruanjianbu 属性
常规
成员
隶属于
管理者
成员(M):
名称
Active Directory 文件夹
soft1 chinaskills.com/Users
soft2 chinaskills.com/Users
soft3 chinaskills.com/Users
soft4 chinaskills.com/Users
添加(D)...
删除(R)
确定
取消
应用(A)


Users 37 个对象
名称
类型
描述
Domain Ad... 安全组 - 全局 指定的域管理员
Domain Co... 安全组 - 全局 加入到域中的所
Domain Co... 安全组 - 全局 域中所有域控制
Domain Gu... 安全组 - 全局 域的所有来宾
Domain Users 安全组 - 全局 所有域用户
engl 用户
eng2 用户
eng3 用户
eng4 用户
Enterpris... 安全组 - 全局 企业的指定系统
finl 用户
fin2 用户
fin3 用户
fin4 用户
gongchengbu 安全组 - 全局
Group Pol... 安全组 - 全局 这个组中的成员
Guest 用户 供来宾访问
HelpServi... 安全组 - 本... 帮助和支持
RAS and I... 安全组 - 本... 这个组中的
ruanjianbu 安全组 - 全局
Schema Ad... 安全组 - 全局 架构的指定
soft1 用户
soft2 用户
soft3 用户
soft4 用户
SUPPORT_3... 用户 这是一个帮
sys1 用户
sys2 用户
sys3 用户
sys4 用户
TelnetCli... 安全组 - 本... 本组的成员
xitongjic... 安全组 - 全局
常规
帐户
地址
配置文件
单位
要为多个对象更改属性，首先选择复选框启用更改，然后选择更改。
UPN 后缀(U):
@chinaskills.com
登录时间(L):
登录时间(H)...
计算机限制(C):
登录到(T)...
帐户选项(O):
用户下次登录时须更改密码
用户不能更改密码
密码永不过期
使用可逆的加密保存密码
帐户过期(N)
登录时间
0 · 2 · 4 · 6 · 8 · 10 · 12 · 14 · 16 · 18 · 20 · 22 · 0
全部
星期日
星期一
星期二
星期三
星期四
星期五
星期六
确定
取消
允许登录
拒绝登录
星期一 至 星期五 从 9:00 点到 18:00 点

2、将此服务器配置为主 DNS 服务器，正确配置 chinaskills.com 域名的正向及反向解析区域，能够正确解析 chinaskills.com 域中的所有服务器；创建对应服务器主机记录，需要关闭网络掩码排序功能。设置 DNS 服务正向区域和反向区域与活动目录集成；要求动态更新设置为非安全；


dnsmgmt - [DNS\DC\正向查找区域\chinaskills.com]
文件(F) 操作(A) 查看(V) 窗口(W) 帮助(H)
DNS
DC
事件查看器
正向查找区域
_msdcs.chinaskills.c
chinaskills.com
_msdcs
_sites
_tcp
_udp
DomainDnsZones
ForestDnsZones
反向查找区域
10.100.100.x Subnet
chinaskills.com 15 个记录
名称 类型 数据
_msdcs
_sites
_tcp
_udp
DomainDnsZones
ForestDnsZones
(与父文件夹相同) 起始授权机构(SOA) [22], dc.chinaskills....
(与父文件夹相同) 名称服务器(NS) dc.chinaskills.com.
(与父文件夹相同) 主机(A) 10.100.100.100
dc 主机(A) 10.100.100.100
dhcp 主机(A) 10.100.100.101
www1 主机(A) 10.100.100.150
bdns 主机(A) 10.100.100.103
www2 主机(A) 10.100.100.160
ftp 主机(A) 10.100.100.107


dnsmgmt - [DNS\DC\反向查找区域\10.100.100.x Subnet]
文件(F) 操作(A) 查看(V) 窗口(W) 帮助(H)
DNS
DC
事件查看器
正向查找区域
_msdcs.chinaskills.c
chinaskills.com
_msdcs
_sites
_tcp
_udp
DomainDnsZones
ForestDnsZones
反向查找区域
10.100.100.x Subnet
10.100.100.x Subnet 8 个记录
名称 类型 数据
(与父文件夹相同) 起始授权机构(SOA) [7], dc.chinaskills.c...
(与父文件夹相同) 名称服务器(NS) dc.chinaskills.com.
10.100.100.100 指针(PTR) dc.chinaskills.com.
10.100.100.101 指针(PTR) dhcp.chinaskills.com.
10.100.100.103 指针(PTR) bdns.chinaskills.com.
10.100.100.107 指针(PTR) ftp.chinaskills.com.
10.100.100.150 指针(PTR) www1.chinaskills.com.
10.100.100.160 指针(PTR) www2.chinaskills.com.

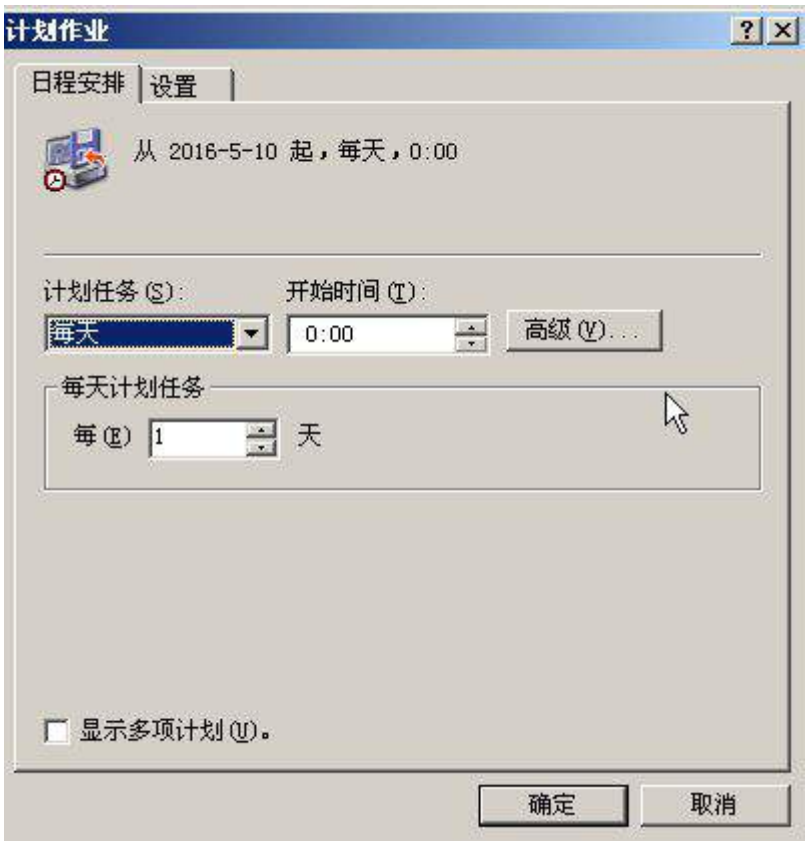


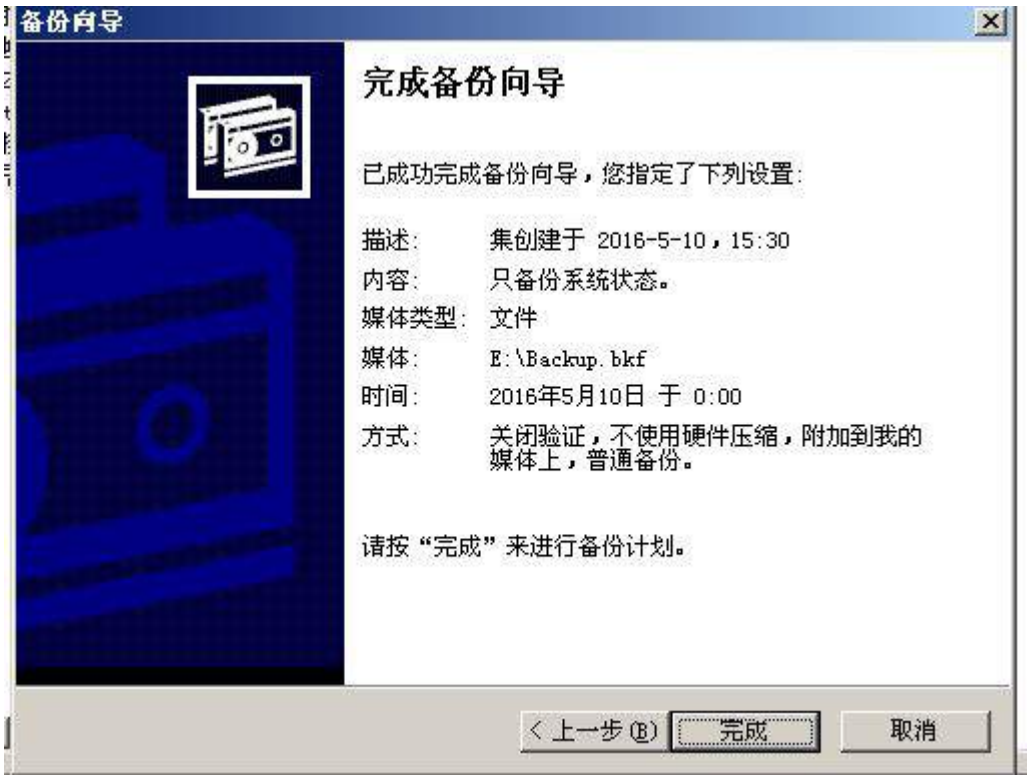
3、将此服务器设置为域控制器，设置域和林的功能级别为 Windwos Server 2003；此外，安装证书服务，设置为企业根，有效期为 5 年，为企业内部自动回复证书申请；


提升域功能级别
域名:
chinaskills.com
当前域功能级别:
Windows Server 2003
此域处于允许范围内最高的功能级别操作状态。有关域功能级别的详细信息，请单击“帮助”。
关闭
帮助(H)

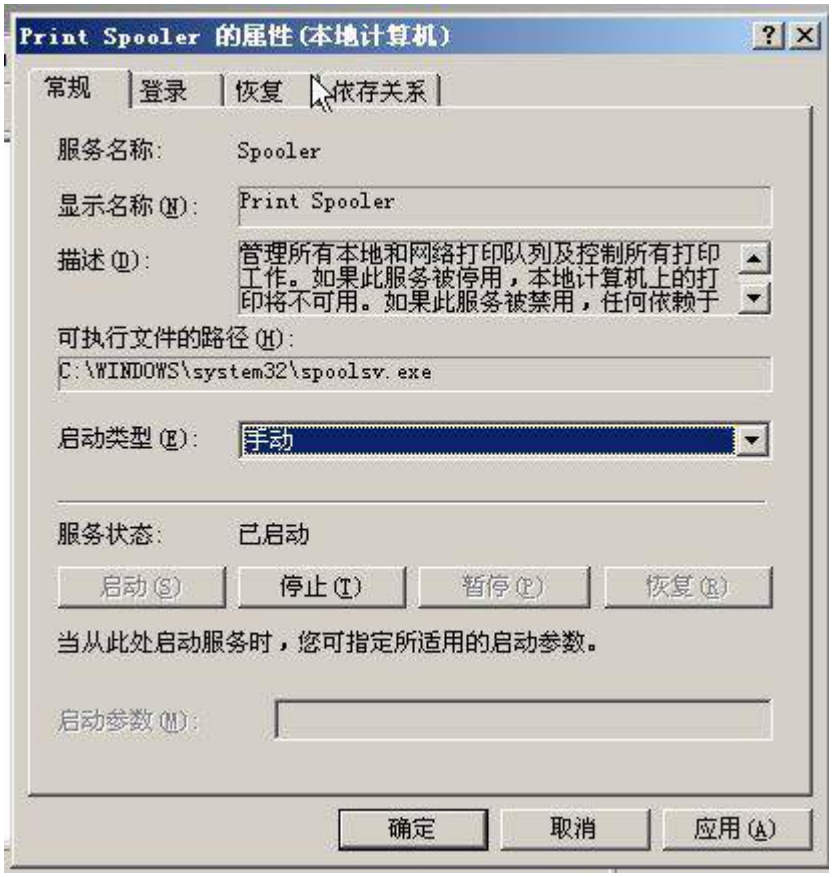

Windows 组件向导
CA 识别信息
输入识别该 CA 的信息。
此 CA 的公用名称(C):
CA1
可分辨名称后缀(D):
DC=chinaskills,DC=com
可分辨名称的预览(P):
CN=CA1,DC=chinaskills,DC=com
有效期限(V):
5
年
截止日期:
2021-5-10 15:16
< 上一步(B)
下一步(N) >
取消
帮助

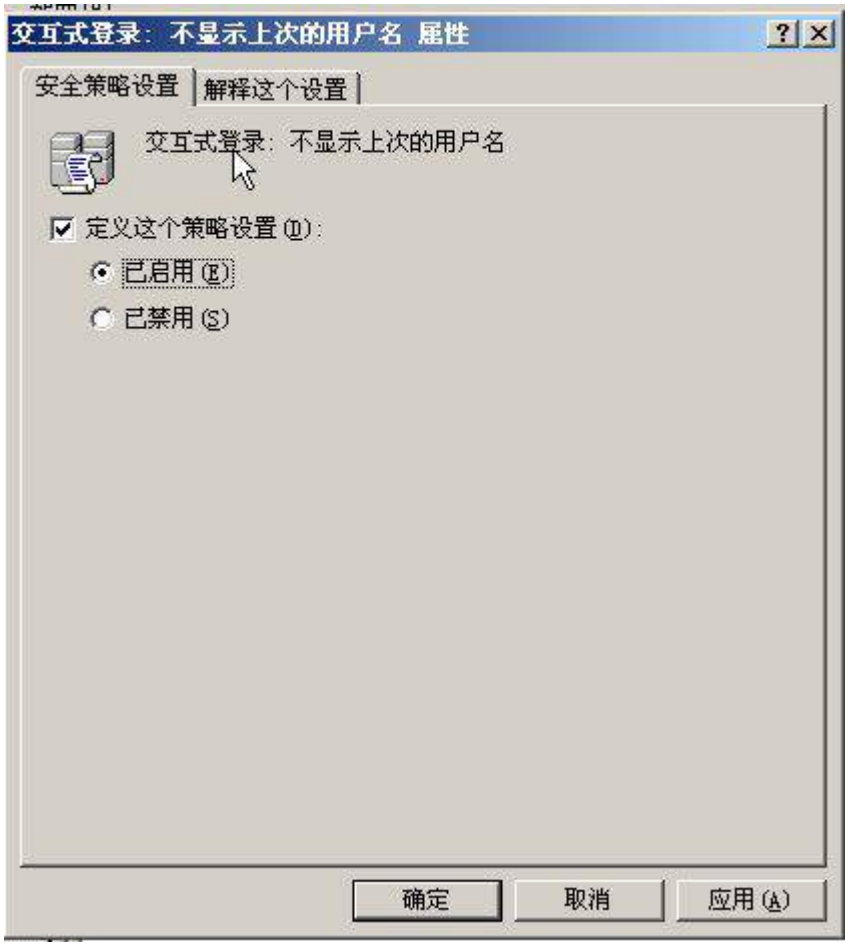
4、制订备份计划，每天的 0 点对“系统状态”进行备份，并采用 VSS 完整备份，备份至 e:\盘；

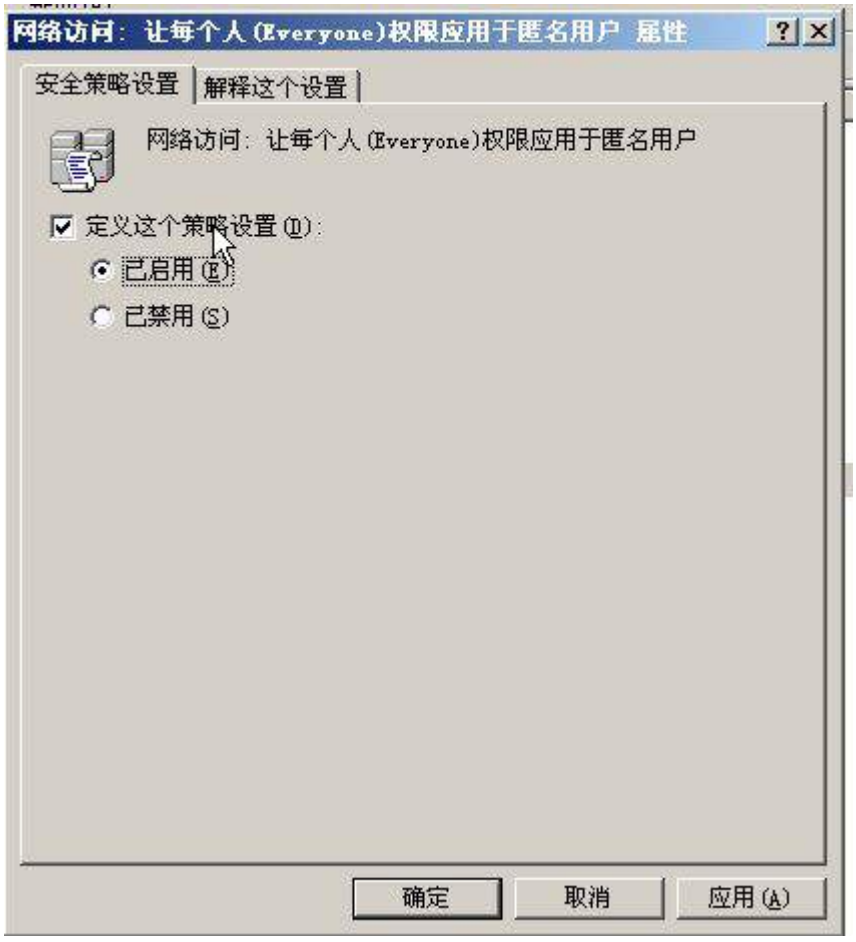


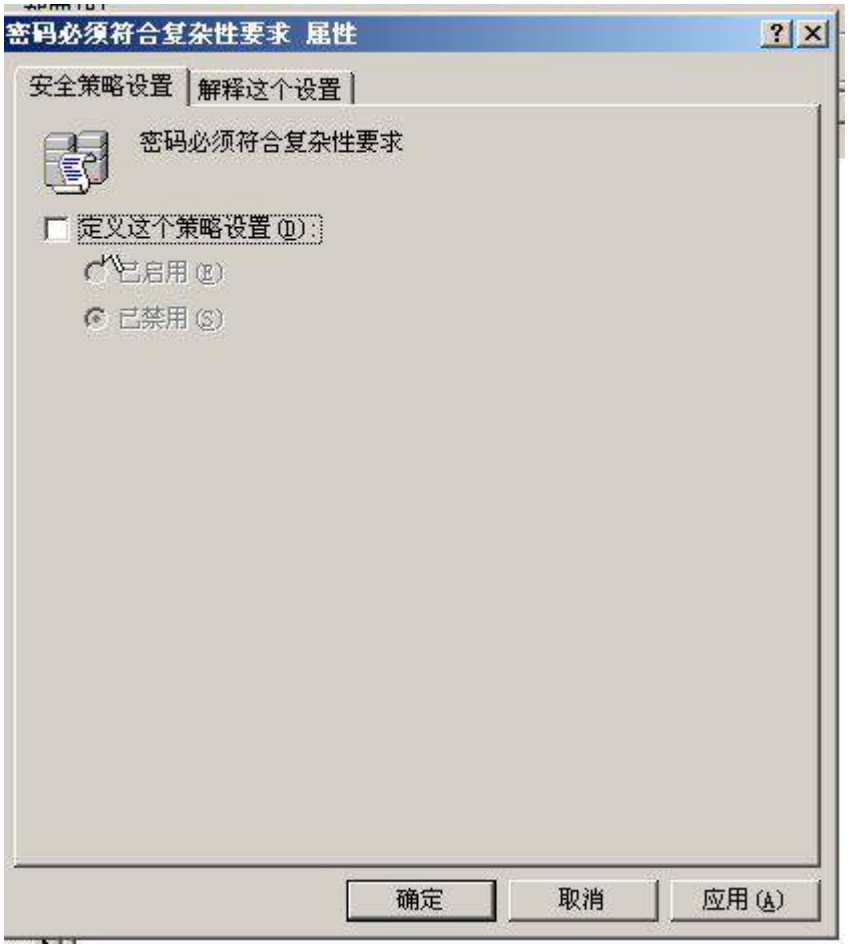


5.设置组策略把的“print spooler”服务改为手动启动；设置组策略对 “不显示上次登录名”选项已启用；设置组策略禁用“将 everyone 权限应用于匿名用户”；更改组策略密码策略为无复杂性要求；


Print Spooler 的属性(本地计算机)
常规
登录
恢复
依存关系
服务名称:
Spooler
显示名称(N):
Print Spooler
描述(D):
管理所有本地和网络打印队列及控制所有打印工作。如果此服务被停用，本地计算机上的打印将不可用。如果此服务被禁用，任何依赖于
可执行文件的路径(H):
C:\WINDOWS\system32\spoolsv.exe
启动类型(E):
手动
服务状态:
已启动
启动(S)
停止(T)
暂停(P)
恢复(R)
当从此处启动服务时，您可指定所适用的启动参数。
启动参数(M):
确定
取消
应用(A)


交互式登录: 不显示上次的用户名 属性
安全策略设置
解释这个设置
交互式登录: 不显示上次的用户名
定义这个策略设置(D):
已启用(E)
已禁用(S)
确定
取消
应用(A)


网络访问：让每个人(Everyone)权限应用于匿名用户 属性
安全策略设置
解释这个设置
网络访问：让每个人(Everyone)权限应用于匿名用户
定义这个策略设置(D)：
已启用(E)
已禁用(S)
确定
取消
应用(A)


密码必须符合复杂性要求 属性
安全策略设置
解释这个设置
密码必须符合复杂性要求
定义这个策略设置(D)：
已启用(E)
已禁用(S)
确定
取消
应用(A)

（三）在主机 **Win2008-A1** 中完成 **DHCP** 服务器的部署

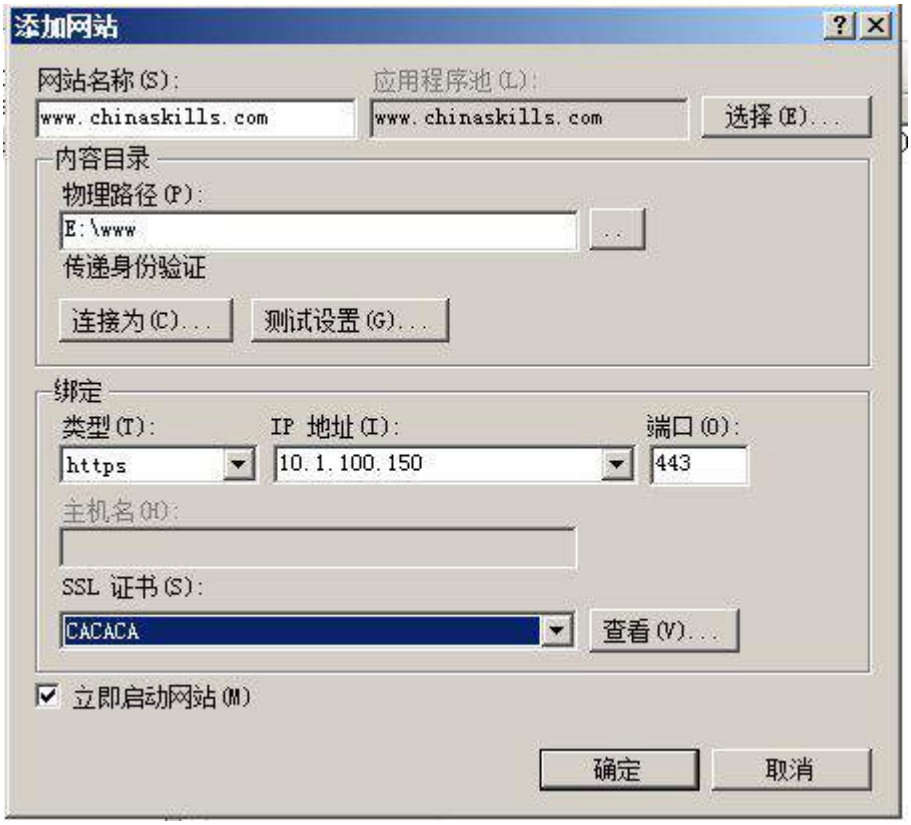
安装 DHCP 服务，为**内网财务部、工程部、软件部和系统集成部**的用户主机动态分配 IPv4 地址，建立作用域，作用域的名称采用对应部门名称的拼音，超级作用域的名称为 DHCPSERVER，为用户分配网关、DNS 服务器及域名；此后将 DHCP 服务管理器有关超级作用域内容展开并截图存储为 dhcp.jpg；

二、在 Server 2 上完成如下操作:

（一）完成虚拟主机的创建

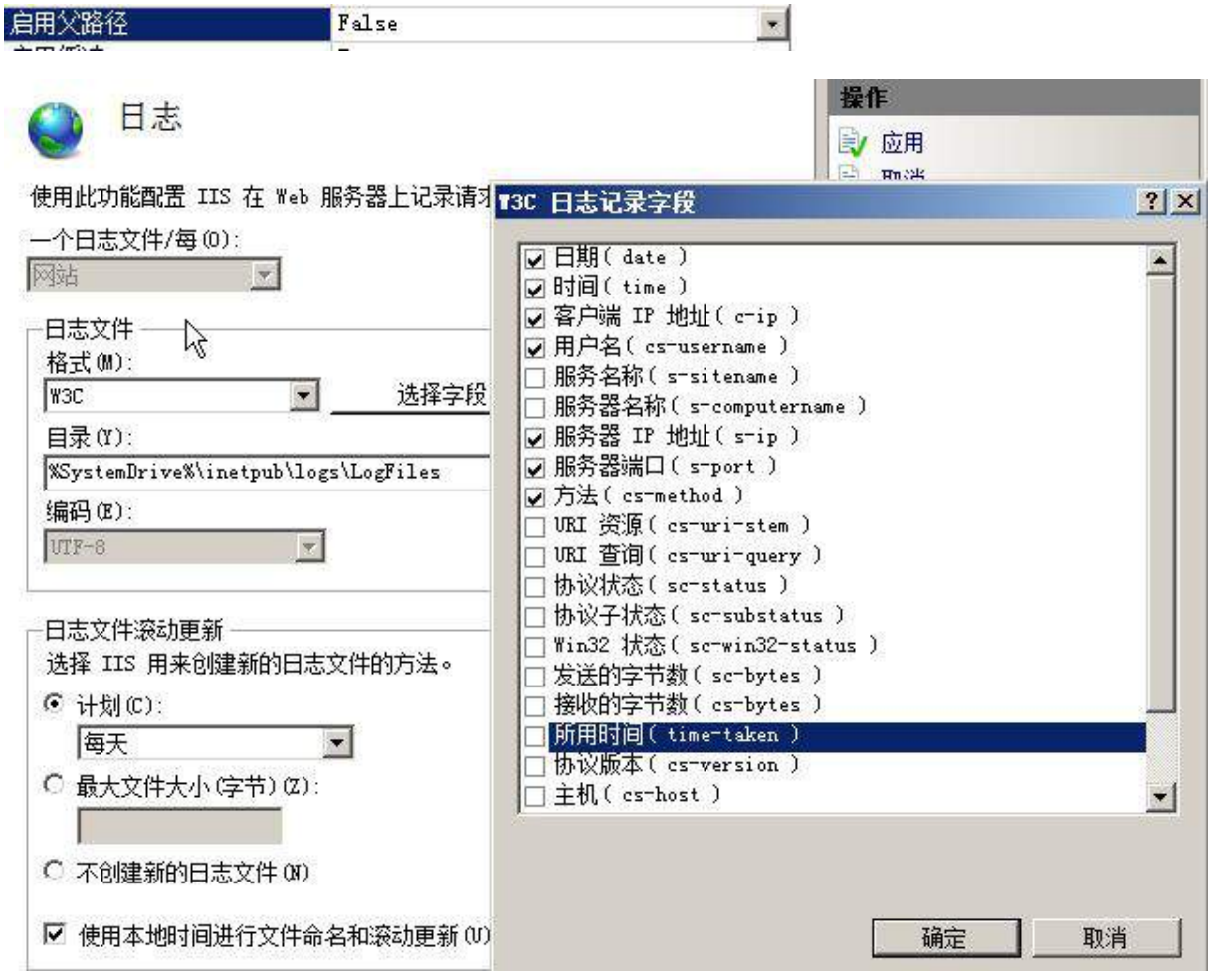
1、安装虚拟机“Win2008-B1”，其内存为 1G，硬盘 20G，并将服务器加入到 Windows 域环境；

2、安装 IIS 组件，创建 www.chinaskills.com 站点，在挂载的磁盘 e:\下创建名称为 www 的目录，在 www 文件夹中创建名称为 chinaskills.html 的主页，其主页显示内容“热烈庆祝 2015 年全国职业技能竞赛开幕”，同时只允许使用 SSL 且只能通过域名方式进行访问；



3、设置网站的最大连接数为 1000,网站连接超时为 60s,网站的带宽为 1000KB/S，使用 W3C 记录日志；禁用父路径；每天创建一个新的日志文件，使用当地时间作为日志

文件名；日志只允许记录日期、时间、客户端 IP 地址、用户名、服务器 IP 地址、服务器端口号和方法；



4、安装 NLB 负载平衡服务，其群集 IPv4 地址为 10.1.100.180/24，新建群集优先级为 2，群集名称为 www. chinaskills.com，采用多播方式；

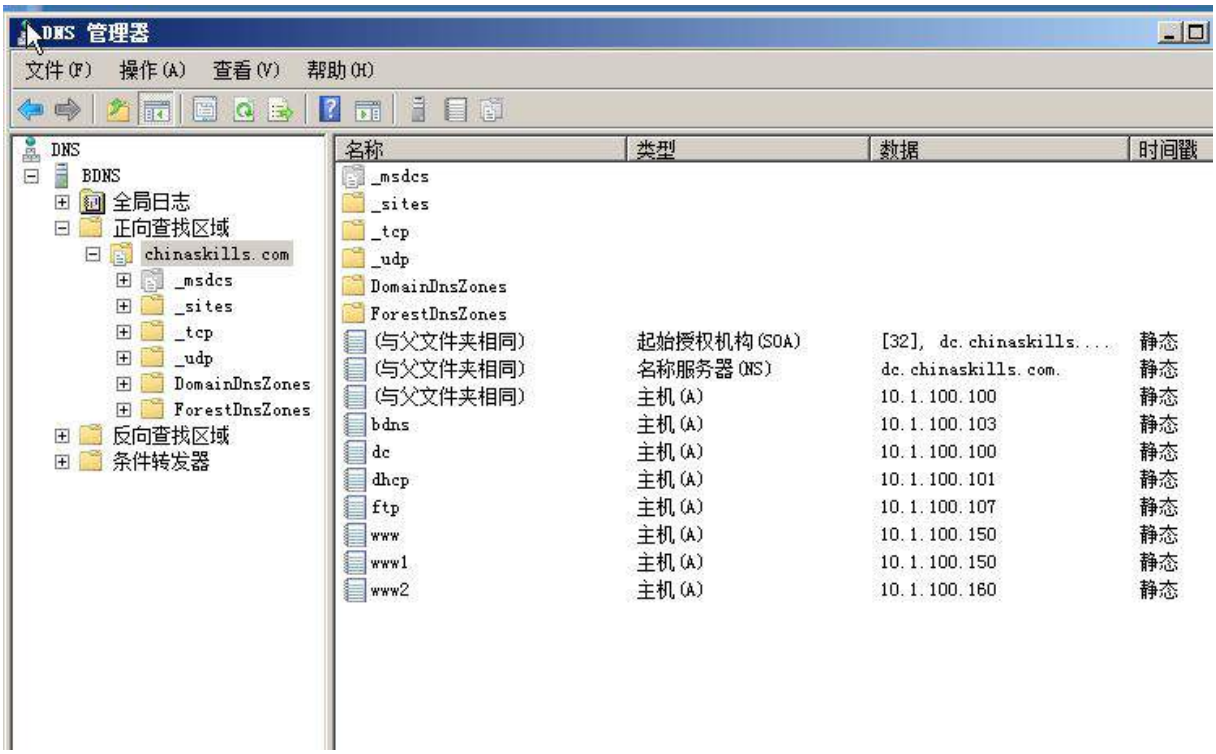
5、配置 DFS 服务，实现两个服务器的网站主页内容保持同步，空间名称为 WEB，文件夹为 WWW，复制组为 www-backup,拓扑采用交错方式，设置复制在周六和周日带宽为

完整，周一至周五带宽为 64M；

（三）在主机 Win2008-B2 中完成备份 DNS 的部署

1、配置此服务器为备份 DNS，其合法域名为 bdns. Chianskills.com

2、将服务器加入到 windows 域中，将所有的主 DNS 的区域都复制到备份 DNS 服务器 上

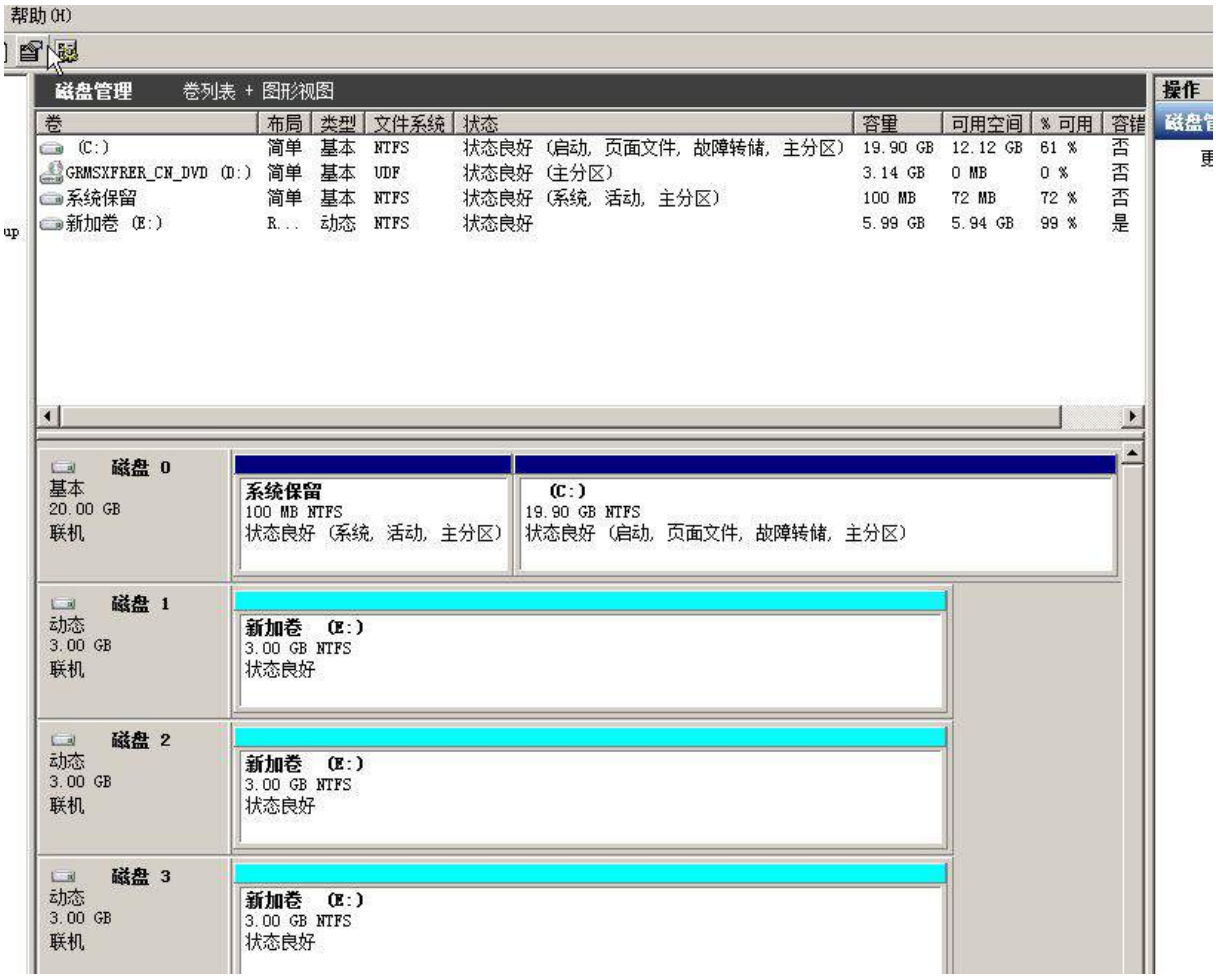


三、在 Server 3 上完成如下操作：

（一）完成虚拟主机的创建

1、安装虚拟机“Win2008-C1”，其内存为 1G，硬盘 20G，并将服务器加入到 Windows 域环境；

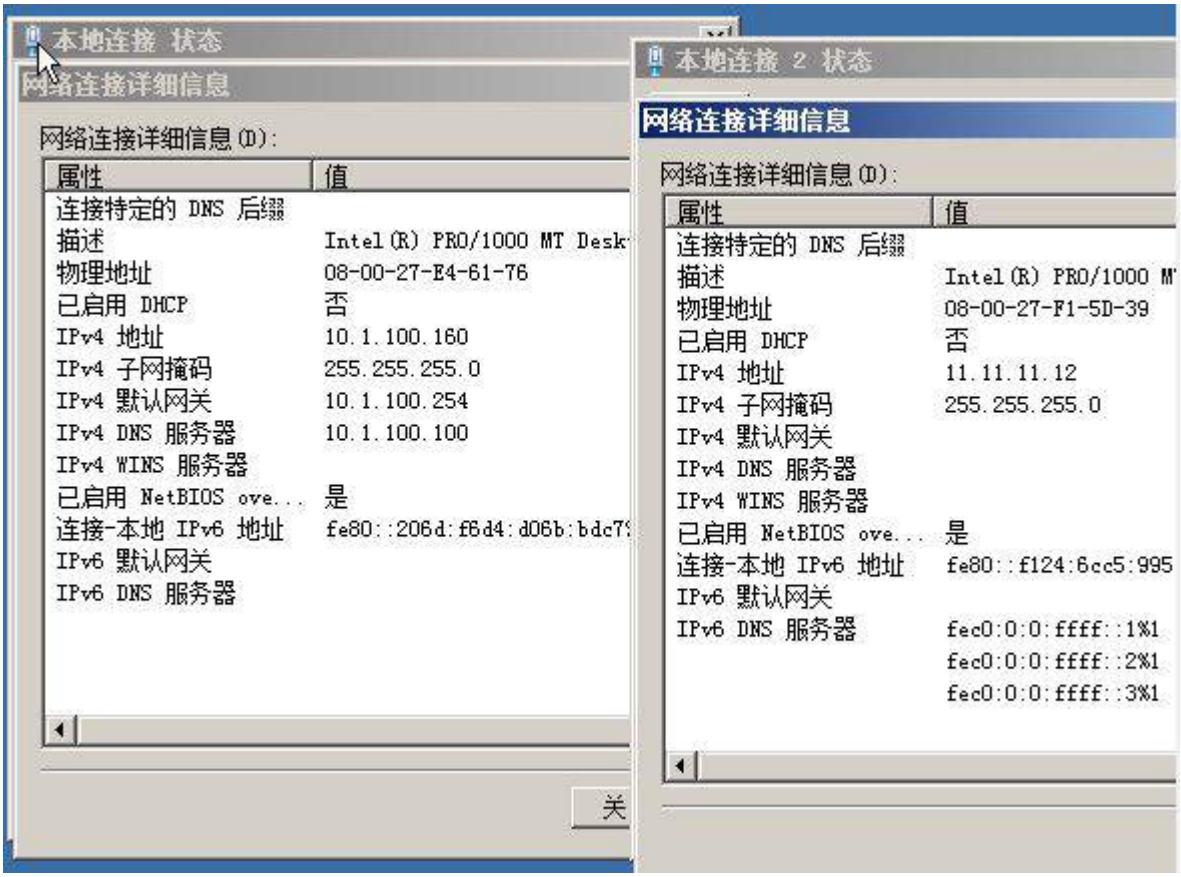
2、在虚拟机“Win2008-C1”中添加 SCSI 控制器，添加 3 块 SCSI 虚拟硬盘，其每块硬盘的大小为 3G，将三块硬盘配置为 RAID5，对应磁盘盘符为 e:\；



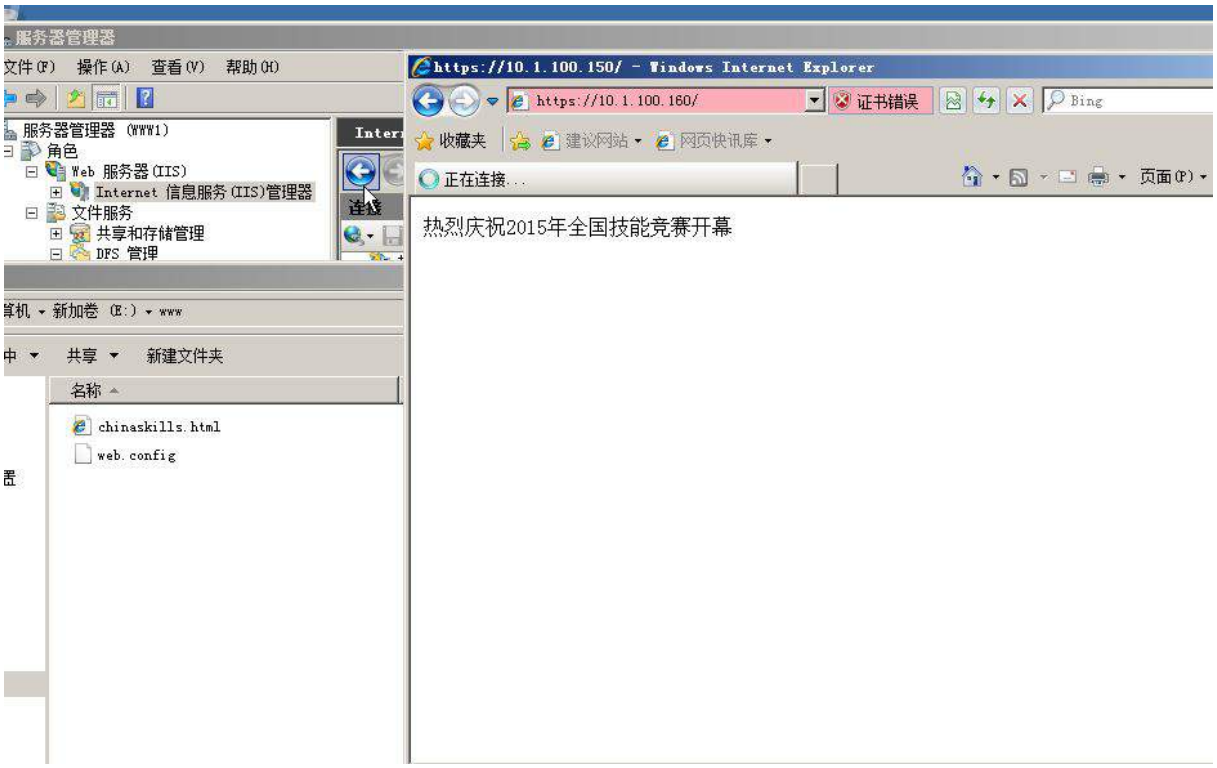
3、在虚拟机“Win2008-C2”其内存为 1G，硬盘 20G，并将服务器加入到 Windows 域环境；

（二）在主机 Win2008-C1 中完成 WEB 服务器 2 的部署

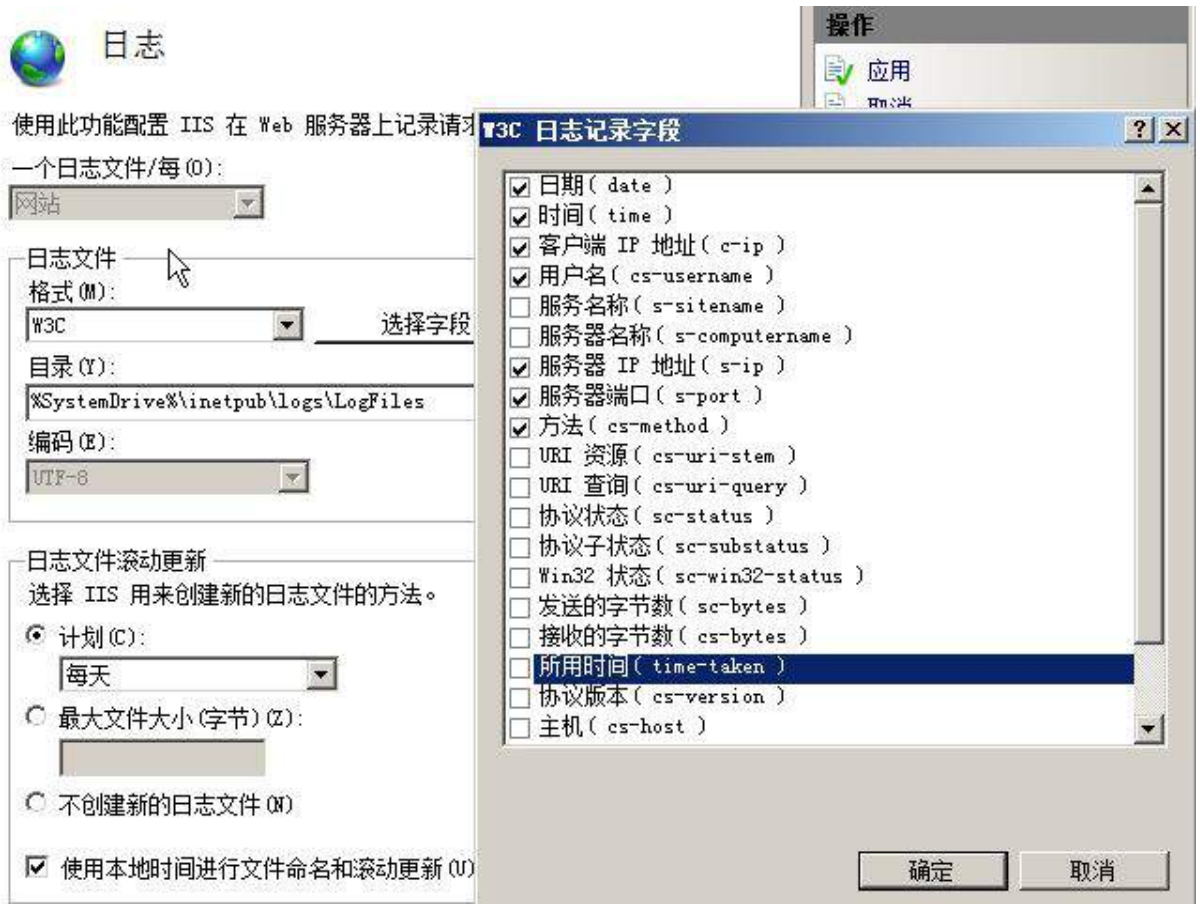
1、在 VirtualBox 上添加安装两块网卡，一块网卡提供网络服务，其 IPv4 地址为 10.1.100.160/24,，另一块网卡为心跳线网卡，其 IPv4 地址为 11.11.11.12；（15 分）



2、安装 IIS 组件，创建 www.chinaskills.com 站点，在挂载的磁盘 e:\下创建名称为 www 的文件，在 www 文件中创建名称为 chinaskills.html 的主页，主页显示内容“热烈庆祝 2015 年全国职业技能竞赛开幕”，同时只允许使用 SSL 且只能采用域名方式进行访问；



3、设置网站的最大连接数为 1000,网站连接超时为 60s,网站的带宽为 1000KB/S,使用 W3C 记录日志；每天创建一个新的日志文件，使用当地时间作为日志文件名；日志只允许记录日期、时间、客户端 IP 地址、用户名、服务器 IP 地址、服务器端口号和方法；



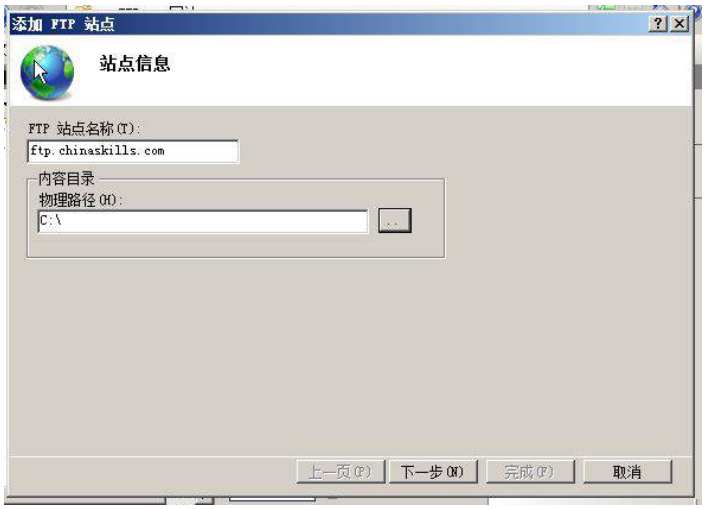
4、安装 NLB 负载平衡服务，其群集 IPv4 地址为 10.1.100.180/24，完整的 Internet 名称为 www.chinaskills.com，采用多播方式；

5、配置 DFS 服务，实现两个服务器的网站主页内容保持同步，空间名称为 WEB，

文件夹为 WWW，复制组为 www-backup,拓扑采用交错方式，设置复制在周六和周日带宽为完整，周一至周五带宽为 64M；在本机网卡的“本地连接 状体”选项框中点击“详细信息”并将此选项框截图存储为 nlb.jpg；

（三）在主机 Win2008-C2 中完成 FTP 服务器以及域控服务器角色迁移的部署

1、安装 IIS 组件的 FTP 组件，创建 FTP 站点，ftp.chinaskills.com 站点只允许软件部的用户都可以上传文件和下载文件，而其它及匿名用户只能下载文件，但不能上传文件，限制用户上传最大空间为 100M，超过 80M 预警，预警采用电子邮件和记录事务日志；



2、建立备份域控服务器，将主域控服务器操作主机角色、全局编录角色迁移至备份域控服务器上；

Linux 操作系统部分

【说 明】

1、所有 Linux 操作系统的 root 用户的密码为 123456，若未按要求设置密码，涉及到该操作系统下的所有分值记为 0 分。

2、虚拟主机的 IP 属性设置请按照网络拓扑结构图以及“表 3：服务器 IP 地址分配表”的要求设定。

3、除有特别规定外，其他未明确规定用户密码均与用户名相同。

4、所有操作系统镜像文件及试题所需的其他软件均存放于每台计算机的/根目录下。

5、题目要求的虚拟机均安装于每台主机的 D：\virtascualPC 目录，即路径为 D：\virtualPC\虚拟主机名称。

一、在 Server 1 上完成如下操作:

（一）完成虚拟主机的创建

安装虚拟机“Centos-A1”,具体要求为内存 512MB,硬盘 10GB；

（二）在主机 Centos-A1 中完成 PXE 服务器的部署

1、在此服务器上以 YUM 方式安装 DHCP 服务，创建作用域网段为 10.100.100.0/24，地址池为 10.100.100.2-10.100.100.5.指定 DNS 服务域名为 dns.jnds.net，指定 DNS 服务器以及网关的 IP 地址信息，设置租约时间 172800s，最大租约时间为 259200s，指明下一跳 TFTP 服务器 IP 信息，同时设置自动安装脚本文件，最终设置 DHCP 服务为开机自动运行；

```
  Verifying  : 1:perl-Module-Pluggable-3.90-136.el6.x86_64                  4/11
  Verifying  : 1:perl-Pod-Escapes-1.04-136.el6.x86_64                       5/11
  Verifying  : 4:perl-5.10.1-136.el6.x86_64                                 6/11
  Verifying  : 2:vim-common-7.2.411-1.8.el6.x86_64                          7/11
  Verifying  : 4:perl-libs-5.10.1-136.el6.x86_64                            8/11
  Verifying  : 1:perl-Pod-Simple-3.13-136.el6.x86_64                        9/11
  Verifying  : 3:perl-version-0.77-136.el6.x86_64                          10/11
  Verifying  : gpm-libs-1.20.6-12.el6.x86_64                               11/11

Installed:
  dhcp.x86_64 12:4.1.1-38.P1.el6.centos  vim-enhanced.x86_64 2:7.2.411-1.8.el6

Dependency Installed:
  gpm-libs.x86_64 0:1.20.6-12.el6
  perl.x86_64 4:5.10.1-136.el6
  perl-Module-Pluggable.x86_64 1:3.90-136.el6
  perl-Pod-Escapes.x86_64 1:1.04-136.el6
  perl-Pod-Simple.x86_64 1:3.13-136.el6
  perl-libs.x86_64 4:5.10.1-136.el6
  perl-version.x86_64 3:0.77-136.el6
  portreserve.x86_64 0:0.0.4-9.el6
  vim-common.x86_64 2:7.2.411-1.8.el6

Complete!
[root@localhost yum.repos.d]# _
```

```
# This declaration allows BOOTP clients to get dynamic addresses,
# which we don't really recommend.

subnet 10.254.239.32 netmask 255.255.255.224 {
  range dynamic-bootp 10.254.239.40 10.254.239.60;
  option broadcast-address 10.254.239.31;
  option routers rtr-239-32-1.example.org;
}

# A slightly different configuration for an internal subnet.
subnet 10.100.100.0 netmask 255.255.255.0 {
  range 10.100.100.2 10.100.100.5;
  option domain-name-servers dns.jnds.net;
  option domain-name "10.100.100.100";
  option routers 10.100.100.254;
  option broadcast-address 10.100.100.254;
  default-lease-time 172800;
  max-lease-time 259201;
}

# Hosts which require special configuration options can be listed in
# host statements.   If no address is specified, the address will be
# allocated dynamically (if possible), but the host-specific information
# will still come from the host declaration.
                                                              54,23         45%
```

```
[root@localhost dhcp]# chkconfig dhcpd on
```

2、在此服务器上以 YUM 方式安装 FTP 服务，并将比赛提供的 CentOS 光盘内容完整拷贝至 FTP 公共目录下，开启 FTP 服务的匿名上传及写入权限，最终设置 FTP 服务为开机自动运行；

```
[root@localhost dhcp]# yum install vsftpd -y
```

```
[root@localhost cdrom]# cp -p /dev/cdrom /var/ftp/
```

```
anonymous_enable=YES
anon_upload_enable=YES
#
# Uncomment this if you want the anonymous FTP user to be able to create
# new directories.
anon_mkdir_write_enable=YES
```

```
[root@localhost vsftpd]# chkconfig vsftpd on
```

3、通过 createrepo 命令对 FTP 主目录下的光盘内容进行关联性重建；

```
[root@localhost cdrom]# createrepo /var/ftp/

Saving Primary metadata
Saving file lists metadata
Saving other metadata
Generating sqlite DBs
Sqlite DBs complete
```

4、在此服务器上以 YUM 方式安装 TFTP 服务，并将服务根目录设置为/tftpboot,

最终设置 TFTP 服务为开机自动运行；

```
# default: off
# description: The tftp server serves files using the trivial file transfer \
#       protocol.  The tftp protocol is often used to boot diskless \
#       workstations, download configuration files to network-aware printers, \
#       and to start the installation process for some operating systems.
service tftp
{
        socket_type             = dgram
        protocol                = udp
        wait                    = yes
        user                    = root
        server                  = /usr/sbin/in.tftpd
        server_args             = -s /tftpboot
        disable                 = yes
        per_source              = 11
        cps                     = 100 2
        flags                   = IPv4
}
```

```
[root@localhost xinetd.d]# chkconfig tftp on
```

二、在 Server 2 上完成如下操作：

（一）完成虚拟主机的创建

1、 安装虚拟机“Centos-B1”,具体要求为内存 512MB，硬盘 10GB；

（二）在主机 Centos-B1 中完成磁盘管理的部署

1、关闭虚拟机的前提下在“Centos-B1”中手动再添加两块硬盘（SCSI 类型），容量均为 8G，分别将两块硬盘设置为一个主分区（2G 容量）和两个逻辑分区（分别 2G 容量），并完成 PV 物理卷的初始化操作；

```
Command (m for help): p

Disk /dev/sdb: 8589 MB, 8589934592 bytes
255 heads, 63 sectors/track, 1044 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x775547c0

   Device Boot      Start         End      Blocks   Id  System
/dev/sdb1               1         262     2104483+  8e  Linux LVM
/dev/sdb2             263         785     4200997+   5  Extended
/dev/sdb5             263         524     2104483+  8e  Linux LVM
/dev/sdb6             525         785     2096451   8e  Linux LVM
```

```
Command (m for help): p

Disk /dev/sdc: 8589 MB, 8589934592 bytes
255 heads, 63 sectors/track, 1044 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x5864d6f8

   Device Boot      Start         End      Blocks   Id  System
/dev/sdc1               1         262     2104483+  8e  Linux LVM
/dev/sdc2             263         785     4200997+   5  Extended
/dev/sdc5             263         524     2104483+  8e  Linux LVM
/dev/sdc6             525         785     2096451   8e  Linux LVM

Command (m for help): _
```

```
[root@localhost ~]# pvcreate /dev/sdb1 /dev/sdb5 /dev/sdb6 /dev/sdc1 /dev/sdc5 /
dev/sdc6
  Physical volume "/dev/sdb1" successfully created
  Physical volume "/dev/sdb5" successfully created
  Physical volume "/dev/sdb6" successfully created
  Physical volume "/dev/sdc1" successfully created
  Physical volume "/dev/sdc5" successfully created
  Physical volume "/dev/sdc6" successfully created
[root@localhost ~]# _
```

2、 将/dev/sdb1 及/dev/sdc5 加入到卷组 VG1 中，其显示的逻辑卷名称为 LV1，格式化为 ext3 文件系统，对应挂载目录为/volume，并针对/volume 目录实现开机自动挂载；

```
[root@localhost ~]# vgcreate VG1 /dev/sdb1 /dev/sdc5
  Volume group "VG1" successfully created
[root@localhost ~]# lvcreate -L +4G -n LV1 VG1
  Logical volume "LV1" created
[root@localhost ~]# mkfs -t ext3 /dev/VG1/LV1
```

```
[root@localhost ~]# mkdir /volume
[root@localhost ~]# mount /dev/VG1/LV1 /volume/
```

```
#
# /etc/fstab
# Created by anaconda on Tue May 10 02:19:28 2016
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
/dev/mapper/VolGroup-lv_root /                       ext4    defaults        1 1
UUID=49ce958c-93B1-4c58-ada3-8149c1372da1 /boot                   ext4    defaul
ts        1 2
/dev/mapper/VolGroup-lv_swap swap                    swap    defaults        0 0
tmpfs                   /dev/shm                tmpfs   defaults        0 0
devpts                  /dev/pts                devpts  gid=5,mode=620  0 0
sysfs                   /sys                    sysfs   defaults        0 0
proc                    /proc                   proc    defaults        0 0
/dev/VG1/LV1            /volume                 ext3    defaults        0 0_
```

3、 针对现有的逻辑卷/dev/vg1/lv1 实现在线扩容，将/dev/sdb5 分区加入到

已有的逻辑卷 LV1 中，实现目录/volume 在线扩容 2G 容量，总容量达到 6G；

```
[root@localhost etc]# vgextend VG1 /dev/sdb5
  Volume group "VG1" successfully extended
[root@localhost etc]# lvresize -L +2G /dev/VG1/LV1
  Extending logical volume LV1 to 6.00 GiB
  Logical volume LV1 successfully resized
```

```
[root@localhost etc]# resize2fs /dev/VG1/LV1
resize2fs 1.41.12 (17-May-2010)
Filesystem at /dev/VG1/LV1 is mounted on /volume; on-line resizing required
old desc_blocks = 1, new_desc_blocks = 1
Performing an on-line resize of /dev/VG1/LV1 to 1572864 (4k) blocks.

The filesystem on /dev/VG1/LV1 is now 1572864 blocks long.

[root@localhost etc]#
[root@localhost etc]# df -h
Filesystem                      Size  Used Avail Use% Mounted on
/dev/mapper/VolGroup-lv_root    8.5G  865M  7.2G  11% /
tmpfs                           246M     0  246M   0% /dev/shm
/dev/sda1                       485M   33M  427M   8% /boot
/dev/sr0                        4.2G  4.2G     0 100% /mnt/cdrom
/dev/mapper/VG1-LV1             6.0G  137M  5.5G   3% /volume
```

4、利用分区/dev/sdb6 及/dev/sdc1 完成条带卷的设置，条带容量为 8KB，建立的条带卷容量为 2G，卷组名称 VG1，条带卷名称为 stripe1；

```
[root@localhost etc]# vgextend VG1 /dev/sdb6 /dev/sdc1
  Volume group "VG1" successfully extended
[root@localhost etc]# lvcreate -i 2 -I 8 -L 2G -n stripe1 VG1
  Logical volume "stripe1" created
```

5、利用分区/dev/sdc6、/dev/sdb6 及/dev/sdc1 完成条带卷的设置，条带容量为 64KB，建立的条带卷容量为 3G，卷组名称 VG1，条带卷名称为 stripe2；

```
[root@localhost etc]# vgextend VG1 /dev/sdc6
  Volume group "VG1" successfully extended
[root@localhost etc]# lvcreate -i 3 -I 64 -L 3G -n stripe2 VG1
  Logical volume "stripe2" created
[root@localhost etc]# _
```

6、借助命令 hdparm 完成磁盘读写速度的测试，具体命令语法为“hdparm -t 逻辑卷名称”，并将截图放置到 hdparm.jpg

```
[root@localhost etc]# hdparm -t /dev/VG1/LV1

/dev/VG1/LV1:
 Timing buffered disk reads: ^[[1028 MB in  3.00 seconds = 342.29 MB/sec
[root@localhost etc]# hdparm -t /dev/
Display all 192 possibilities? (y or n)
[root@localhost etc]# hdparm -t /dev/VG1/stripe1

/dev/VG1/stripe1:
 Timing buffered disk reads: 948 MB in  3.00 seconds = 315.64 MB/sec
[root@localhost etc]# hdparm -t /dev/VG1/stripe2

/dev/VG1/stripe2:
 Timing buffered disk reads: 1522 MB in  3.00 seconds = 506.88 MB/sec
[root@localhost etc]#
```

（三）在主机 **Centos-B1** 中完成 **FTP** 服务器的部署

1、配置多站点 FTP 服务，创设三个 FTP 服务站点，域名分别为 ftp.jnds.net、ftp1.jnds.net 以及 ftp2.jnds.net，除站点 ftp.jnds.net 采用默认配置外，其余站点配置文件名分别为 vsftpd1.conf 以及 vsftpd2.conf，站点主目录分别为 /var/ftp1 以及 /var/ftp2；

```
[root@localhost vsftpd]# cp -p vsftpd.conf vsftpd2.conf
[root@localhost vsftpd]# ls
ftpusers   vsftpd1.conf  vsftpd.conf
user_list  vsftpd2.conf  vsftpd_conf_migrate.sh
[root@localhost vsftpd]# _
```

```
#chroot_list_file=/etc/vsftpd/chroot_list
#
# You may activate the "-R" option to the builtin ls. This is disabled by
# default to avoid remote users being able to cause excessive I/O on large
# sites. However, some broken FTP clients such as "ncftp" and "mirror" assume
# the presence of the "-R" option, so there is a strong case for enabling it.
#ls_recurse_enable=YES
#
# When "listen" directive is enabled, vsftpd runs in standalone mode and
# listens on IPv4 sockets. This directive cannot be used in conjunction
# with the listen_ipv6 directive.
listen=YES
#
# This directive enables listening on IPv6 sockets. To listen on IPv4 and IPv6
# sockets, you must run two copies of vsftpd with two configuration files.
# Make sure, that one of the listen options is commented !!
#listen_ipv6=YES

pam_service_name=vsftpd
userlist_enable=YES
tcp_wrappers=YES
listen_address=10.100.100.104
local_root=/var/ftp1_

-- INSERT --                                                  121,21        Bot
```

```
#chroot_list_file=/etc/vsftpd/chroot_list
#
# You may activate the "-R" option to the builtin ls. This is disabled by
# default to avoid remote users being able to cause excessive I/O on large
# sites. However, some broken FTP clients such as "ncftp" and "mirror" assume
# the presence of the "-R" option, so there is a strong case for enabling it.
userlist_enable=YES
tcp_wrappers=YES
listen_address=10.100.100.105
local_root=/var/ftp2
~
~
```

2、在站点 ftp.jnds.net 中，建立用户 ftpuser1 及 ftpuser2，使得两个用户登录后的主目录是各自家目录，并将两用户限制在监牢（chroot）中

```
[root@localhost yum.repos.d]#
[root@localhost yum.repos.d]# useradd -d /home/ftpuser1 ftpuser1
[root@localhost yum.repos.d]# useradd -d /home/ftpuser2 ftpuser2
[root@localhost yum.repos.d]# _
```

```
# the presence of the "-R" option, so there is a strong case for enabling it.
#ls_recurse_enable=YES
#
# When "listen" directive is enabled, vsftpd runs in standalone mode and
# listens on IPv4 sockets. This directive cannot be used in conjunction
# with the listen_ipv6 directive.
listen=YES
#
# This directive enables listening on IPv6 sockets. To listen on IPv4 and IPv6
# sockets, you must run two copies of vsftpd with two configuration files.
# Make sure, that one of the listen options is commented !!
#listen_ipv6=YES

pam_service_name=vsftpd
userlist_enable=YES
tcp_wrappers=YES
listen_address=10.100.100.104
local_root=/var/ftp1
chroot_local_user=YES
```

3、在站点 ftp1.jnds.net 中，建立本地用户 ftpuser3 及 ftpuser4，两个用户共用同一个主目录，并在主目录中具备上传及下载权限。

```
[root@localhost vuser]# useradd ftpuser3
[root@localhost vuser]# useradd ftpuser4
```

```
listen_address=10.1.100.105
local_root=/var/ftp1
write_enable=YES_
```

4、在站点 ftp2.jnds.net 中，借助自签名证书完成 ftps 服务的配置，结合 ssl 实现安全传输，服务证书名为 vsftpd.pem，服务私钥名为 ftpssl.pem，证书有效期为 100 天 ；

```
[root@localhost certs]# openssl x509 -days 100 -req -in ftpssl.csr -signkey ftps
sl.pem -out vsftpd.pem
Signature ok
subject=/C=XX/L=Default City/O=Default Company Ltd
Getting Private key
[root@localhost certs]# _
```

三、在 Server 3 上完成如下操作：

（一）完成虚拟主机的创建

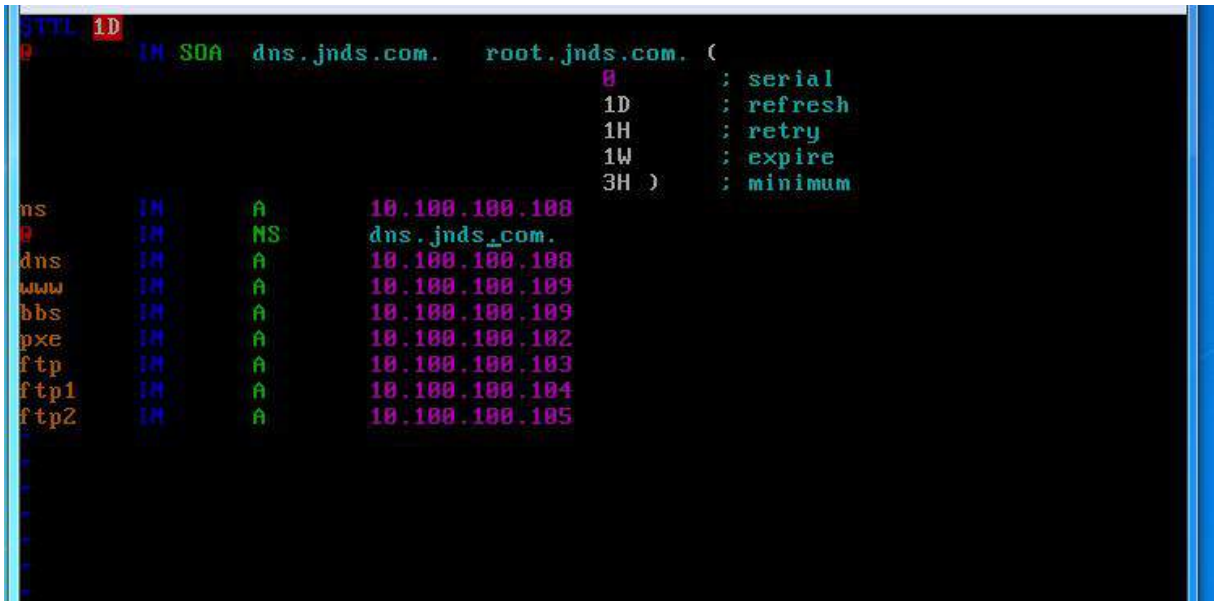
1、安装名为“Centos-C1”的虚拟机，具体要求为硬盘大小为 12GB，内存为 768MB，系统为 Centos6.5。分区大小为：SWAP 分区大小为 512M；/boot 分区大小为 500M，文件类型为 ext3；/home 分区大小为 1G，文件类型为 ext3，其余为/分

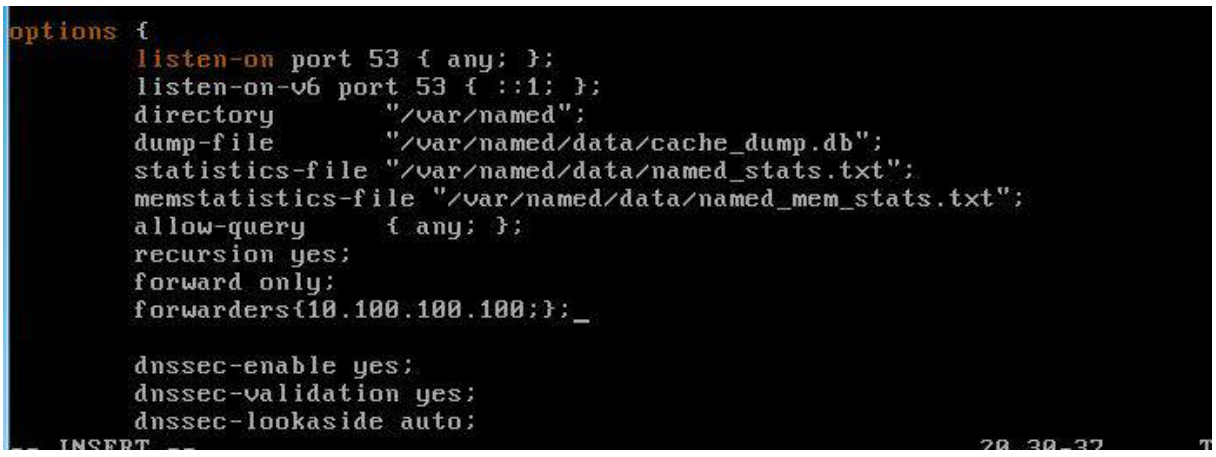
区，文件类型为 ext3；

（二）在主机 Centos-C1 中完成 BIND 域名服务器以及代理服务器的部署

1、在此服务器中安装配置 bind 服务，负责区域“jnds.net”内主机解析，五台主

机分别为 dns.jnds.net 、www.jnds.net、bbs.jnds.net、pxe.jnds.net、ftp.jnds.net、ftp1.jnds.net、ftp2.jnds.net ,做好正反向 DNS 服务解析，对访问 chinaskills.com 域的解析转发给 win2003_A1；





2、安装并完成代理服务器 squid 的初始配置，使用 8080 作为代理服务端口，指

定 DNS 服务器 IP 地址信息，使得 squid 服务器能够解析域名；

3、设置 squid 代理服务器采用 ufs 缓存机制，缓存目录设置为/cache,目录容量为 5GB，L1 及 L2 级目录数量分别为 16 及 256，定义高缓存值为 512MB；

4、针对主机 10.100.100.109/24 提供代理服务，为缓解请求队列忙碌，设置重定向器池进程数为 20，并将缓存日志存放于/var/squid/cache.log 中；

四、在 Server 4 上完成如下操作：

（一）完成虚拟主机的创建

1、Server4 主机系统需借助指定光盘安装 CentOS6.5，并在此 Linux 平台上采用 KVM 方式安装虚拟机“Centos-D1”，具体要求为硬盘大小为 12GB，内存为 768MB，系统为 CentOS6.5；（小提示：如无法正确安装虚拟机 Centos-D1，下述题目中所涉及的虚拟机题目可在 Server4 真实主机中完成）

（二）在主机 Centos-D1 中完成 Apache 服务器以及 MySQL 数据库服务器的部署

1、在此服务器中安装 httpd 服务，建立站点 www.jnds.net，其网站主目录为/var/www/html，首页内容为“chinaskills’ s website” ；

```
# This can often be determined automatically, but we recommend you specify
# it explicitly to prevent problems during startup.
#
# If this is not set to valid DNS name for your host, server-generated
# redirections will not work.   See also the UseCanonicalName directive.
#
# If your host doesn't have a registered DNS name, enter its IP address here.
# You will have to access it by its address anyway, and this will make
# redirections work in a sensible way.
#
ServerName www.jnds.net:80

#
# UseCanonicalName: Determines how Apache constructs self-referencing
# URLs and the SERVER_NAME and SERVER_PORT variables.
# When set "Off", Apache will use the Hostname and Port supplied
# by the client.   When set "On", Apache will use the value of the
# ServerName directive.
#
UseCanonicalName Off

#
# DocumentRoot: The directory out of which you will serve your
# documents. By default, all requests are taken from this directory, but
# symbolic links and aliases may be used to point to other locations.
#
DocumentRoot "/var/www/html"
```

2、使用 openssl 申请证书，创建自签名证书 server.crt 和私钥 server.key，要求只允许使用域名通过 SSL 加密访问；

```
[root@localhost certs]# ls
ca-bundle.crt        localhost.crt    Makefile          server.crt  server.key
ca-bundle.trust.crt  make-dummy-cert  renew-dummy-cert  server.csr
[root@localhost certs]#
```

3、将此服务器配置为 MYSQL 服务器，创建数据库为 userdatabase，在库中创建表为 username，在表中创建 5 个用户，分别为 myuser1、myuser2、myuser3、myuser4、myuser5，口令与用户名相同，需要对登录网站的用户进行身份验证，表结构如下；

字段名	数据类型	主键	自增
ID	int	是	是
name	varchar(10)	否	否
birthday	datetime	否	否
sex	char(1)	否	否
Password	Char（8）	否	否

```
mysql> create database userdatabase;
Query OK, 1 row affected (0.00 sec)

mysql> use userdatabase
Database changed
mysql> create table username(
    -> ID int primary key auto_increment,
    -> name varchar(10),
    -> birthday datetime,
    -> sex char(1),
    -> Password char(8));
Query OK, 0 rows affected (0.04 sec)

mysql> desc username;
+----------+-------------+------+-----+---------+----------------+
| Field    | Type        | Null | Key | Default | Extra          |
+----------+-------------+------+-----+---------+----------------+
| ID       | int(11)     | NO   | PRI | NULL    | auto_increment |
| name     | varchar(10) | YES  |     | NULL    |                |
| birthday | datetime    | YES  |     | NULL    |                |
| sex      | char(1)     | YES  |     | NULL    |                |
| Password | char(8)     | YES  |     | NULL    |                |
+----------+-------------+------+-----+---------+----------------+
5 rows in set (0.00 sec)
```

```
mysql> insert into username(name,Password)value("myuser1",password("myuser1"));
Query OK, 1 row affected, 1 warning (0.00 sec)

mysql> insert into username(name,Password)value("myuser2",password("myuser2"));
Query OK, 1 row affected, 1 warning (0.00 sec)

mysql> insert into username(name,Password)value("myuser4",password("myuser3"));
Query OK, 1 row affected, 1 warning (0.00 sec)

mysql> insert into username(name,Password)value("myuser4",password("myuser4"));
Query OK, 1 row affected, 1 warning (0.00 sec)

mysql> insert into username(name,Password)value("myuser5",password("myuser5"));
Query OK, 1 row affected, 1 warning (0.00 sec)

mysql> select * from username;
+----+---------+----------+------+----------+
| ID | name    | birthday | sex  | Password |
+----+---------+----------+------+----------+
|  1 | myuser1 | NULL     | NULL | *A8866F0 |
|  2 | myuser2 | NULL     | NULL | *05BB382 |
|  3 | myuser4 | NULL     | NULL | *19F17B0 |
|  4 | myuser4 | NULL     | NULL | *0AEDED0 |
|  5 | myuser5 | NULL     | NULL | *F7AE551 |
+----+---------+----------+------+----------+
5 rows in set (0.00 sec)
```

4、在服务器端使用 iptables 设置防火墙功能,只允许用户访问这台服务器的 WWW 服务，而服务器只能被动地接受连接请求，不能主动的发起连接；

```
[root@localhost certs]# iptables -P OUTPUT DROP
[root@localhost certs]# iptables -I OUTPUT 1 -p tcp -m state --state=RELATED,ESTABLISHED --sport 80 -j ACCEPT
[root@localhost certs]# iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:22
REJECT     all  --  0.0.0.0/0            0.0.0.0/0           reject-with icmp-host-prohibited

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
REJECT     all  --  0.0.0.0/0            0.0.0.0/0           reject-with icmp-host-prohibited

Chain OUTPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED tcp spt:80
[root@localhost certs]#
```

2015 年全国职业院校技能大赛

网络搭建与应用竞赛

（总分 1000 分）

赛题说明

一、竞赛内容分布

“网络搭建与应用”竞赛共分二个部分，其中：

第一部分：网络搭建及安全部署项目，占总分的比例为 45%；

第二部分：服务器配置及应用项目，占总分的比例为 55%；

二、竞赛注意事项

（1）禁止携带和使用移动存储设备、计算器、通信工具及参考资料。

（2）请根据大赛所提供的比赛环境，检查所列的硬件设备、软件清单、材料清单是否齐全，计算机设备是否能正常使用。

（3）本试卷共有两个部分。请选手仔细阅读比赛试卷，按照试卷要求完成各项操作。

（4）操作过程中，需要及时保存设备配置。比赛结束后，所有设备保持运行状态，不要拆、动硬件连接。

（5）比赛完成后，比赛设备、软件和赛题请保留在座位上，禁止将比赛所用的所有物品（包括试卷和草纸）带离赛场。

（6）所有需要提交的文档均放置在桌面的 PC1“比赛文档”文件夹中，禁止在纸质资料上填写与竞赛无关的标记，如违反规定，可视为 0 分。

（7）裁判以各参赛队提交的竞赛结果文档为主要评分依据。所有提交的文档必须按照赛题所规定的命名规则命名，文档中有对应题目的小标题，截图有截图的简要说明，否则按无效内容处理。

（8）与比赛相关的工具软件放置在 D 盘的 tools 文件夹中。

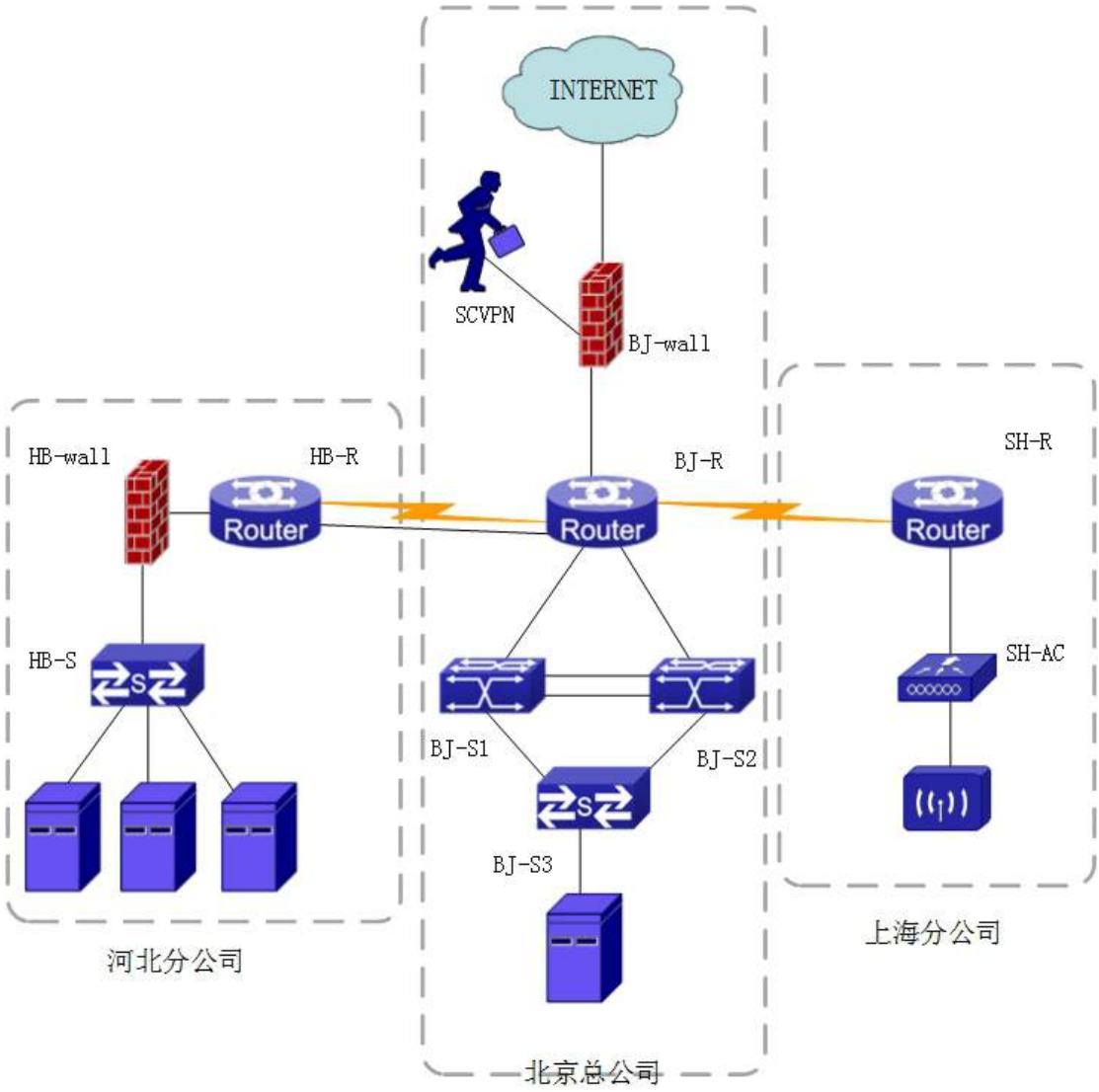


表 1 网络设备连接表

A 设备连接至 B 设备			
设备名称	接口	设备名称	接口
BJ-R	GigaEthernet0/4	BJ-wall1	Ethernet0/4
BJ-R	GigaEthernet 0/3	HB-R	GigaEthernet 0/3
BJ-R	Serial0/1	HB-R	Serial0/2
BJ-R	Serial0/2	SH-R	Serial0/1
BJ-R	GigaEthernet0/5	BJ-S1	Ethernet1/0/22
BJ-R	GigaEthernet 0/6	BJ-S2	Ethernet1/0/22
BJ-S1	Ethernet1/0/23	BJ-S2	Ethernet1/0/23
BJ-S1	Ethernet1/0/24	BJ-S2	Ethernet1/0/24
BJ-S1	Ethernet1/0/21	BJ-S3	Ethernet1/24
BJ-S2	Ethernet1/0/21	BJ-S3	Ethernet1/23
HB-R	GigaEthernet 0/4	HB-wall	Ethernet0/4
HB-wall	Ethernet0/3	HB-S	Ethernet1/24

SH-R	GigaEthernet 0/4	SH-AC	ethernet 1/0/24
SH-AC	ethernet 1/0/23	SH-AP	LAN
Server1	NIC	HB-S	Ethernet1/0/10
Server 2	NIC	HB-S	Ethernet1/0/11
Server 3	NIC	HB-S	Ethernet1/0/12
Server4	NIC	BJ-S3	Ethernet1/0/24

表 2 网络设备 IP 地址分配表

设备	设备名称	设备接口	IP 地址
路由器	BJ-R	GigaEthernet 0/3	
		GigaEthernet0/4	
		GigaEthernet0/5	
		GigaEthernet0/6	
		Serial0/1	
		Serial0/2	
	HB-R	GigaEthernet 0/3	
		GigaEthernet 0/4	
		Serial0/2	
	SH-R	GigaEthernet 0/4	
		Serial0/1	
三层交换机	BJ-S1	VLAN200 (Ethernet1/0/22)	
	BJ-S2	VLAN200 (Ethernet1/0/22)	
防火墙 1	BJ-wall	Loopback0	67.8.9.1/28
		Ethernet 0/4	
防火墙 2	HB-wall	Ethernet 0/3	
		Ethernet 0/4	
无线控制器	SH-AC	vlan 200 (Ethernet1/0/24)	
		Vlan 10	
		Vlan 20	

表 3：服务器 IP 地址分配表

宿主机	虚拟主机名称	域名信息	服务角色	系统及版本信息	IPv4 地址信息
Server 1	Win2008-A1	dc.chinaskills.com	域控制器 DNS 服务器 CA 证书服务器	Windows Server 2008 R2	IP: 10.100.100.100

	Win2003-A1	mail.chinaskills.com	邮件、DFS 服务器	Windows Server 2003 R2	IP: 10.100.100.101
	Centos-A1	mail.jnds.net	邮件服务器和 LVM	Centos 6.5	IP: 10.100.100.102
Server 2	Win2008-B1	dc.nvsc.com	域控制器 DNS 服务器	Windows Server 2008 R2	IP: 10.100.100.150
	Win2008-B2	dfs. nvsc.com	Web、dfs 服务器	Windows Server 2008 R2	IP: 10.100.100.103
	Centos-B1	www1.jnds.net	Web 服务器	Centos 6.5	IP: 10.100.100.104 IP: 10.100.100.159
	Centos-B2	ssh.jnds.net	SSH、TFTP 服务器	Centos 6.5	IP: 10.100.100.106
Server 3	Win2008-C1	ftp.chinaskills.com	ftp、nfs 服务器	Windows Server 2008 R2	IP: 10.100.100.160
	Centos-C1	www2.jnds.net	Web、ca 及负载均衡	Centos 6.5	IP: 10.100.100.105 IP: 10.100.100.160
	Centos-C2	dns.jnds.net ftp.jnds.net	BIND、FTP 服务器	Centos 6.5	IP: 10.100.100.109
Server 4 (Linux 虚拟化主机)	Centos-D1	www.jnds.net bbs.jnds.net	Apache web 服务器 MySQL 数据库服务器	Centos 6.5	IP: 10.100.100.110

网络搭建部分(450 分)

【注意事项】

1、设备 console 线有两条。交换机， AC，防火墙使用同一条 console 线，路由器使用另外一条 console 线。

2、设备配置完毕后，保存最新的设备配置。保存文档方式分为两种：

a) 交换机和路由器要把 show running-config 的配置保存在 PC1 桌面的相应文档中，文档命名规则为：设备名称.doc,例如：RT1 路由器文件命名

为：RT1.doc，然后放入到 PC1 桌面上“比赛文档”文件夹中

b) 防火墙等截图方式的设备，把截图的图片放到同一 word 文档中，文档命名规则为：设备名称.doc,例如：防火墙 FW1 文件命名为：FW1.doc，保存后放入到 PC1 桌面上“比赛文档”文件夹中。

1、物理连接与 IP 地址划分

(1) 按照网络拓扑图制作以太网网线，并连接设备。要求符合 T568A 和 T568B 的标准，其线缆长度适中。

(2) 根据“拓扑结构图”和“表 2:网络设备 IP 地址分配表”所示，对网络中的所有设备接口配置 IP 地址。

总公司中整个网络互联地址规划使用 10.0.0.0/8 地址段，为了节省 IP 资源，做到合理分配，财务部有 16 名员工、工程部有 60 名员工、软件部和系统集成部两个部门都有 125 名员工，服务器的网段为 10.100.100.0/24。上海分公司使用 172.16.0.0/16 地址段,保证上海分公司行政部至少有 60 台主机，销售部至少有 40 台主机，河北分公司使用 192.168.1.0/24 网段，保证河北分公司行政部至少有 100 台主机，销售部至少有 40 台主机，后勤部至少 10 台主机。总公司与分公司所有设备互联地址使用/30 的掩码进行分配，并把地址填入上面网络设备 IP 地址分配表中的空白处。地址分配后把地址填入上面网络设备 IP 地址分配表中的空白处。

注意:

- 网关地址为网段的最后一个地址。
- Tunnel 的 IP 分配地址使用北京总公司的地址范围，请合理使用。

2、交换机配置

(1) 为交换机设备命名，命名规则参考为表 1 中的“设备名称”。

(2) 在两台三层交换设备上开启 SSH 管理功能，使用安全 IP 技术，只允许 10.100.100.11 主机对三层交换设备进行管理，能通过 CRT 软件进行登录，用户名为 dcn，口令为 2015ssh，enable 密码为 2015network。

(3) 依据“拓扑结构图”和下表，把相应端口加入到 vlan 中；

设备	VLAN 名称	VLAN ID	接口
BJ-S1	CAIWUBU	10	————
	GONGCHENGBU	20	————
	RUANJIANBU	30	————
	XITONGJICHENGBU	40	————
	Link_to_bj-1	200	Ethernet1/0/22
BJ-S2	CAIWUBU	10	————
	GONGCHENGBU	20	————
	RUANJIANBU	30	————
	XITONGJICHENGBU	40	————
	Link_to_bj-1	200	Ethernet1/0/22
BJ-S3	CAIWUBU	10	Ethernet1/1 - Ethernet1/5
	Market	20	Ethernet1/6 - Ethernet1/10
	Software	30	Ethernet1/11 - Ethernet1/15
	Renshibu	40	Ethernet1/16 - Ethernet1/20
HB-S1	Market	1	Ethernet1/1 - Ethernet1/5
	Software		Ethernet1/6 - Ethernet1/10
	Houqinbu		Ethernet1/11 - Ethernet1/15
SH-AC	Link_to_SH - R1	200	ethernet 1/0/24
	XINGZHENGBU	10	ethernet 1/0/5
	XIAOSHOUBU	20	ethernet 1/0/6

(4) 使用端口汇聚技术，将 BJ-RS1 三层交换机接口 ethernet 1/0/23 和 ethernet 1/0/24 与 BJ-S1 二层交换机接口 Ethernet1/23 和 Ethernet1/24 配置为端口汇聚，汇聚接口为动态方式，负载分担方式基于目的 IP 地址。

(5) 在总公司公司内网两台核心交换机之间做 VRRP，并使得 BJ-S1 为 vlan 10

的转发路由器。

(6) 在总公司内网的 BJ-S1、BJ-S2 和 BJ-S3 设置 MSTP，要求 BJ-S1 为 vlan 10 的根网桥，并实现 vlan 10 的数据通过左边链路进行访问。

(7) 公司为了统一管理，通过 SNMP 技术使用网管软件对 BJ-RS1 进行管理，配置只读字串为 public ，读写字串为 private，网管主机的地址为 10.100.100.10。

(8) 在北京总公司的接入交换机上 BJ-S2 上进行端口镜像，将 Ethernet1/0/2- Ethernet1/0/20 的数据流量转发到 Ethernet1/0/21 端口来实现对网络的监听。

(9) 在北京总公司的接入交换机上 BJ-S1 上的 Ethernet1/0/1 端口开启 ARP 的防护功能，防止 PC 机发出网关欺骗报文。

(10) 在总公司的网络中，在 BJ-S1 上 Ethernet1/4 接口上，要求 mac 为 00-FF-51-FD-AE-15 的主机不能访问财务部的主机 MAC 地址为：E0-94-67-05-5D-84，其余主机正常访问。

(11) 在北京总公司的接入交换机 BJ - S1 上通过交换机的端口安全对 Ethernet1/6 口进行 MAC 地址绑定 E0-94-67--5D-05-84，对 Ethernet1/7 进行设置，最多可以学习 5 个 MAC 地址，对于学习到更多的 MAC 地址时，直接进行丢弃且不产生通知。

(12) 在 BJ - S1 上实现禁止 VLAN40 网段的任何计算机通过 BT 下载和做 BT 种子，BT 常用端口范围 6881~6890。

3、路由器配置与调试

(1) 为路由设备命名，命名规则参考为表 1 中的“设备名称”。

(2) 在北京总公司网络中采用动态路由协议 RIPv2，根据“网络拓扑结构图”所示，通过配置实现网络的互通。

(3) 在河北分公司路由器上配置如下的 Loopback 接口，通过路由汇总功能来尽可能减少路由表的条目。

接口名称	IP 地址
Loopback0	1.1.1.1/24
Loopback1	1.1.2.1/24
Loopback2	1.1.3.1/24
Loopback3	1.1.4.1/24
Loopback4	1.1.5.1/24

(4) 在上海分公司与总公司之间采用 OSPF 动态路由协议，在 SH-AC 上使用 OSPF 技术保障网络正常通信。

(5) 在总公司与上海分公司的互联网出口设备上，需要将去往互联网的默认路由引入到动态路由中。

(6) 在 SH-R 上使用 QOS 进行流量整形 ，使其到北京总公司服务器网络的 CIR 为 80000 ， Excess Burst size 为 9000 ， Burst size 为 8000 ，超额的流量不需要做处理。

(7) 在河北分公司与总公司之间采用 OSPF 动态路由协议，保障网络正常通信。

(8) 在总公司的路由器上配置 SSH 功能，使得 Centos-B2 的 Linux 系统可以通过远程安全访问总公司的路由器，用户名为 ssh1，密码为口令为 2015ssh。

(9) 在总公司路由器上为内网出外网时设置 QOS ，分别为 vlan10 保留 20%的带宽 、vlan 20 30%的带宽、vlan30 为 800 Kbps 带宽。

4、广域网配置

(1) 北京总公司允许 VLAN10、VLAN20、VLAN30、VLAN40 的用户通过源 NAT 访问外网，类型为端口 NAT。使用外网口 IP 地址进行映射。

(2) 上海分公司通过外网口 IP 地址进行 NAT 映射，保证上海分公司可以正常访问互联网。

(3) 北京总公司与上海分公司之间申请串行链路专线 ，采用 PPP 封装，认证方式为先 chap 再 pap，用户名称为对端设备名称，密码：123456。

(4) 河北分公司与北京总公司之间采用双链路互联，实现链路的备份功能，在以太网链路出现故障时走上的串行线路。

5、防火墙配置

(1) 把防火墙进行设备命名，命名规则参考为表 1 中的“设备名称”。

(2) 在北京总公司出口防火墙 BJ-wall 上配置环回接口 Loopback0，用来模拟 Internet。

(3) 在北京总公司出口防火墙 BJ-wall 上配置 SSL 方式远程接入 VPN，允许远程办公用户可以访问服务群资源，其使用的合法用户名为 vpn1、vpn2、vpn3、vpn4、vpn5，其共同口令为 2015network，其拨入的计算获取的 IP 地址段为 10.0.10.10~10.0.10.20。

(4) 在总公司 BJ-wall 上设置关键词过滤，禁止办公室用户浏览在网页中出现“色情”一词超过三次或三次以上的网站。

(5) 在总公司 BJ-wall 上设置规则，不允许办公室用户登录 QQ。

(6) 在河北分公司的 HB-wall 和路由器之间通过使用 OSPF 协议，并对其进行认证，完成网络互通。

(7) 在河北分公司的 HB-wall 上配置防 DDOS 攻击，来保证分公司的网络安全

性。

(8) 为了保障网络资源合理使用，在总公司 BJ-wall 上配置禁止 VLAN10 和 VLAN30 网段所有 P2P 视频数据通过。每个用户的网络速率为上行最大 64K，下行最大 128K。

6、无线配置

(1) 把无线控制器进行设备命名，命名规则参考为表 1 中的“设备名称”。

(2) 无线控制器建立 2 个 SSID,SSID 分别为 sale1 和 sale2，sale2 的 SSID 设置为隐藏，工作信道为自动；使用无线控制器提供 DHCP 服务，获得 sale1 的地址在 vlan10 内，获得 sale2 的地址在 vlan20 内,用户动态分配 IP 地址和网关，DNS 地址为：202.106.0.20，其分配的地址段为自行计算，需要排除网关，地址租约为 2 天。用户接入无线网络时需要输入密码，加密模式为 wpa-personal,其口令为：chinaskill。

(3) 激活无线网络的二层隔离，实现同一个 AP 下无线局域网内用户不能互相访问。

(4) 保障无线信息的覆盖性，无线 AP 的发射功率设置为 80%。

(5) 为了控制带宽，保证正常使用，配置无线局域网用户上行速度为 2Mbps，下行速度为 4Mbps。

(6) 阻止 MAC 地址为 F0-DE-F1-F2-8C-CC 的主机连接上海分公司的无线。

Windows 操作系统

【说 明】

（1）题目中所涉及 Windows 操作系统的 administrator 管理员以及其他普通用户密码均为 2015Network_X（X 为组号），若未按照要求设置密码，涉及到该操作的所有分值记为 0 分。

（2）虚拟主机的 IP 属性设置请按照网络拓扑结构图以及“表 3：服务器 IP 地址分配表”的要求设定。

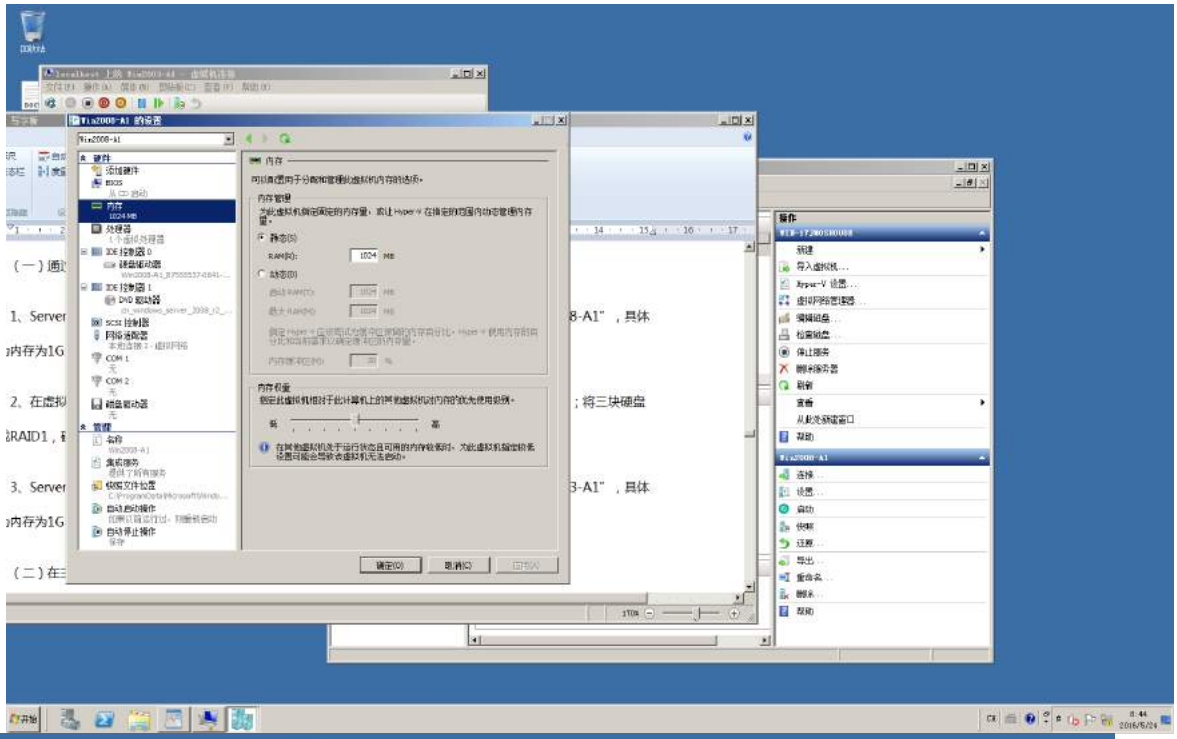
（3）所有系统镜像文件及试题所需的其它软件均存放在每台主机的 D:\soft 文件夹中，并将题目要求的截图内容以.jpg 格式存储于各物理机桌面 BACKUP_X（X 为组号）文件夹中，文件名、扩展名和存放位置错误，涉及到的所有操作分值记为 0 分。

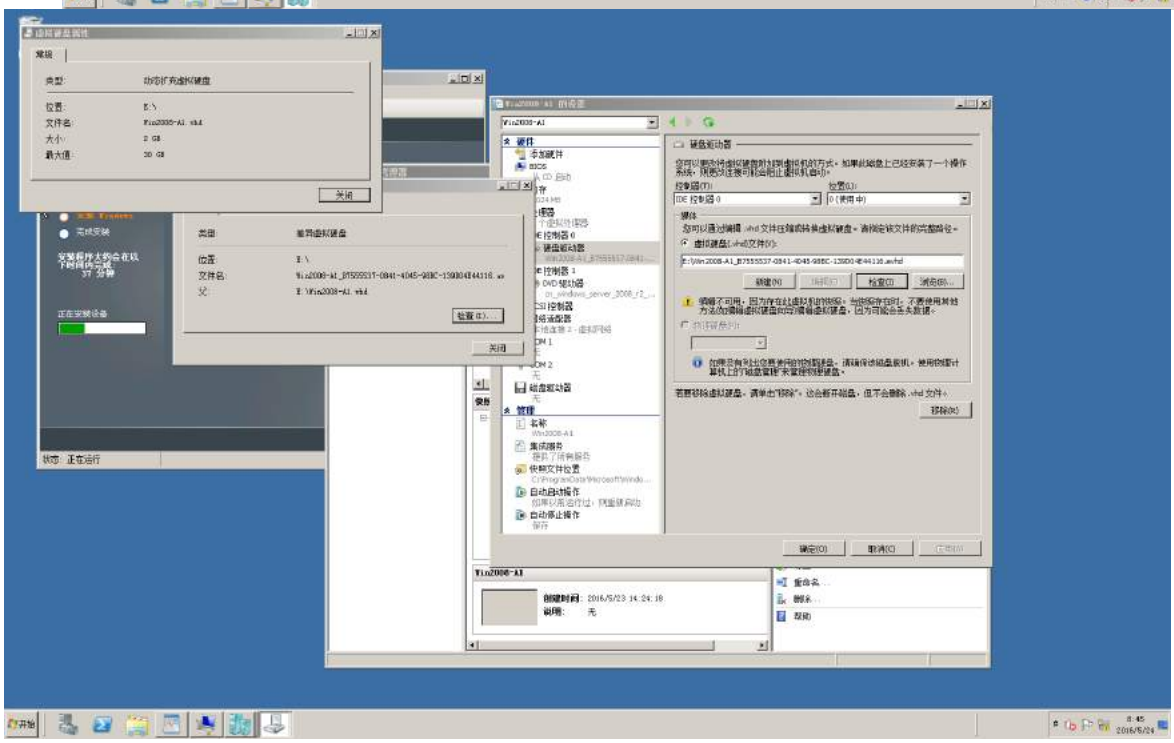
（4）题目要求的虚拟机均安装于每台主机的 D：\virtualPC 目录，即路径为 D：\virtualPC\虚拟主机名称。

一、在 Server 1 上完成如下操作:

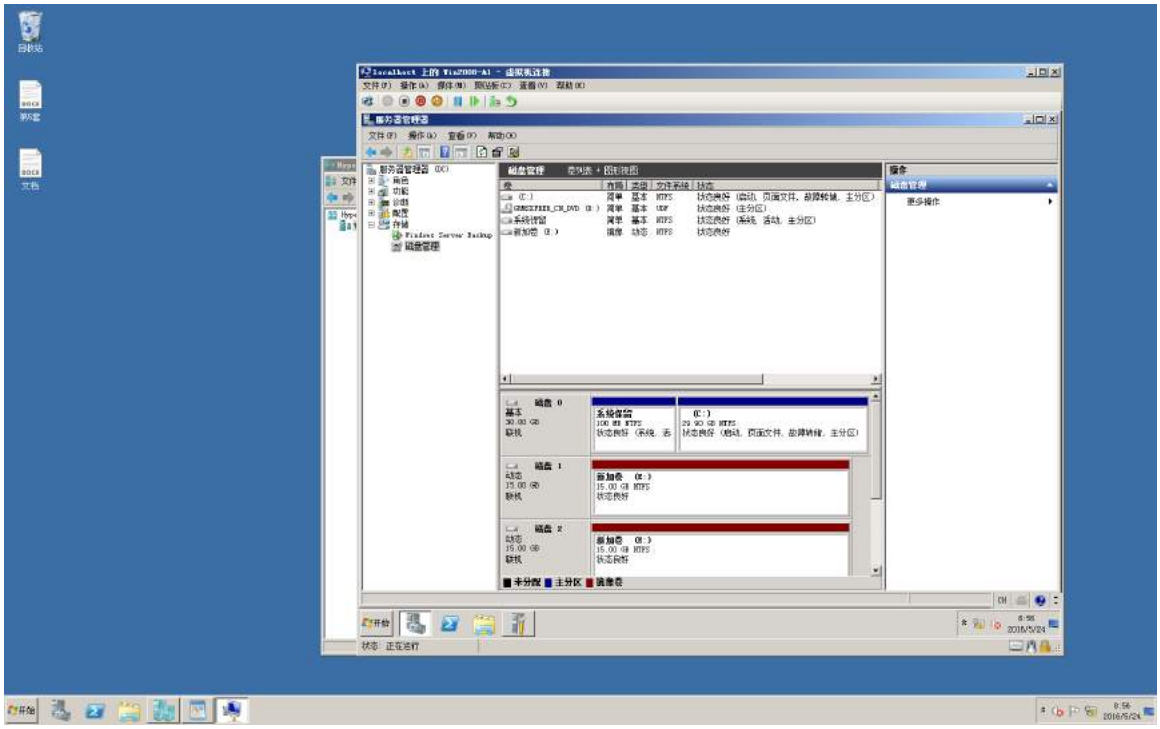
（一）通过 Hyper-V 完成虚拟主机的创建

1、Server1 主机系统为 Windows，需要在此 Windows 平台上采用 Hyper-V 方式安装虚拟机“Win2008-A1”，具体要求为内存为 1G，硬盘 30G；

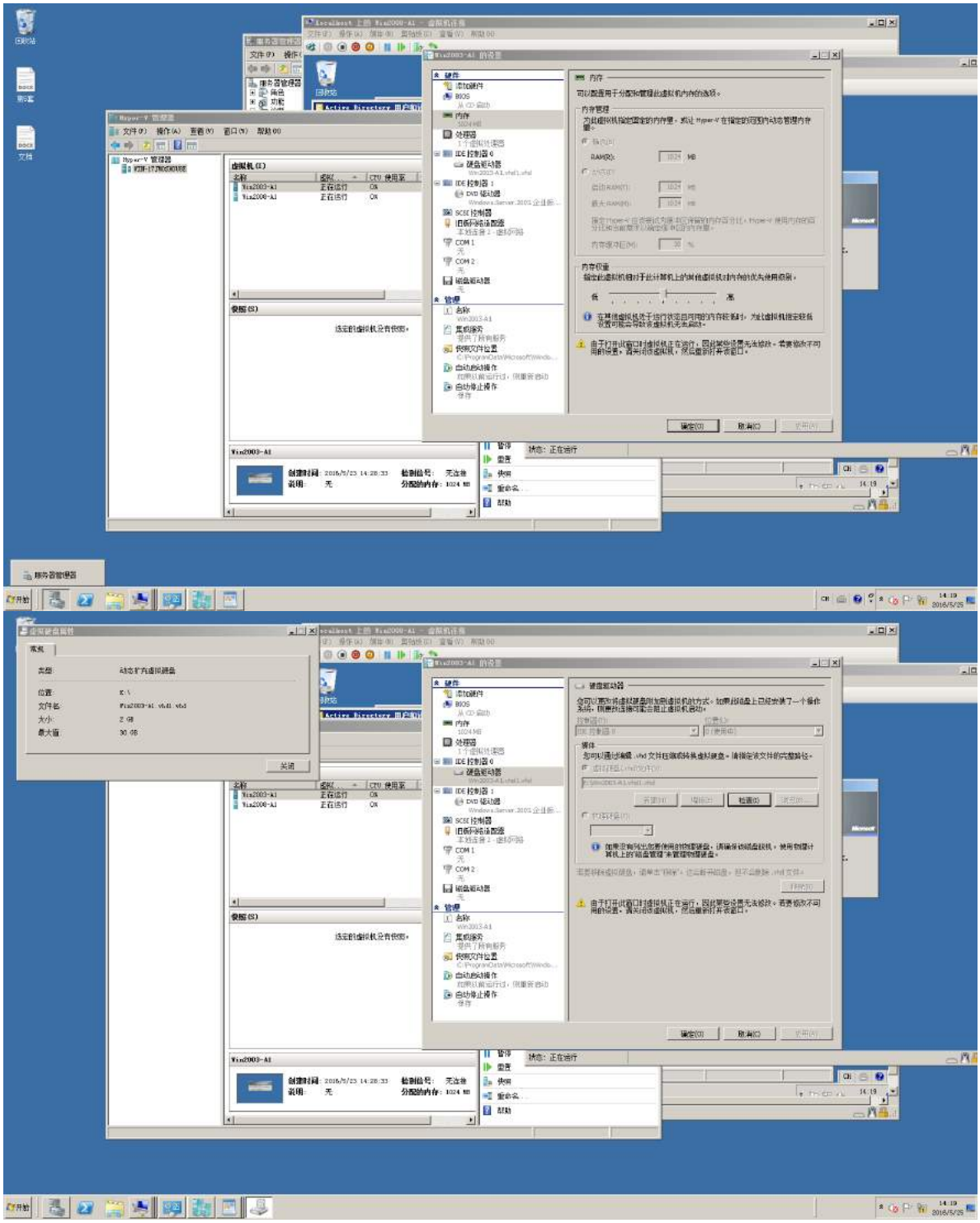




2、在虚拟机“Win2008-A1”中添加 SCSI 控制器，添加二块 SCSI 虚拟硬盘，其每块硬盘的大小为 15G；将三块硬盘制作成 RAID1，磁盘盘符为 e:\;

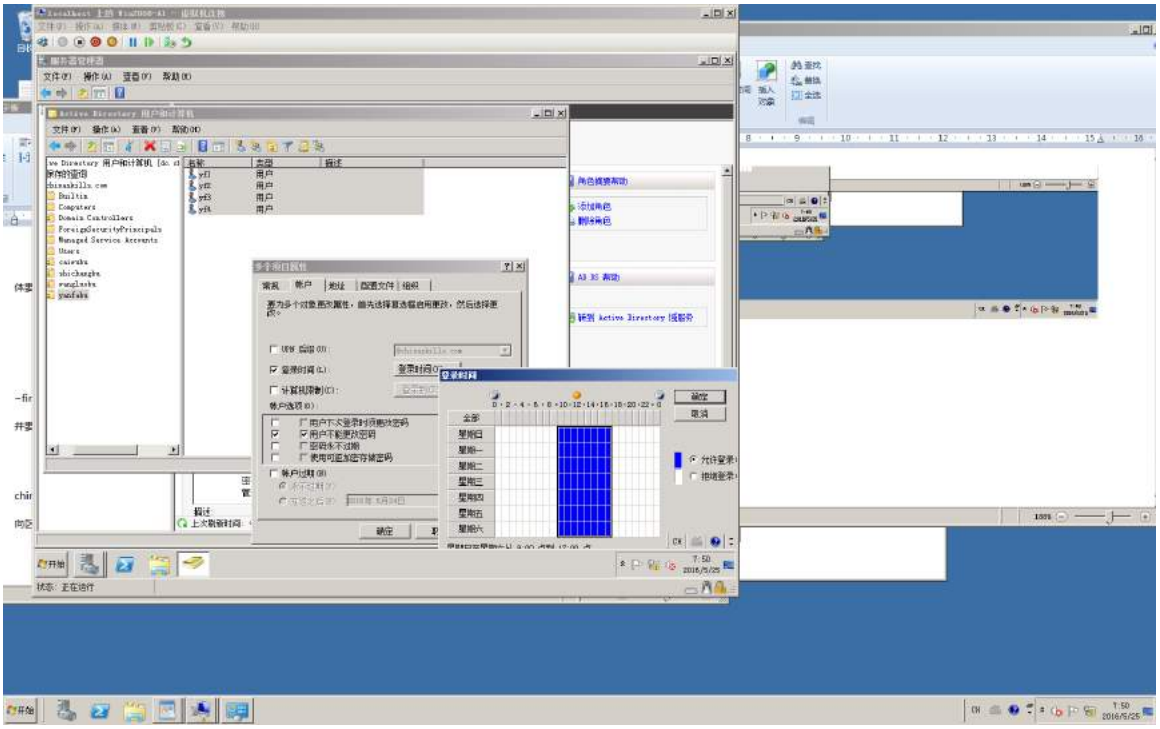


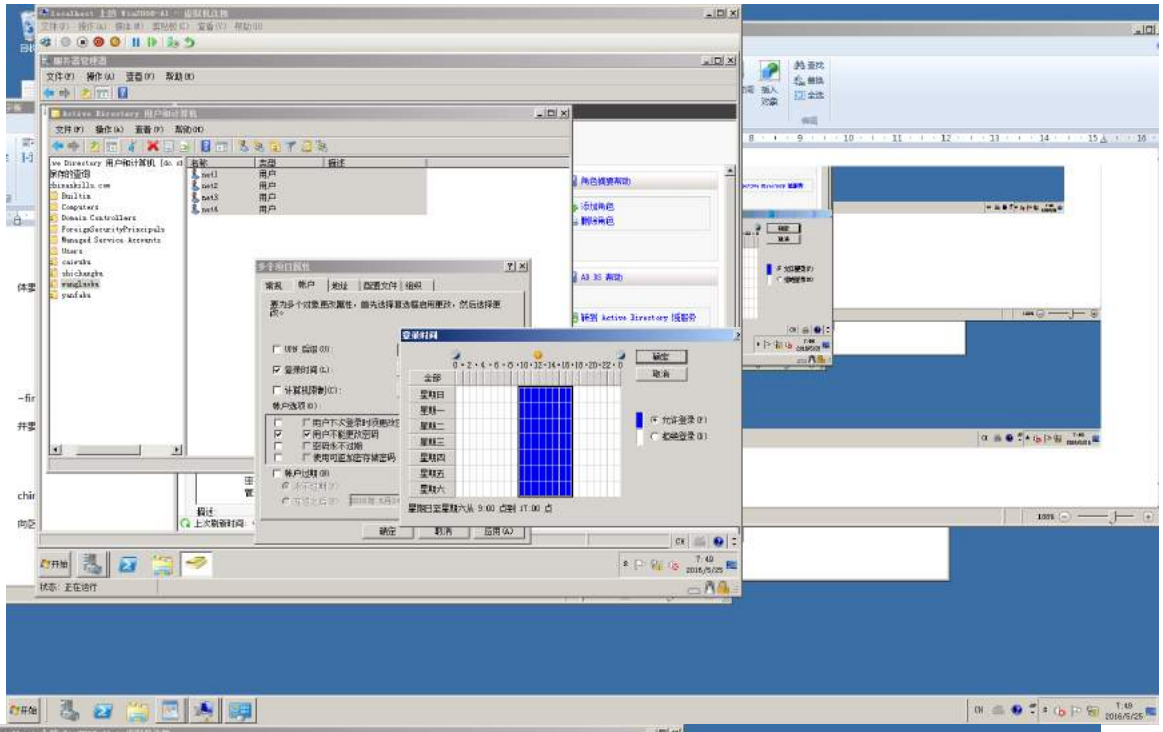
3、Server1 主机系统为 Windows，需要在此 Windows 平台上采用 Hyper-V 方式安装虚拟机“Win2003-A1”，具体要求为内存为 1G，硬盘 30G，并将服务器加入到 Windows 域环境；

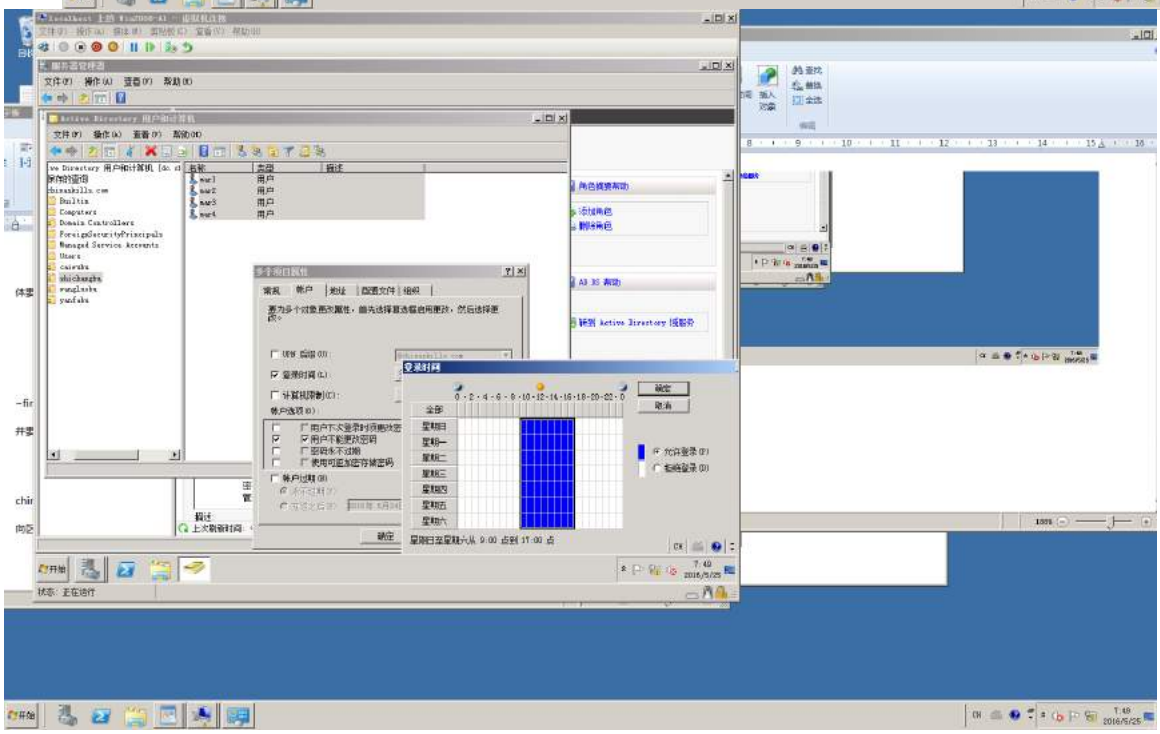


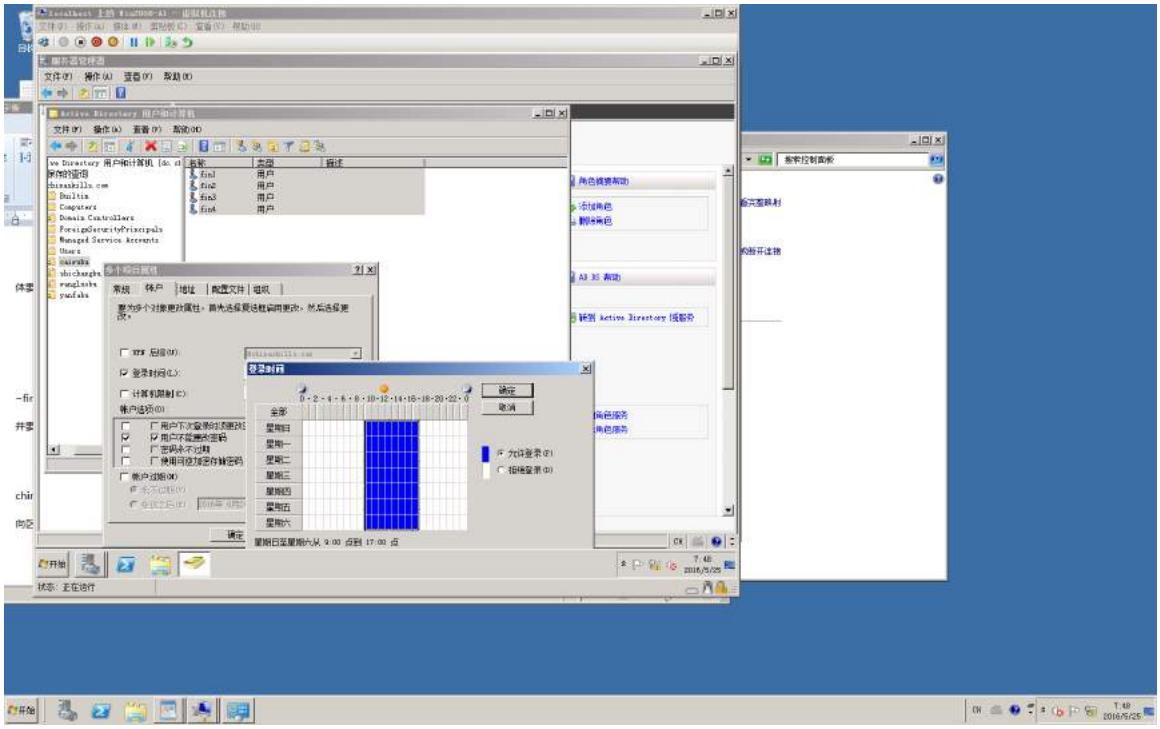
（二）在主机 Win2008-A1 中完成域控制器的部署

1、创建 4 个组织单元，单元名采用对应部门名称的拼音来命名，每个部门都创建 4 个用户，财务部用户：fin1~fin4、市场部用户：mar1~mar4、网络部用户：net1~net4、研发部用户： yf1~yf4，所有用户不能修改其用户口令，并要求用户只能在上班时间可以登录（每周工作日 9:00~17:00）；

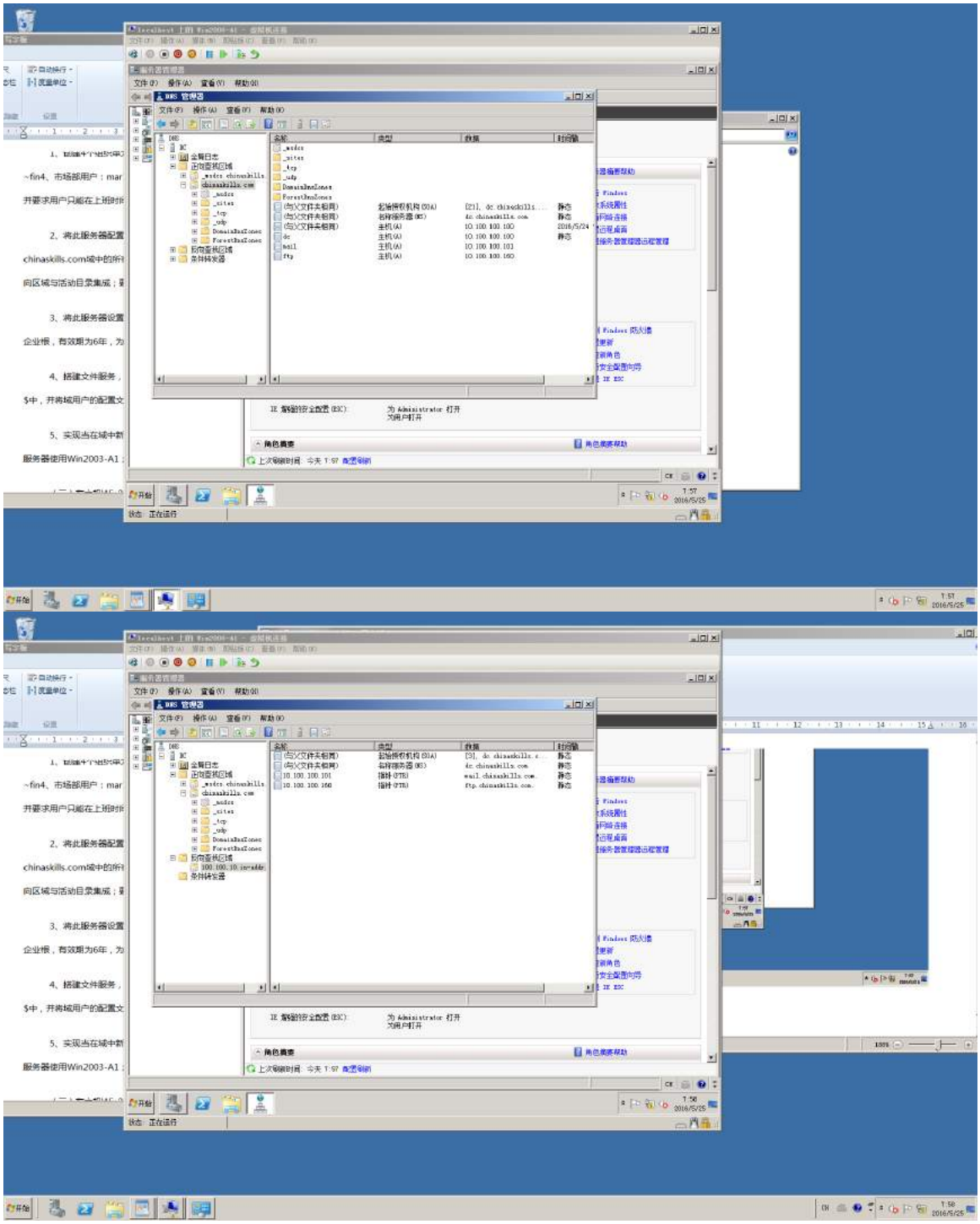


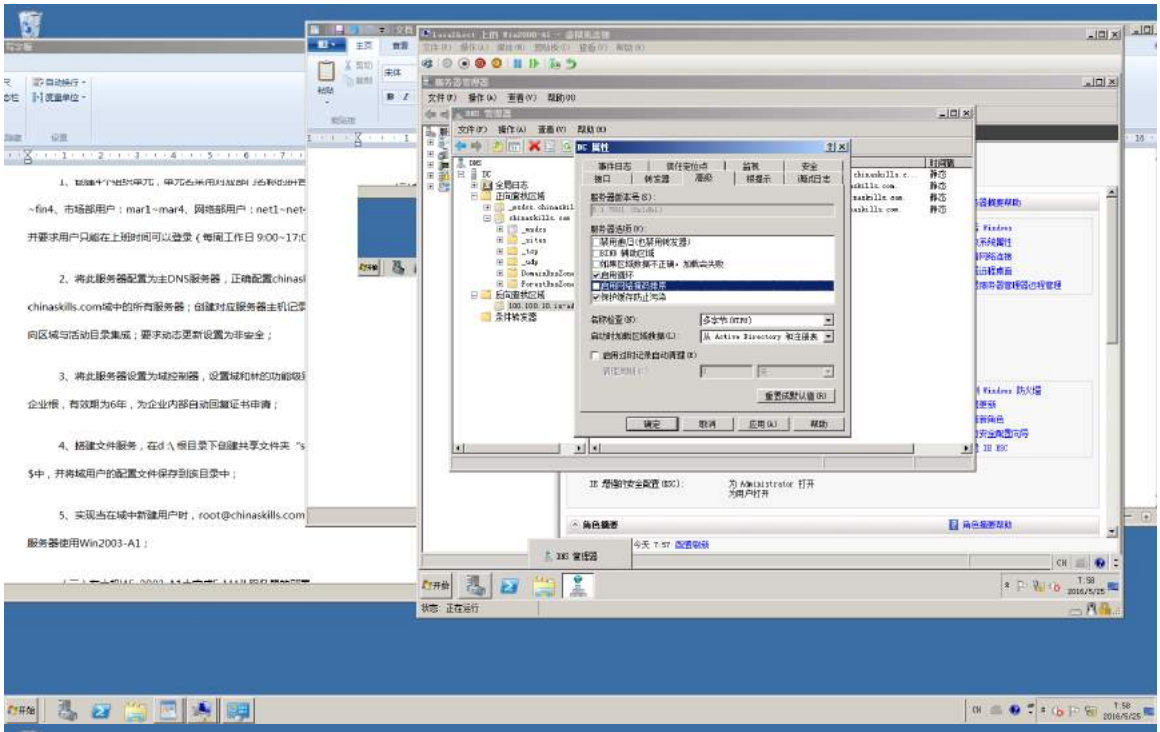


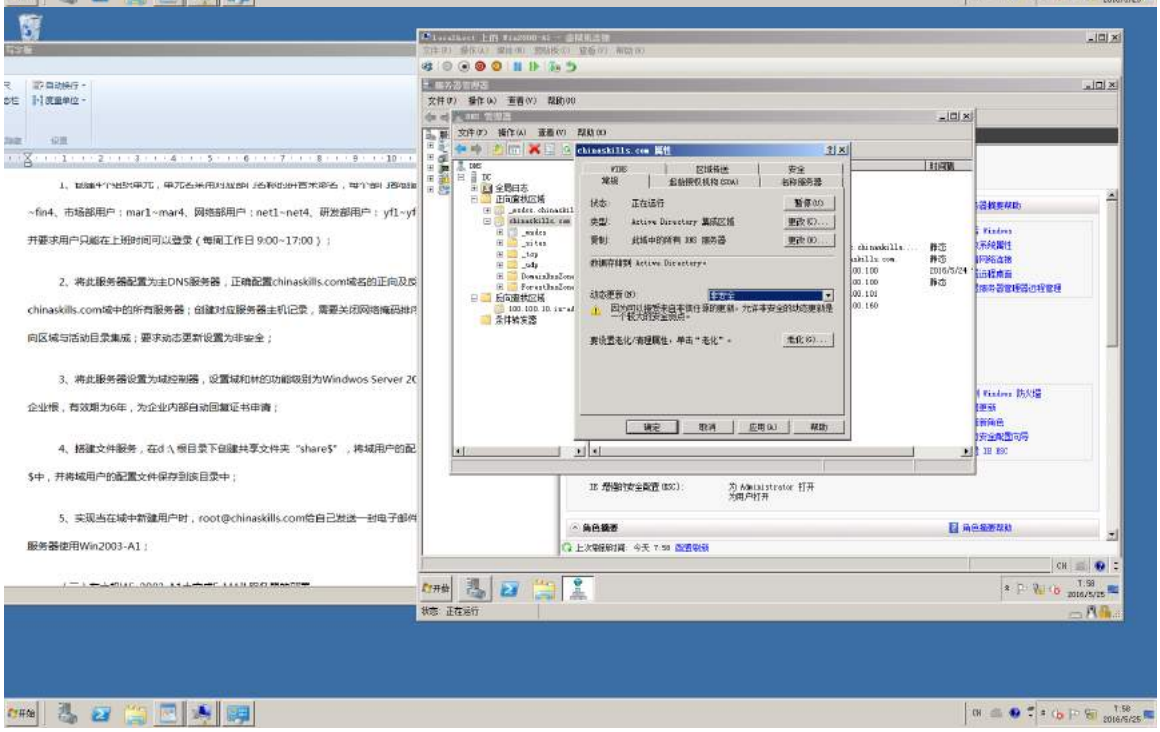


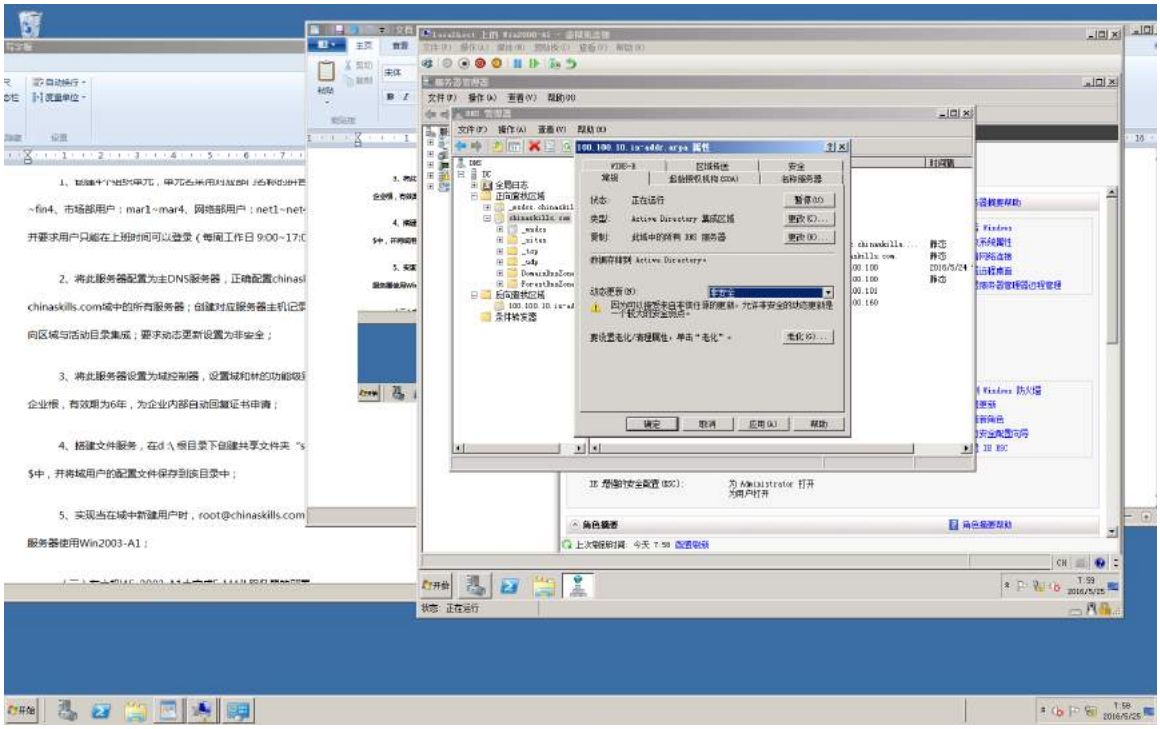


2、将此服务器配置为主 DNS 服务器，正确配置 chinaskills.com 域名的正向及反向解析区域，能够正确解析 chinaskills.com 域中的所有服务器；创建对应服务器主机记录，需要关闭网络掩码排序功能，设置 DNS 服务正向区域和反向区域与活动目录集成；要求动态更新设置为非安全；

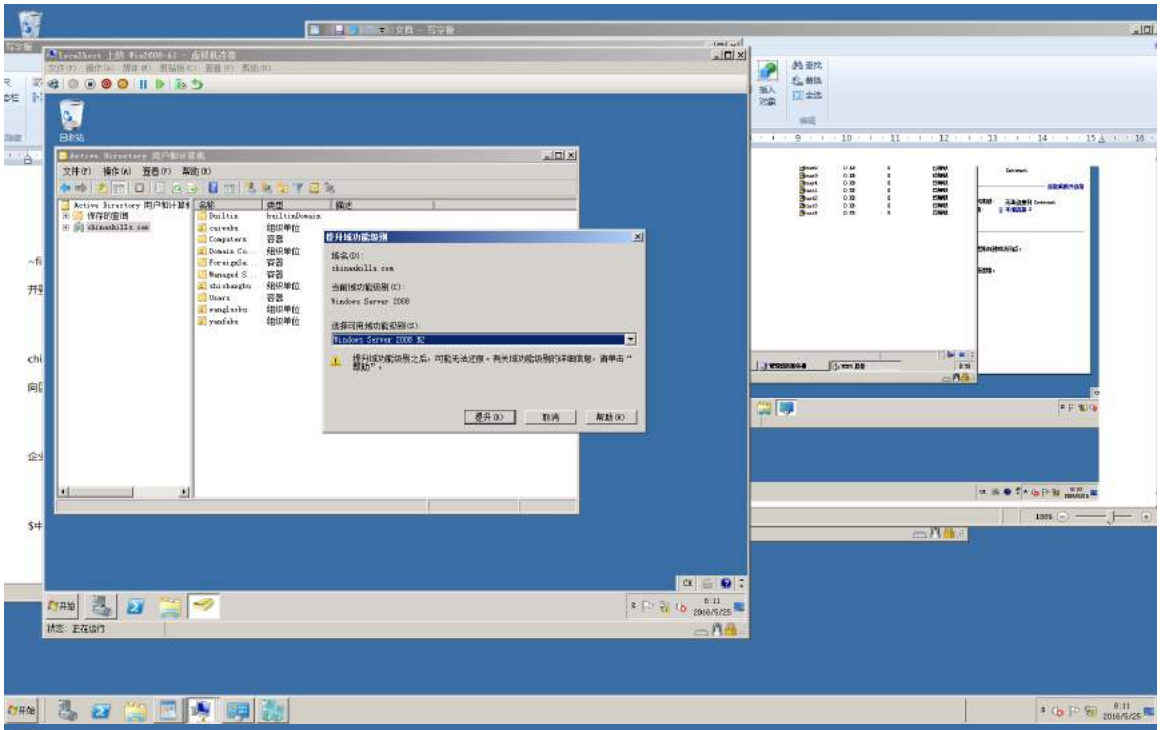


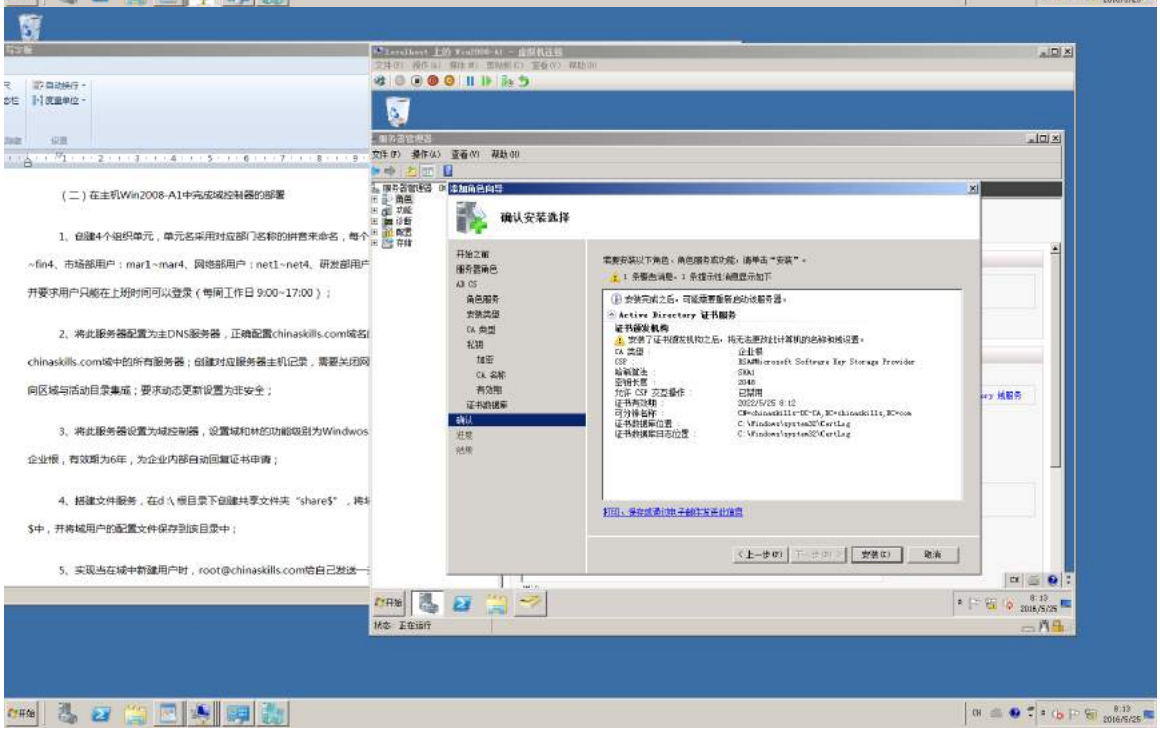


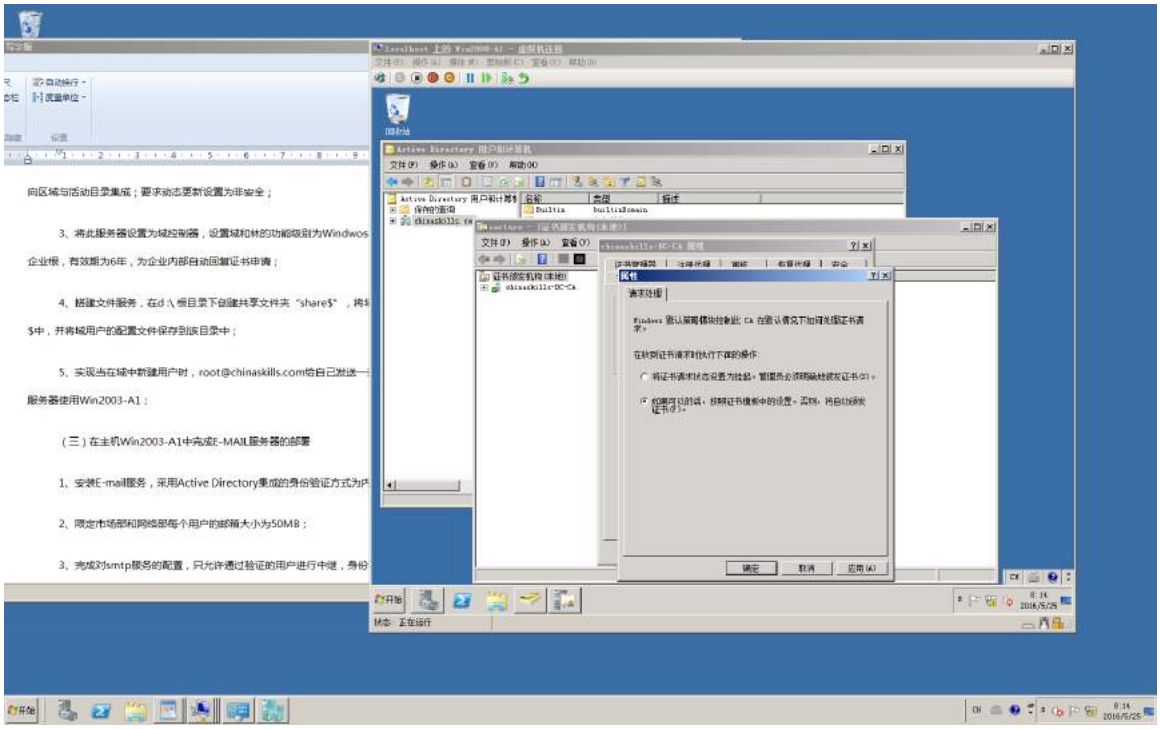




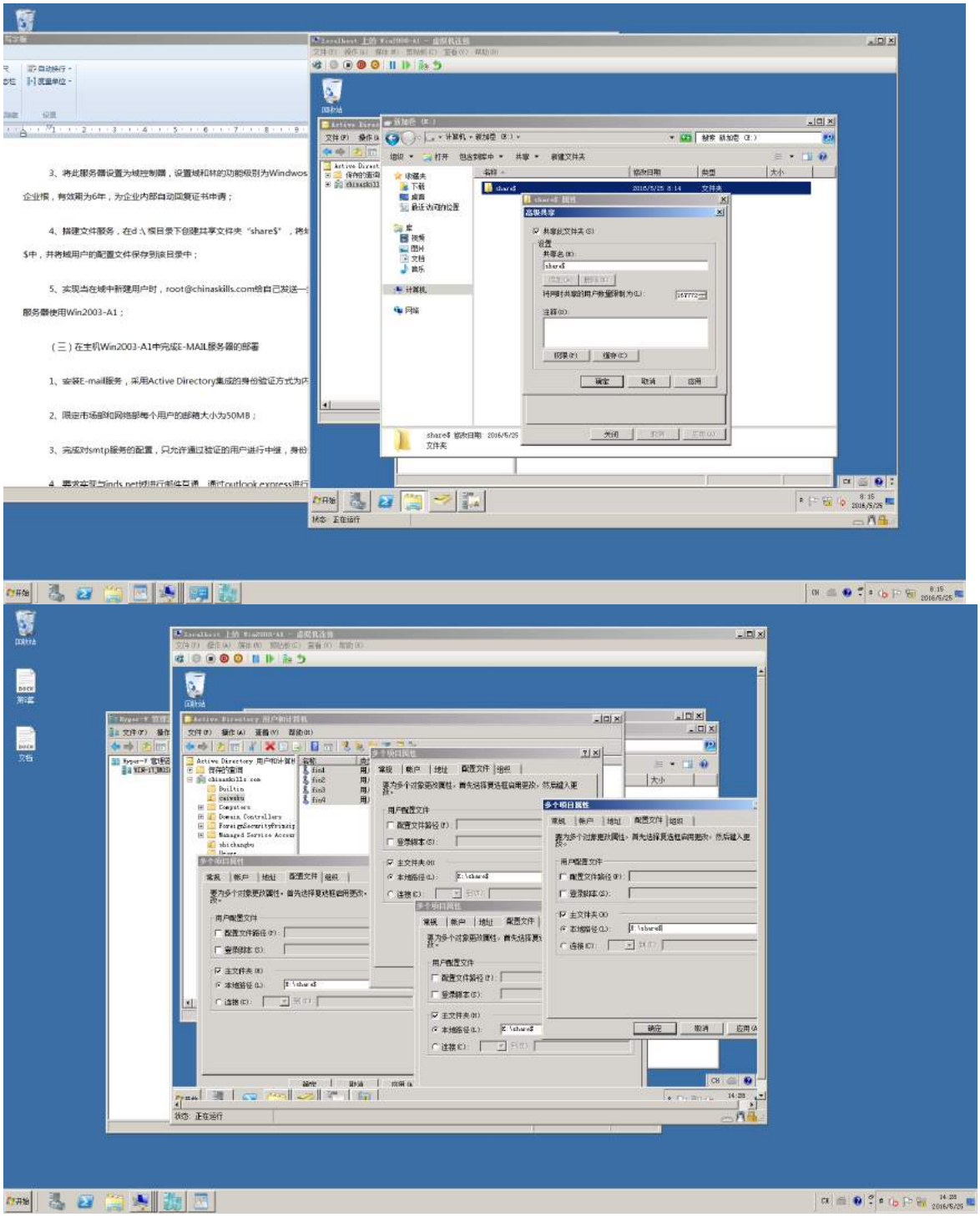
3、将此服务器设置为域控制器，设置域和林的功能级别为 Windwos Server 2008；此外，安装证书服务，设置为企业根，有效期为 6 年，为企业内部自动回复证书申请；



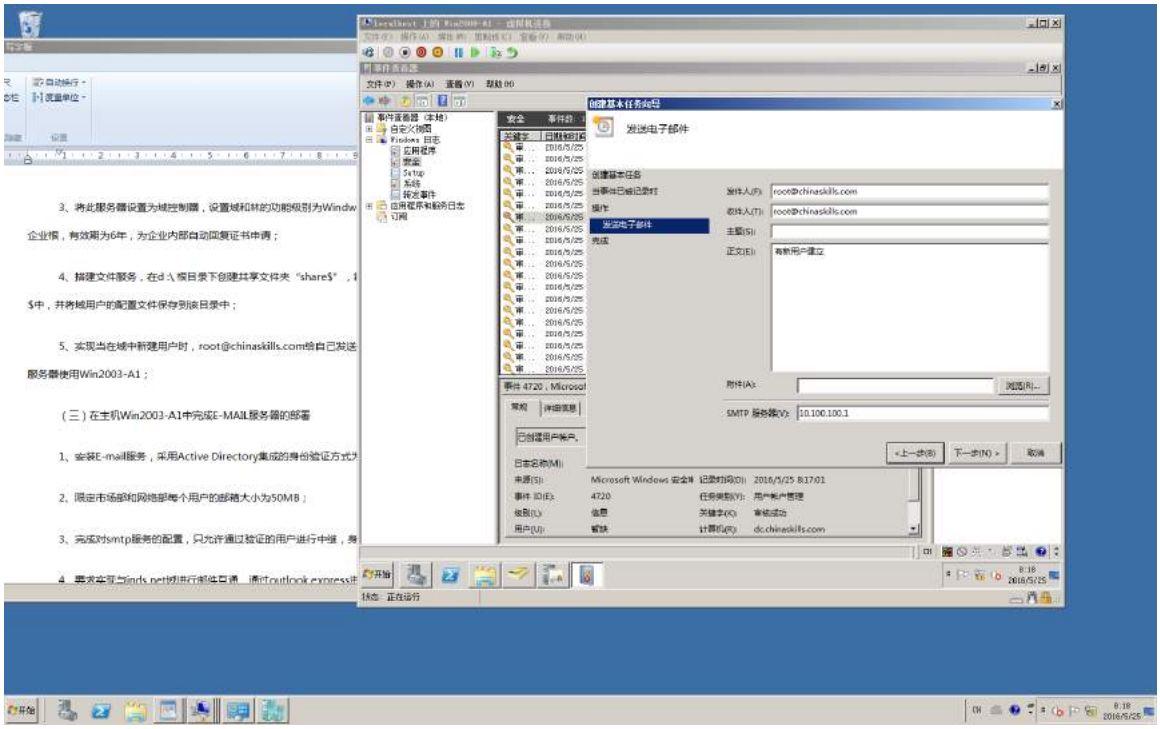

（二）在主机Win2008-A1中完成域控制器的部署
1、创建4个组织单元，单元名采用对应部门名称的拼音来命名，每个
~fin4、市场部用户：mar1~mar4、网络部用户：net1~net4、研发部用户
并要求用户只能在上班时间可以登录（每周工作日 9:00~17:00）；
2、将此服务器配置为主DNS服务器，正确配置chinaskills.com域名
chinaskills.com域中的所有服务器；创建对应服务器主机记录，需要关闭网
向区域与活动目录集成；要求动态更新设置为非安全；
3、将此服务器设置为域控制器，设置域和林的功能级别为Windwos
企业根，有效期为6年，为企业内部自动回复证书申请；
4、搭建文件服务，在d:\根目录下创建共享文件夹“share$”，将
$中，并将域用户的配置文件保存到该目录中；
5、实现当在域中新建用户时，root@chinaskills.com给自己发送一
确认安装选择



4、搭建文件服务，在 d :\ 根目录下创建共享文件夹“share$”，将域用户的配置文件夹数据统一保存在 share$中，并将域用户的配置文件保存到该目录中；

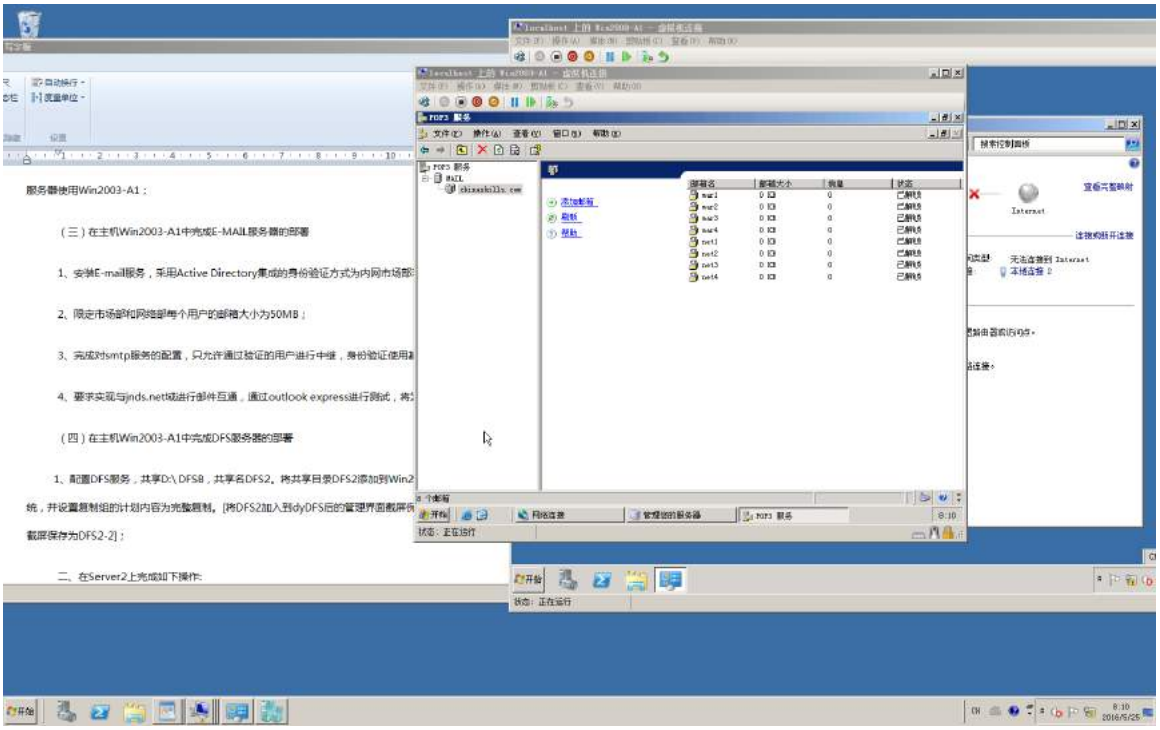


5.实现当在域中新建用户时，root@chinaskills.com 给自己发送一封电子邮件，内容为“有新用户建立”，邮件服务器使用 Win2003-A1；

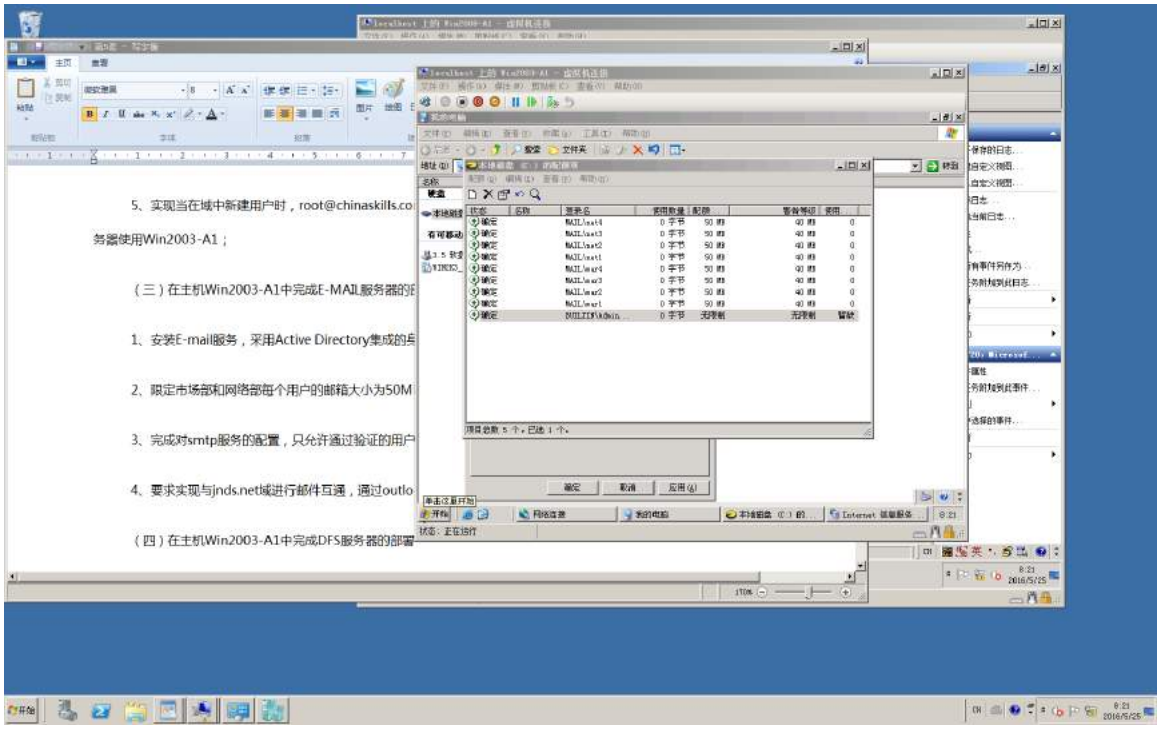


（三）在主机 Win2003-A1 中完成 E-MAIL 服务器的部署

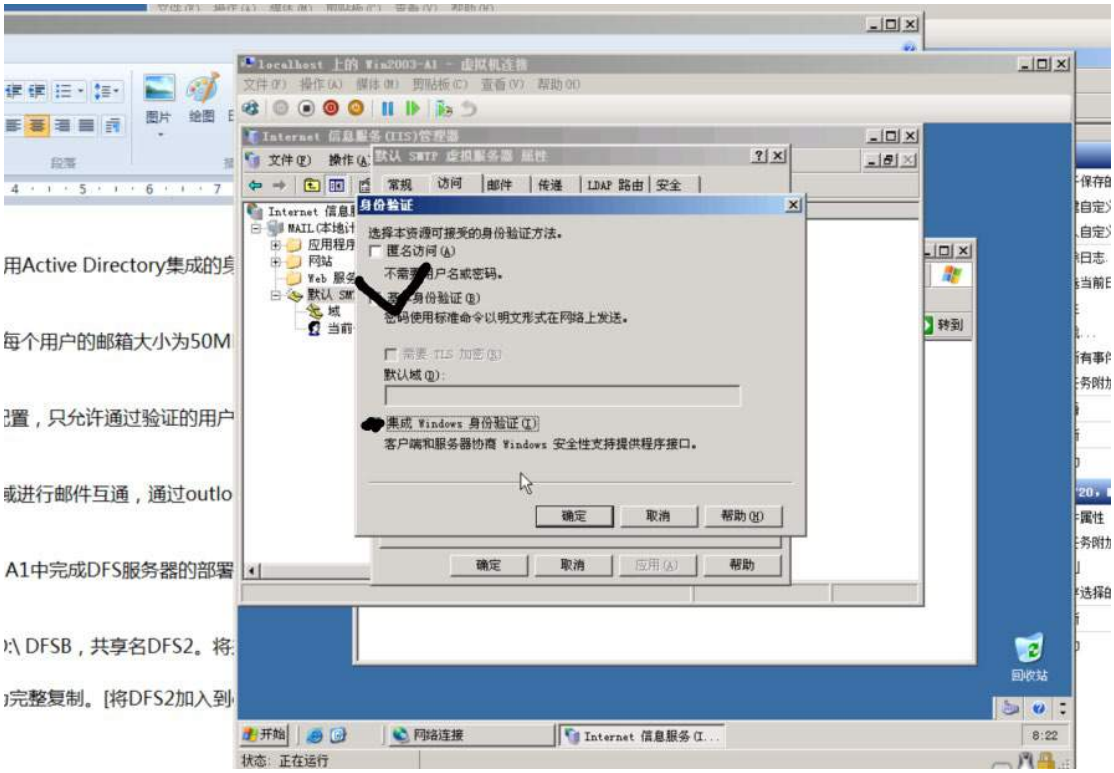
1、安装 E-mail 服务，采用 Active Directory 集成的身份验证方式为内网市场部和网络部的用户创建邮箱；

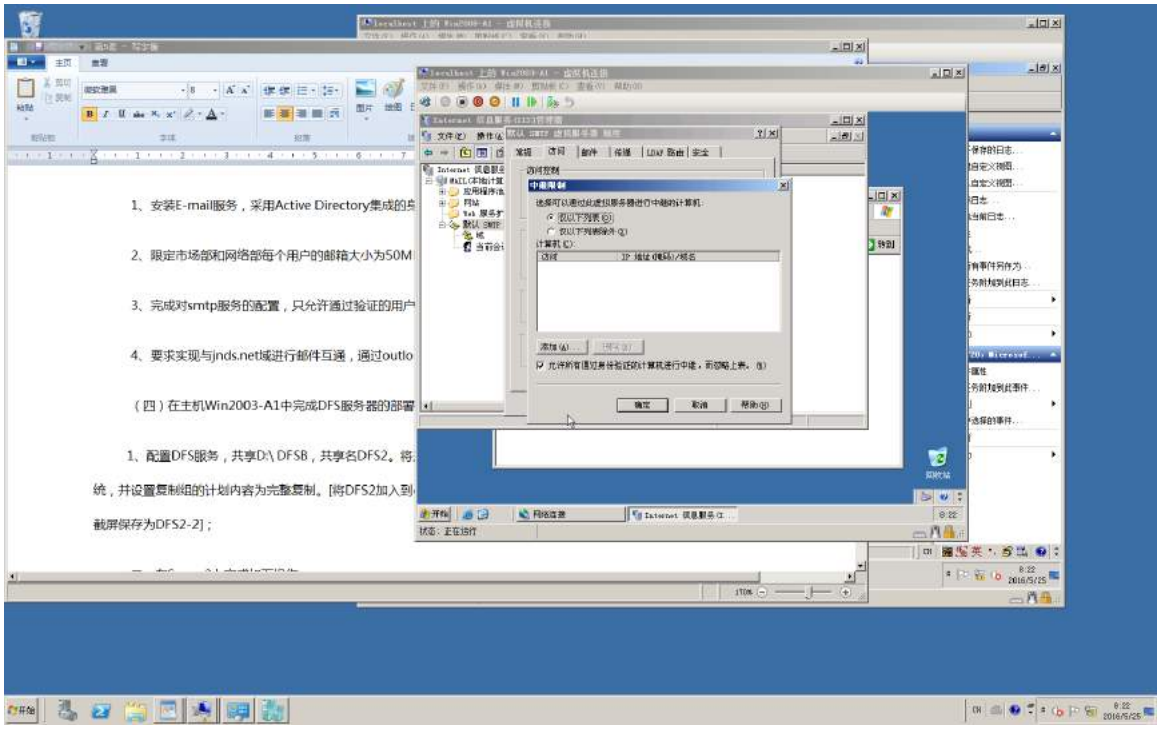


2、限定市场部和网络部每个用户的邮箱大小为 50MB；

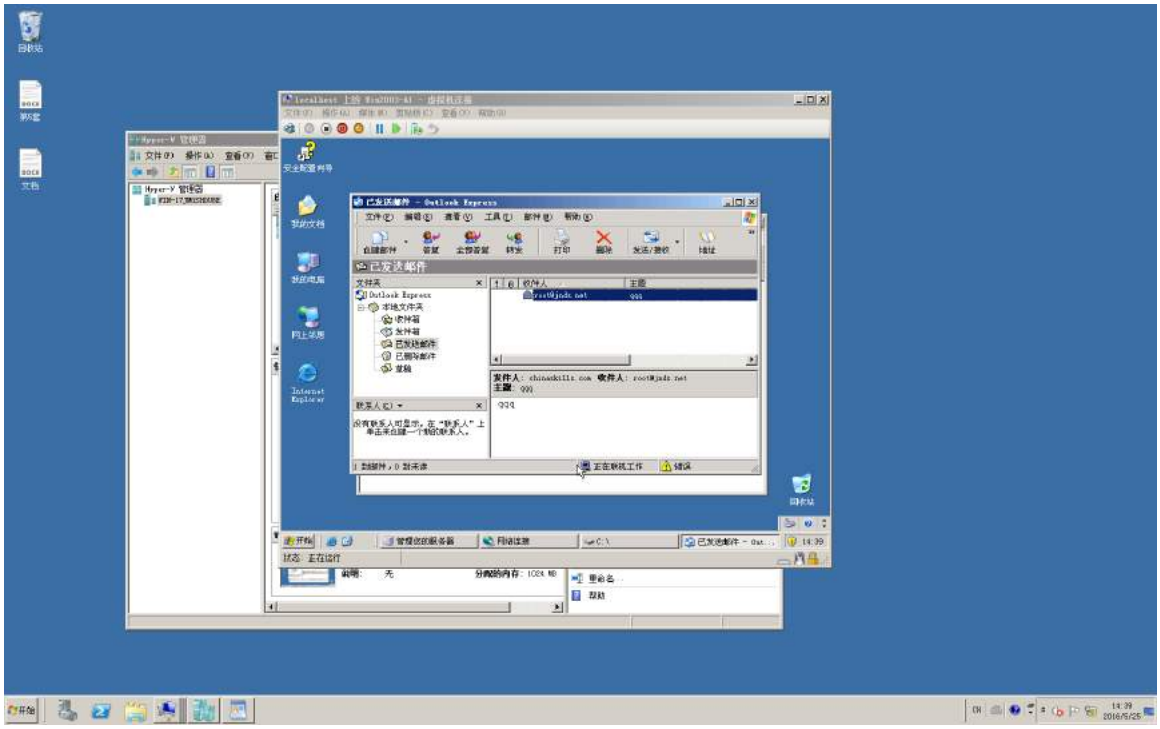


3、完成对 smtp 服务的配置，只允许通过验证的用户进行中继，身份验证使用基本认证方式；



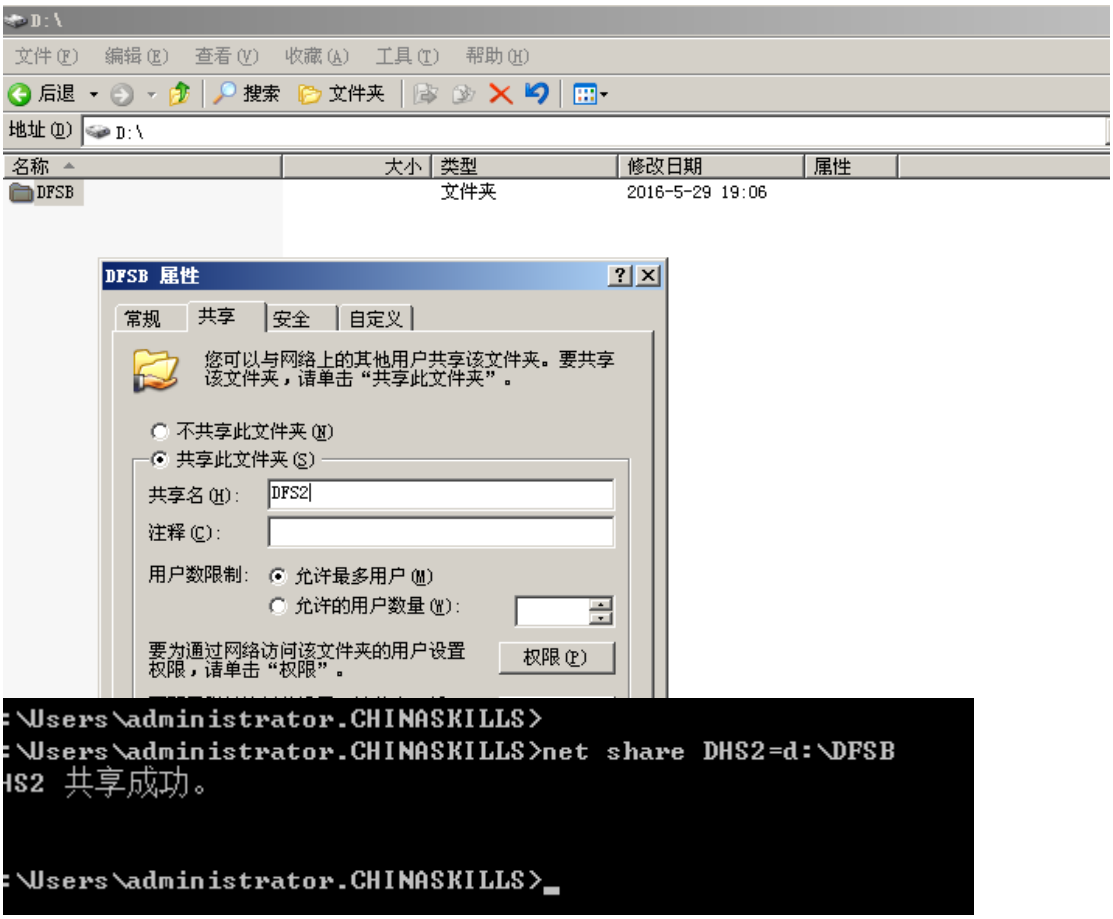


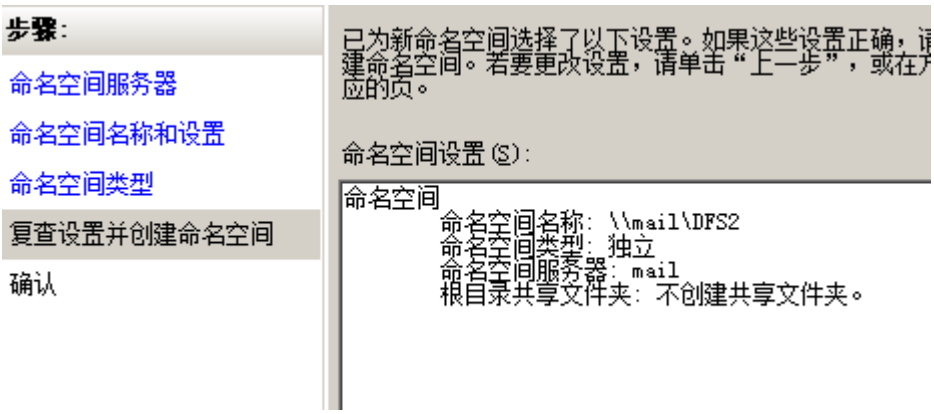
4、要求实现与jnds.net域进行邮件互通，通过outlook express进行测试，将发送成功的界面截图存储为 mail；

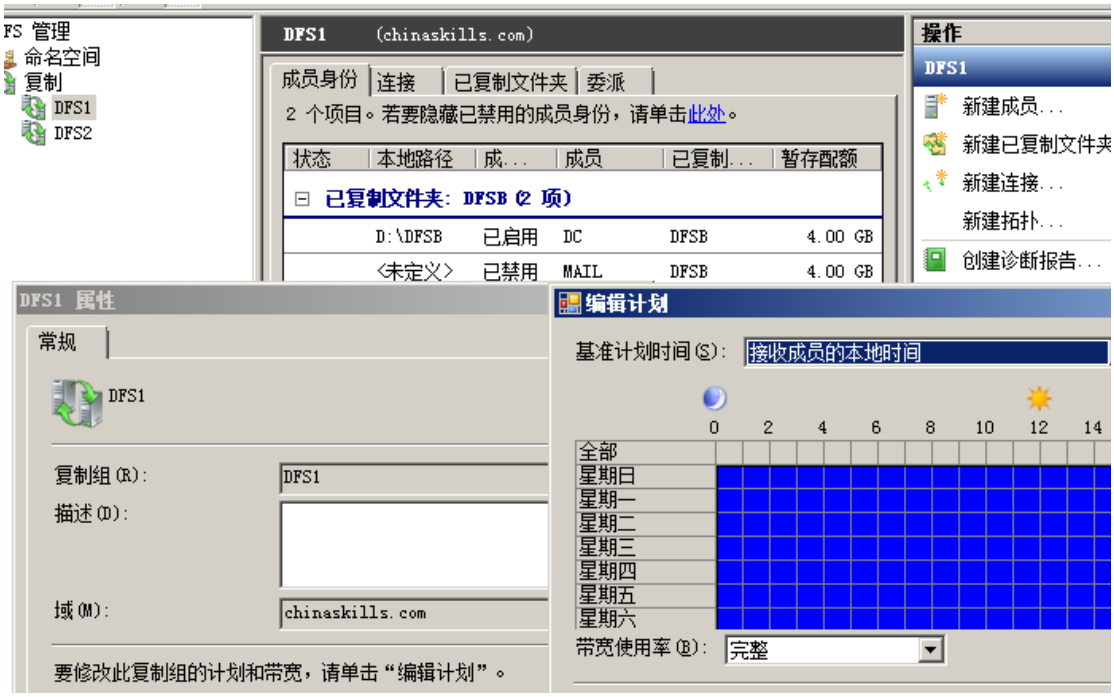


（四）在主机 Win2003-A1 中完成 DFS 服务器的部署

1、配置 DFS 服务，共享 D:\ DFSB，共享名 DFS2。将共享目录 DFS2 添加到 Win2008-B2 创建的 WEB 分布式文件系统，并设置复制组的计划内容为完整复制。[将 DFS2 加入到 dyDFS 后的管理界面截屏保存为 DFS2-1，设置复制方式的界面截屏保存为 DFS2-2]；





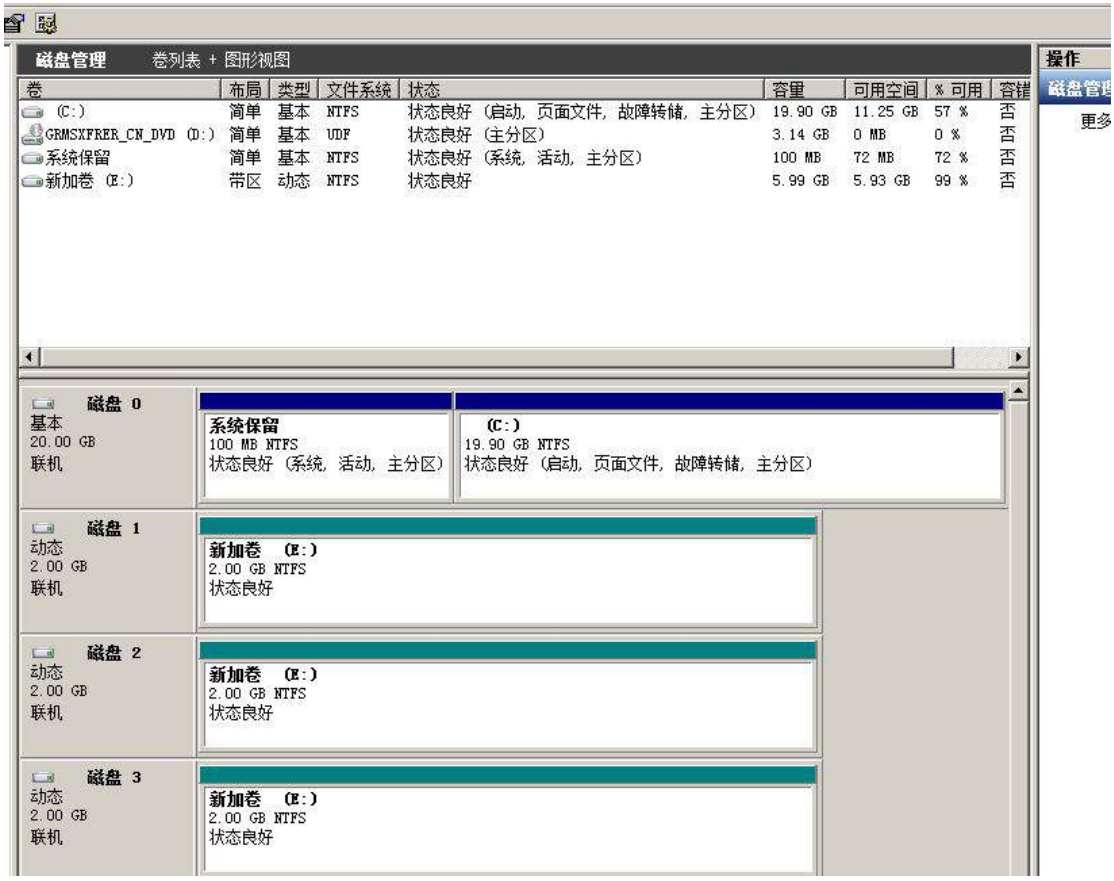


二、在 Server2 上完成如下操作:

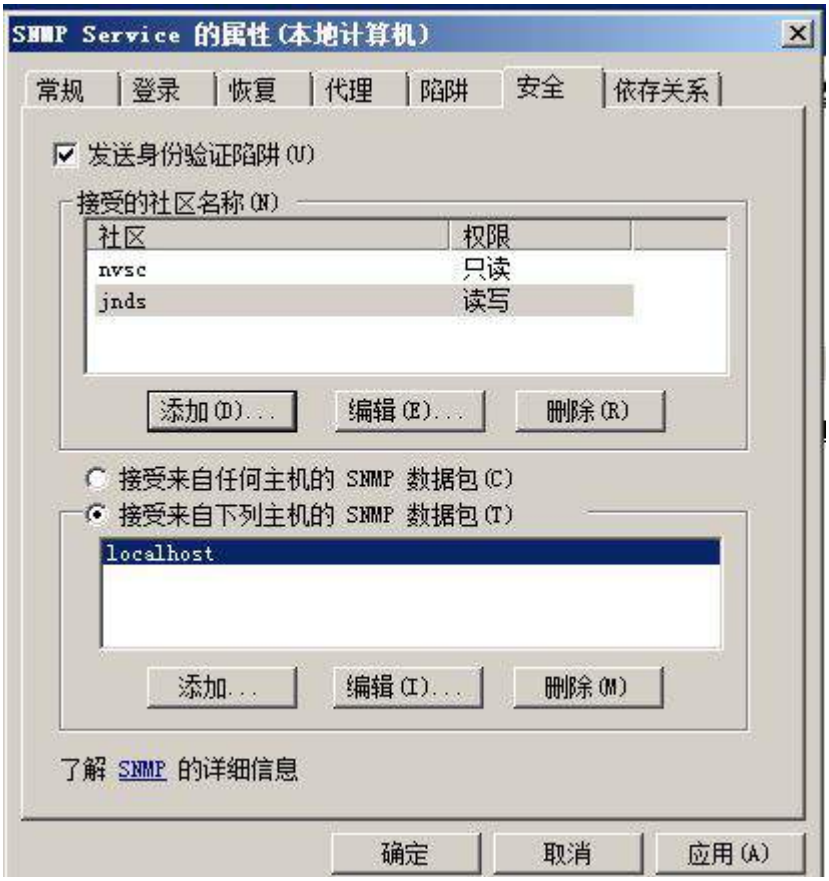
（一）完成虚拟主机的创建

1、安装虚拟机“Win2008-B1”，其内存为 1G，硬盘 20G，并将服务器加入到 Windows 域环境;

2、在虚拟机“Win2008-B1”中添加 SCSI 控制器，添加 3 块 SCSI 虚拟硬盘，其每块硬盘的大小为 2G。将三块硬盘配置为 RAID0，对应磁盘盘符为 e:\;



3、在虚拟机“Win2008-B1”中添加 SNMP 协议，启动 SNMP 网络管理功能，以保证服务器可以被网络管理工作站管理，共同体名称添加两个，只读的为 nvsc，读写的为 jnds。

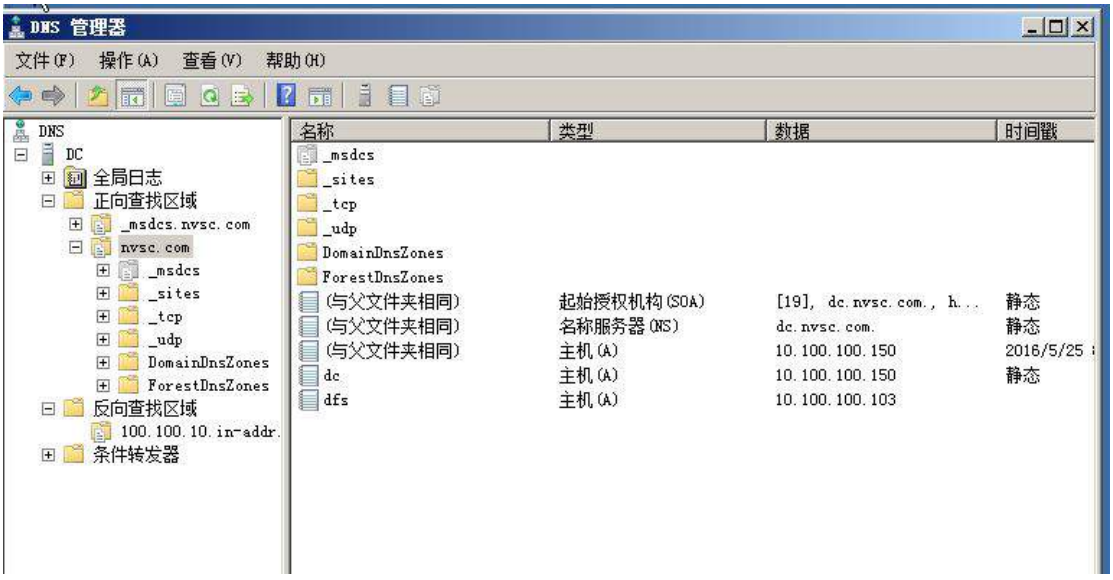


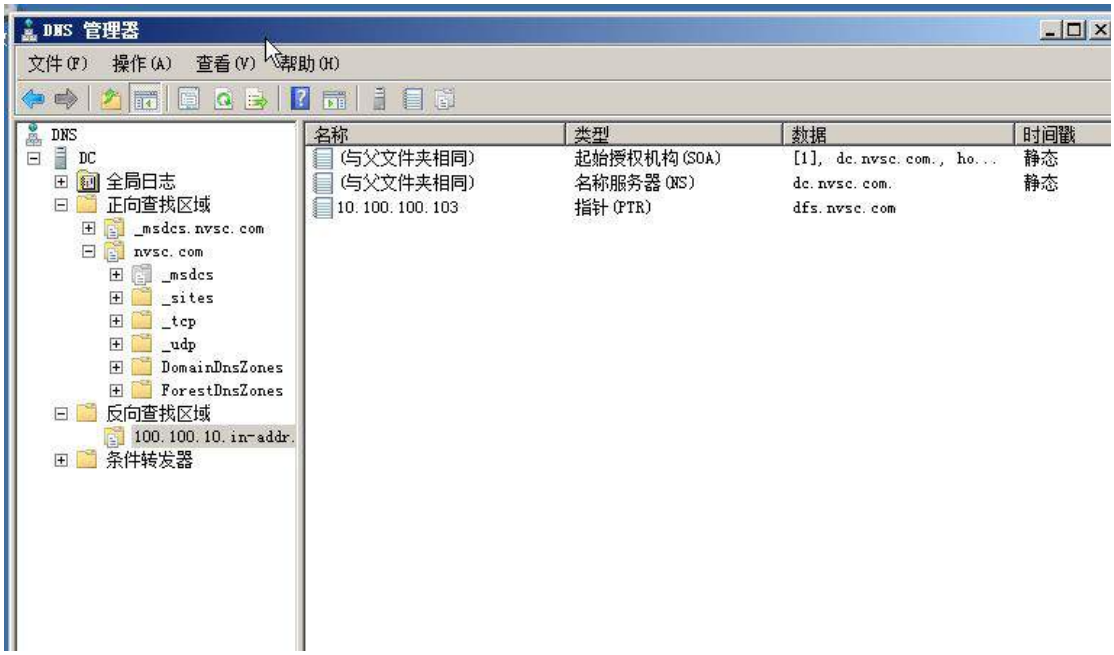
4、安装虚拟机“Win2008-B2”， 其内存为 512M，硬盘 20G，将服务器加入至 Windows 域中；

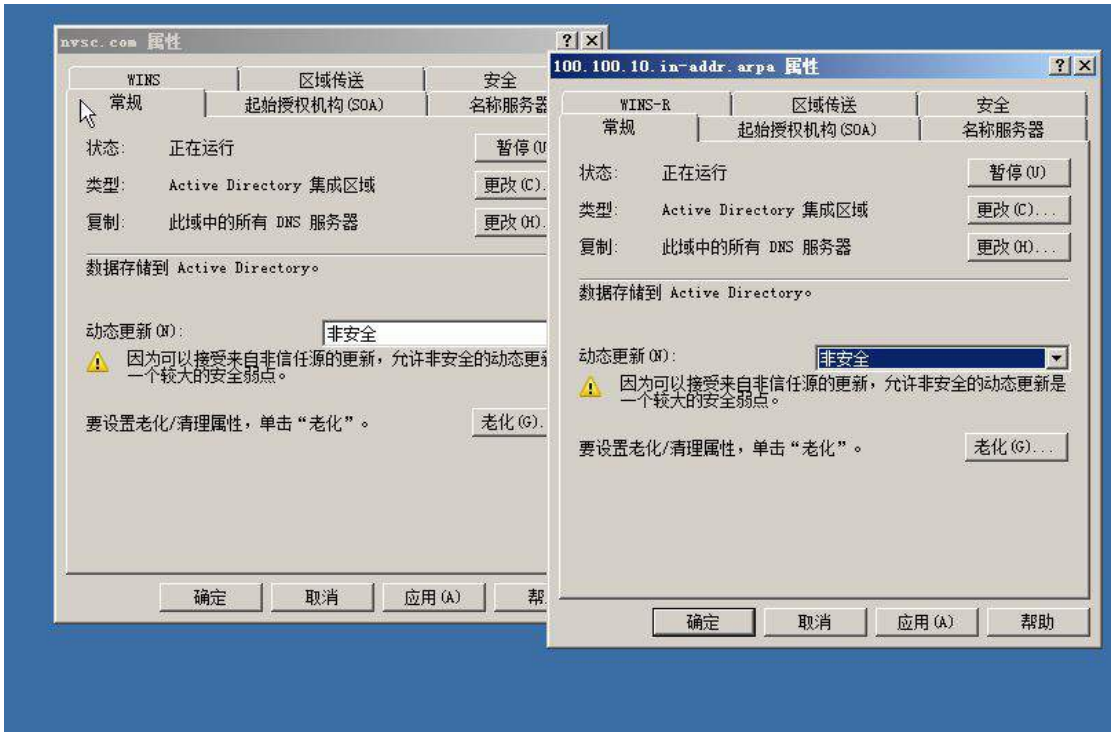
（二）在主机 Win2008-B1 中完成 WEB 服务器 1 的部署

1、将此服务器设置为域控制器，设置域和林的功能级别为 Windwos Server 2008；

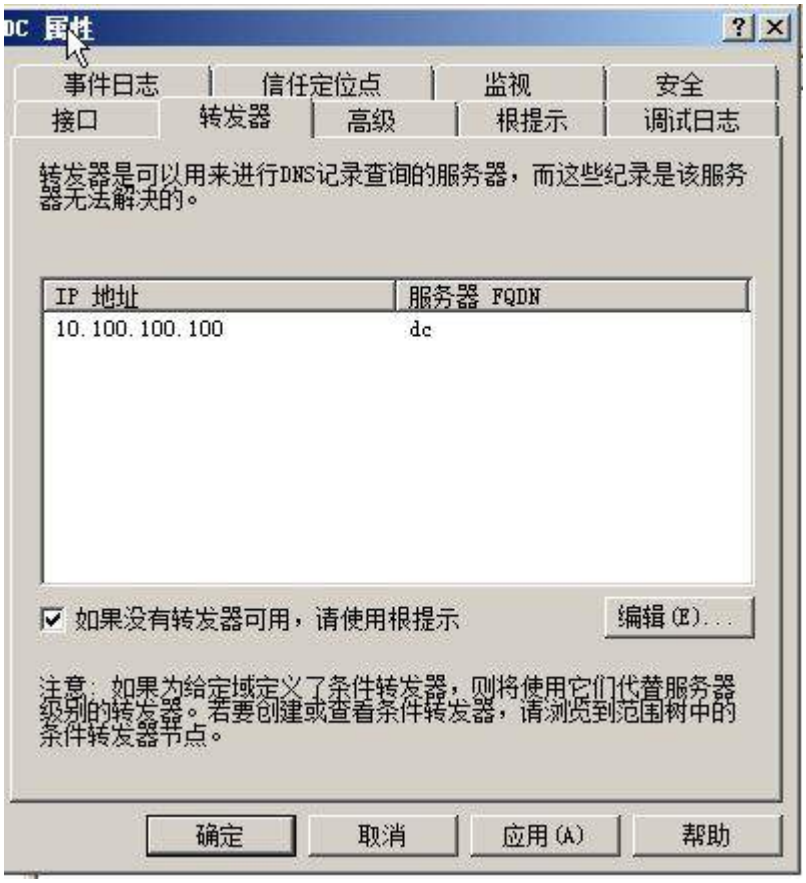
2、将此服务器配置为主 DNS 服务器，正确配置 nvsc.com 域名的正向及反向解析区域，能够正确解析 nvsc.com 域中的所有服务器；创建对应服务器主机记录，设置 DNS 服务正向区域和反向区域与活动目录集成；要求动态更新设置为非安全；





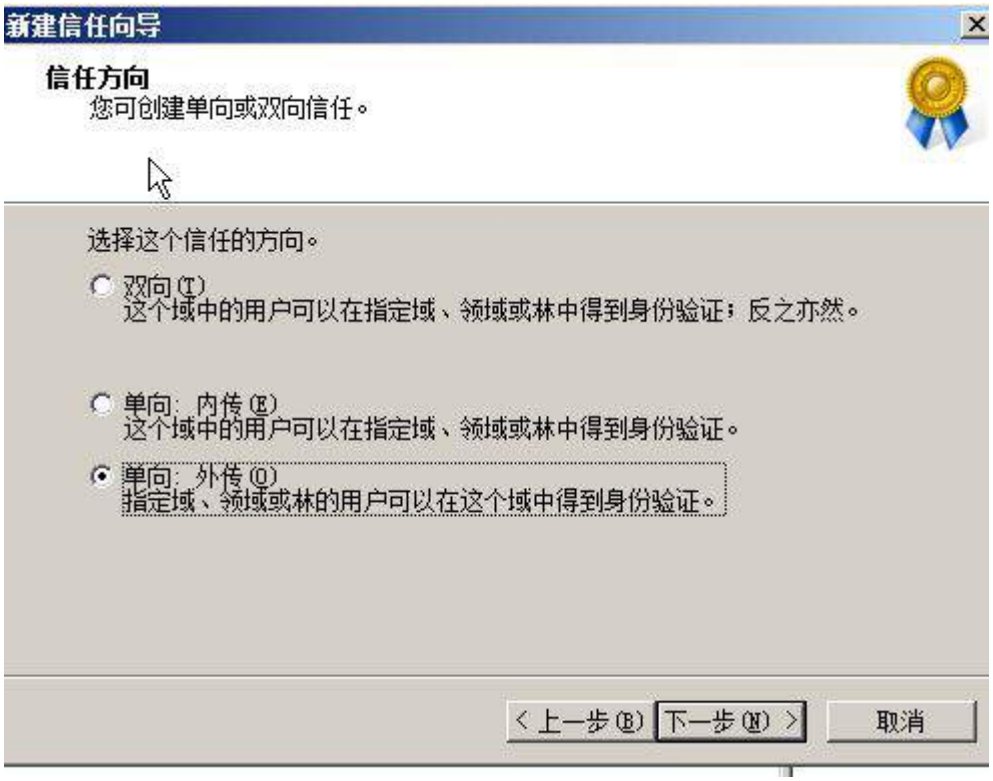


3、将两个域的 DNS 服务器互相设置转发器。



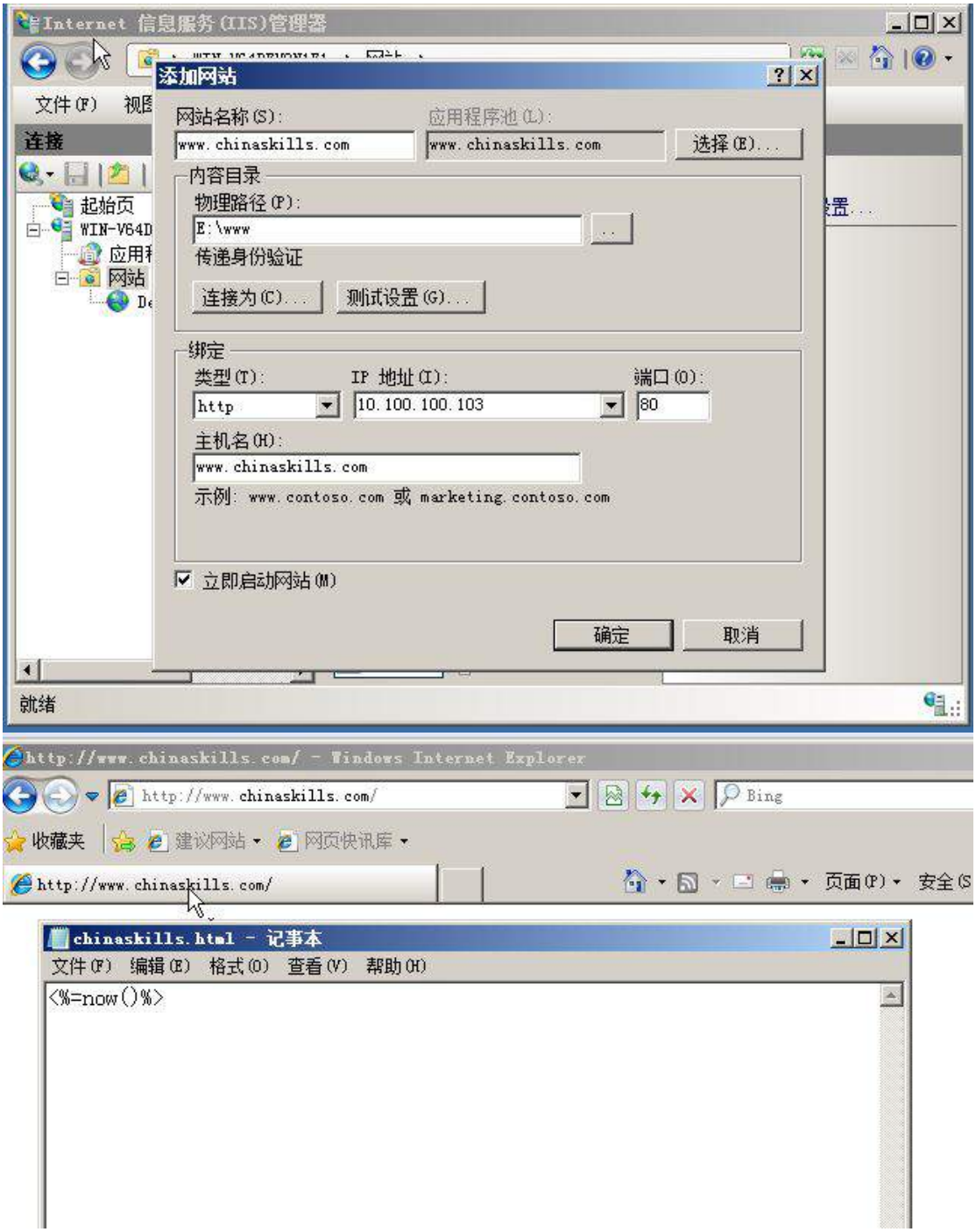
4、在 D 盘下新建文件夹 test，并将其文件夹进行共享，共享名为 share。

5、通过使用单向信任关系，实现 chinaskills.com 域的研发部的员工访问 nvsc.com 域的共享资源 test 文件夹。

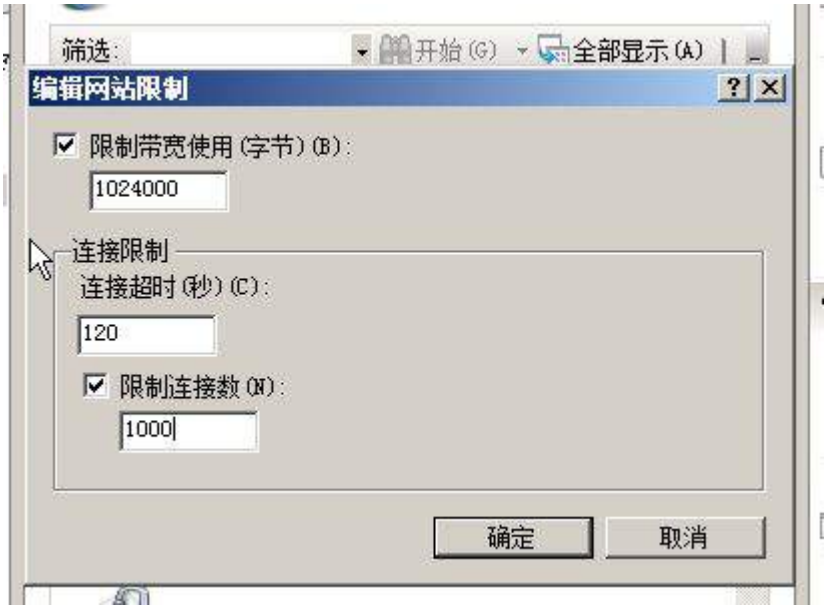


（三）在主机 Win2008-B2 中完成 web 及 DFS 服务器的部署

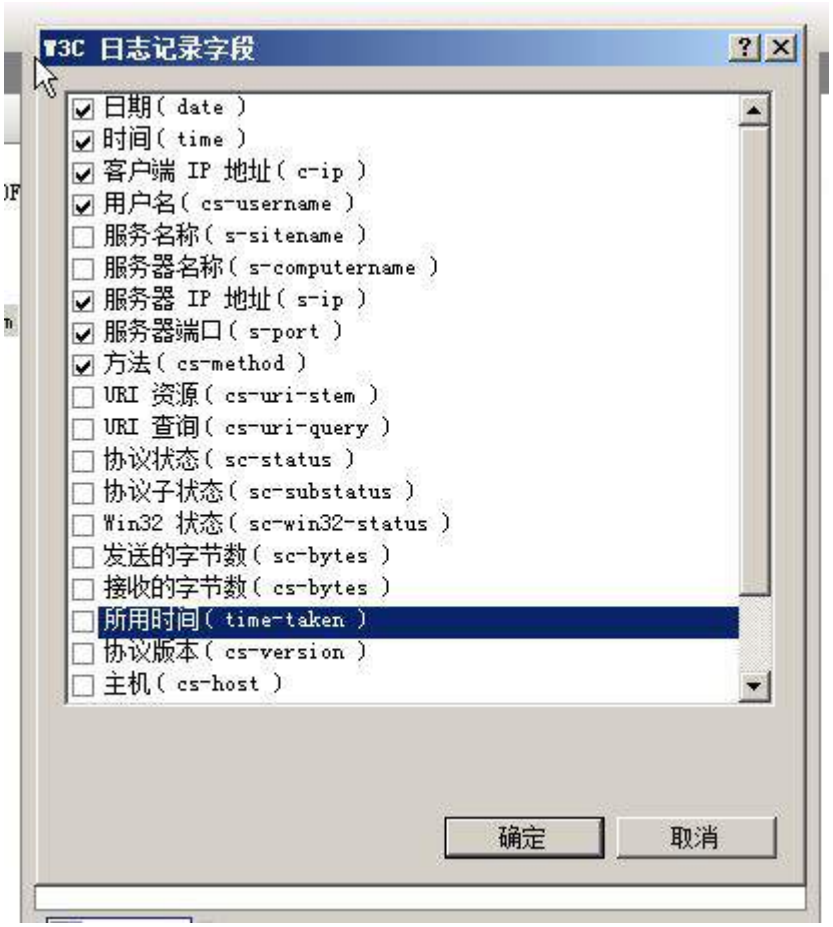
1、安装 IIS 组件，创建 www. chinaskills.com 站点，在挂载的磁盘 e:\下创建名称为 www 的目录，在 www 文件夹中创建名称为 chinaskills.html 的主页，其主页显示内容“<%=now()%>”，同时只允许使用 SSL 且只能通过域名方式进行访问；



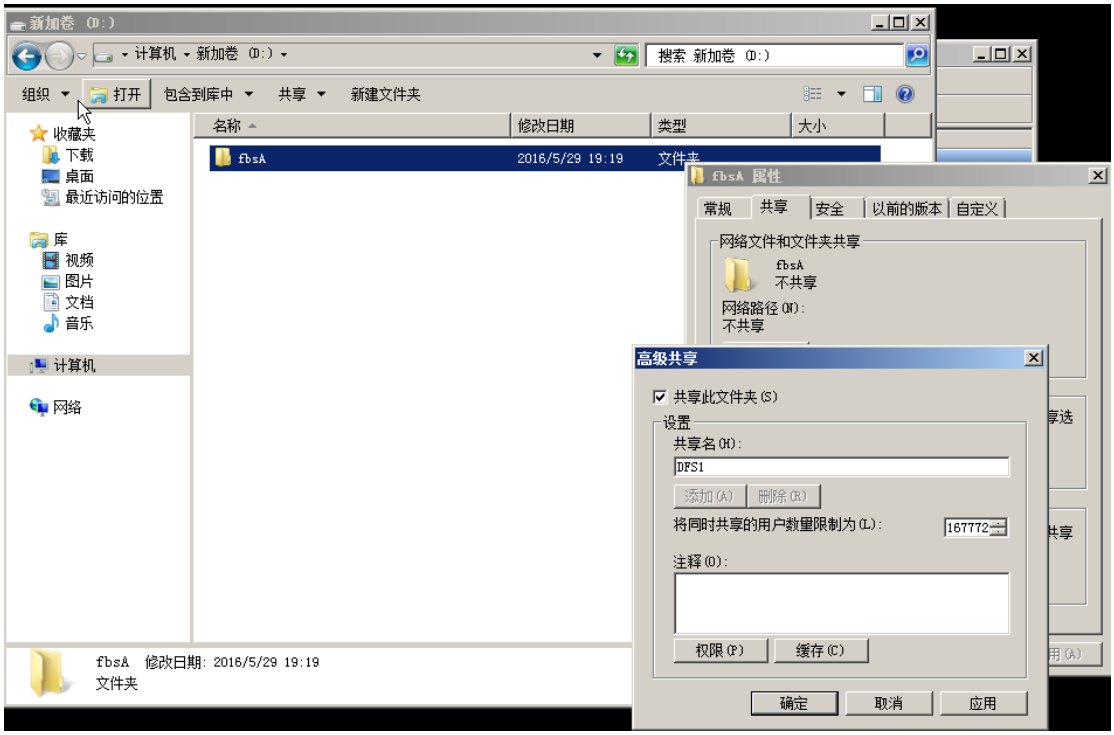
2、设置网站的最大连接数为 1000，网站连接超时为 120s，网站的带宽为 1000KB/S，使用 W3C 记录日志；禁用父路径；每天创建一个新的日志文件，使用当地时间作为日志文件名；日志只允许记录日期、时间、客户端 IP 地址、用户名、服务器 IP 地址、服务器端口号和方法；

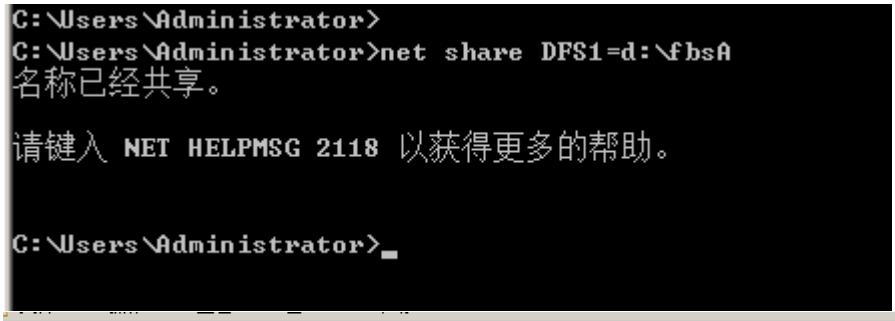

筛选:
开始(G)
全部显示(A)
编辑网站限制
限制带宽使用(字节)(B):
1024000
连接限制
连接超时(秒)(C):
120
限制连接数(N):
1000
确定
取消

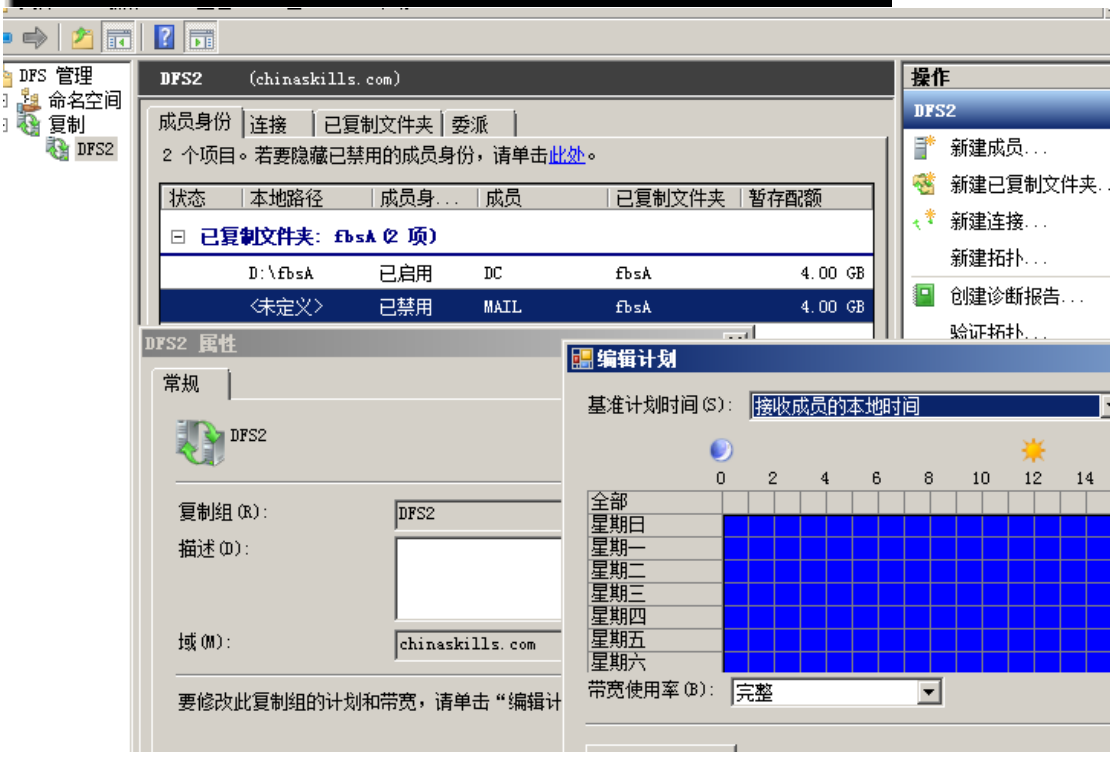

启用父路径
False
日志
使用此功能配置 IIS 在 Web 服务器上记录请求的方式。
格式(M):
W3C
选择字段(S)...
目录(Y):
%SystemDrive%\inetpub\logs\LogFiles
编码(E):
UTF-8
日志文件滚动更新
选择 IIS 用来创建新的日志文件的方法。
计划(C):
每天
最大文件大小(字节)(Z):
不创建新的日志文件(N)
使用本地时间进行文件命名和滚动更新(U)



3、配置 DFS 服务作为分布式文件系统的命名空间服务器，共享 D:\fbsA，共享名为 DFS1，空间名称为 WEB，将 DFS1 作为分布式命名空间的根目录，实现与 win2003-C2 服务器的内容保持同步；





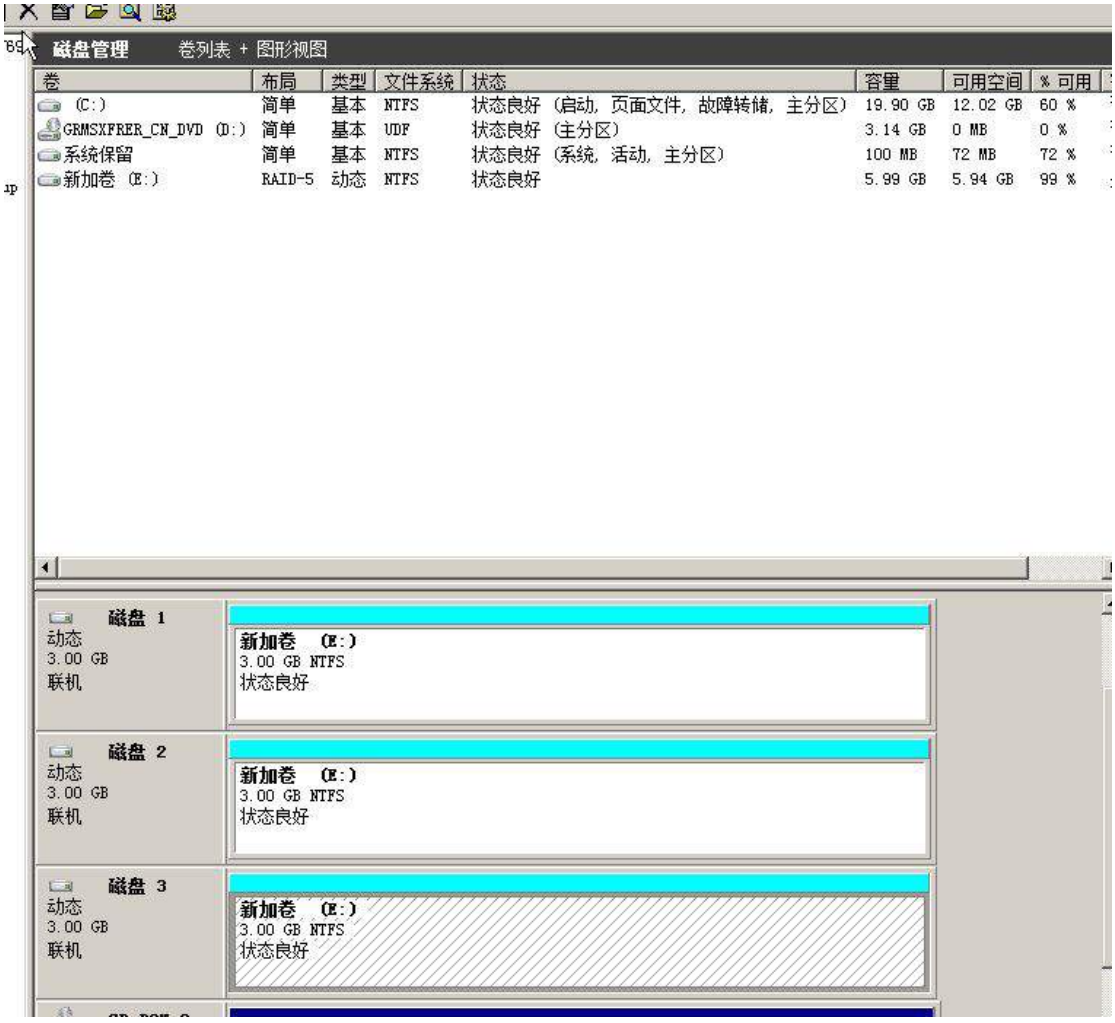


三、在 Server3 上完成如下操作:

（一）完成虚拟主机的创建

1、安装虚拟机“Win2008-C1”，其内存为 1G，硬盘 20G，并将服务器加入到 Windows 域环境；

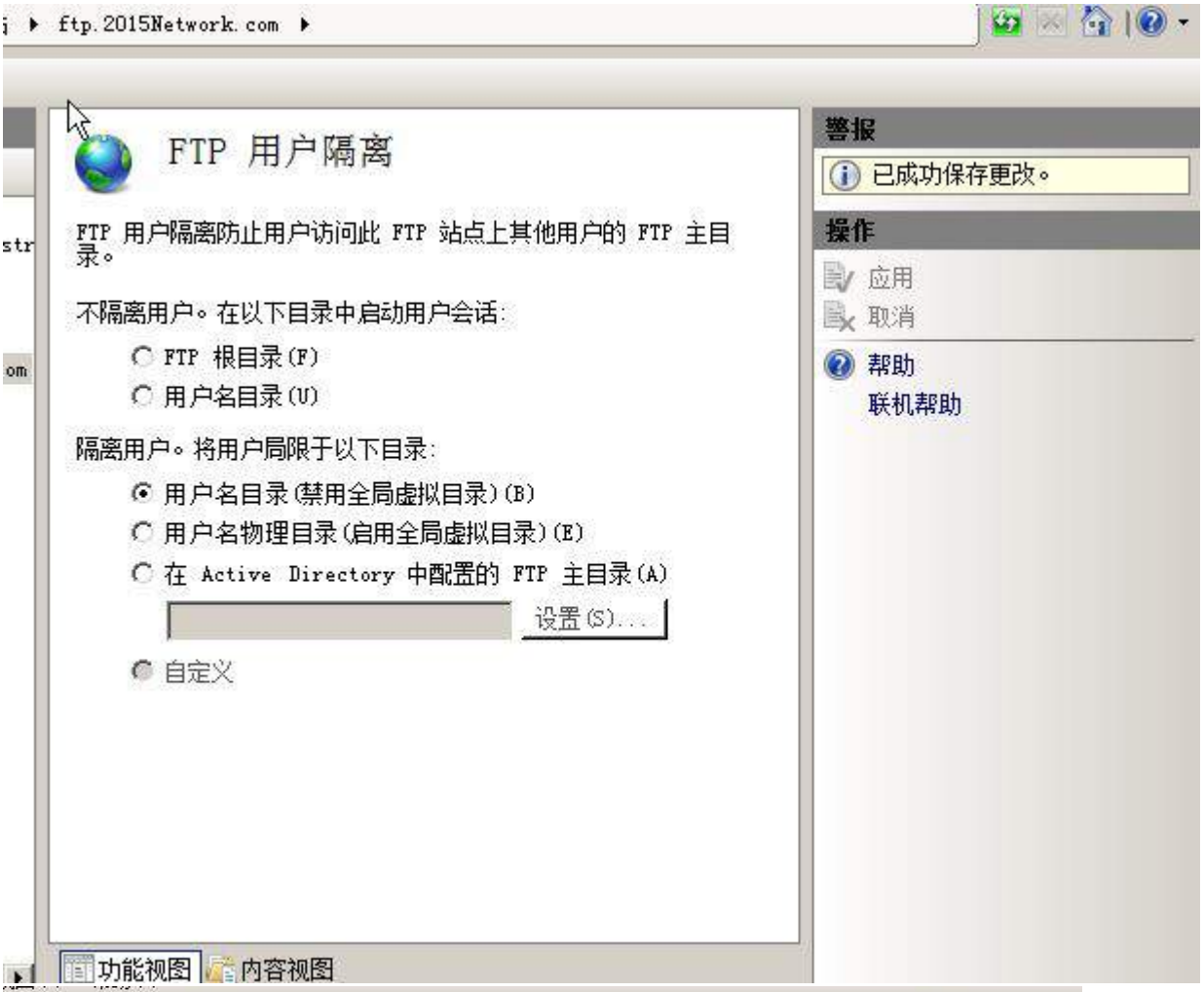
2、在虚拟机“Win2008-C1”中添加 SCSI 控制器，添加 3 块 SCSI 虚拟硬盘，其每块硬盘的大小为 3G，将三块硬盘配置为 RAID5，对应磁盘盘符为 e:\；



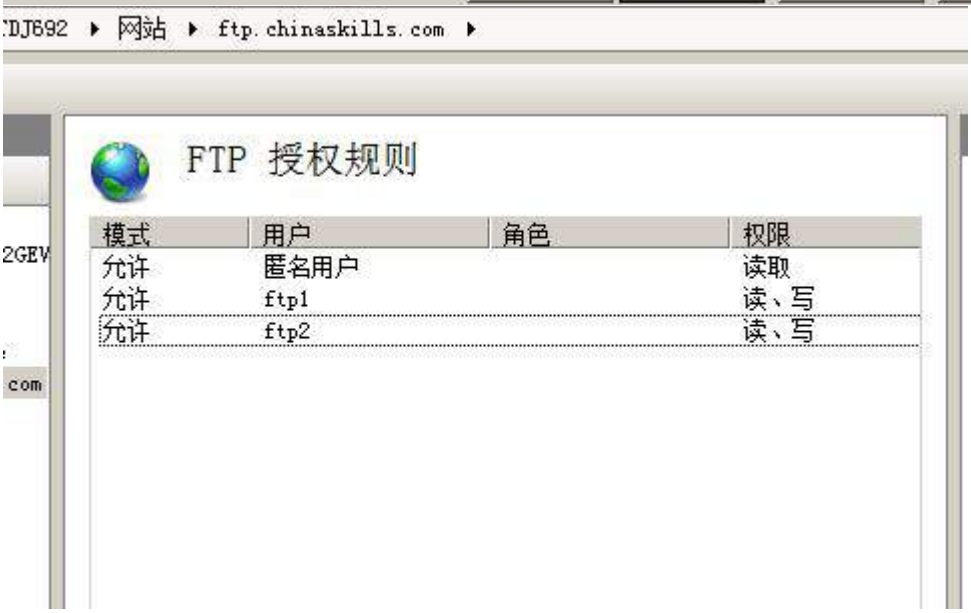
（二）在主机 Win2008-C1 中完成 FTP 服务器的部署

1、安装 FTP 服务。

2、使用隔离用户创建名为 ftp.chinaskills.com 的 FTP 站点，FTP 主目录为 c:\inetpub\ftproot。使用 ftp.chinaskills.com 可访问该 FTP 站点。域用户 ftp1、ftp2 及匿名用户均可登录，但匿名用户权限只读，ftp1,ftp2 可以读写。

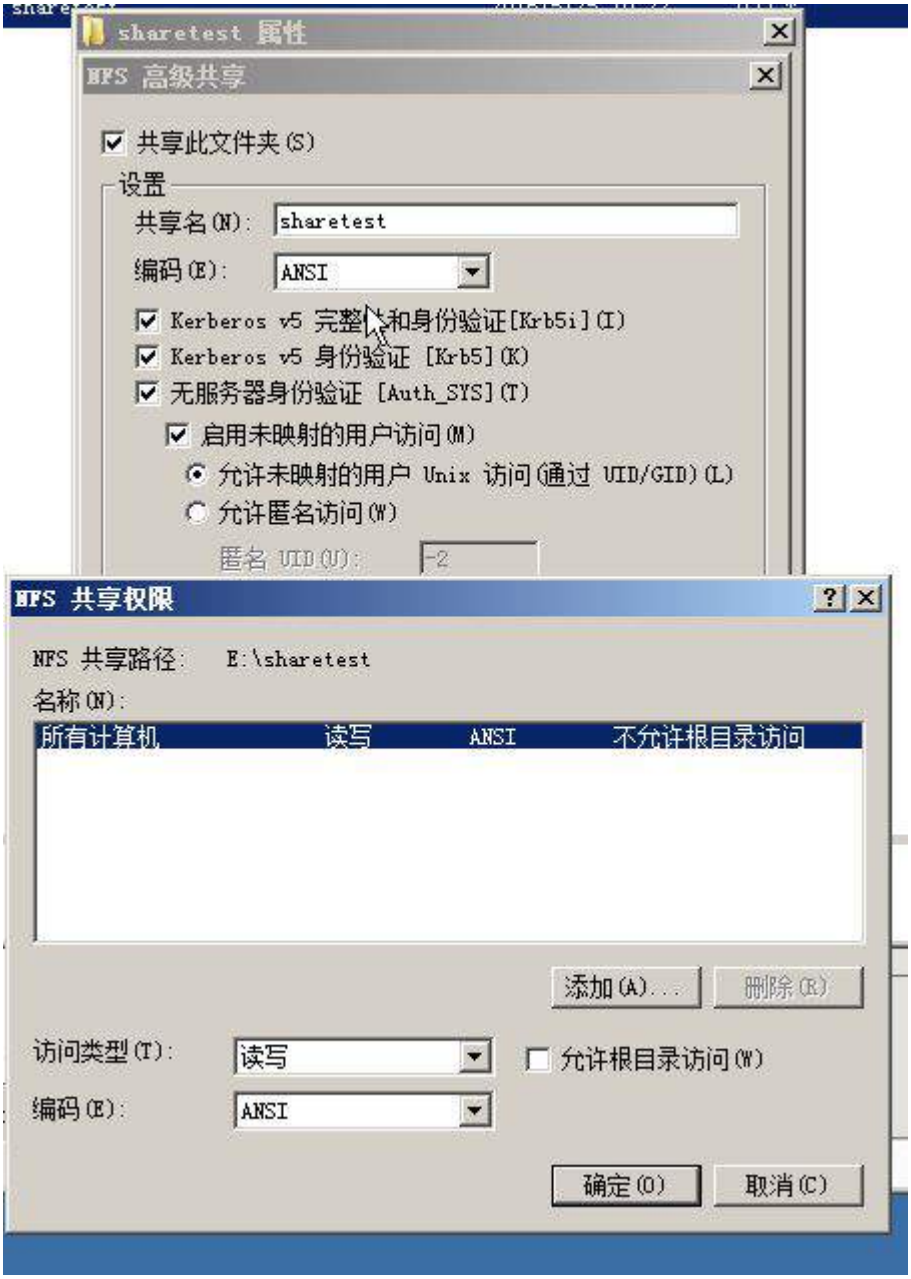

ftp.2015Network.com
FTP 用户隔离
FTP 用户隔离防止用户访问此 FTP 站点上其他用户的 FTP 主目录。
不隔离用户。在以下目录中启动用户会话:
FTP 根目录(F)
用户名目录(U)
隔离用户。将用户局限于以下目录:
用户名目录(禁用全局虚拟目录)(B)
用户名物理目录(启用全局虚拟目录)(E)
在 Active Directory 中配置的 FTP 主目录(A)
设置(S)...
自定义
警报
已成功保存更改。
操作
应用
取消
帮助
联机帮助
功能视图
内容视图


添加 FTP 站点
站点信息
FTP 站点名称(T):
ftp.chinaskills.com
内容目录
物理路径(H):
C:\inetpub\ftproot



（三）在主机 Win2008-C1 中完成 NFS 服务器的部署

1、安装 NFS 相关功能和角色，设置 NFS 目录共享为 d:\sharetest，权限为读写；



2、配置用户名映射，将 CentOS-B2 的 root 用户映射为 administrator 的权限，可以完全访问 NFS 共享目录；

3、在 CentOS-B2 中使用命令进行验证，是否可以成功访问。

Linux 操作系统部分

【说 明】

1、所有 Linux 操作系统的 root 用户的密码为 123456，若未按要求设置密码，涉及到该操作系统下的所有分值记为 0 分。

2、虚拟主机的 IP 属性设置请按照网络拓扑结构图以及“表 3：服务器 IP 地址分配表”的要求设定。

3、除有特别规定外，其他未明确规定用户密码均与用户名相同。

4、所有操作系统镜像文件及试题所需的其他软件均存放于每台计算机的/根目录下，并将题目要求的截图内容以.jpg 格式存储于各物理机桌面 BACKUP_X（X 为组号）文件夹中，文件名、扩展名和存放位置错误，涉及到的所有操作分值记为 0 分。

5、题目要求的虚拟机均安装于每台主机的 D：\virtualPC 目录，即路径为 D：\virtualPC\虚拟主机名称。

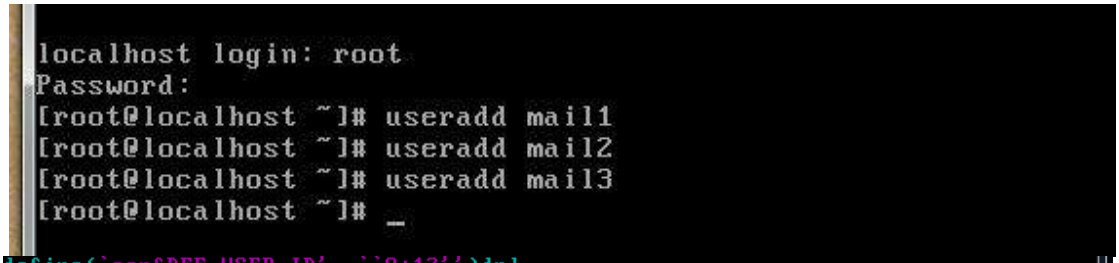
一、在 Server1 上完成如下操作:

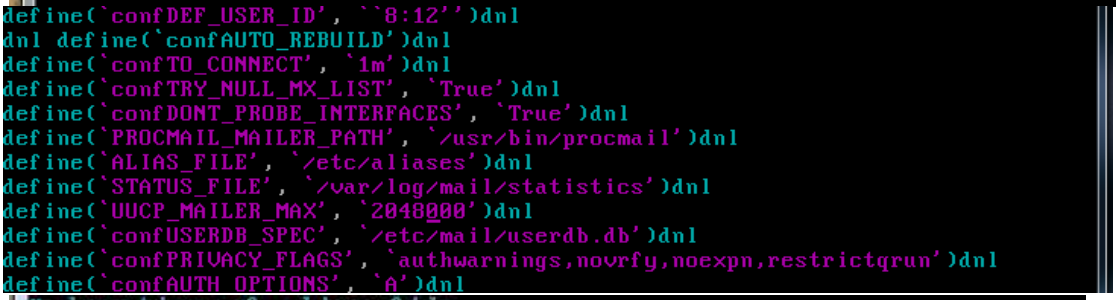
（一）完成虚拟主机的创建

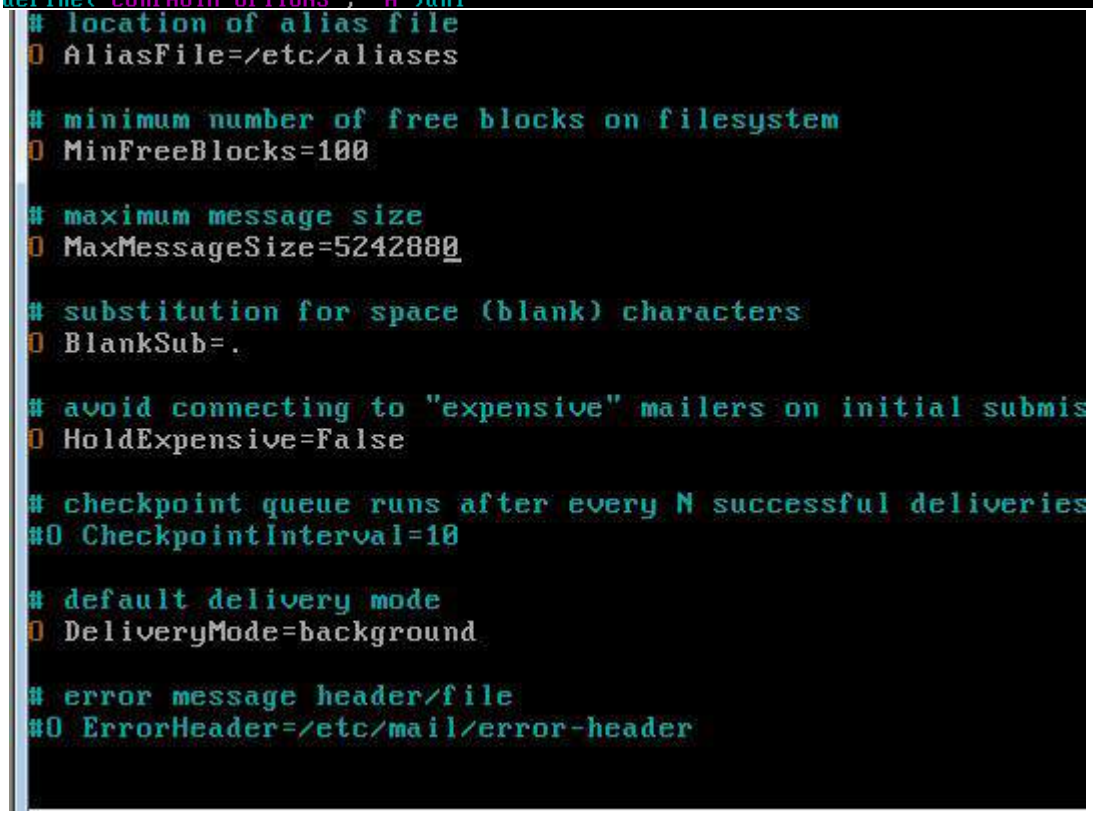
安装名为“Centos-A1”的虚拟机，具体要求为硬盘大小为 20GB，内存为 700MB，系统为 Centos6.5。分区大小为：SWAP 分区大小为 512M；/boot 分区大小为 150M，文件类型为 ext4，/home 分区大小为 1G，文件类型为 ext3，其余为/分区，文件类型为 ext3；将分区结果进行截图，保存为 Centos-A1。

（二）在主机 Centos-A1 中完成 E-MAIL 服务器的部署

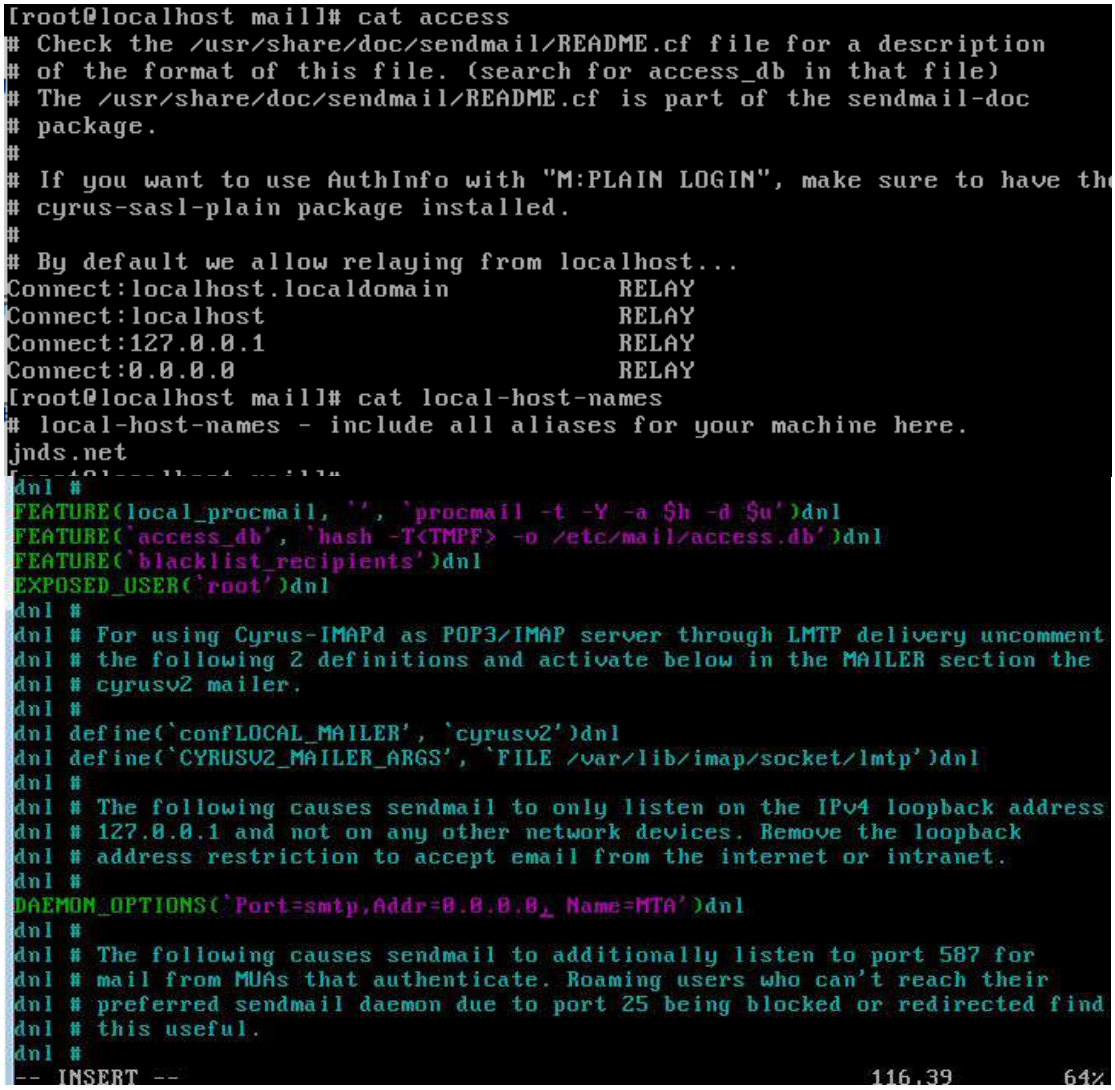
1、在此服务器上安装配置 sendmail 服务，创建创建三个用户 mail1,mail2,mail3；每个用户的邮箱大小为 20MB，限定用户发邮件时，附件大小为 5MB；



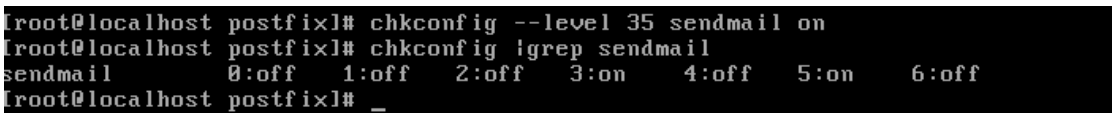




2、为每个员工创建邮箱账户，实现不同用户之间的正常通讯，用户密码为 123，邮件服务器的域名后缀为 jnds.net，邮件服务器要在所有 IP 地址上进行侦听；



3、设置 sendmail 服务需要运行级别 3 和 5 级别开机自动启动，其它运行级别必须为关闭；



4、创建名称为 everyone 的邮件列表，发给 everyone@jnds.net 的邮件，每个员工均可收到；

```
usenet:          news
ftpadm:          ftp
ftpadmin:        ftp
ftp-adm:         ftp
ftp-admin:       ftp
www:             webmaster
webmaster:       root
noc:             root
security:        root
hostmaster:      root
info:            postmaster
marketing:       postmaster
sales:           postmaster
support:         postmaster


# trap decode to catch security attacks
decode:          root

# Person who should get root's mail
#root:           marc
everyone         mail1,mail2,mail3
```

5、要求实现与 chinaskills.com 域进行邮件互通，将成功接收到 chinaskills.com 域邮件的界面截图存储为 mail1；

（三）在主机 Centos-A1 中完成磁盘管理的部署

1、在“Centos-A1”中设置/volume 的空间容量为 30GB，卷组命名为 VG1，逻辑卷命名为 LV1[显示逻辑卷信息截屏保存为 lv1，显示挂载信息截屏保存为 vg1]。

```
[root@localhost ~]# lvcreate -L 29G -n LV1 VG1
  Logical volume "LV1" created
[root@localhost ~]# lvdisplay
  --- Logical volume ---
  LV Path                /dev/VG1/LV1
  LV Name                LV1
  VG Name                VG1
  LV UUID                63s1tB-xfKS-Gw5M-ziQF-TZx6-aL2T-UQudVM
  LV Write Access        read/write
  LV Creation host, time localhost.localdomain, 2016-06-06 11:29:09 -0400
  LV Status              available
  # open                 0
  LV Size                29.00 GiB
  Current LE             7424
  Segments               3
  Allocation             inherit
  Read ahead sectors     auto
  - currently set to     256
  Block device           253:0

[root@localhost ~]# _
```

二、在 Server2 上完成如下操作：

（一）完成虚拟主机的创建

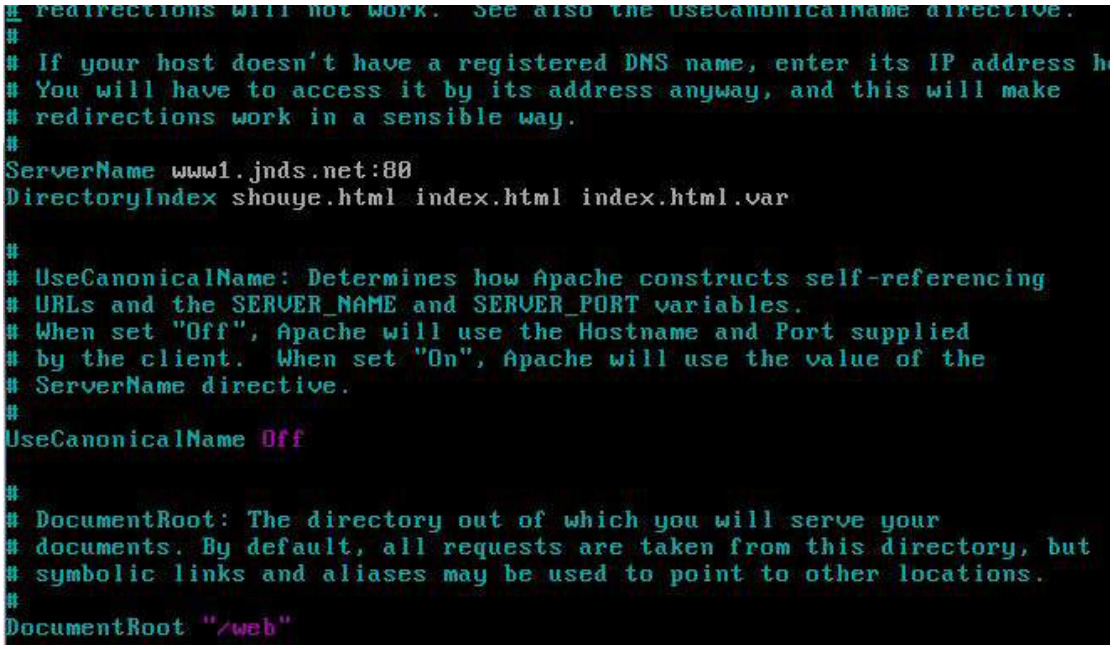
1、安装虚拟机“Centos-B1”,具体要求为内存 512MB，硬盘 10GB；

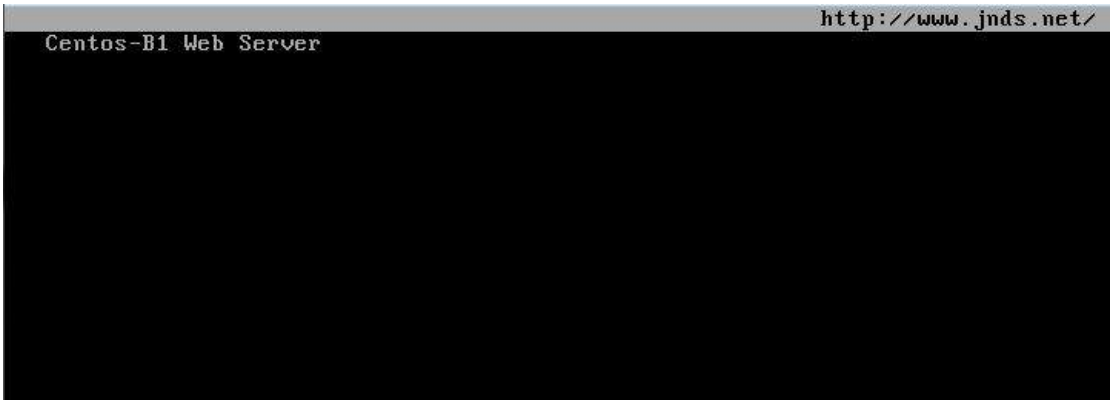
2、安装虚拟机“Centos-B2”,具体要求为内存 512MB,硬盘 10GB;

（二）在主机 Centos-B1 中完成 WEB 服务器 1 的部署

1、在 Centos-B1 上搭建一个 WEB 服务器。站点根目录在/web，首页

文件命名为 shouye.html，内容为 Centos-B1 Web Server。将 www 服务的主配置文件在/root 目录下创建硬链接文件。





（三）在主机 Centos-B2 中完成 SSH 服务器的部署

1、安装 SSH 服务，设置端口号为：2222，不允许管理员进行远程登录。

```
#       $OpenBSD: sshd_config,v 1.80 2008/07/02 02:24:18 djm Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/bin:/usr/bin

# The strategy used for options in the default sshd_config shipped
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options change
# default value.

Port 2222
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

# Disable legacy (protocol version 1) support in the server for ne
# installations. In future the default will change to require expl
# activation of protocol 1
Protocol 2

# HostKey for protocol version 1
#HostKey /etc/ssh/ssh_host_key
-- INSERT --                                                  1,4-
```

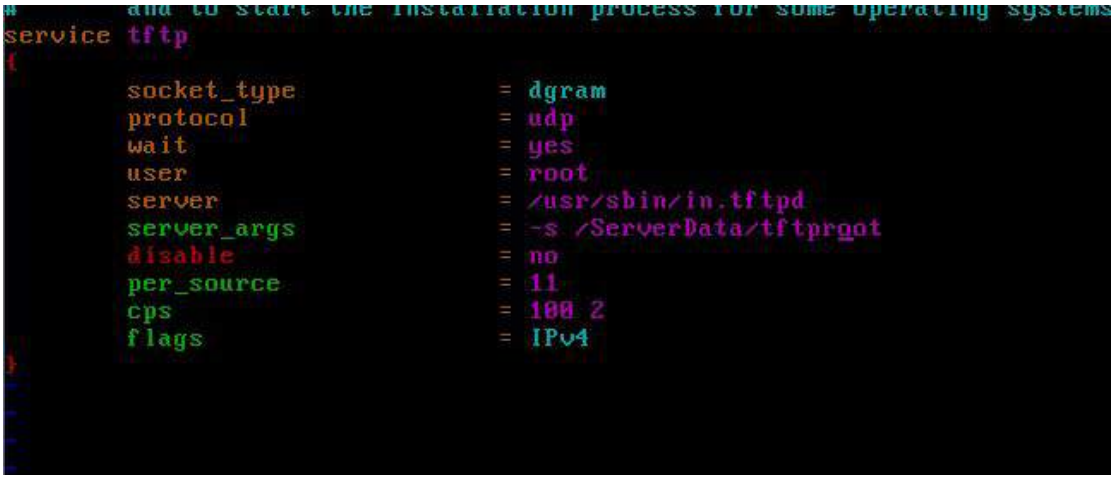
```
#PasswordAuthentication yes
#PermitEmptyPasswords no
PasswordAuthentication NO

# Change to no to disable s/key password
#ChallengeResponseAuthentication yes
```

2、使用 SecureCRT 软件进行连接，要求通过使用密钥，使用户在进行登录时免去输入密码的烦恼。

```
[root@localhost ~]# ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Created directory '/root/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
cc:08:aa:e6:51:af:f1:14:a7:00:bd:76:45:36:b6:b6 root@localhost.localdomain
The key's randomart image is:
+--[ RSA 2048]----+
|        =        |
|   .   + o       |
|  . ..  +        |
|   ....o+.       |
|   .= o.ES       |
|  .o + +         |
| .o . +          |
|o . =            |
| . . .           |
```

（四）在主机 Centos-B2 中完成 TFTP 服务器的部署

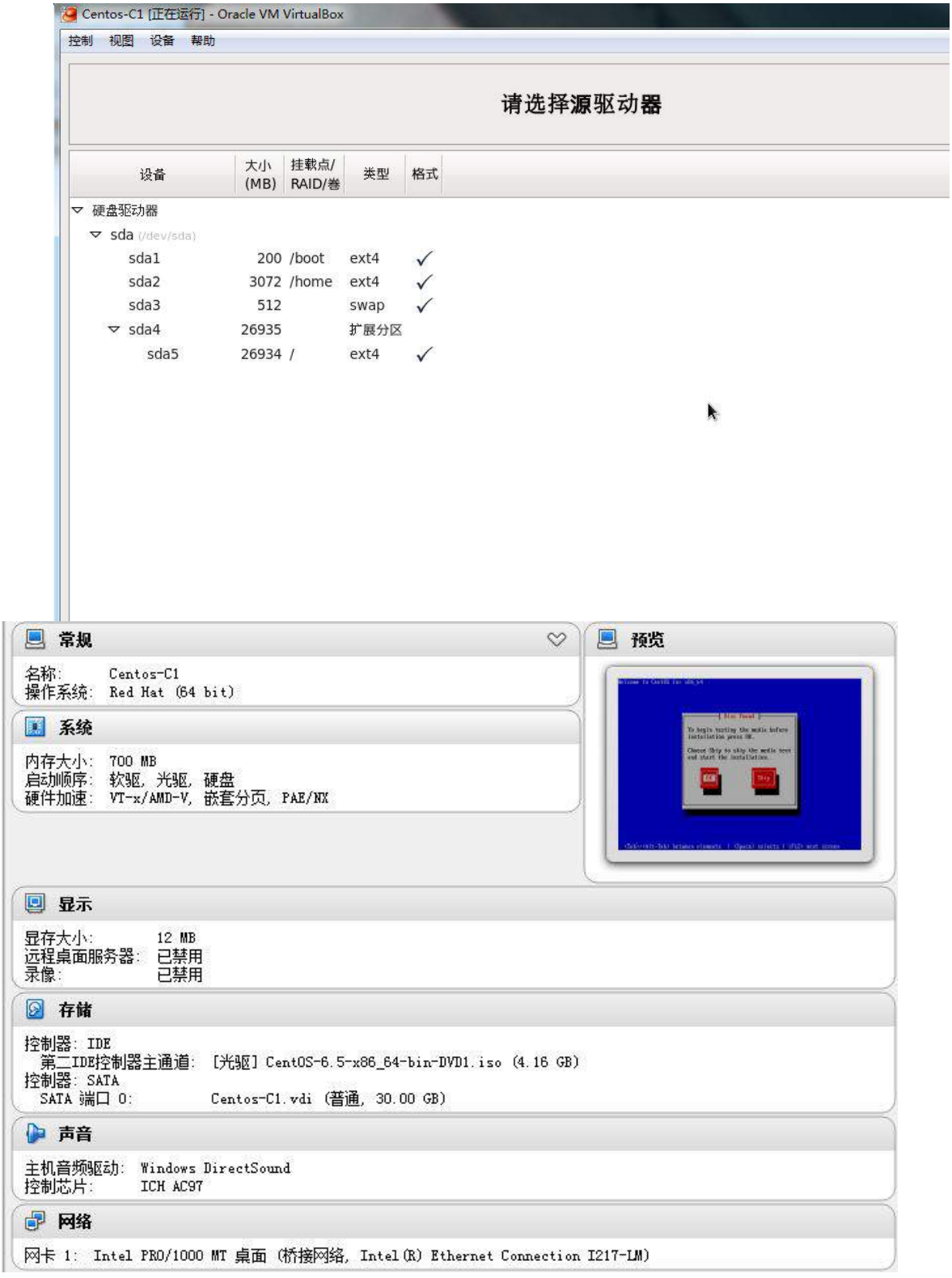
1、安装TFTP服务，将TFTP服务的根目录设置在/ServerData/tftproot。



在 Server3 上完成如下操作：

（一）完成虚拟主机的创建

1、安装名为“Centos-C1”的虚拟机，具体要求为硬盘大小为 30GB，内存为 700MB，系统为 Centos6.5。分区大小为：SWAP 分区大小为 512M；/boot 分区大小为 200M，文件类型为 ext4；/home 分区大小为 3G，文件类型为 ext4，其余为/分区，文件类型为 ext4；将其结果进行截图，保存为 Centos-C1。



2、安装虚拟机“Centos-C2”,具体要求为内存 512MB，硬盘 10GB；

（二）在主机 Centos-C1 中完成 WEB 服务器 2 的部署

1、在 Centos-C1 上搭建 WEB 服务器。站点根目录在/houbeiweb，首页文件命名为 shouye.html，内容为 Centos-C1 Web Server。

```
# You will have to access it by its address anyway, and this will make
# redirections work in a sensible way.
#
ServerName www2.jnds.net:80

DirectoryIndex shoye.html index.html index.html.var
#
# UseCanonicalName: Determines how Apache constructs self-referencing
# URLs and the SERVER_NAME and SERVER_PORT variables.
# When set "Off", Apache will use the Hostname and Port supplied
# by the client.  When set "On", Apache will use the value of the
# ServerName directive.
#
UseCanonicalName Off

#
# DocumentRoot: The directory out of which you will serve your
# documents. By default, all requests are taken from this directory, bu
# symbolic links and aliases may be used to point to other locations.
#
DocumentRoot "/houbeiweb"

#
```

2、借助自签名证书完成 web 服务的配置，结合 ssl 实现安全传输，复制一个 CA 服务器认证证书, 在 win2008-B2 安装此证书，实现安全的访问；

```
[root@localhost certs]# openssl x509 -days 365 -req -in server.csr -signkey serv
er.key -out server.crt
Signature ok
subject=/C=XX/L=Default City/O=Default Company Ltd
Getting Private key
[root@localhost certs]# ls
ca-bundle.crt        localhost.crt    Makefile          server.crt  server.key
ca-bundle.trust.crt  make-dummy-cert  renew-dummy-cert  server.csr
[root@localhost certs]#
```

3、将 Centos-B1 与 Centos-C1 提供负载平衡提供 Web 服务。其中虚拟地址为 10.10.100.250/24，Centos-B1 作为均衡管理主机。将 Centos-B1 设置完成 IP 地址的界面截屏保存命名为 3-1，将 Centos-C1 设置完成 IP 地址的界面截屏保存为 3-2。

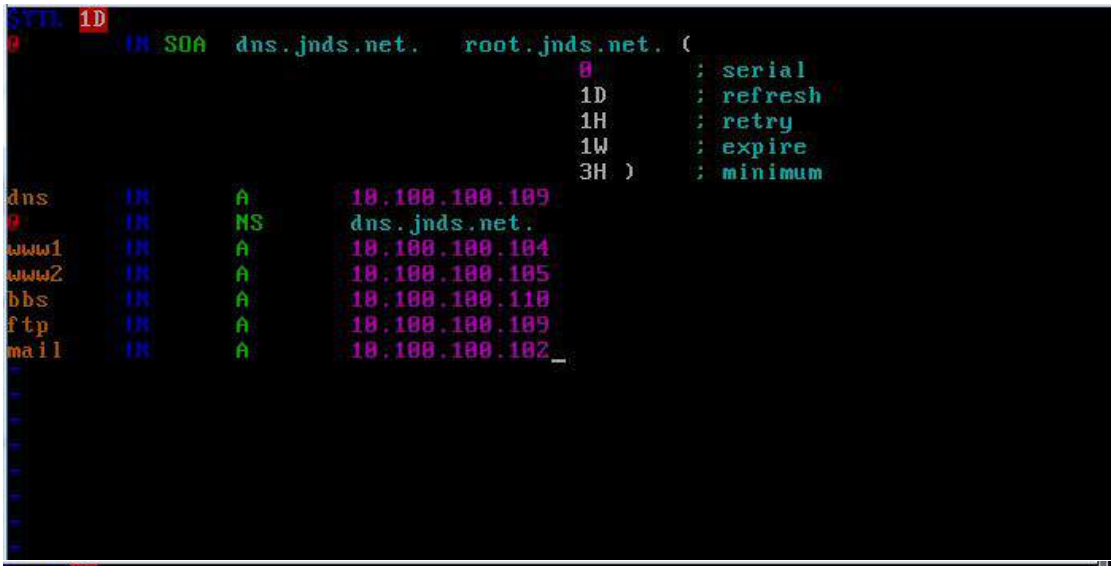
```
[root@localhost network-scripts]# ipvsadm
IP Virtual Server version 1.2.1 (size=4096)
Prot LocalAddress:Port Scheduler Flags
  -> RemoteAddress:Port           Forward Weight ActiveConn InActConn
TCP  10.100.100.250:http rr
  -> www1.jnds.net:http           Masq    1      0          1
  -> www2.jnds.net:http           Local   1      0          3
```

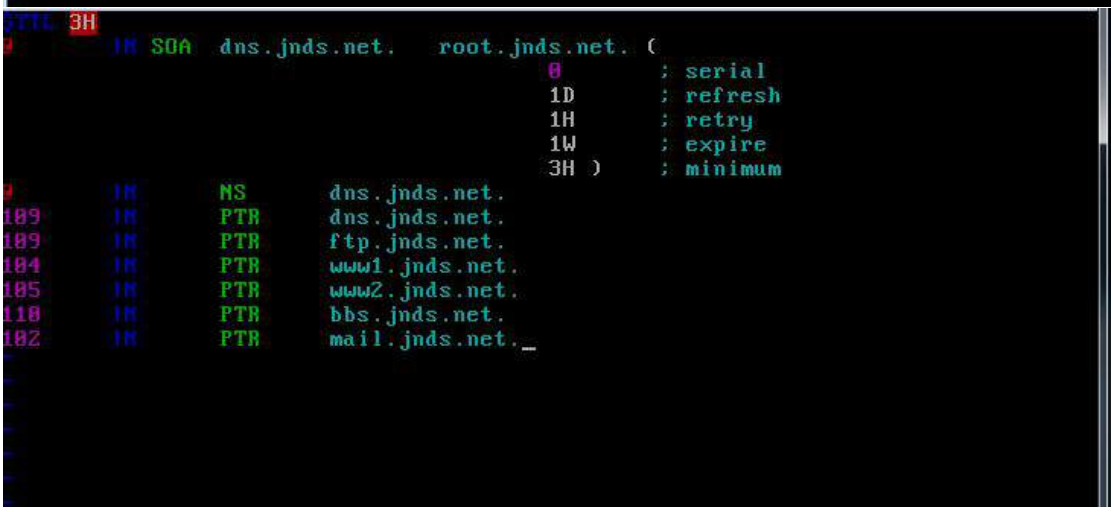
```
eth0:0    Link encap:Ethernet  HWaddr 08:00:27:94:A3:26
          inet addr:10.100.100.250  Bcast:10.100.100.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:108 errors:0 dropped:0 overruns:0 frame:0
          TX packets:108 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:29874 (29.1 KiB)  TX bytes:29874 (29.1 KiB)

lo:0      Link encap:Local Loopback
          inet addr:10.100.100.250  Mask:255.255.255.255
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
```

```
lo:0      Link encap:Local Loopback
          inet addr:10.100.100.250  Mask:255.255.255.255
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
```

（三）在主机 Centos-C2 中完成 bind、 FTP 服务器的部署

1、在此服务器中安装配置 bind 服务，负责区域“jnds.net”内主机解析，分别为 dns.jnds.net 、www1.jnds.net、www2.jnds.net、bbs.jnds.net、smb.jnds.net、ftp.jnds.net 以及 mail.jnds.net,做好正反向 DNS 服务解析；





2、配置 FTP 服务，创设 FTP 服务站点，绑定 ftp 服务地址为 10.100.100.109，域名为 ftp.jnds.net，站点主目录分别为 /var/ftp1，不允许匿名用户访问，开启 ftp 支持被动数据传输模式；

```
# Example config file /etc/vsftpd/vsftpd.conf
#
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
# READ THIS: This example file is NOT an exhaustive list of vsftpd optio
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd
# capabilities.
#
# Allow anonymous FTP? (Beware - allowed by default if you comment this
#anonymous_enable=YES
listen_address=10.100.100.109
local_root=/var/ftp1
pasv_enable=YES_
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 0
# if your users expect that (022 is used by most other ftpd's)
-- INSERT --                                                    15,16
```

3、建立虚拟用户 ftpuser1 及 ftpuser2，密码和用户相同，用户的宿主目录为/home/vsftpd，实现 ftpuser1 用户具有上传和下载的权限，但不能删除文件，ftpuser2 用户可以下载，但不能上传和对文件进行改名；

```
# You may activate the "-R" option to the builtin ls. This is disabled by
# default to avoid remote users being able to cause excessive I/O on large
# sites. However, some broken FTP clients such as "ncftp" and "mirror" assume
# the presence of the "-R" option, so there is a strong case for enabling it.
#ls_recurse_enable=YES
#
# When "listen" directive is enabled, vsftpd runs in standalone mode and
# listens on IPv4 sockets. This directive cannot be used in conjunction
# with the listen_ipv6 directive.
listen=YES
#
# This directive enables listening on IPv6 sockets. To listen on IPv4 and IPv6
# sockets, you must run two copies of vsftpd with two configuration files.
# Make sure, that one of the listen options is commented !!
#listen_ipv6=YES

pam_service_name=vsftpd
userlist_enable=YES
tcp_wrappers=YES
guest_enable=YES
guest_username=ftp
user_config_dir=/etc/vsftpd/vuser_conf
```

```
[root@localhost vsftpd]# db_load -T -t hash -f vuser vuser.db
[root@localhost vsftpd]# cat vuser
ftpuser1
ftpuser1
ftpuser2
ftpuser2
[root@localhost vsftpd]# _
```

```
[root@localhost vuser_conf]# cat ftpuser1
local_root=/home/vsftpd
anon_upload_enable=YES
anon_world_readable_only=YES
anon_other_write_enable=YES
[root@localhost vuser_conf]# cat ftpuser2
local_root=/home/vsftpd
anon_upload_enable=NO
anon_world_readable_only=YES
anon_other_write_enable=NO
[root@localhost vuser_conf]# _
```

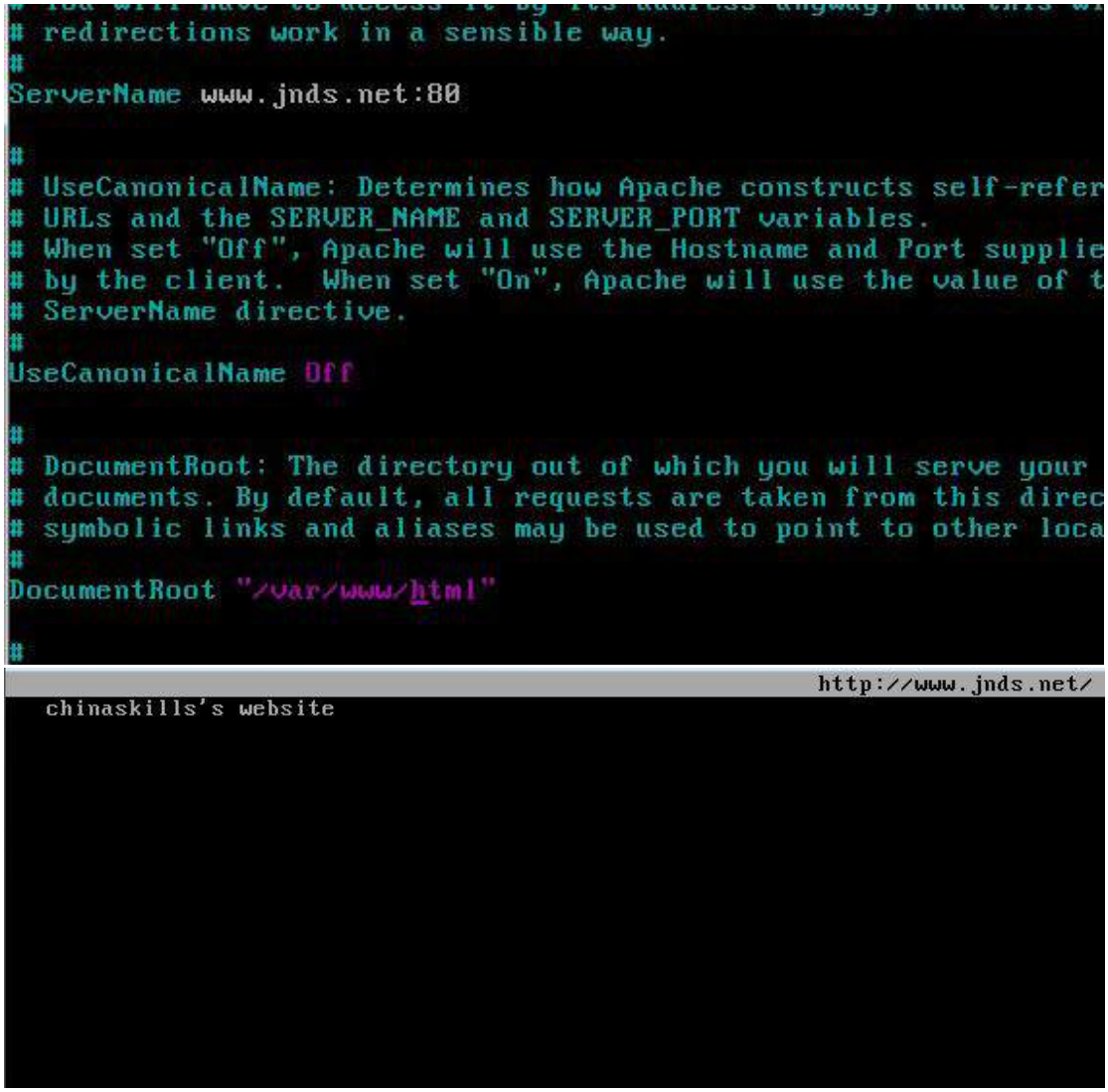
三、在 Server4 上完成如下操作：

（一）完成虚拟主机的创建

1、Server4 主机系统为 CentOS6.5，需要在此 Linux 平台上采用 KVM 方式安装虚拟机“Centos-D1”，具体要求为硬盘大小为 12GB，内存为 768MB，系统为 CentOs6.5；（小提示：如无法正确安装虚拟机 Centos-D1，下述题目中所涉及的虚拟机题目可在 Server4 真实主机中完成）

（二）在主机 Centos-D1 中完成 Apache 服务器以及 MySQL 数据库服务器的部署

1、在此服务器中安装 httpd 服务，建立站点 www.jnds.net，其网站主目录为/var/www/html，首页内容为“chinaskills’ s website” ；



2、使用 openssl 申请证书，创建自签名证书 server.crt 和私钥 server.key，要求只允许使用域名通过 SSL 加密访问；

3、将此服务器配置为 MYSQL 服务器，创建数据库为 userdatabase，在库中创建表为 username，在表中创建 5 个用户，分别为 myuser1、myuser2、myuser3、myuser4、myuser5，口令与用户名相同，需要对登录网站的用户进行身份验证，表结构如下；

字段名	数据类型	主键	自增
ID	int	是	是
name	varchar(10)	否	否
birthday	datetime	否	否
sex	char(1)	否	否
Password	Char（8）	否	否

```
mysql> select * from username;
+----+---------+----------+------+----------+
| ID | name    | birthday | sex  | Password |
+----+---------+----------+------+----------+
|  1 | myuser1 | NULL     | NULL | *A8866F0 |
|  2 | myuser2 | NULL     | NULL | *05BB382 |
|  3 | myuser3 | NULL     | NULL | *19F17B0 |
|  4 | myuser4 | NULL     | NULL | *0AEDED0 |
|  5 | myuser5 | NULL     | NULL | *F7AE551 |
+----+---------+----------+------+----------+
5 rows in set (0.00 sec)
```

```
[root@localhost certs]# mysqladmin -u root password "123456"
[root@localhost certs]# mysql -u root -p123456
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 3
Server version: 5.1.71 Source distribution

Copyright (c) 2000, 2013, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> create database userdatabse;
Query OK, 1 row affected (0.00 sec)

mysql> use userdatabse
Database changed
```

```
mysql> desc username;
+----------+-------------+------+-----+---------+----------------+
| Field    | Type        | Null | Key | Default | Extra          |
+----------+-------------+------+-----+---------+----------------+
| ID       | int(11)     | NO   | PRI | NULL    | auto_increment |
| name     | varchar(10) | YES  |     | NULL    |                |
| birthday | datetime    | YES  |     | NULL    |                |
| sex      | char(1)     | YES  |     | NULL    |                |
| Password | char(8)     | YES  |     | NULL    |                |
+----------+-------------+------+-----+---------+----------------+
5 rows in set (0.00 sec)
```

4、在服务器端使用 iptables 设置防火墙功能,只允许用户访问这台服务器的 WWW 服务，而服务器只能被动地接受连接请求，不能主动的发起连接；

```
[root@localhost certs]# iptables -P OUTPUT DROP
[root@localhost certs]# iptables -I OUTPUT 1 -p tcp -m state --state=RELATED,EST
ABLISHED --sport 80 -j ACCEPT
```

2015 年全国职业院校技能大赛
网络搭建与应用竞赛
（总分 1000 分）

赛题说明

一、竞赛内容分布

“网络搭建与应用”竞赛共分二个部分，其中：

第一部分：网络搭建及安全部署项目，占总分的比例为 45%；

第二部分：服务器配置及应用项目，占总分的比例为 55%；

二、竞赛注意事项

（1）禁止携带和使用移动存储设备、计算器、通信工具及参考资料。

（2）请根据大赛所提供的比赛环境，检查所列的硬件设备、软件清单、材料清单是否齐全，计算机设备是否能正常使用。

（3）本试卷共有两个部分。请选手仔细阅读比赛试卷，按照试卷要求完成各项操作。

（4）操作过程中，需要及时保存设备配置。比赛结束后，所有设备保持运行状态，不要拆、动硬件连接。

（5）比赛完成后，比赛设备、软件和赛题请保留在座位上，禁止将比赛所用的所有物品（包括试卷和草纸）带离赛场。

（6）所有需要提交的文档均放置在桌面的 PC1“比赛文档”文件夹中，禁止在纸质资料上填写与竞赛无关的标记，如违反规定，可视为 0 分。

（7）裁判以各参赛队提交的竞赛结果文档为主要评分依据。所有提交的文档必须按照赛题所规定的命名规则命名，文档中有对应题目的小标题，截图有截图的简要说明，否则按无效内容处理。

（8）与比赛相关的工具软件放置在 D 盘的 tools 文件夹中。

项目背景及网络拓扑

某企业总部设立在广州，分部设在深圳，为了实现快捷的信息交流和资源共享，需要跨越互联网进行实时数据传输。

广州公司、深圳公司都采用防火墙接入互联网络，用来保护内网用户资源，为了保障与深圳公司业务数据流传输的高可用性，总公司与分公司通过租用 ISP 专线链路相连，做为主链路，承载数据流。另外通过 Internet 建立虚拟专用网，做为备用链路。

广州公司为了安全管理每个部门的用户，使用 VLAN 技术将每个部门的用户划分到不同的 VLAN 中，总公司内网用户采用了有线接入方式。

由于深圳公司业务发展迅速，在原有的有线架构实现与总公司互联的基础上，增加了无线接入方式，更方便来访人员访问网络资源。

为了实现快捷的信息传递和公司业务的需求，允许 SOHO 办公和出差的员工能够方便、快捷、安全的访问总公司内网服务器群。

为了公司的业务安全，所有接入交换机都启用安全管理手段，防止非授权访问，无线用户之间相互隔离。

具体的拓扑结构如下图所示：

注：二层交换机没有 OSPF

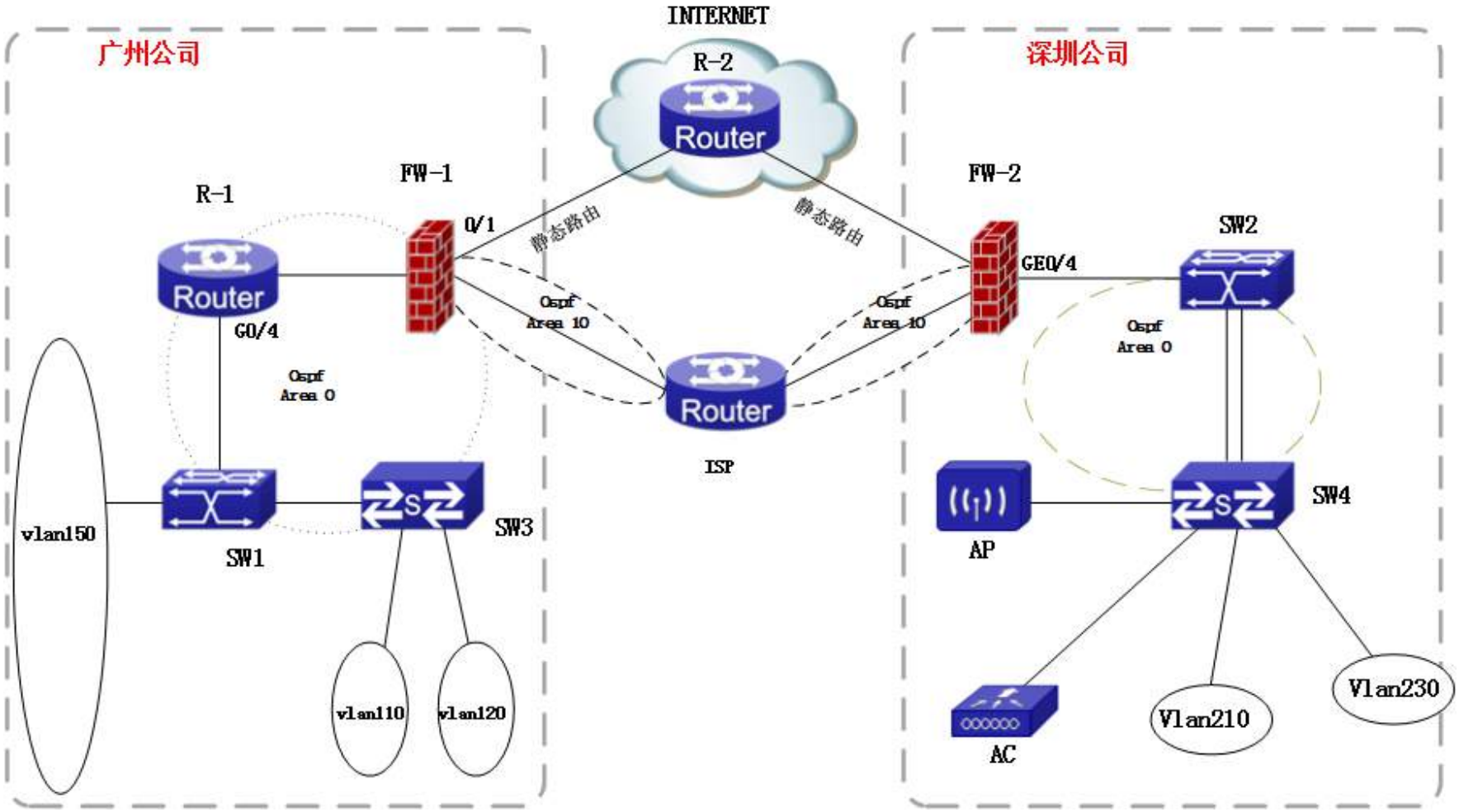


表 1 网络设备连接和 IP 地址表

A 设备连接至 B 设备			
设备名称	接口	设备名称	接口
R-1	GigaEthernet0/3	FW1	Ethernet0/4
R-1	GigaEthernet 0/4	SW1	Ethernet1/0/24
SW1	Ethernet1/0/23	SW3	Ethernet1/24
FW-1	Ethernet0/3	R-1	GigaEthernet0/3
FW-1	Ethernet0/2	ISP	GigaEthernet0/3
R-1	GigaEthernet0/4	FW-2	Ethernet0/3
ISP	GigaEthernet0/4	FW-2	Ethernet0/2
FW-2	Ethernet0/4	SW2	Ethernet1/0/24
SW2	Ethernet1/0/22	SW4	Ethernet1/22
SW2	Ethernet1/0/21	SW4	Ethernet1/21
SW4	Ethernet1/22	AP	lan
SW4	Ethernet1/21	AC	Ethernet1/0/24

设备	设备名称	设备接口	IP 地址
路由器	R1	GigaEthernet0/3	
		GigaEthernet0/4	
	R2	GigaEthernet0/3	
		GigaEthernet0/4	
	ISP	GigaEthernet0/3	
		GigaEthernet0/4	
防火墙	FW1	Ethernet0/2	
		Ethernet0/3	
		Ethernet0/4	
	FW2	Ethernet0/2	
		Ethernet0/3	
		Ethernet0/4	
三层交换机	SW1	Ethernet1/0/24(vlan100)	
	SW2	Ethernet1/0/24(vlan100)	

表 2：服务器 IP 地址分配表

宿主机	虚拟主机名称	域名信息	服务角色	系统及版本信息	IPv4 地址信息
PC1	Win2008-A1	dns.chinaskills.org	DNS 服务器	Windows Server 2008 R2	IP: 10.1.5.100
	Win2003-A1	dfs.chinaskills.org	DFS 服务器	Windows Server 2003	IP: 10.1.5.101

				R2	
	Centos-A1	mail.jnds.net	邮件服务器	Centos 6.5	IP: 10.1.5.102
	Centos-A2	已有系统			
PC2	Win2008-B1	rodc.chinaskills.org	RODC 和 NAP 服务器	Windows Server 2008 R2	IP: 10.1.5.150
	Win2008-B2	www.chinaskills.org	Web 及 DFS 服务器	Windows Server 2008 R2	IP: 10.1.5.103
	Centos-B1	www1.jnds.net	WEB 服务器	Centos 6.5	IP: 10.1.5.104 IP: 10.1.5.105
	Centos-B2	ftp.jnds.net ftp1.jnds.net ftp2.jnds.net	TFTP 和 NIS 服务器	Centos 6.5	IP: 10.1.5.106 IP: 10.1.5.107
PC3	Win2008-C1	dc.chinaskills.org	域控制器和 NFS 服务器	Windows Server 2008 R2	IP: 10.1.5.160 IP: 10.1.5.161 IP：2001:DA8:3010::1/64
	Win2003-C1 已有系统	mail.chinaskills.org	E-mail 和 FTP 服务器	Windows Server 2003 R2	IP：10.1.5.108 IP：2001:DA8:3010::2/64
	Centos-C1	www2.jnds.net	Web 及负载均衡	Centos6.5	IP: 10.1.5.109 IP: 10.1.5.110 IP：2001:DA8:3010::3/64
	Centos-C2	dns.jnds.net	Bind 及 FTP 服务器	Centos6.5	IP: 10.1.5.250
PC4（Linux 虚拟化主机）	Centos-D1	bbs.jnds.net	MySQL 数据库服务器	Centos 6.5	IP: 10.1.5.120

网络搭建部分（450分）

1、 设备 console 线有两条。交换机， AC，防火墙使用同一条 console 线，路由器使用另外一条 console 线。

2、 设备配置完毕后，保存最新的设备配置。保存文档方式分为两种：

a) 交换机和路由器要把 show running-config 的配置保存在 PC1 桌面的相应文档中，文档命名规则为：设备名称.doc,例如：RT1 路由器文件命名为：RT1.doc，然后放入到 PC1 桌面上“比赛文档”文件夹中

b) 防火墙等截图方式的设备，把截图的图片放到同一 word 文档中，文档命名规则为：设备名称.doc,例如：防火墙 FW1 文件命名为：FW1.doc, 保存后放入到 PC1 桌面上“比赛文档”文件夹中。

1、 物理连接与 IP 地址划分

（1） 按照网络拓扑图制作以太网网线，并连接设备。要求符合 T568A 和 T568B 的标准，其线缆长度适中。

（2） 互联地址使用 192.168.2.0/30，总部使用 10.1.0.1 网段，服务器区为 10.1.5.0/24.根据“拓扑结构图”和“表 2:网络设备 IP 地址分配表”所示，对网络中的所有设备接口配置 IP 地址。

2、 交换机配置

（1）为交换机设备命名，命名规则参考为表 1 中的“设备名称”。

（2）在所有交换机上开启 telnet 登录,用户名和密码都为 jnjs123。

（3）在 SW1 和 SW2 上配置 OSPF 路由协议和基于接口和区域的验证，采用 MD5 方式，用户名和密码都为 jnjs123。

（4） 根据表中的 vlan 划分，在各交换机上划分 VLAN。

（5）在 SW1 上配置 DHCP 服务，实现 VLAN110 和 VLAN120 自动获取 IP 地址，并指定其各自的网关。排除地址范围为 10.1.1.1~10.1.1.10 和 10.1.2.1~10.1.2.10。

（6）为了防止网络中的 DHCP 无赖设备攻击，需要在网络中部署 DHCP 监听技术，为了保障客户机正常获取 IP 地址，需要配置 DHCP 中继技术。

（7）在 SW1 上配置端口镜像，要求把 E0/0/23 口的进出流量都镜像到 e0/0/10 接口。

（8）限制 SW1 的 VLAN150 的输入带宽限制最大值为 2M，突发流量为 1M。禁止交换机所有以太口对 445 端口的 TCP 和 UDP 数据通讯。接入 VLAN110 的计算机只允许来自 VLAN120 地址的计算机进行远程控制（远程控制协议使用 3389 端口）。

（9）在 SW2 和 SW4 上配置接口链路聚合，实现基于目标 IP 地址的负载分担。

（10）配置 DHCP 服务，实现 AC、AP 和无线用户分别自动获取管理地址及对应无线用户 IP 地址，并指定其各自的网关。

（11）在 SW3 的 Fa 0/5 上配置端口安全，安全 MAC 地址为：00-12-F1-00-ab-01，安全 IP 地址为 10.1.1.60/24，并进行 IP 和 MAC 地址的绑定配置。

（12）在 SW3 和 SW4 上配置端口安全，实现每个接口只允许 1 个主机访问，违规关闭接口。

（13）在 SW3 和 SW4 上开启快速生成树，使所有的接入端口为 portfast 端口。

路由器配置与调试

（1） 为路由器设备命名，命名规则参考为表 1 中的“设备名称”。

（2） 把下面的设备 RID 设置上，要求不能增加接口的相关信息。

设备名称	RID
R1	1.1.1.1
R2	2.2.2.2
ISP	4.4.4.4
FW-1	5.5.5.5
FW-2	3.3.3.3
SW1	6.6.6.6
SW2	7.7.7.7

（3）为所有路由器开启 telnet 登录，允许远程管理路由器，采用 Radius 和本地验证。密码为 jnds123。

（4）在 R1 和 ISP 上配置 OSPF 路由协议，实现深圳公司与珠海公司的通信。

（5）在 R1 和 ISP 路由器上配置 OSPF 基于接口和区域的验证，采用 MD5 验证方式，密钥为 jnjs123。

（6）在 R1 配置默认路由指向 FW-1，并分发于广州公司 LAN，使 VLAN110、120 都能访问互联网。

（7）在 R1 配置接口描述，例如“R-1 路由器的 FA0/1 接口与 R-1 连接”其描述为“R-1 TO R-2 interface FA0/1”。

（8)在 R1 配置 Radius 客户端,Radius 服务器地址为 10.1.5.8,密钥为 jnjs123。

（9）在 R1 在接口 s2/0 限制出口流量，正常流量值和突发流量分别限制速率为 1M 和 2M。

（10）在 R2 配置两条静态路由，分别指向广州公司与深圳。

3、 广域网和防火墙配置

（1）为防火墙设备命名，命名规则参考为表 1 中的“设备名称”。

（2）在 FW-1 配置 12tp VPN，实现远程访问用户可以通过拨入 VPN 连接安全访问内部服务器群 VLAN150 的服务，其分配的地址池为 10.1.4.0/24。

（3）配置 Site-To-Site VPN，对等体分别为 FW-1 的 GE3 接口与 FW-2 的 GE2 接口，允许承载 ping 服务。作为广州公司和深圳公司的备份链路，当租用 ISP 链路出现问题时作为备份链路。

（4）将 FW-1 的以太口 2 连接的网络为 DMZ 区域，表示服务器用户；以太口 3 连接的网络为 trust 区域，表示内网用户；以太口 1 连接的网络为 untrust 区域，表示互联网。

（5）在 FW-1 上配置安全策略最大限度的保证内网和服务器群安全，保护内网和服务器群的安全，防止 DDOS 攻击。

（6）在 FW-1 上创建时间访问控制列表，内网用户只有工作日（周一~周五）的工作时间（9:00~18:00）才能访问互联网。允许互联网用户访问 WEB 服务和 FTP 服务；允许远程 VPN 拨入的用户访问内网所有资源；允许深圳公司用户访问服务群中的所有服务。

（7）在 FW-1 上配置 NAT，实现内部网络（VLAN110、VLAN120、VLAN130）访问互联网，其使用合法的公网地址为 211.1.1.1/28；实现将内网的 WEB、FTP（10.1.5.10、10.1.5.11）资源发布到互联网上，分别使用 FW-1 的外网接口 211.1.1.1/30 地址的相对应端口。

（8）在 FW-1 和 FW-2 配置 OSPF 基于接口和区域的验证，采用 MD5 方式，密码为 jnjs123。

（9)在 FW-1 配置 OSPF 虚链路,实现广州公司与深圳公司的网络互通。配置 GE0/1 接口的静态路由指向互联网，以实现内网用户正常访问互联网。

（10）在 FW-2 上配置 OSPF 路由，实现广州公司与深圳公司可以通过 ISP 路由器正常通信。

（11）Dos 和 DDos 攻击主要分“网络带宽攻击”和“连通性攻击”两种，SynFlood 攻击，land 攻击，Tear Drop 攻击，Ping of Death 攻击会消耗操作系统资源，Smuf 攻击，ICMP Flood 攻击，Session Flood 攻击会消耗网络带宽资源。请在防火墙做适当的配置,防止内网用户免受来自 Internet 上所有 Dos/DDoS 的攻击。

（12）VLAN200- VLAN210 的计算机下行上行速率为 300K。每天 08：00~12：00,14:00~18:00 不允许所有办公室用户计算机访问互联网。记录内网用户访问互联网的URL。内网用户不能访问盛大网游(www.sd.com),巨人网游(www.jr.com)的网页。凡是一个网页含有超过 2 次“色情”、“反动”、“暴力”等字样时必须过滤。启动 NAT 转换策略，使内部所有网段转换成 WAN 上接口的 IP 地址。

4、 无线配置

（1） 把无线控制器进行设备命名，命名规则参考为表 1 中的“设备名称”。

（2） 无线控制器建立 2 个 SSID,SSID 分别为 sale1 和 sale2，sale2 的 SSID 设置为隐藏，工作信道为自动；使用无线控制器提供 DHCP 服务，获得 sale1 的地址在 vlan10 内，获得 sale2 的地址在 vlan20 内,用户动态分配 IP 地址和网关，DNS 地址为：202.106.0.20，其分配的地址段为自行计算，需要排除网关，地址租约为 2 天。用户接入无线网络时需要输入密码，加密模式为 wpa-personal,其口令为：chinaskill。

（3） 激活无线网络的二层隔离，实现同一个 AP 下无线局域网内用户不能互相访问。

（4） 保障无线信息的覆盖性，无线 AP 的发射功率设置为 90%。

（5） 阻止 MAC 地址为 F0-DE-F1-F2-8C-CC 的主机连接上海分公司的无线。

Windows 操作系统

【说 明】

（1）题目中所涉及 Windows 操作系统的 administrator 管理员以及其他普通用户密码均为 2015Network_X（X 为组号），若未按照要求设置密码，涉及到该操作的所有分值记为 0 分。

（2）虚拟主机的 IP 属性设置请按照网络拓扑结构图以及“表 3：服务器 IP 地址分配表”的要求设定。

（3）所有系统镜像文件及试题所需的其它软件均存放在每台主机的 D:\soft 文件夹中，并将题目要求的截图内容以.jpg 格式存储于各物理机桌面 BACKUP_X（X 为组号）文件夹中，文件名、扩展名和存放位置错误，涉及到的所有操作分值记为 0 分。

（4）题目要求的虚拟机均安装于每台主机的 D：\virtualPC 目录，即路径为 D：\virtualPC\虚拟主机名称。

一、在 PC 1 上完成如下操作:

（一）通过 Hyper-V 完成虚拟主机的创建

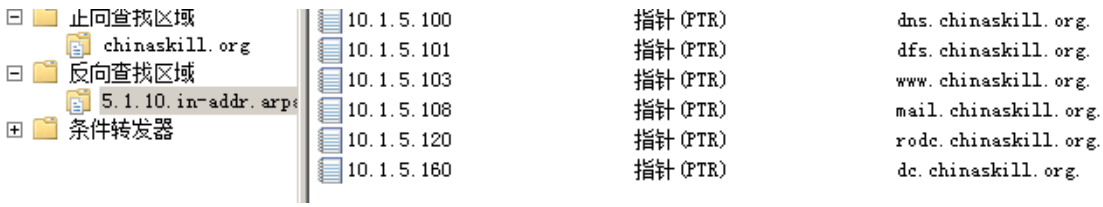
1、PC1 主机系统为 Windows，需要在此 Windows 平台上采用 Hyper-V 方式安装虚拟机“Win2008-A1”，具体要求为内存为 1G，硬盘 30G；

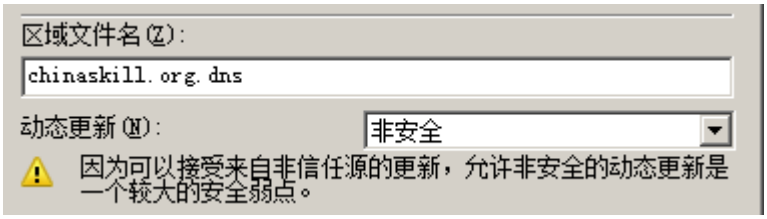
2、在虚拟机“Win2008-A1”中添加 SCSI 控制器，添加二块 SCSI 虚拟硬盘，其每块硬盘的大小为 15G；将二块硬盘制作成 RAID1，磁盘盘符为 e:\；

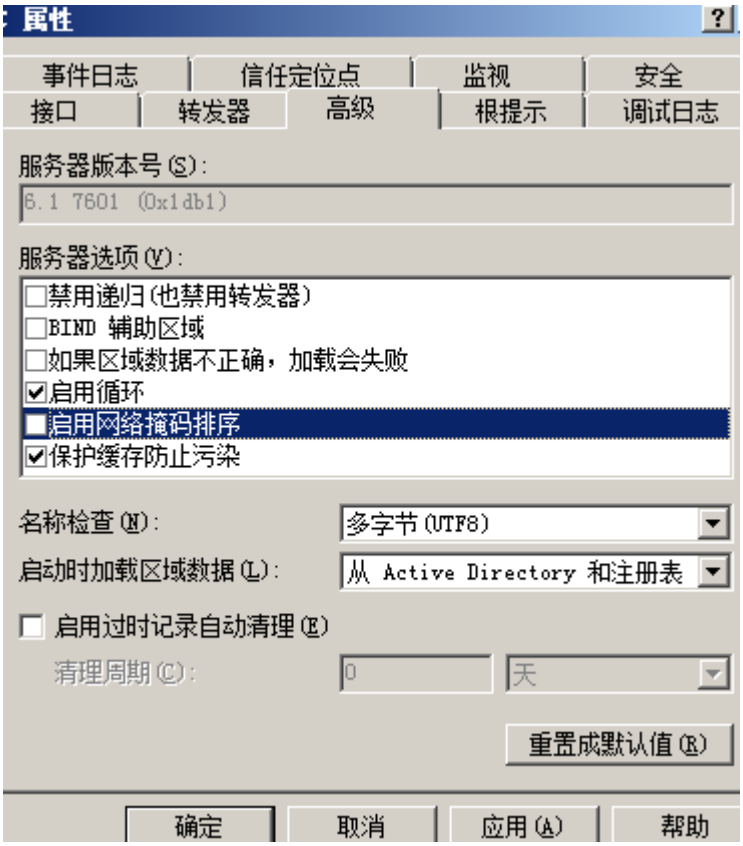
3、PC1 主机系统为 Windows，需要在此 Windows 平台上采用 Hyper-V 方式安装虚拟机“Win2003-A1”，具体要求为内存为 1G，硬盘 30G，并将服务器加入到 Windows 域环境；

（二）在主机 **Win2008-A1** 中完成 **DNS** 服务器的部署

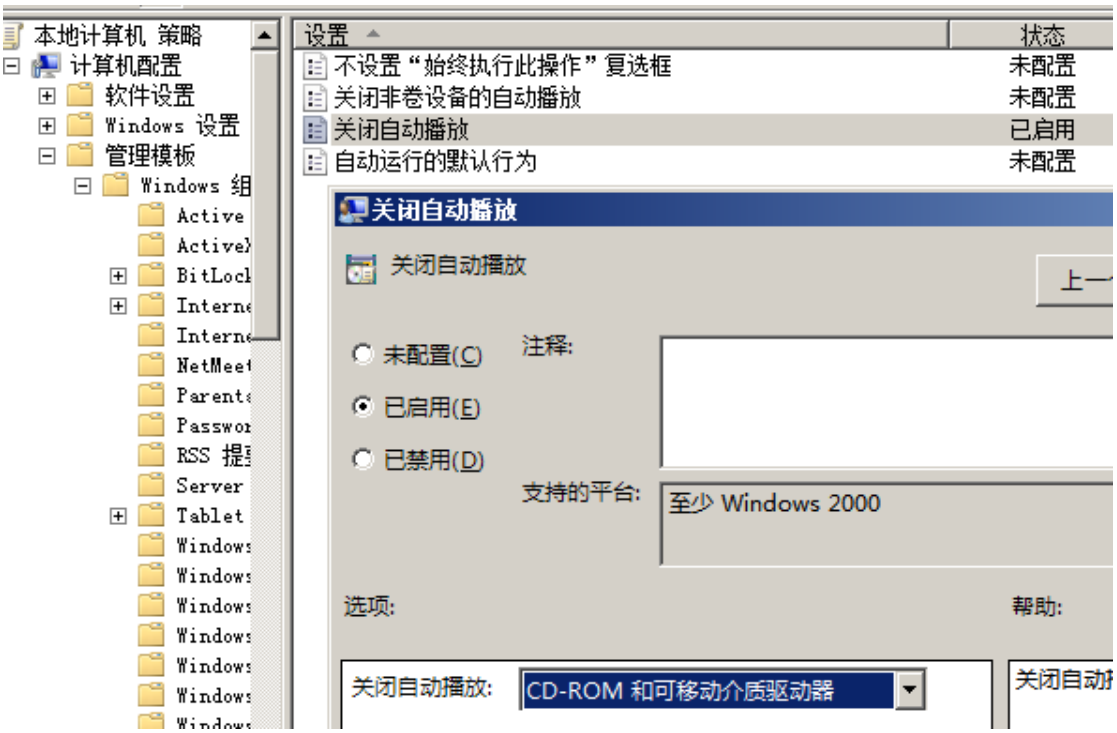
1、将此服务器配置为主 DNS 服务器，正确配置 chinaskills.org 域名的正向及反向解析区域，能够正确解析 chinaskills.org 域中的所有服务器；创建对应服务器主机记录，需要关闭网络掩码排序功能，设置 DNS 服务正向区域和反向区域与活动目录集成；要求动态更新设置为非安全；

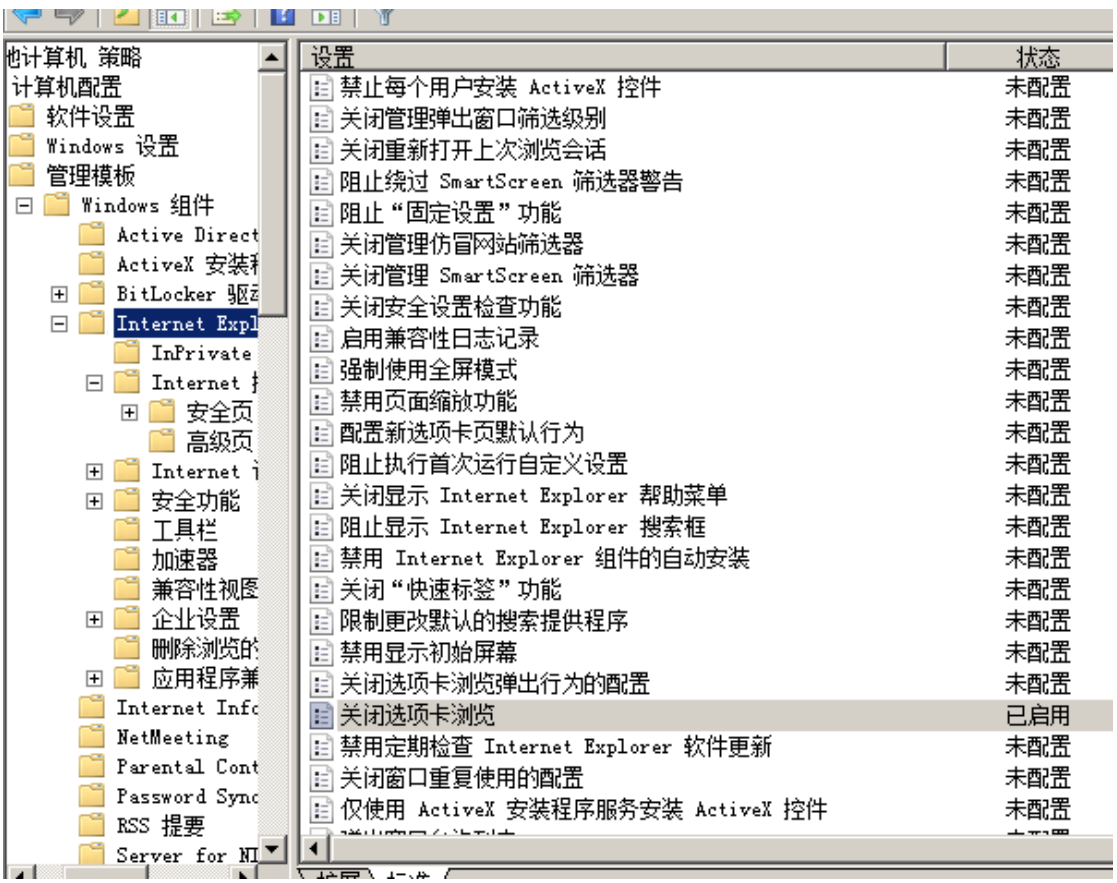




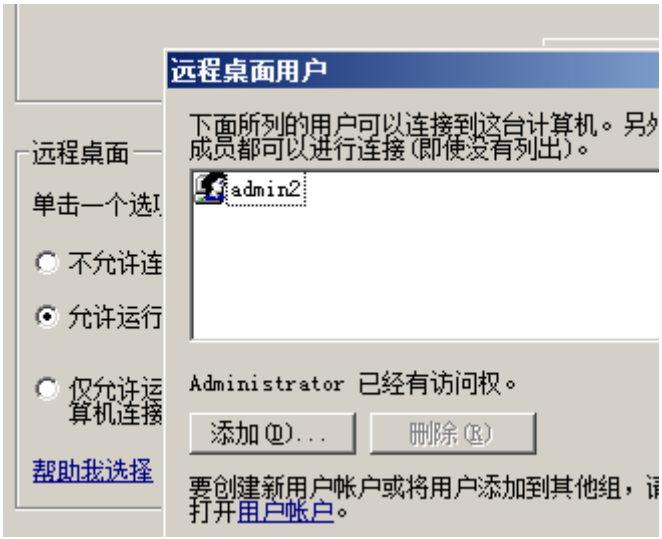


2、配置组策略，要求所有域内计算机禁用光盘自动播放，不在桌面显示网上邻居图标，禁用 IE 的安全选项卡。；

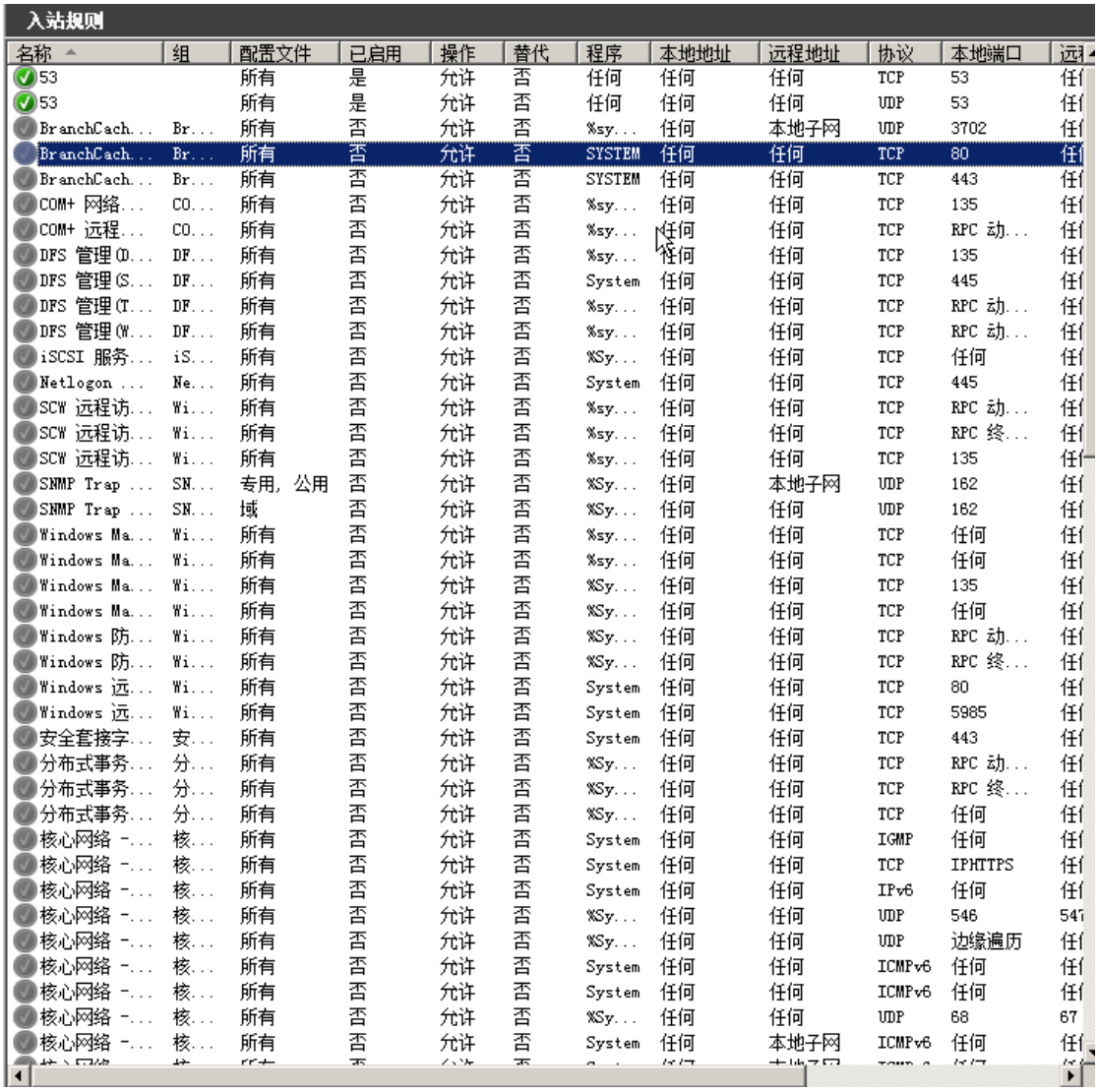

本地计算机 策略
计算机配置
软件设置
Windows 设置
管理模板
Windows 组
设置
状态
不设置“始终执行此操作”复选框 未配置
关闭非卷设备的自动播放 未配置
关闭自动播放 已启用
自动运行的默认行为 未配置
关闭自动播放
关闭自动播放
上一
未配置(C)
已启用(E)
已禁用(D)
注释:
支持的平台:
至少 Windows 2000
选项:
帮助:
关闭自动播放:
CD-ROM 和可移动介质驱动器


计算机配置
软件设置
Windows 设置
管理模板
Windows 组件
设置
状态
禁止每个用户安装 ActiveX 控件 未配置
关闭管理弹出窗口筛选级别 未配置
关闭重新打开上次浏览会话 未配置
阻止绕过 SmartScreen 筛选器警告 未配置
阻止“固定设置”功能 未配置
关闭管理仿冒网站筛选器 未配置
关闭管理 SmartScreen 筛选器 未配置
关闭安全设置检查功能 未配置
启用兼容性日志记录 未配置
强制使用全屏模式 未配置
禁用页面缩放功能 未配置
配置新选项卡页默认行为 未配置
阻止执行首次运行自定义设置 未配置
关闭显示 Internet Explorer 帮助菜单 未配置
阻止显示 Internet Explorer 搜索框 未配置
禁用 Internet Explorer 组件的自动安装 未配置
关闭“快速标签”功能 未配置
限制更改默认的搜索提供程序 未配置
禁用显示初始屏幕 未配置
关闭选项卡浏览弹出行为的配置 未配置
关闭选项卡浏览 已启用
禁用定期检查 Internet Explorer 软件更新 未配置
关闭窗口重复使用的配置 未配置
仅使用 ActiveX 安装程序服务安装 ActiveX 控件 未配置

3. 打开远程桌面功能，允许使用 admin2 登录；

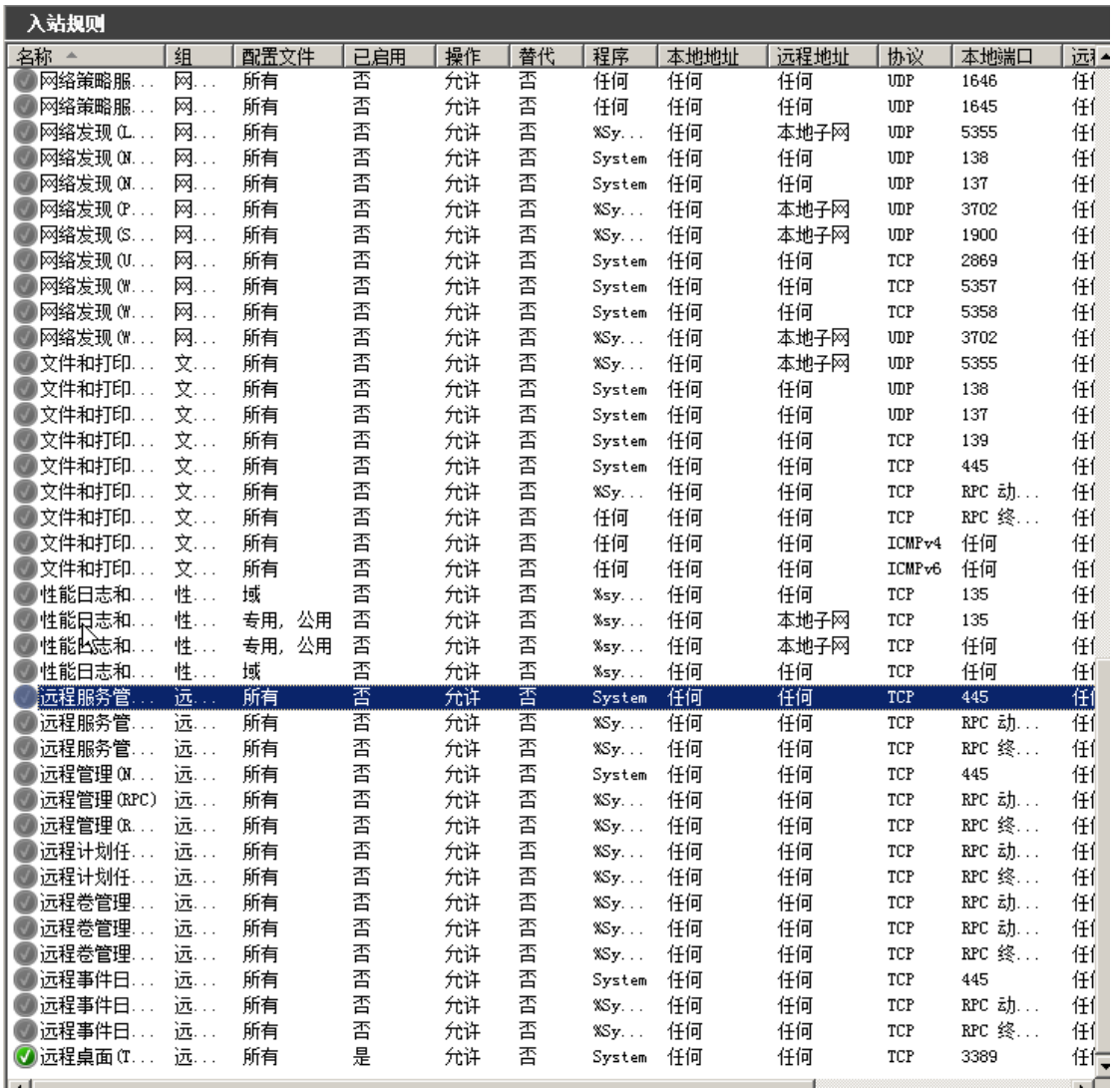


4. 开启系统防火墙，关闭除服务端口外的其他端口；



入站规则

名称	组	配置文件	已启用	操作	替代	程序	本地地址	远程地址	协议	本地端口	远程
53		所有	是	允许	否	任何	任何	任何	TCP	53	任
53		所有	是	允许	否	任何	任何	任何	UDP	53	任
BranchCach...	Br...	所有	否	允许	否	%sy...	任何	本地子网	UDP	3702	任
BranchCach...	Br...	所有	否	允许	否	SYSTEM	任何	任何	TCP	80	任
BranchCach...	Br...	所有	否	允许	否	SYSTEM	任何	任何	TCP	443	任
COM+ 网络...	CO...	所有	否	允许	否	%sy...	任何	任何	TCP	135	任
COM+ 远程...	CO...	所有	否	允许	否	%sy...	任何	任何	TCP	RPC 动...	任
DFS 管理(D...	DF...	所有	否	允许	否	%sy...	任何	任何	TCP	135	任
DFS 管理(S...	DF...	所有	否	允许	否	System	任何	任何	TCP	445	任
DFS 管理(T...	DF...	所有	否	允许	否	%sy...	任何	任何	TCP	RPC 动...	任
DFS 管理(W...	DF...	所有	否	允许	否	%sy...	任何	任何	TCP	RPC 动...	任
iSCSI 服务...	iS...	所有	否	允许	否	%Sy...	任何	任何	TCP	任何	任
Netlogon ...	Ne...	所有	否	允许	否	System	任何	任何	TCP	445	任
SCW 远程访...	Wi...	所有	否	允许	否	%sy...	任何	任何	TCP	RPC 动...	任
SCW 远程访...	Wi...	所有	否	允许	否	%sy...	任何	任何	TCP	RPC 终...	任
SCW 远程访...	Wi...	所有	否	允许	否	%sy...	任何	任何	TCP	135	任
SNMP Trap ...	SN...	专用, 公用	否	允许	否	%Sy...	任何	本地子网	UDP	162	任
SNMP Trap ...	SN...	域	否	允许	否	%Sy...	任何	任何	UDP	162	任
Windows Ma...	Wi...	所有	否	允许	否	%sy...	任何	任何	TCP	任何	任
Windows Ma...	Wi...	所有	否	允许	否	%sy...	任何	任何	TCP	任何	任
Windows Ma...	Wi...	所有	否	允许	否	%Sy...	任何	任何	TCP	135	任
Windows Ma...	Wi...	所有	否	允许	否	%Sy...	任何	任何	TCP	任何	任
Windows 防...	Wi...	所有	否	允许	否	%Sy...	任何	任何	TCP	RPC 动...	任
Windows 防...	Wi...	所有	否	允许	否	%Sy...	任何	任何	TCP	RPC 终...	任
Windows 远...	Wi...	所有	否	允许	否	System	任何	任何	TCP	80	任
Windows 远...	Wi...	所有	否	允许	否	System	任何	任何	TCP	5985	任
安全套接字...	安...	所有	否	允许	否	System	任何	任何	TCP	443	任
分布式事务...	分...	所有	否	允许	否	%Sy...	任何	任何	TCP	RPC 动...	任
分布式事务...	分...	所有	否	允许	否	%Sy...	任何	任何	TCP	RPC 终...	任
分布式事务...	分...	所有	否	允许	否	%Sy...	任何	任何	TCP	任何	任
核心网络 -...	核...	所有	否	允许	否	System	任何	任何	IGMP	任何	任
核心网络 -...	核...	所有	否	允许	否	System	任何	任何	TCP	IPHTTPS	任
核心网络 -...	核...	所有	否	允许	否	System	任何	任何	IPv6	任何	任
核心网络 -...	核...	所有	否	允许	否	%Sy...	任何	任何	UDP	546	547
核心网络 -...	核...	所有	否	允许	否	%Sy...	任何	任何	UDP	边缘遍历	任
核心网络 -...	核...	所有	否	允许	否	System	任何	任何	ICMPv6	任何	任
核心网络 -...	核...	所有	否	允许	否	System	任何	任何	ICMPv6	任何	任
核心网络 -...	核...	所有	否	允许	否	%Sy...	任何	任何	UDP	68	67
核心网络 -...	核...	所有	否	允许	否	System	任何	本地子网	ICMPv6	任何	任

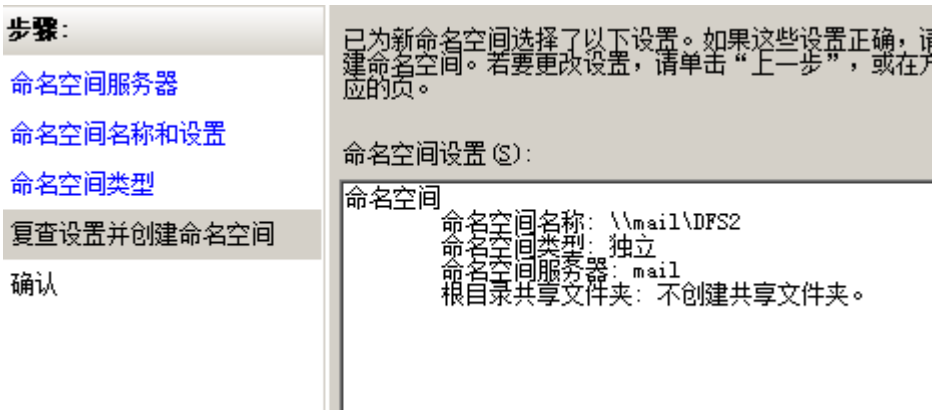


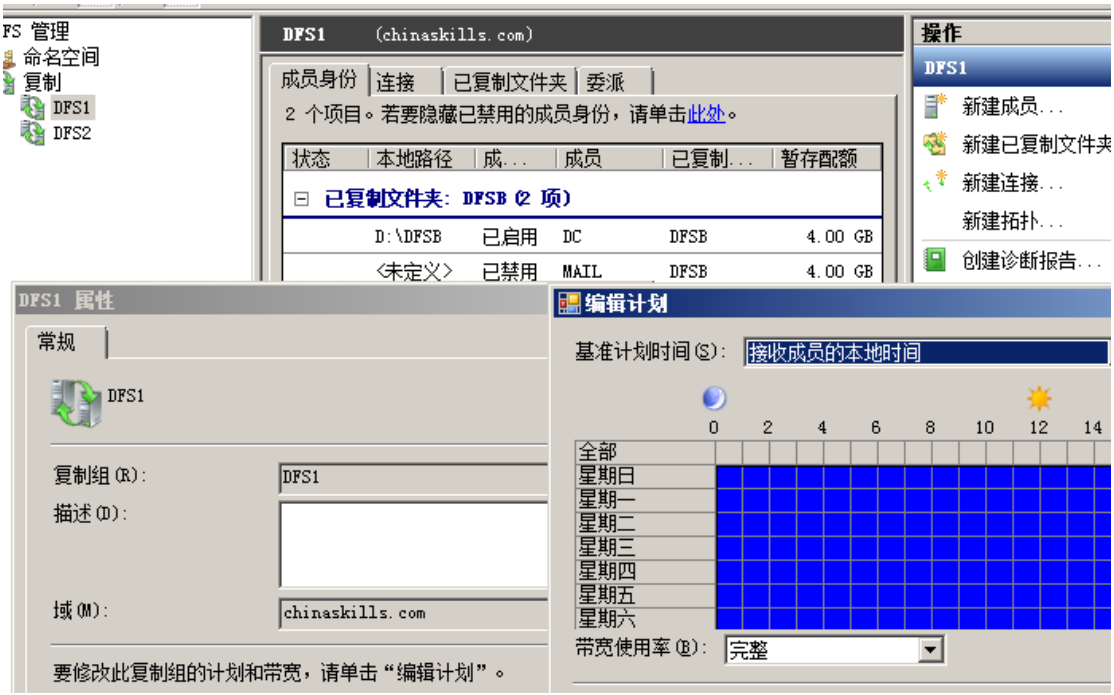
入站规则

名称	组	配置文件	已启用	操作	替代	程序	本地地址	远程地址	协议	本地端口	远
网络策略服...	网...	所有	否	允许	否	任何	任何	任何	UDP	1646	任
网络策略服...	网...	所有	否	允许	否	任何	任何	任何	UDP	1645	任
网络发现 (L...	网...	所有	否	允许	否	%Sy...	任何	本地子网	UDP	5355	任
网络发现 (N...	网...	所有	否	允许	否	System	任何	任何	UDP	138	任
网络发现 (N...	网...	所有	否	允许	否	System	任何	任何	UDP	137	任
网络发现 (P...	网...	所有	否	允许	否	%Sy...	任何	本地子网	UDP	3702	任
网络发现 (S...	网...	所有	否	允许	否	%Sy...	任何	本地子网	UDP	1900	任
网络发现 (U...	网...	所有	否	允许	否	System	任何	任何	TCP	2869	任
网络发现 (W...	网...	所有	否	允许	否	System	任何	任何	TCP	5357	任
网络发现 (W...	网...	所有	否	允许	否	System	任何	任何	TCP	5358	任
网络发现 (W...	网...	所有	否	允许	否	%Sy...	任何	本地子网	UDP	3702	任
文件和打印...	文...	所有	否	允许	否	%Sy...	任何	本地子网	UDP	5355	任
文件和打印...	文...	所有	否	允许	否	System	任何	任何	UDP	138	任
文件和打印...	文...	所有	否	允许	否	System	任何	任何	UDP	137	任
文件和打印...	文...	所有	否	允许	否	System	任何	任何	TCP	139	任
文件和打印...	文...	所有	否	允许	否	System	任何	任何	TCP	445	任
文件和打印...	文...	所有	否	允许	否	%Sy...	任何	任何	TCP	RPC 动...	任
文件和打印...	文...	所有	否	允许	否	任何	任何	任何	TCP	RPC 终...	任
文件和打印...	文...	所有	否	允许	否	任何	任何	任何	ICMPv4	任何	任
文件和打印...	文...	所有	否	允许	否	任何	任何	任何	ICMPv6	任何	任
性能日志和...	性...	域	否	允许	否	%sy...	任何	任何	TCP	135	任
性能日志和...	性...	专用，公用	否	允许	否	%sy...	任何	本地子网	TCP	135	任
性能日志和...	性...	专用，公用	否	允许	否	%sy...	任何	本地子网	TCP	任何	任
性能日志和...	性...	域	否	允许	否	%sy...	任何	任何	TCP	任何	任
远程服务管...	远...	所有	否	允许	否	System	任何	任何	TCP	445	任
远程服务管...	远...	所有	否	允许	否	%Sy...	任何	任何	TCP	RPC 动...	任
远程服务管...	远...	所有	否	允许	否	%Sy...	任何	任何	TCP	RPC 终...	任
远程管理 (N...	远...	所有	否	允许	否	System	任何	任何	TCP	445	任
远程管理 (RPC)	远...	所有	否	允许	否	%Sy...	任何	任何	TCP	RPC 动...	任
远程管理 (R...	远...	所有	否	允许	否	%Sy...	任何	任何	TCP	RPC 终...	任
远程计划任...	远...	所有	否	允许	否	%Sy...	任何	任何	TCP	RPC 动...	任
远程计划任...	远...	所有	否	允许	否	%Sy...	任何	任何	TCP	RPC 终...	任
远程卷管理...	远...	所有	否	允许	否	%Sy...	任何	任何	TCP	RPC 动...	任
远程卷管理...	远...	所有	否	允许	否	%Sy...	任何	任何	TCP	RPC 动...	任
远程卷管理...	远...	所有	否	允许	否	%Sy...	任何	任何	TCP	RPC 终...	任
远程事件日...	远...	所有	否	允许	否	System	任何	任何	TCP	445	任
远程事件日...	远...	所有	否	允许	否	%Sy...	任何	任何	TCP	RPC 动...	任
远程事件日...	远...	所有	否	允许	否	%Sy...	任何	任何	TCP	RPC 终...	任
远程桌面 (T...	远...	所有	是	允许	否	System	任何	任何	TCP	3389	任

（三）在主机 Win2003-A1 中完成 DFS 服务器的部署

1、配置 DFS 服务，共享 D:\ DFSB，共享名 DFS2。将共享目录 DFS2 添加到 Win2008-B2 创建的 WEB 分布式文件系统，并设置复制组的计划内容为完整复制。[将 DFS2 加入到 dyDFS 后的管理界面截屏保存为 DFS2-1，设置复制方式的界面截屏保存为 DFS2-2]；





二、在 PC2 上完成如下操作:

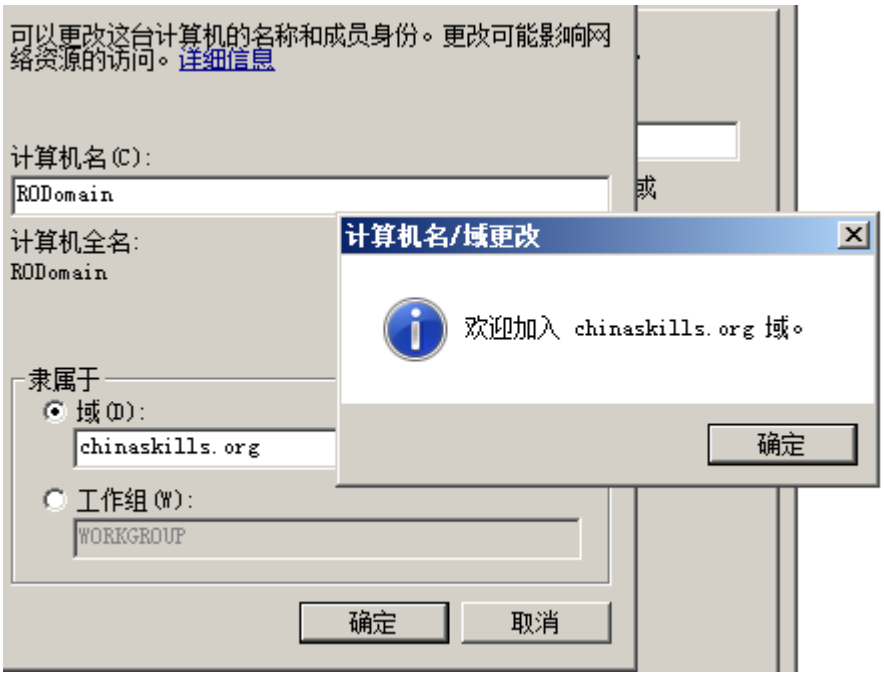
（一）完成虚拟主机的创建

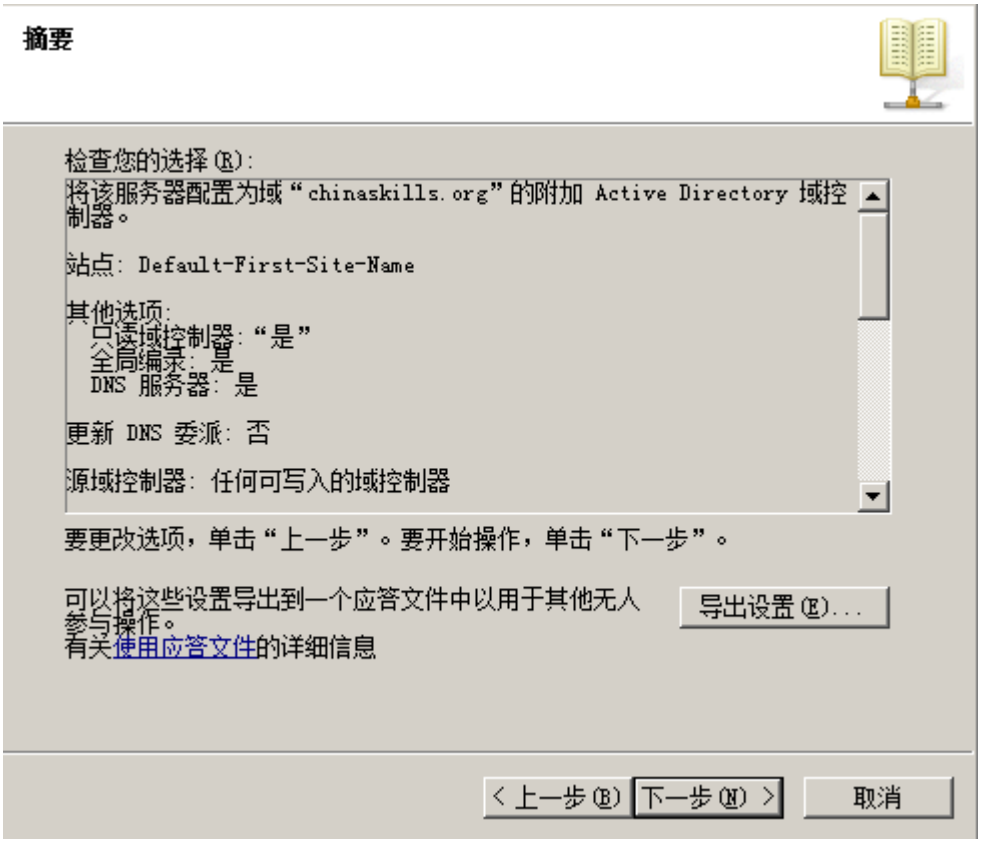
1、安装虚拟机“Win2008-B1”，其内存为 1G，硬盘 20G，并将服务器加入到 Windows 域环境；

2、安装虚拟机“Win2008-B2”， 其内存为 512M，硬盘 20G，将服务器加入至 Windows 域中；

（二）在主机 **Win2008-B1** 中完成 **RODC** 的部署

1. 将 Win2008-B1 的主机名修改为 RODomain，把 RODomain 作为只读域控制器，加入到 chinaskills.org 中。**（将升级域完成的摘要界面截屏保存为 RD1-1）**

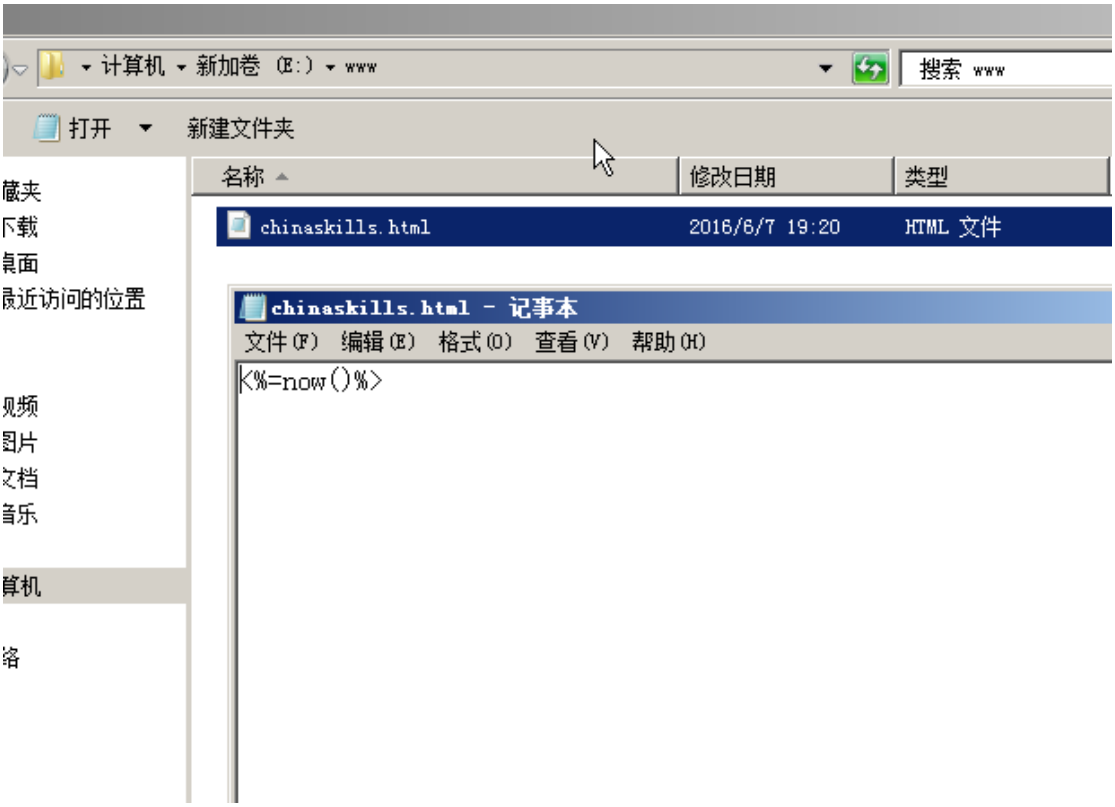


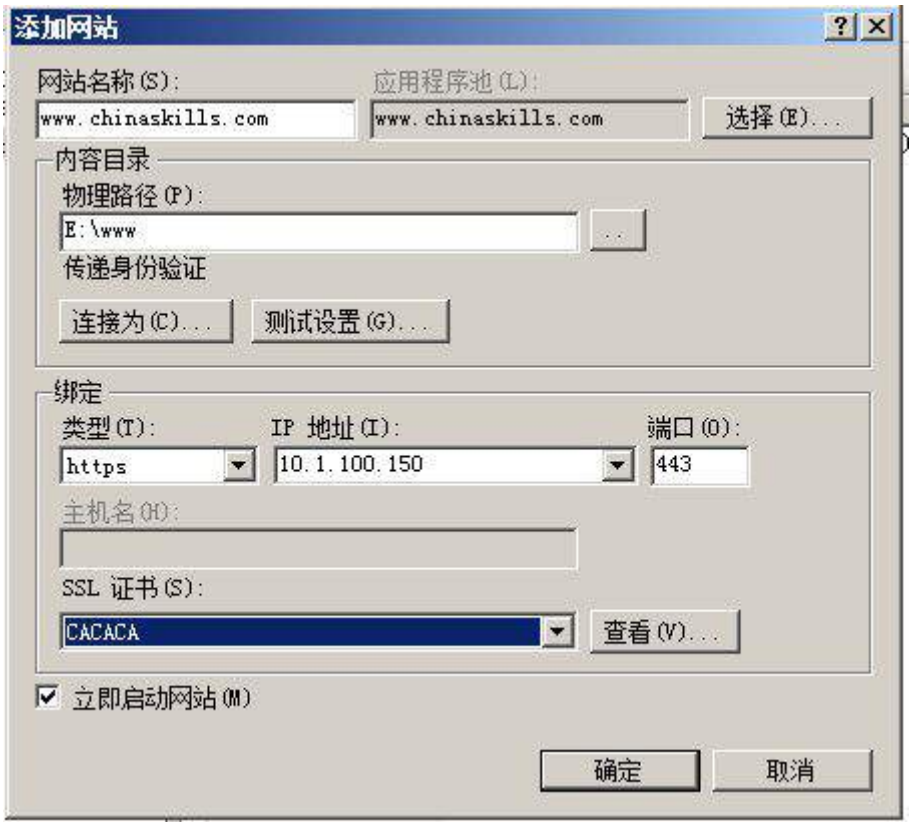


（三）在主机 Win2008-B2 中完成 web 及 DFS 服务器的部署

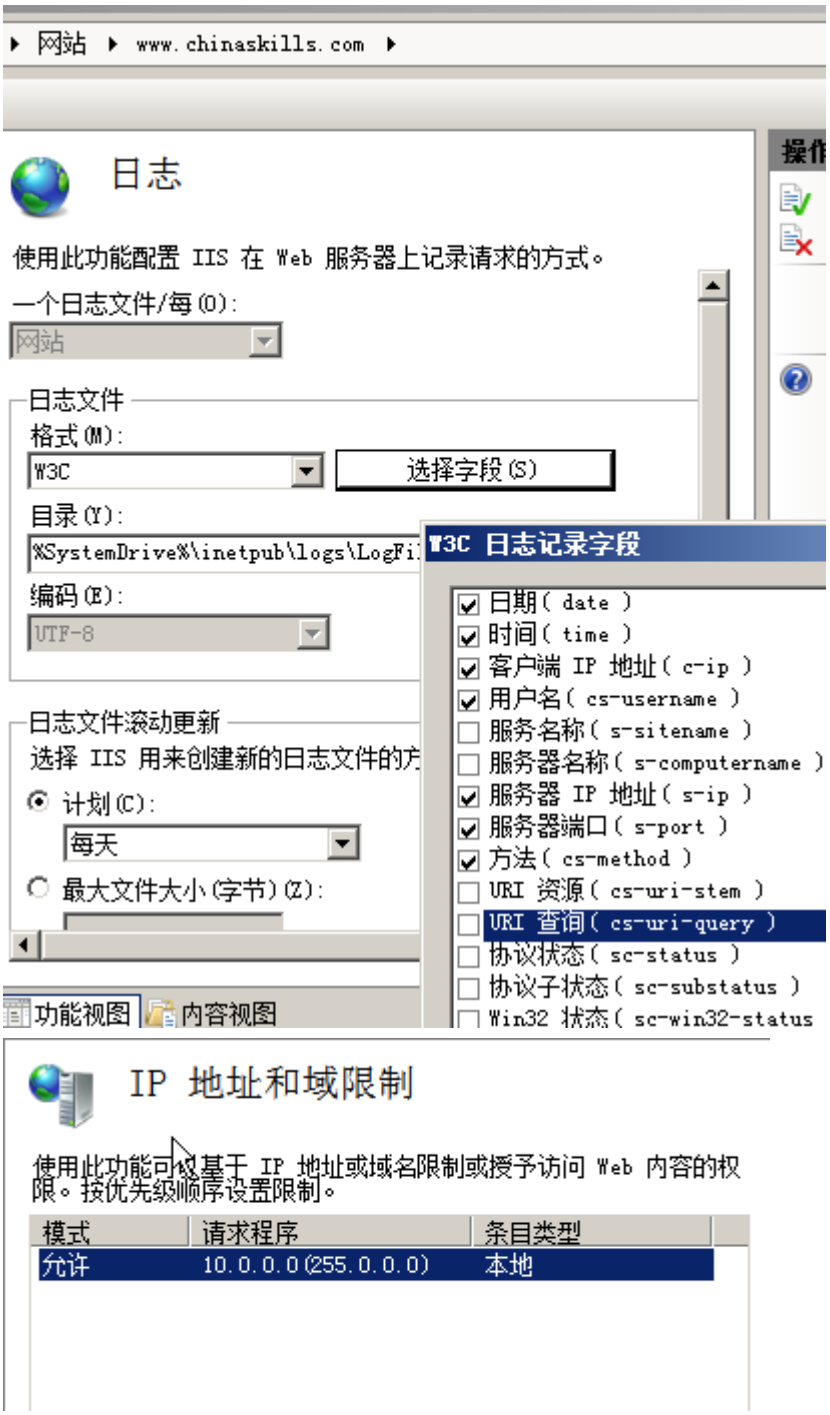
1、安装 IIS 组件，创建 www. chinaskills.com 站点，在挂载的磁盘 e:\下创建名称为 www 的目录，在 www 文件夹中创建名称为 chinaskills.html 的主

页，其主页显示内容“<%=now()%>”，同时只允许使用 SSL 且只能通过域名方式进行访问；

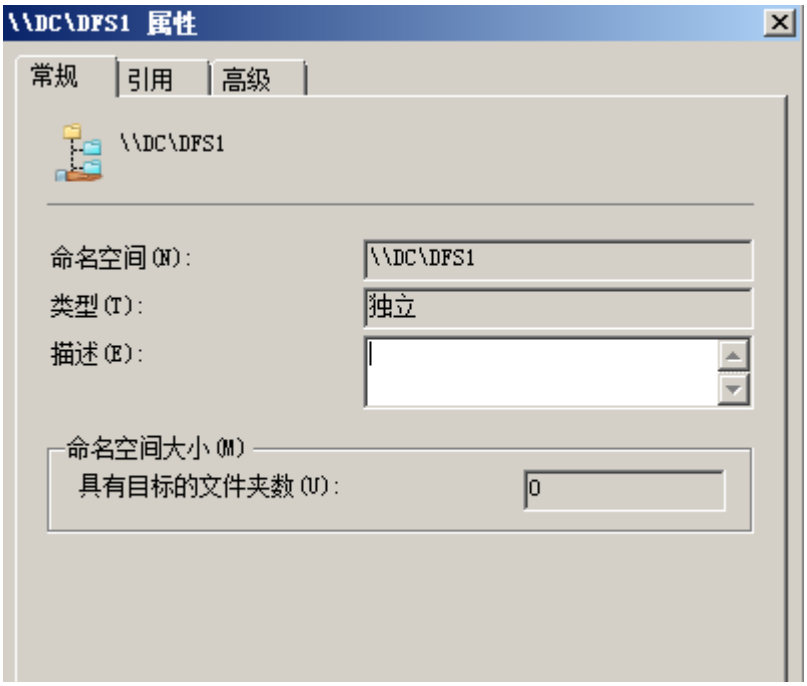


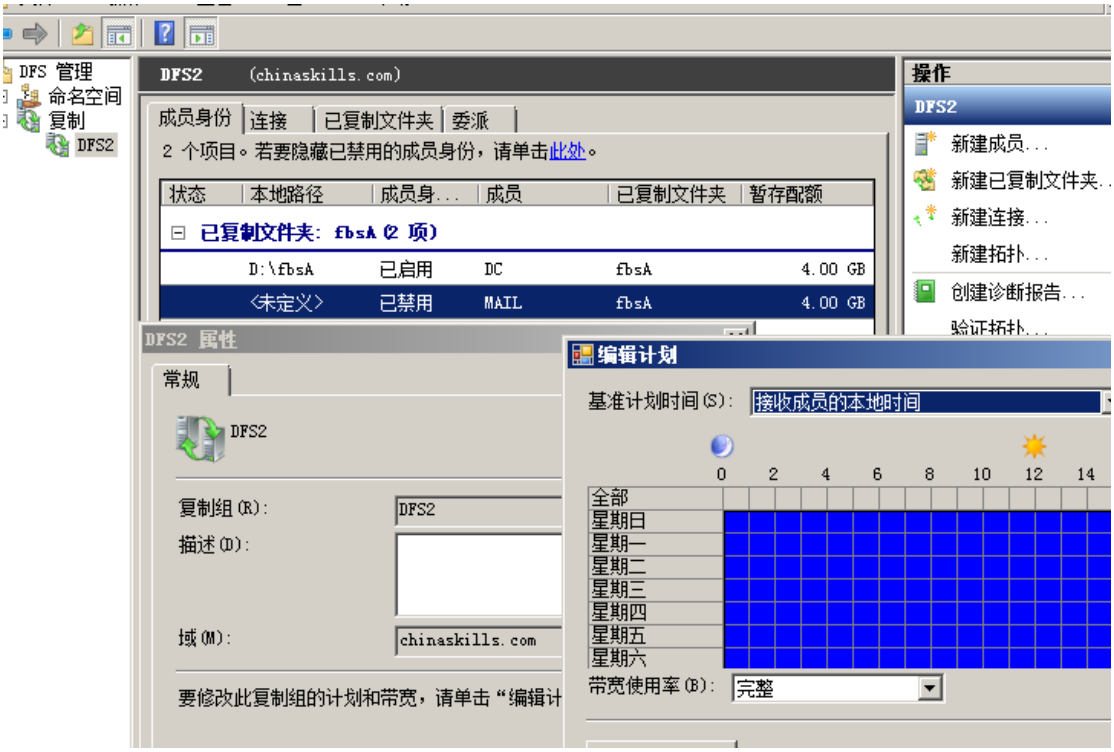


2、设置网站的最大连接数为 1000，网站连接超时为 120s，网站的带宽为 1000KB/S，使用 W3C 记录日志；禁用父路径；每天创建一个新的日志文件，使用当地时间作为日志文件名；日志只允许记录日期、时间、客户端 IP 地址、用户名、服务器 IP 地址、服务器端口号和方法；设置 IP 列表只允许 IP 为 10.0.0.0/255.0.0.0 的用户访问。



3、配置 DFS 服务作为分布式文件系统的命名空间服务器，共享 D:\fbsA，共享名为 DFS1，空间名称为 WEB，将 DFS1 作为分布式命名空间的根目录，实现与 win2003-A1 服务器的内容保持同步；

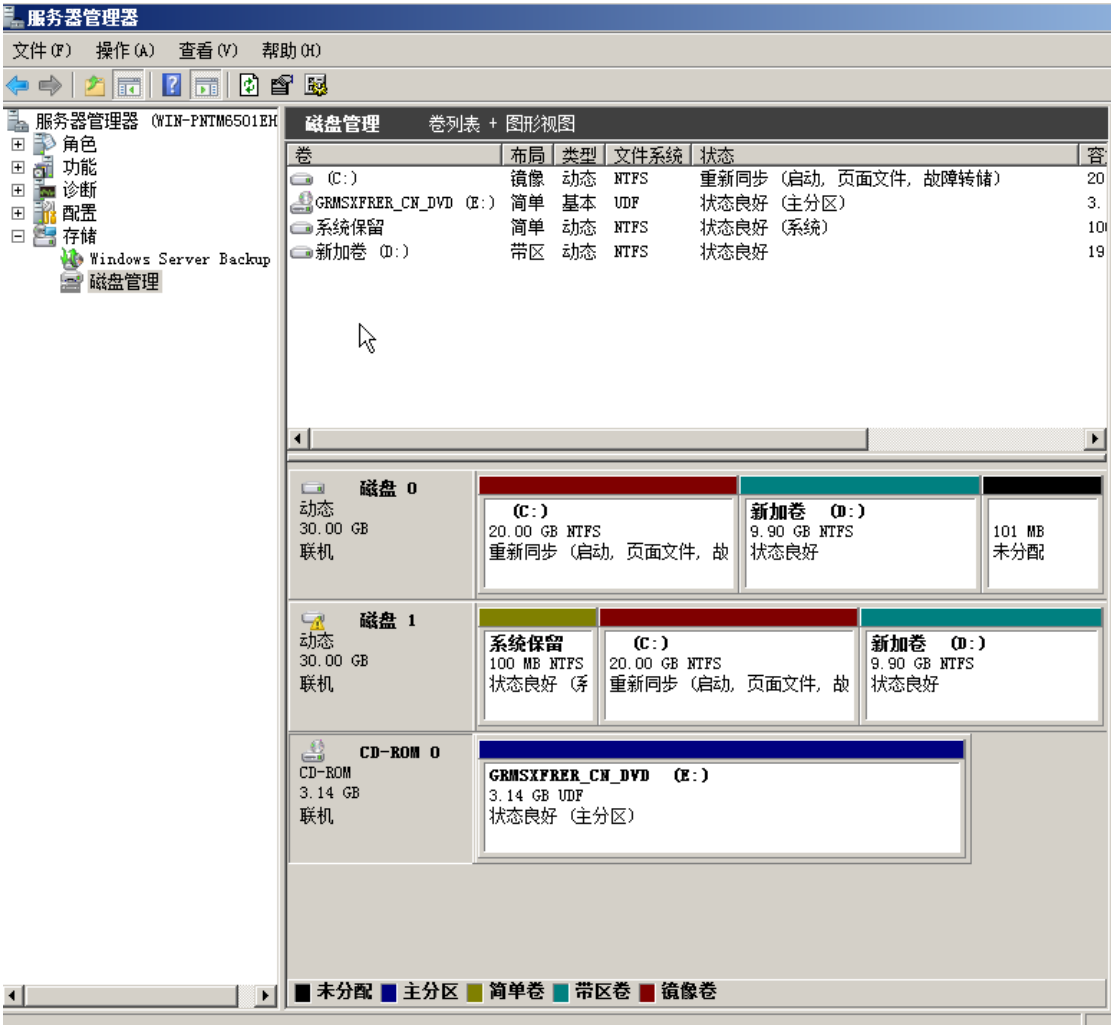




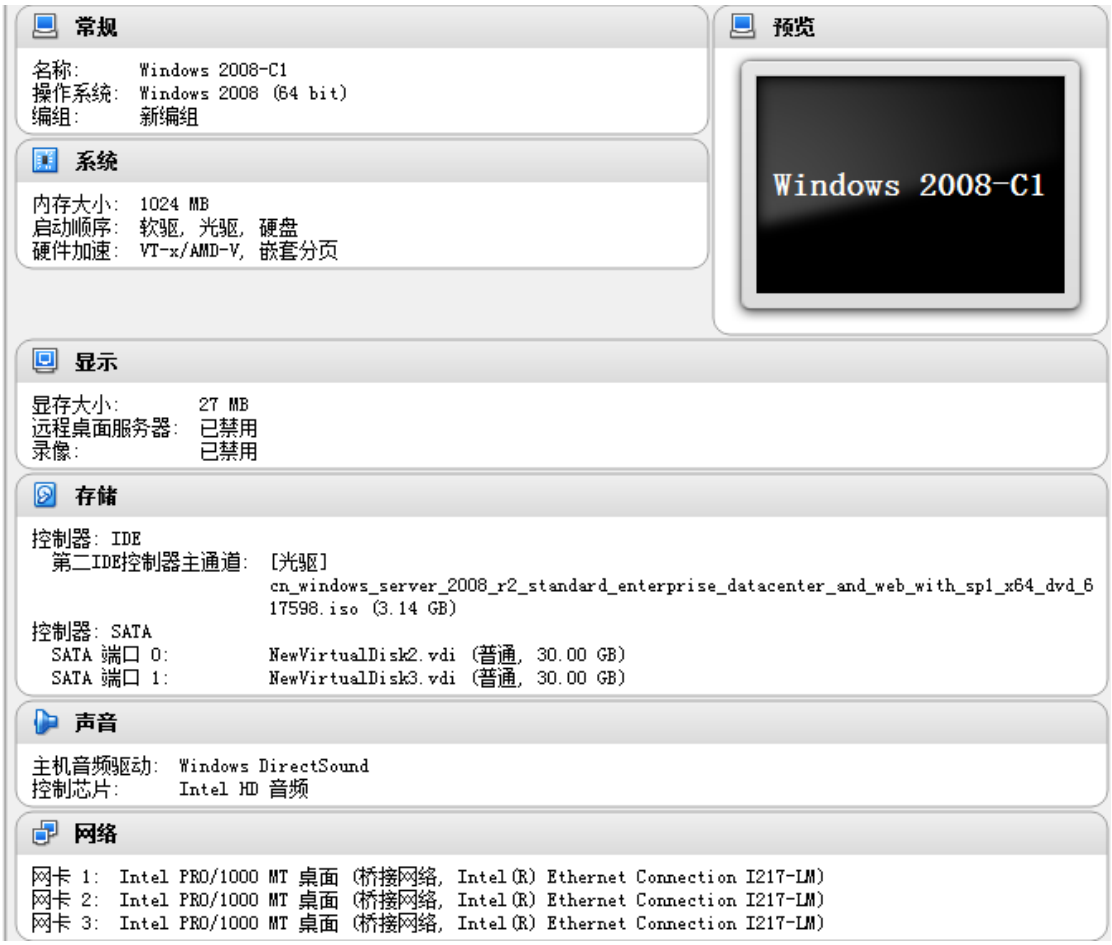
三、在 **PC3** 上完成如下操作:

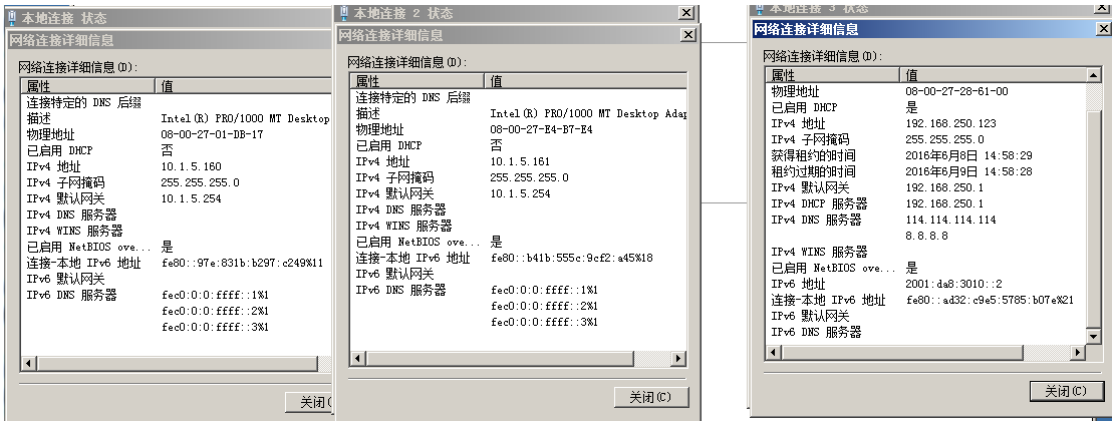
（一）完成虚拟主机的创建

1、安装虚拟机“Win2008-C1”，其内存为 1G，系统有两个 30G 的硬盘，系统分区使用 20G，**需要支持容错功能。其余为数据分区，要提高分区的访问速度。**



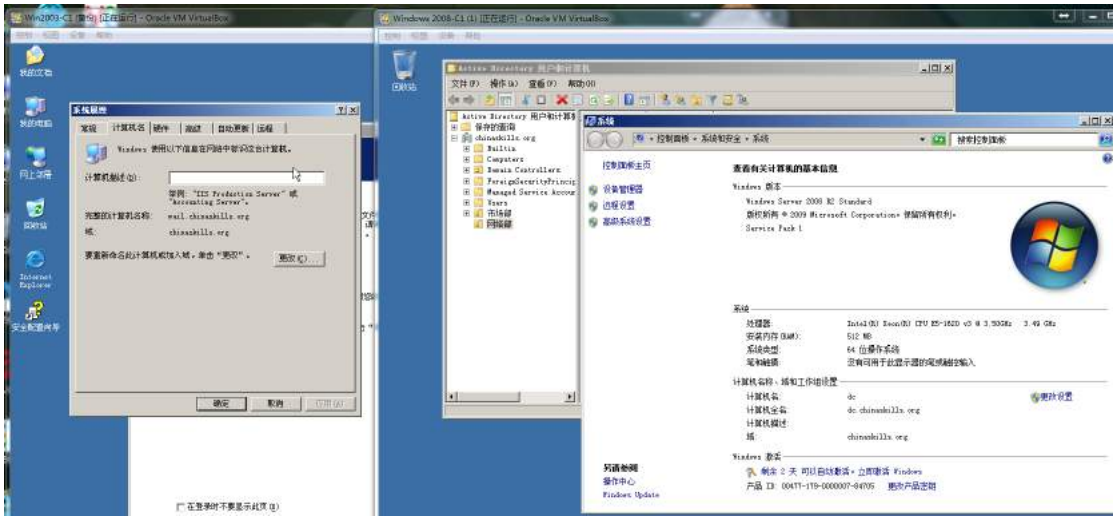
2、在虚拟机“Win2008-C1”中配置三个网卡，IP 地址如表所示。并将服务器加入到 Windows 域环境；；





（二）完成域的升级和迁移

1、将标识为“PC3”的计算机上的已有虚拟机 Win2003-C1 启动。对其进行滚动升级，将原用 chinaskills.org 域的域控制器 Win2003-C1 升级到新安装的 Windows Server 2008 服务器 Win2008-C1。



2、将已有虚拟机 Win2003-C1 的 DHCP 服务和 DNS 服务迁移到 Win2008-C1 服务器上。

（三）在主机 Win2008-C1 上完成域控制器的基本配置

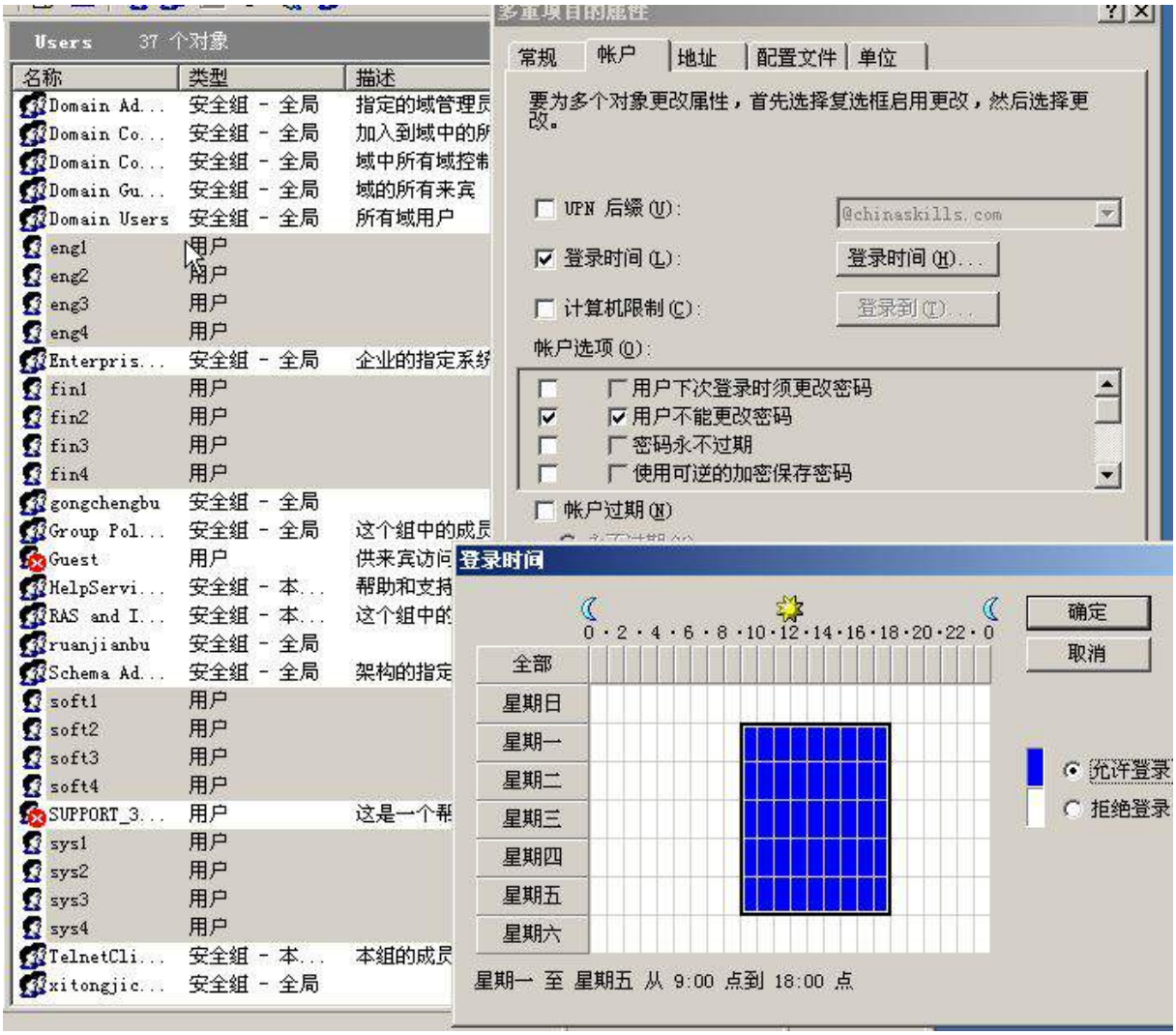
1、创建 4 个组织单元，单元名采用对应部门名称的拼音来命名，每个部门都创建 4 个用户，财务部用户：fin1~fin4、市场部用户：mar1~mar4、网络部用户：net1~net4、研发部用户： yf1~yf4，所有用户不能修改其用户口令，并要求用户只能在上班时间可以登录（每周工作日 9:00~17:00），出于用户安全考虑，第一次登录时要求更改密码。；


xitongjichengbu 属性
常规
成员
隶属于
管理者
成员(M):
名称
Active Directory 文件夹
sys1
chinaskills.com/Users
sys2
chinaskills.com/Users
sys3
chinaskills.com/Users
sys4
chinaskills.com/Users
添加(D)...
删除(R)
确定
取消
应用(A)

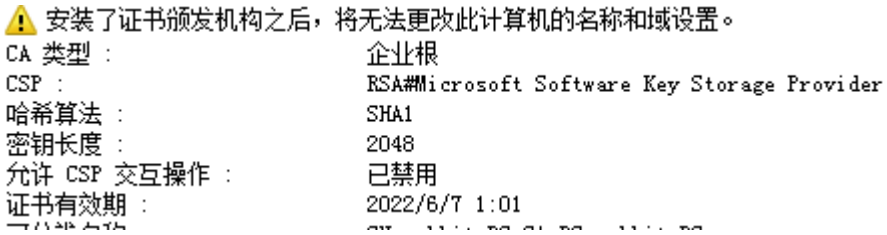

caiwubu 属性
常规
成员
隶属于
管理者
成员(M):
名称
Active Directory 文件夹
fin1
chinaskills.com/Users
fin2
chinaskills.com/Users
fin3
chinaskills.com/Users
fin4
chinaskills.com/Users
添加(D)...
删除(R)
确定
取消
应用(A)


gongchengbu 属性
常规
成员
隶属于
管理者
成员(M):
名称
Active Directory 文件夹
eng1 chinaskills.com/Users
eng2 chinaskills.com/Users
eng3 chinaskills.com/Users
eng4 chinaskills.com/Users
添加(D)...
删除(R)
确定
取消
应用(A)


ruanjianbu 属性
常规
成员
隶属于
管理者
成员(M):
名称
Active Directory 文件夹
soft1 chinaskills.com/Users
soft2 chinaskills.com/Users
soft3 chinaskills.com/Users
soft4 chinaskills.com/Users
添加(D)...
删除(R)
确定
取消
应用(A)

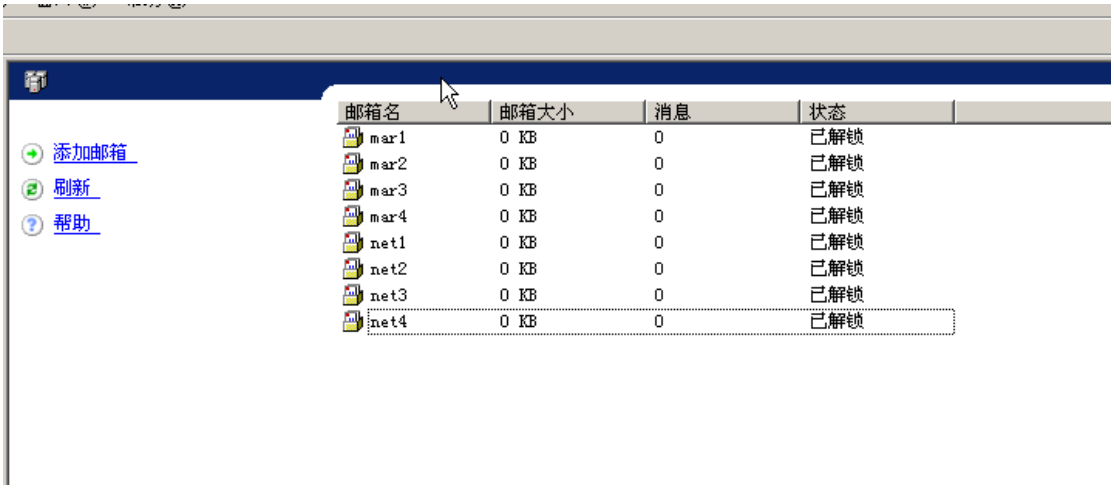


2、安装证书服务，设置为企业根，有效期为 6 年，为企业内部自动回复证书申请；

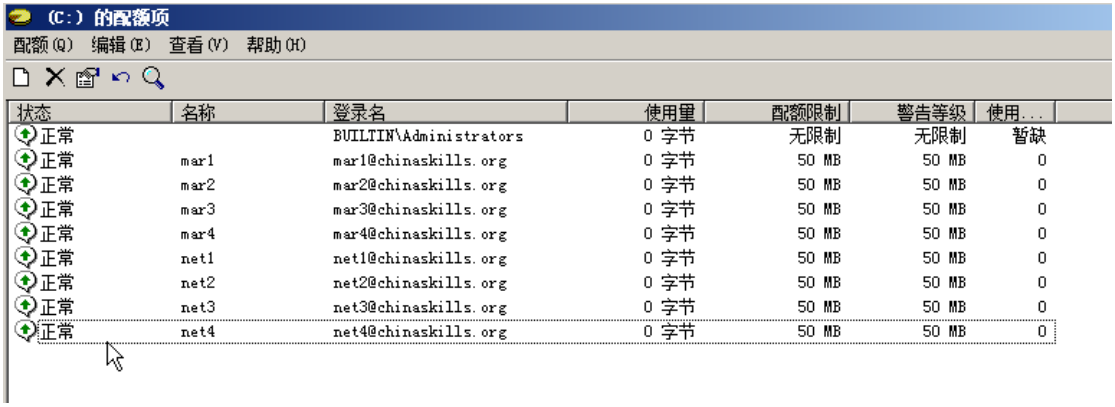


（四）在主机 Win2003-C1 中完成 E-MAIL 服务器的部署

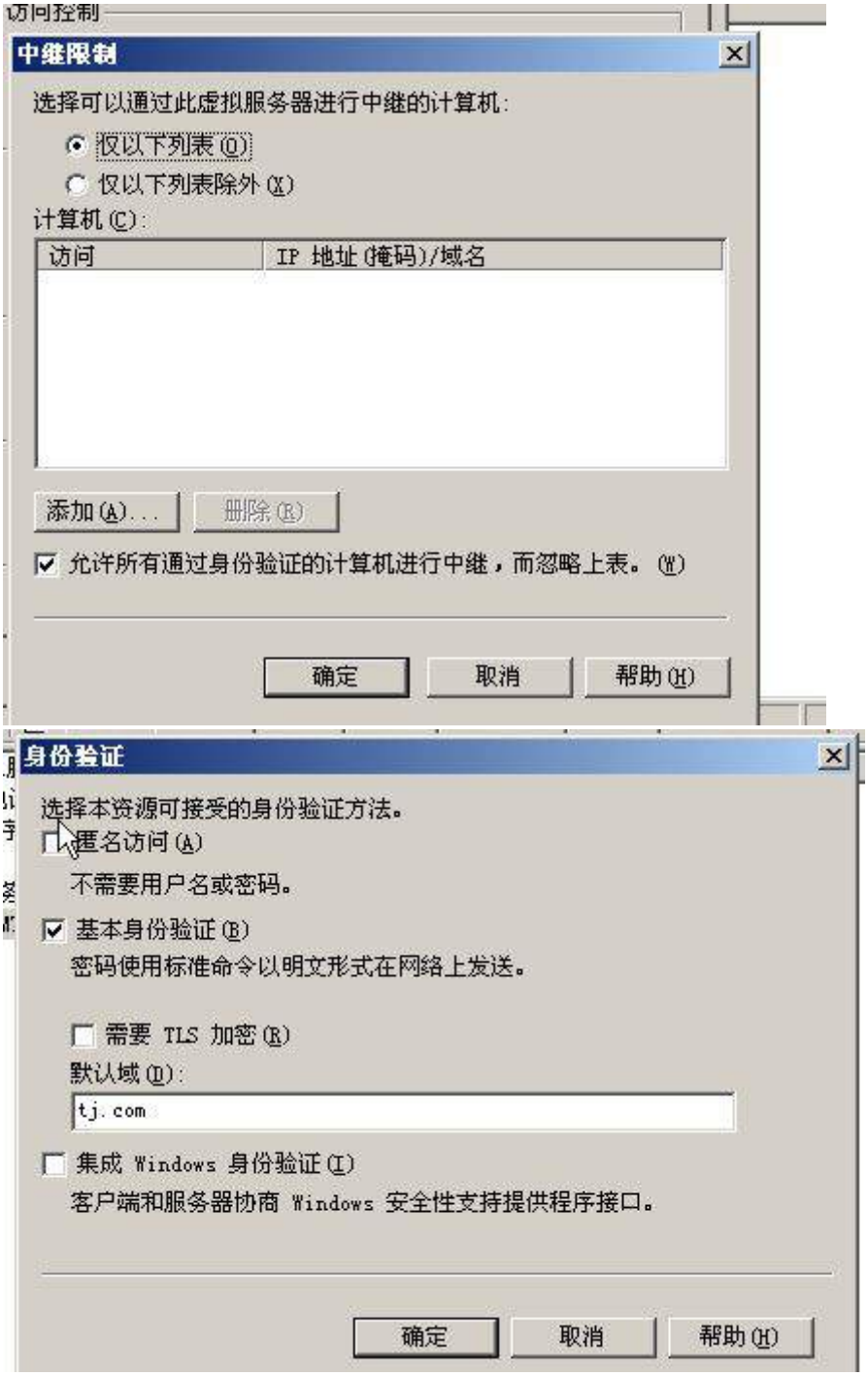
1、安装 E-mail 服务，采用 Active Directory 集成的身份验证方式为内网市场部和网络部的用户创建邮箱；



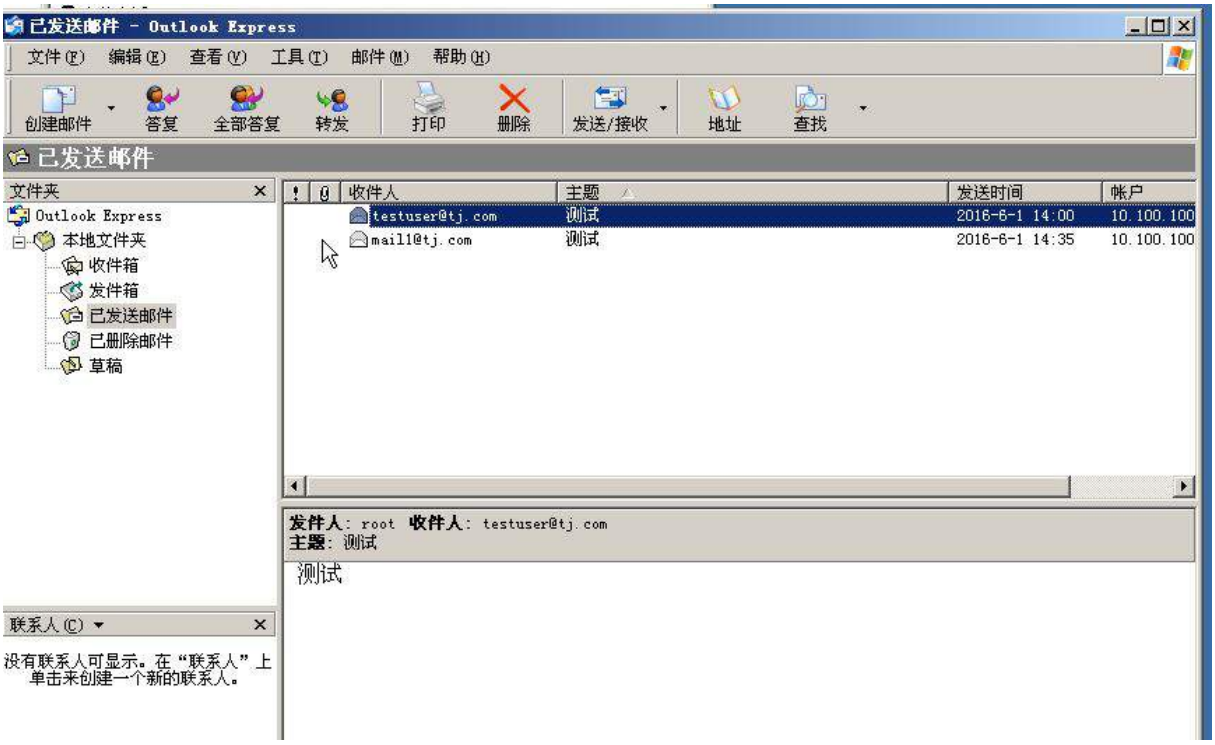
2、限定市场部和网络部每个用户的邮箱大小为 50MB；



3、完成对 smtp 服务的配置，只允许通过验证的用户进行中继，身份验证使用基本认证方式；



4、要求实现与 jnds.net 域进行邮件互通，通过 outlook express 进行测试，将发送成功的界面截图存储为 mail；

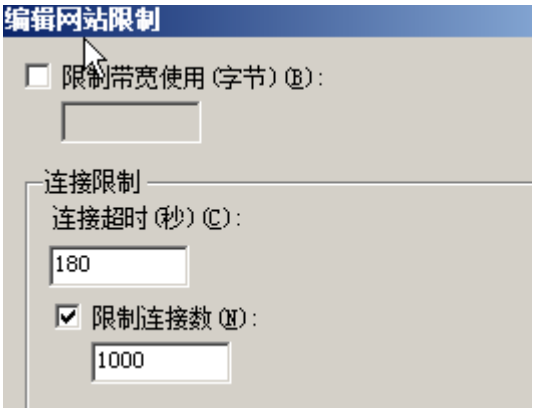


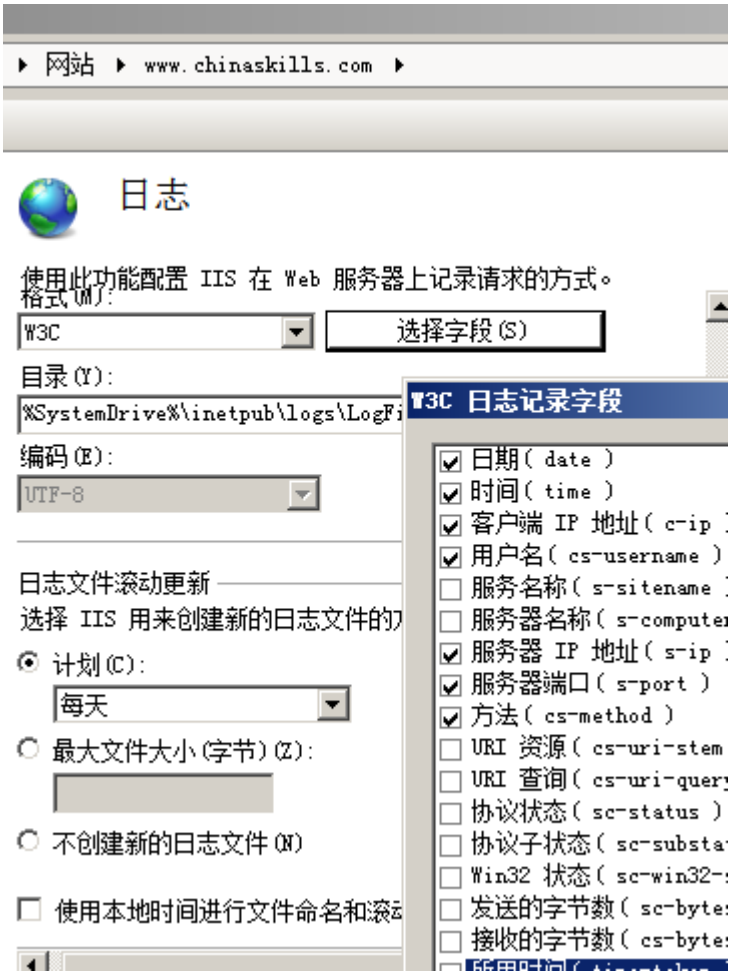
（五）在主机 **Win2003-C1** 中完成 **FTP** 服务器的部署

1、安装 FTP 服务。

2、使用隔离用户创建名为 ftp.chinaskills.com 的 FTP 站点，FTP 主目录为 c:\inetpub\ftproot。使用 ftp.chinaskills.com 可访问该 FTP 站点。域用户 ftp1、ftp2 及匿名用户均可登录，但匿名用户权限只读，ftp1,ftp2 可以读写。

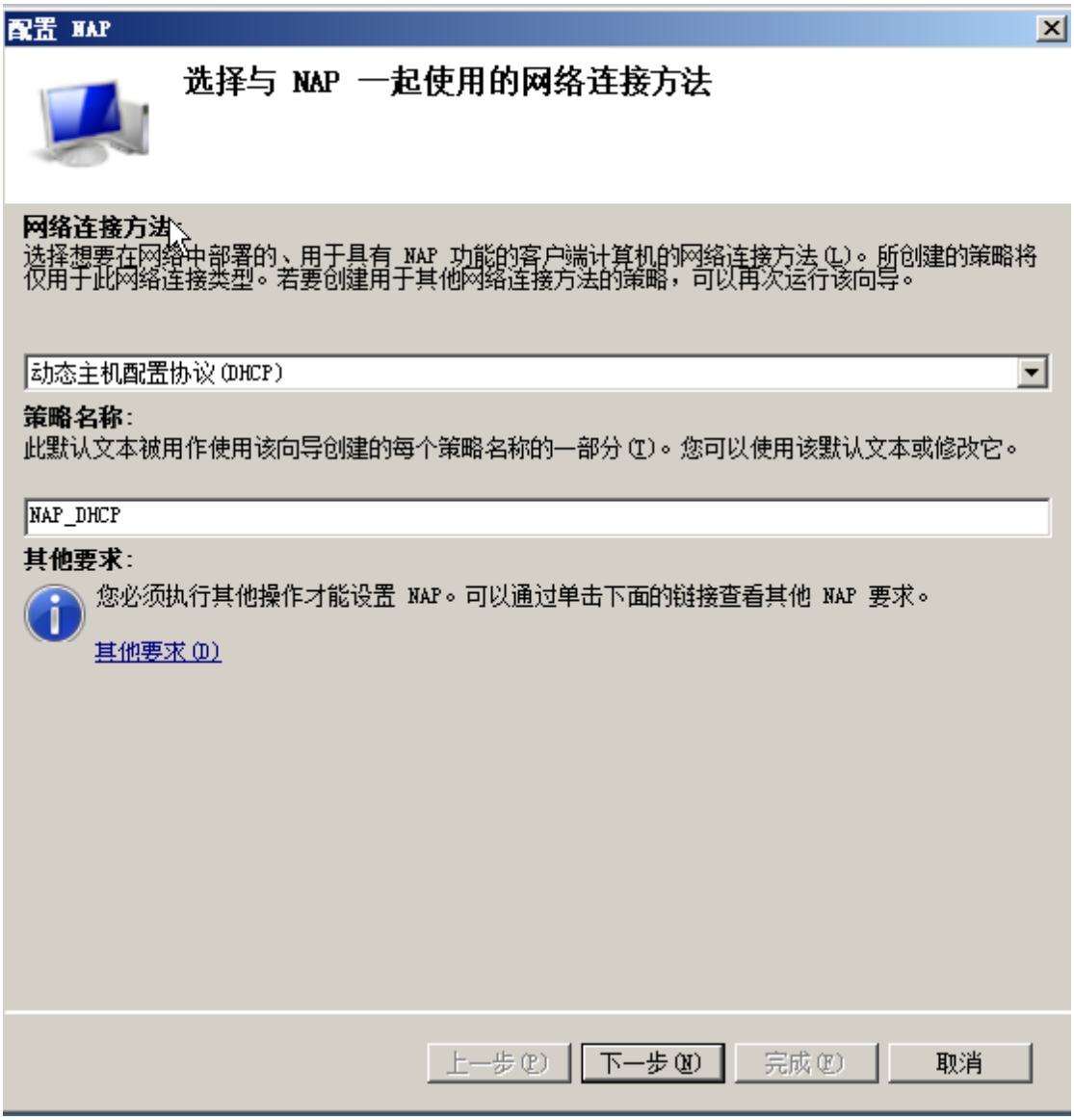
3、限制站点的最大连接数为 1000，连接超时 180s；使用 W3C 记录日志；每天创建一个新的日志文件，使用当地时间作为日志文件名；日志只允许记录日期、时间、客户端 IP 地址、用户名、服务器 IP 地址、服务器端口号和方法。

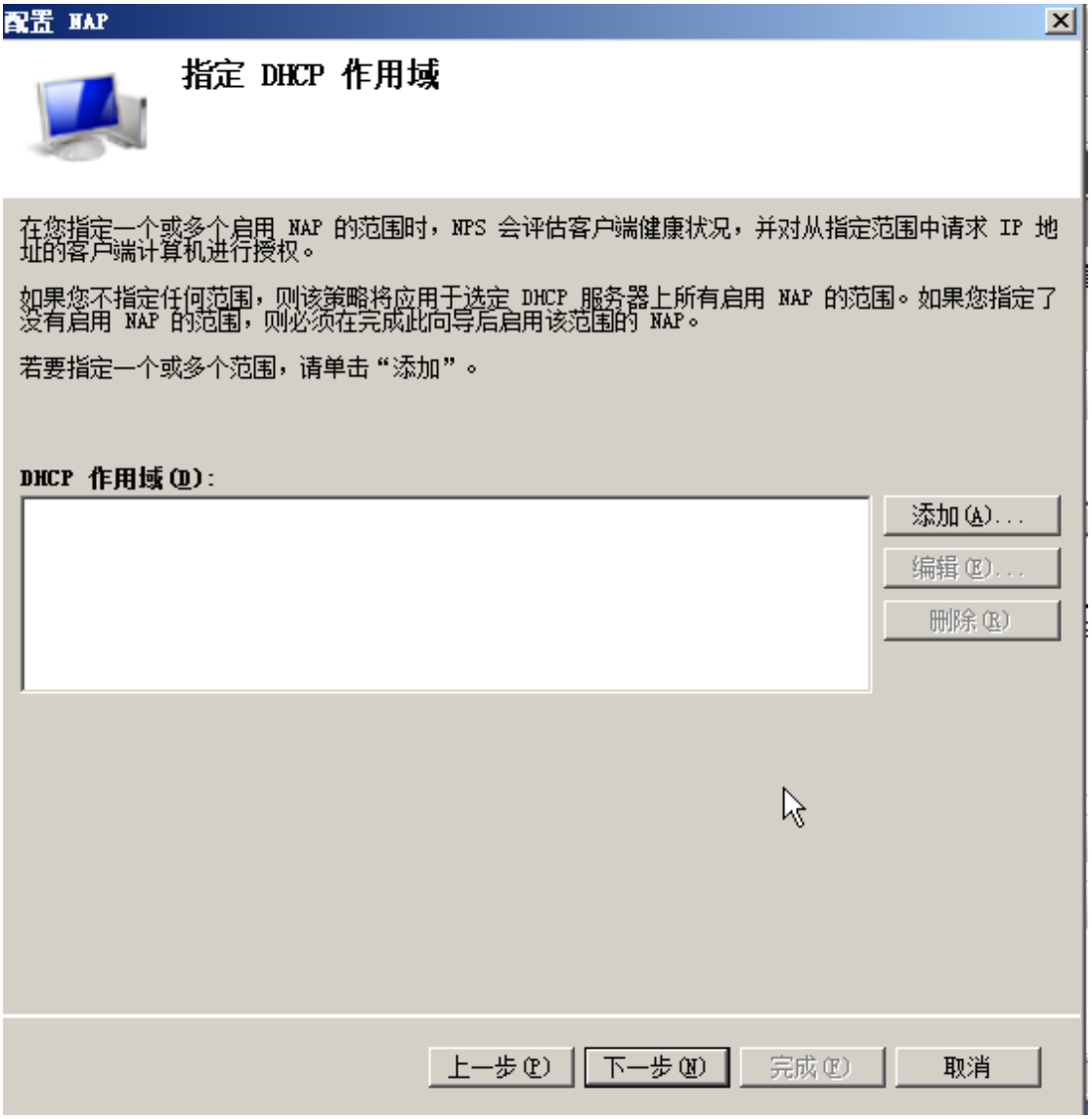




（六）在主机 Win2008-C1 中完成 NAP 服务器的部署

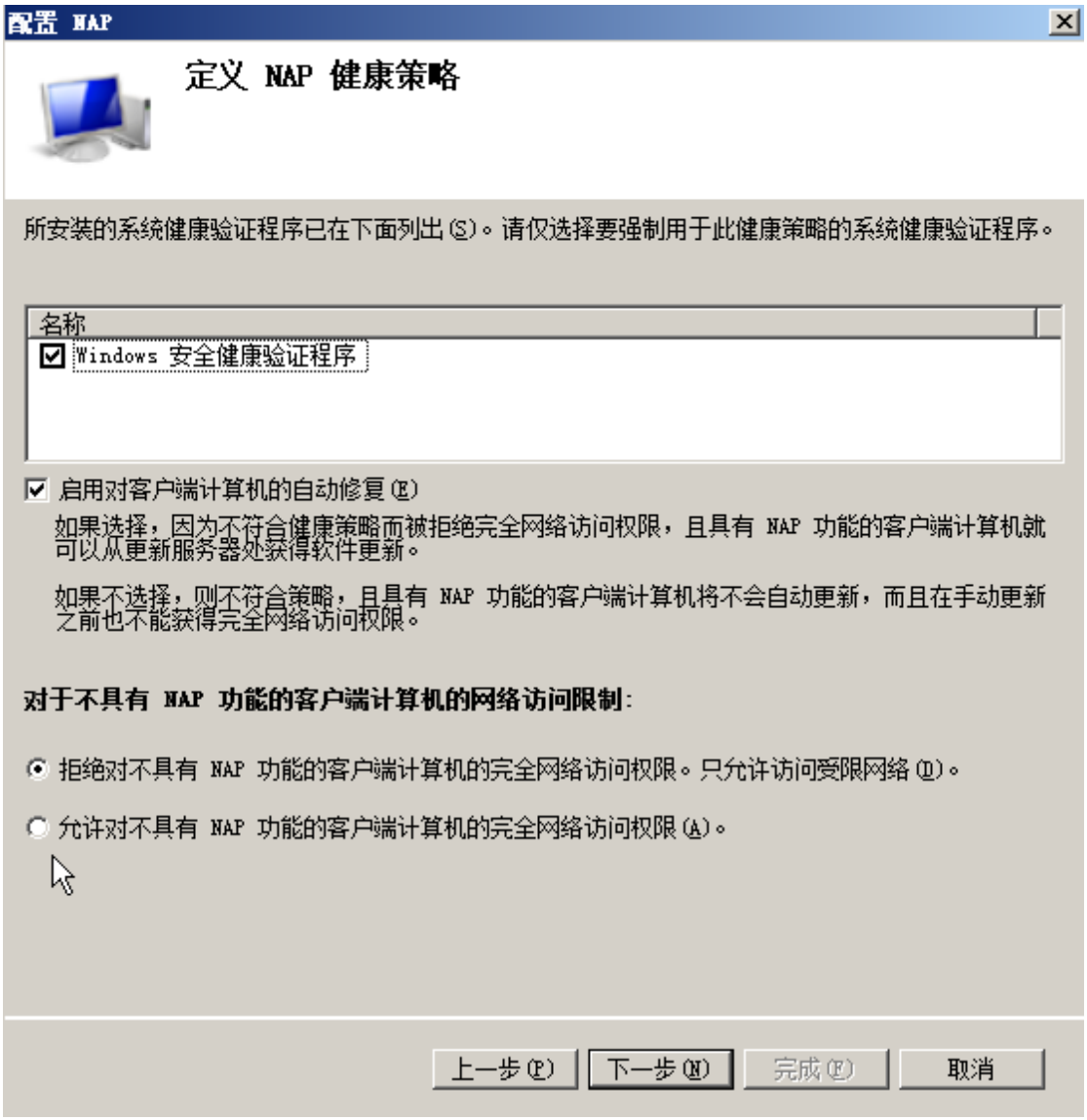
1. 将 **Win2008-C1** 配置成为网络访问策略的服务器（NPS）。将 DHCP 设置为与 NAP 一起使用的网络连接方法，策略名称为 NAP_DHCP。NAP 应用于 DHCP 上所有的作用域和域中的所有用户。不使用跟新服务器组。启动客户端计算机自动更新，拒绝对不具有 NAP 功能的客户端计算机完全访问网络，只允许访问受限网络。


配置 NAP
选择与 NAP 一起使用的网络连接方法
网络连接方法:
选择想要在网络中部署的、用于具有 NAP 功能的客户端计算机的网络连接方法(L)。所创建的策略将仅用于此网络连接类型。若要创建用于其他网络连接方法的策略，可以再次运行该向导。
动态主机配置协议(DHCP)
策略名称:
此默认文本被用作使用该向导创建的每个策略名称的一部分(T)。您可以使用该默认文本或修改它。
NAP_DHCP
其他要求:
您必须执行其他操作才能设置 NAP。可以通过单击下面的链接查看其他 NAP 要求。
其他要求(D)
上一步(P)
下一步(N)
完成(F)
取消

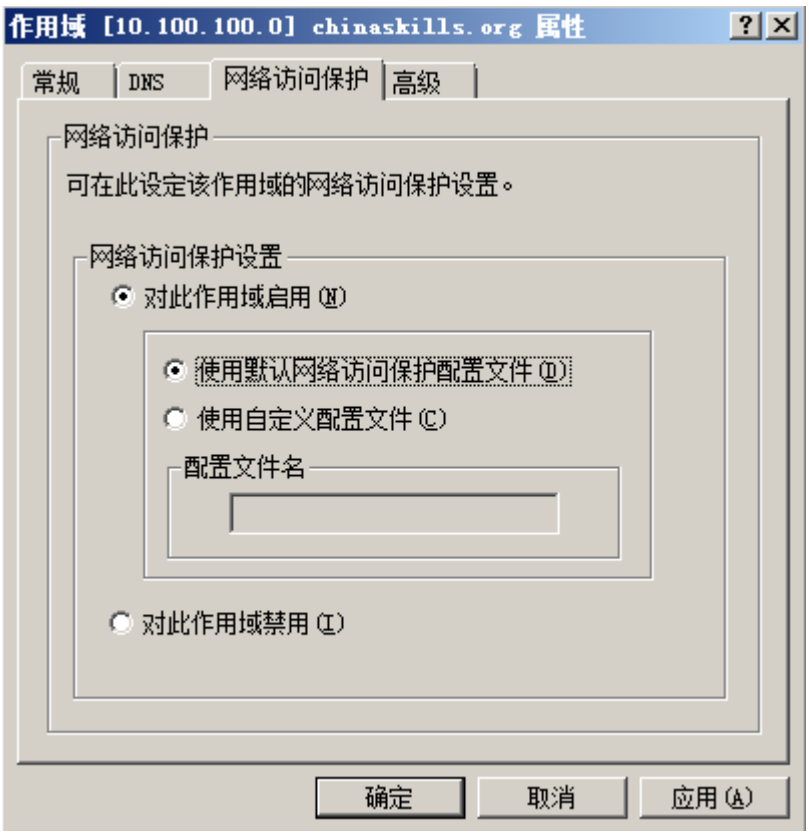

配置 NAP
指定 DHCP 作用域
在您指定一个或多个启用 NAP 的范围时，NPS 会评估客户端健康状况，并对从指定范围中请求 IP 地址的客户端计算机进行授权。
如果您不指定任何范围，则该策略将应用于选定 DHCP 服务器上所有启用 NAP 的范围。如果您指定了没有启用 NAP 的范围，则必须在完成此向导后启用该范围的 NAP。
若要指定一个或多个范围，请单击“添加”。
DHCP 作用域(D):
添加(A)...
编辑(E)...
删除(R)
上一步(P)
下一步(N)
完成(F)
取消

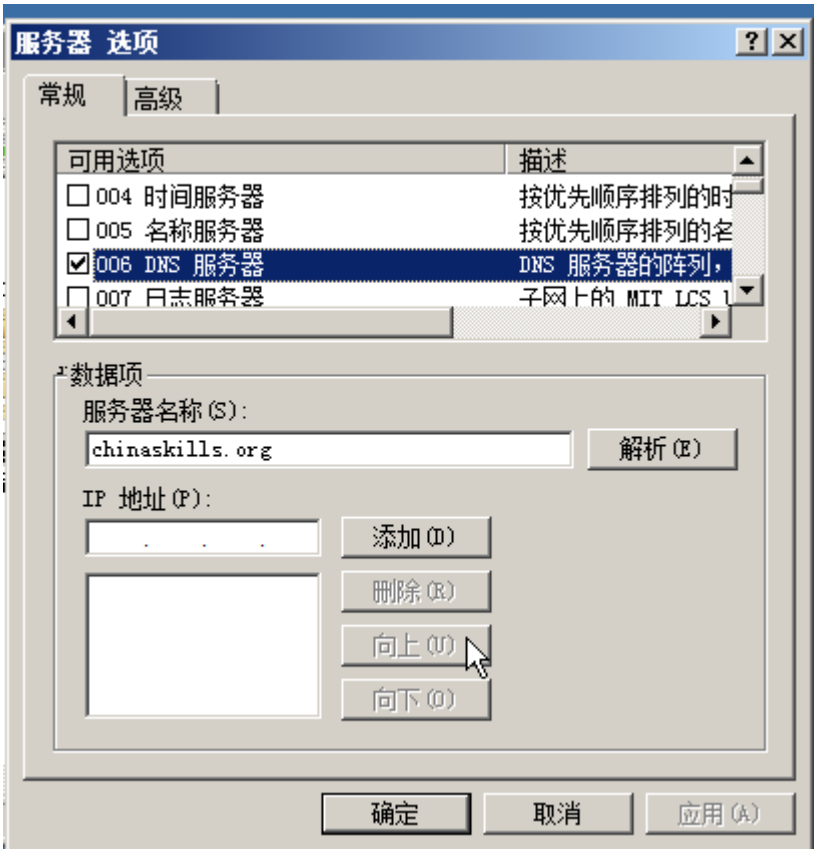

配置 NAP
配置计算机组
若要授予或拒绝访问计算机组的权限，请将组添加到计算机组中。
如果没有选择任何组，则该策略将应用于所有用户。
计算机组:
添加(A)...
删除(R)
上一步(P)
下一步(N)
完成(F)
取消

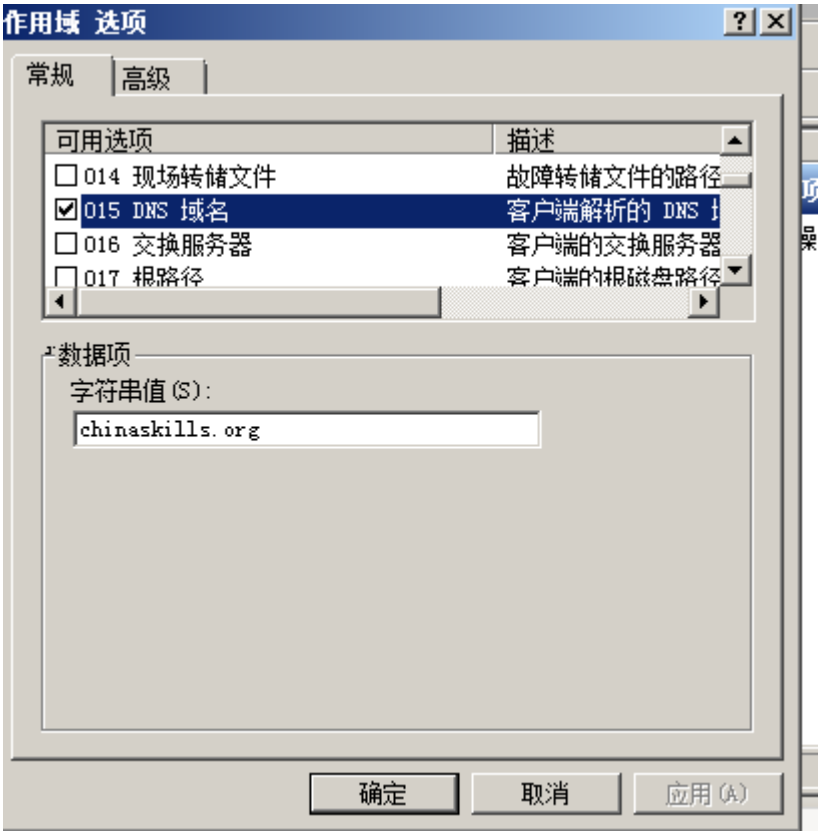

配置 NAP
指定 NAP 更新服务器组和 URL
更新服务器组:
更新服务器存储着 NAP 客户端所需的软件更新。更新服务器组包含一个或多个更新服务器。
选择您已经配置的更新服务器组(L),或单击“新建组”以创建新组。
<无>
新建组(G)...
URL 疑难解答:
如果您具有指导用户如何让计算机和设备符合 NAP 健康策略的网页,请键入该网页的统一资源定位器(URL)(F)。
如果您没有帮助网页,请不要键入 URL。
http://
上一步(P)
下一步(N)
完成(F)
取消

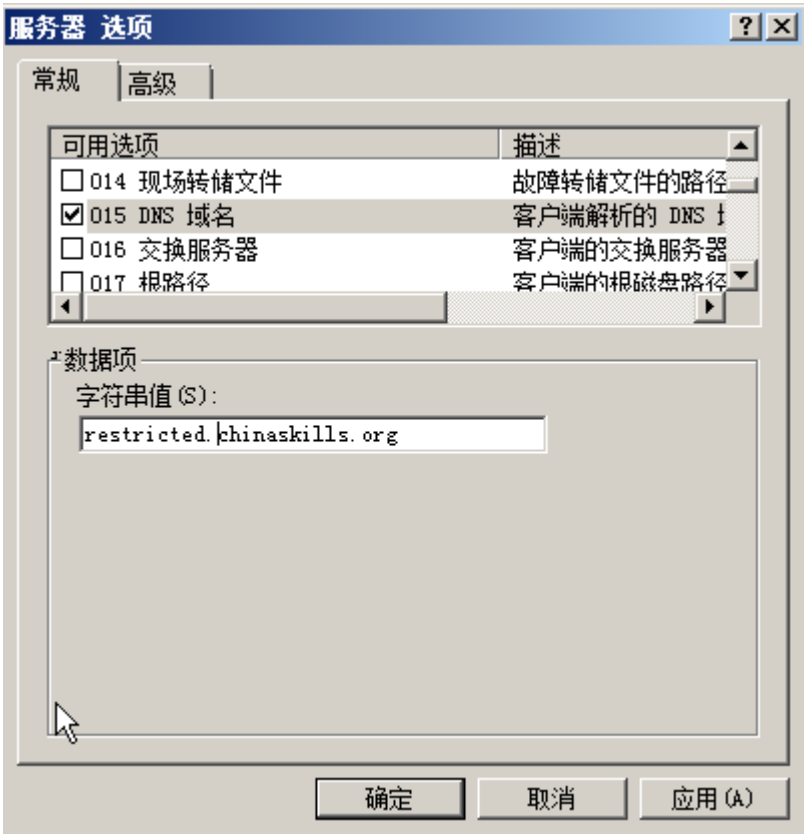


2. 修改 DHCP 服务设定，对 chinaskills.org 域启用网络访问保护。默认用户通过检查后可以完全访问网络的客户端获取的 DNS 域名为 chinaskills.org。默认的访问保护级别的用户获取的 DNS 域名为 restricted. chinaskills.org。


作用域 [10.100.100.0] chinaskills.org 属性
常规
DNS
网络访问保护
高级
网络访问保护
可在此设定该作用域的网络访问保护设置。
网络访问保护设置
对此作用域启用(N)
使用默认网络访问保护配置文件(D)
使用自定义配置文件(C)
配置文件名
对此作用域禁用(I)
确定
取消
应用(A)

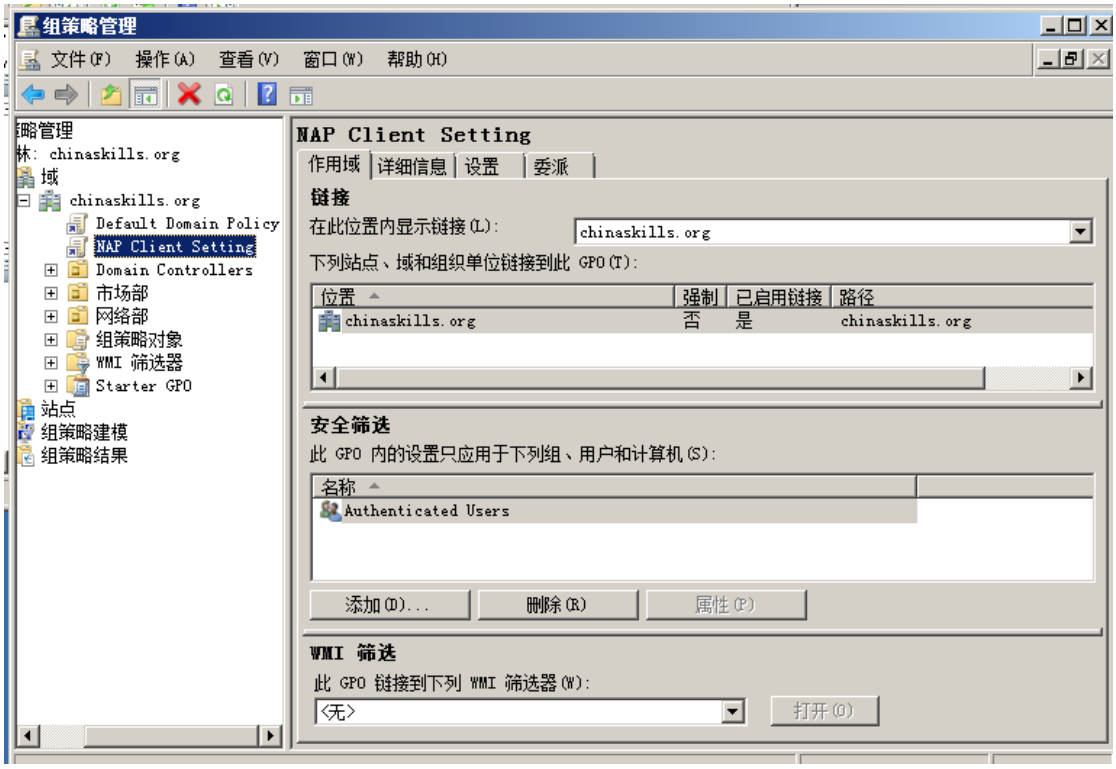

服务器 选项
常规
高级
可用选项
描述
004 时间服务器
按优先顺序排列的时
005 名称服务器
按优先顺序排列的名
006 DNS 服务器
DNS 服务器的阵列,
007 日志服务器
子网上的 MIT LCS
数据项
服务器名称(S):
chinaskills.org
解析(E)
IP 地址(P):
添加(D)
删除(R)
向上(U)
向下(O)
确定
取消
应用(A)



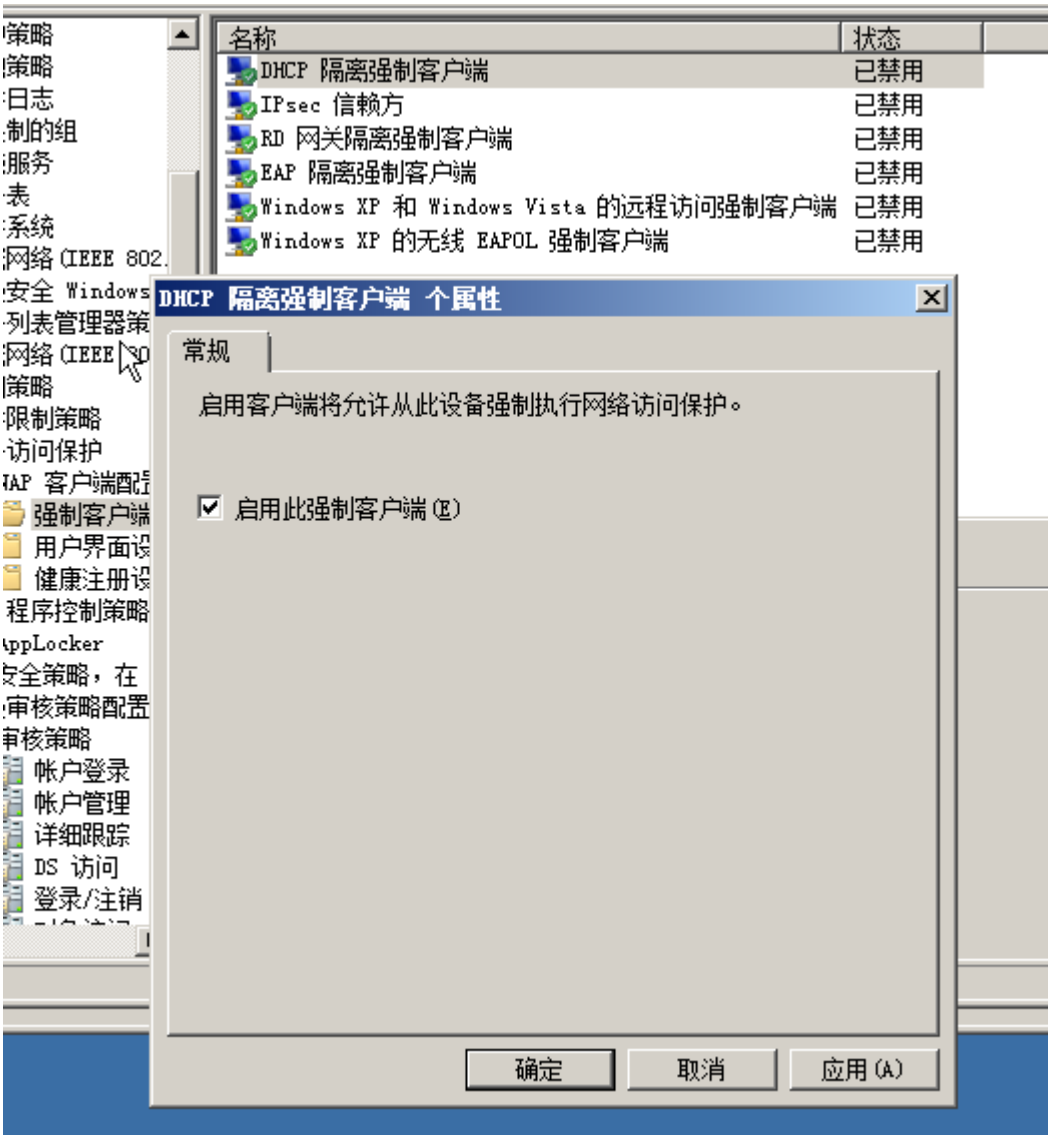


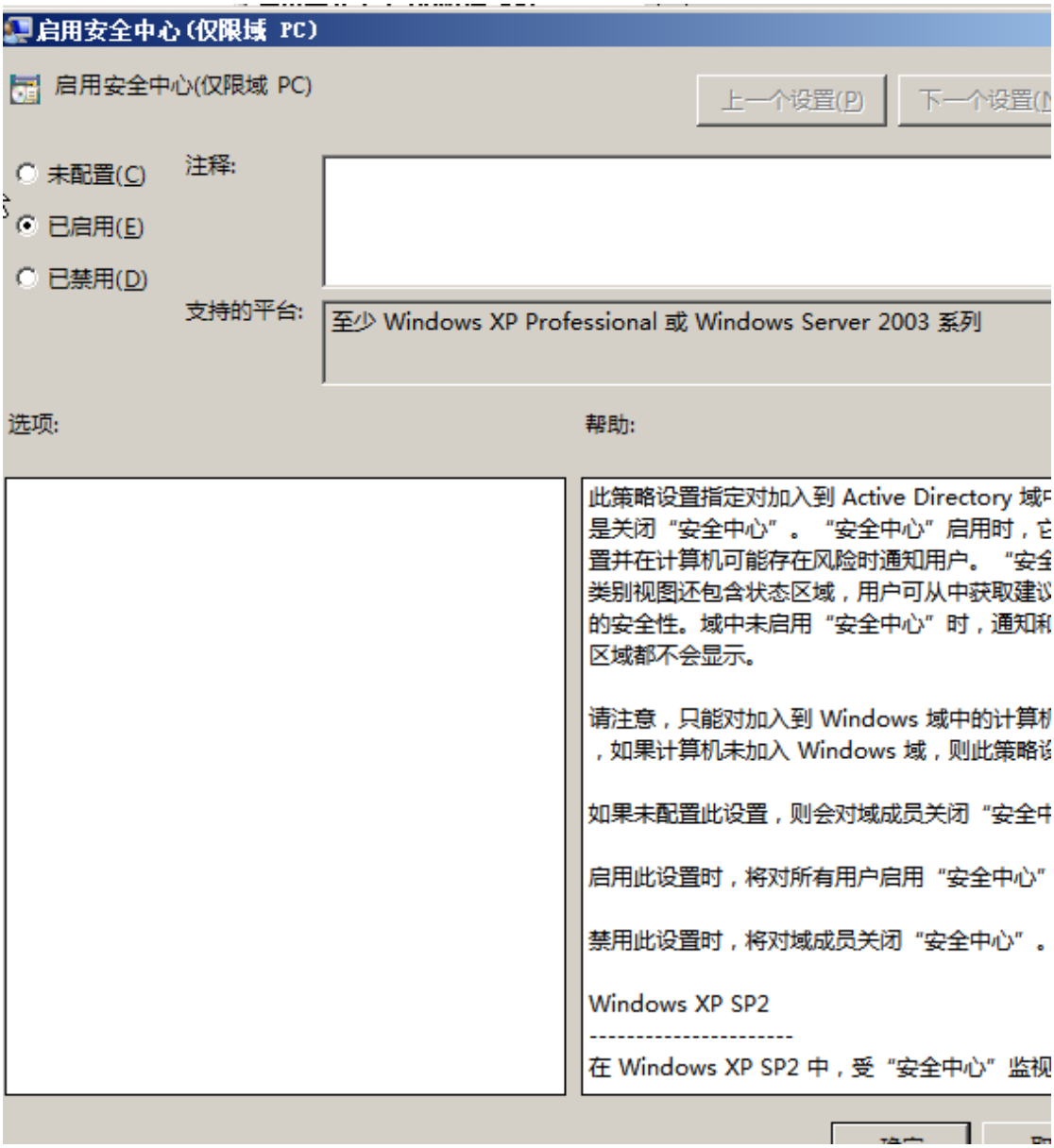
3. 在 **Win2008-C1** 中创建 chinaskills.org 域的组策略对象，命名为“NAP Client

Setting”。

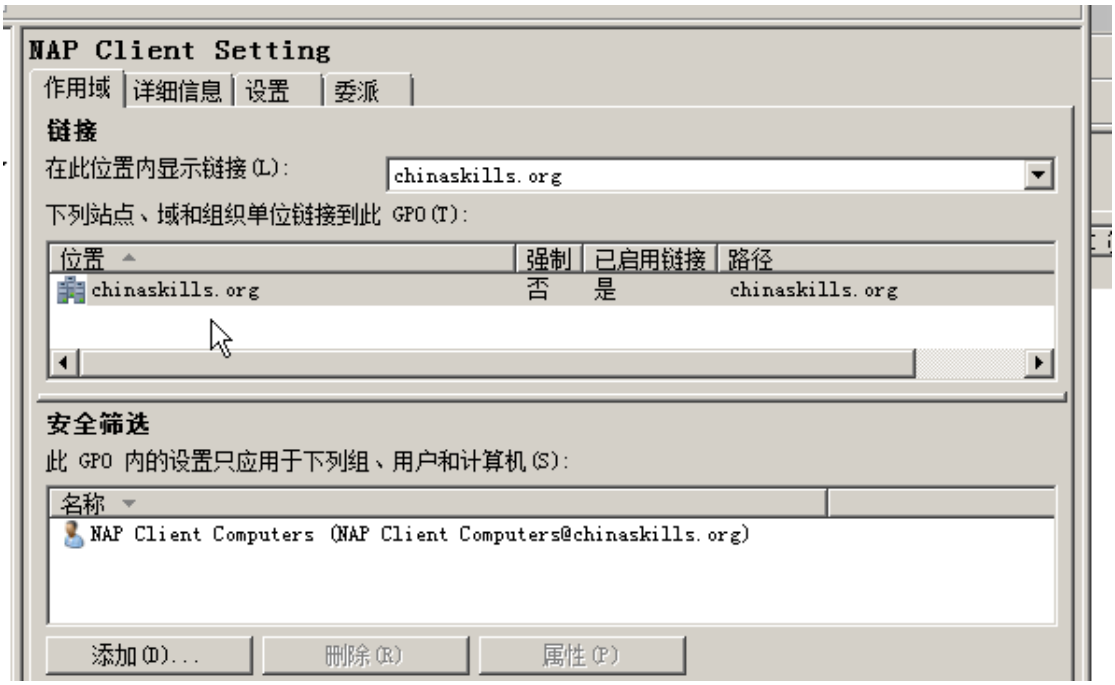


4. 在 NAP Client Setting 策略中设置“网络访问保护代理”系统服务自动启动。设置 NAP 策略 DHCP 强制隔离客户端。启动安全中心。

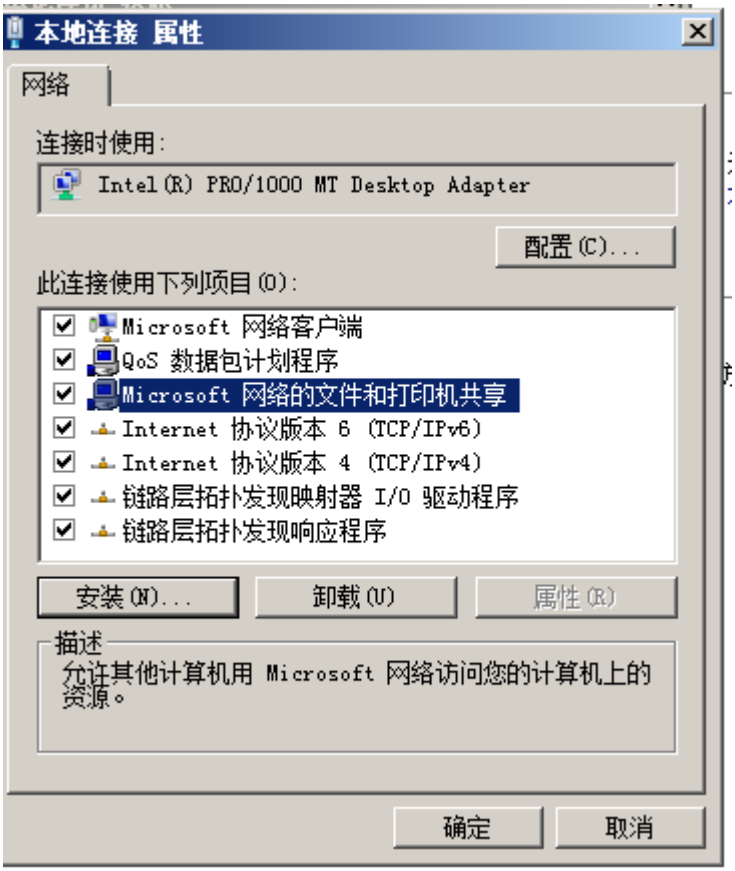

名称
状态
DHCP 隔离强制客户端
已禁用
IPsec 信赖方
已禁用
RD 网关隔离强制客户端
已禁用
EAP 隔离强制客户端
已禁用
Windows XP 和 Windows Vista 的远程访问强制客户端
已禁用
Windows XP 的无线 EAPOL 强制客户端
已禁用
DHCP 隔离强制客户端 个属性
常规
启用客户端将允许从此设备强制执行网络访问保护。
启用此强制客户端(E)
确定
取消
应用(A)



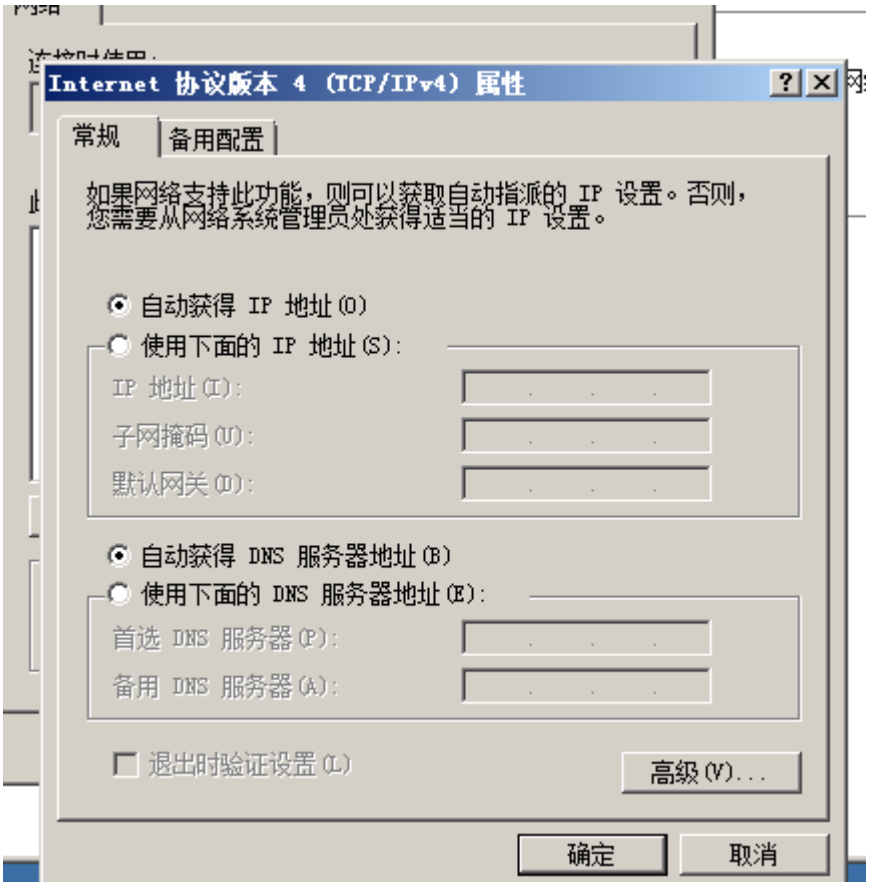
5. 删除 NAP Client Setting 策略安全筛选中原有的内容，添加 NAP Client Computers。



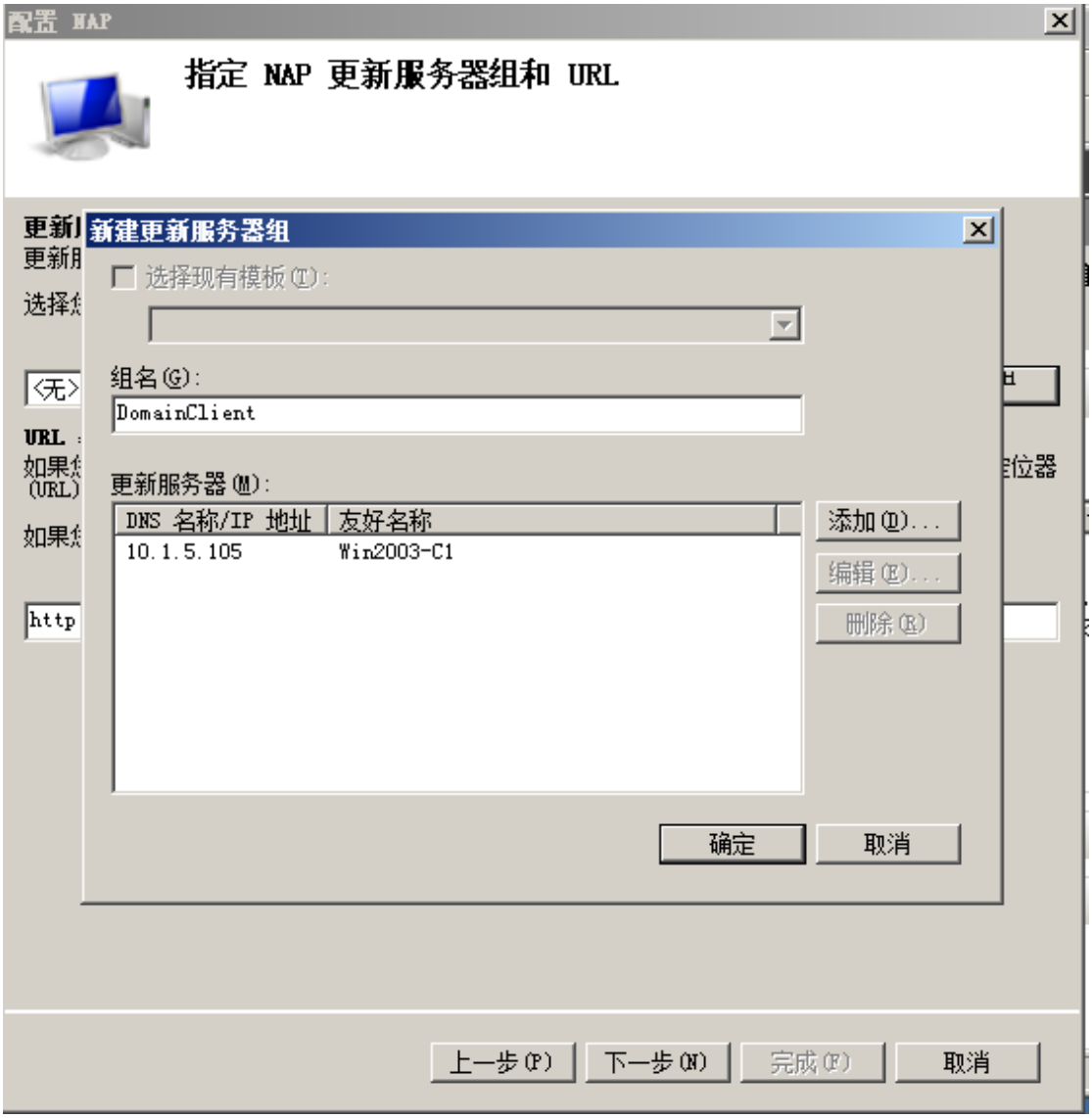
6. 在 **Win2008-C1** 中启动网络共享和文件发现功能。



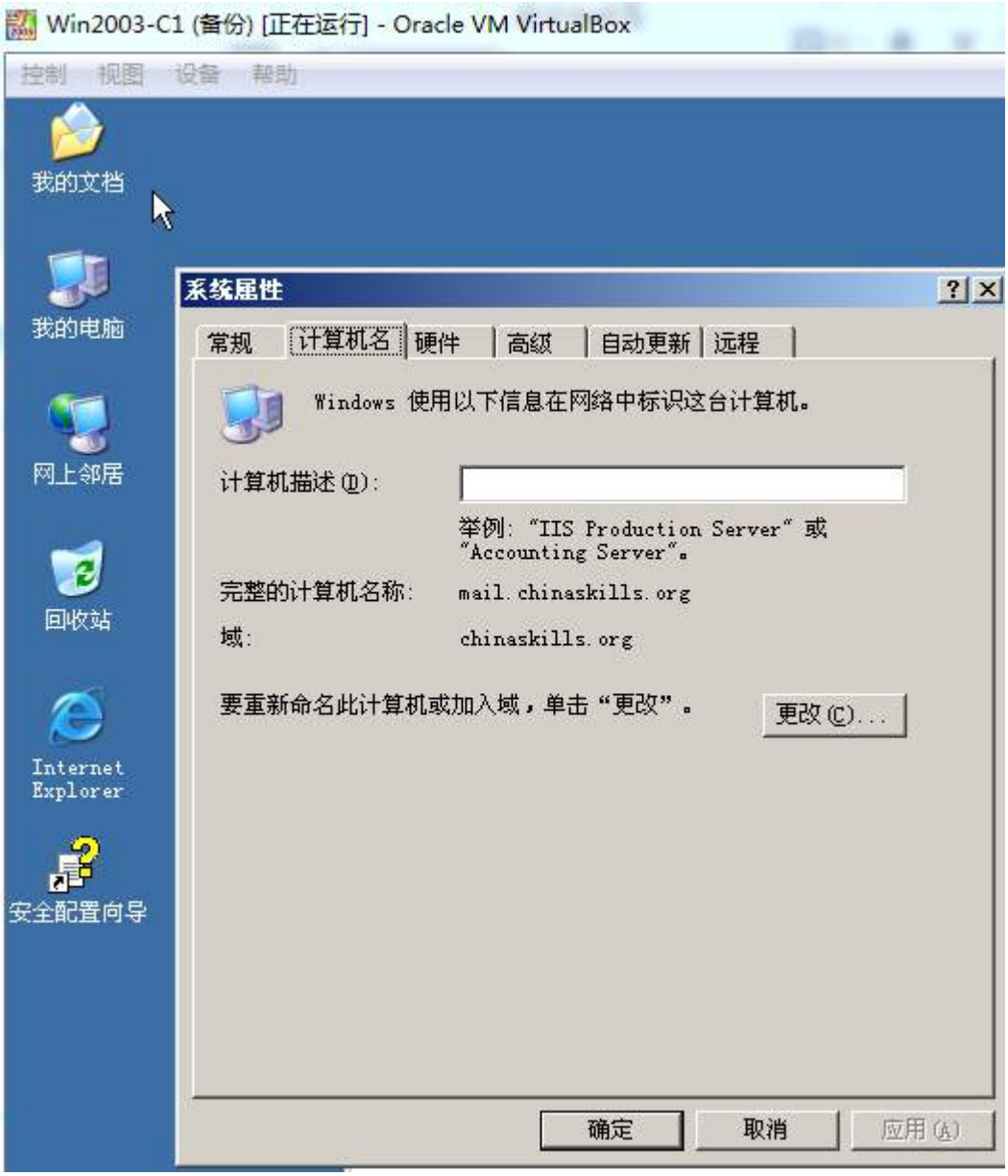
7. 将 Win2003-C1 的网卡设置为自动获取 IP 地址。

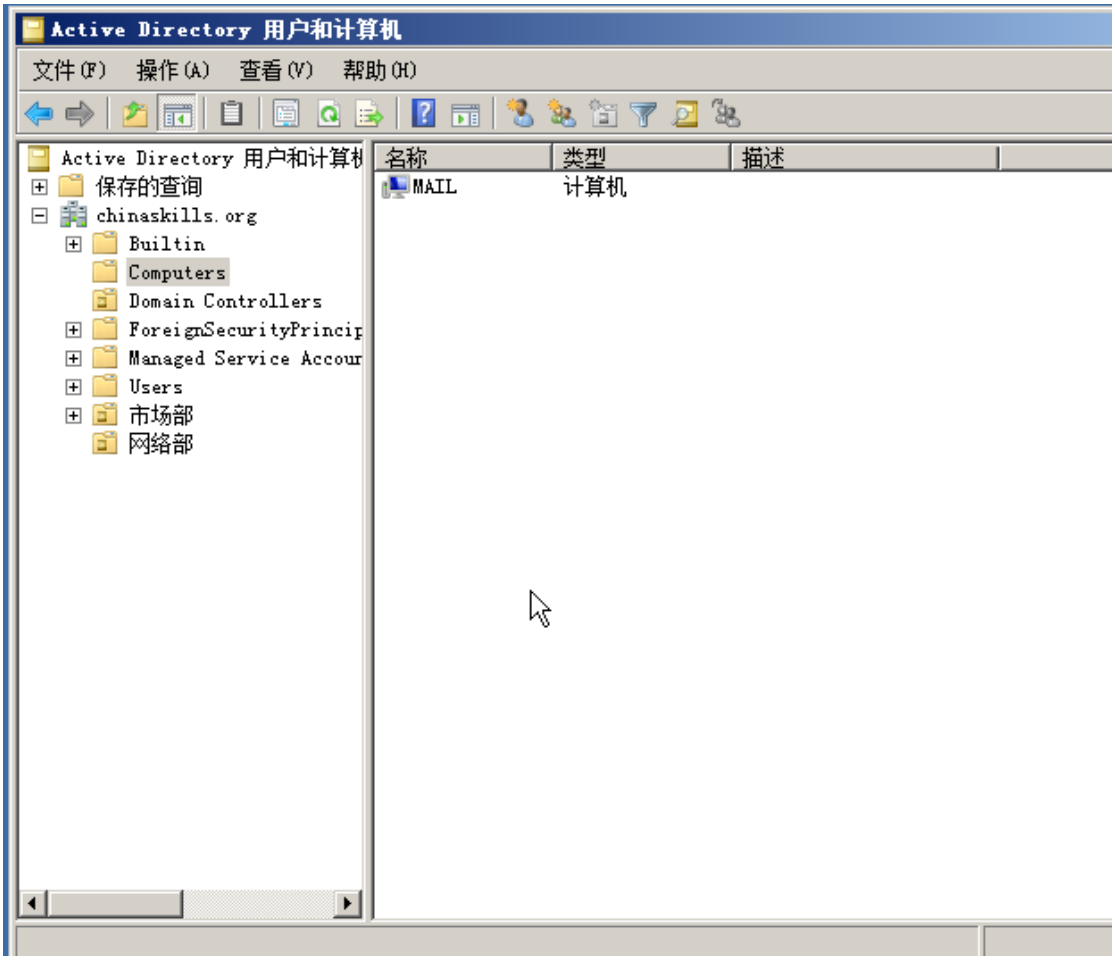


8. 修改 **Win2008-C1** 中的网络策略，在 DHCP 不支持 NAP 情况下，添加 NAP 强制更新服务器组，组名 DomainClient，将 Win2003-C1 获取的 IP 作为组中的好友。



9. Win2003-C1 刷新获取的地址，加入到 chinaskills.org 的域中。并在域控制器的Computers 中添加Win2003-C1。保证客户端的“Network Access Protection Agent”服务处于自动运行状态。


Win2003-C1 (备份) [正在运行] - Oracle VM VirtualBox
控制 视图 设备 帮助
我的文档
我的电脑
网上邻居
回收站
Internet Explorer
安全配置向导
系统属性
常规 计算机名 硬件 高级 自动更新 远程
Windows 使用以下信息在网络中标识这台计算机。
计算机描述(D):
举例: "IIS Production Server" 或 "Accounting Server"。
完整的计算机名称: mail.chinaskills.org
域: chinaskills.org
要重新命名此计算机或加入域，单击"更改"。
更改(C)...
确定
取消
应用(A)


Active Directory 用户和计算机
文件(F) 操作(A) 查看(V) 帮助(H)
Active Directory 用户和计算机
保存的查询
chinaskills.org
Builtin
Computers
Domain Controllers
ForeignSecurityPrincip
Managed Service Accour
Users
市场部
网络部
名称
类型
描述
MAIL
计算机


Network Access Protection Agent 的属性(本地计算机)
常规
登录
恢复
依存关系
服务名称: napagent
显示名称: Network Access Protection Agent
描述: 网络访问保护(NAP)代理服务收集和管理网络上客户端计算机的健康信息。NAP 代理收集的信
可执行文件的路径:
C:\Windows\System32\svchost.exe -k NetworkService
启动类型(E): 自动
帮助我配置服务启动选项。
服务状态: 已启动
启动(S)
停止(T)
暂停(P)
恢复(R)
当从此处启动服务时，您可指定所适用的启动参数。
启动参数(M):
确定
取消
应用(A)

Linux 操作系统部分

【说 明】

1、所有 Linux 操作系统的 root 用户的密码为 123456，若未按要求设置密码，涉及到该操作系统下的所有分值记为 0 分。

2、虚拟主机的 IP 属性设置请按照网络拓扑结构图以及“表 3：服务器 IP 地址分配表”的要求设定。

3、除有特别规定外，其他未明确规定用户密码均与用户名相同。

4、所有操作系统镜像文件及试题所需的其他软件均存放于每台计算机的/根目录下，并将题目要求的截图内容以.jpg 格式存储于各物理机桌面 BACKUP_X（X 为组号）文件夹中，文件名、扩展名和存放位置错误，涉及到的所有操作分值记为 0 分。

5、题目要求的虚拟机均安装于每台主机的 D：\virtualPC 目录，即路径为 D：\virtualPC\虚拟主机名称。

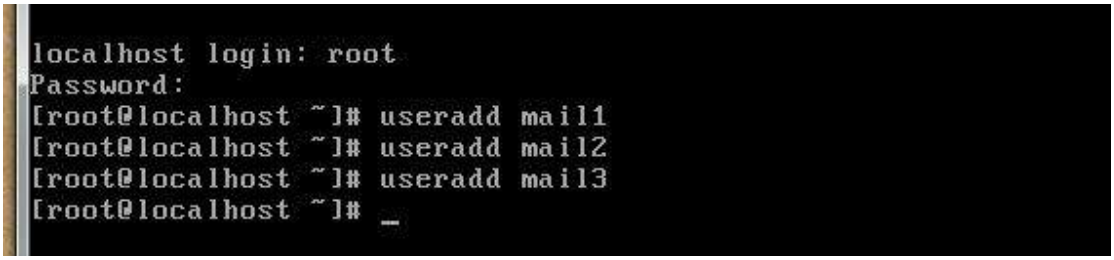
一、在 PC1 上完成如下操作:

（一）完成虚拟主机的创建

安装名为“Centos-A1”的虚拟机，具体要求为硬盘大小为 20GB，内存为 700MB，系统为 Centos6.5。分区大小为：SWAP 分区大小为 512M；/boot 分区大小为 150M，文件类型为 ext4；/home 分区大小为 1G，文件类型为 ext4，其余为/分区，文件类型为 ext4；将其结果进行截图，保存为 Centos-A1。

（二）在主机 Centos-A1 中完成 E-MAIL 服务器的部署

1、在此服务器上配置基于 SMTP 认证的 postfix 邮件服务，创建创建三个用户 mail1,mail2,mail3；每个用户的邮箱大小为 20MB，限定用户发邮件时，附件大小为 5MB；



```
# location of alias file
O AliasFile=/etc/aliases

# minimum number of free blocks on filesystem
O MinFreeBlocks=100

# maximum message size
O MaxMessageSize=5242880

# substitution for space (blank) characters
O BlankSub=.

# avoid connecting to "expensive" mailers on initial submis
O HoldExpensive=False

# checkpoint queue runs after every N successful deliveries
#O CheckpointInterval=10

# default delivery mode
O DeliveryMode=background

# error message header/file
#O ErrorHeader=/etc/mail/error-header
```

2、为每个员工创建邮箱账户，实现不同用户之间的正常通讯，用户密码为123，邮件服务器的域名后缀为 jnds.net，邮件服务器要在所有 IP 地址上进行侦听；

```
myhostname = mail.jnds.net
#myhostname = virtual.domain.tld

# The mydomain parameter specifies the local internet domain name
# The default is to use $myhostname minus the first component.
# $mydomain is used as a default value for many other configurati
# parameters.
#
mydomain = jnds.net

# SENDING MAIL
#
# The myorigin parameter specifies the domain that locally-posted
# mail appears to come from. The default is to append $myhostname,
# which is fine for small sites.  If you run a domain with multip
# machines, you should (1) change this to $mydomain and (2) set u
# a domain-wide alias database that aliases each user to
# user@that.users.mailhost.
#
# For the sake of consistency between sender and recipient address
# myorigin also specifies the default domain name that is appende
# to recipient addresses that have no @domain part.
#
myorigin = $mydomain
```

```
# addresses that this mail system receives mail on.  By default,
# the software claims all active interfaces on the machine. The
# parameter also controls delivery of mail to user@[ip.address].
#
# See also the proxy_interfaces parameter, for network addresses that
# are forwarded to us via a proxy or network address translator.
#
# Note: you need to stop/start Postfix when this parameter changes.
#
inet_interfaces = all
#inet_interfaces = $myhostname
#inet_interfaces = $myhostname, localhost
#net_interfaces = localhost

# Enable IPv4, and IPv6 if supported
inet_protocols = all

# The proxy_interfaces parameter specifies the network interface
# addresses that this mail system receives mail on by way of a
# proxy or network address translation unit. This setting extends
# the address list specified with the inet_interfaces parameter.
#
# You must specify your proxy/NAT addresses when your system is a
# backup MX host for other domains, otherwise mail delivery loops
-- INSERT --                                                  113,2
```

3、设置 postfix 服务需要运行级别 3 和 5 级别开机自动启动，其它运行级别必须为关闭；

```
[root@localhost postfix]# chkconfig --level 35 postfix on
[root@localhost postfix]# chkconfig |grep postfix
postfix         0:off   1:off   2:on    3:on    4:on    5:on    6:off
```

4、将 163.com 服务器发来的邮件全部挡掉，并回传讯息给原发信端。

```
setgid_group = postdrop

# html_directory: The location of the Postfix HTML documentation.
#
html_directory = no

# manpage_directory: The location of the Postfix on-line manual pages.
#
manpage_directory = /usr/share/man

# sample_directory: The location of the Postfix sample configuration files.
# This parameter is obsolete as of Postfix 2.1.
#
sample_directory = /usr/share/doc/postfix-2.6.6/samples

# readme_directory: The location of the Postfix README files.
#
readme_directory = /usr/share/doc/postfix-2.6.6/README_FILES
smtpd_sender_restrictions = check_recipient_access hash:/etc/postfix/drop_domain
~
~
```

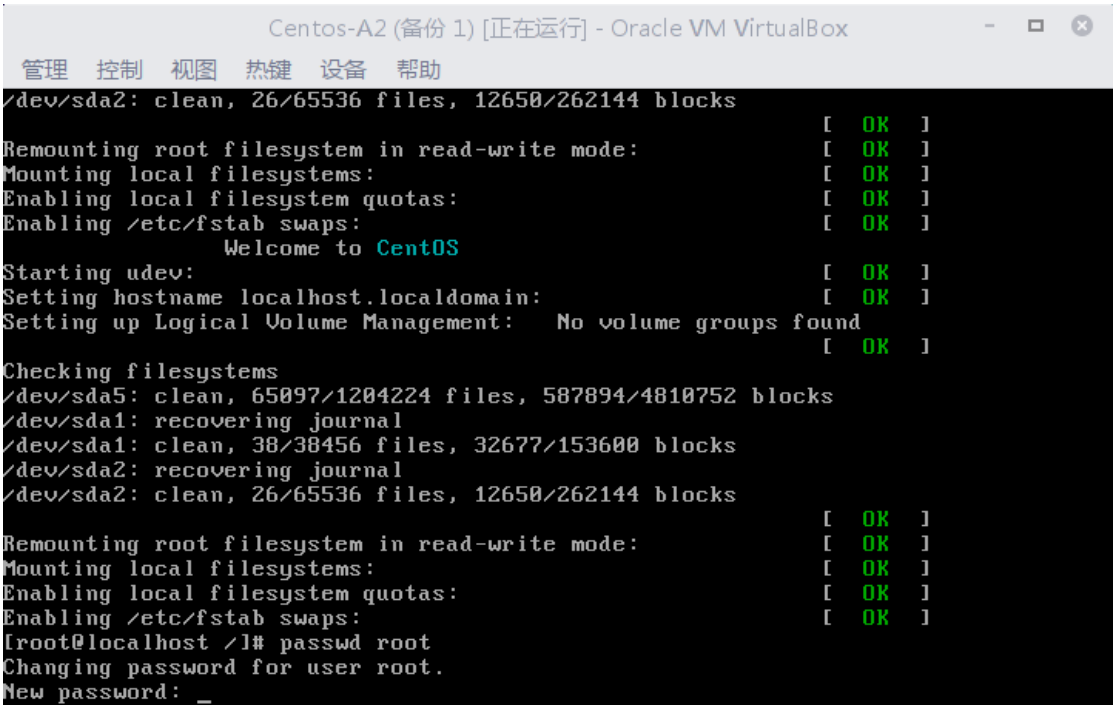
```
[root@localhost postfix]# cat drop_domain
163.com DISCARD
[root@localhost postfix]#
```

（三）在主机 Centos-A2 中完成密码的清除和 yum 的部署

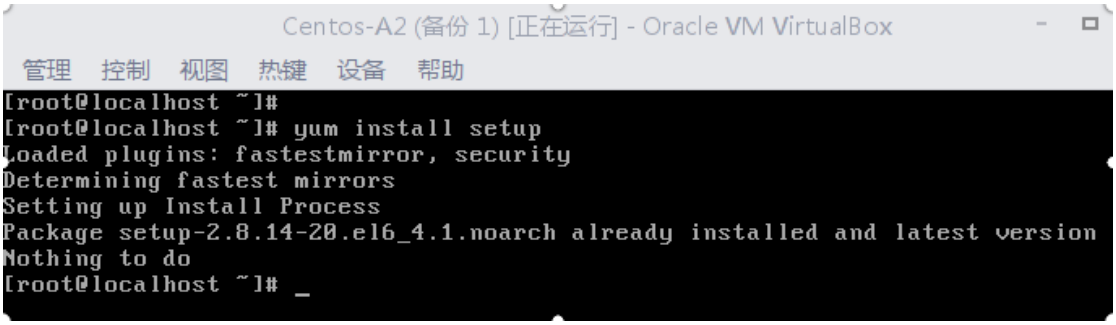
注：如果由于不会破解密码无法实现 2-4 题，可以询问监考人员该系统的密

码，但需要扣除 10 分。

1、将标识为“PC1”的计算机上的已有虚拟机 Centos-A2 启动，请破解 Root 的密码，并将新密码设置为 nvsc.com；



2、配置 Centos-A2 的 yum，并通过 yum 安装 setup 工具包，截图为 yum；



3、配置 Centos-A2 的 IPv6 地址为：2001:DA8:3010::2/64，截图为 ipv6；

```
[root@localhost network-scripts]# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:8C:FA:4F
          inet6 addr: 2001:da8:3010::2/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fe8c:fa4f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:352 errors:0 dropped:0 overruns:0 frame:0
          TX packets:81 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:33460 (32.6 KiB)  TX bytes:6642 (6.4 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:114 errors:0 dropped:0 overruns:0 frame:0
          TX packets:114 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:7192 (7.0 KiB)  TX bytes:7192 (7.0 KiB)

[root@localhost network-scripts]# _
```

4、为了防止管理员之外的人员再次破解 Root 密码，请配置 BOOT 启动密码为：2015network，截图为 boot；

```
[root@localhost network-scripts]# grub-md5-crypt
Password:
Retype password:
$1$OyMtp$TUjSGXe5rCS.GyqjuN0FJ1
[root@localhost network-scripts]# _
```

```
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this file
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/mapper/VolGroup-lv_root
#          initrd /initrd-[generic-]version.img
#boot=/dev/sda
default=0
timeout=5
splashimage=(hd0,0)/grub/splash.xpm.gz
hiddenmenu
password --md5 $1$OyMtp$TUjSGXe5rCs.GyqjN0FJ1
title CentOS (2.6.32-431.el6.x86_64)
        lock
        root (hd0,0)
        kernel /vmlinuz-2.6.32-431.el6.x86_64 ro root=/dev/mapper/VolGroup-lv_ro
ot rd_NO_LUKS rd_NO_MD rd_LVM_LV=VolGroup/lv_swap crashkernel=auto LANG=zh_CN.UT
F-8 rd_LVM_LV=VolGroup/lv_root  KEYBOARDTYPE=pc KEYTABLE=us rd_NO_DM rhgb quiet
        initrd /initramfs-2.6.32-431.el6.x86_64.img
~
~
```

二、在 PC 2 上完成如下操作：

（一）完成虚拟主机的创建

1、安装虚拟机“Centos-B1”,具体要求为内存 512MB，硬盘 10GB；

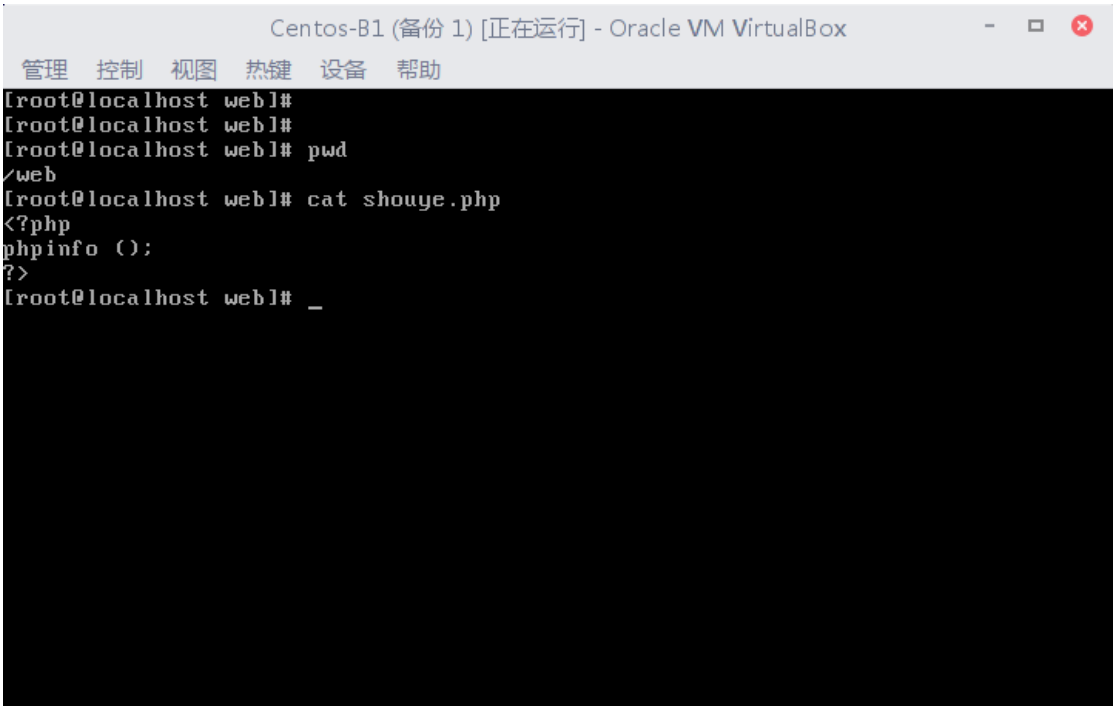
2、安装虚拟机“Centos-B2”,具体要求为内存 512MB,硬盘 10GB；

（二）在主机 Centos-B1 中完成 WEB 服务器 1 的部署

1、在 Centos-B1 上搭建一个 WEB 服务器。站点根目录在/web，首页文件命名为 shouye.php，内容为

```
<?php
  phpinfo();
```

?>。



2、建立一个名为 confighttp 的 shell 脚本放置在用户主目录。该脚本的功能是打开编辑 httpd.conf 配置文件。

3、配置使得用户只能使用域名访问网站，不能使用 ip 地址。

4、将/home 目录打包并压缩成 gzip 格式，文件名为 var.tar.gz，保存到/tmp 目录下。

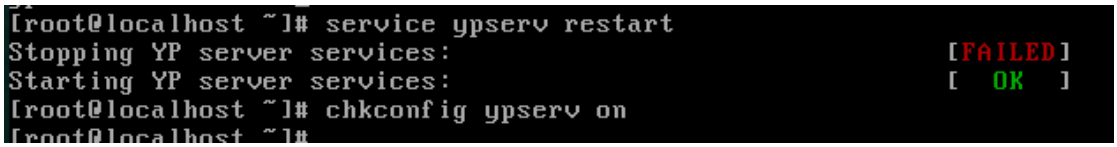
```
[root@localhost network-scripts]# tar -zcvf /tmp/var.tar.gz /home
```

（三）在主机 Centos-B1 中完成 NIS 客户端的部署

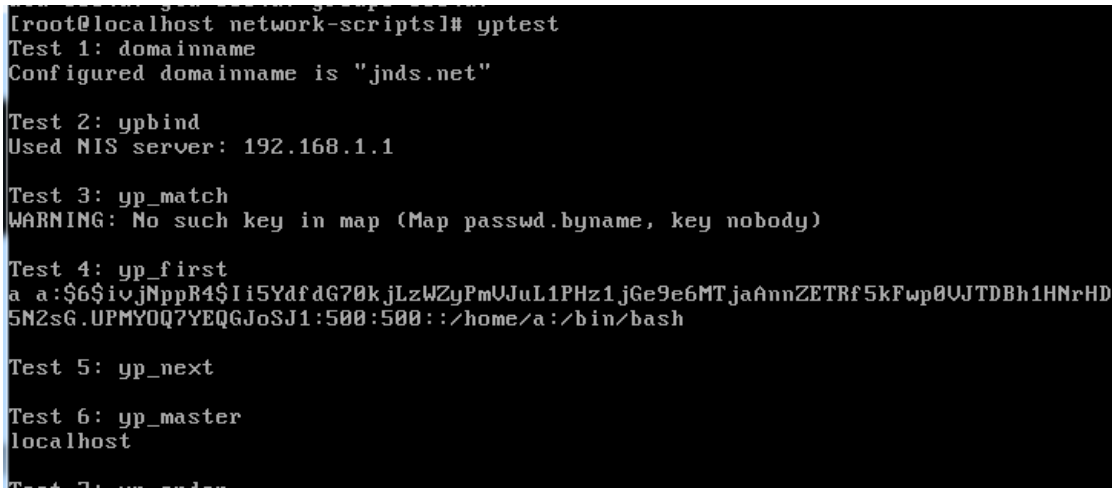
1、安装 NIS 服务，设置 NIS 域名为 jnds.net，指定通过 NIS 进行身份认证。

```
[root@localhost ~]# nisdomainname jnds.net
[root@localhost ~]# nisdomainname
jnds.net
[root@localhost ~]# rpm -qa !gerp yp
-bash: gerp: command not found
[root@localhost ~]# ^C
[root@localhost ~]# rpm -qa !grep yp
perl-Crypt-SSLeay-0.57-16.el6.i686
cryptsetup-luks-1.2.0-7.el6.i686
ypbind-1.20.4-30.el6.i686
python-crypto-2.0.1-22.el6.i686
freetype-2.3.11-14.el6_3.1.i686
xorg-x11-fonts-Type1-7.2-9.1.el6.noarch
libgcrypt-1.4.5-11.el6_4.i686
cryptsetup-luks-libs-1.2.0-7.el6.i686
yp-tools-2.9-12.el6.i686
ypserv-2.19-26.el6_4.2.i686
[root@localhost ~]# _
```

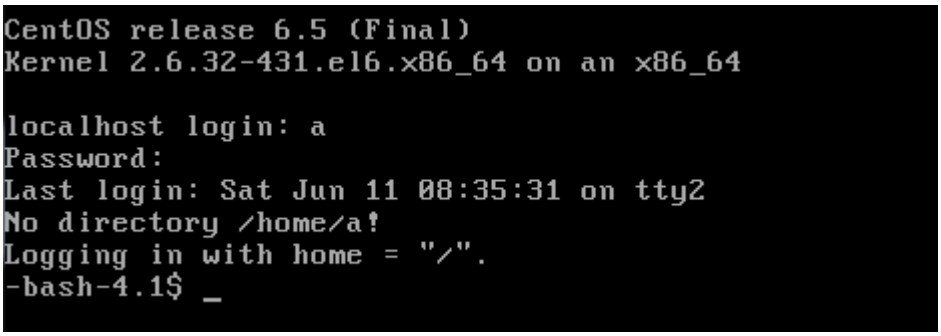
2、启动服务，并设置开机自动启动。



3、使用 yptest 进行测试，将测试结果截图为 yptest。

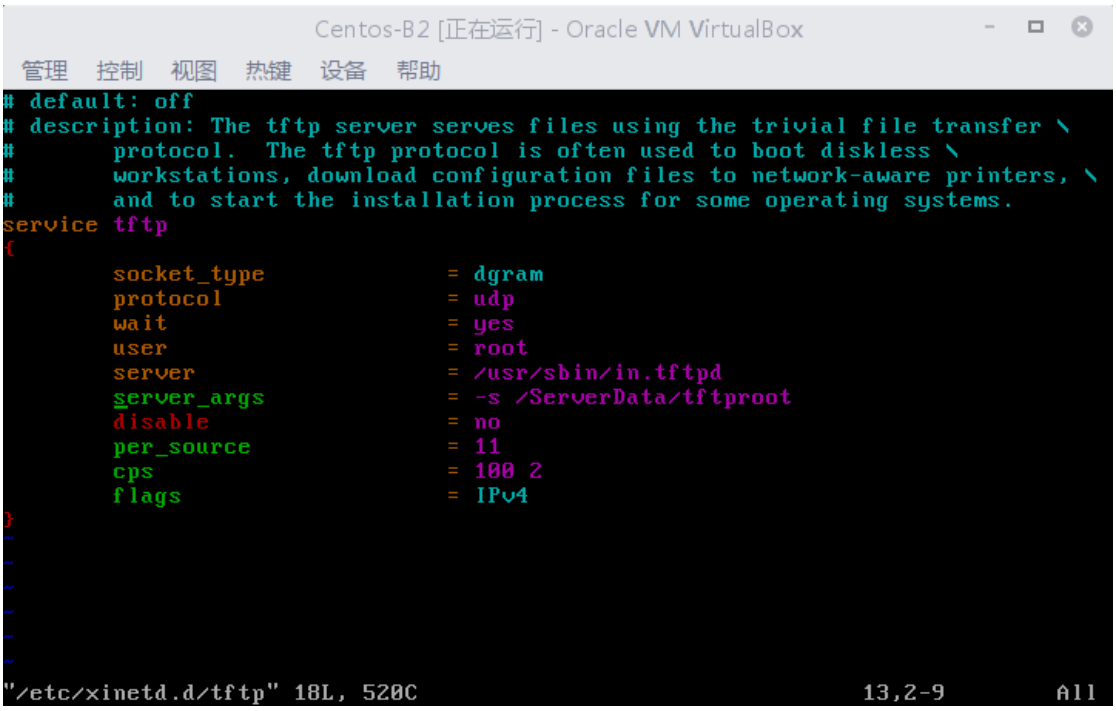


4、使用用户 a 登录，要求显示登录成功的界面，并截图为 suc。

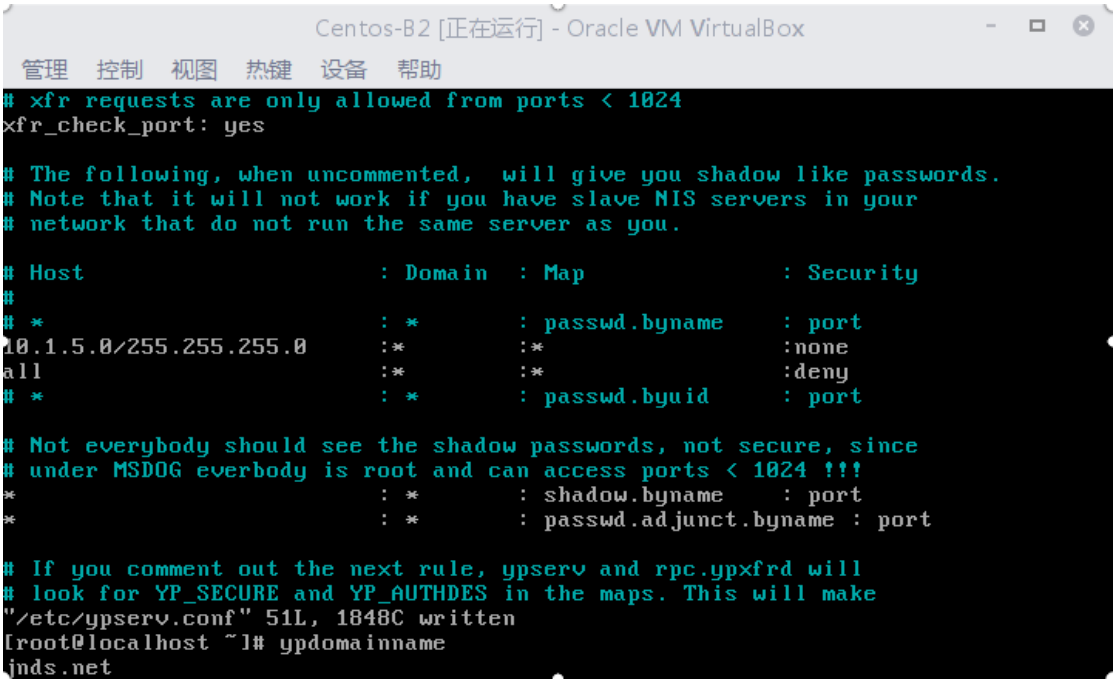


（四）在主机 Centos-B2 中完成 TFTP 和 NIS 服务器的部署(20 分)

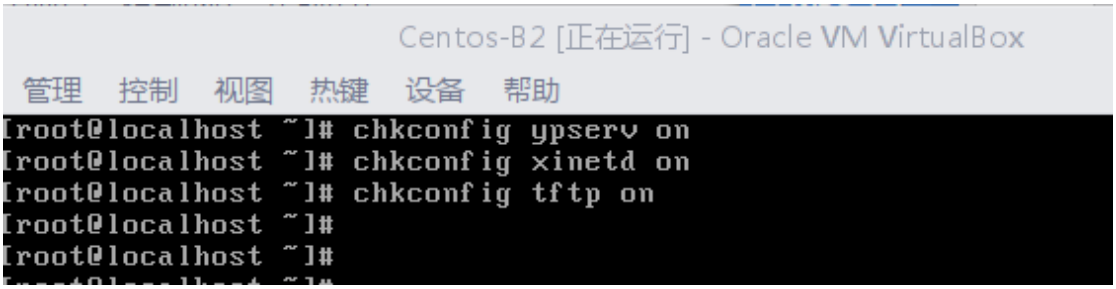
1、安装 TFTP 服务，将 TFTP 服务的根目录设置在/ServerData/tftproot



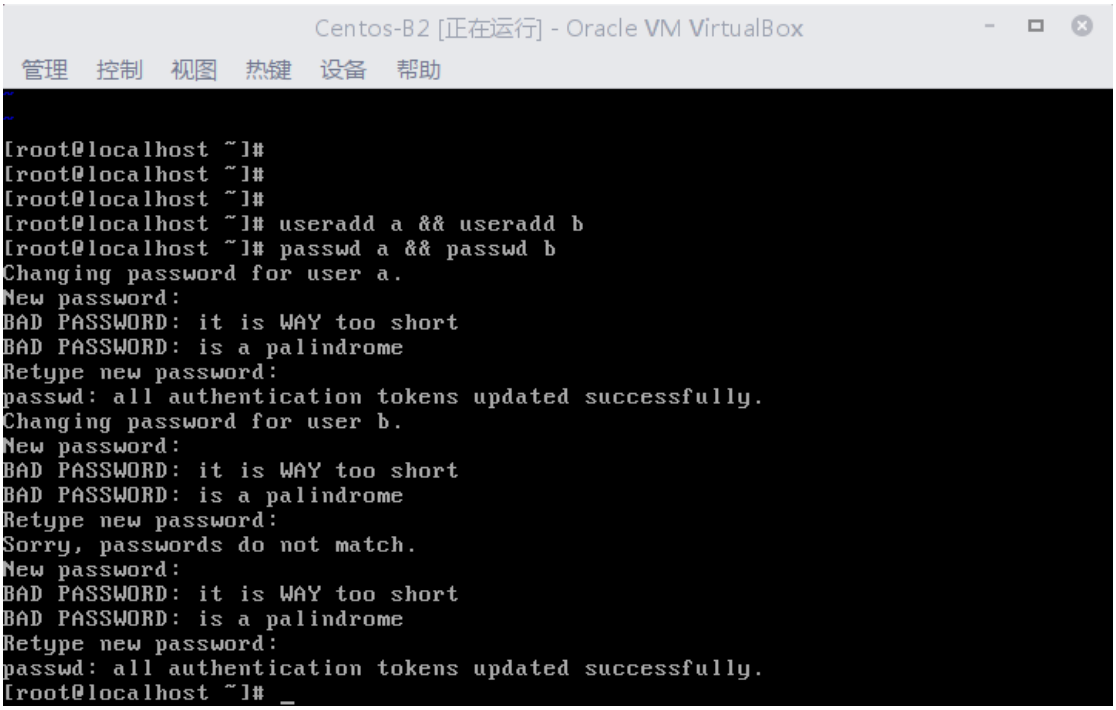
2、安装 NIS 服务，设置 NIS 域名为 jnds.net，只允许本网段可以访问。



3、启动服务，并设置开机自动启动。



4、新建用户 a 和 b，密码为 1 和 2。



三、在 PC 3 上完成如下操作：

（一）完成虚拟主机的创建

1、安装名为“Centos-C1”的虚拟机，具体要求为硬盘大小为 30GB，内存为 768MB，系统为 Centos6.5。分区大小为：SWAP 分区大小为 512M；/boot 分区大小为 200M，文件类型为 ext3；/home 分区大小为 3G，文件类型为 ext3，其余为/分区，文件类型为 ext3；将其结果进行截图，保存为 Centos-C1。

名称: Centos-C1
操作系统: Red Hat (64-bit)

系统

内存大小: 768 MB
启动顺序: 软驱, 光驱, 硬盘
硬件加速: VT-x/AMD-V, 嵌套分页, PAE/NX, KVM 半虚拟化

显示

显存大小: 12 MB
远程桌面服务器: 已禁用
录像: 已禁用

存储

控制器: IDE
第二IDE控制器主通道: [光驱] CentOS-6.5-i386-bin-DVD1.iso (3.58 GB)
控制器: SATA
SATA 端口 0: Centos-C1.vdi (普通, 30.00 GB)

Centos-C1 [正在运行] - Oracle VM Vir

管理 控制 视图 热键 设备 帮助

Please Select A Devi

Device	Size (MB)	Mount Point/ RAID/Volume	Type	Format
Hard Drives				
sda (/dev/sda)				
sda1	200	/boot	ext3	✓
sda2	3072	/home	ext3	✓
sda3	512		swap	✓
sda4	26935		Extended	
sda5	26934	/	ext3	✓

2、安装虚拟机“Centos-C2”,具体要求为内存 512MB,硬盘 10GB；

（二）在主机 Centos-C1 中完成 WEB 服务器 2 的部署

1、在 Centos-C1 上搭建 WEB 服务器。站点根目录在/houbeiweb，首页文件命名为 shouye.php，内容为

<?php

phpinfo();

?>。

，修改配置文件禁止目录浏览。

```
"/houbeiweb/shouye.php" [New] 3L, 21C written
[root@localhost ~]# cat /houbeiweb/shouye.php
<?php
        phpinfo();
?>
[root@localhost ~]# _
```

```
290 # symbolic links and aliases may
291 #
292 DocumentRoot "/houbeiwen"
293
294 #
295 # Each directory to which Apache
296 # to which services and features
297 # directory (and its subdirector
298 #
299 # First, we configure the "defau
300 # features.
301 #
302 <Directory />
303     Options FollowSymLinks
304     AllowOverride None
305     DirectoryIndex shouye.html
306 </Directory>
307
308 #
309 # Note that from this point forw
310 # particular features to be enab
```

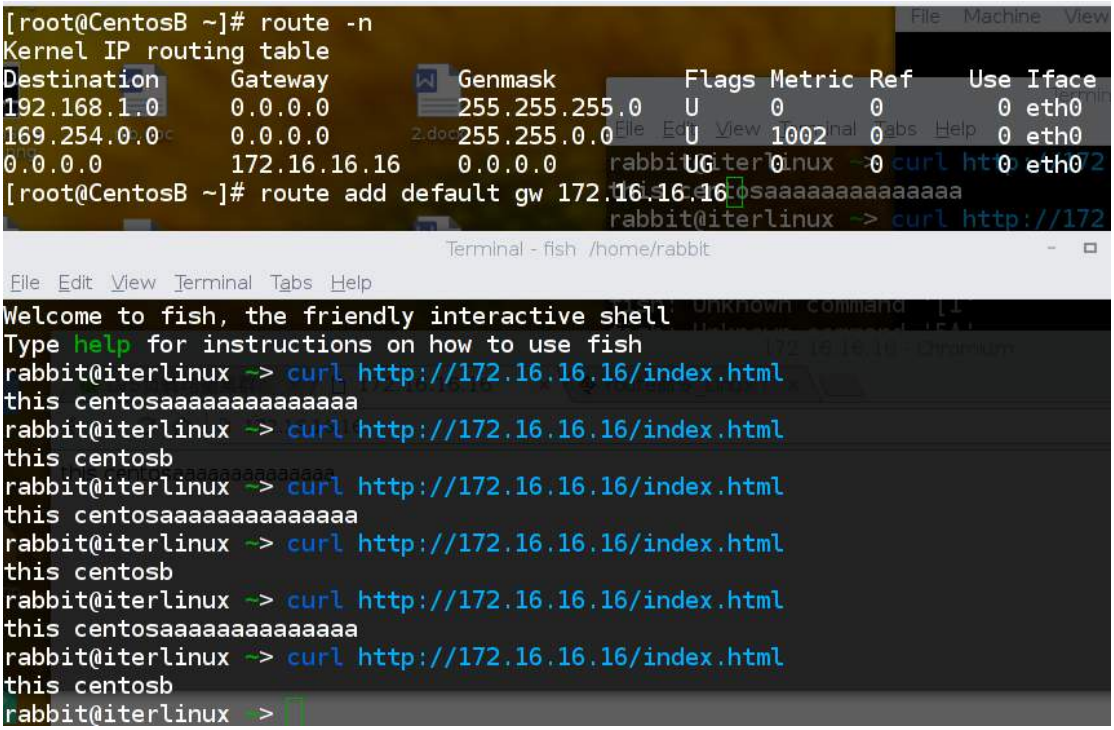
```
319 #
320 # Possible values for the Options directive are "N
321 # or any combination of:
322 #   Indexes Includes FollowSymLinks SymLinksifOwne
323 #
324 # Note that "MultiViews" must be named *explicitly
325 # doesn't give it to you.
326 #
327 # The Options directive is both complicated and im
328 # http://httpd.apache.org/docs/2.2/mod/core.html#o
329 # for more information.
330 #
331     Options -Indexes FollowSymLinks
332
333 #
334 # AllowOverride controls what directives may be pl
```

2、借助自签名证书完成 web 服务的配置，结合 ssl 实现安全传输，复制一个 CA 服务器认证证书, 在 win7-D1 安装此证书，实现安全的访问；

```
104 # certificate can be generated using the genkey(1) command.
105 SSLCertificateFile /etc/pki/tls/certs/win7.crt
106
107 #   Server Private Key:
108 #   If the key is not combined with the certificate, use this
109 #   directive to point at the key file.  Keep in mind that if
110 #   you've both a RSA and a DSA private key you can configure
111 #   both in parallel (to also allow the use of DSA ciphers, etc.)
112 SSLCertificateKeyFile /etc/pki/tls/private/localhost.key
113
114 #   Server Certificate Chain:
115 #   Point SSLCertificateChainFile at a file containing the
"/etc/httpd/conf.d/ssl.conf" 222L, 9468C written
[root@localhost ~]#
```

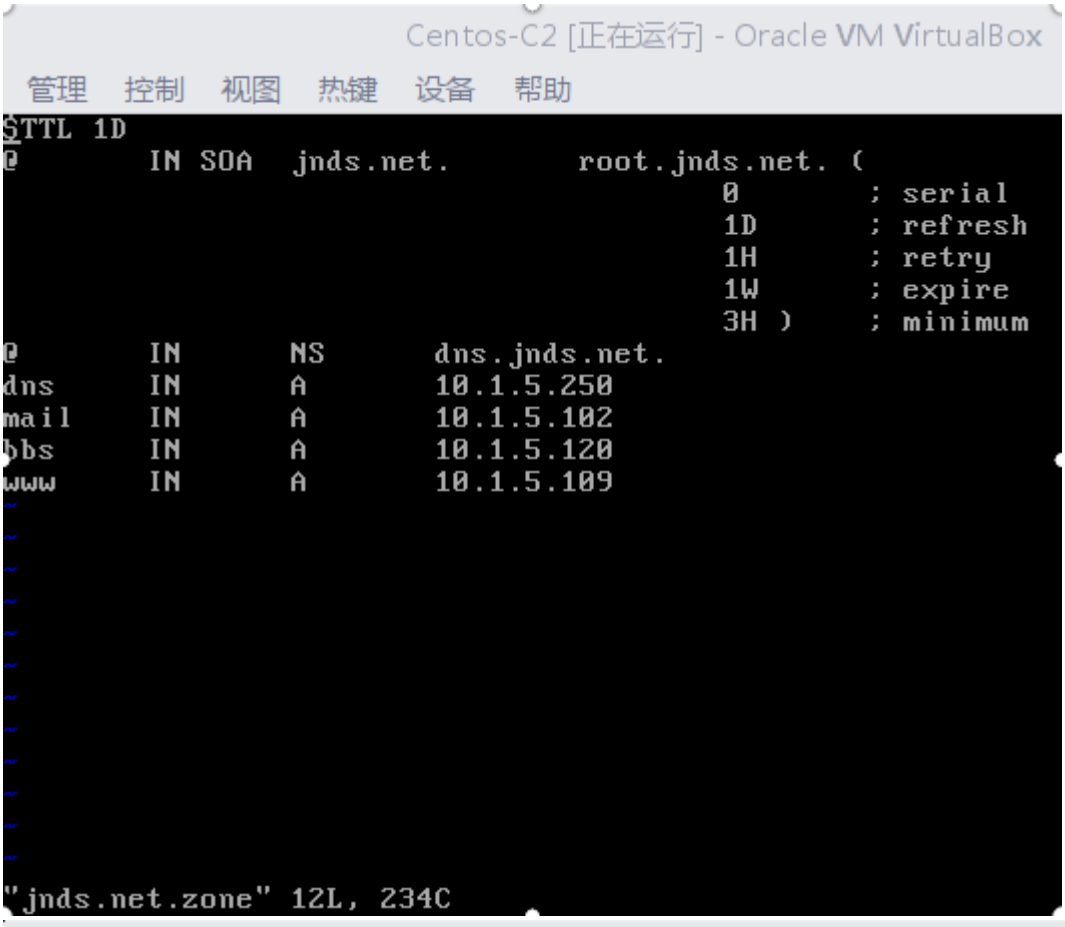
3、将 **Centos-B1** 与 Centos-C1 提供负载平衡的 Web 服务。其中虚拟地

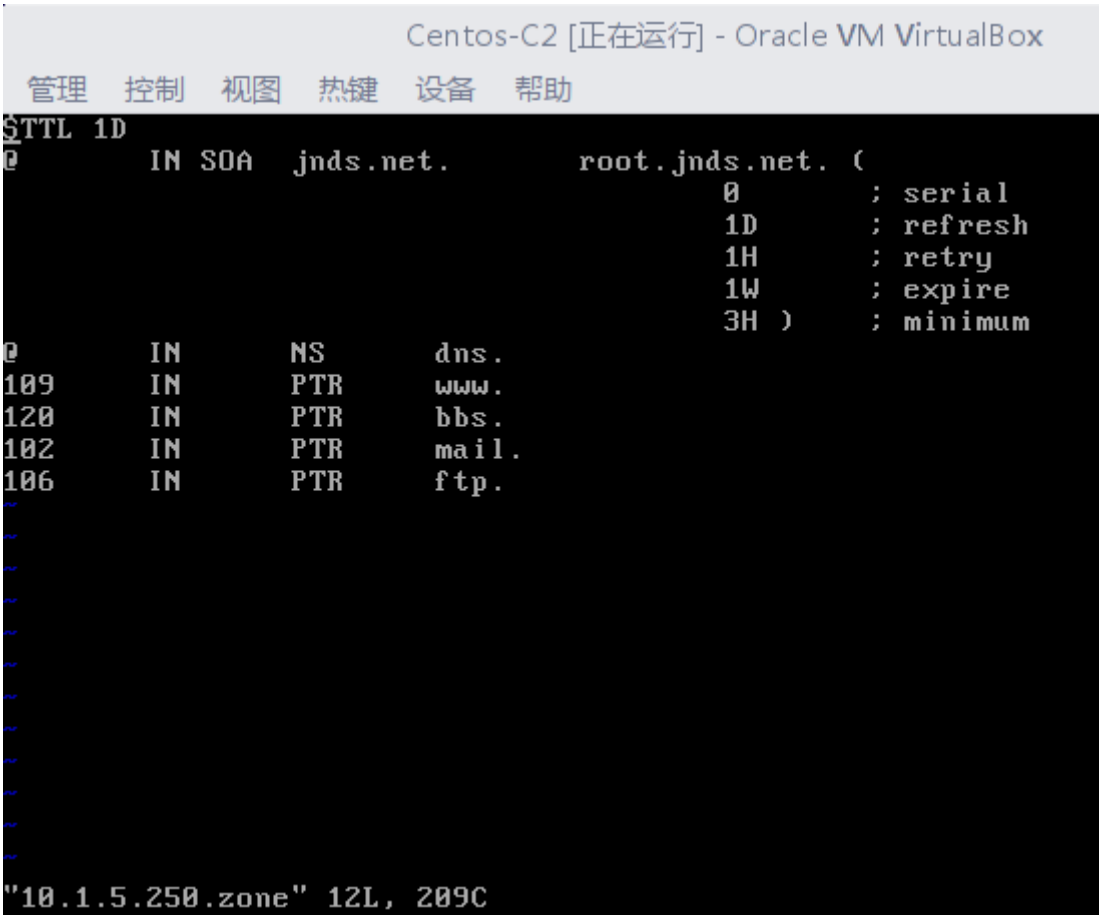
址为 10.10.100.250/24，**Centos-B1** 作为均衡管理主机。将 **Centos-B1** 设置完成 IP 地址的界面截屏保存命名为 3-1，将 Centos-C1 设置完成 IP 地址的界面截屏保存为 3-2。(有文档，类似这张图。按文档做)



（三）在主机 Centos-C2 中完成 bind、 FTP 服务器的部署

1、在此服务器中安装配置 bind 服务，负责区域“jnds.net”内主机解析，分别为 dns.jnds.net 、www.jnds.net、bbs.jnds.net、ftp.jnds.net 以及 mail.jnds.net,做好正反向 DNS 服务解析；


Centos-C2 [正在运行] - Oracle VM VirtualBox
管理 控制 视图 热键 设备 帮助
$TTL 1D
@ IN SOA jnds.net. root.jnds.net. (
0 ; serial
1D ; refresh
1H ; retry
1W ; expire
3H) ; minimum
@ IN NS dns.jnds.net.
dns IN A 10.1.5.250
mail IN A 10.1.5.102
bbs IN A 10.1.5.120
www IN A 10.1.5.109
"jnds.net.zone" 12L, 234C


Centos-C2 [正在运行] - Oracle VM VirtualBox
管理 控制 视图 热键 设备 帮助
$TTL 1D
@ IN SOA jnds.net. root.jnds.net. (
0 ; serial
1D ; refresh
1H ; retry
1W ; expire
3H) ; minimum
@ IN NS dns.
109 IN PTR www.
120 IN PTR bbs.
102 IN PTR mail.
106 IN PTR ftp.
"10.1.5.250.zone" 12L, 209C

2、配置 FTP 服务，创设 FTP 服务站点，域名为 ftp.jnds.net，站点主目录分别为 /var/ftp1，登录后显示 banner 文字说明为“欢迎使用本 ftp 服务器”，开启 ASCII 模式上传数据；

```
 13 #
 14 # Uncomment this to allow loc
 15 local_enable=YES
 16 local_root=/var/ftp1
 17 #
 18 # Uncomment this to enable an
```

```
 81 # ASCII mangling is a horrible feature of the protocol.
 82 ascii_upload_enable=YES
 83 #ascii_download_enable=YES
 84 #
 85 # You may fully customise the login banner string:
 86 ftpd_banner=Welcome to use local FTP service.
```

3、建立虚拟用户 ftpuser1 及 ftpuser2，用户的宿主目录为/home/vsftpd，实现 ftpuser1 用户具有上传和下载的权限，但不能删除文件，ftpuser2 用户可以下载，但不能上传和对文件进行改名；

```
# You may activate the "-R" option to the builtin ls. This is disabled by
# default to avoid remote users being able to cause excessive I/O on large
# sites. However, some broken FTP clients such as "ncftp" and "mirror" assume
# the presence of the "-R" option, so there is a strong case for enabling it.
#ls_recurse_enable=YES
#
# When "listen" directive is enabled, vsftpd runs in standalone mode and
# listens on IPv4 sockets. This directive cannot be used in conjunction
# with the listen_ipv6 directive.
listen=YES
#
# This directive enables listening on IPv6 sockets. To listen on IPv4 and IPv6
# sockets, you must run two copies of vsftpd with two configuration files.
# Make sure, that one of the listen options is commented !!
#listen_ipv6=YES

pam_service_name=vsftpd
userlist_enable=YES
tcp_wrappers=YES
guest_enable=YES
guest_username=ftp
user_config_dir=/etc/vsftpd/vuser_conf
```

```
[root@localhost vsftpd]# db_load -T -t hash -f vuser vuser.db
[root@localhost vsftpd]# cat vuser
ftpuser1
ftpuser1
ftpuser2
ftpuser2
[root@localhost vsftpd]# _
```

```
[root@localhost vuser_conf]# cat ftpuser1
local_root=/home/vsftpd
anon_upload_enable=YES
anon_world_readable_only=YES
anon_other_write_enable=YES
[root@localhost vuser_conf]# cat ftpuser2
local_root=/home/vsftpd
anon_upload_enable=NO
anon_world_readable_only=YES
anon_other_write_enable=NO
[root@localhost vuser_conf]# _
```

四、在 PC 4 上完成如下操作：

（一）完成物理主机的创建

1、PC 4 主机系统为 CentOS6.5，需要在此 Linux 平台上采用 KVM 方式安装虚拟机“Centos-D1”，具体要求为硬盘大小为 12GB，内存为 768MB，系统为 CentOs6.5；（小提示：如无法正确安装虚拟机 Centos-D1，下述题目中所涉及的虚拟机题目可在 Server4 真实主机中完成）

2、完成 SNMP 的配置，只读字串为 public，读写字串为 private；

3、开启系统防火墙，只对该系统服务的端口进行监听，截图为 4-1；

```
[root@localhost etc]# service iptables status
Table: filter
Chain INPUT (policy DROP)
num  target     prot opt source               destination
1    ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp dpt:161
2    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:161

Chain FORWARD (policy DROP)
num  target     prot opt source               destination

Chain OUTPUT (policy DROP)
num  target     prot opt source               destination
1    ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp spt:161
2    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp spt:161
```

（二）在主机 CentOS-D1 中完成 MySQL 数据库服务器的部署

1、采用 MySQL 数据库作为认证来源，创建用户认证数据库为 www，建立保存用户名及密码的表名为 users，建立 web1 以及 web2 两个用户，将其密码均设置为 2015，并对密码采用 password 函数加密，完成后使用适当命令对表结构进行截图，名称为 db1，表结构如下；

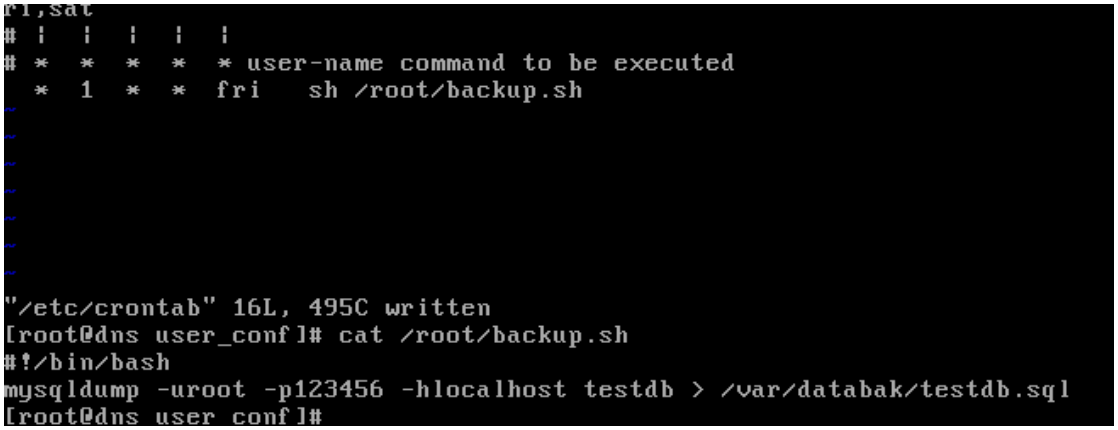
字段名	数据类型	主键	自增
Sno	int	是	是
Sname	varchar(10)	否	否
Ssex	char(1)	否	否

```
mysql> create database www;
Query OK, 1 row affected (0.00 sec)

mysql> use www
Database changed
mysql> create table users(
    -> Sno int primary key auto_increment,
    -> Sname varchar(10),
    -> Ssex char(1));
Query OK, 0 rows affected (0.05 sec)
```

```
mysql> desc users;
+-------+-------------+------+-----+---------+----------------+
| Field | Type        | Null | Key | Default | Extra          |
+-------+-------------+------+-----+---------+----------------+
| Sno   | int(11)     | NO   | PRI | NULL    | auto_increment |
| Sname | varchar(10) | YES  |     | NULL    |                |
| Ssex  | char(1)     | YES  |     | NULL    |                |
+-------+-------------+------+-----+---------+----------------+
3 rows in set (0.00 sec)
```

```
mysql> insert into users(Sname,Ssex)value("web1",password("2015"));
Query OK, 1 row affected, 1 warning (0.00 sec)

mysql> insert into users(Sname,Ssex)value("web2",password("2015"));
Query OK, 1 row affected, 1 warning (0.00 sec)

mysql> select * from users;
+-----+-------+------+
| Sno | Sname | Ssex |
+-----+-------+------+
|   1 | web1  | *    |
|   2 | web2  | *    |
+-----+-------+------+
2 rows in set (0.00 sec)
```

2.每周五凌晨 1：00 备份数据库 testdb 到/var/databak/testdb.sql。[定期备份设置截屏截屏保存为 db2]。


fri,sat
| | | | |
* * * * * user-name command to be executed
* 1 * * fri sh /root/backup.sh
"/etc/crontab" 16L, 495C written
[root@dns user_conf]# cat /root/backup.sh
#!/bin/bash
mysqldump -uroot -p123456 -hlocalhost testdb > /var/databak/testdb.sql
[root@dns user_conf]#

2015 年全国职业院校技能大赛

网络搭建与应用竞赛

(总分 1000 分)

赛题说明

一、竞赛内容分布

“网络搭建与应用”竞赛共分二个部分，其中：

第一部分：网络搭建及安全部署项目，占总分的比例为 45%；

第二部分：服务器配置及应用项目，占总分的比例为 55%；

二、竞赛注意事项

（1）禁止携带和使用移动存储设备、计算器、通信工具及参考资料。

（2）请根据大赛所提供的比赛环境，检查所列的硬件设备、软件清单、材料清单是否齐全，计算机设备是否能正常使用。

（3）本试卷共有两个部分。请选手仔细阅读比赛试卷，按照试卷要求完成各项操作。

（4）操作过程中，需要及时保存设备配置。比赛结束后，所有设备保持运行状态，不要拆、动硬件连接。

（5）比赛完成后，比赛设备、软件和赛题请保留在座位上，禁止将比赛所用的所有物品（包括试卷和草纸）带离赛场。

（6）所有需要提交的文档均放置在桌面的 SERVER1“比赛文档”文件夹中，禁止在纸质资料上填写与竞赛无关的标记，如违反规定，可视为 0 分。

（7）裁判以各参赛队提交的竞赛结果文档为主要评分依据。所有提交的文档必须按照赛题所规定的命名规则命名，文档中有对应题目的小标题，截图有截图的简要说明，否则按无效内容处理。

（8）与比赛相关的工具软件放置在 D 盘的 tools 文件夹中。

项目背景及网络拓扑

你是 xx 公司网络管理员，从公司建立初期便就职于该公司，见证了公司从一个只有几个人的小公司走向拥有多家子公司的大型公司的成长历程。你也从一名管理员成长为网络技术部经理。现在，根据你在公司这些年的工作历程，将公司的网络从无到有搭建起来。

拓扑结构如下图所示：

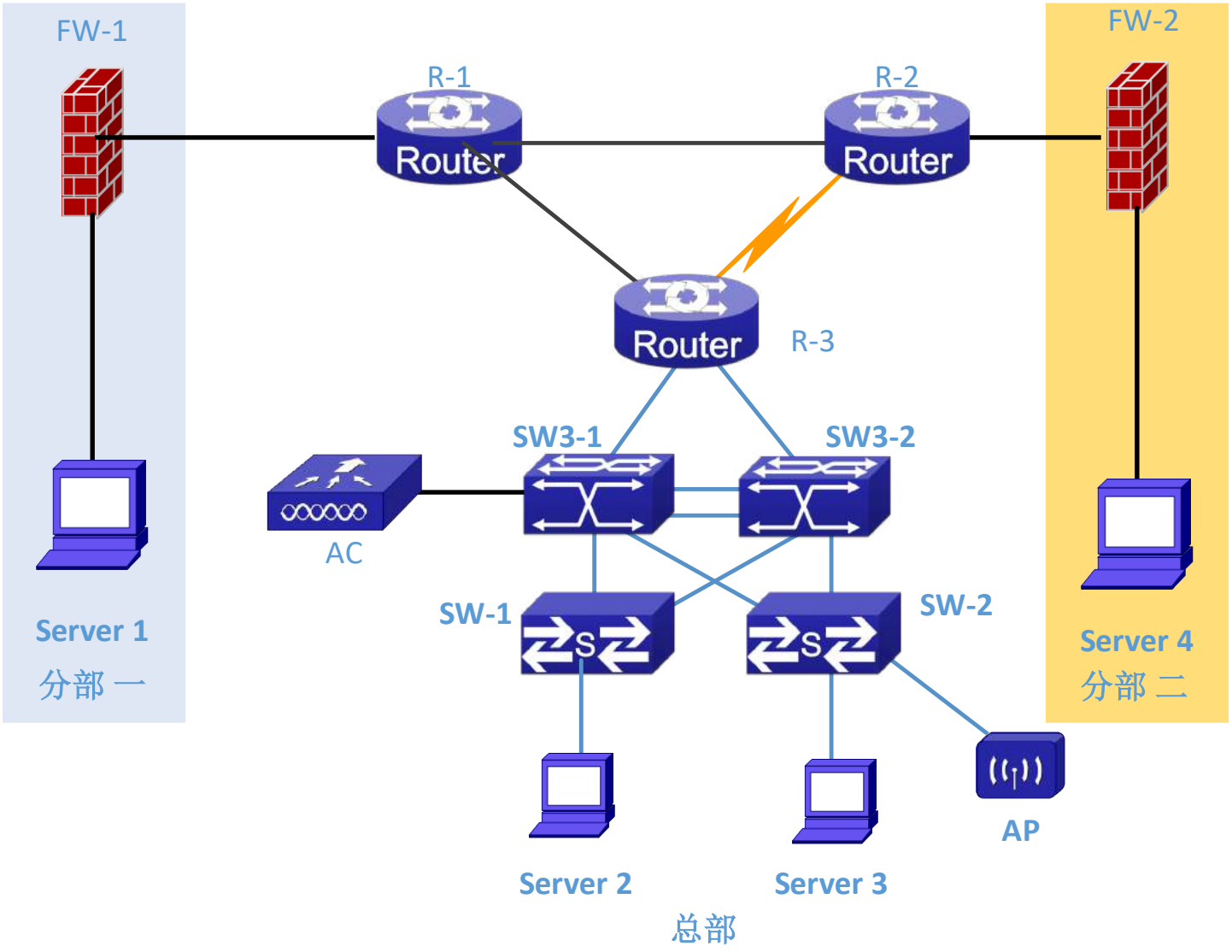

FW-1
R-1
R-2
FW-2
Router
Router
Router
R-3
SW3-1
SW3-2
AC
SW-1
SW-2
Server 1
分部 一
Server 4
分部 二
AP
Server 2
Server 3
总部

表 1 网络设备连接表

A 设备连接至 B 设备			
设备名称	**接口**	**设备名称**	**接口**
R-1	G 0/3	FW-1	E 0/3
R-1	G 0/4	R-2	G 0/4
R-1	G 0/5	R-3	G 0/5
R-2	G 0/3	FW-2	E0/3
R-2	S 0/1	R-3	S 0/2
R-3	G 0/4	SW3-2	E 1/0/20
R-3	G 0/3	SW3-1	E 1/0/20
SW3-1	E 1/0/17	AC	E 1/0/24
SW3-1	E 1/0/21-24	SW3-2	E 1/0/21-24
SW3-1	E 1/0/18	SW-2	E 1/24
SW3-1	E 1/0/19	SW-1	E 1/23
SW3-2	E 1/0/18	SW-2	E 1/23
SW3-2	E 1/0/19	SW-1	E 1/24
SW-2	E1/2	AP	Lan
SERVER1	NIC	FW-1	Eth 0/4
SERVER2	NIC	SW-1	E 1/1
SERVER3	NIC	SW-2	E 1/1
SERVER4	NIC	FW-2	Eth0/4

表 2 网络设备 IP 地址分配表

设备	设备名称	设备接口	IP 地址
路由器	R-1	G 0/3	202.100.1.14/28
		G 0/4	100.10.1.1/30
		G 0/5	135.20.1.1/30
	R-2	G 0/3	202.110.1.14/28
		G 0/4	100.10.1.2/30
		S 0/1	50.1.1.1/30
	R-3	G 0/3	10.0.0.1/30
		G 0/4	10.0.0.5/30
		G 0/5	135.20.1.2/30
		S 0/1	50.1.1.2/30
三层交换机	SW3-1	VLAN200 (E 1/0/20)	
		VLAN150 (E 1/0/17)	
		VLAN100	
		VLAN10 SVI	
		VLAN20 SVI	
		VLAN30 SVI	
		VLAN40 SVI	
	SW3-2	VLAN210 (E 1/0/20)	
		VLAN150	
		VLAN100	
		VLAN10 SVI	
		VLAN20 SVI	
		VLAN30 SVI	
		VLAN40 SVI	
防火墙 1	FW-1	Eth 0/3	202.100.1.1/28
		Eth 0/4	10.100.1.1/24
防火墙 2	FW-2	Eth 0/3	202.110.1.1/28
		Eth 0/4	10.101.1.1/24
无线控制器	AC	Vlan150 (E 1/0/24)	
		Vlan5	
		Vlan15	

表 3：服务器 IP 地址分配表

宿主机	虚拟主机名称	域名信息	服务角色	系统及版本信息	IPv4地址信息
Server 1	Win2003-A1	DC1.2015Network.com	域控制器 DNS 服务器	Windows Server 2003 R2	IP:10.100.1.101
	Win2008-A1	vpn1.2015Network.com	VPN	Windows Server 2008 R2	IP:10.100.1.102
	Centos-A1	smb.jnds.net	SAMBA 共享服务器	Centos 6.5	IP:10.100.1.103
Server 2	Win2008-B1	www.2015Network.com vpn2.2015Network.com	WWW 服务器 VPN	Windows Server 2008 R2	IP:10.1.100.101
	Centos-B1	raid.jnds.net	逻辑卷及磁盘阵列服务	Centos 6.5	IP:10.1.100.102
	Centos-B2	dhcp.jnds.net	DHCP 服务器	Centos 6.5	IP:10.1.100.103
Server 3	Win2003-C1	bdns.2015Network.com	备份 DNS	Windows Server 2003 R2	IP:10.1.101.101
	Centos-C1	dns.jnds.net	BIND 域名服务器 Squid 代理服务器	Centos 6.5	IP:10.1.101.102
	Centos-C2	www.jnds.net www.lab.jnds.net	Apache web 服务器	Centos 6.5	IP:10.1.101.103
Server 4 (Linux 虚拟化主机)	Centos-D1	chinaskill.jnds.net mysql.jnds.net	Apache web 服务器 MySQL 数据库服务器	Centos 6.5	IP:10.101.1.101

网络搭建部分(450 分)

【注意事项】

1、设备 console 线有两条。交换机， AC，防火墙使用同一条 console 线，路由器使用另外一条 console 线。

2、设备配置完毕后，保存最新的设备配置。保存文档方式分为两种：

a) 交换机和路由器要把 show running-config 的配置保存在 SERVER1 桌面的相应文档中，文档命名规则为：设备名称.doc,例如：RT1 路由器文件命名为：RT1.doc，然后放入到 SERVER1 桌面上“比赛文档”文件夹中。

b) 防火墙等截图方式的设备，把截图的图片放到同一 word 文档中，文档命名规则为：设备名称.doc,例如：防火墙 FW1 文件命名为：FW1.doc，保存后放入到 SERVER1 桌面上“比赛文档”文件夹中。

1、 物理连接与 IP 地址划分

(1) 按照网络拓扑图制作以太网网线，并连接设备。要求符合 T568A 和 T568B 的标准，其线缆长度适中。

(2) 根据“拓扑结构图”和“表 2:网络设备 IP 地址分配表”所示，对网络中的所有设备接口配置 IP 地址。

公司中整个网络互联地址规划使用 10.0.0.0/8 地址段，为了节省 IP 资源，做到合理分配，财务部(VLAN10)有 30 名员工、工程部(VLAN20)有 40 名员工、软件部(VLAN30)和系统集成部(VLAN40)两个部门都有 10 名员工。SERVER2 与 SERVER3 服务器的 IP 段为 10.1.100.0/24 和 10.1.101.0/24，所有设备互联地址使用/30 的掩码进行分配，并把地址填入上面网络设备 IP 地址分配表中的空白处。地址分配后把地址填入上面网络设备 IP 地址分配表中的空白处。

注意:

- 网关地址为网段的最后可用地址。

2、 交换机配置

(1) 为交换机设备命名，命名规则参考为表 1 中的“设备名称”。

(2) 在两台三层交换设备上开启 telnet 管理功能，同时要求每台网络设备只允许 6 条线路管理网络设备,管理设备使用 telnet 作为用户名,口令为 telnet，enable 密码为 2015network，enable 密码的加密方式为密文加密。

(3) 依据“拓扑结构图”和下表，把相应端口加入到 vlan 中;

设备	VLAN 名称	VLAN ID	接口
SW3-1	CAIWUBU	10	————
	GONGCHENGBU	20	————
	RUANJIANBU	30	————
	XITONGJICHENGBU	40	————
	Link_to_SW-1	Trunk	E 1/0/18
	Link_to_SW-2	Trunk	E 1/0/19

	Link_to_SW3-2	Trunk	E1/0/21-E1/0/24
SW3-2	CAIWUBU	10	————
	GONGCHENGBU	20	————
	RUANJIANBU	30	————
	XITONGJICHENGBU	40	————
	Link_to_SW-1	Trunk	E 1/0/18
	Link_to_SW-2	Trunk	E 1/0/19
	Link_to_SW3-1	Trunk	E1/0/21-E1/0/24
SW-1	Link_to_SW3-1	Trunk	E 1/23
	Link_to_SW3-2	Trunk	E 1/24
	Server	100	E 1/1
SW-2	Link_to_SW3-1	Trunk	E 1/24
	Link_to_SW3-2	Trunk	E 1/23
	Server	100	E 1/1
	Link_to_AP	150	E 1/2

(4) 使用端口汇聚技术，将 SW3-1 三层交换机接口 ethernet 1/0/21 到 ethernet 1/0/24 与 SW3-2 二层交换机接口 Ethernet1/0/21 到 Ethernet1/0/24 配置为端口汇聚，汇聚接口为静态方式，负载分担方式基于源-目地 IP。

(5) 公司为了统一管理，通过 SNMP 技术使用网管软件对交换机进行管理，配置只读字串为 public ，读写字串为 private，网管主机的地址为 10.100.100.10。

(6) SW3-1 和 SW3-2 上运行 VRRP 协议，针对 VLAN10、20、30、40、100、150 进行冗余备份，虚拟网关地址使用本网段最后一个可用地址，SW3-2 使用倒数第 2 个可用地址，SW3-1 使用倒数第 3 个可用地址；SW3-2 的优先级为 110。

(7) SW3-1、SW3-2、SW-1 和 SW-2 组成的冗余环境中启用多实例生成树来防止网络中的物理环路，SW3-2 做为根桥，SW3-1 做为备份根。

3、 路由器配置与调试

(1) 为路由设备命名，命名规则参考为表 1 中的“设备名称”。

(2) 配置动态路由协议，将设备接口分配到不同的区域中。R-1 到 FW-1，R-2 到 FW-2 配置 RIPv2 路由协议；R-3、SW3-1、SW3-2 之间配置 RIPv2 路由协议，R-3 到 R-2 和 R-3 到 R-1 间配置 OSPF 路由协议。

(3) 把下面的设备 RID 设置上，要求不能增加接口的相关信息。

设备名称	RID
R-1	1.1.1.1
R-2	2.2.2.2
R-3	3.3.3.3

(4) R-2 的 S0/1 接口配置为被动接口，不发送路由更新消息。

(5) R-2 不参与 R-1/R-2/R-3 之间 DR 与 BDR 之间的选举。

(6) 在 R-3 上使用 QOS 进行流量整形 ，使其到 R-2 的 CIR 为 40000 ，Excess Burst size 为 9000 ，Burst size 为 8000 ，超额的流量不需要做处理。

4、 广域网配置

(1) FW-1 和 FW-2 允许内部服务器访问总部网络，为保证安全性进行地址转换工作，类型为端口 NAT，使用外网口 IP 地址进行映射。

(2) R-2 与 R-3 之间并采用 PPP 封装，PAP 认证方式，用户名称为对端设备名称，密码：123456。

5、 无线配置

(1) 把无线控制器进行设备命名，命名规则参考为表 1 中的“设备名称”。

(2) 无线控制器建立 2 个 SSID，SSID 分别为 ssid1 和 ssid2，ssid1 的 SSID 设置为隐藏，工作信道为 6；使用无线控制器提供 DHCP 服务，获得 ssid1 的地址在 vlan5 内，获得 ssid2 的地址在 vlan15 内，为用户动态分配 IP 地址和网关，DNS 地址为：8.8.8.8，其分配的地址段为自行计算，需要排除网关，地址租约为 3 天。

(3) 保障无线信息的覆盖性，无线 AP 的发射功率设置为 90%。

(4) 为了控制带宽，保证正常使用，配置无线局域网用户上行速度为 3Mbps，下行速度为 4Mbps。

6、 防火墙配置

(1) 把防火墙进行设备命名，命名规则参考为表 1 中的“设备名称”。

(2) FW-1 禁止访问 www.jd.com。

(3) FW-2 为了保证带宽的正常使用，限制 P2P 应用的下行带宽最高为 10M。

(4) FW-1 阻止用户访问网页内容中含有“暴力”相关内容的网站。

(5) FW-2 限制分部二的用户，仅在办公时间以外的时间（办公时间：周一到周五，9:00-18:00）访问外网。

7、 网络配置优化

(1) 交换机设备中增加 SSH 方式管理的需求，使用 SSH 用户名为 SwitchSSH，密码为 PassWD1QAz（注意密码大小写），同时限制 Telnet 的登录用户仅有 192.168.1.10 的 IP 可以管理交换机设备。

(2) R-3、SW3-1、SW3-2 之间的 RIP 协议修改路由更新时间为 15s，以便加快路由更新的速度。

(3) 关闭交换机设备的 Web 网管功能，防止用户通过 Http 方式登录到交换机设备。

(4) 修改 SW3-1、SW3-2 的 VRRP 报文交互时间，按照 2s/5s/7s 的周期依次修改每个 VRRP 组的交互时间，避免同一时间设备处理过多的 VRRP 报文消息。

(5) SW-1 和 SW-2 上，将不需要进行生成树运算的端口配置为 Portfast 模式，减少由于设备端口 UP/Down 对生成树环境的干扰，加快 PC 机接入网络的速度。

8、 VPN 技术应用

(1) FW-1 和 FW-2 之间，配置 IPsecVPN 以便确保数据在传输过程中处于加密状态。

9、 无线网络安全

(1) 通过 AC 的设置，用户接入无线网络时需要输入密码，加密模式为 wpa2-personal，其口令为：chinaskill。

(2) 激活无线网络的二层隔离，实现同一个 AP 下无线局域网内用户不能互相访问。

Windows 操作系统

【说 明】

（1）题目中所涉及 Windows 操作系统的 administrator 管理员以及其他普通用户密码均为 2015Netw1rk（注意区分大小写），若未按照要求设置密码，涉及到该操作的所有分值记为 0 分。

（2）虚拟主机的 IP 属性设置请按照网络拓扑结构图以及“表 3：服务器 IP 地址分配表”的要求设定。

（3）除非作特殊说明，在同一主机下需要安装相同操作系统版本的虚拟机时，可采用 Oracle VM VirtualBox 软件自带的克隆系统功能实现。

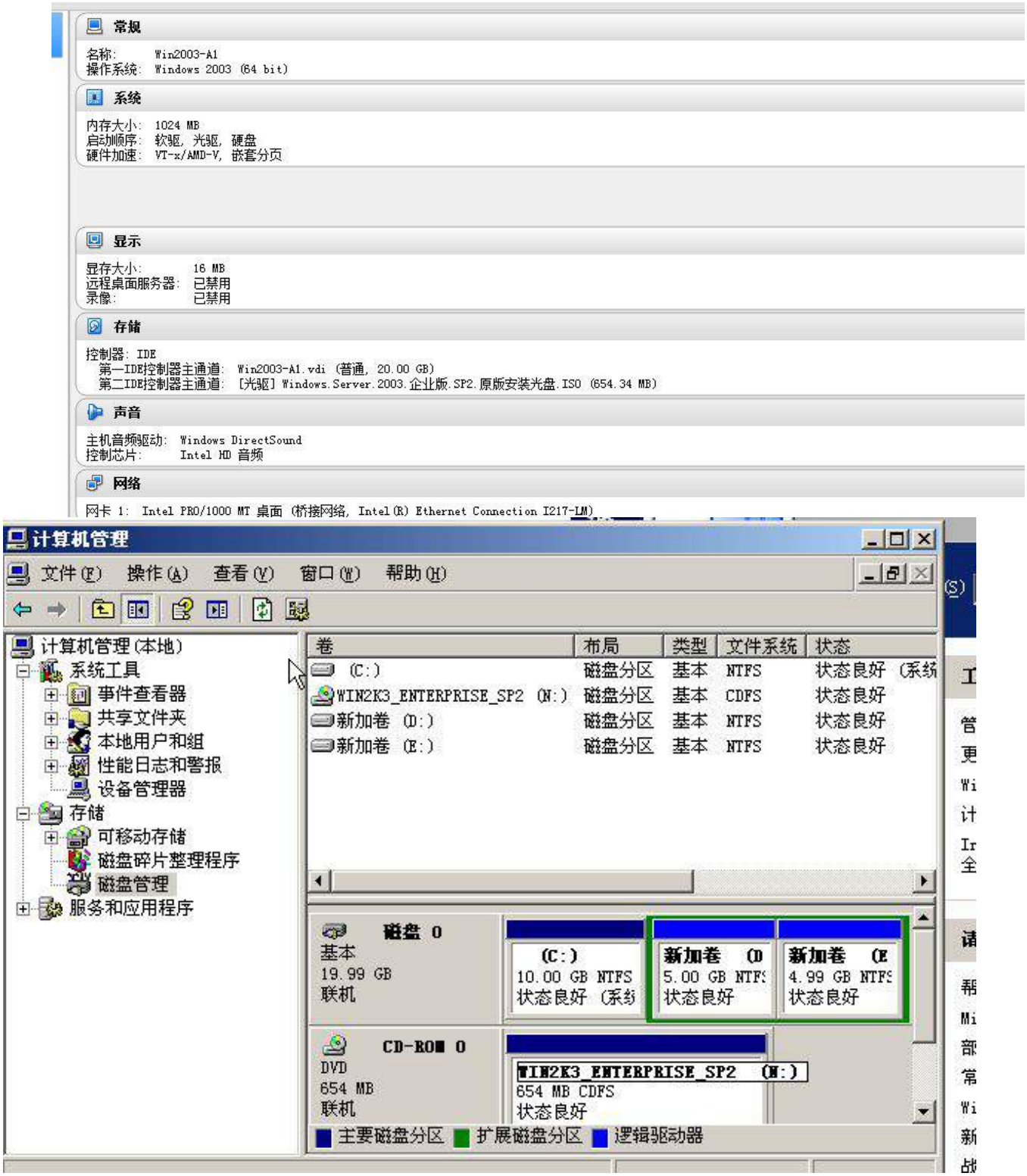
（4）所有系统镜像文件及试题所需的其它软件均存放在每台主机的 D:\soft 文件夹中，并将题目要求的截图内容以.jpg 格式存储于桌面 BACKUP 文件夹中。

（5）题目要求的虚拟机均安装于每台主机的 D：\virtualPC 目录，即路径为 D：\virtualPC\虚拟主机名称。

一、在 Server 1 上完成如下操作:

（一）完成虚拟主机的创建

1、安装虚拟机“Win2003-A1”，具体要求为内存为 1G，硬盘 20G,网卡为桥接模式；虚拟机分区分别为 C、D、E；主分区一个，容量 10G；扩展分区为 10G，两个逻辑分区分别为 5G。



2、在虚拟机“Win2003-A1”中添加 SCSI 控制器，再添加三块 SCSI 虚拟硬盘，其每块硬盘的大小为 5G；制作成一个 RAID-5 卷，磁盘盘符为 F:\。

名称: Win2003-A1
操作系统: Windows 2003 (64 bit)

系统

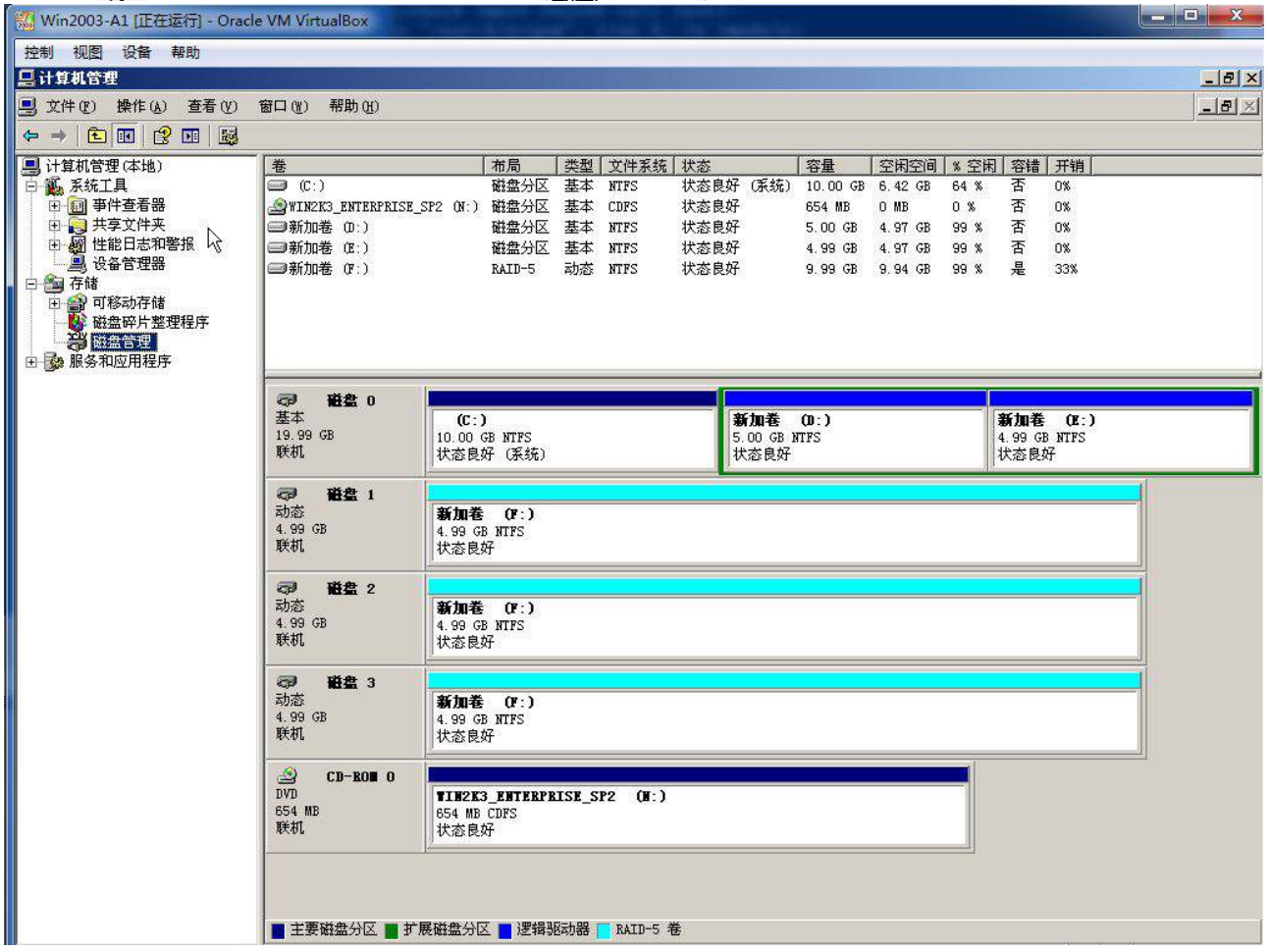
内存大小: 1024 MB
启动顺序: 软驱, 光驱, 硬盘
硬件加速: VT-x/AMD-V, 嵌套分页

显示

显存大小: 16 MB
远程桌面服务器: 已禁用
录像: 已禁用

存储

控制器: IDE
第一IDE控制器主通道: Win2003-A1.vdi (普通, 20.00 GB)
第二IDE控制器主通道: [光驱] Windows.Server.2003.企业版.SP2.原版安装光盘.ISO (654.3 MB)
控制器: SCSI
SCSI 端口 0: NewVirtualDisk1.vdi (普通, 5.00 GB)
SCSI 端口 1: NewVirtualDisk2.vdi (普通, 5.00 GB)
SCSI 端口 2: NewVirtualDisk3.vdi (普通, 5.00 GB)

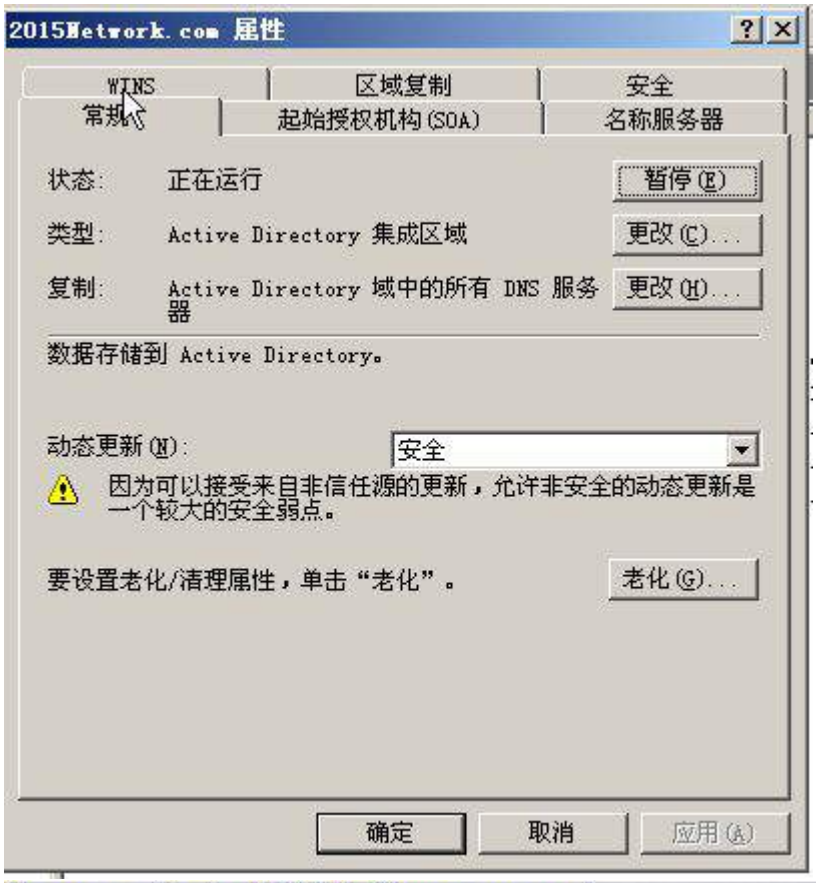


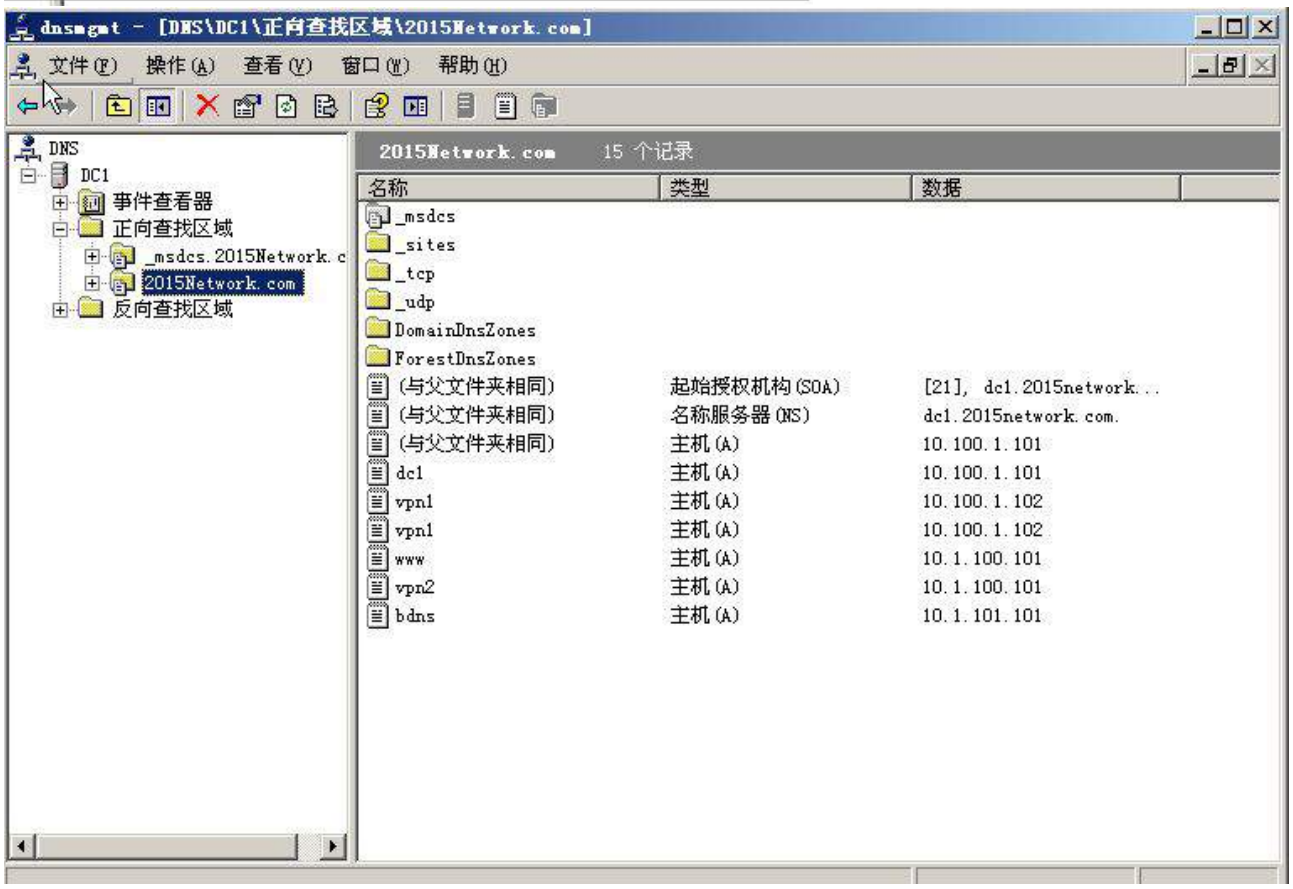
3、安装虚拟机“Win2008-A1”，具体要求为内存为 1G，硬盘 20G，并将该虚拟机加入到域中。

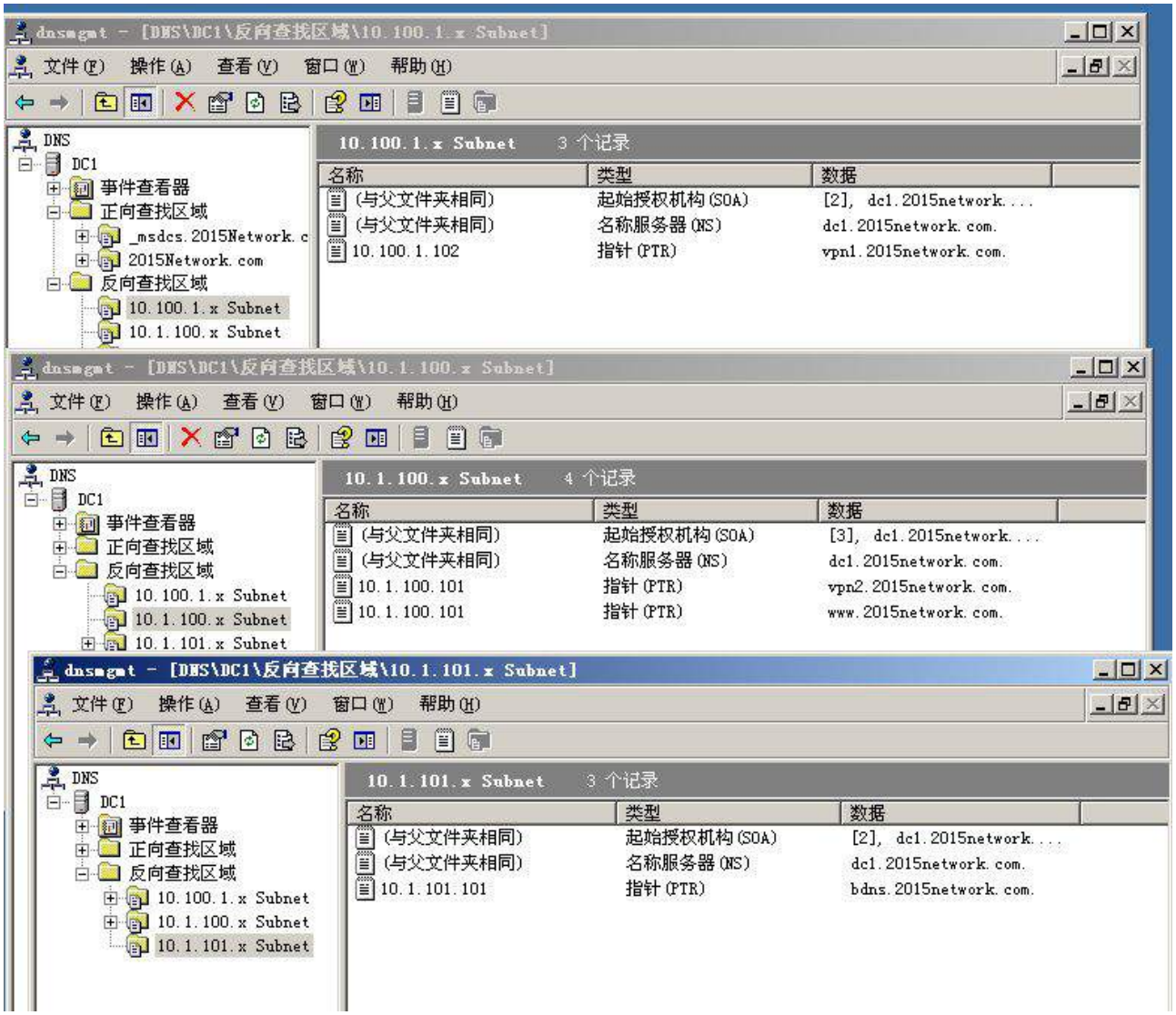
（二）在主机 Win2003-A1 中完成域控制器的部署

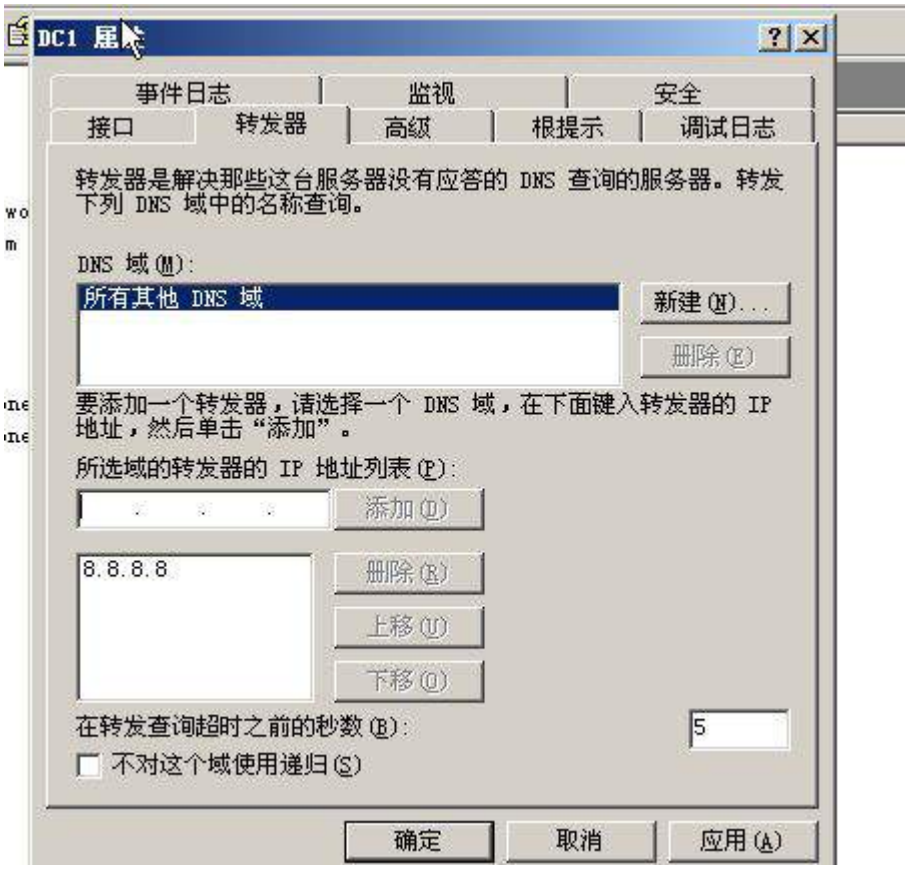
1、将虚拟机“Win2003-A1” 配置为主域控制器，并安装配置 CA 证书服务，配置为企业根。

2、将此服务器配置为主 DNS 服务器，正确配置 2015Network.com 域名的正向区域与 IPV4 反向区域，能够正确解析网络中的所有服务器，当遇到无法解析的域名时，将其请求转发至 8.8.8.8 互联网域名服务器。


2015Network.com 属性
WINS
区域复制
安全
常规
起始授权机构(SOA)
名称服务器
状态: 正在运行
暂停(P)
类型: Active Directory 集成区域
更改(C)...
复制: Active Directory 域中的所有 DNS 服务器
更改(H)...
数据存储到 Active Directory。
动态更新(N): 安全
因为可以接受来自非信任源的更新，允许非安全的动态更新是一个较大的安全弱点。
要设置老化/清理属性，单击“老化”。
老化(G)...
确定
取消
应用(A)

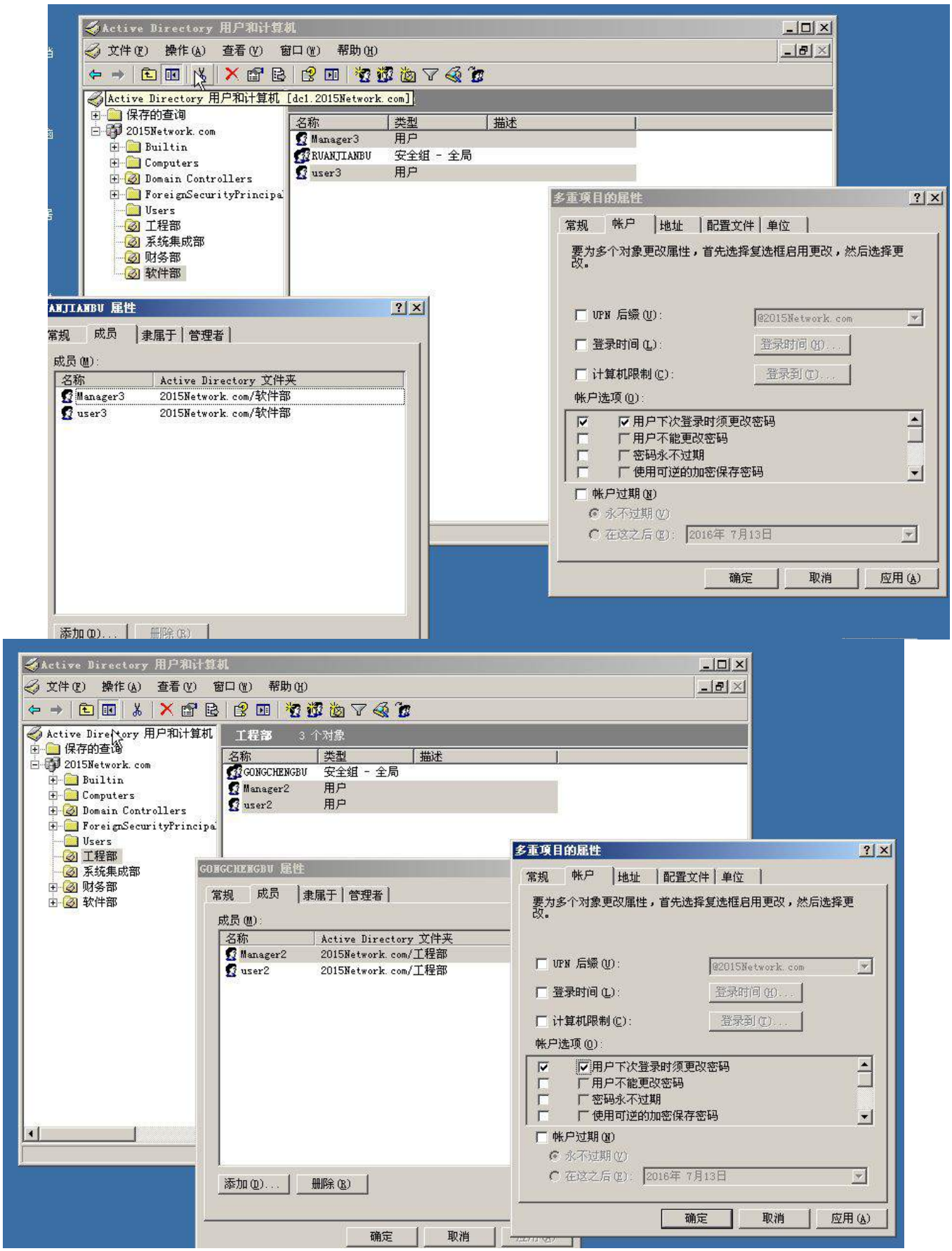

dnsmgmt - [DNS\DC1\正向查找区域\2015Network.com]
文件(F) 操作(A) 查看(V) 窗口(W) 帮助(H)
DNS
DC1
事件查看器
正向查找区域
_msdcs.2015Network.c
2015Network.com
反向查找区域
2015Network.com 15 个记录
名称 类型 数据
_msdcs
_sites
_tcp
_udp
DomainDnsZones
ForestDnsZones
(与父文件夹相同) 起始授权机构(SOA) [21], dc1.2015network...
(与父文件夹相同) 名称服务器(NS) dc1.2015network.com.
(与父文件夹相同) 主机(A) 10.100.1.101
dc1 主机(A) 10.100.1.101
vpn1 主机(A) 10.100.1.102
vpn1 主机(A) 10.100.1.102
www 主机(A) 10.1.100.101
vpn2 主机(A) 10.1.100.101
bdns 主机(A) 10.1.101.101

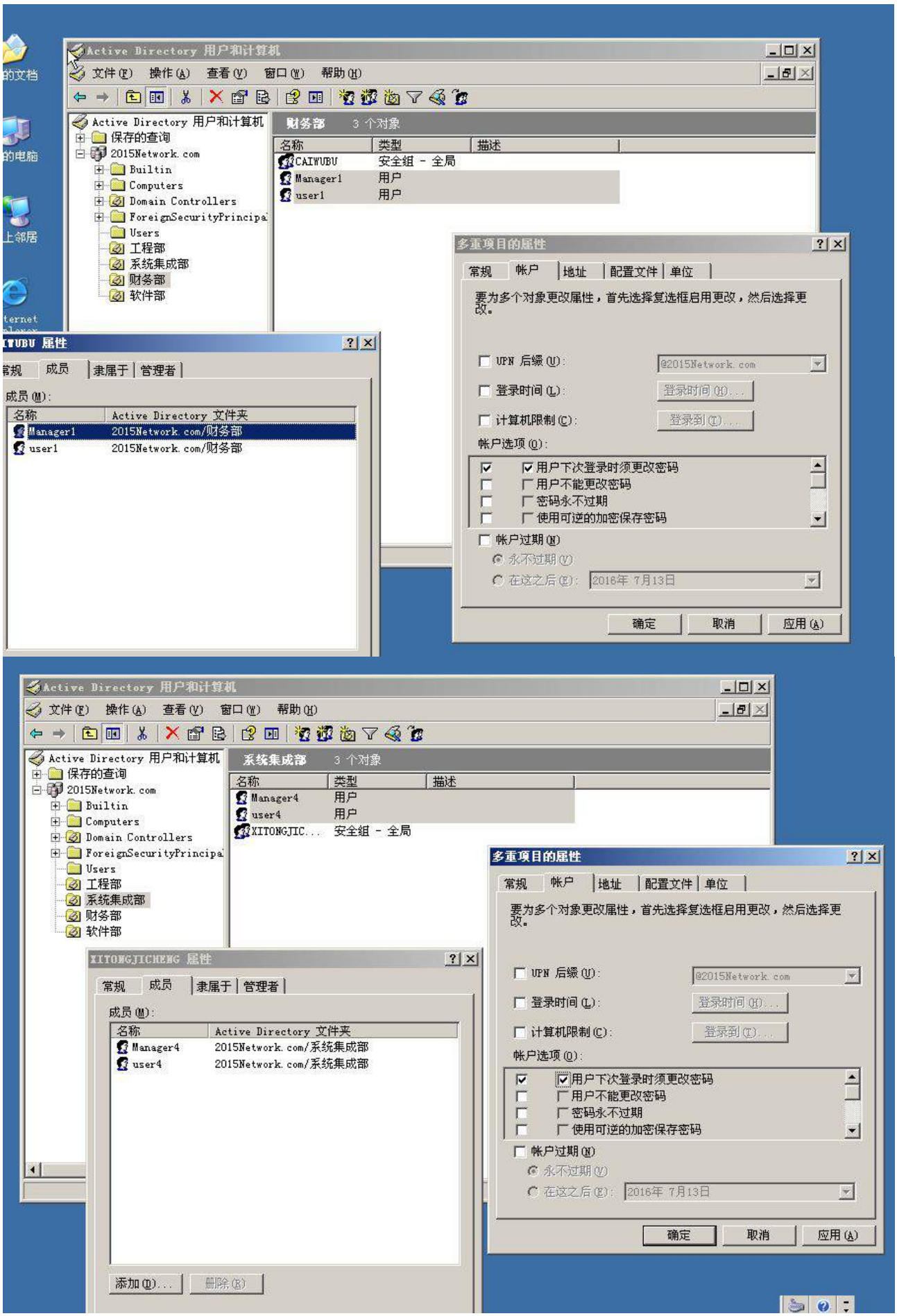

dnsmgmt - [DNS\DC1\反向查找区域\10.100.1.x Subnet]
文件(F) 操作(A) 查看(V) 窗口(W) 帮助(H)
DNS
DC1
事件查看器
正向查找区域
_msdcs.2015Network.c
2015Network.com
反向查找区域
10.100.1.x Subnet
10.1.100.x Subnet
10.100.1.x Subnet 3 个记录
名称 类型 数据
(与父文件夹相同) 起始授权机构(SOA) [2], dc1.2015network....
(与父文件夹相同) 名称服务器(NS) dc1.2015network.com.
10.100.1.102 指针(PTR) vpn1.2015network.com.
dnsmgmt - [DNS\DC1\反向查找区域\10.1.100.x Subnet]
文件(F) 操作(A) 查看(V) 窗口(W) 帮助(H)
DNS
DC1
事件查看器
正向查找区域
反向查找区域
10.100.1.x Subnet
10.1.100.x Subnet
10.1.101.x Subnet
10.1.100.x Subnet 4 个记录
名称 类型 数据
(与父文件夹相同) 起始授权机构(SOA) [3], dc1.2015network....
(与父文件夹相同) 名称服务器(NS) dc1.2015network.com.
10.1.100.101 指针(PTR) vpn2.2015network.com.
10.1.100.101 指针(PTR) www.2015network.com.
dnsmgmt - [DNS\DC1\反向查找区域\10.1.101.x Subnet]
文件(F) 操作(A) 查看(V) 窗口(W) 帮助(H)
DNS
DC1
事件查看器
正向查找区域
反向查找区域
10.100.1.x Subnet
10.1.100.x Subnet
10.1.101.x Subnet
10.1.101.x Subnet 3 个记录
名称 类型 数据
(与父文件夹相同) 起始授权机构(SOA) [2], dc1.2015network....
(与父文件夹相同) 名称服务器(NS) dc1.2015network.com.
10.1.101.101 指针(PTR) bdns.2015network.com.



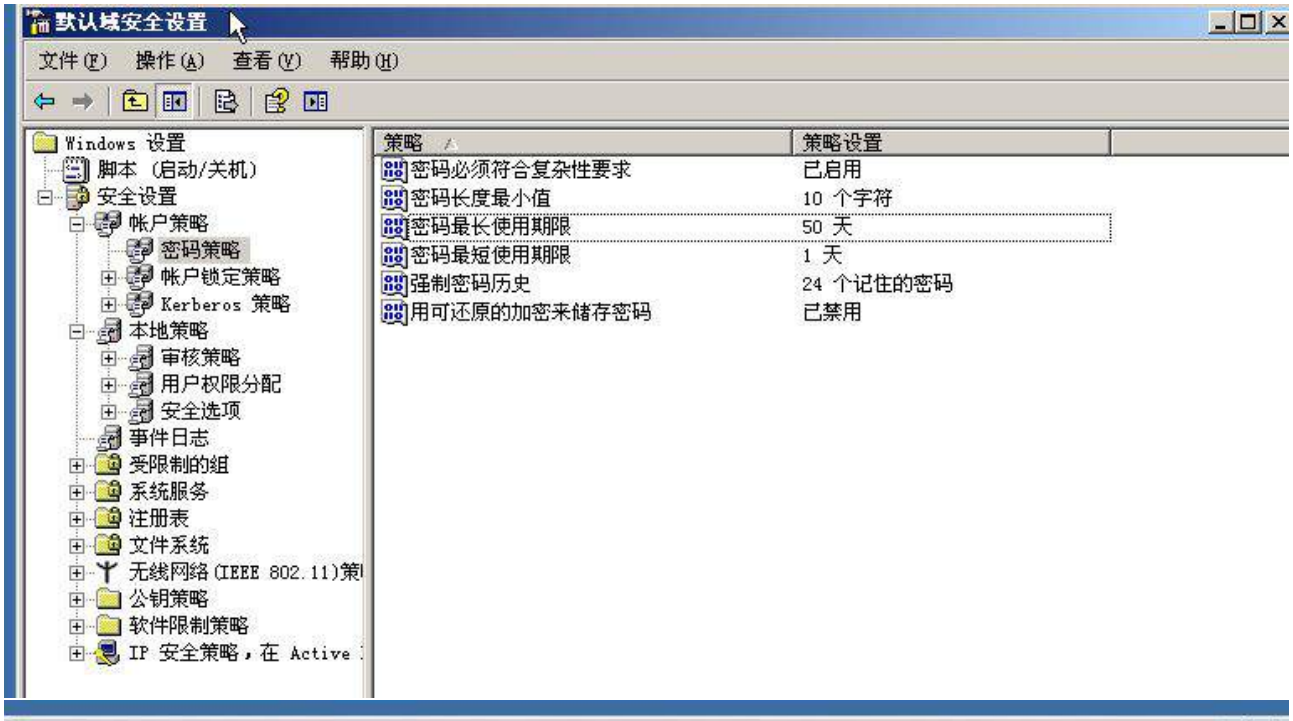
3、创建 4 个 OU，创建 8 个用户，具体内容见下表：

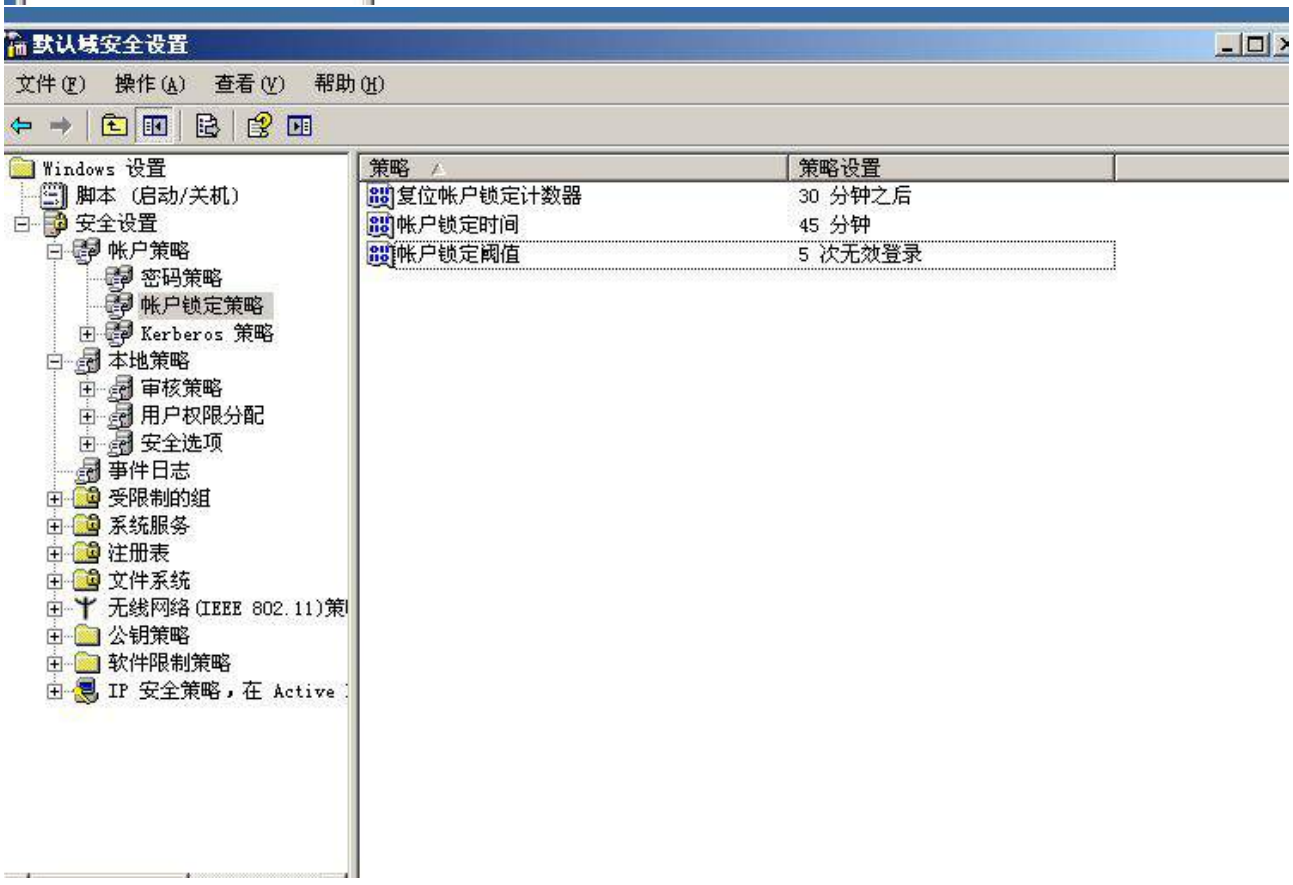
部门	组	隶属用户
财务部	CAIWUBU	Manager1（部门主任）、user1（员工）
工程部	GONGCHENGBU	Manager2（部门主任）、user2（员工）
软件部	RUANJIANBU	Manager3（部门主任）、user3（员工）
系统集成部	XITONGJICHENG	Manager4（部门主任）、user4（员工）


Active Directory 用户和计算机
文件(F) 操作(A) 查看(V) 窗口(W) 帮助(H)
Active Directory 用户和计算机 [dc1.2015Network.com]
保存的查询
2015Network.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal
Users
工程部
系统集成部
财务部
软件部
名称 类型 描述
Manager3 用户
RUANJIANBU 安全组 - 全局
user3 用户
多重项目的属性
常规 帐户 地址 配置文件 单位
要为多个对象更改属性，首先选择复选框启用更改，然后选择更改。
UPN 后缀(U):
@2015Network.com
登录时间(L):
登录时间(H)...
计算机限制(C):
登录到(T)...
帐户选项(O):
用户下次登录时须更改密码
用户不能更改密码
密码永不过期
使用可逆的加密保存密码
帐户过期(N)
永不过期(V)
在这之后(E):
2016年 7月13日
确定 取消 应用(A)
ANJIANBU 属性
常规 成员 隶属于 管理者
成员(M):
名称 Active Directory 文件夹
Manager3 2015Network.com/软件部
user3 2015Network.com/软件部
添加(D)... 删除(R)
Active Directory 用户和计算机
文件(F) 操作(A) 查看(V) 窗口(W) 帮助(H)
工程部 3 个对象
名称 类型 描述
GONGCHENGBU 安全组 - 全局
Manager2 用户
user2 用户
GONGCHENGBU 属性
常规 成员 隶属于 管理者
成员(M):
名称 Active Directory 文件夹
Manager2 2015Network.com/工程部
user2 2015Network.com/工程部
添加(D)... 删除(R)
确定 取消
多重项目的属性
常规 帐户 地址 配置文件 单位
要为多个对象更改属性，首先选择复选框启用更改，然后选择更改。
UPN 后缀(U):
@2015Network.com
登录时间(L):
登录时间(H)...
计算机限制(C):
登录到(T)...
帐户选项(O):
用户下次登录时须更改密码
用户不能更改密码
密码永不过期
使用可逆的加密保存密码
帐户过期(N)
永不过期(V)
在这之后(E):
2016年 7月13日
确定 取消 应用(A)


Active Directory 用户和计算机
文件(F) 操作(A) 查看(V) 窗口(W) 帮助(H)
Active Directory 用户和计算机
保存的查询
2015Network.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal
Users
工程部
系统集成部
财务部
软件部
财务部 3 个对象
名称 类型 描述
CAIWUBU 安全组 - 全局
Manager1 用户
user1 用户
CAIWUBU 属性
常规 成员 隶属于 管理者
成员(M):
名称 Active Directory 文件夹
Manager1 2015Network.com/财务部
user1 2015Network.com/财务部
多重项目的属性
常规 帐户 地址 配置文件 单位
要为多个对象更改属性，首先选择复选框启用更改，然后选择更改。
UPN 后缀(U):
@2015Network.com
登录时间(L):
登录时间(H)...
计算机限制(C):
登录到(T)...
帐户选项(O):
用户下次登录时须更改密码
用户不能更改密码
密码永不过期
使用可逆的加密保存密码
帐户过期(N)
永不过期(V)
在这之后(E):
2016年 7月13日
确定 取消 应用(A)
Active Directory 用户和计算机
文件(F) 操作(A) 查看(V) 窗口(W) 帮助(H)
Active Directory 用户和计算机
保存的查询
2015Network.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal
Users
工程部
系统集成部
财务部
软件部
系统集成部 3 个对象
名称 类型 描述
Manager4 用户
user4 用户
XITONGJIC... 安全组 - 全局
XITONGJICHENG 属性
常规 成员 隶属于 管理者
成员(M):
名称 Active Directory 文件夹
Manager4 2015Network.com/系统集成部
user4 2015Network.com/系统集成部
添加(D)... 删除(R)
多重项目的属性
常规 帐户 地址 配置文件 单位
要为多个对象更改属性，首先选择复选框启用更改，然后选择更改。
UPN 后缀(U):
@2015Network.com
登录时间(L):
登录时间(H)...
计算机限制(C):
登录到(T)...
帐户选项(O):
用户下次登录时须更改密码
用户不能更改密码
密码永不过期
使用可逆的加密保存密码
帐户过期(N)
永不过期(V)
在这之后(E):
2016年 7月13日
确定 取消 应用(A)

4、域用户在首次登录时需要修改口令，采用复杂密码，密码长度最小为 10 位，密码最长存留其为 30 天，帐户锁定阈值为 5 次，如果到过阈值需要锁定 45 分钟。

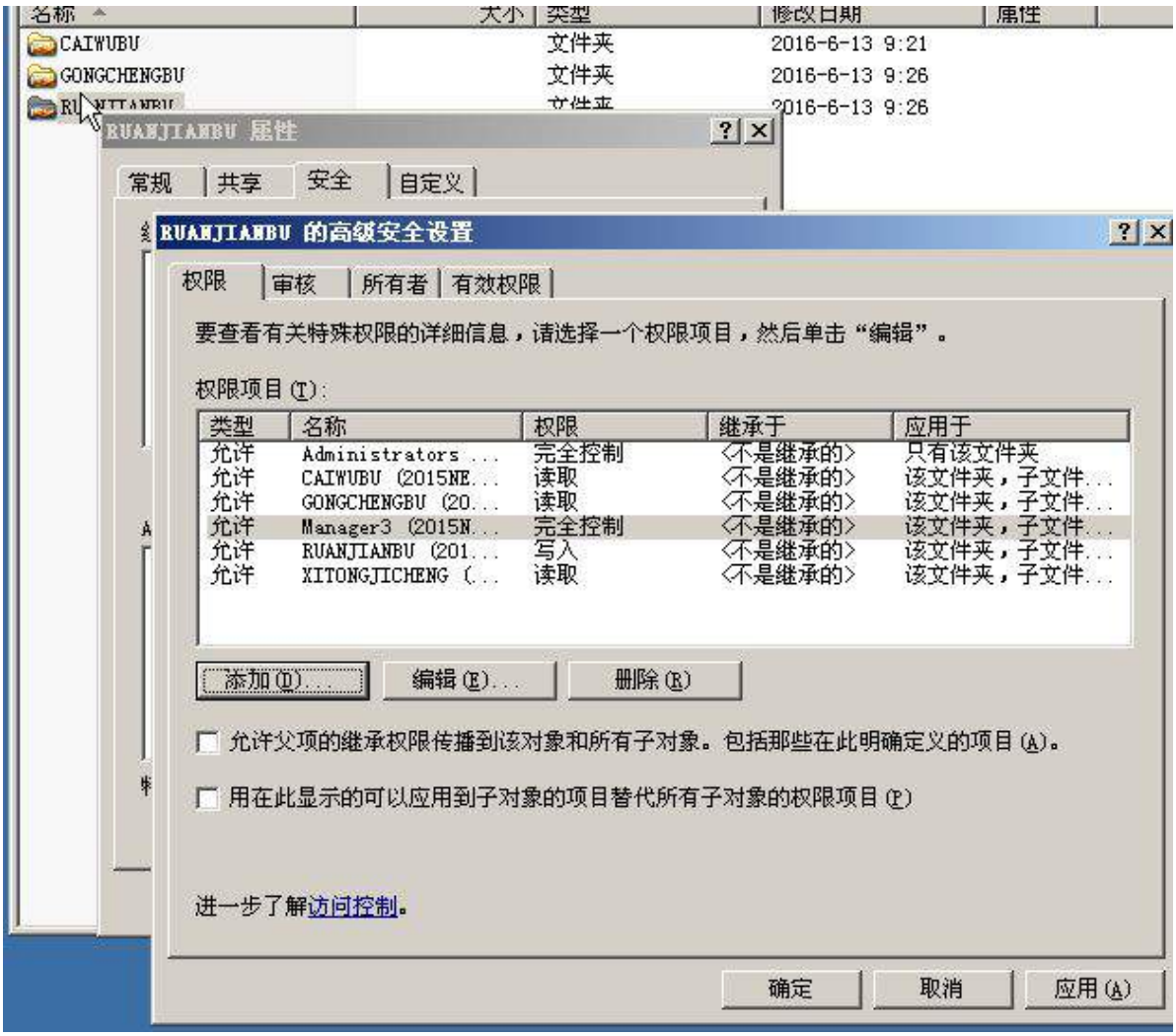


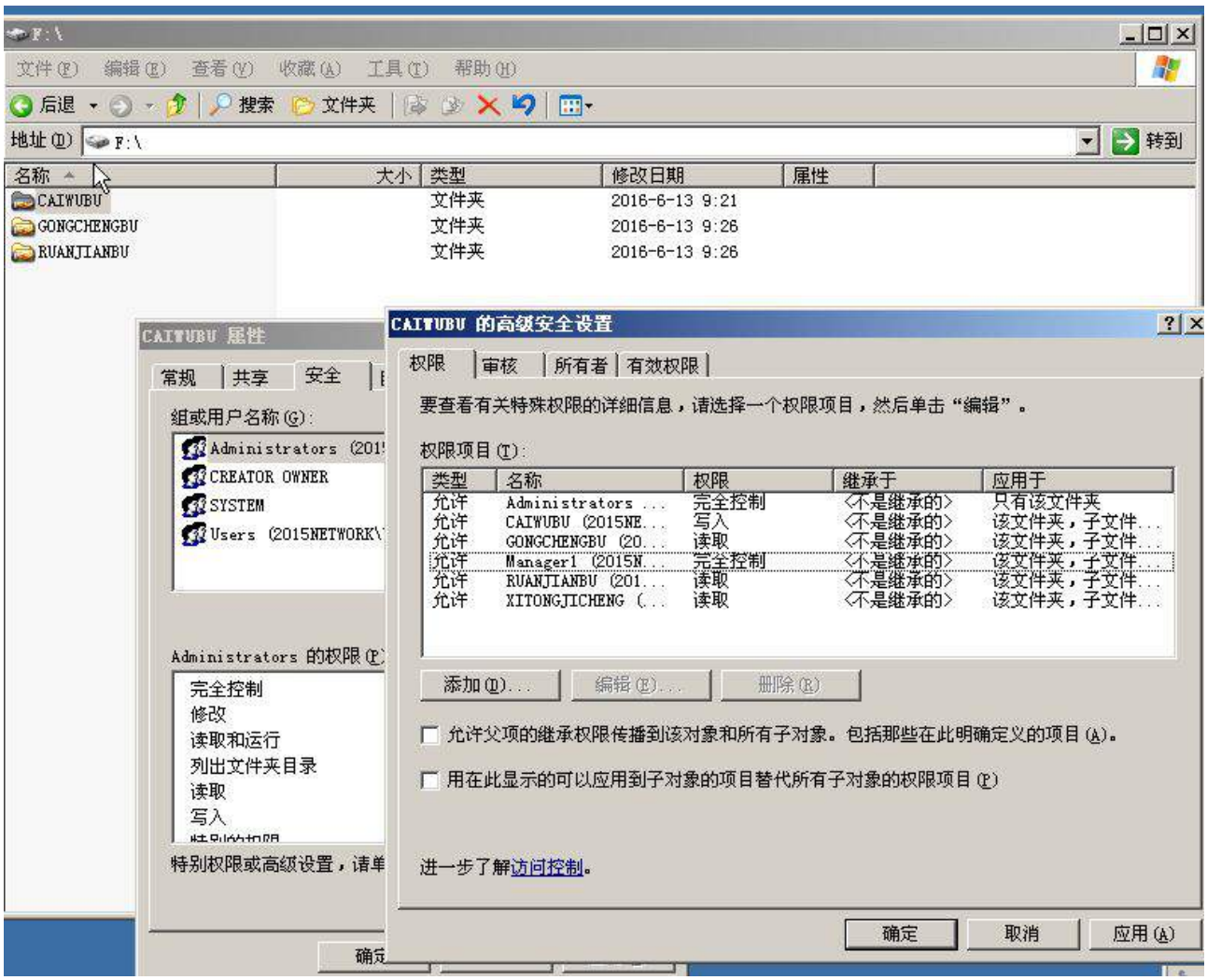


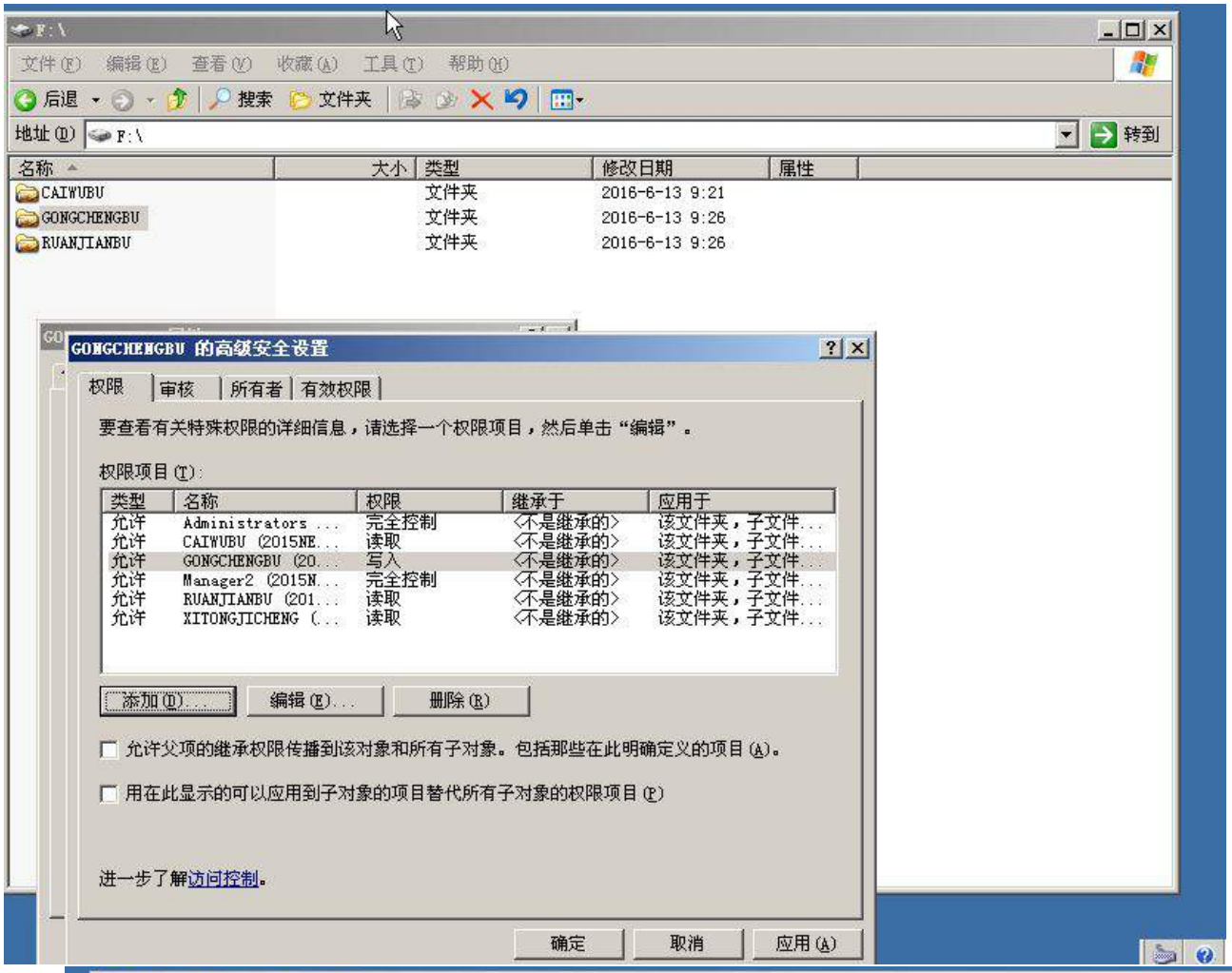
5、根据部门的不同，在 RAID5 分区中建立 3 个共享文件夹，下表列出了访问权限及磁盘限制。

文件夹名称	共享权限/NTFS 权限	硬盘限制

CAIWUBU	其它部门可以浏览，不可以上传，财务部的员工可以有上传权限，部门主任具有完全控制权限。	部门主任限制空间为 1G，超过 800M 报警；部门中其他人员为 500M，超过 400M 报警
GONGCHENGBU	其它部门可以浏览，不可以上传，工程部的员工可以有上传权限，部门主任具有完全控制权限。	部门主任限制空间为 1G，超过 800M 报警；部门中其他人员为 500M，超过 400M 报警
RUANJIANBU	其它部门可以浏览，不可以上传，软件部的员工可以有上传权限，部门主任具有完全控制权限。	部门主任限制空间为 1G，超过 800M 报警；其它员工为 500M，超过 400M 报警


名称
大小
类型
修改日期
属性
CAIWUBU
文件夹
2016-6-13 9:21
GONGCHENGBU
文件夹
2016-6-13 9:26
2016-6-13 9:26
RUANJIANBU 属性
常规
共享
安全
自定义
RUANJIANBU 的高级安全设置
权限
审核
所有者
有效权限
要查看有关特殊权限的详细信息，请选择一个权限项目，然后单击“编辑”。
权限项目(T):
类型
名称
权限
继承于
应用于
允许 Administrators ... 完全控制 <不是继承的> 只有该文件夹
允许 CAIWUBU (2015NE... 读取 <不是继承的> 该文件夹，子文件...
允许 GONGCHENGBU (20... 读取 <不是继承的> 该文件夹，子文件...
允许 Manager3 (2015N... 完全控制 <不是继承的> 该文件夹，子文件...
允许 RUANJIANBU (201... 写入 <不是继承的> 该文件夹，子文件...
允许 XITONGJICHENG (... 读取 <不是继承的> 该文件夹，子文件...
添加(D)...
编辑(E)...
删除(R)
允许父项的继承权限传播到该对象和所有子对象。包括那些在此明确定义的项目(A)。
用在此显示的可以应用到子对象的项目替代所有子对象的权限项目(P)
进一步了解访问控制。
确定
取消
应用(A)


F:\
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
后退 搜索 文件夹
地址(D) F:\
转到
名称 大小 类型 修改日期 属性
CAIWUBU 文件夹 2016-6-13 9:21
GONGCHENGBU 文件夹 2016-6-13 9:26
RUANJIANBU 文件夹 2016-6-13 9:26
CAIWUBU 属性
常规 共享 安全
组或用户名称(G):
Administrators (201
CREATOR OWNER
SYSTEM
Users (2015NETWORK\
Administrators 的权限(P)
完全控制
修改
读取和运行
列出文件夹目录
读取
写入
特别权限或高级设置，请单
确定
CAIWUBU 的高级安全设置
权限 审核 所有者 有效权限
要查看有关特殊权限的详细信息，请选择一个权限项目，然后单击“编辑”。
权限项目(T):
类型 名称 权限 继承于 应用于
允许 Administrators ... 完全控制 <不是继承的> 只有该文件夹
允许 CAIWUBU (2015NE... 写入 <不是继承的> 该文件夹，子文件...
允许 GONGCHENGBU (20... 读取 <不是继承的> 该文件夹，子文件...
允许 Manager1 (2015N... 完全控制 <不是继承的> 该文件夹，子文件...
允许 RUANJIANBU (201... 读取 <不是继承的> 该文件夹，子文件...
允许 XITONGJICHENG (... 读取 <不是继承的> 该文件夹，子文件...
添加(D)... 编辑(E)... 删除(R)
允许父项的继承权限传播到该对象和所有子对象。包括那些在此明确定义的项目(A)。
用在此显示的可以应用到子对象的项目替代所有子对象的权限项目(P)
进一步了解访问控制。
确定 取消 应用(A)


F:\
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
后退 搜索 文件夹
地址(D) F:\
转到
名称 大小 类型 修改日期 属性
CAIWUBU 文件夹 2016-6-13 9:21
GONGCHENGBU 文件夹 2016-6-13 9:26
RUANJIANBU 文件夹 2016-6-13 9:26
GONGCHENGBU 的高级安全设置
权限 审核 所有者 有效权限
要查看有关特殊权限的详细信息，请选择一个权限项目，然后单击“编辑”。
权限项目(T):
类型 名称 权限 继承于 应用于
允许 Administrators ... 完全控制 <不是继承的> 该文件夹，子文件...
允许 CAIWUBU (2015NE... 读取 <不是继承的> 该文件夹，子文件...
允许 GONGCHENGBU (20... 写入 <不是继承的> 该文件夹，子文件...
允许 Manager2 (2015N... 完全控制 <不是继承的> 该文件夹，子文件...
允许 RUANJIANBU (201... 读取 <不是继承的> 该文件夹，子文件...
允许 XITONGJICHENG (... 读取 <不是继承的> 该文件夹，子文件...
添加(D)... 编辑(E)... 删除(R)
允许父项的继承权限传播到该对象和所有子对象。包括那些在此明确定义的项目(A)。
用在此显示的可以应用到子对象的项目替代所有子对象的权限项目(P)
进一步了解访问控制。
确定 取消 应用(A)


本地磁盘 (C:) 的配额项
配额(Q) 编辑(E) 查看(V) 帮助(H)
状态 名称 登录名 使用数量 配额限制 警告等级 使用...
确定 2015NETWOR... 0 字节 500 MB 400 MB 0
确定 2015NETWOR... 0 字节 1 GB 800 MB 0
确定 2015NETWOR... 0 字节 500 MB 400 MB 0
确定 2015NETWOR... 0 字节 1 GB 800 MB 0
确定 2015NETWOR... 0 字节 500 MB 400 MB 0
确定 2015NETWOR... 0 字节 1 GB 800 MB 0
确定 BUILTIN\Ad... 0 字节 无限制 无限制 暂缺

（三）在主机 Win2008-A1 中完成 VPN 服务器的部署

1、将此服务器加入 2015Network.com 域，同时完成路由和远程访问服务的配置，建立和 win2008-B1 的站点对站点的 VPN 连接；IP 地址自行指定，拨入用户使用主机的本地用户。

2、VPN 类型为采用计算机证书方式的 L2TP，证书服务器为 win2008-B1（可先设置为 PPTP 拨入类型，最终采用计算机证书方式的 L2TP 类型）。

3、设置请求拨号时间在周一至周五的所有时段。

二、在 Server 2 上完成如下操作:

（一）完成虚拟主机的创建

1、安装虚拟机“Win2008-B1”， 其内存为 1G，硬盘 20G，将服务器加入至 Windows 域中。

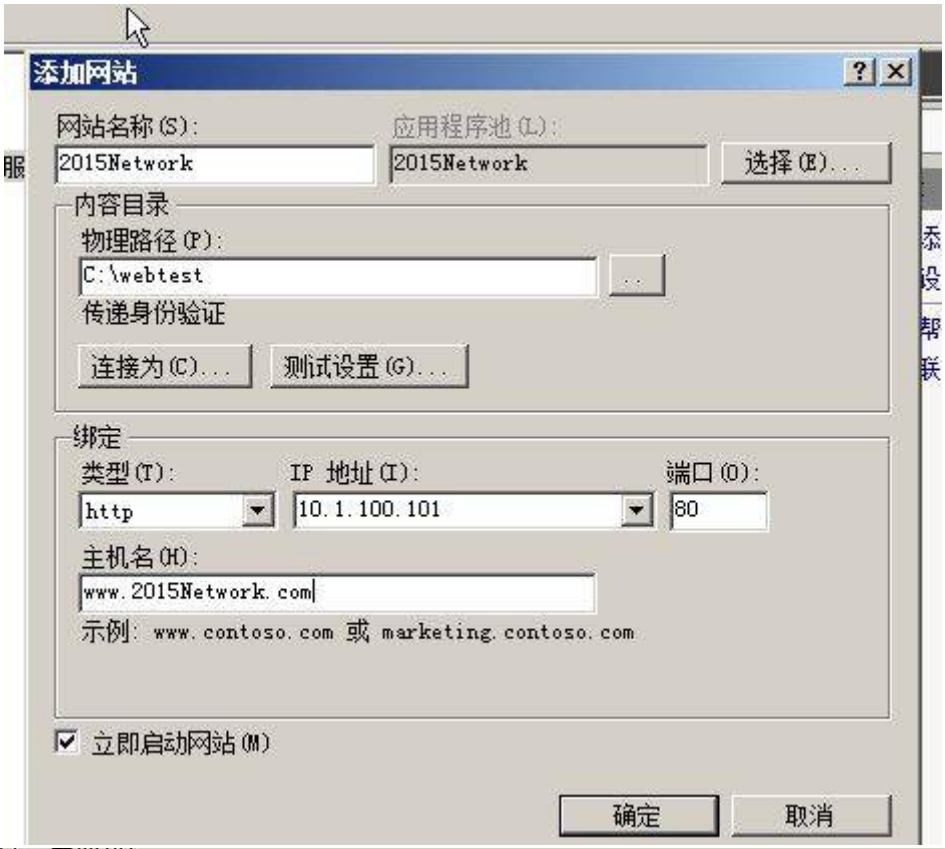
（二）在主机 Win2008-B1 中完成 VPN 的部署

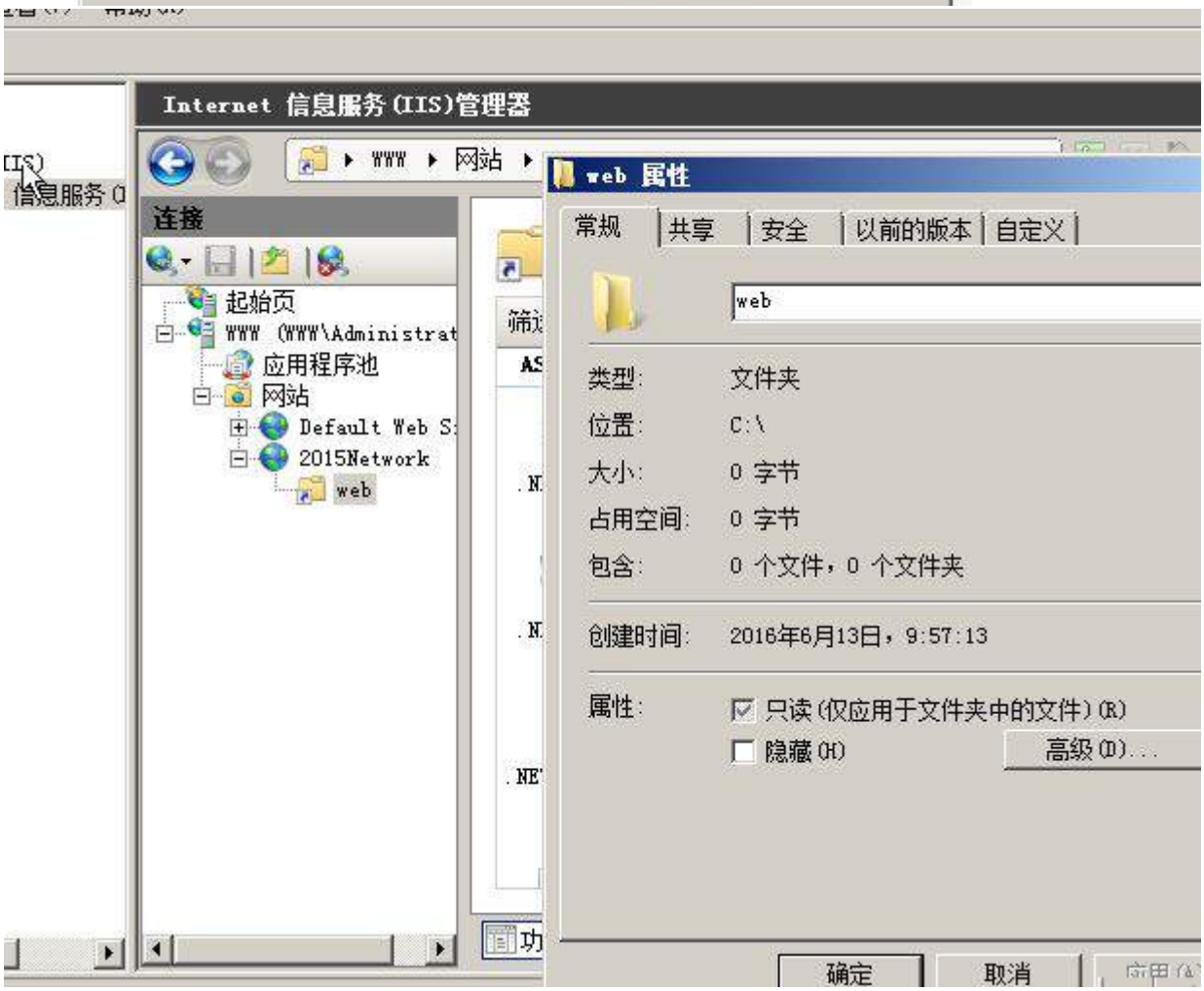
1、在此服务器完成路由和远程访问服务的配置，建立和 win2003-A1 的站点对站点的 VPN 连接； IP 地址自行指定，拨入用户使用域用户，非主机上的本地用户。

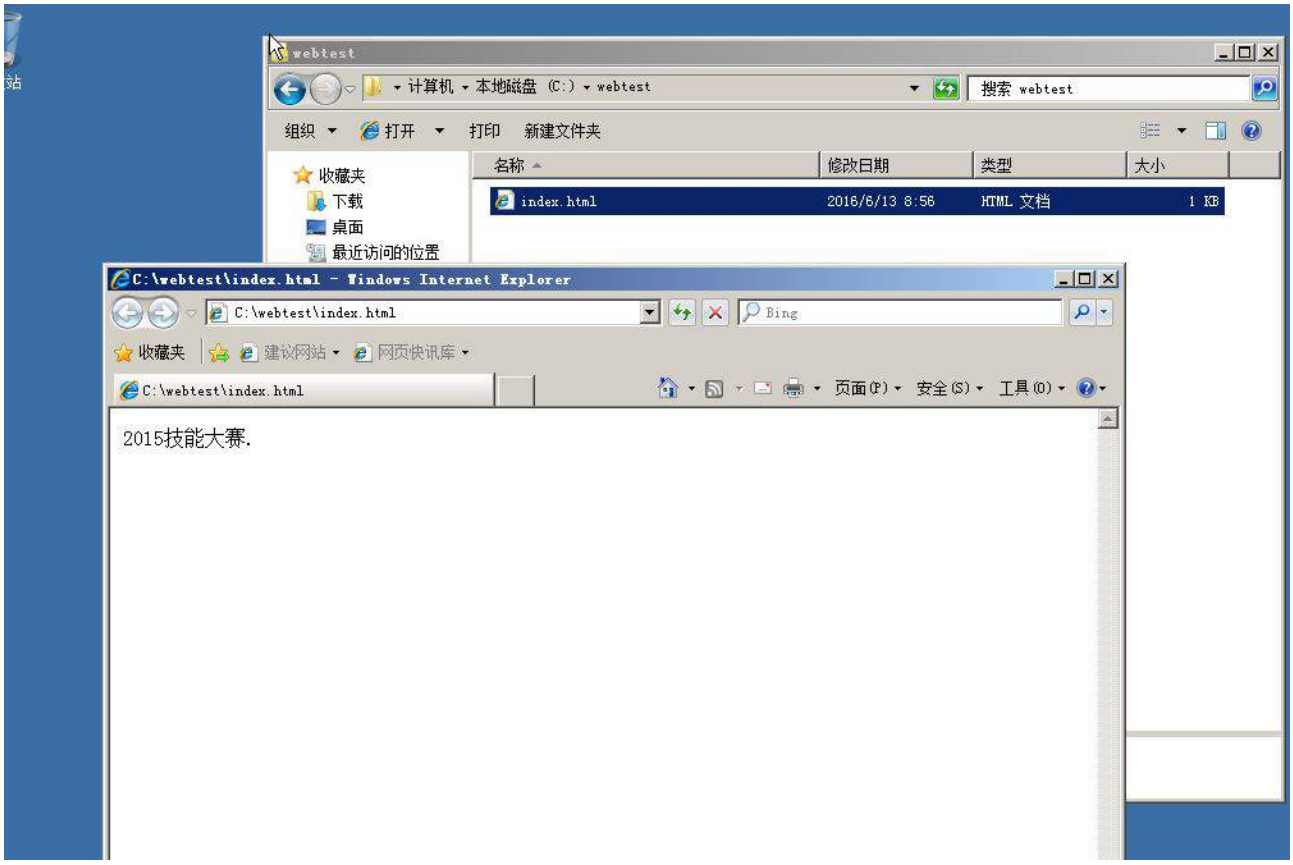
2、VPN 类型为采用计算机证书方式的 L2TP，证书服务器为 win2003-A1（可先设置为 PPTP 拨入类型，最终采用计算机证书方式的 L2TP 类型）；VPN 用户远程访问权限通过“远程访问策略控制访问“。

（三）在主机 Win2008-B1 中完成 WWW 服务器的部署

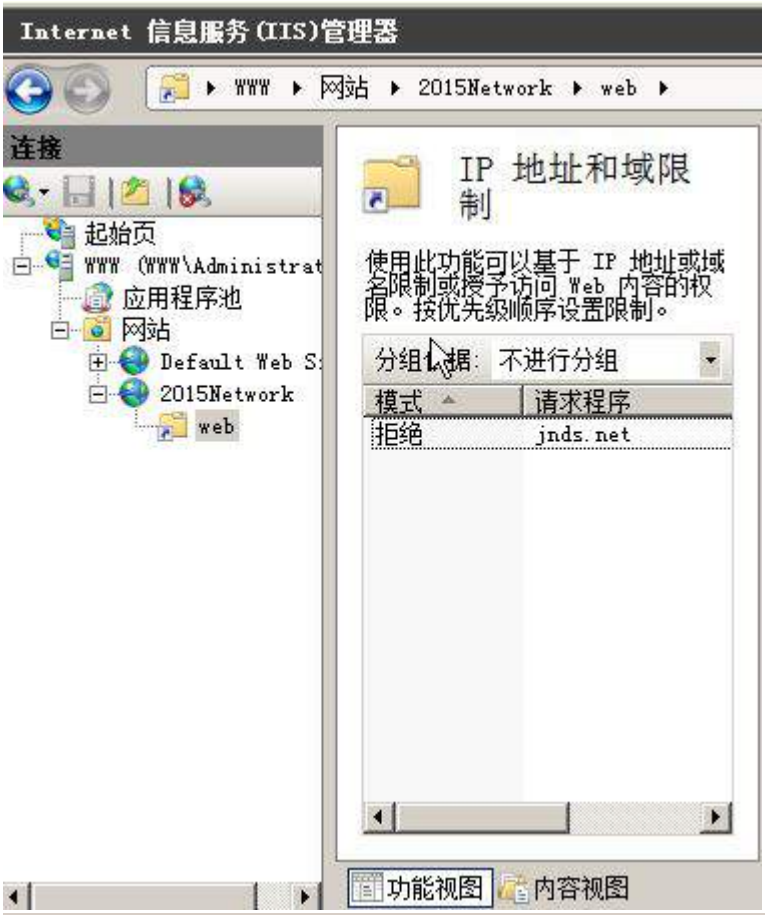
1、配置 IIS 服务器，创建名为 2015Network 的站点，主目录路径为 c:\webtest，并配置主机头 www.2015Network.com；此外，创建虚拟目录 web，目录路径为 c:\web，设置首页显示内容为“2015 技能大赛。”。

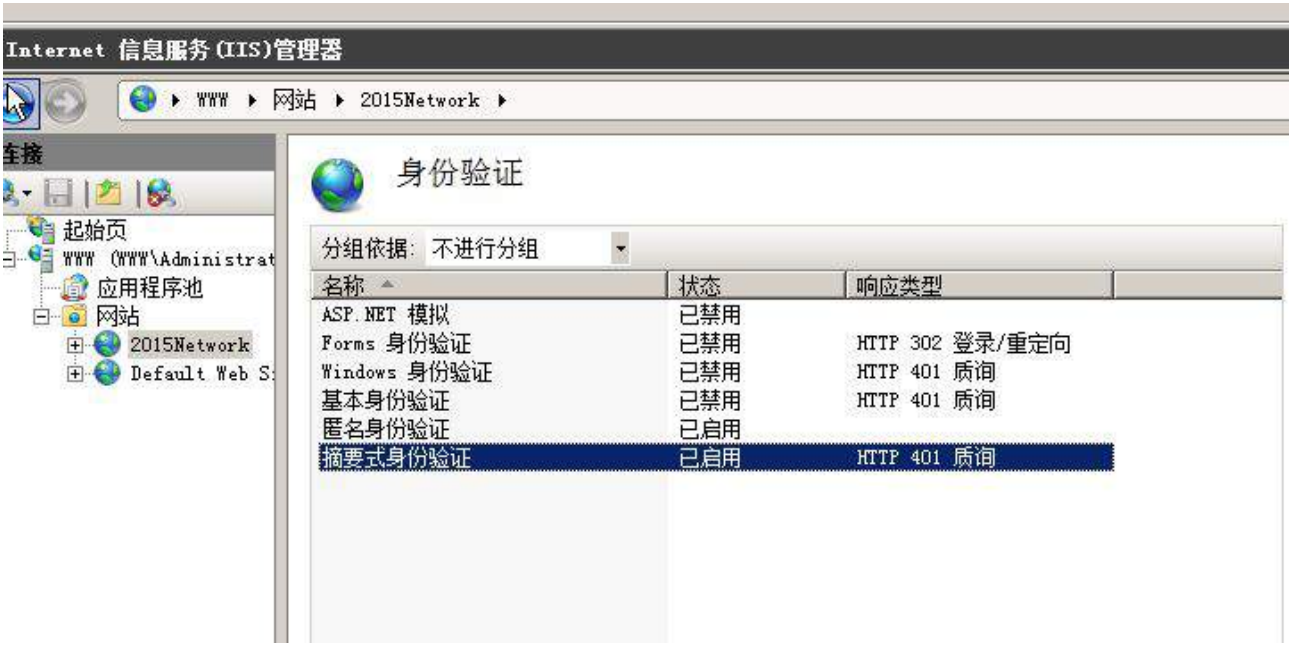

添加网站
网站名称(S):
2015Network
应用程序池(L):
2015Network
选择(E)...
内容目录
物理路径(P):
C:\webtest
传递身份验证
连接为(C)...
测试设置(G)...
绑定
类型(T):
http
IP 地址(I):
10.1.100.101
端口(O):
80
主机名(H):
www.2015Network.com
示例: www.contoso.com 或 marketing.contoso.com
立即启动网站(M)
确定
取消


Internet 信息服务(IIS)管理器
WWW ▸ 网站 ▸
连接
起始页
WWW (WWW\Administrat
应用程序池
网站
Default Web S
2015Network
web
web 属性
常规
共享
安全
以前的版本
自定义
web
类型: 文件夹
位置: C:\
大小: 0 字节
占用空间: 0 字节
包含: 0 个文件，0 个文件夹
创建时间: 2016年6月13日，9:57:13
属性:
只读(仅应用于文件夹中的文件)(R)
隐藏(H)
高级(D)...
确定
取消



2、限制所有后缀为 jnds.net 的主机均不能访问此网站；设置网站应用摘要式身份验证方式，访问者必须输入正确的域用户和密码方可进行访问。





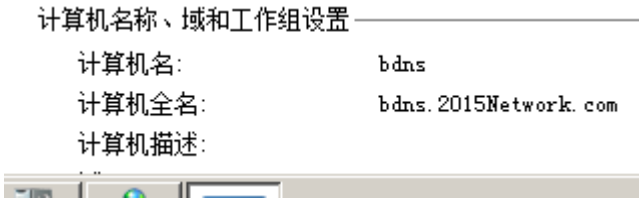
三、在 Server 3 上完成如下操作:

（一）完成虚拟主机的创建

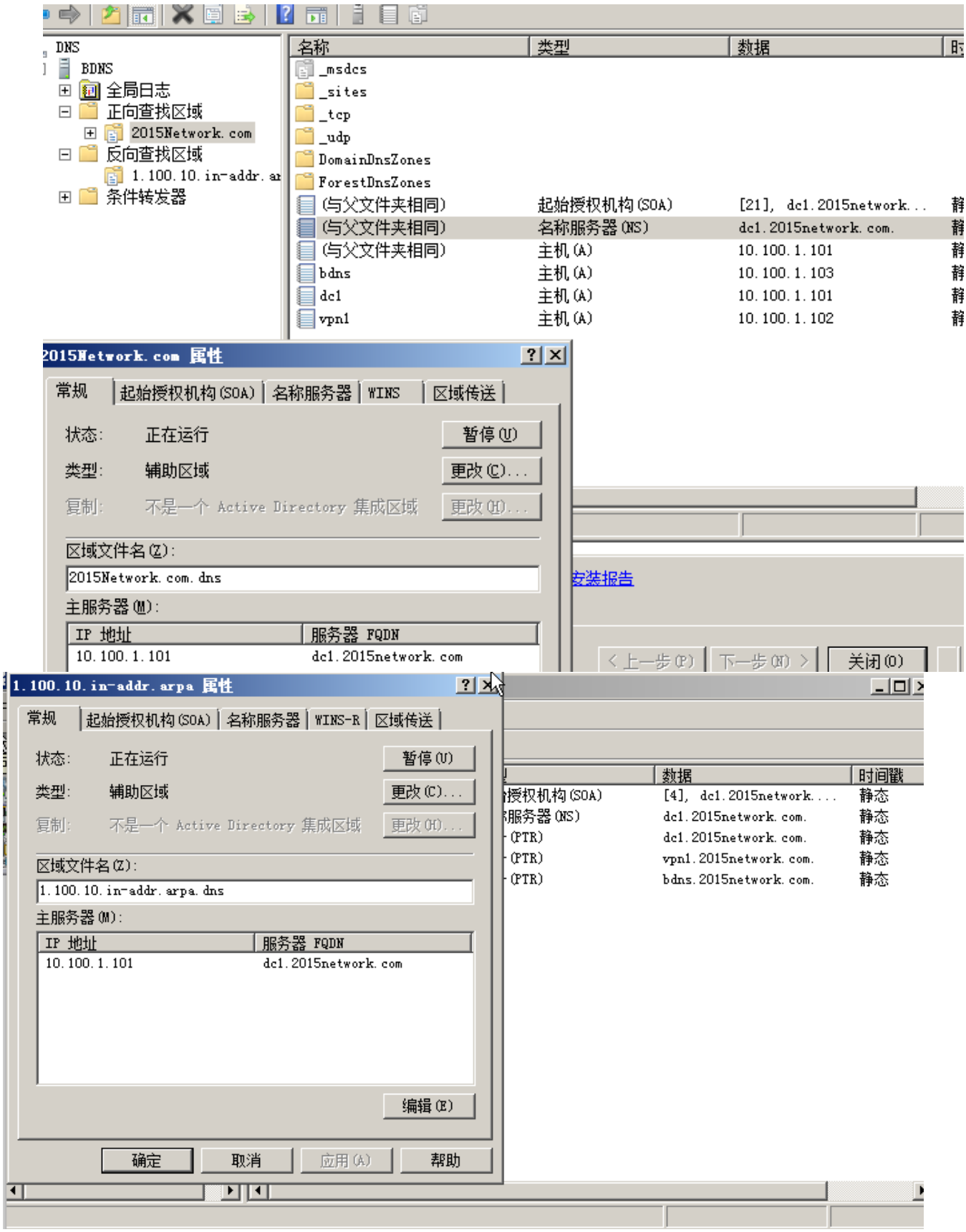
1、在虚拟机“Win2003-C1”，其内存为 1G，硬盘 20G，并将服务器加入到 Windows 域环境。

（二）在主机 Win2003-C1 中完成备份 DNS 的部署

1、配置此服务器为备份 DNS，其合法域名为 bdns. 2015Network.com。



2、将服务器加入到 windows 域中，将所有的主 DNS 的区域都复制到备份 DNS 服务器上。



Linux 操作系统部分

【说 明】

1、所有 Linux 操作系统的 root 用户的密码为 123456，若未按要求设置密码，涉及到该操作系统下的所有分值记为 0 分。

2、虚拟主机的 IP 属性设置请按照网络拓扑结构图以及“表 3：服务器 IP 地址分配表”的要求设定。

3、除有特别规定外，其他未明确规定用户密码均与用户名相同。

4、如果宿主机是 Linux 的操作系统，所有操作系统镜像文件及试题所需的其他软件均存放于每台计算机的/根目录下；如果宿主机是 windows 的操作系统，所有系统镜像文件及试题所需的其它软件均存放在每台主机的 D:\soft 文件夹中。并将题目要求的截图内容以.jpg 格式存储于 BACKUP 文件夹中。

5、题目要求的虚拟机均安装于每台主机的 D：\virtualPC 目录，即路径为 D：\virtualPC\虚拟主机名称。

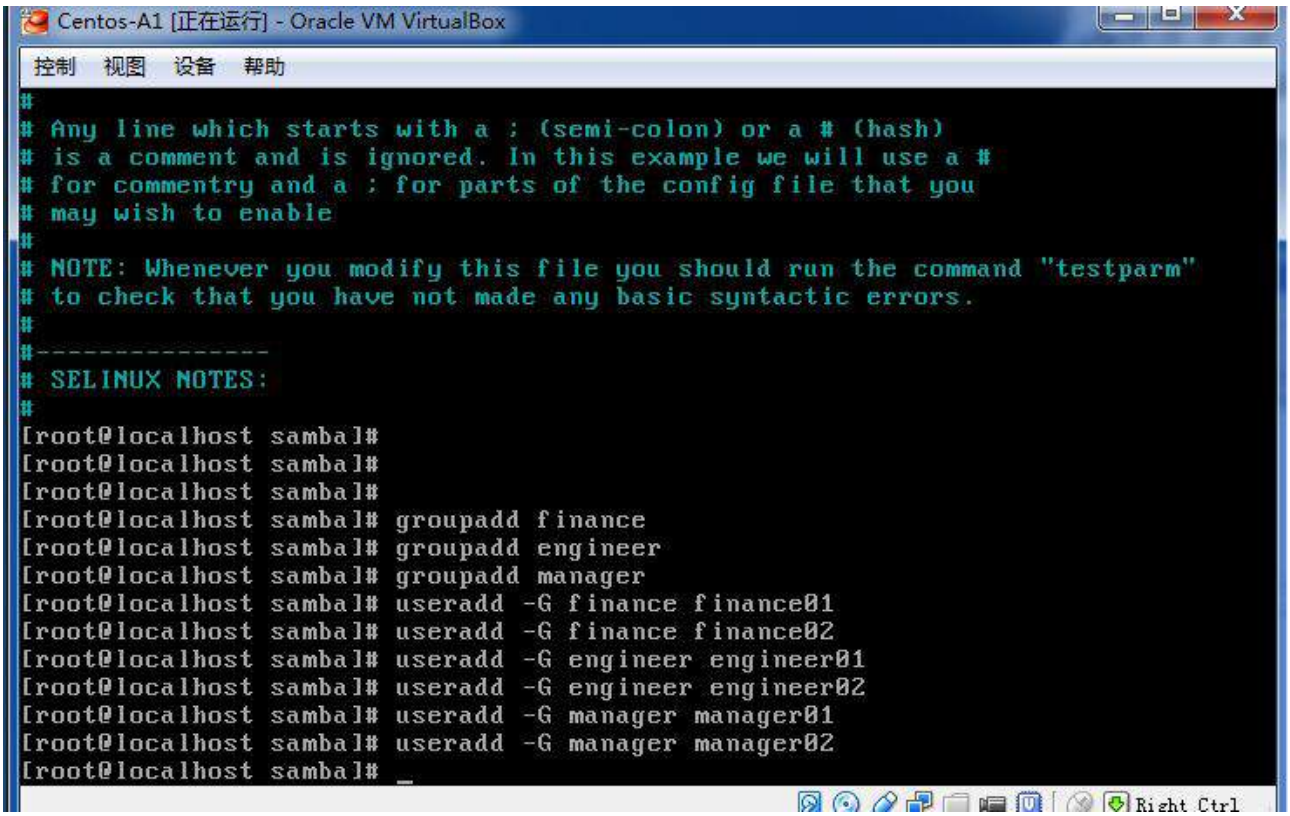
一、在 Server 1 上完成如下操作:

（一）完成虚拟主机的创建

安装虚拟机“Centos-A1”,具体要求为内存 512MB,硬盘 10GB。

（二）在主机 Centos-A1 中完成 Samba 共享服务器的部署

1、在此服务器中安装配置 Samba 服务，为公司配置财务、工程、经理 3 个用户组，设为 finance、engineer、manager；每个组设置 2 个用户，用户分别为： finance01、finance02、engineer01、 engineer02 、manager01、manager02。



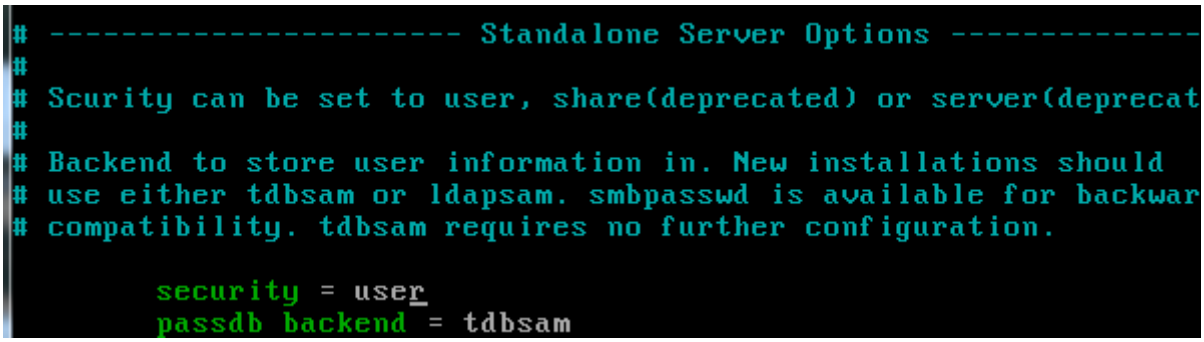
2、服务器采用用户验证的方式，每个用户可以访问且只能访问自己的宿主目录，且有完全的权限，每个人都不能看到其他人的宿主目录。

3、建立目录/opt/finance，finance 组具有可读可写的权限， manager 组和用户 engineer02 具有读权限。

4、建立一个/opt/manager 的目录，只有经理组的人可以访问，并读写，用户 engineer02 具有读权限，但其他人看不到该目录。

5、建立一个文件交换目录 exchange，所有的人都能读写，包括 guest 用户，但每个人不能删除别人的文件。

6、阻止客户端上传含有特定关键字的文件或目录到 samba 共享资源，客户端不允许在目录/opt/finance 中上传可执行文件（.exe）及位图（.jpg）文件；客户端不允许在/opt/manager 目录中上传包含 root 关键字的文件或目录。



```
[root@localhost samba]#
[root@localhost samba]# mkdir /opt/finance
[root@localhost samba]# mkdir /opt/engineer
[root@localhost samba]# mkdir /opt/manager
[root@localhost samba]# chmod 777 /opt/finance/
[root@localhost samba]# chmod 777 /opt/engineer/
[root@localhost samba]# chmod 777 /opt/manager/
[root@localhost samba]# _
```

```
[root@localhost samba]#
[root@localhost samba]# mkdir /opt/exchange
[root@localhost samba]# chmod 1777 /opt/exchange/
[root@localhost samba]# _
```

```
[finance]
path = /opt/finance
browseable = no
writable = no
write list = @finance
read list = @manager,engineer02
veto file = /*.exe/,/*.jpg/
[manager]
path = /opt/manager
browseable = no
writable = no
write list = @manager
read list =engineer02
veto file =/*root*/
[exchange]
path = /opt/exchange
guest ok =yes
writable = yes
```

二、在 Server 2 上完成如下操作：

（一）完成虚拟主机的创建

1、安装虚拟机“Centos-B1”,具体要求为内存 768MB，硬盘 20GB；分区大小为：/boot 分区大小为 500M，文件类型为 ext4；/home 分区大小为 2G，文件类型为 ext4，/分区为 10G，文件类型为 ext4。


常规
名称: Centos-B1
操作系统: Red Hat (64 bit)
预览
系统
内存大小: 768 MB
启动顺序: 软驱, 光驱, 硬盘
硬件加速: VT-x/AMD-V, 嵌套分页, PAE/NX
显示
显存大小: 12 MB
远程桌面服务器: 已禁用
录像: 已禁用
存储
控制器: IDE
第二IDE控制器主通道: [光驱] CentOS-6.5-x86_64-bin-DVD1.iso (4.16 GB)
控制器: SATA
SATA 端口 0: Centos-B1__.vdi (普通, 20.00 GB)
声音
主机音频驱动: Windows DirectSound
控制芯片: ICH AC97
网络
网卡 1: Intel PRO/1000 MT 桌面 (桥接网络, Intel(R) Ethernet Connection I217-LM)


Centos-B1 [正在运行] - Oracle VM VirtualBox
控制 视图 设备 帮助
请选择源驱动器
设备
大小 (MB)
挂载点/ RAID/卷
类型
格式
硬盘驱动器
sda (/dev/sda)
sda1 500 /boot ext4
sda2 10240 / ext4
sda3 2048 /home ext4
空闲 7691

2、安装虚拟机“Centos-B2”,具体要求为内存 512MB，硬盘 10GB。

（二）在主机 Centos-B1 中完成磁盘管理的部署

1、在“Centos-B1”中额外添加 5 块硬盘，容量分别为 2G。

2、此操作需要 1 块硬盘，通过格式化建立两个主分区以及一个逻辑分区，创建一个逻辑卷。逻辑卷命名为 engineering，属于卷组 vol，且大小为 10 个扩展；在卷组 vol 的逻辑卷每个扩展的大小为 32MiB；使用 vfat 格式化这个新的逻辑卷，此逻辑卷在系统启动的时候应该能自动挂在到/mnt/engineering。

```
Command (m for help): p

Disk /dev/sdb: 2147 MB, 2147483648 bytes
255 heads, 63 sectors/track, 261 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0xd9403e21

   Device Boot      Start         End      Blocks   Id  System
/dev/sdb1               1          63      506016   83  Linux
/dev/sdb2              64         126      506047+  83  Linux
/dev/sdb3             127         261     1084387+   5  Extended
/dev/sdb5             127         261     1084356   83  Linux

Command (m for help): _
```

```
[root@localhost ~]# vgcreate -s 32MiB vol /dev/sdb1 /dev/sdb2 /dev/sdb5
  Volume group "vol" successfully created
[root@localhost ~]# lvcreate -L 320MiB -n engineering vol
  Logical volume "engineering" created
[root@localhost ~]# _
```

```
[root@localhost ~]# mkfs.vfat /dev/vol/engineering
mkfs.vfat 3.0.9 (31 Jan 2010)
unable to get drive geometry, using default 255/63
[root@localhost ~]# _
```

```
#
# /etc/fstab
# Created by anaconda on Sun Jun 12 20:30:36 2016
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
/dev/mapper/VolGroup-lv_root /                       ext4    defaults        1 1
UUID=cc4ee8bd-c295-460a-807a-c1ddbcd353ea /boot                   ext4    defaul
ts        1 2
/dev/mapper/VolGroup-lv_swap swap                    swap    defaults        0 0
tmpfs                   /dev/shm                tmpfs   defaults        0 0
devpts                  /dev/pts                devpts  gid=5,mode=620  0 0
sysfs                   /sys                    sysfs   defaults        0 0
proc                    /proc                   proc    defaults        0 0
/dev/voil/engineering   /mnt/entineering        ext3    defaults        0 0_
~
~
~
```

3、在每天下午 6 :50 删除/mytmp 目录下的全部子目录和全部文件；每逢星期一下午 8:00 将/home 目录下的所有目录和文件归档并压缩为文件：backup.tar.gz；在每天下午 5:55 将 IDE 接口的 CD-ROM 卸载（假设：CD-ROM 的设备名为 hdc）；在早晨 8:00 前开机后启动。

```
管理  控制  视图  热键  设备  帮助
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root
HOME=/

# For details see man 4 crontabs

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr .
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7)
ri,sat
# |  |  |  |  |
# *  *  *  *  * user-name command to be executed
  50 6  *  *  * rm -r /mytmp
  *  21 *  *  mon tar -zcvf backup.tar.gz /home
  55 17 *  *  * umount -f /dev/hdc
  55 7 *  *  *  mount /dev/hdc /mnt/hdc
~
```

（三）在主机 Centos-B2 中完成 DHCP 服务器的部署

1、在此服务器中安装配置 DHCP 服务。要求 DHCP 服务器在子网 10.1.100.0/24 中给客户机动态分配的 IP 地址在 10.1.100.200 和 10.1.100.250 之间。

2．默认租用时间为 21600s，最大租约时间为 43200s。

3．客户机分配的 DNS 服务器地址是 10.1.101.102，设置域为 2015Network.com。

```
# A slightly different configuration for an internal subnet.
subnet 10.1.100.0 netmask 255.255.255.0 {
  range 10.1.100.200 10.1.100.250;
  option domain-name-servers 10.1.101.102;
  option domain-name "2015Network.com";
  option routers 10.1.100.254;
  option broadcast-address 10.1.100.255;
  default-lease-time 21600;
  max-lease-time 43200;
}
```

三、在 Server 3 上完成如下操作：

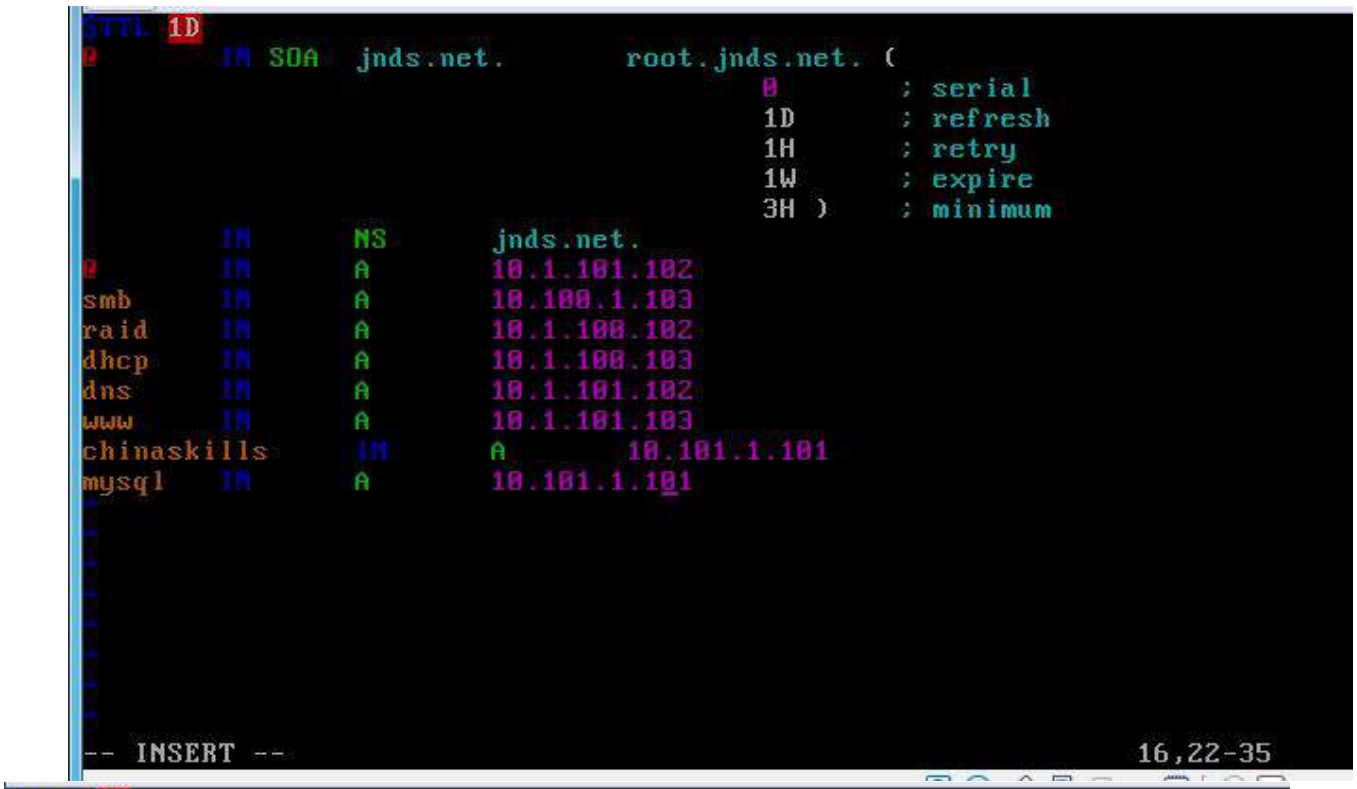
（一）完成虚拟主机的创建

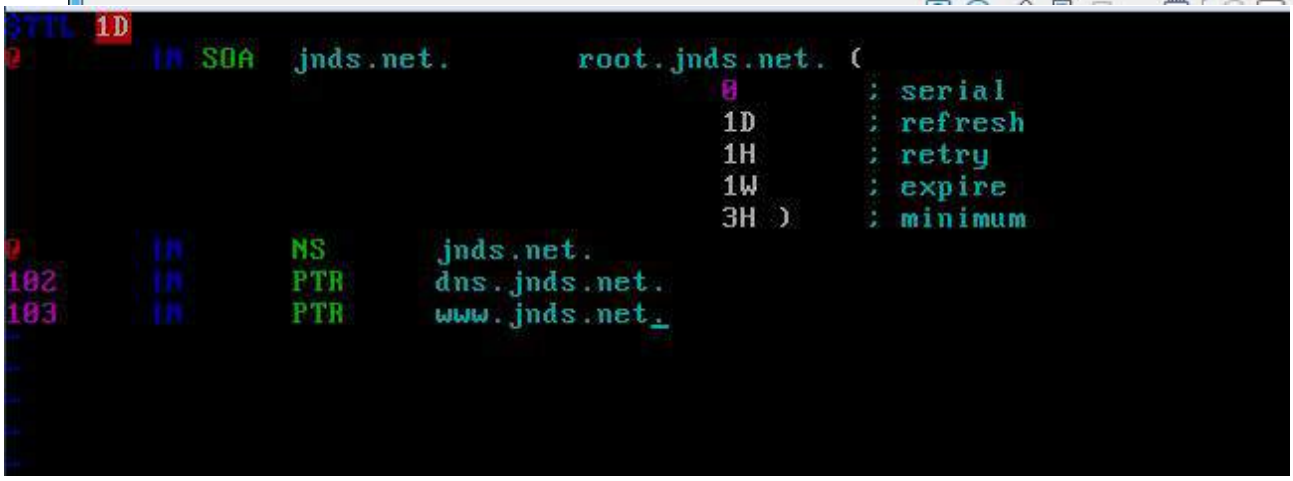
1、安装名为“Centos-C1”的虚拟机，具体要求为硬盘大小为 20GB，内存为 512MB。

2、安装名为“Centos-C2”的虚拟机，具体要求为硬盘大小为 20GB，内存为 512MB。

（二）在主机 Centos-C1 中完成 BIND 域名服务器以及代理服务器的部署

1、在此服务器中安装配置 bind 服务，负责区域“jnds.net”内主机解析，五台主机分别为 dns.jnds.net、squid.jnds.net、www.jnds.net、www.jnds.lab.net、smb.jnds.net、raid.jnds.net、dhcp.jnds.net、chinaskill.jnds.net、mysql.jnds.net，做好正反向 DNS 服务解析，对访问 2015Network.com 域的解析转发给 Win2003-A1。


$TTL 1D
@ IN SOA jnds.net. root.jnds.net. (
0 ; serial
1D ; refresh
1H ; retry
1W ; expire
3H) ; minimum
IN NS jnds.net.
@ IN A 10.1.101.102
smb IN A 10.100.1.103
raid IN A 10.1.100.102
dhcp IN A 10.1.100.103
dns IN A 10.1.101.102
www IN A 10.1.101.103
chinaskills IN A 10.101.1.101
mysql IN A 10.101.1.101
-- INSERT --
16,22-35


$TTL 1D
@ IN SOA jnds.net. root.jnds.net. (
0 ; serial
1D ; refresh
1H ; retry
1W ; expire
3H) ; minimum
@ IN NS jnds.net.
102 IN PTR dns.jnds.net.
103 IN PTR www.jnds.net.

```
$TTL 1D
@       IN SOA  jnds.net.       root.jnds.net. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
@       IN      NS      jnds.net.
102     IN      PTR     raid.jnds.net.
103     IN      PTR     dhcp.jnds.net.
```

```
$TTL 1D
@       IN SOA  jnds.net.       root.jnds.net. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
@       IN      NS      jnds.net.
101     IN      PTR     chinaskills.jnds.net.
101     IN      PTR     mysql.jnds.net
```

```
//
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//

options {
        listen-on port 53 { any; };
        listen-on-v6 port 53 { any; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        allow-query     { any; };
        recursion yes;
        foward only;
        forwarders{10.100.100.1;};

        dnssec-enable yes;
        dnssec-validation yes;
        dnssec-lookaside auto;
-- INSERT --                                            20,28-35      Top
```

2、安装并完成代理服务器 squid 的初始配置，使用 8080 作为代理服务端口，配置 DNS 服务器使 squid 服务器的域名能够正确解析。

```
http_access allow localnet
http_access allow localhost

# And finally deny all other access to this proxy
http_access deny all

# Squid normally listens to port 3128
http_port 8080
dns_nameservers 10.1.101.102
```

3、设置 squid 代理服务器采用 ufs 缓存机制，缓存目录设置为/cache,目录容量为 5GB，L1 及 L2 级目录数量分别为 16 及 256，定义高速缓存值为 512MB。

```
# Uncomment and adjust the following to add a disk cache directory.
cache_dir ufs /cache 5120 16 256
cache_mem 512 MB
```

4、针对主机 10.1.101.103/24 提供代理服务，为缓解请求队列忙碌，设置重定向器池进程数为 20，并将缓存日志存放于/var/squid/cache.log 中。

```
visible_hostname 10.1.101.103/24
redirect_children 20
cache_log /var/squid/cache.log
# Add any of your own refresh_pattern entries above these.
```

（三）在主机 Centos-C2 中完成 Apache 服务器的部署

1、在此服务器中安装配置 WEB 服务，建立 web 站点：www.jnds.net 和 www.lab.jnds.net。

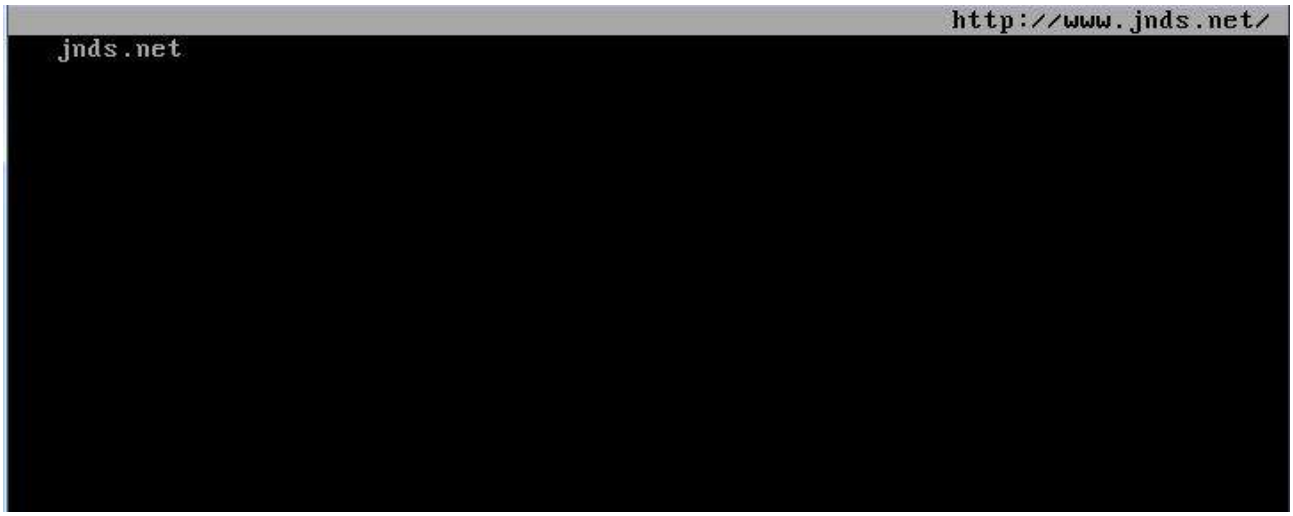
```
<VirtualHost *:80>
    DocumentRoot /www
    ServerName www.jnds.net
</VirtualHost>
<VirtualHost *:80>
    DocumentRoot /lab
    ServerName www.lab.jnds.net
</VirtualHost>
```

2、在站点 www. jnds.net 上建立两个虚拟目录 en 和 cn，其对应的物理路径分别是/data/CN 和/data/EN。配置 Web 服务器对虚拟目录/data/CN 启用用户认证，只允许 webadmin 用户访问。配置 Web 服务器对虚拟目录/data/EN 仅允许来自网络 jnds.com 域和 10.1.101.0/24 网段的客户机访问该虚拟目录。

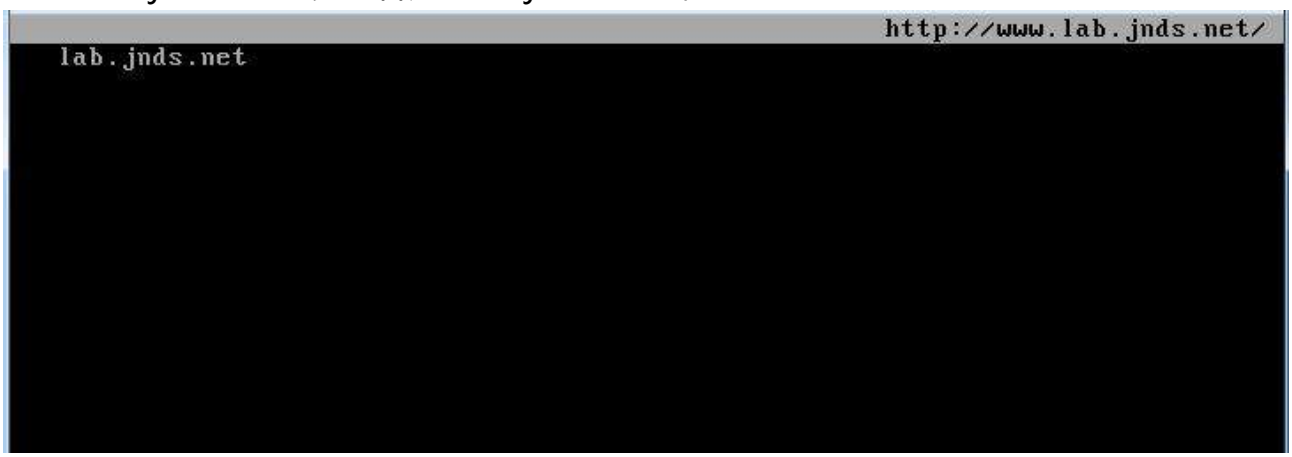
```
Alias /en "/data/EN"
Alias /cn "/data/CN"

<Directory "/data/CN">
    Options Indexes MultiViews FollowSymLinks
    AllowOverride ALL
        authtype basic
        authuserfile /etc/httpd/htpasswd
        require user webadmin
    Order allow,deny
    Allow from all
</Directory>
<Directory "/data/EN">
    Options Indexes MultiViews FollowSymLinks
    Order allow,deny
    Allow from jnds.com 10.1.101.0/24
</Directory>
```

3、建立主页，要求如下：

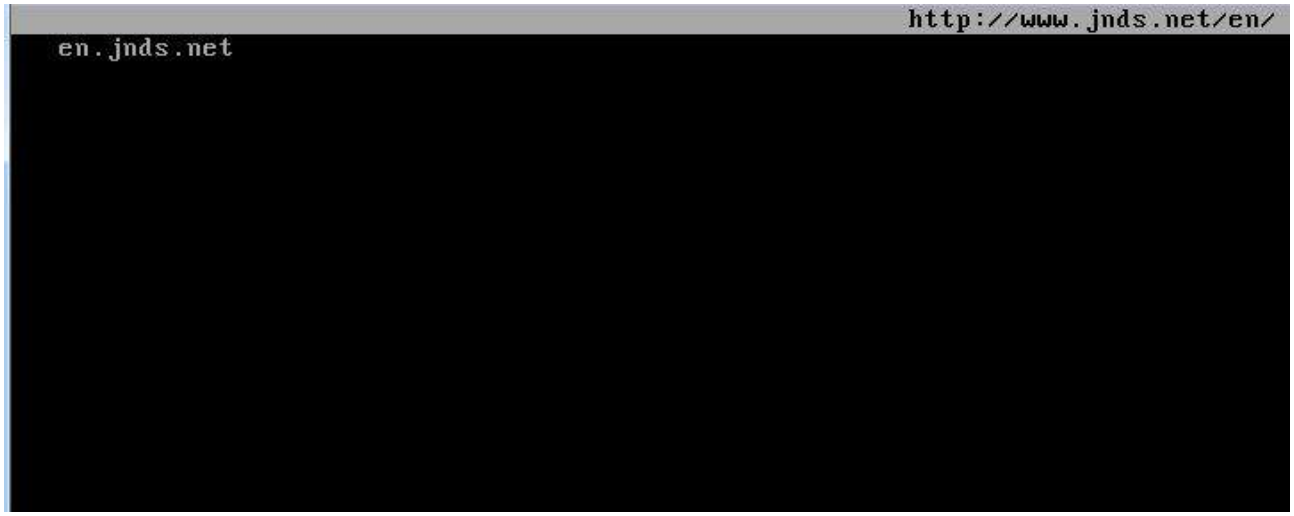
www. jnds.net 主页内容为“jnds.net”；



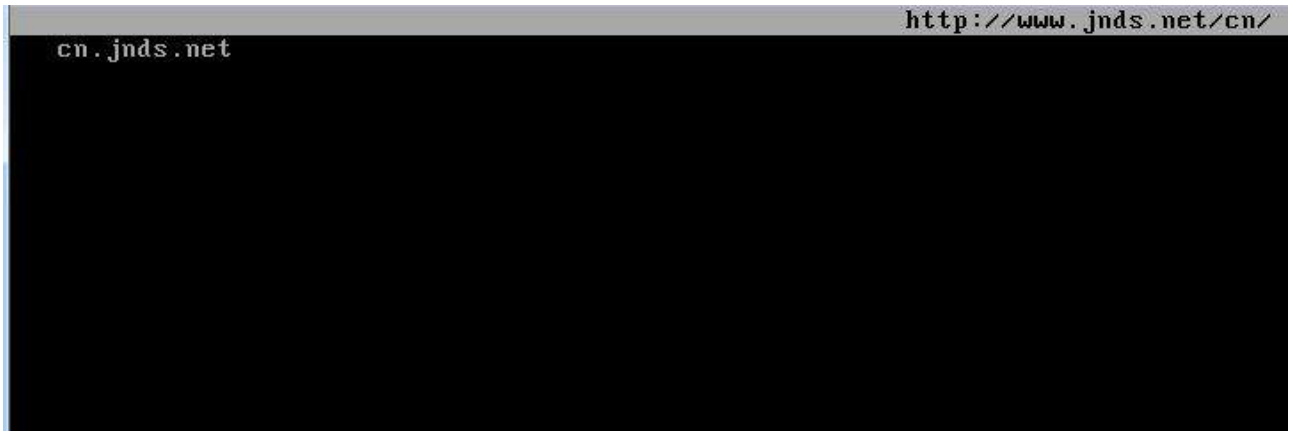
www.lab. jnds.net 主页内容为“lab.jnds.net”；



www. jnds.net/en 主页内容为“en. jnds. net”；



www. jnds. net /cn 主页内容为“cn. jnds. net”



四、 在 Server 4 上完成如下操作：

（一）完成虚拟主机的创建

1、Server4 主机系统为 CentOS 6.5，需要在此 Linux 平台上采用 KVM 方式安装虚拟机“Centos-D1”，具体要求为硬盘大小为 12GB，内存为 768MB，系统为 CentOs6.5；（小提示：如无法正确安装虚拟机 Centos-D1，下述题目中所涉及的虚拟机题目可在 Server4 真实主机中完成）。

（二）在主机 Centos-D1 中完成 Apache 服务器以及 MySQL 数据库服务器的部署

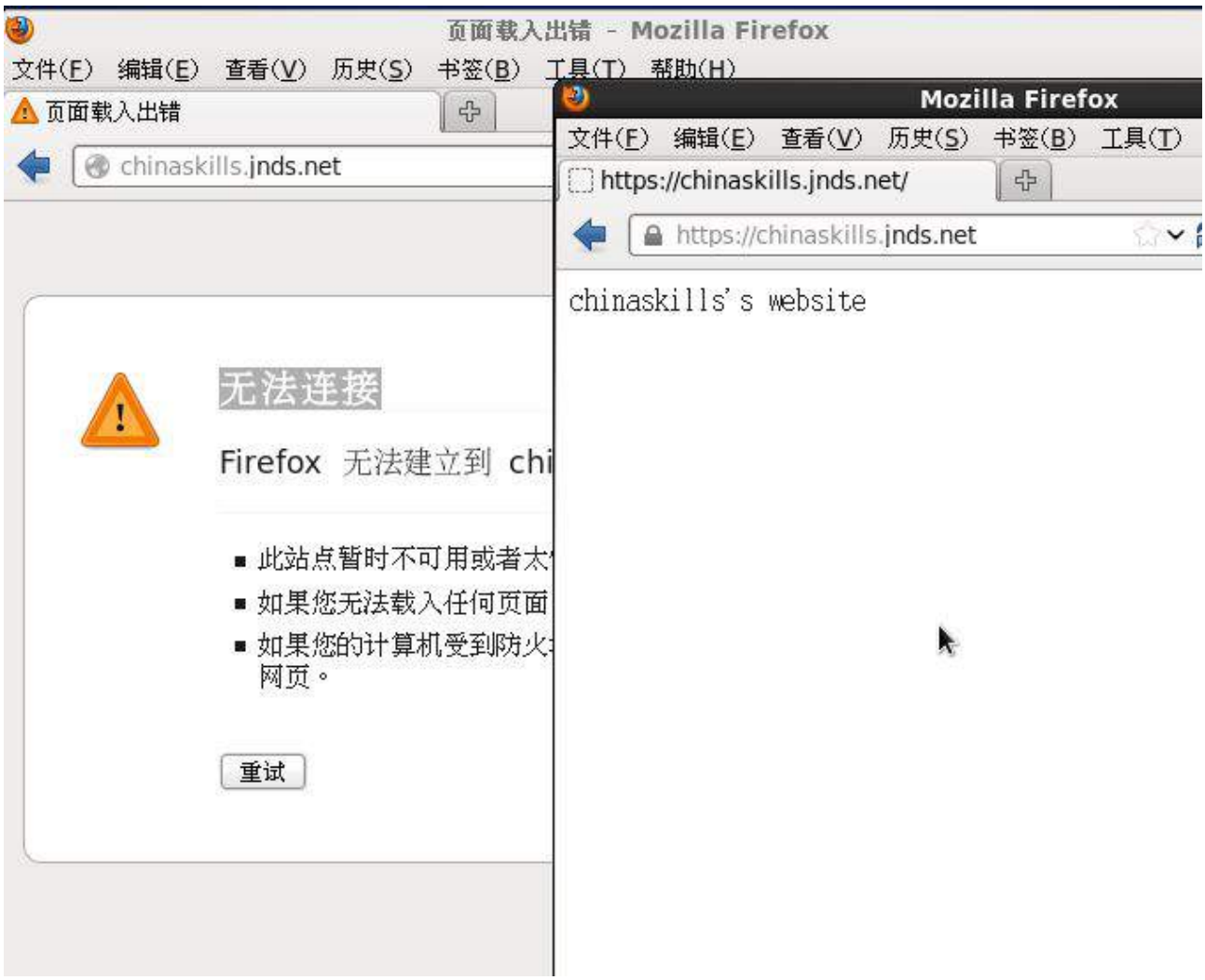
1、在此服务器中安装 httpd 服务，建立站点 chinaskill.jnds.net，其网站主目录为 /var/www/html，首页内容为“chinaskills’ s website”。

```
ServerName chinaskills.jnds.net:80

#
# UseCanonicalName: Determines how Apache constructs self-referencing
# URLs and the SERVER_NAME and SERVER_PORT variables.
# When set "Off", Apache will use the Hostname and Port supplied
# by the client.  When set "On", Apache will use the value of the
# ServerName directive.
#
UseCanonicalName Off

#
# DocumentRoot: The directory out of which you will serve your
# documents. By default, all requests are taken from this directory, bu
# symbolic links and aliases may be used to point to other locations.
#
DocumentRoot "/var/www/html"
```

```
                                                    http://chinaskills.jnds.net/
   chinaskills's website
```

2、使用 openssl 申请证书，创建自签名证书 server.crt 和私钥 server.key，要求只允许使用域名通过 SSL 加密访问。

```
[root@localhost conf]# openssl genrsa -out server.key 1024
Generating RSA private key, 1024 bit long modulus
.................................++++++
.....++++++
e is 65537 (0x10001)
[root@localhost conf]# openssl x509 -days 365 -req -in server.csr -signkey serve
r.key -out server.crt
Signature ok
subject=/C=XX/L=Default City/O=Default Company Ltd
Getting Private key
[root@localhost conf]#
```



3、将此服务器配置为 MYSQL 服务器，创建数据库为 userdatabase，在库中创建表为 username，在表中创建 5 个用户，分别为 myuser1、myuser2、myuser3、myuser4、myuser5，口令与用户名相同，需要对登录网站的用户进行身份验证，表结构如下：

字段名	数据类型	主键	自增
ID	int	是	是
name	varchar(10)	否	否
birthday	datetime	否	否
sex	char(1)	否	否
Password	Char（8）	否	否

```
mysql> create database userdatabase;
Query OK, 1 row affected (0.00 sec)

mysql> use userdatabase
Database changed
mysql> create table username(
    -> ID int primary key auto_increment,
    -> name varchar(10),
    -> birthday datetime,
    -> sex char(1),
    -> Password char(8));
Query OK, 0 rows affected (0.05 sec)

mysql> insert into username(name,Password)value("myuser1","myuser1");
Query OK, 1 row affected (0.00 sec)

mysql> insert into username(name,Password)value("myuser2","myuser2");
Query OK, 1 row affected (0.00 sec)

mysql> insert into username(name,Password)value("myuser3","myuser3");
Query OK, 1 row affected (0.00 sec)

mysql> insert into username(name,Password)value("myuser4","myuser4");
Query OK, 1 row affected (0.00 sec)

mysql> select * from username;
+----+---------+----------+------+----------+
| ID | name    | birthday | sex  | Password |
+----+---------+----------+------+----------+
|  1 | myuser1 | NULL     | NULL | myuser1  |
|  2 | myuser2 | NULL     | NULL | myuser2  |
|  3 | myuser3 | NULL     | NULL | myuser3  |
|  4 | myuser4 | NULL     | NULL | myuser4  |
+----+---------+----------+------+----------+
4 rows in set (0.00 sec)

mysql> _
```

4、在服务器端使用 iptables 设置防火墙功能，只允许用户访问这台服务器的 WWW 服务，而服务器只能被动地接受连接请求，不能主动的发起连接。

```
[root@localhost conf]# iptables -P OUTPUT DROP
[root@localhost conf]# iptables -I OUTPUT 1 -p tcp -m state --state=RELATED,ESTA
BLISHED --sport 80 --j ACCEPT
[root@localhost conf]# _
```

2015 年全国职业院校技能大赛

网络搭建与应用竞赛

(总分 1000 分)

赛题说明

一、竞赛内容分布

“网络搭建与应用”竞赛共分二个部分，其中：

第一部分：网络搭建及安全部署项目，占总分的比例为 45%；

第二部分：服务器配置及应用项目，占总分的比例为 55%；

二、竞赛注意事项

（1）禁止携带和使用移动存储设备、计算器、通信工具及参考资料。

（2）请根据大赛所提供的比赛环境，检查所列的硬件设备、软件清单、材料清单是否齐全，计算机设备是否能正常使用。

（3）本试卷共有两个部分。请选手仔细阅读比赛试卷，按照试卷要求完成各项操作。

（4）操作过程中，需要及时保存设备配置。比赛结束后，所有设备保持运行状态，不要拆、动硬件连接。

（5）比赛完成后，比赛设备、软件和赛题请保留在座位上，禁止将比赛所用的所有物品（包括试卷和草纸）带离赛场。

（6）所有需要提交的文档均放置在桌面的 SERVER1“比赛文档”文件夹中，禁止在纸质资料上填写与竞赛无关的标记，如违反规定，可视为 0 分。

（7）裁判以各参赛队提交的竞赛结果文档为主要评分依据。所有提交的文档必须按照赛题所规定的命名规则命名，文档中有对应题目的小标题，截图有截图的简要说明，否则按无效内容处理。

（8）与比赛相关的工具软件放置在 D 盘的 tools 文件夹中。

项目背景及网络拓扑

某集团公司在北京市设置总公司，在上海设置分公司，在重庆设立了办事处，为了实现快捷的信息交流和资源共享，需要构建一个跨越三地的集团网络。总公司有三个部门，分别为财务部、工程部、人事部三个部门，上海分公司设有行政部和销售部，重庆办事处设立了销售部和工程部。

具体的拓扑结构如下图所示：

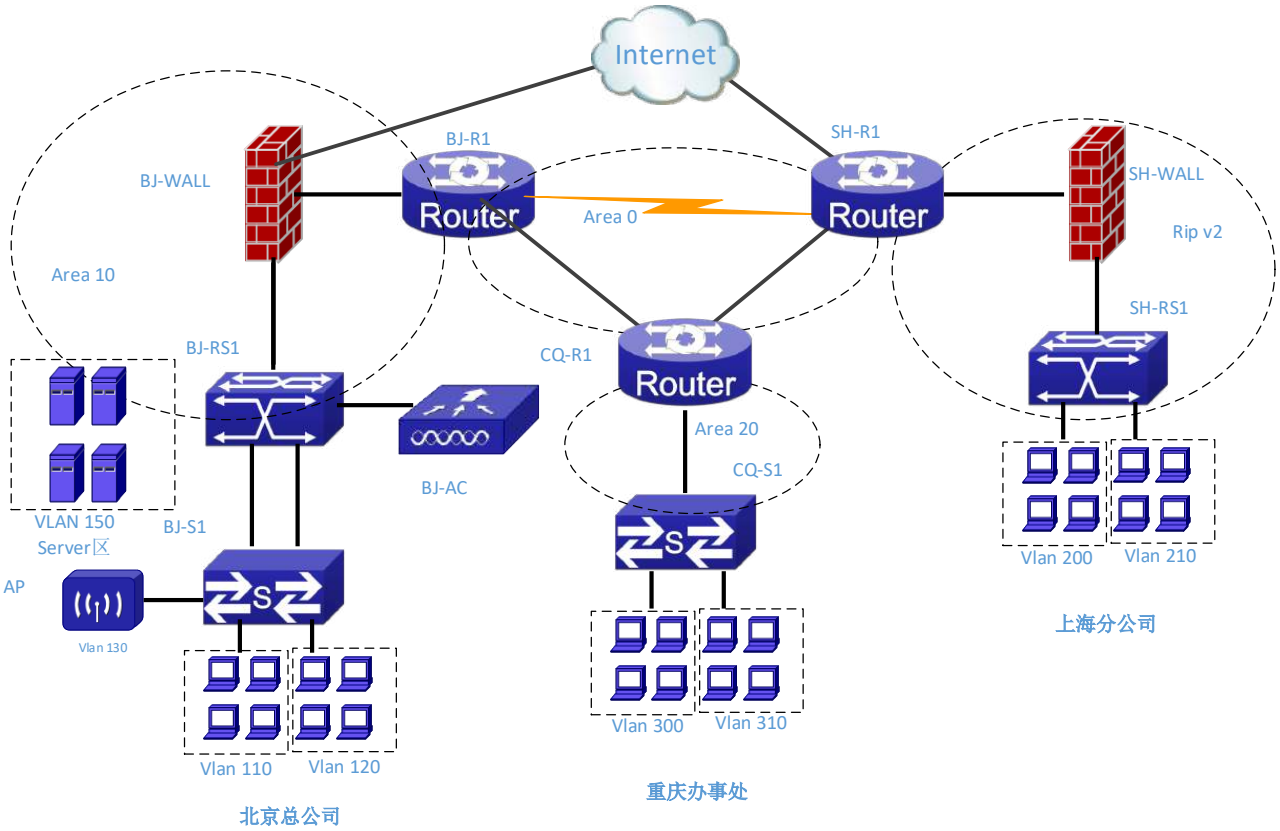


表 1 网络设备连接表

A 设备连接至 B 设备			
设备名称	**接口**	**设备名称**	**接口**
BJ-R1	S0/1	SH-R1	S0/2
BJ-R1	G0/3	CQ-R1	G0/3
BJ-R1	G0/4	BJ-WALL	E0/1
SH-R1	G0/3	CQ-R1	G0/4
SH-R1	G0/4	SH-WALL	E0/1
SH-R1	G0/5	BJ-WALL	E0/3
CQ-R1	G0/5	CQ-S1	E1/24
BJ-WALL	E0/2	BJ-RS1	E1/0/24
BJ-RS1	E1/0/21	BJ-S1	E1/21
BJ-RS1	E1/0/22	BJ-S1	E1/22
SH-WALL	E0/2	SH-RS1	E1/0/24
Server1	NIC	BJ-RS1	E1/0/2
Server 2	NIC	BJ-RS1	E1/0/3
Server 3	NIC	BJ-RS1	E1/0/4
Server4	NIC	BJ-RS1	E1/0/5

表 2 网络设备 IP 地址分配表

设备	设备名称	设备接口	IP 地址
路由器	BJ-R1	G0/3	10.1.0.17/30
		G0/4	19.1.1.1/30
		S0/1	10.1.0.30/30
	SH-R1	G0/3	10.1.0.2/30
		G0/4	19.1.3.1/30
		G0/5	211.1.1.2/24
		S0/2	10.1.0.29/30
	CQ-R1	G0/3	10.1.0.18/30
		G0/4	10.1.0.1/30
		G0/5.300	
		G0/5.310	
防火墙	BJ-WALL	E0/1	19.1.1.2/30
		E0/2	
	SH-WALL	E0/1	19.1.3.2/30
		E0/2	
		E0/3	211.1.1.1/24
三层交换机	BJ-RS1	E1/0/24(vlan100)	
		VLAN110(财务)	
		VLAN120(人事)	
		VLAN130(工程)	
		VLAN150	
	SH-RS1	VLAN200	
		VLAN210	
		E1/0/24(vlan100)	
无线网络	BJ-AC	子网 VLAN130	11.1.3.0/24

表 3：服务器 IP 地址分配表

宿主机	虚拟主机名称	域名信息	服务角色	系统及版本信息	IPv4 地址信息
Server 1	Win2003-A1	dc.2015Network.com	域控制器 DNS 服务器 CA 证书服务器	Windows Server 2003 R2	IP：10.100.100.1
	Win2008-A1	dhcp.2015Network.com	DHCP 服务器	Windows Server 2008 R2	IP：10.100.100.2
	Centos-A1	smb.jnds.net	SAMBA 共享服务器	Centos 6.5	IP：10.100.100.3
Server 2	Win2008-B1	ftp.2015Network.com	FTP 服务器	Windows Server 2008	IP：10.100.100.4

				R2	
	Centos-B1	raid.jnds.net	逻辑卷及磁盘阵列服务	Centos 6.5	IP：10.100.100.5
	Centos-B2	ftp.jnds.net ftp1.jnds.net ftp2.jnds.net	FTP 文件服务器	Centos 6.5	IP：10.100.100.105 IP：10.100.100.106 IP：10.100.100.107
Server 3	Win2003-C1	sh.2015Network.com mail.2015Network.com	子域控制器 EMAIL 服务器	Windows Server 2003 R2	IP：10.100.100.6
	Centos-C1	dns.jnds.net nfs.jnds.net	BIND 域名服务器 NFS 服务器	Centos 6.5	IP：10.100.100.109
Server 4 (Linux 虚拟化主机)	Centos-D1	www.jnds.net mysql.jnds.net	Apache web 服务器 MySQL 数据库服务器	Centos 6.5	IP：10.100.100.161

网络搭建部分(450 分)

【注意事项】

1、设备 console 线有两条。交换机， AC，防火墙使用同一条 console 线，路由器使用另外一条 console 线。

2、设备配置完毕后，保存最新的设备配置。保存文档方式分为两种：

a) 交换机和路由器要把 show running-config 的配置保存在 SERVER1 桌面的相应文档中，文档命名规则为：设备名称.doc,例如：RT1 路由器文件命名为：RT1.doc，然后放入到 SERVER1 桌面上“比赛文档”文件夹中

b) 防火墙等截图方式的设备，把截图的图片放到同一 word 文档中，文档命名规则为：设备名称.doc,例如：防火墙 FW1 文件命名为：FW1.doc, 保存后放入到 SERVER1 桌面上“比赛文档”文件夹中。

1、 物理连接与 IP 地址划分

(1) 按照网络拓扑图制作以太网网线，并连接设备。要求符合 T568A 和 T568B 的标准，其线缆长度适中。

(2) 根据“拓扑结构图”和“表 2:网络设备 IP 地址分配表”所示，对网络中的所有设备接口配置 IP 地址。

公司中整个用户地址规划使用 11.0.0.0/8 地址段，为了节省 IP 资源，做到合理分配，财务部(VLAN10)有 30 名员工、工程部(VLAN20)有 40 名员工、软件部(VLAN30)和系统集成部(VLAN40)两个部门都有 10 名员工。所有服务器的 IP 段为 10.100.100.0/24，所有设备互联地址使用/30 的掩码进行分配，并把地址填入上面网络设备 IP 地址分配表中的空白处。地址分配后把地址填入上面网络设备 IP 地址分配表中的空白处。

注意:

- 网关地址为网段的最后可用地址。

2、 交换机配置

(1) 为交换机设备命名，命名规则参考为表 1 中的“设备名称”。

(2) 在两台三层交换设备上开启 telnet 管理功能，要求每台网络设备只允许 15 条线路管理网络设备,口令为 2015telnet。Enable 密码为 2015telnet，enable 密码的加密方式为密文加密。

(3) 依据“拓扑结构图”和下表，把相应端口加入到 vlan 中。

设备	VLAN ID	接口
BJ-S1	110	E1/8-12
	120	E1/13-16
	130	E1/1-3
BJ-RS1	150	E1/0/2-5
SH-RS1	200	E1/0/2-10
	210	E1/0/11-20
CQ-S1	300	E1/2-10
	310	E1/11-20

(4) 使用端口汇聚技术，将 BJ-RS1 三层交换机接口 E1/0/21 和 E1/0/22 与 BJ-S1 二层交换机接口 E1/21 和 E1/22 配置为端口汇聚，汇聚接口为动态方式。

(5) 在 BJ-RS1 和 BJ-S1 上配置 MSTP，创建实例 10 和实例 20，将 VLAN110 和 120 加入到实例 10，vlan130 和 150 加入到实例 20，将 BJ-RS1 设置为根。

(6) 在 BJ-RS1 上配置 DHCP 服务，使得 VLAN120 自动获取 IP 地址，并指定网关。

(7) 在 BJ-RS1 上配置端口镜像，将流量映射到 E1/9 口上。

(8) 在 BJ-S1 的 E 1/5 上配置端口安全，安全 MAC 地址为：00-12-F1-00-ab-01。

(9) 在 CQ-S1 上配置流量控制，限制出口带宽为 5M，入口带宽为 2M。

(10) 在 SH - RS1 上设置交换机的端口安全，设置 VLAN210 的端口最多可以学习 5 个 MAC 地址，当学习到更多的 MAC 地址时，直接进行丢弃且不产生通知。

(11) 根据“网络拓扑结构图”所示，在三层交换机上配置路由协议。

3、 路由器配置与调试

(1) 为路由设备命名，命名规则参考为表 1 中的“设备名称”。

(2) 把下面的设备 RID 设置上，要求不能增加接口的相关信息。

设备名称	RID
BJ-R1	0.0.0.1
SH-R1	0.0.0.6
CQ-R1	0.0.0.7
BJ-WALL	0.0.0.2
SH-WALL	0.0.0.3
BJ-RS1	0.0.0.4
SH-RS1	0.0.0.5

(3) 根据“网络拓扑结构图”所示，在 BJ-R1、CQ-R1 和 SH-R1 上配置 OSPF 协议，配置基于接口验证功能，采用 MD5 方式。

(4) 根据“网络拓扑结构图”所示，在北京总公司内部配置 OSPF 路由协议。

(5) 在上海分公司采用 RIPv2 动态路由协议。

(6) 重庆办事处的路由器和交换机之间配置单臂路由。

(7) 在 SH-R1 上配置路由重分发，重分发到 OSFP 中的路由类型为 E1，度量值为 55。重分发到 RIP 中的路由度量值为 2。

(8) 在 SH-R1 上使用 QOS，使其对出接口 S0/2 的流量限制在 300kbps，没有超额的流量允许发送，超额的流量丢弃。对入接口 G0/4 的流量限制在 2Mbps,没有超额的流量允许发送，超额的流量丢弃。

4、 广域网配置

(1) 北京总公司与上海分公司之间申请串行链路专线 ，并采用 PPP 封装，chap 认证方式，用户名称为对端设备名称，密码：123456。

(2) 上海分公司通过外网口 IP 地址进行 NAT 映射.保证上海分公司可以正常上网。

5、 防火墙配置

(1) 把防火墙进行设备命名，命名规则参考为表 1 中的“设备名称”。

(2) 在 BJ-WALL 上配置 OSPF 路由协议。

(3) 在 BJ-WALL 上配置 NAT，实现内部网络（VLAN110、VLAN120、VLAN130）访问互联网，其使用合法的公网地址为 211.1.1.10~211.1.1.20。

(4) 实现将内网的 WEB、FTP（10.100.100.161、10.100.100.4）资源发布的互联上，其合法公网地址为 211.1.1.21/24。

(5) 配置远程访问 IPSec VPN，实现移动办公用户可以通过互联网安全访问内部服务器群 VLAN150 的 dns、ftp、http、https、ping、pop3、Smtp 等服务，其分配的地址池为 10.1.4.0/24，创建五个用户，并将用户绑定到固定的 IP 地址。

(6) SH-WALL 上配置路由协议。

(7) SH-WALL 为了保证带宽的正常使用，限制 P2P 应用的下行带宽最高为 10M。

6、 无线配置

(1) 通过 AC 配置 用户接入无线网络时 SSID 为 VLAN130

(2) 通过 AC 配置配置 DHCP 功能，地址范围为（10.1.3.10~10.1.3.200）

(3) 通过 AC 配置采用 WEP 加密方式，加密口令为 1234567890

Windows 操作系统

【说 明】

（1）题目中所涉及 Windows 操作系统的 administrator 管理员以及其他普通用户密码均为 2015Netw1rk（注意区分大小写），若未按照要求设置密码，涉及到该操作的所有分值记为 0 分。

（2）虚拟主机的 IP 属性设置请按照网络拓扑结构图以及“表 3：服务器 IP 地址分配表”的要求设定。

（3）除非作特殊说明，在同一主机下需要安装相同操作系统版本的虚拟机时，可采用 Oracle VM VirtualBox 软件自带的克隆系统功能实现。

（4）所有系统镜像文件及试题所需的其它软件均存放在每台主机的 D:\soft 文件夹中，并将题目要求的截图内容以.jpg 格式存储于桌面 BACKUP 文件夹中。

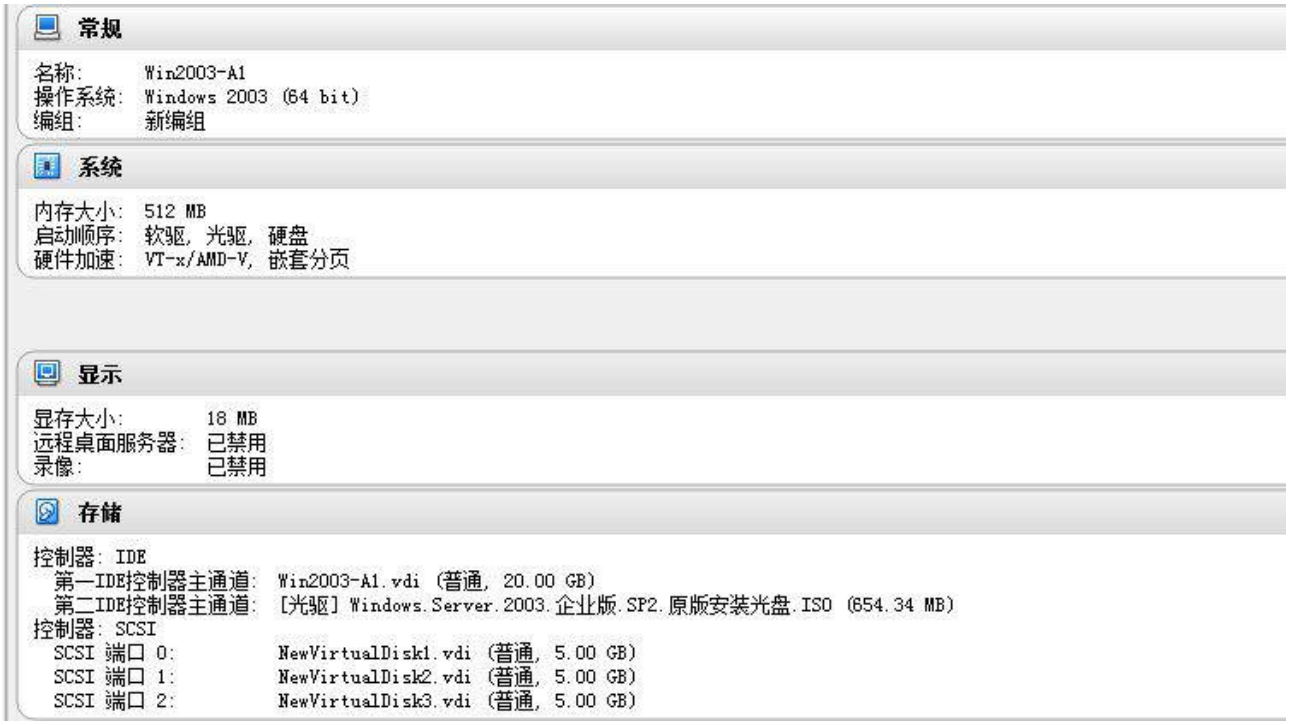
（5）题目要求的虚拟机均安装于每台主机的 D：\virtualPC 目录，即路径为 D：\virtualPC\虚拟主机名称。

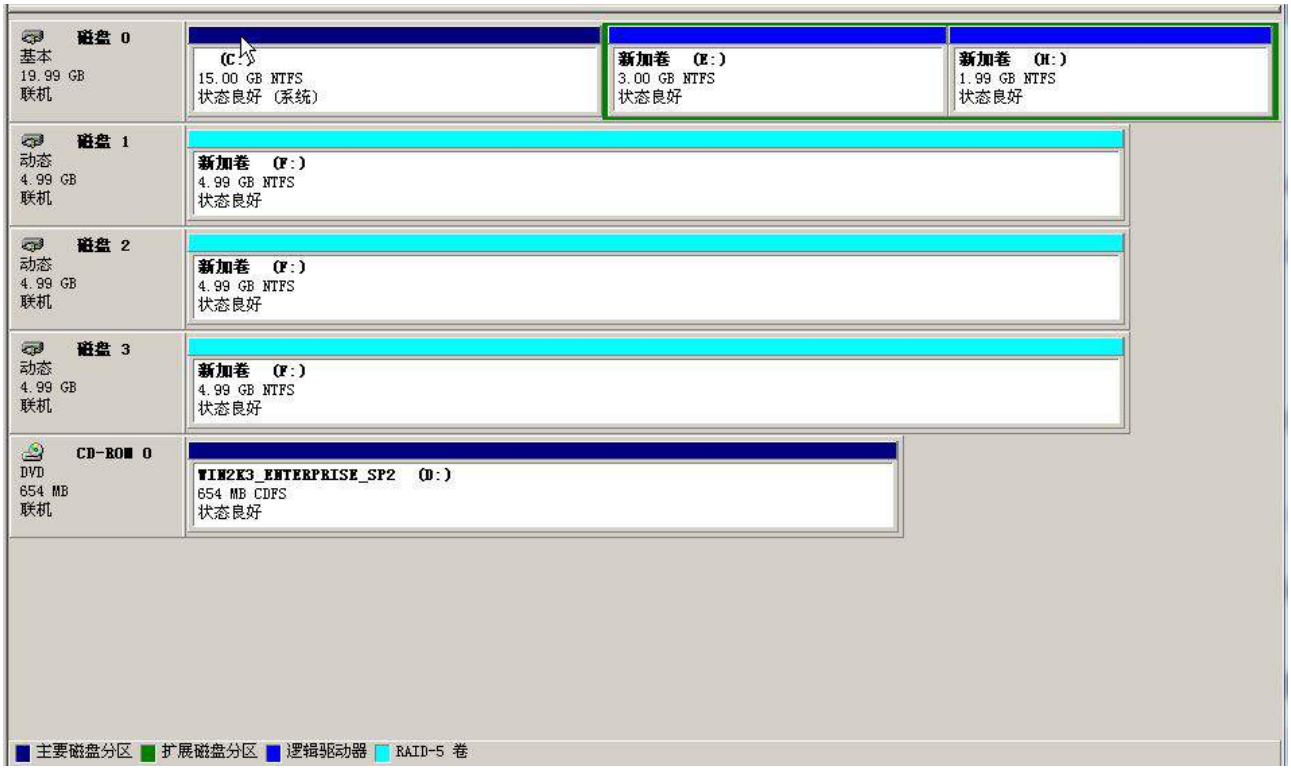
一、在 Server 1 上完成如下操作:

（一）完成虚拟主机的创建

1、安装虚拟机“Win2003-A1”，具体要求为内存为 512M，硬盘 20G，网卡为桥接模式；虚拟机分区分别为主分区 15GB，扩展分区 5GB。分为两个逻辑分区，大小分别为 3GB 和 2GB。

2、在虚拟机“Win2003-A1”中添加 SCSI 控制器，再添加三块 SCSI 虚拟硬盘，其每块硬盘的大小为 5G；制作成一个 RAID-5 卷，磁盘盘符为 F:\。

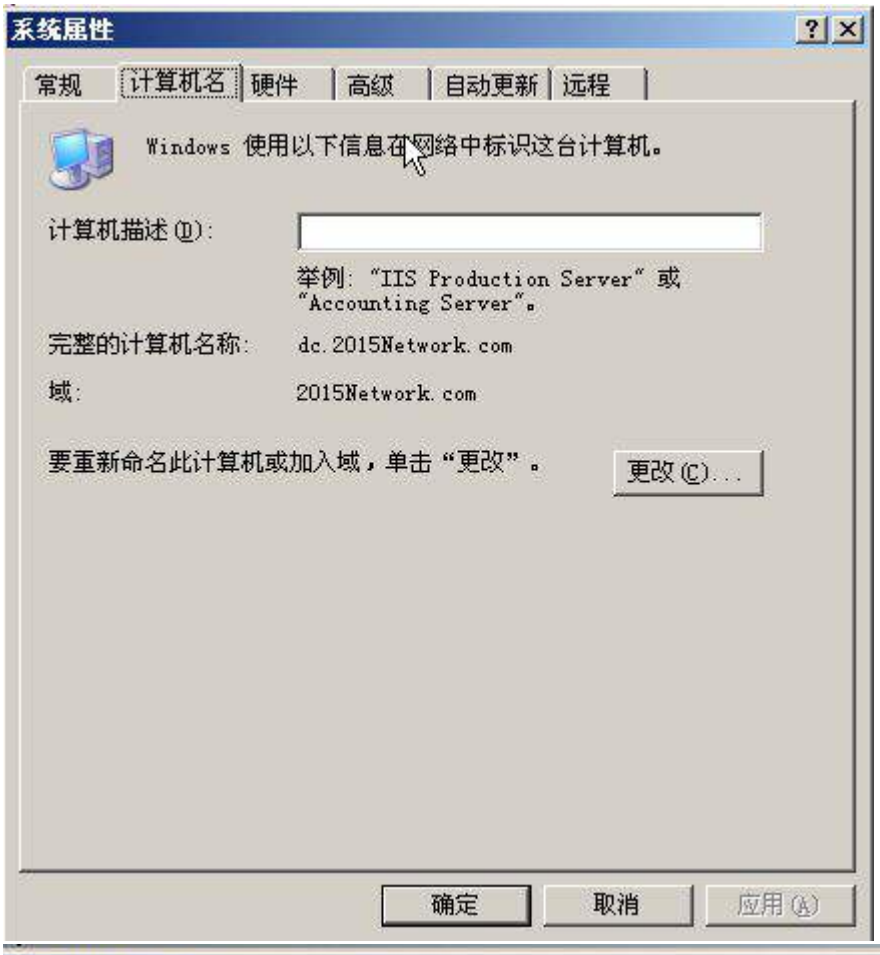




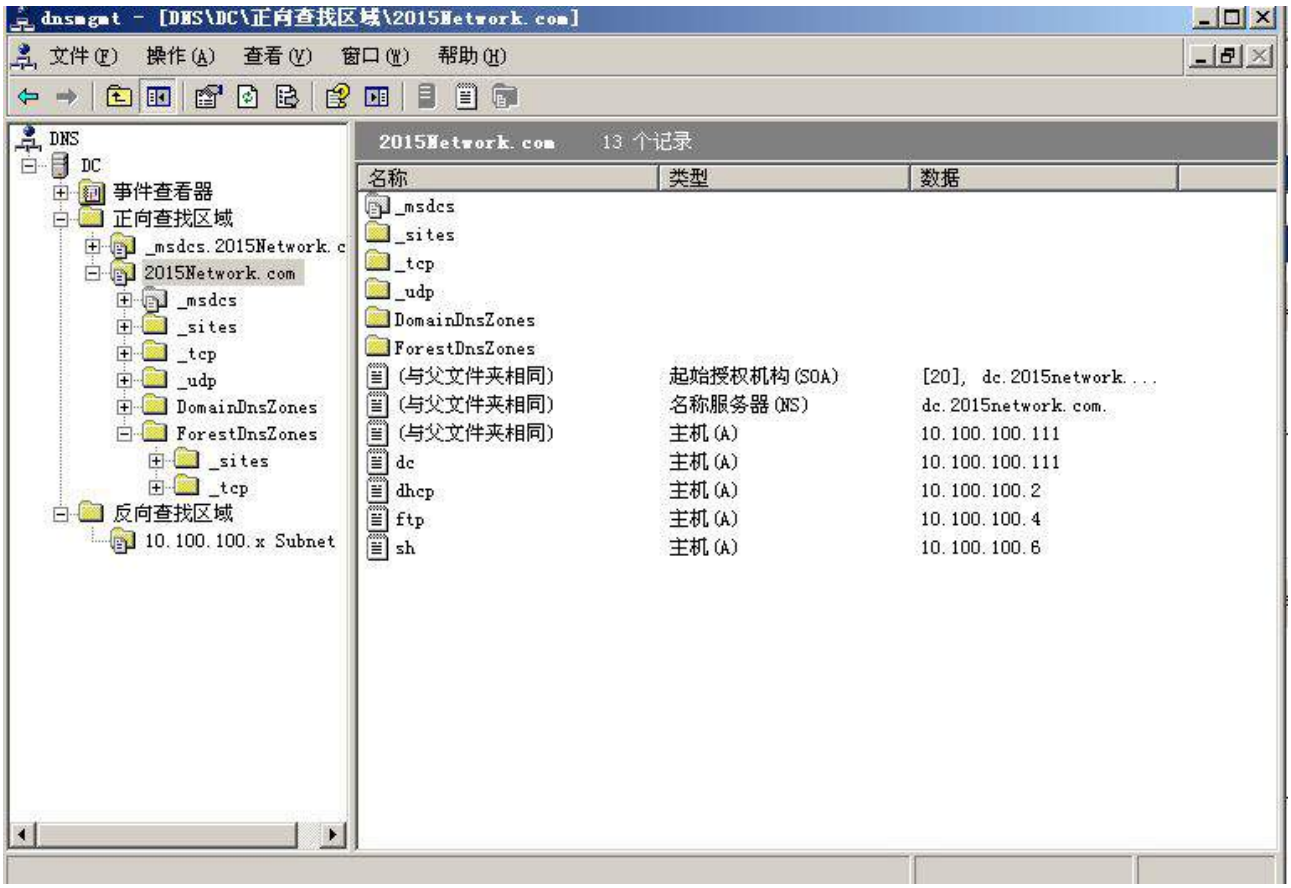
3、安装虚拟机“Win2008-A1”，具体要求为内存为 1G，硬盘 20G，并将该虚拟机加入到域中。

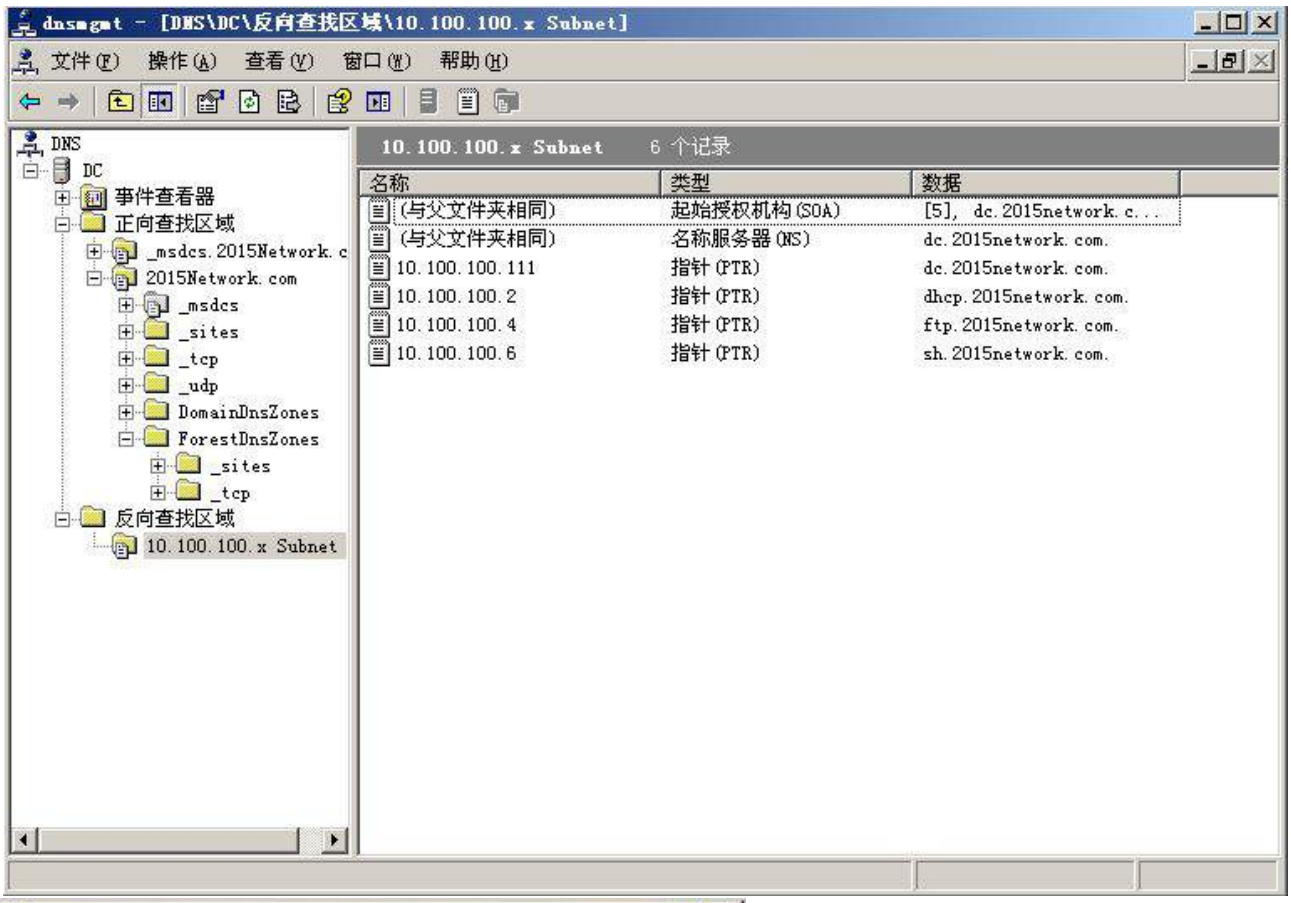
（二）在主机 Win2003-A1 中完成域控制器的部署

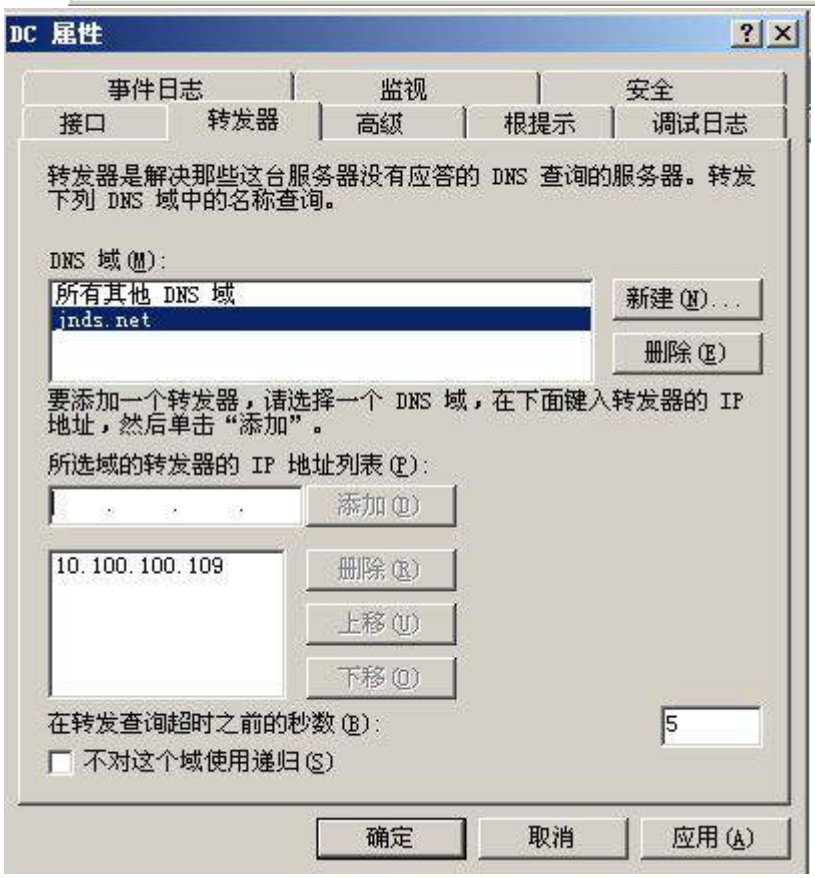
1、将在虚拟机“Win2003-A1” 配置为主域控制器。域名为 2015Network.com，NetBIOS 域名为 2015Network，服务器的 FQDN 为 dc.2015Network.com，域的功能级别为 2003 模式。同时，该服务器为 DNS 服务器，负责解析 2015Network.com 域名。实现 DNS 转发功能。


系统属性
常规
计算机名
硬件
高级
自动更新
远程
Windows 使用以下信息在网络中标识这台计算机。
计算机描述(D):
举例: "IIS Production Server" 或 "Accounting Server"。
完整的计算机名称: dc.2015Network.com
域: 2015Network.com
要重新命名此计算机或加入域，单击"更改"。
更改(C)...
确定
取消
应用(A)

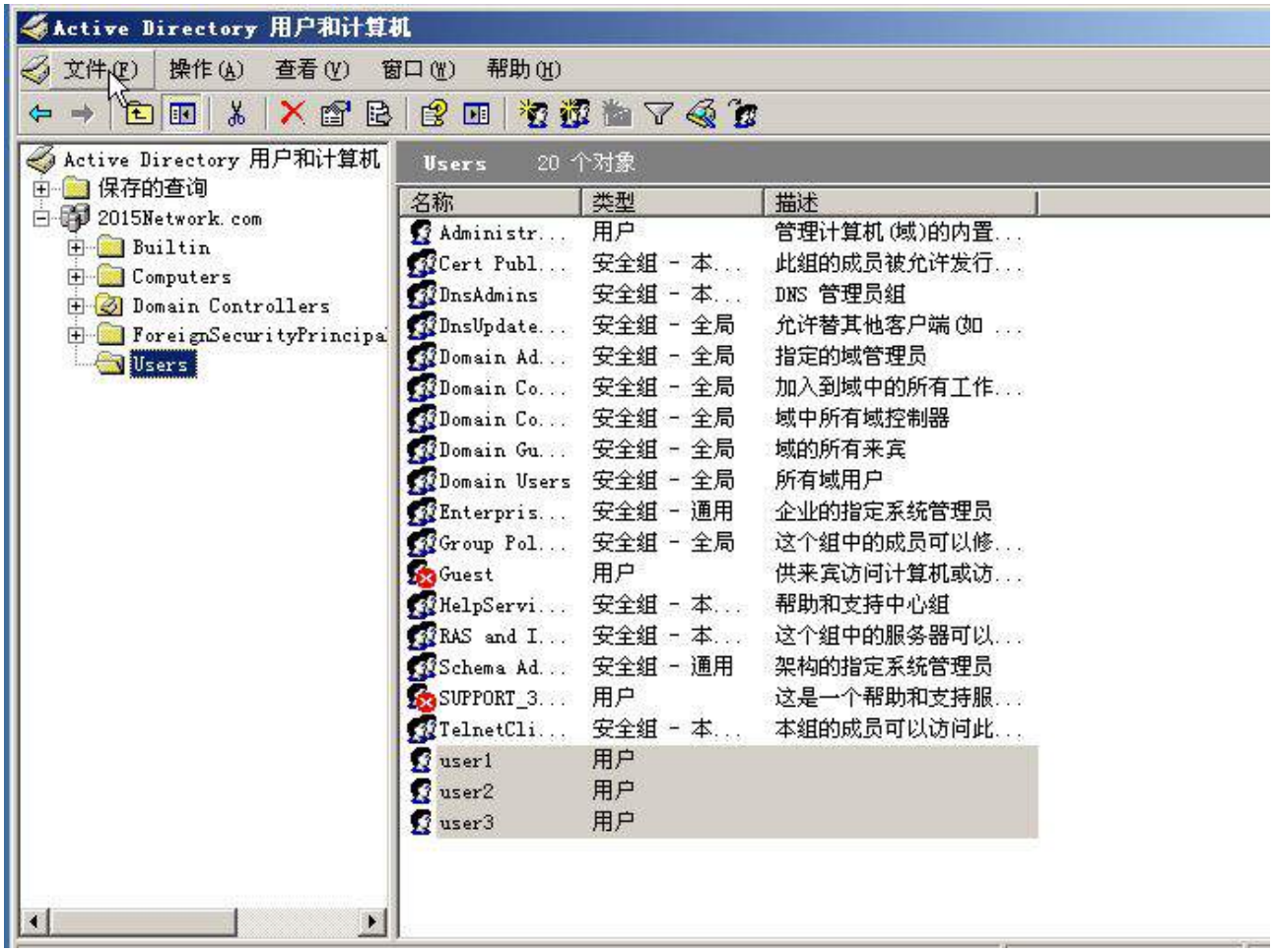

提升域功能级别
域名:
2015Network.com
当前域功能级别:
Windows Server 2003
此域处于允许范围内最高的功能级别操作状态。有关域功能级别的详细信息，请单击"帮助"。
关闭
帮助(H)

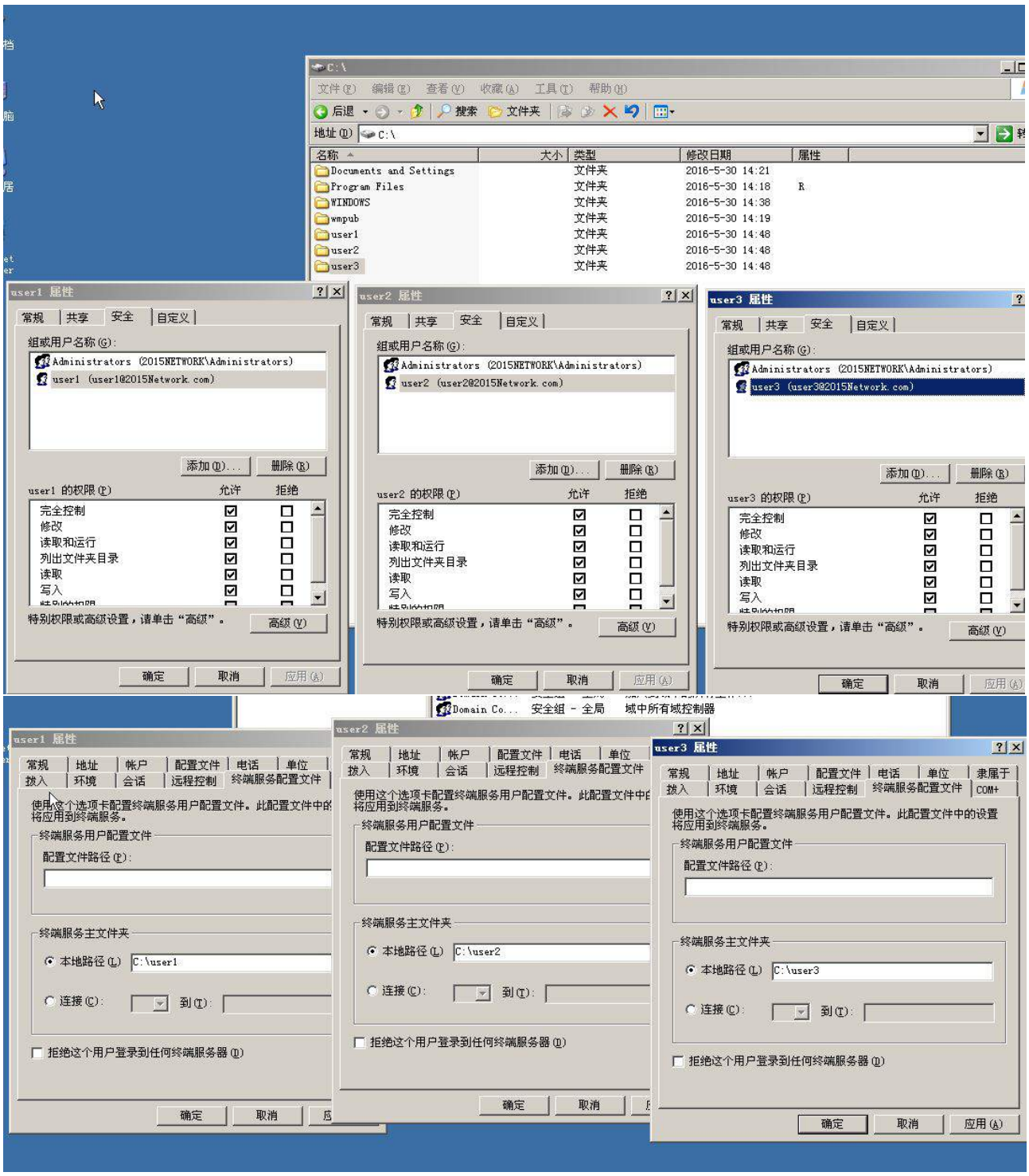

dnsmgmt - [DNS\DC\正向查找区域\2015Network.com]
文件(F) 操作(A) 查看(V) 窗口(W) 帮助(H)
DNS
DC
事件查看器
正向查找区域
_msdcs.2015Network.c
2015Network.com
_msdcs
_sites
_tcp
_udp
DomainDnsZones
ForestDnsZones
_sites
_tcp
反向查找区域
10.100.100.x Subnet
2015Network.com 13 个记录
名称 类型 数据
_msdcs
_sites
_tcp
_udp
DomainDnsZones
ForestDnsZones
(与父文件夹相同) 起始授权机构(SOA) [20], dc.2015network....
(与父文件夹相同) 名称服务器(NS) dc.2015network.com.
(与父文件夹相同) 主机(A) 10.100.100.111
dc 主机(A) 10.100.100.111
dhcp 主机(A) 10.100.100.2
ftp 主机(A) 10.100.100.4
sh 主机(A) 10.100.100.6


dnsmgmt - [DNS\DC\反向查找区域\10.100.100.x Subnet]
文件(F) 操作(A) 查看(V) 窗口(W) 帮助(H)
DNS
DC
事件查看器
正向查找区域
_msdcs.2015Network.c
2015Network.com
_msdcs
_sites
_tcp
_udp
DomainDnsZones
ForestDnsZones
_sites
_tcp
反向查找区域
10.100.100.x Subnet
10.100.100.x Subnet 6 个记录
名称 类型 数据
(与父文件夹相同) 起始授权机构(SOA) [5], dc.2015network.c...
(与父文件夹相同) 名称服务器(NS) dc.2015network.com.
10.100.100.111 指针(PTR) dc.2015network.com.
10.100.100.2 指针(PTR) dhcp.2015network.com.
10.100.100.4 指针(PTR) ftp.2015network.com.
10.100.100.6 指针(PTR) sh.2015network.com.

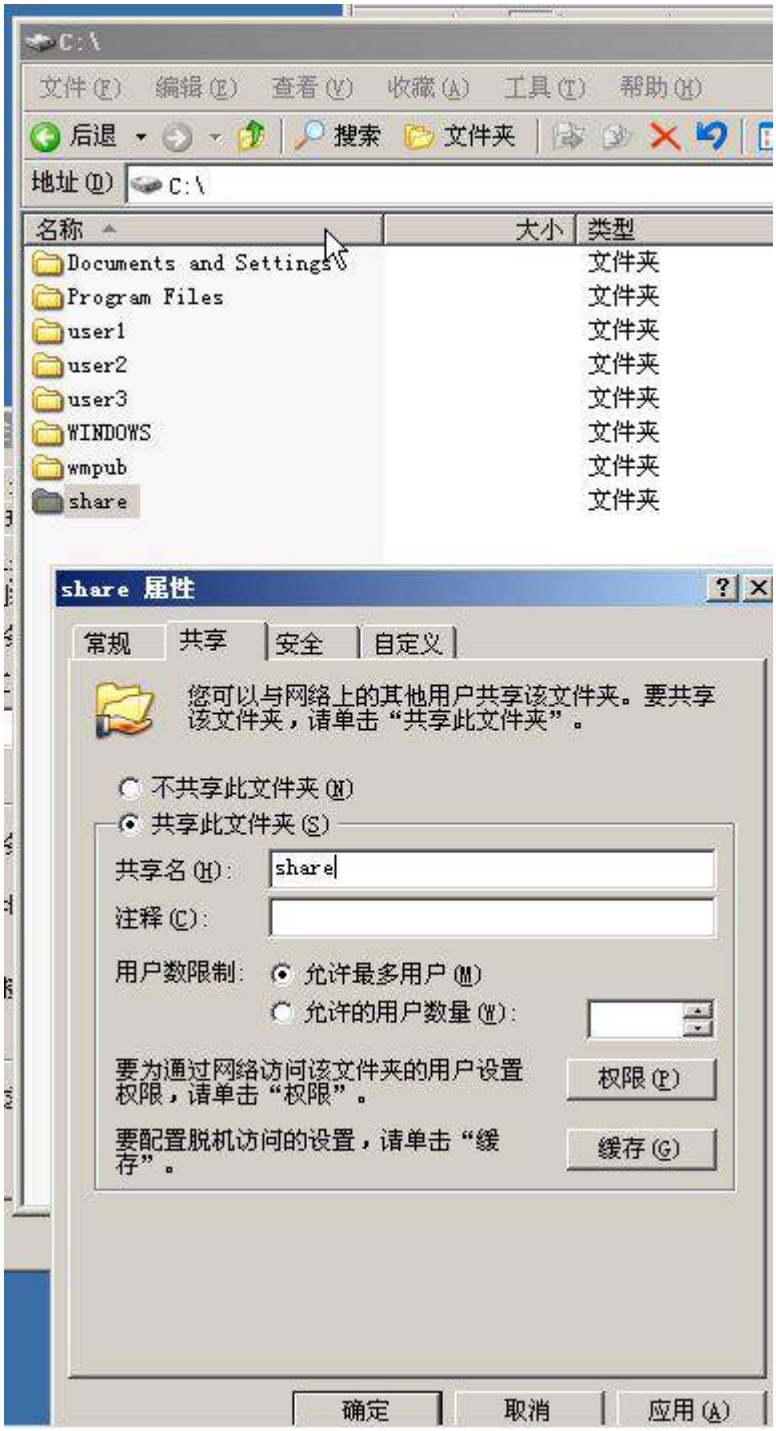

DC 属性
事件日志 监视 安全
接口 转发器 高级 根提示 调试日志
转发器是解决那些这台服务器没有应答的 DNS 查询的服务器。转发下列 DNS 域中的名称查询。
DNS 域(M):
所有其他 DNS 域
jnds.net
新建(N)...
删除(E)
要添加一个转发器，请选择一个 DNS 域，在下面键入转发器的 IP 地址，然后单击“添加”。
所选域的转发器的 IP 地址列表(P):
添加(D)
10.100.100.109
删除(R)
上移(U)
下移(O)
在转发查询超时之前的秒数(B):
5
不对这个域使用递归(S)
确定 取消 应用(A)

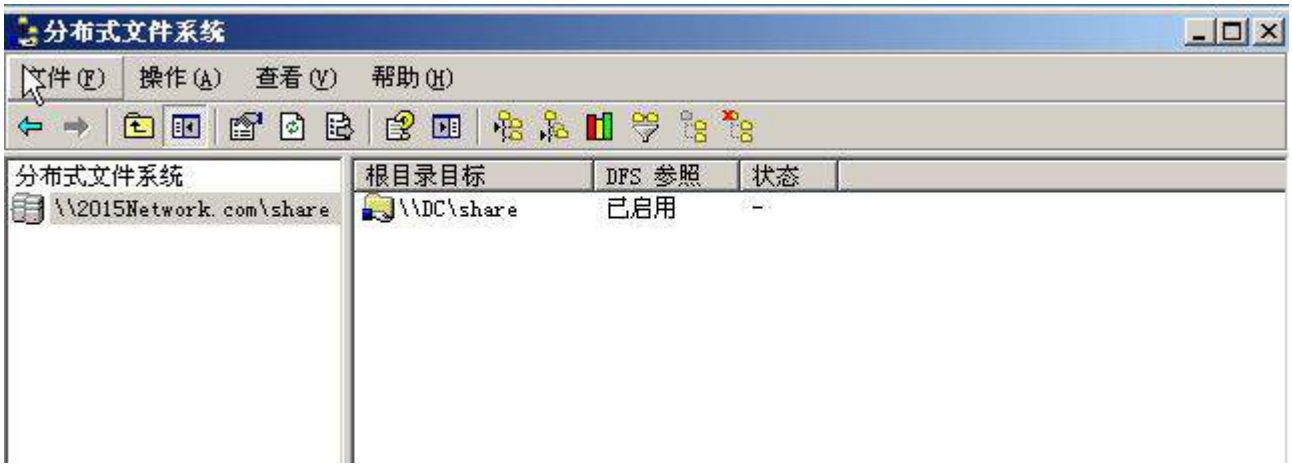
2、在计算机中添加 user1,user2,user3 用户，并在 C：\建立三个文件夹 user1,user2,user3，每个用户只能将文件保存在自己的文件夹中，并不能让其他用户访问自己的文件夹。



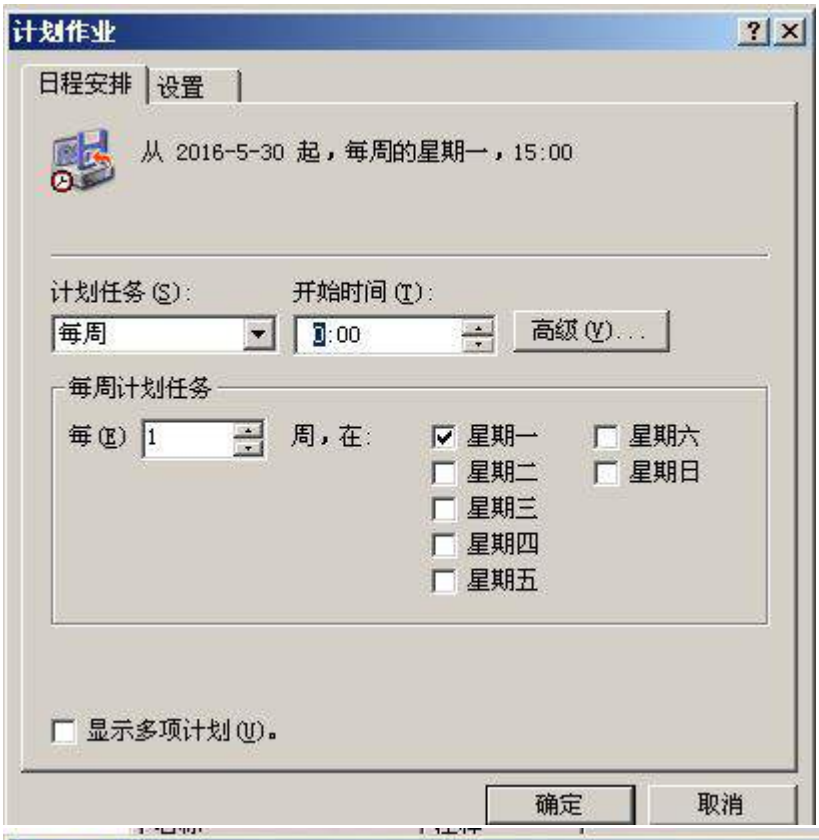

C:\
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
后退 搜索 文件夹
地址(D) C:\
名称 大小 类型 修改日期 属性
Documents and Settings 文件夹 2016-5-30 14:21
Program Files 文件夹 2016-5-30 14:18 R
WINDOWS 文件夹 2016-5-30 14:38
wmpub 文件夹 2016-5-30 14:19
user1 文件夹 2016-5-30 14:48
user2 文件夹 2016-5-30 14:48
user3 文件夹 2016-5-30 14:48
user1 属性
常规 共享 安全 自定义
组或用户名称(G):
Administrators (2015NETWORK\Administrators)
user1 (user1@2015Network.com)
添加(D)... 删除(R)
user1 的权限(P) 允许 拒绝
完全控制
修改
读取和运行
列出文件夹目录
读取
写入
特别权限或高级设置，请单击“高级”。
高级(V)
确定 取消 应用(A)
user2 属性
常规 共享 安全 自定义
组或用户名称(G):
Administrators (2015NETWORK\Administrators)
user2 (user2@2015Network.com)
添加(D)... 删除(R)
user2 的权限(P) 允许 拒绝
完全控制
修改
读取和运行
列出文件夹目录
读取
写入
特别权限或高级设置，请单击“高级”。
高级(V)
确定 取消 应用(A)
user3 属性
常规 共享 安全 自定义
组或用户名称(G):
Administrators (2015NETWORK\Administrators)
user3 (user3@2015Network.com)
添加(D)... 删除(R)
user3 的权限(P) 允许 拒绝
完全控制
修改
读取和运行
列出文件夹目录
读取
写入
特别权限或高级设置，请单击“高级”。
高级(V)
确定 取消 应用(A)
Domain Co... 安全组 - 全局 域中所有域控制器
user1 属性
常规 地址 帐户 配置文件 电话 单位
拨入 环境 会话 远程控制 终端服务配置文件
使用这个选项卡配置终端服务用户配置文件。此配置文件中的设置将应用到终端服务。
终端服务用户配置文件
配置文件路径(P):
终端服务主文件夹
本地路径(L) C:\user1
连接(C): 到(T):
拒绝这个用户登录到任何终端服务器(D)
确定 取消
user2 属性
常规 地址 帐户 配置文件 电话 单位
拨入 环境 会话 远程控制 终端服务配置文件
使用这个选项卡配置终端服务用户配置文件。此配置文件中的设置将应用到终端服务。
终端服务用户配置文件
配置文件路径(P):
终端服务主文件夹
本地路径(L) C:\user2
连接(C): 到(T):
拒绝这个用户登录到任何终端服务器(D)
确定 取消
user3 属性
常规 地址 帐户 配置文件 电话 单位 隶属于
拨入 环境 会话 远程控制 终端服务配置文件 COM+
使用这个选项卡配置终端服务用户配置文件。此配置文件中的设置将应用到终端服务。
终端服务用户配置文件
配置文件路径(P):
终端服务主文件夹
本地路径(L) C:\user3
连接(C): 到(T):
拒绝这个用户登录到任何终端服务器(D)
确定 取消 应用(A)

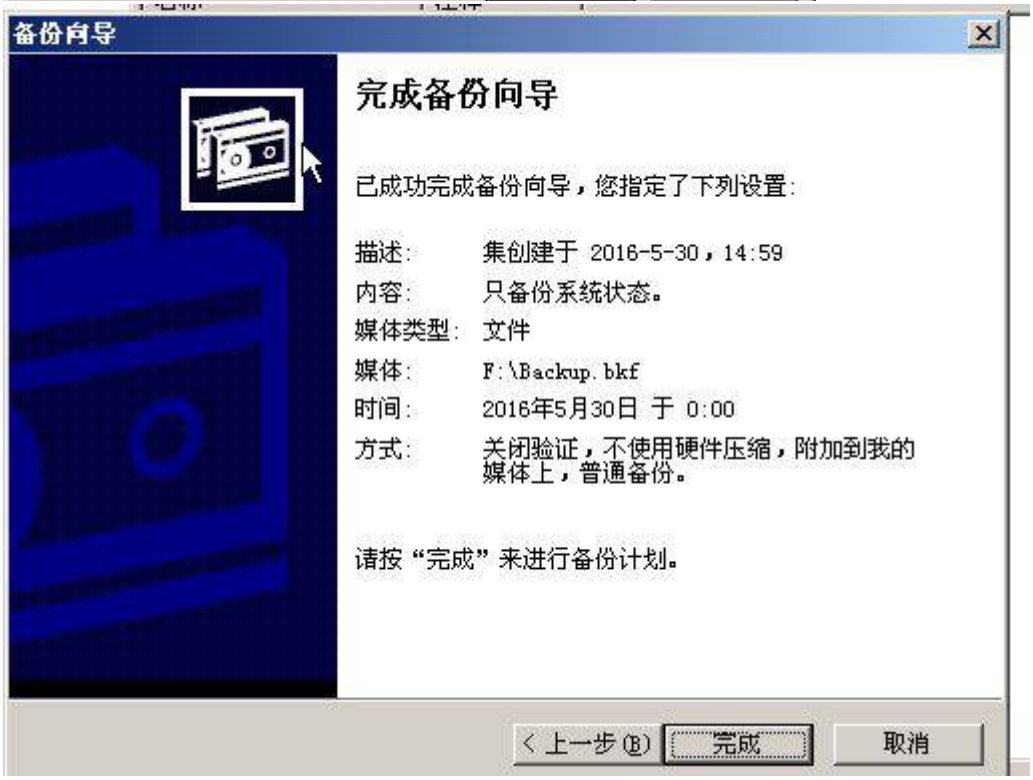
3、在 C：\下建立一个共享文件夹 share，并在活动目录中将此共享文件夹发布。

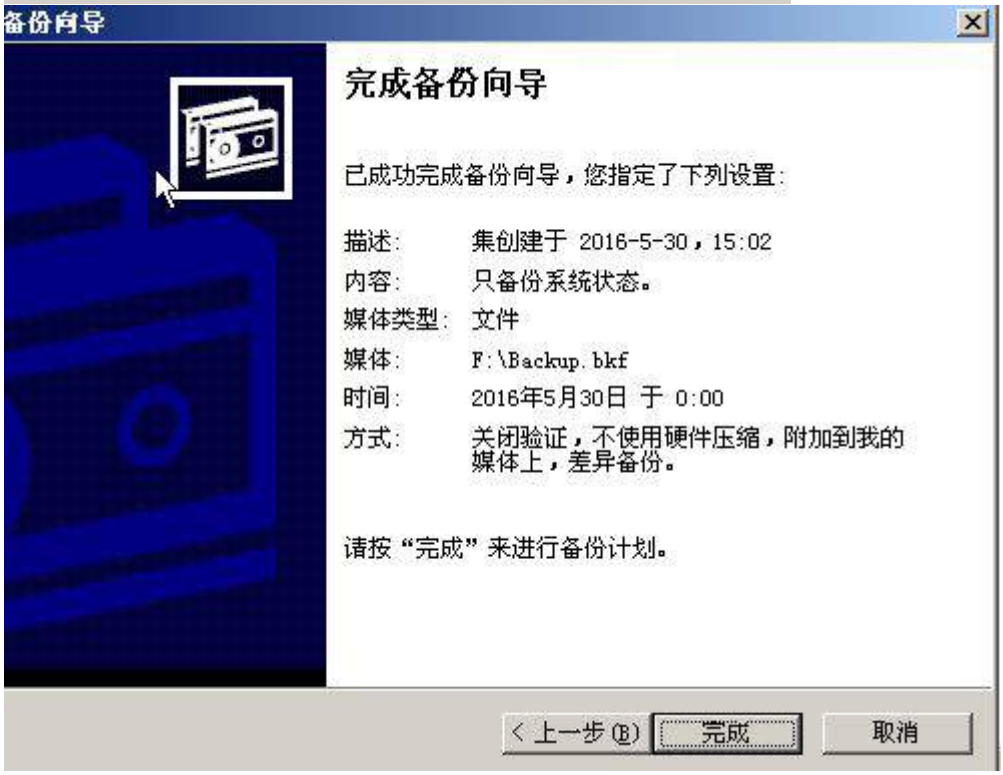




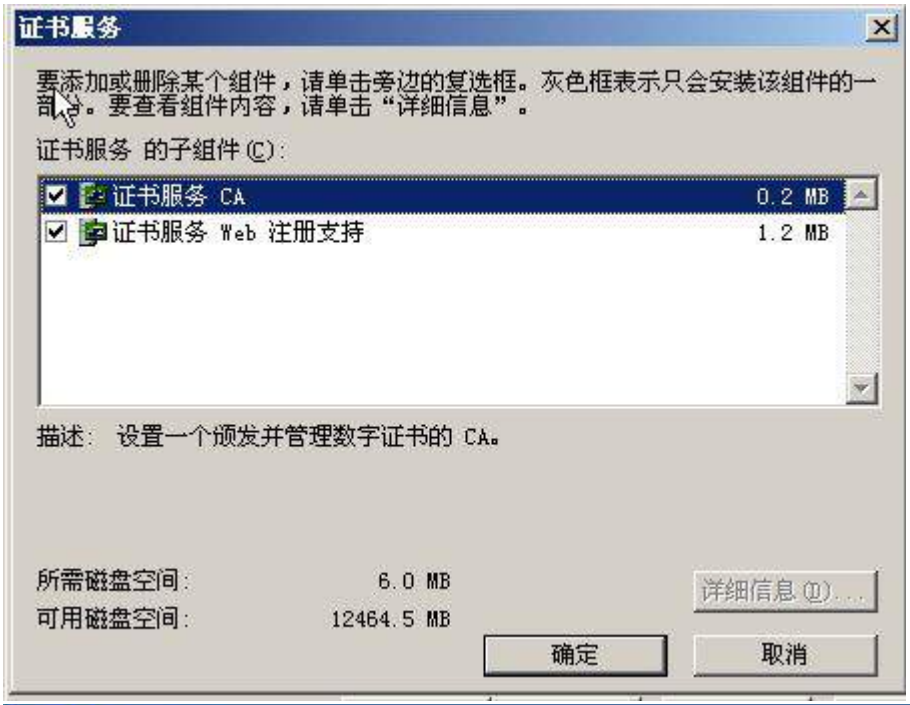
4、制定备份计划，每周一的午夜 0 点对活动目录进行正常备份，每周二至周五的午夜 0 点对活动目录进行差异备份，并将备份放置在 RAID5 卷中。

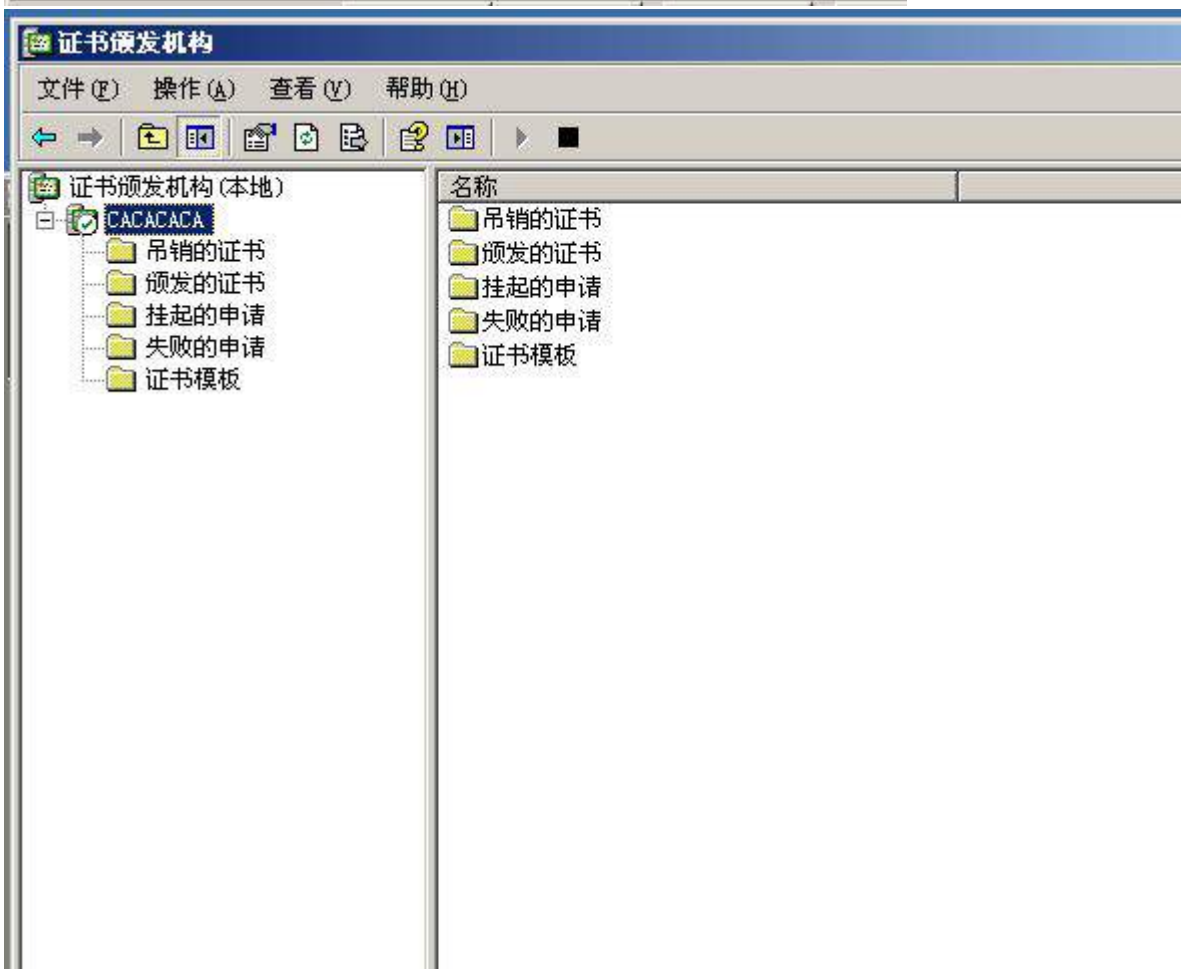

计划作业
日程安排
设置
从 2016-5-30 起，每周的星期一，15:00
计划任务(S):
开始时间(T):
每周
1:00
高级(V)...
每周计划任务
每(E) 1
周，在:
星期一
星期二
星期三
星期四
星期五
星期六
星期日
显示多项计划(U)。
确定
取消


备份向导
完成备份向导
已成功完成备份向导，您指定了下列设置:
描述: 集创建于 2016-5-30，14:59
内容: 只备份系统状态。
媒体类型: 文件
媒体: F:\Backup.bkf
时间: 2016年5月30日 于 0:00
方式: 关闭验证，不使用硬件压缩，附加到我的媒体上，普通备份。
请按“完成”来进行备份计划。
< 上一步(B)
完成
取消



5、在此域控制器上安装证书 CA 服务，并要求能够通过 WEB 申请证书。

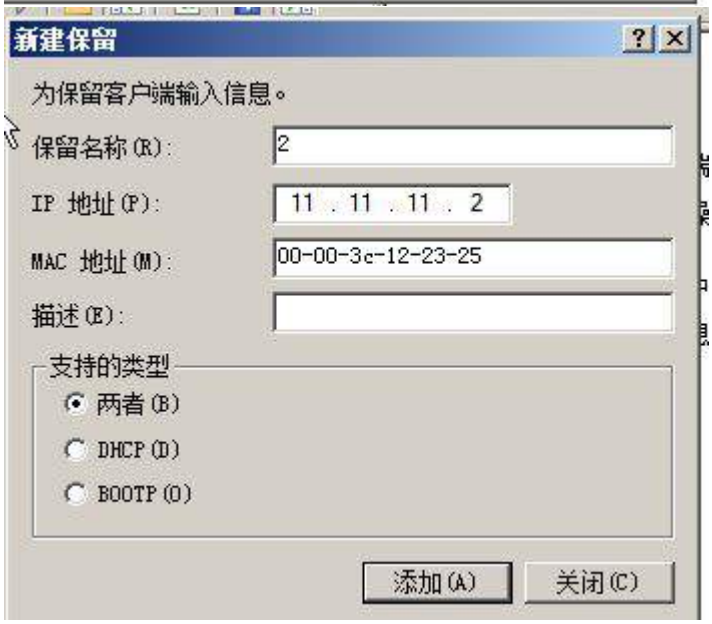




（三）在主机 Win2008-A1 中完成 DHCP 服务器的部署

1、为财务部的 VLAN 110 用户分配 IP 地址，创建 IP 作用域为相应 VLAN 号，DNS 和网关根据需求指定，租约期限为 30 天。

2、将财务部 VLAN 的第一个可用 IP 与 MAC 地址：00-00-3c-12-23-24 绑定，将财务部 VLAN 的第二个可用 IP 与 MAC 地址：00-00-3c-12-23-25 绑定。



二、在 Server 2 上完成如下操作:

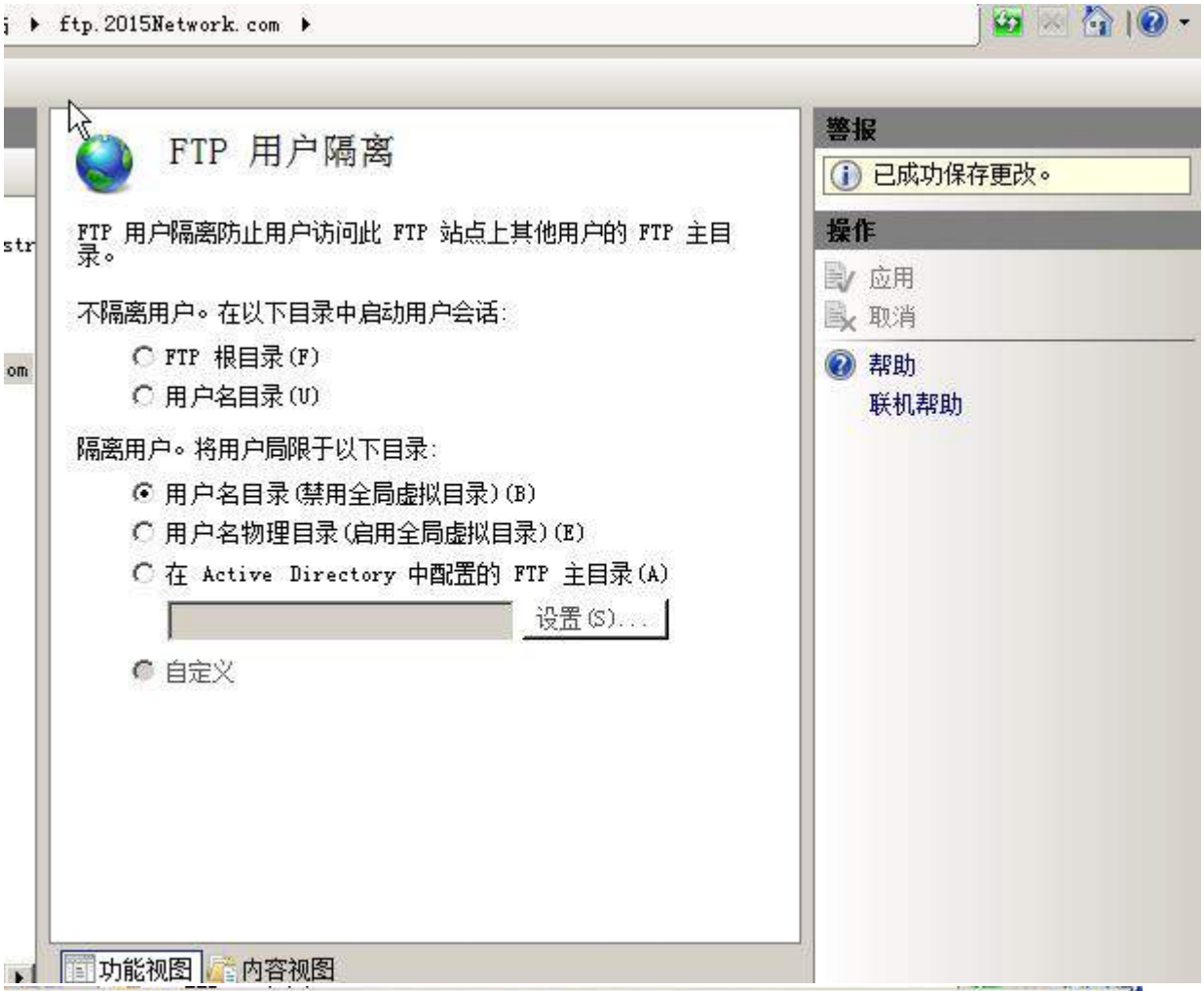
（一）完成虚拟主机的创建

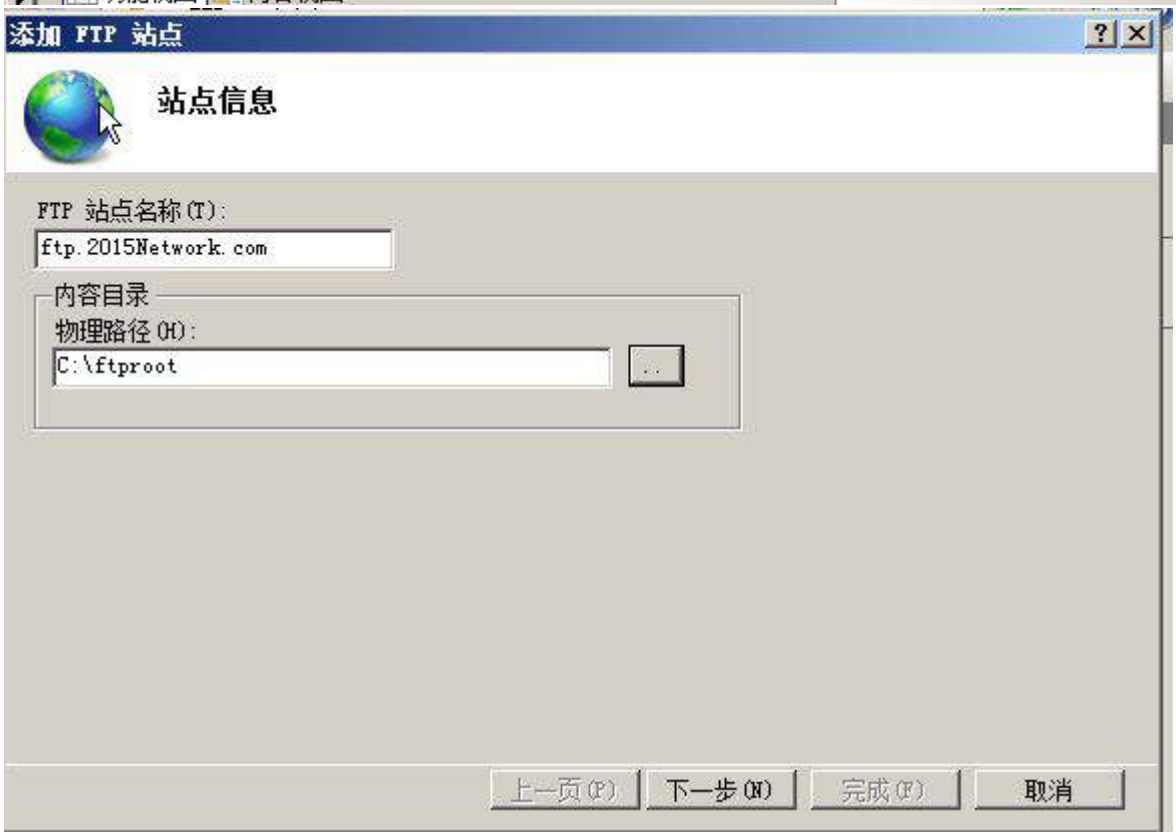
1、安装虚拟机“Win2008-B1”， 其内存为 1G，硬盘 20G，将服务器加入至 Windows 域中;

（二）在主机 Win2008-B1 中完成 FTP 服务器的部署

1、以隔离用户方式创建名为 ftp.2015Network.com 的 FTP 站点，FTP 主目录路径为 c:\ ftproot；创建文件夹 ftp1 和 ftp2，使得用户 ftp1 仅对文件夹 ftp1 有读写权限、用

户 ftp2 仅对文件夹 ftp2 有读写权限。





三、在 Server 3 上完成如下操作:

（一）完成虚拟主机的创建

1、在虚拟机“Win2003-C1”，其内存为 1G，硬盘 20G，并将服务器加入到 Windows 域环境;

常规

名称: Win2003-C1
操作系统: Windows 2003 (64 bit)
编组: 新编组

系统

内存大小: 1024 MB
启动顺序: 软驱, 光驱, 硬盘
硬件加速: VT-x/AMD-V, 嵌套分页

显示

显存大小: 18 MB
远程桌面服务器: 已禁用
录像: 已禁用

存储

控制器: IDE
第一IDE控制器主通道: Win2003-C1.vdi (普通, 20.00 GB)
第二IDE控制器主通道: [光驱] Windows.Server.2003.企业版.SP2.原版安装光盘.ISO (654.34 MB)

声音

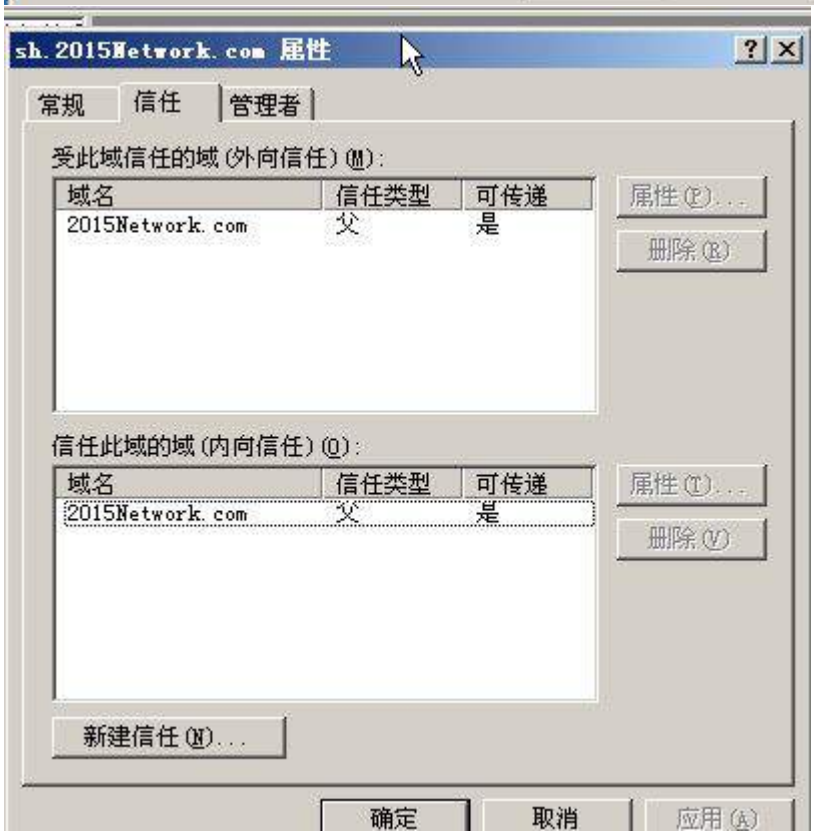
主机音频驱动: Windows DirectSound
控制芯片: Intel HD 音频

网络

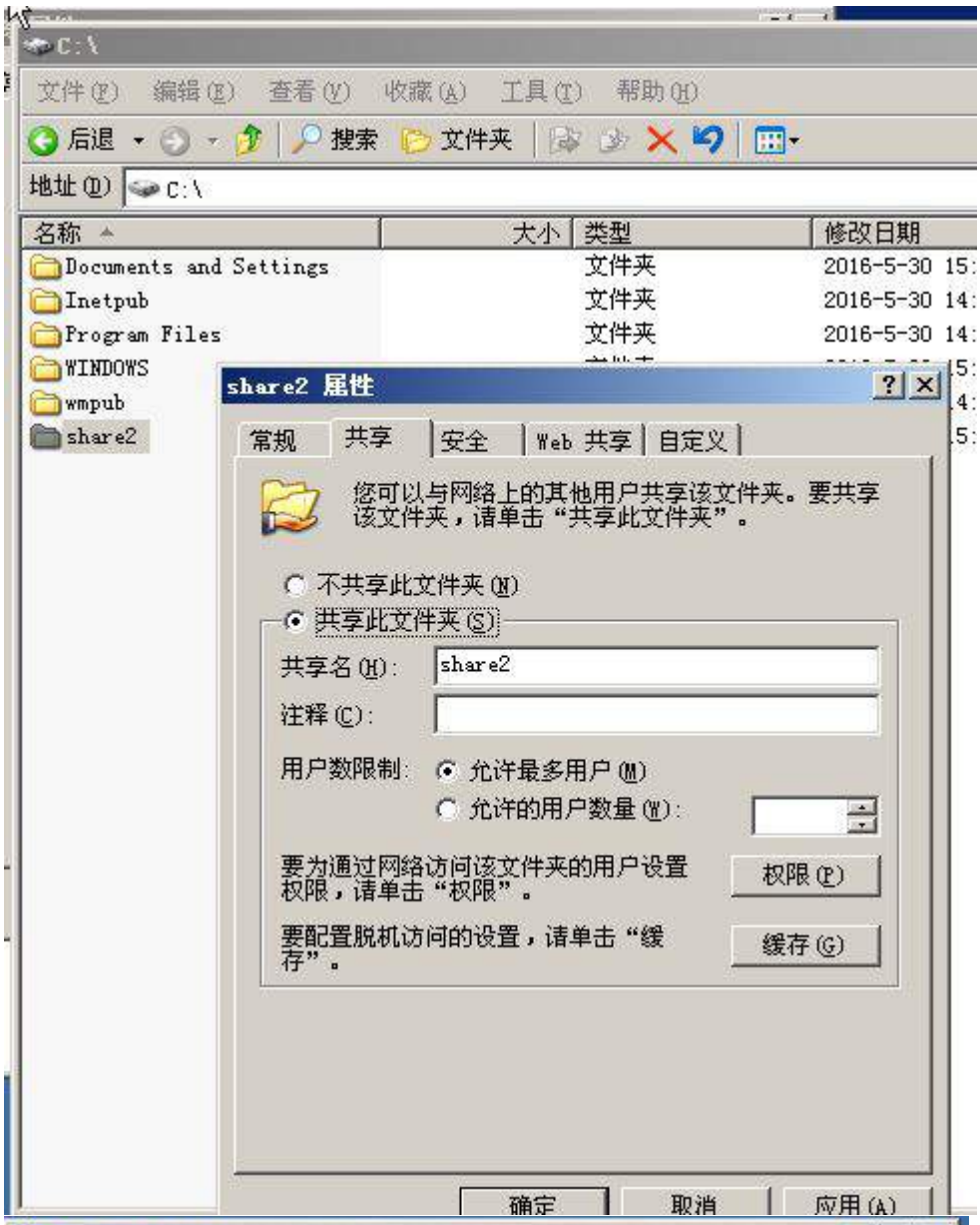
网卡 1: Intel PRO/1000 MT 桌面 (桥接网络, Intel(R) Ethernet Connection I217-LM)

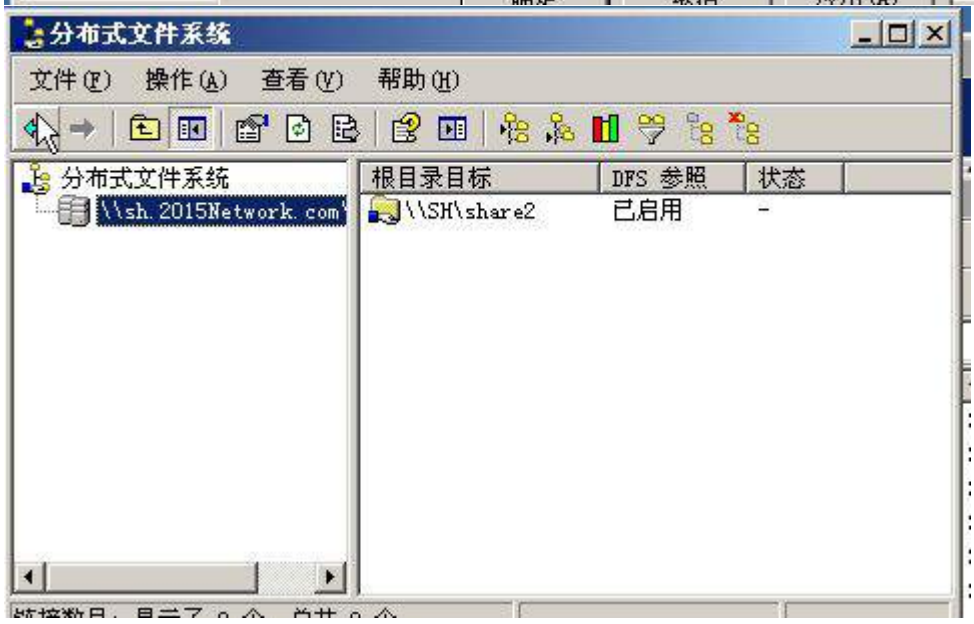
(二) 在主机 Win2003-C1 中完成域控制器的部署

1、创建新林中的新域，域名 sh.2015Network.com，并要求与域 dc.2015Network.com 建立双向信任与委托关系；



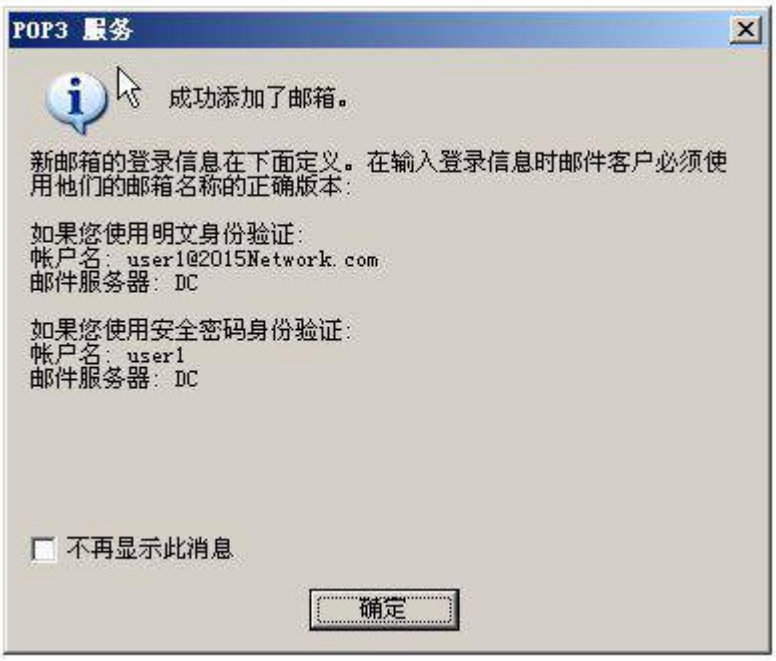
2、在域 sh.2015Network.com 上建立共享文件夹 share2，并发布到活动目录中。

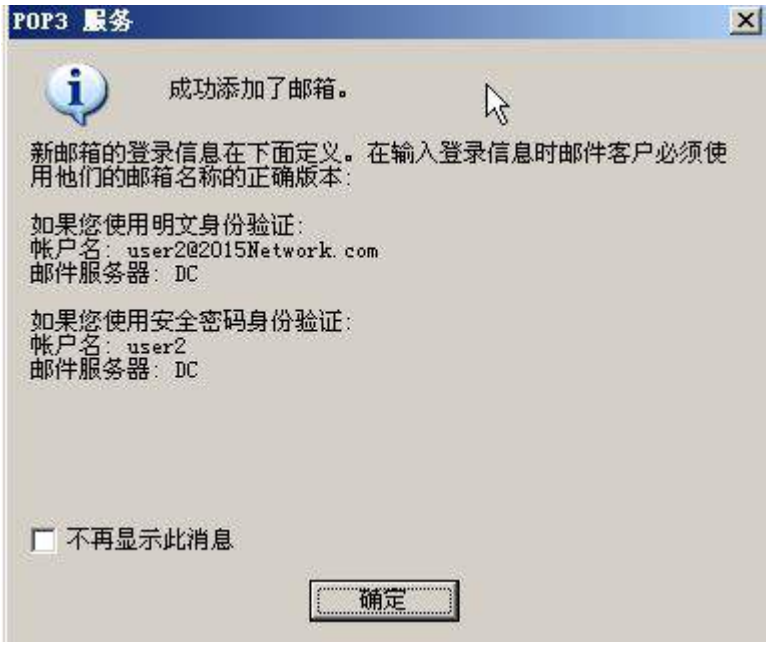




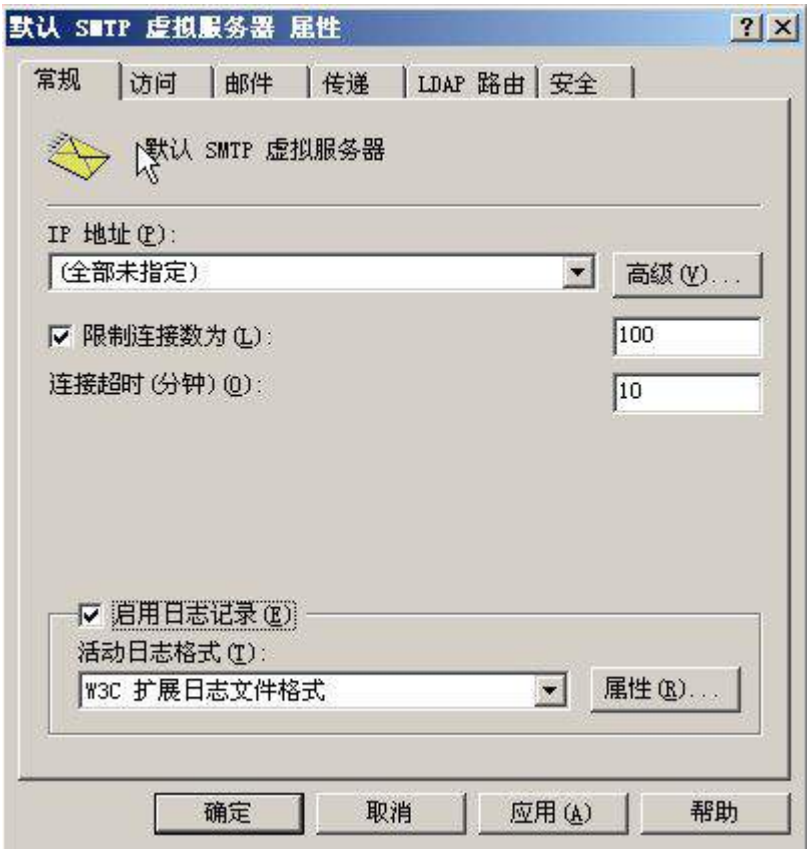
（三）在主机 Win2003-C1 中完成邮件服务器的部署

1、在当前服务器中设置电子邮件服务，并采用本地 windows 帐户的身份验证方式，创建 user1@2015Network.com 及 user2@2015Network.com 用户邮箱。





2、完成对 smtp 服务的配置，限制最大连接数为 100，启用日志记录。



3、借助 outlook 程序进行测试，以用户 user1@2015Network.com 角色给用户 user2@2015Network.com 发送一封邮件。

Linux 操作系统和集群部分

【说 明】

1、所有 Linux 操作系统的 root 用户的密码为 123456，若未按要求设置密码，涉及到该操作系统下的所有分值记为 0 分。

2、虚拟主机的 IP 属性设置请按照网络拓扑结构图以及“表 3：服务器 IP 地址分配表”的要求设定。

3、除有特别规定外，其他未明确规定用户密码均与用户名相同。

4、如果宿主机是 Linux 的操作系统，所有操作系统镜像文件及试题所需的其他软件均存放于每台计算机的/根目录下；如果宿主机是 windows 的操作系统，所有系统镜像文件及试题所需的其它软件均存放在每台主机的 D:\soft 文件夹中。并将题目要求的截图内容以.jpg 格式存储于 BACKUP 文件夹中。

5、题目要求的虚拟机均安装于每台主机的 D：\virtualPC 目录，即路径为 D：\virtualPC\虚拟主机名称。

一、在 Server 1 上完成如下操作:

（一）完成虚拟主机的创建

安装虚拟机“Centos-A1 “，具体要求为内存 512MB，硬盘 10GB。

（二）在主机 Centos-A1 中完成 Samba 文件共享服务器的部署

1、在此服务器中安装配置 Samba 服务，创建三个用户 m1,m2,m3，分别对应三个共享目录分别为/opt/a1, /opt/a2, /opt/a3, 并创建一个公共目录/opt/public。

```
Complete!
[root@localhost yum.repos.d]# useradd m1
[root@localhost yum.repos.d]# useradd m2
[root@localhost yum.repos.d]# useradd m3
[root@localhost yum.repos.d]# mkdir /opt/a1
[root@localhost yum.repos.d]# mkdir /opt/a2
[root@localhost yum.repos.d]# mkdir /opt/a3
[root@localhost yum.repos.d]# mkdir /opt/public
[root@localhost yum.repos.d]# chmod 777 /opt/a1
[root@localhost yum.repos.d]# chmod 777 /opt/a2
[root@localhost yum.repos.d]# chmod 777 /opt/a3
[root@localhost yum.repos.d]# chmod 777 /opt/public/
[root@localhost yum.repos.d]# _
```

```
;       guest ok = yes


# A publicly accessible directory, but read only, except for people
# the "staff" group
        [m1]
        path = /opt/a1
        write list = m1
        writable =yes
        valid user =@manager
        [m2]
        path = /opt/a2
        write =no
        write list =m1
        valid user=m1,m2,m3
        [m3]
        path = /opt/a3
        writable=no
        write list=m1
        valid user=m1,m2,m3
        [public]
        path = /opt/public
        public = yes_

-- INSERT --                                                    300,1
```

2、默认以匿名访问，可以对/opt/public 有读权限，进入其它文件夹时需要对其身份认证。

```
# ----------------------- Standalone Server Options ------------------------
#
# Scurity can be set to user, share(deprecated) or server(deprecated)
#
# Backend to store user information in. New installations should
# use either tdbsam or ldapsam. smbpasswd is available for backwards
# compatibility. tdbsam requires no further configuration.

        security = share
        map to guest =bad user_
        passdb backend = tdbsam


# ----------------------- Domain Members Options ------------------------
#
# Security must be set to domain or ads
#
# Use the realm option only with security = ads
# Specifies the Active Directory realm the host is part of
#
```

3、其中，m1 用户属于 manager 组，对/opt/a1，/opt/a2，/opt/a3 共享有读写权限。m2,m3 为同一项目组 Finance 的成员，可以互相对彼此文件有读的权限。/opt/a1 的共享只有 manager 组用户可以访问。

```
;       guest ok = yes


# A publicly accessible directory, but read only, except for people
# the "staff" group
        [m1]
        path = /opt/a1
        write list = m1
        writable =yes
        valid user =@manager
        [m2]
        path = /opt/a2
        write =no
        write list =m1
        valid user=m1,m2,m3
        [m3]
        path = /opt/a3
        writable=no
        write list=m1
        valid user=m1,m2,m3
        [public]
        path = /opt/public
        public = yes_

-- INSERT --                                                    300,14
```

4、阻止客户端上传含有特定关键字的文件或目录到 samba 共享资源，客户端不允许在目录/opt/finance 中上传可执行文件（.exe）及位图（.jpg）文件；客户端不允许在/opt/sales 目录中上传包含 root 关键字的文件或目录。

```
[m1]
path = /opt/a1
write list = m1
writable =yes
valid user =@manager
veto files =/*.exe/,/*.jpg/
[m2]
path = /opt/a2
write =no
write list =m1
valid user=m1,m2,m3
veto files =/*root*/
```

二、在 Server 2 上完成如下操作：

（一）完成虚拟主机的创建

1、安装虚拟机“Centos-B1”,具体要求为内存 512MB，硬盘 20GB；分区大小为：SWAP 分区大小为 1G；/boot 分区大小为 500M，文件类型为 ext4；/home 分区大小为 2G，文件类型为 ext4， /分区为 10G，文件类型为 ext4。

2、安装虚拟机“Centos-B2”,具体要求为内存 512MB，硬盘 10GB。

（二）在主机 Centos-B1 中完成磁盘管理的部署

1、在“Centos-B1”中额外添加 4 块硬盘，容量分别为 2G。

2、此操作需要 1 块硬盘，系统应该有 2GiB 的交换空间。配置足够的交换空间，满足以下条件，不删除任何已经存在的 swap 分区，额外的 swap 空间应该均匀分布在两个硬盘上（同等大小），系统启动时，swap 分区应该自动挂载。

```
[root@localhost ~]# dd if=/dev/zero of=/512MB bs=1M count=512
512+0 records in
512+0 records out
536870912 bytes (537 MB) copied, 4.15754 s, 129 MB/s
```

```
[root@localhost ~]# mkswap /512MB
mkswap: /512MB: warning: don't erase bootbits sectors
        on whole disk. Use -f to force.
Setting up swapspace version 1, size = 524284 KiB
no label, UUID=a8ad3f78-3355-441c-a86d-bc227bdadbc8
[root@localhost ~]# swapon /512MB
[root@localhost ~]# freew
-bash: freew: command not found
[root@localhost ~]# free
             total       used       free     shared    buffers     cached
Mem:       1020348     824372     195976          0      29320     627872
-/+ buffers/cache:     167180     853168
Swap:      1572848          0    1572848
[root@localhost ~]#
```

```
[root@localhost ~]# mkswap /dev/sdb1
Setting up swapspace version 1, size = 530108 KiB
no label, UUID=24812254-c18e-459a-98f1-86ce2326c5ca
[root@localhost ~]# swapon /dev/sdb1
[root@localhost ~]# free
             total       used       free     shared    buffers     cached
Mem:       1020348     824960     195388          0      29324     627872
-/+ buffers/cache:     167764     852584
Swap:      2102952          0    2102952
[root@localhost ~]# _
```

```
#
# /etc/fstab
# Created by anaconda on Mon May 30 14:25:35 2016
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
UUID=5e619871-b6e2-466e-ad03-a6950982dead /                       ext4    defaul
ts        1 1
UUID=2aa59d50-9e8a-402d-8bdd-9fadf9310b99 /boot                   ext4    defaul
ts        1 2
UUID=9840bd37-96bb-4e21-a804-750ba9f5e21c /home                   ext4    defaul
ts        1 2
UUID=493c7bf9-2e07-42cf-b1a2-d12d18700372 swap                    swap    defaul
ts        0 0
tmpfs                   /dev/shm                tmpfs   defaults        0 0
devpts                  /dev/pts                devpts  gid=5,mode=620  0 0
sysfs                   /sys                    sysfs   defaults        0 0
proc                    /proc                   proc    defaults        0 0
/512MB                  swap                    swap    defaults        0 0
/dev/sdb1               swap                    swap    defaults        0 0_
```

（三）在主机 Centos-B2 中完成 FTP 服务器的部署

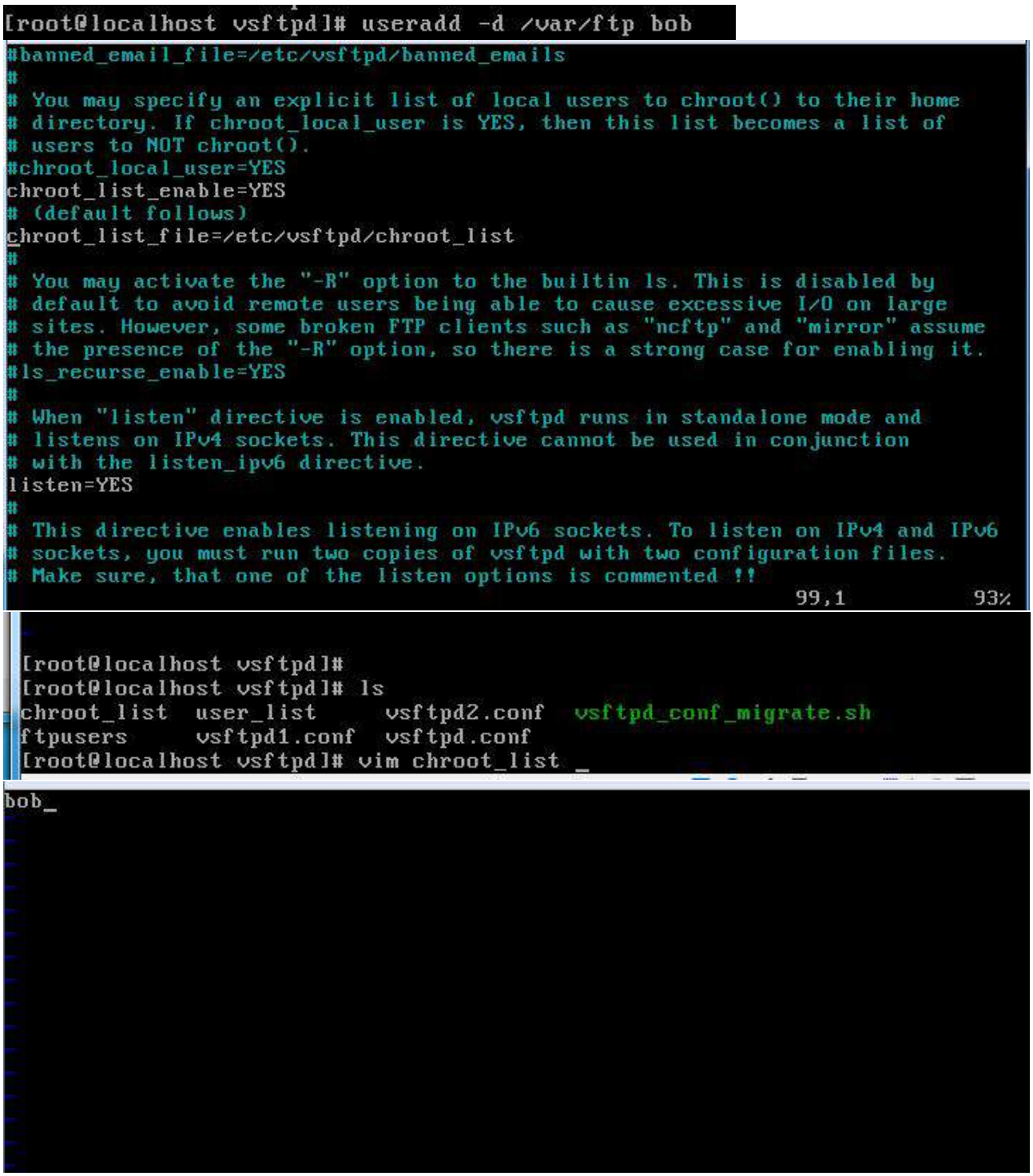
1、配置多站点 FTP 服务，创设三个 FTP 服务站点，域名分别为 ftp.jnds.net、ftp1.jnds.net 以及 ftp2.jnds.net，除站点 ftp.jnds.net 采用默认配置外，其余站点配置文件名分别为 vsftpd1.conf 以及 vsftpd2.conf，站点主目录分别为 /var/ftp1 以及/var/ftp2。

```
[root@localhost vsftpd]# cp vsftpd.conf vsftpd1.conf
[root@localhost vsftpd]# cp vsftpd.conf vsftpd2.conf
[root@localhost vsftpd]# ls
ftpusers   vsftpd1.conf  vsftpd.conf
user_list  vsftpd2.conf  vsftpd_conf_migrate.sh
[root@localhost vsftpd]# _
```

```
# (default follows)
#chroot_list_file=/etc/vsftpd/chroot_list
#
# You may activate the "-R" option to the builtin ls. This is disabled by
# default to avoid remote users being able to cause excessive I/O on large
# sites. However, some broken FTP clients such as "ncftp" and "mirror" assume
# the presence of the "-R" option, so there is a strong case for enabling it.
#ls_recurse_enable=YES
#
# When "listen" directive is enabled, vsftpd runs in standalone mode and
# listens on IPv4 sockets. This directive cannot be used in conjunction
# with the listen_ipv6 directive.
listen=YES
#
# This directive enables listening on IPv6 sockets. To listen on IPv4 and IPv6
# sockets, you must run two copies of vsftpd with two configuration files.
# Make sure, that one of the listen options is commented !!
#listen_ipv6=YES

pam_service_name=vsftpd
userlist_enable=YES
tcp_wrappers=YES
listen_address=10.100.100.107
local_root=/var/ftp2
"vsftpd2.conf" 121L, 4650C                                    121,1         Bot
```

```
# (default follows)
#chroot_list_file=/etc/vsftpd/chroot_list
#
# You may activate the "-R" option to the builtin ls. This is disabled by
# default to avoid remote users being able to cause excessive I/O on large
# sites. However, some broken FTP clients such as "ncftp" and "mirror" assume
# the presence of the "-R" option, so there is a strong case for enabling it.
#ls_recurse_enable=YES
#
# When "listen" directive is enabled, vsftpd runs in standalone mode and
# listens on IPv4 sockets. This directive cannot be used in conjunction
# with the listen_ipv6 directive.
listen=YES
#
# This directive enables listening on IPv6 sockets. To listen on IPv4 and IPv6
# sockets, you must run two copies of vsftpd with two configuration files.
# Make sure, that one of the listen options is commented !!
#listen_ipv6=YES

pam_service_name=vsftpd
userlist_enable=YES
tcp_wrappers=YES
listen_address=10.100.100.106
local_root=/var/ftp1
"vsftpd1.conf" 121L, 4650C                                    121,1         Bot
```

2、创建用户 bob 并登录站点 ftp.jnds.net 后，不能访问除其主目录外的其他目录。



3、站点 ftp1.jnds.net 中指定匿名用户能够上传但不能进行下载操作，匿名用户主目录为/var/ftp1/upload；站点 ftp2.jnds.net 中设置匿名用户具备上传权限但仅能够下载其自身上传的文件内容，匿名用户主目录为/var/ftp2/upload。

```
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
#
# Allow anonymous FTP? (Beware - allowed by default if you comment this out).
anonymous_enable=YES
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
local_umask=022
#
# Uncomment this to allow the anonymous FTP user to upload files. This only
# has an effect if the above global write enable is activated. Also, you will
# obviously need to create a directory writable by the FTP user.
anon_upload_enable=YES
anon_world_readable_only=YES
anon_root=/var/ftp2/upload
#
# Uncomment this if you want the anonymous FTP user to be able to create
-- INSERT --                                                29,20         7%
```

```
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
#
# Allow anonymous FTP? (Beware - allowed by default if you comment this out).
anonymous_enable=YES
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
local_umask=022
#
# Uncomment this to allow the anonymous FTP user to upload files. This only
# has an effect if the above global write enable is activated. Also, you will
# obviously need to create a directory writable by the FTP user.
anon_upload_enable=YES
anon_world_readable_only=NO
anon_root=/var/ftp1/upload
#
```

4、站点 ftp.jnds.net 禁止 10.1.2.0 访问，对 10.1.3.0 网段做如下限制：每 IP 最大的连接数为 2，本地用户传输率为 200Kbps，禁止上传 mp3,avi 文件。

```
#
# hosts.allow   This file contains access rules which are used to
#               allow or deny connections to network services that
#               either use the tcp_wrappers library or that have been
#               started through a tcp_wrappers-enabled xinetd.
#
#               See 'man 5 hosts_options' and 'man 5 hosts_access'
#               for information on rule syntax.
#               See 'man tcpd' for information on tcp_wrappers
#
vsftpd:10.1.2.*:deny
vsftpd:10.1.3.*:setenv VSFTPD_LOAD_CONF /etc/vsftpd/1
```

```
[root@localhost vsftpd]# vim 1_
```

```
max_per_ip=2
local_rate=200000
deny_file={*.mp3,*.avi}
```

三、在 Server 3 上完成如下操作：

（一）完成虚拟主机的创建

1、安装名为“Centos-C1”的虚拟机，具体要求为硬盘大小为 20GB，内存为 512MB。

（二）在主机 Centos-C1 中完成 BIND 域名服务器的部署

1、在此服务器中安装配置 bind 服务，负责区域“jnds.net”内主机解析，三台主机分别为 www.jnds.net 、raid.jnds.net、ftp.jnds.net、ftp1.jnds.net 、ftp2.jnds.net、smb.jnds.net、dns.jnds.net、mysql.jnds.net、nfs.jnds.net，做好正反向 DNS 服务解析，对 2015Network.com 域的解析转发给 win2003_A1。

```
$TTL 3H
@       IN SOA  jnds.net.       root.jnds.net. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
@       IN      NS      jnds.net.
109     IN      PTR     jnds.net.
161     IN      PTR     www.jnds.net.
5       IN      PTR     raid.jnds.net.
105     IN      PTR     ftp.jnds.net.
106     IN      PTR     ftp1.jnds.net.
107     IN      PTR     ftp2.jnds.net.
3       IN      PTR     smb.jnds.net.
109     IN      PTR     dns.jnds.net.
161     IN      PTR     mysql.jnds.net.
109     IN      PTR     nfs.jnds.net.
~
~
~
~
~
-- INSERT --                                            2,18-25       All
```

```
$TTL 1D
@       IN SOA  jnds.net.       root.jnds.net. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
        IN      NS      jnds.net.
@       IN      A       10.100.100.109
www     IN      A       10.100.100.161
raid    IN      A       10.100.100.5
ftp     IN      A       10.100.100.105
ftp1    IN      A       10.100.100.106
ftp2    IN      A       10.100.100.107
smb     IN      A       10.100.100.3
dns     IN      A       10.100.100.109
mysql   IN      A       10.100.100.161
nfs     IN      A       10.100.100.109
~
~
~
~
~
-- INSERT --                                            8,16-33       All
```

```
//
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//

options {
        listen-on port 53 { any; };
        listen-on-v6 port 53 { any; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        allow-query     { any; };
        recursion yes;
        forward only;
        forwarders{10.100.100.100};_

        dnssec-enable yes;
        dnssec-validation yes;
        dnssec-lookaside auto;
-- INSERT --                                                    20,29-36      Top
```

2、通过配置，在本机上可以使用 rndc 来控制域名服务运行。

```
        managed-keys-directory "/var/named/dynamic";
};

 key "rndc-key" {
        algorithm hmac-md5;
        secret "1LGrtJ6HXtBSOgBkBzaqOA==";
 };

 controls {
        inet 127.0.0.1 port 953
                allow { 127.0.0.1; } keys { "rndc-key"; };
 };
logging {
        channel default_debug {
"named.conf" 53L, 1167C written
[root@localhost etc]#
[root@localhost etc]#
[root@localhost etc]# service named restart
Stopping named: .                                          [  OK  ]
Starting named:                                            [  OK  ]
[root@localhost etc]# rndc reload
WARNING: key file (/etc/rndc.key) exists, but using default configuration file (
/etc/rndc.conf)
server reload successful
[root@localhost etc]# _
```

（三）在主机 Centos-C1 中完成 NFS 服务器服务器的部署

1、配置 NFS 服务，服务开机自启动。按下表要求共享目录。

```
[root@localhost nfsuser]#
[root@localhost nfsuser]# chkconfig nfs on
[root@localhost nfsuser]# _
```

共享目录	共享要求
/var/test	10.1.3.0/24 这个网段的用户具有读写权限，其它只读。
/var/tmp	所有人都可以读写，root 写入的文件还具有

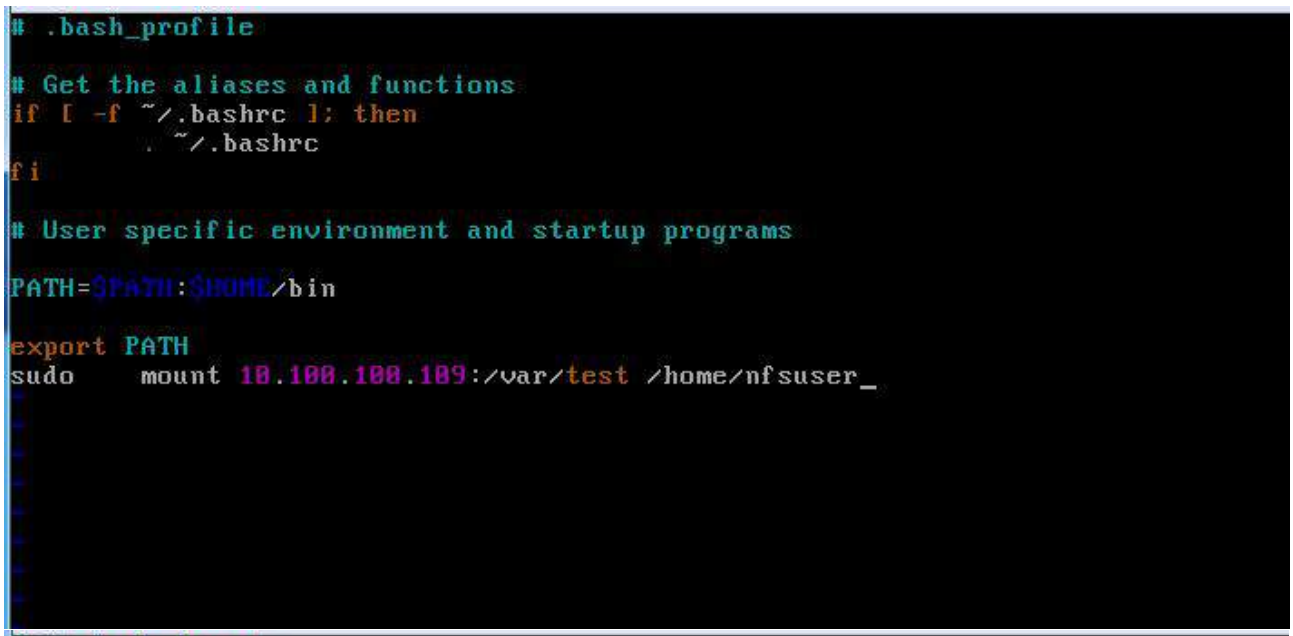
	root 的权限。

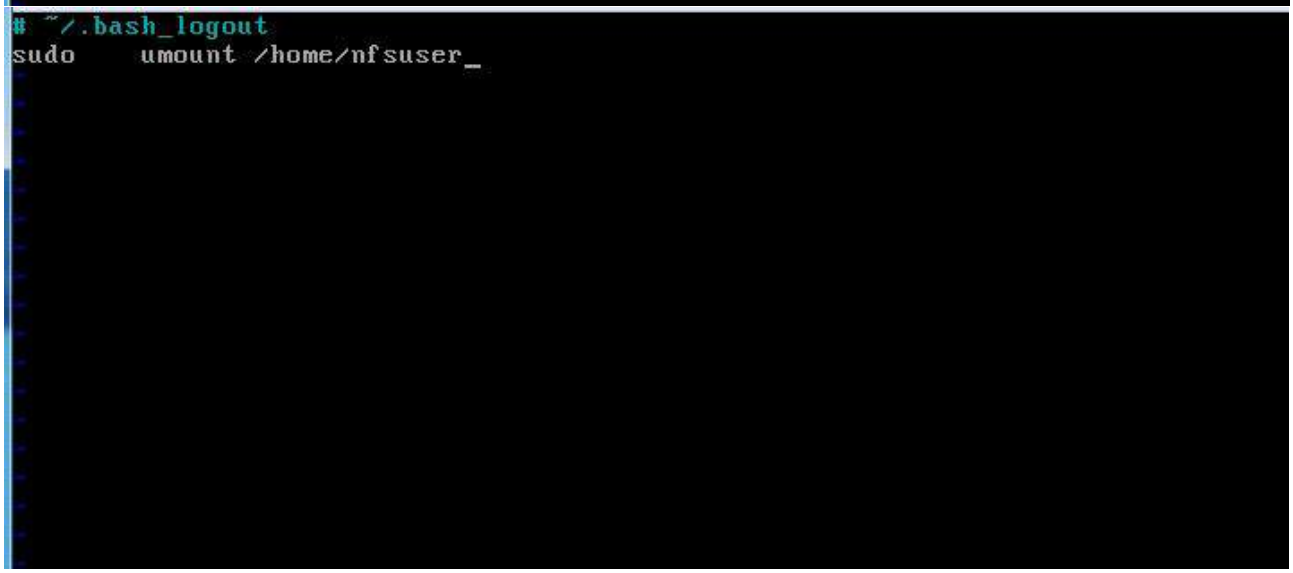
```
/var/test       10.1.3.0/24(rw) *(ro)
/var/tmp        *(ro,no_root_squash)
```

2、创建用户 nfsuser，当 nfsuser 在终端登录时，自动 mount 共享的/var/test 目录到/home/nfsuser/，退出时自动 umount。

```
[root@localhost etc]# useradd nfsuser
```

```
## Allow root to run any commands anywhere
root    ALL=(ALL)       ALL

## Allows members of the 'sys' group to run networking, software,
## service management apps and more.
# %sys ALL = NETWORKING, SOFTWARE, SERVICES, STORAGE, DELEGATING, PROCESSES, LOC
ATE, DRIVERS

## Allows people in group wheel to run all commands
# %wheel        ALL=(ALL)       ALL

## Same thing without a password
# %wheel        ALL=(ALL)       NOPASSWD: ALL

## Allows members of the users group to mount and unmount the
## cdrom as root
# %users  ALL=/sbin/mount /mnt/cdrom, /sbin/umount /mnt/cdrom

## Allows members of the users group to shutdown this system
# %users  localhost=/sbin/shutdown -h now

## Read drop-in files from /etc/sudoers.d (the # here does not mean a comment)
#includedir /etc/sudoers.d
nfsuser         ALL=(ALL)       NOPASSWD:ALL_
-- INSERT --
```





四、 在 Server 4 上完成如下操作：

（一）完成虚拟主机的创建

1、Server4 主机系统为 CentOS6.5，需要在此 Linux 平台上采用 KVM 方式安装虚拟机“Centos-D1”，具体要求为硬盘大小为 12GB，内存为 768MB，系统为 CentOs6.5；（小提示：如无法正确安装虚拟机 Centos-D1，下述题目中所涉及的虚拟机题目可在

Server4 真实主机中完成)

（二）在主机 Centos-D1 中完成 Apache 服务器以及 MySQL 数据库服务器的部署

1、在此服务器中安装 httpd 服务，建立站点 www.jnds.net，其网站主目录为 /var/www/html，首页内容为“chinaskills‘ s website”。

```
# redirections work in a sensible way.
#
ServerName www.jnds.net:80

#
# UseCanonicalName: Determines how Apache constructs self-referencing
# URLs and the SERVER_NAME and SERVER_PORT variables.
# When set "Off", Apache will use the Hostname and Port supplied
# by the client.  When set "On", Apache will use the value of the
# ServerName directive.
#
UseCanonicalName Off

#
# DocumentRoot: The directory out of which you will serve your
# documents. By default, all requests are taken from this directory, but
# symbolic links and aliases may be used to point to other locations.
#
DocumentRoot "/var/www/html"

#
# Each directory to which Apache has access can be configured with respect
# to which services and features are allowed and/or disabled in that
```

```
                                                    http://www.jnds.net/
  chinaskills's website
```

2、使用 openssl 申请证书，创建自签名证书 server.crt 和私钥 server.key，要求只允许使用域名通过 SSL 加密访问。

```
[root@localhost conf]# openssl genrsa -des 1024 >server.key
Generating RSA private key, 1024 bit long modulus
.....................++++++
.....................................++++++
e is 65537 (0x10001)
Enter pass phrase:
Verifying - Enter pass phrase:
[root@localhost conf]# openssl req -new -key server.key -out server.csr
```

```
[root@localhost tls]# openssl x509 -days 365 -req -in server.csr -signkey server
.key -out server.crt
Signature ok
subject=/C=XX/L=Default City/O=Default Company Ltd
Getting Private key
[root@localhost tls]#
```

3、安装 mysql 服务，修改 root 用户的密码为 123456，创建数据库 testdb，创建用户 testuser，其对 testdb 数据库有完全控制权，仅可在本机登录。按如下结构创建表 table1。每周五凌晨 1：00 备份数据库 testdb 到/var/databak/testdb.sql。

```
[root@localhost conf]# mysqladmin -u root password "123456"
[root@localhost conf]# mysql -u root -p123456
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 3
Server version: 5.1.71 Source distribution

Copyright (c) 2000, 2013, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

```
mysql> create database testdb;
Query OK, 1 row affected (0.01 sec)

mysql> create user "testuser"@"localhost" identified by "123456";
Query OK, 0 rows affected (0.00 sec)

mysql> grant all on testdb.* to "testuser"@"localhost";
Query OK, 0 rows affected (0.01 sec)
```

字段名	数据类型	主键	自增
ID	int	是	是
name	varchar(10)	否	否
birthday	datetime	否	否
sex	cahr(1)	否	否

```
mysql> use testdb
Database changed
mysql> create table table1( ID int primary key auto_increment, name varchar(10),
 birthday datetime, sex char(1));
Query OK, 0 rows affected (0.09 sec)

mysql> desc table1;
+----------+-------------+------+-----+---------+----------------+
| Field    | Type        | Null | Key | Default | Extra          |
+----------+-------------+------+-----+---------+----------------+
| ID       | int(11)     | NO   | PRI | NULL    | auto_increment |
| name     | varchar(10) | YES  |     | NULL    |                |
| birthday | datetime    | YES  |     | NULL    |                |
| sex      | char(1)     | YES  |     | NULL    |                |
+----------+-------------+------+-----+---------+----------------+
4 rows in set (0.01 sec)

mysql> _
```

```
[root@localhost /]# vim backup.sh_
```

```
mysqldump -u root -p123456 testdb>/var/databak/test.sql_
```

```
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root
HOME=/

# For details see man 4 crontabs

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,th
ri,sat
# |  |  |  |  |
# *  *  *  *  * user-name command to be executed
  0  1  *  *  5 root /backup.sh_
```

4、在服务器端使用 iptables 设置防火墙功能,只允许用户访问这台服务器的 WWW 服务，而服务器只能被动地接受连接请求，不能主动的发起连接。

```
[root@localhost etc]# iptables -P OUTPUT DROP
[root@localhost etc]# iptables -I OUTPUT 1 -p tcp -m state --state=RELATED,ESTAB
LISHED --sport 80 -j ACCEPT
[root@localhost etc]# iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTAB
LISHED
ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:2
2
REJECT     all  --  0.0.0.0/0            0.0.0.0/0           reject-with icmp-ho
st-prohibited

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
REJECT     all  --  0.0.0.0/0            0.0.0.0/0           reject-with icmp-ho
st-prohibited

Chain OUTPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTAB
LISHED tcp spt:80
[root@localhost etc]# _
```

2015 年全国职业院校技能大赛
网络搭建与应用竞赛
（总分 1000 分）

赛题说明

一、竞赛内容分布

“网络搭建与应用”竞赛共分二个部分，其中：
第一部分：网络搭建及安全部署项目，占总分的比例为 45%；
第二部分：服务器配置及应用项目，占总分的比例为 55%；

二、竞赛注意事项

（1）禁止携带和使用移动存储设备、计算器、通信工具及参考资料。
（2）请根据大赛所提供的比赛环境，检查所列的硬件设备、软件清单、材料清单是否齐全，计算机设备是否能正常使用。
（3）本试卷共有两个部分。请选手仔细阅读比赛试卷，按照试卷要求完成各项操作。
（4）操作过程中，需要及时保存设备配置。比赛结束后，所有设备保持运行状态，不要拆、动硬件连接。
（5）比赛完成后，比赛设备、软件和赛题请保留在座位上，禁止将比赛所用的所有物品（包括试卷和草纸）带离赛场。
（6）所有需要提交的文档均放置在桌面的 PC1“比赛文档”文件夹中，禁止在纸质资料上填写与竞赛无关的标记，如违反规定，可视为 0 分。
（7）裁判以各参赛队提交的竞赛结果文档为主要评分依据。所有提交的文档必须按照赛题所规定的命名规则命名，文档中有对应题目的小标题，截图有截图的简要说明，否则按无效内容处理。
（8）与比赛相关的工具软件放置在 D 盘的 tools 文件夹中。

二、竞赛项目背景及网络拓扑

1. 项目描述

下图是某集团公司在天津设有总公司，在上海设有分公司，为了实现信息交流和资源共享，需要构建一个跨越两地的集团网络。总公司采用节点和链路冗余的网络架构及双出口的网络接入模式，采用防火墙接入互联网络，保护内网用户资源，采用路由器接入城域网专用链路来传输集团业务数据。

总公司为了安全管理每个部门的用户，使用 VLAN 技术将每个部门的用户划分到不同的 VLAN 中。上海分公司采用路由器接入互联网络和城域网专用线路，分公司的内网用户接入采用无线接入方式访问网络资源。为了保障总公司与分公司业务数据传输的高可用性，租用广域网专用线路 ISP 为主链路，采用基于 IPSEC-VPN 技术作为因特网链路的备份链路，以实现业务流量的高可用性。总公司与分公司网络采用 OSPF 路由协议；而总公司防火墙与内网路由器的连接采用 RIP 路由协议，集团网络具体拓扑结构如图 1 所示。

2、网络拓扑规划

网络拓扑结构规划如图 1 所示。

图1 集团网络拓扑-结构图

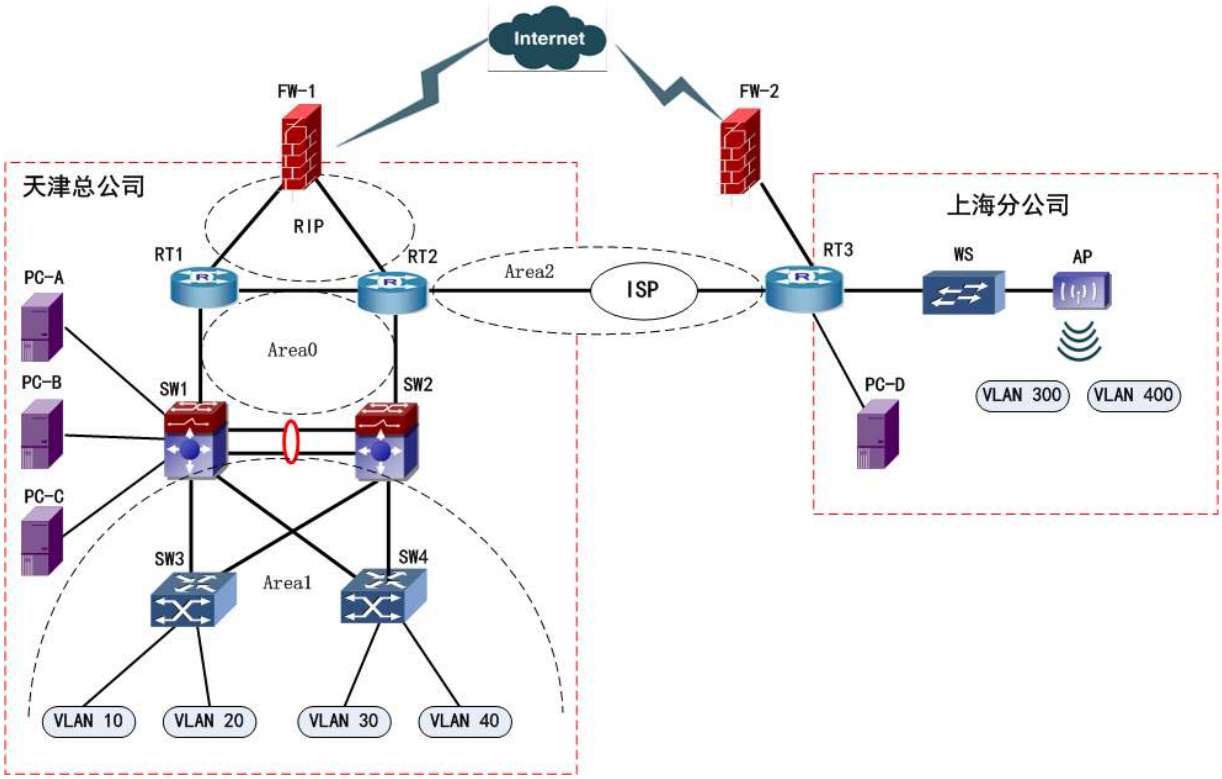


图 1　网络拓扑结构图

本次公司的网络构建包括总公司和分公司的两个部分。总公司局域网核心采用双交换机的构架，通过 VRRP 结合 MSTP 技术实现负载均衡和链路备份。两台核心交换机分别连接到核心路由器，核心路由器连接到网络出口防火墙，同时核心路由器通过 ISP 专线连接到分公司的出口路由器。总公司的网络出口使用防火墙连接到公网，通过配置防火墙来实现内网用户访问 Internet 以及保护内网的安全。总公司和分公司之间的办公用户通过 VPN 建立的隧道相互通信，有效的保证了数据传输的安全性。

服务器集中放置在网络中心机房，直接连接到核心交换机。分公司的网络的出口路由器分别连接到 ISP 和 VPN 设备，通过部署防火墙来保护内网的安全，内网的用户分别通过专网或 VPN 建立的安全隧道来访问总公司的资源。

三、工程建设的内容

本工程项目主要建设内容为：

1. 总公司与分公司布线系统建设

总公司与分公司内部局域网的布线系统搭建，包括数据及语音的布线系统。

2. 总公司局域网建设

总公司网络构建（有线双核心网络）、可用性及安全规则部署。

3. 分公司局域网建设

分公司网络构建（无线网络）、可用性及安全规则部署。

4. 总公司与分公司广域网互联建设

总公司与分公司之间采用数据专线、VPN 方式互联。

5. 总公司应用平台建设

在总公司的网络中心机房，部署 Windows 2003 Server R2、Windows 2008 Server R2 及 LINUX 服务器系统，并在此之上架设 DNS、WEB、DHCP、FTP、MAIL、KVM 安装、Apache、Sendmail、BIND、Samba 等应用服务。

第一部分 网络搭建及安全部署项目(450 分)

【注意事项】

（1）设备配置完毕后，保存最新的设备配置。路由器和交换机等终端配置设备请按题目要求提交 show running-config 结果，并将网络、无线、防火墙等设备通过 web 或是客户端配置的设备请按题目要求提交相关截图，并将这些结果写入竞赛结果文档中。

（2）本部分竞赛结果文档文件名称为：工位号_网络配置文档.doc（如 47 号工位的文件命名为：47_网络配置文档.doc），注意对截图进行必要说明。

（3）对竞赛结果文档进行适当的排版，删除不必要的重复行和空行，小标题使用“五号”“加粗”，正文采用“五号”字。

（4）文档保存到本地计算机的桌面，考试结束时将竞赛结果文件全部备份到本机桌面以自己工位号建立的文件夹中。

一、网络设备配置要求

1. 设备连接关系:

表 1-3 网络设备 1 连接到设备 2 表

设备一	设备二	设备一端口	设备二端口	线缆类型
RT1	FW1	GE0/5	E0/0	双绞线
RT1	RT2	GE0/4	GE0/4	双绞线
RT1	SW1	GE0/3	E1/0/1	双绞线
RT2	FW1	GE0/5	E0/1	双绞线
RT2	RT3	S0/1	S0/1	V35
RT2	SW2	GE0/3	E1/0/1	双绞线
RT3	WS	GE0/4	E1/0/1	双绞线
RT3	FW2	GE0/3	E0/1	双绞线
SW1	SW2	E1/0/13-14	E1/0/13-14	双绞线
SW1	SW3	E1/0/21	E1/23	双绞线
SW1	SW4	E1/0/22	E1/24	双绞线
SW2	SW3	E1/0/22	E1/24	双绞线
SW2	SW4	E1/0/21	E1/23	双绞线
WS	AP	E1/0/2	LAN 口	双绞线
SW1	PC-A	E1/0/10	NIC	双绞线
SW1	PC-B	E1/0/11	NIC	双绞线
SW1	PC-C	E1/0/12	NIC	双绞线
RT3	PC-D	GE0/5	NIC	双绞线

2. 网络设备 IP 地址自行分配表。

表 1-4 网络设备 IP 地址表

设备	设备名称	设备接口	IP 地址/
路由器	RT1	GigaEthernet0/3	
		GigaEthernet0/4	
		GigaEthernet0/5	
	RT2	Serial0/1	

		GigaEthernet0/3	
		GigaEthernet0/4	
		GigaEthernet0/5	
	RT3	Serial0/1	
		GigaEthernet0/3	
		GigaEthernet0/4	
		GigaEthernet0/5	
三层交换机	SW1	VLAN1000 (Ethernet1/0/1)	
		VLAN3000 (Ethernet1/0/13-14)	
		VLAN10 SVI	
		VLAN20 SVI	
		VLAN30 SVI	
		VLAN40 SVI	
		管理 VLAN50 SVI	
		服务器群 VLAN100 (Ethernet1/0/10-12)	
	SW2	VLAN2000 (Ethernet1/0/1)	
		VLAN3000 (Ethernet1/0/13-14)	
		VLAN10 SVI	
		VLAN20 SVI	
		VLAN30 SVI	
		VLAN40 SVI	
		管理 VLAN50 SVI	
二层交换机	SW3	管理 VLAN50 SVI	
	SW4	管理 VLAN50 SVI	
防火墙 1	FW1	Ethernet0/1	
		Ethernet0/2	
		Ethernet0/3	200.200.200.1/24
防火墙 2	FW2	Ethernet0/1	
		Ethernet0/3	200.200.200.2/24
无线控制器	WS	VLAN300 SVI	
		VLAN400 SVI	

3. 服务器 IP 地址自行分配表:

表 1-5：服务器 IP 地址分配表

宿主机	虚拟主机名称	域名信息	服务角色	系统及版本信息	IPv4 地址信息
PC-A	Win2003-	dns1.tj.com	主 DNS、WWW	Windows	10.100.100.1

	A1	web.tj.com	服务器	Server 2003 R2	
	Win2003-A2	Dns2.tj.com	备份 DNS、认证服务器	Windows Server 2003 R2	10.100.100.2
	Win2008-A1	dc.tj.com	DC 域控制器	Windows Server 2008 R2	10.100.100.3
PC-B	Win2008-B1	erp.tj.com	WEB 服务器 FTP 服务器	Windows Server 2008 R2	10.100.100.4
	Win2003-B1	Mail1.tj.com	邮件服务器	Windows Server 2003 R2	10.100.100.5
	Windows-XP B1	pc. tj.net	工作站	Windows XP	10.100.100.6
PC-C	Win2003-C1	dc.ykca.com	DC 域控制器 CA 证书服务器	Windows Server 2003 R2	10.100.100.7
	Win2008-C1	rodc.ykca.com	只读域控制器	Windows Server 2008 R2	10.100.100.8
	Centos-C1	Mail2.linu.net	Sandmail 邮件服务器	Centos 6.5	10.100.100.100
	Centos-C2	ftp.linu.net ftp1.linu.net	FTP 文件服务器	Centos 6.5	10.100.100.101
PC-D	Centos-D1	www.linu.net	Apache Web 服务器	Centos 6.5	10.100.100.102
	Centos-D2	dns.linu.net smb.linu.net	BIND 域名服务器 MySQL 数据库服务器 NFS 共享服务器 SAMBA 共享服务器	Centos 6.5	10.100.100.103

二、网络搭建部分

1. 物理连接与 IP 地址划分

（1）按照网络拓扑图制作以太网网线跳线，用于 SW1、SW2、RT1、SW3 设备的连接，并增加标识。要求符合 T568A 和 T568B 的标准，其线缆长度适中；

（2）根据“拓扑结构图”和“表 1-4-网络设备 IP 地址分配表”和“表 1-5-服务器 IP

地址分配表”所示，请对网络中的所有网络设备接口和服务器分别规划部署 IP 地址；

总公司中整个网络地址规划使用 10.0.0.0/16 地址段,其中市场部有 65 名员工、工程部有 93 名员工、软件部和系统集成部两个部门各有 125 名员工，服务器的网段地址为 10.0.100.0/24。上海分公司使用 10.0.200.0/23 地址段,保证上海分公司行政部至少有 110 台主机，销售部至少有 33 台主机。天津总公司与上海分公司所有设备互联地址使用/30 的掩码进行分配，并把分配后的地址填入上述表 1-4 及表 1-5 分配表中的空白处。

注意：

- 要求网络地址根据上述题目要求合理规划；
- 网关地址规划为本网段的最后一个地址。

2. 交换机配置

（1）为交换机设备命名，命名规则参考为表 1 中的“设备名称”，设备名称的命名规则与拓扑图图示名称相符；

（2）依据“拓扑结构图”和 1-6 表，在交换机上完成 VLAN 配置和端口分配，不允许不必要的 VLAN 通过；

表 1-6 VLAN 虚拟 IP 地址表

设备	VLAN 名称	VLAN ID	接口
SW1	Link_To_管理 vlan	50	Ethernet1/0/20
	Link_To_PC-A、PC-B、PC-C	100	Ethernet1/0/10—12
	Link_To_RT1	1000	Ethernet1/0/1
	Link_To_SW2	3000	Ethernet1/0/13-14
SW2	Link_To_管理 vlan	50	Ethernet1/0/20
	Link_To_RT2	2000	Ethernet1/0/1
	Link_To_SW1	3000	Ethernet1/0/13-14
SW3	Link_To_ SW1/SW2	trunk	Ethernet 1/0/23-24
	SCB（市场部）	10	Ethernet 1/0/1-5
	GCB（工程部）	20	Ethernet 1/0/6-10
SW4	Link_To_ SW1/SW2	trunk	Ethernet 1/0/23-24
	RJB（软件部）	30	Ethernet 1/0/1-5
	XTJCB（系统集成部）	40	Ethernet 1/0/6-10

（3）天津总公司两个核心交换机 SW1 和 SW2 之间使用双线路连接，分别下联到接入交换机 SW3 和 SW4，采用基于 VLAN 生成树，实现网络中的二层的负载均衡和冗余备份。交换机创建两个实例：分别为 Instance 10 和 Instance 20，其中 Instance 10 关联 VLAN 10 和 VLAN30，Instance 20 关联 VLAN20 和 VLAN40。SW1 为缺省 Instance0 和 Instance10 的根交换机，为 Instance20 备份交换机；SW2 为 Instance20 根交换机，为缺省 Instance0 和 Instance10 的备份交换机,按需求设置 STP 优先级为 4096。同时结合 VRRP 技术实现 VLAN10、VLAN20、VLAN30、VLAN40 内的用户网关的冗余备份。设置 SW1 为 VLAN10、30 的 Master，设置 SW2 为 VLAN20、40 的 Master。要求 VRRP 组中高优先级设置为 130，低优先级设置为 110，开启抢占特性，实现冗余切换。并将各 VLAN 的虚拟 IP 地址规划填入下表 1-7 所示：

表 1-7VLAN 虚拟 IP 地址表

VLAN-ID	VRRP 备份组号（VRID）	VRRP 虚拟 IP 地址
VLAN10	10	
VLAN20	20	
VLAN30	30	

VLAN40	40	

（4）将 SW1 三层交换机 Ethernet 1/0/13 和 Ethernet 1/0/14 接口与 SW2 三层交换机 Ethernet1/0/13 和 Ethernet1/0/14 接口配置为静态模式的端口聚合；

（5)将 SW1 上总部服务器群中 Ethernet1/0/11 入方向的数据流镜像至 Ethernet1/0/20；

（6）总部服务器群连接在核心交换机 SW1 的 Ethernet1/0/10-12 上配置端口安全，最多允许动态学习 70 个 MAC 地址，超过 70 时，来自新主机的数据帧将丢失；

（7）在交换机 SW1 上使用 pim-dm 方式开启组播，让所有 VLAN 都可以传送组播包，并在端口 E1/0/21-22 开启流控和设置多播风暴控制，允许通过的多播报文为每秒 64000 个。

3. 路由器配置

（1）为路由设备命名，命名规则参考为表 1 中的“设备名称”，设备名称的命名规则与拓扑图图示名称相符；

（2）在路由器 RT2 和 RT3 设备上与其它网络设备连接的接口都要进行描述；

（3）根据网络拓扑图所示，为了保障专用线路的链路安全，需要在 ISP（RT2 与 RT3 之间）连接的链路上配置 PPP 协议，采用双向 PAP 的验证方式，速率为 115200bps，用户名分别为 RT2 和 RT3，密码均为 123465789；

（4）天津总公司内网采用 OSPF 动态路由协议，防火墙 FW1 与路由器 RT1、RT2 之间采用 RIP 协议，通过专线实现与分公司的互联互通，并自行规划设备 RouterID，并填入下表 1-8：

表 1-8 设备 Router ID 地址表

设备名称	RID
RT1	
RT2	
RT3	
SW1	
SW2	

（5）集团公司网络采用了 OSPF 和 RIPv2 两种动态路由协议，合理规划开销值，实现集团公司访问外网数据流主走 RT1，备走 RT2；

（6）请在集团公司配置必要的链路上配置被动接口，以阻止不必要的报文通往非 OSPF 区域；

（7）在路由器 RT3 上配置地址转换，使上海分公司内网的主机可以通过地址转换访问 Internet，内网全局地址可参考表 1-4 规划，地址池名称为 shpool。

4. 无线配置

（1）上海分公司用户采用无线接入方式，其中 VLAN300 用户的 SSID 为 SH001，协议为 802.11g，信道为 6；无线控制器做为 DHCP 服务器为 VLAN300 用户动态分配 IP 地址，地址租约时长为 2 天。用户接入无线网络时采用 OPEN 认证方式；

（2）VLAN400 用户的 SSID 为 SH002，协议为 802.11b，信道为 13；使用无线控制器做为 DHCP 服务器，为 VLAN400 用户动态分配 IP 地址和网关，地址租约时长为 3 天。用户接入无线网络时需要采用 WPA-PSK 加密方式，其口令为 1234567890；

（3）配置每个 AP 下可以连接的无线用户数为 25，用户的老化时间为 5 分钟；

（4）配置 AC 上 QOS 关联分公司 AP，AP 的 profileID 为 1，为默认配置。QOS 配置在 VLAN300 网段上即 VAP300，并设置其最大带宽为 20480000；

（5)配置无线局域网每用户上行速度为 2Mbps，下行速度为 3Mbps，突发速度为 4Mbps；

（6）将 MAC 地址为 C139.C139.C139 的无线客户端加入黑名单。

注意：

- 将截图粘贴到“工位号_网络无线配置文档.doc”中，标记为“(1)无线网络相关配置截图”，并对截图进行必要的说明；保存到指定位置。

三、网络安全部分：

1. 防火墙配置

（1）集团公司内网 VLAN10、VLAN30 用户可以通过防火墙 FW-1 做 NAT 访问 Internet，上海分公司所有用户可以通过防火墙 FW-2 访问 Internet；

（2）集团公司和上海分公司内网的 Web 服务器分别需要对外提供服务；

（3）为了保障公司网络的安全性，在两台 FW 上做以下防护部署：

- IP 地址扫描攻击防护功能，其中在 3 秒时间内，有 10 个以上相同 IP 地址的 ICMP 包请求，则发出警报，ICMP 洪水攻击防护警戒值为 70，行为为丢弃，但允许数据包通行；
- 配置 SYN Flood 攻击防护功能，警戒值为 300，行为为丢弃；
- 配置 ICMP Flood 攻击防护功能；
- DNS Query Flood 攻击防护功能；
- 配置 smurf 和 Fraggle 攻击防护功能；
- 配置 ARP 欺骗防护功能。

（4）为了保障上海分公司外网资源合理使用，在 FW-2 上配置禁止所有 P2P 数据通过；

（5）在 FW1 中禁止 UDP 的 4000 端口以及 TCP 的 6000 端口的双向数据包通信；

（6）在 FW1 中配置 RIP 协议，并引入 OSPF 区域；

（7）管理网段的用意可以 ping 通 PC-A、PC-B、PC-C。

- 防火墙提交的截图：用户配置防火墙的所有关键配置点信息(包括 FW1 和 FW2)。
- 将截图粘贴到“工位号_防火墙配置文档.doc”中，标记为“防火墙配置截图”，对截图进行必要的说明，保存到指定位置。

---

2. VPN 配置

（1）为了保障集团公司与上海分公司之间传输业务的高可用性，当总公司与分公司之间的 ISP 专线中断后，需要采用互联网链路做为备份链路，在集团公司与上海分公司的两端防火墙上配置 IPSEC VPN，采用 esp-md5-des-g2 提议部署；

（2）在集团公司出口防火墙上配置 SSL 远程接入 VPN，允许公网办公用户远程访问邮件、FTP 业务，用户名为 vpn1、vpn2、vpn3，口令为 2015SEC，拨入终端获取的 IP 地址段为 10.0.150.0/24。

- VPN 提交截图：用户配置 VPN 的所有信息(包括 VPN1 和 VPN2)，包含配置过程中出现的每一个界面都需要截图。
- 将截图粘贴到“工位号_VPN 配置文档.doc”中，标记为“VPN 配置相关截图”，并对截图进行必要的说明，并保存到指定位置。

---

3. 系统安全配置

（1）总部三层交换机不转发源 IP 地址等于目的 IP 地址的数据报，和源端口等于目的端口的数据报，且在网络内只允许使用默认选项的 ping 命令，即 ICMP request 报文不可分片，且净荷长度一般小于 100；

（2）配置访问控制列表，禁止 VLAN10 的用户访问 Windows FTP 服务器，禁止 VLAN40 的用户访问 SAMBA 服务器；

（3）分别在集团公司的接入交换机上 SW3 及 SW4 上的 Ethernet1/1 开启端口的保护功能，防止 PC 机发出网关欺骗报文；

（4）对服务器群资源进行震荡波、SQL 蠕虫病毒的防护；

（5）请将软件部某开发终端主机 IP 地址与 MAC 地址绑定（该终端的 MAC 地址为：47-01-39-04-17-ff,IP 地址可参考表 1-4 中软件部的一个可用 IP 地址）；

（6）请配置 SW3 交换机的 Ethernet 1/1-2 端口为 802.1X 认证端口，交换机的管理地址、终端的 IP 地址、认证服务器的地址请根据前面规划进行设置；

（7）在 SW1 交换机上配置 DHCP Server 服务，为 VLAN40 网络中的 PC 分配动态 IP 地址。其中可分配的网段范围、网关、DNS 地址可根据 1-4 表规划确定。

【结果文件的提交】

在 RT1、RT2、RT3、SW1、SW2、SW3、SW4 上运行 show running-config，将运行结果粘贴到“工位号_网络配置文档.doc”中（如 47 号工位的文件命名为：47_网络配置文档.doc），此时文档已经包含有：

（1）无线网络相关配置截图，

（2）VPN 配置相关截图，

（3）防火墙配置相关截图，

（4）请将路由器和交换机的 show running-config 信息接着写入：

①RT1 的 show running-config 信息；②RT2 的 show running-config 信息；

③RT3 的 show running-config 信息；④SW1 的 show running-config 信息；

⑤SW2 的 show running-config 信息；⑥SW3 的 show running-config 信息；

⑦SW4 的 show running-config 信息

所有设备需要通过文档的方式保存，名称与设备名称一致。并将所有文档保存到计算机桌面以自己参赛工位号文件夹内，若缺少文件，涉及到该文件对应设备下的所有分值记为 0 分。

第二部分服务器配置及应用项目

项目实施 Windows 操作系统部分

【注意事项】

（1）题目中所涉及 Windows 操作系统的 administrator 管理员用户密码为 2015Net（注意区分大小写），若未按照要求设置密码，涉及到该操作的所有分值记为 0 分。

（2）系统主机及虚拟主机的 IP 属性设置请按照网络拓扑结构图以及“表 1-5：IP 地址自行规划表”的要求设定。

（3）除非作特殊说明，在同一主机下需要安装相同操作系统版本的虚拟机时，可采用 OracleVM VirtualBox 软件自带的克隆系统功能实现。

（4)所有系统镜像文件及试题所需的其它软件均存放在每台主机的D:\soft 文件夹中，并将题目要求的截图内容以.jpg 格式存储于桌面 Backup 文件夹中。

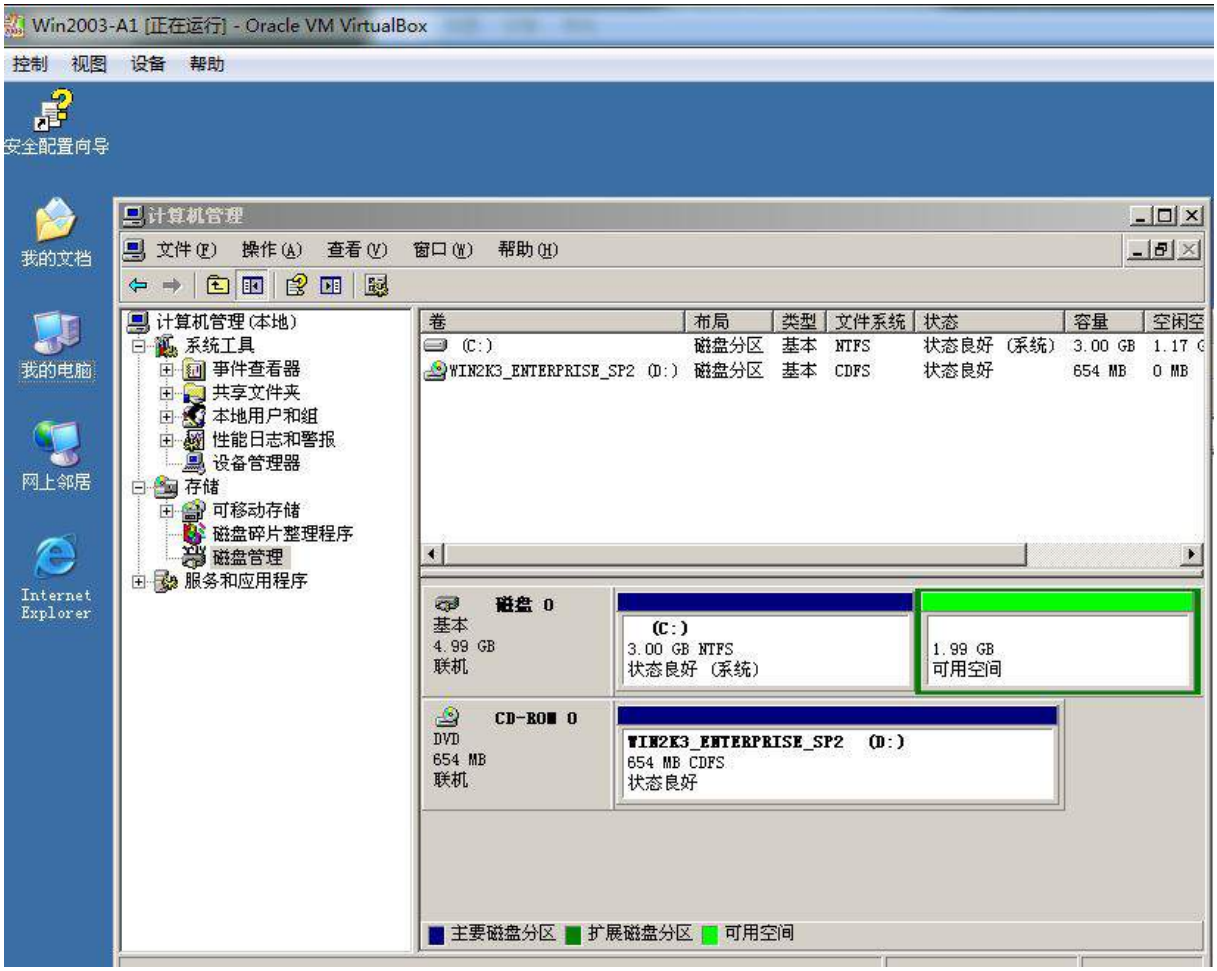
（5）请各位选手按下列要求完成各项服务器配置，在完成配置后提交能反映各个配置项目结果的窗口截图，比如 PC-A 中 Windows2003 系统的所有截图按照试题顺序粘贴在文件名为：工位号_PC-A.doc（如 47 号工位的文件命名为：47_PC-A.doc）的文档中。文档中要求有试题的题号小标题，并对每个截图进行必要的说明，无截图的项目不得分。

（6）所有设备需要通过文档的方式保存，名称与设备名称一致。并将所有文档保存到计算机桌面以自己参赛工位号文件夹内，若缺少文件，涉及到该文件对应设备下的所有分值记为 0 分。

一、在 PC-A 上完成如下操作

1. 完成虚拟主机的创建

（1）创建虚拟机“Win2003-A1”，具体要求为内存 512MB，硬盘 5GB，主分区 3GB，扩展分区 2GB；

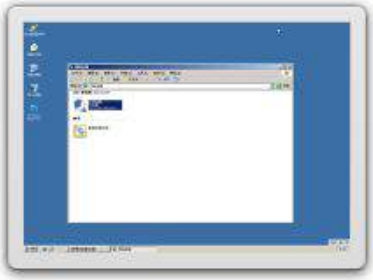


（2）创建虚拟机“Win2003-A2”，具体要求为内存 512MB，硬盘 5GB，主分区 3GB，扩展分区 2GB；

常规

名称: Win2003-A2
操作系统: Windows 2003 (64 bit)

预览



系统

内存大小: 512 MB
启动顺序: 软驱, 光驱, 硬盘
硬件加速: VT-x/AMD-V, 嵌套分页

显示

显存大小: 18 MB
远程桌面服务器: 已禁用
录像: 已禁用

存储

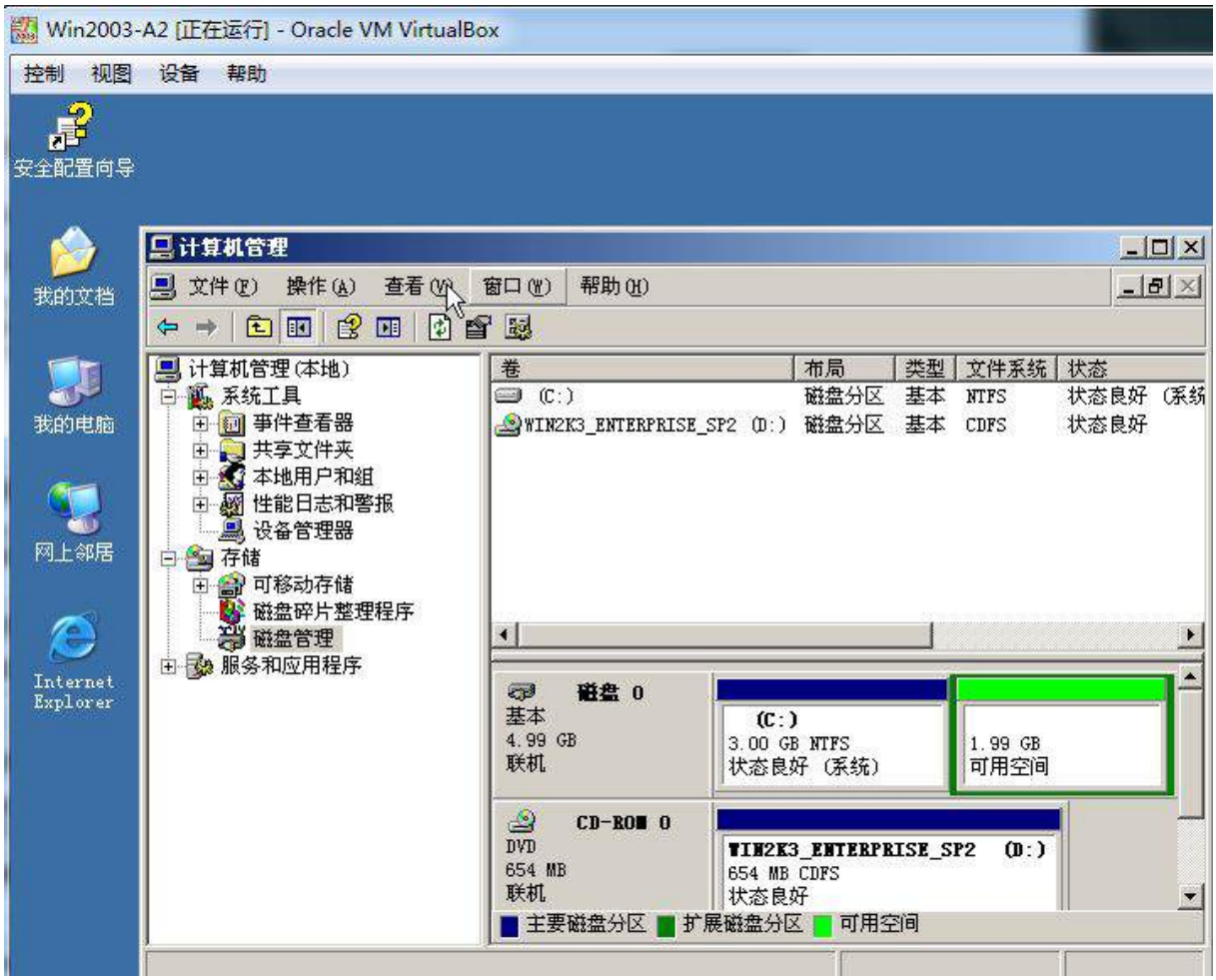
控制器: IDE
第一IDE控制器主通道: Win2003-A2.vdi (普通, 5.00 GB)
第二IDE控制器主通道: [光驱] Windows.Server.2003.企业版.SP2.原版安装光盘.ISO (654.34 MB)

声音

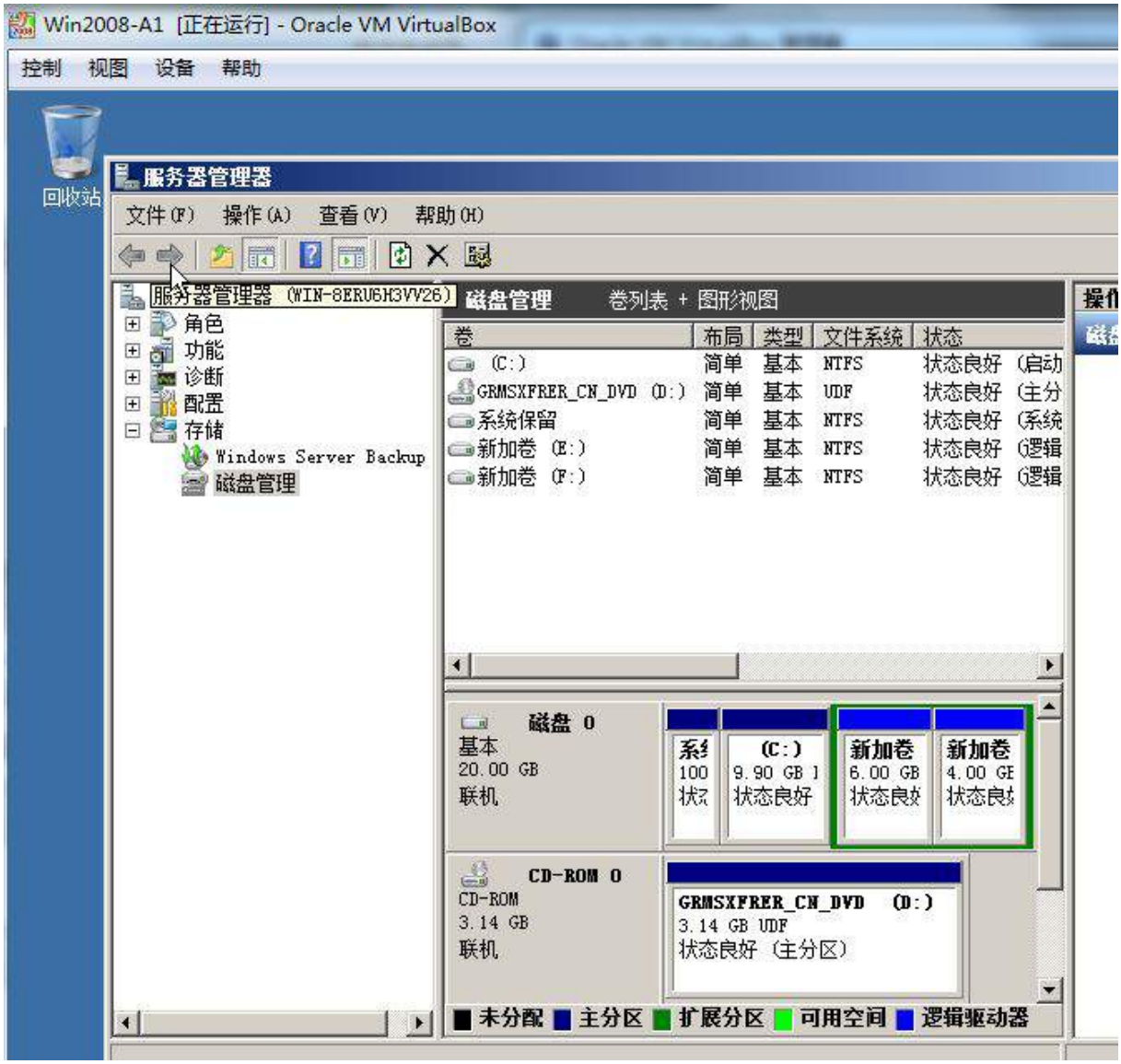
主机音频驱动: Windows DirectSound
控制芯片: Intel HD 音频

网络

网卡 1: Intel PRO/1000 MT 桌面 (桥接网络, Intel(R) Ethernet Connection I217-LM)



（3）创建虚拟机“Win2008-A1”,具体要求为内存 900MB,硬盘 20GB，主分区 10GB，扩展分区 10GB，分为两个逻辑分区，大小分别为 6GB 和 4GB；



（4）根据“拓扑结构图”和自行规划的“表 1-4”和“表 1-5”所示内容为 PC-A 物理主机及三台虚拟机配置正确的 IP 地址、子网掩码、网关和 DNS，将 PC-A 物理主机的 IP 地址配置界面截图保存，在 Windows 系统中使用 ipconfig/all 将显示所有结果的界面截图保存。

2. 在主机 Win2003-A1 和 Win2003-A2 中分别完成 DNS、WWW 服务器的部署

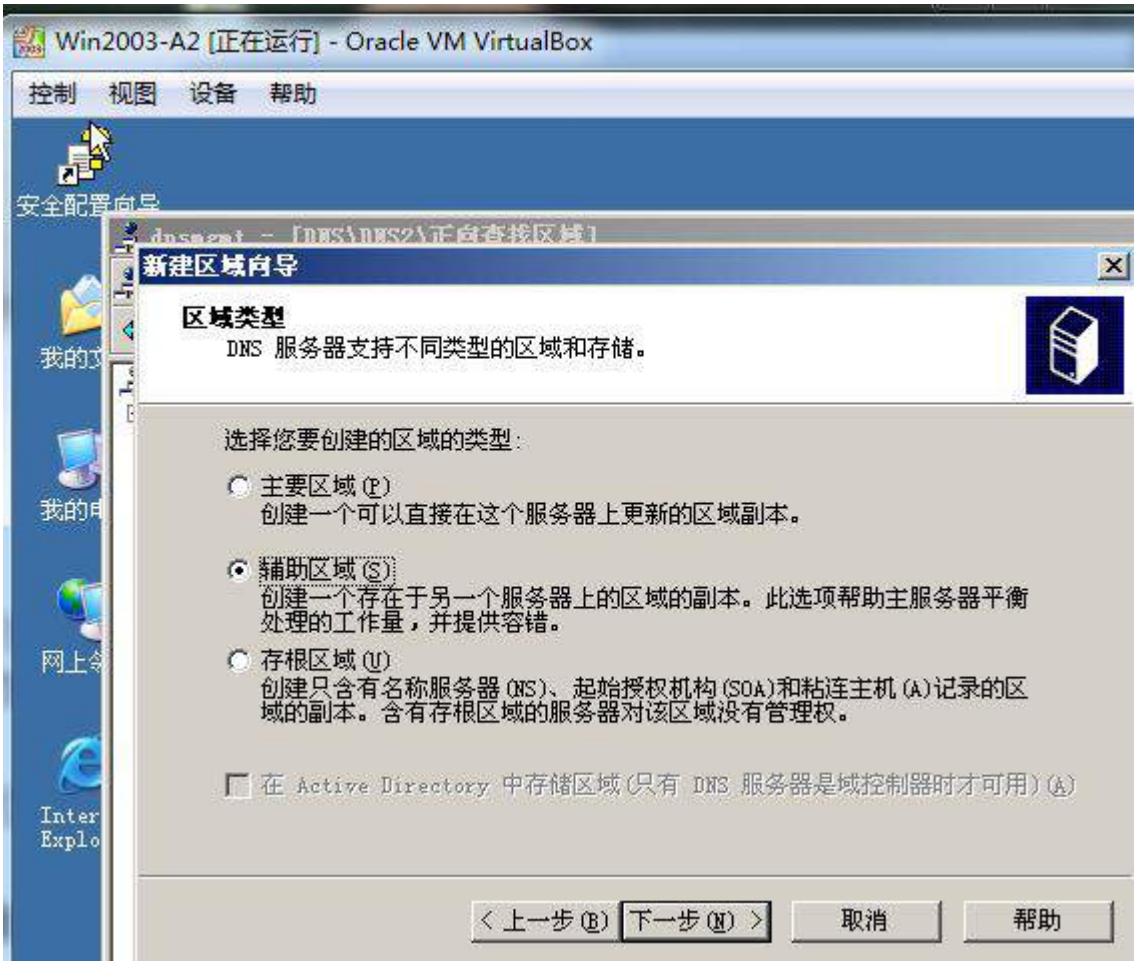
（1）将上述两服务器配置为 DNS 和 WWW 服务器，完成实现 HTTP、DNS 服务的配置，实现 dns.tj.com 对应 IP 地址分配表 1-5 规划内容，web.tj.com 对应 IP 地址分配表 1-5 规划内容进行设置；

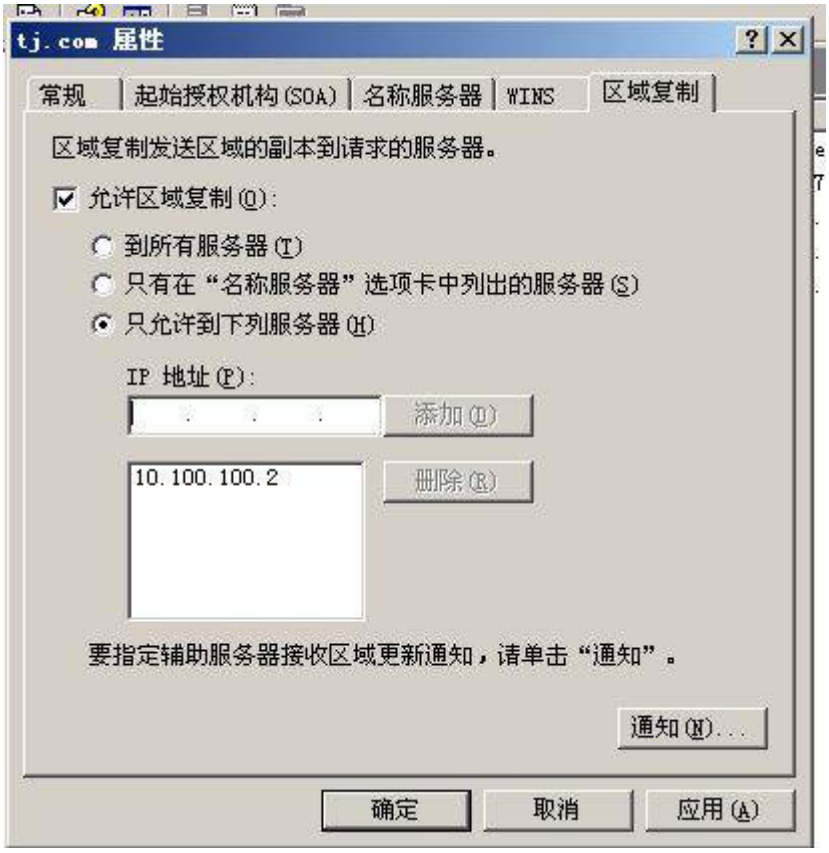
（2）创建 IIS 默认主页，内容为“Erp 服务器 Win2003_A1 安装成功!”，通过 IE 浏览器访问地址 http://x.x.x.x（IP 地址参见分配表 1-5 自行规划内容），将 IE 浏览器显示内容截图，确保截图包含地址栏，截图粘贴到竞赛结果文件指定位置；

（3）在 Windows 2003 中的 DNS 管理器中，将 tj.com 的正向查询区域记录界面截图，确保截图可以看到 erp、ftp、www 的主机地址。将截图粘贴到竞赛结果文件指定位置。

3. Windows 2003 系统中实现负载均衡配置

作为公司总部， ERP 系统是公司经营的关键系统，为了保证服务可靠性，采用 Windows 2003 Server 负载均衡技术，实现 2 台虚拟机对 HTTP 服务的负载均衡，并建立辅助 DNS 服务器，实现 Sin2003-A1 中 tj.com 解析区域的复制。


Win2003-A2 [正在运行] - Oracle VM VirtualBox
控制 视图 设备 帮助
新建区域向导
区域类型
DNS 服务器支持不同类型的区域和存储。
选择您要创建的区域的类型：
主要区域(P)
创建一个可以直接在这个服务器上更新的区域副本。
辅助区域(S)
创建一个存在于另一个服务器上的区域的副本。此选项帮助主服务器平衡处理的工作量，并提供容错。
存根区域(U)
创建只含有名称服务器(NS)、起始授权机构(SOA)和粘连主机(A)记录的区域的副本。含有存根区域的服务器对该区域没有管理权。
在 Active Directory 中存储区域(只有 DNS 服务器是域控制器时才可用)(A)
< 上一步(B)
下一步(N) >
取消
帮助


tj.com 属性
常规
起始授权机构(SOA)
名称服务器
WINS
区域复制
区域复制发送区域的副本到请求的服务器。
允许区域复制(O):
到所有服务器(T)
只有在“名称服务器”选项卡中列出的服务器(S)
只允许到下列服务器(H)
IP 地址(P):
添加(D)
10.100.100.2
删除(R)
要指定辅助服务器接收区域更新通知，请单击“通知”。
通知(N)...
确定
取消
应用(A)

（1）在 PC-A 虚拟机系统中，2 台 Windows 2003 Server 的负载均衡服务的拓扑结构如图 2-1 负载均衡拓扑结构图所示：

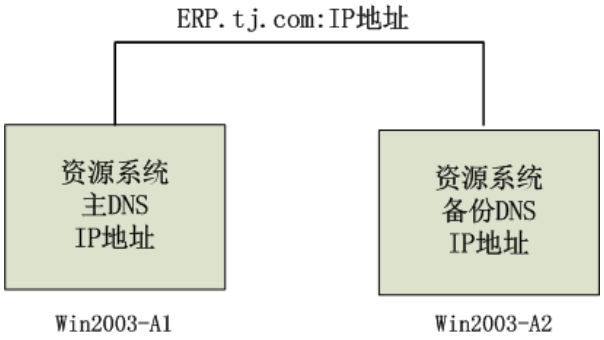
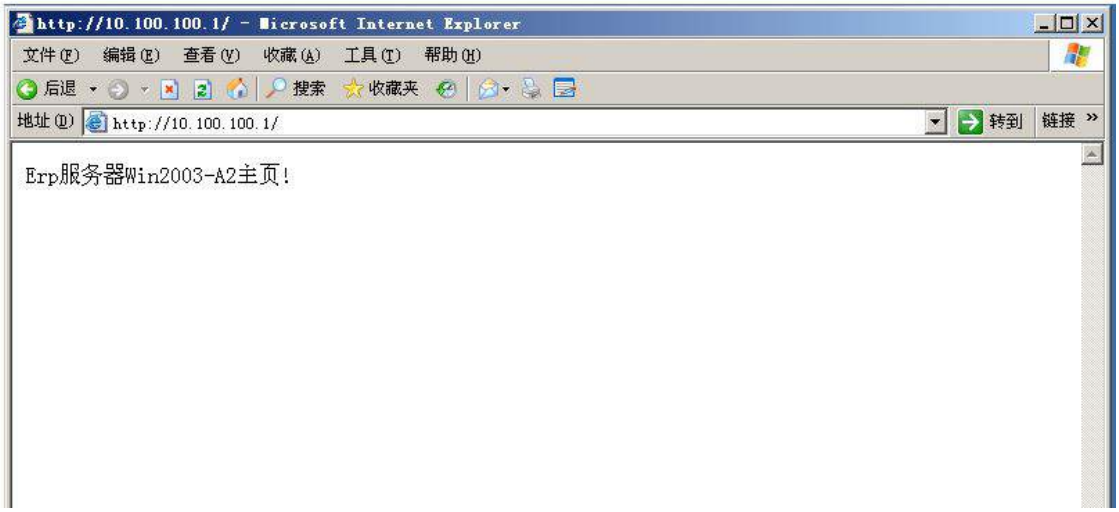
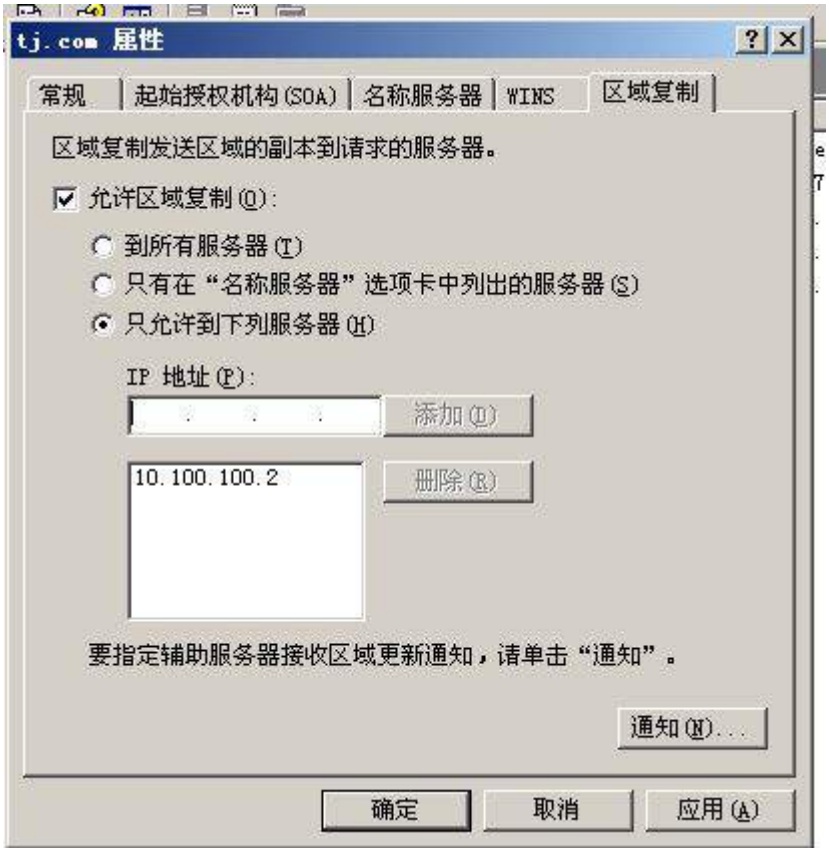


图 2-1　负载均衡拓扑结构图

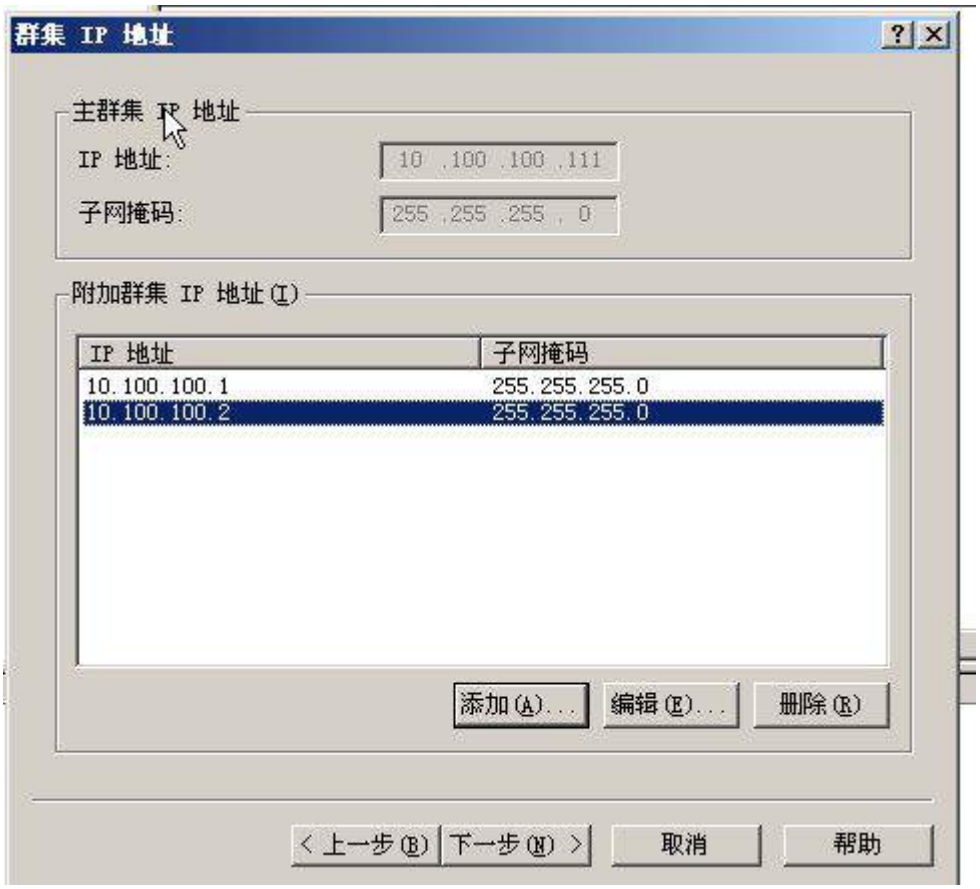
（2）在 PC-A 的虚拟机中，实现第二台 Windows 2003 Server 的安装，设置 IP 地址可参看服务器 IP 地址规划表 1-5，主机名为 Win2003-A2。实现与 Win2003-A1 相同的 HTTP 网络服务，但创建默认主页内容为“Erp 服务器 Win2003-A2 主页!”；

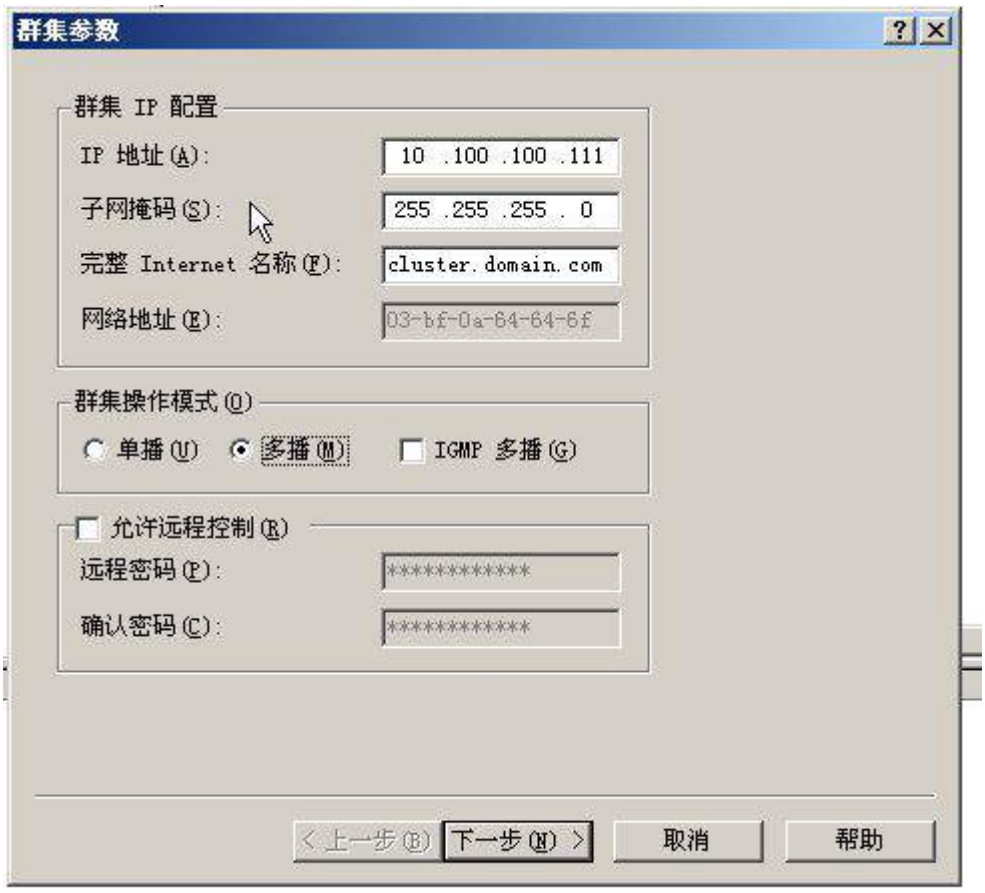


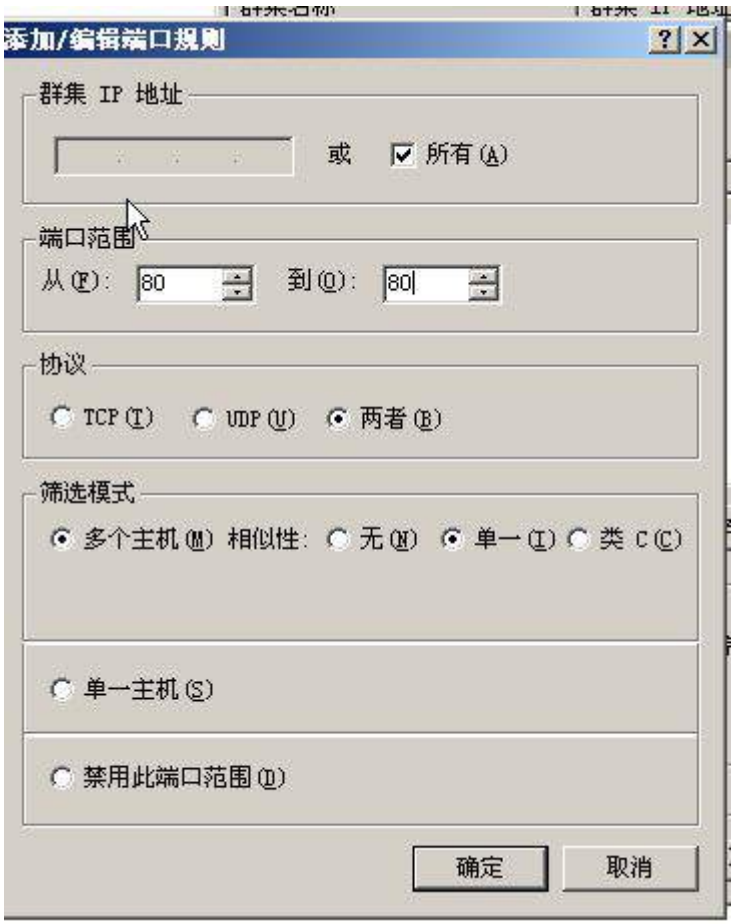
（3）在 win2003-A2 中，进行辅助 DNS 服务器配置，实现 win2003-A1 中 tj.com 解析区域的复制，要求 win2003-A1 的 DNS 服务器只允许由 win2003-A2 复制解析区域；



（4）按照图 2-1 负载均衡拓扑结构图确定的配置信息，设置这 2 台虚拟机的负载均衡，操作模式为多播，只对 80 端口启用负载均衡。

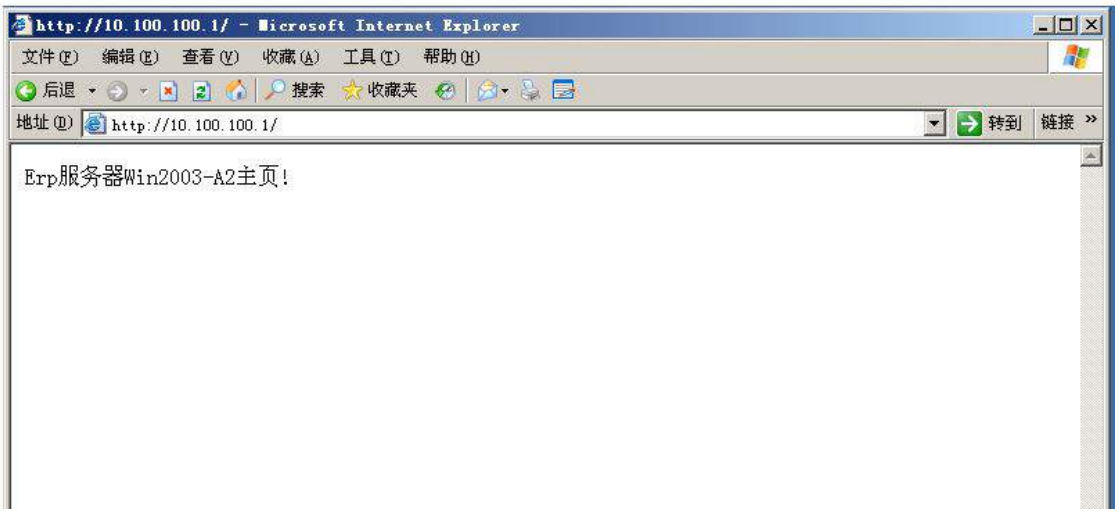



群集参数
群集 IP 配置
IP 地址(A):
10 .100 .100 .111
子网掩码(S):
255 .255 .255 . 0
完整 Internet 名称(F):
cluster.domain.com
网络地址(E):
03-bf-0a-64-64-6f
群集操作模式(O)
单播(U)
多播(M)
IGMP 多播(G)
允许远程控制(R)
远程密码(P):
确认密码(C):
< 上一步(B)
下一步(N) >
取消
帮助

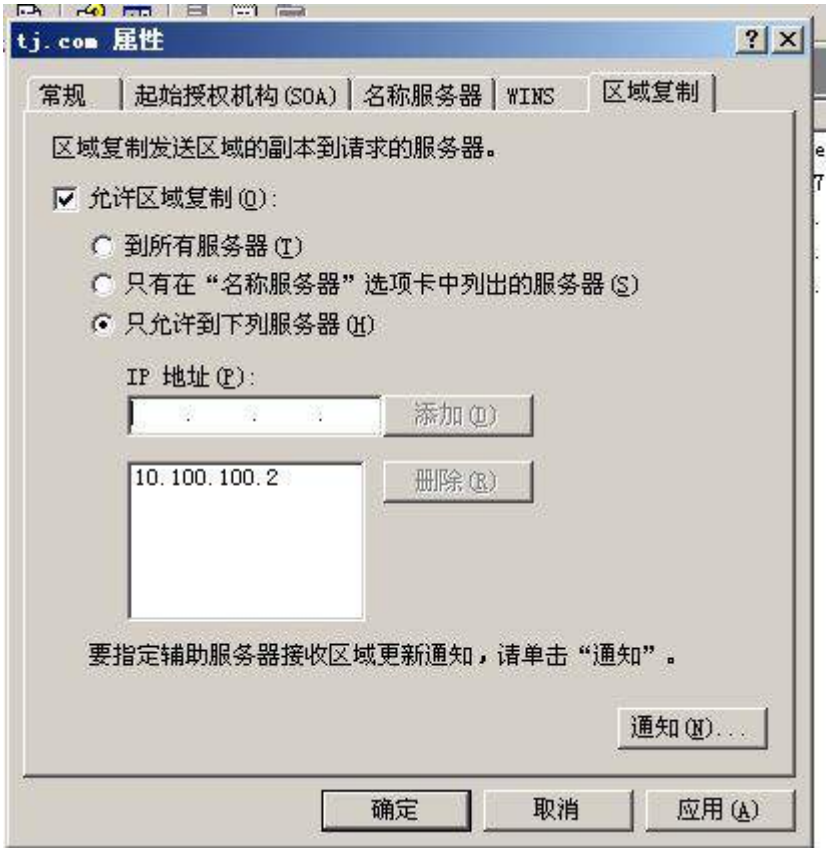


（5）验证并保存下列结果文件：

①在上述配置操作完成后，在 Win2003-A2 中，利用 IE 浏览器访问 http://x.x.x.x（IP 地址参见分配表 1-5 自行规划内容），将 IE 浏览器显示内容截图，确保截图包含地址栏，将截图粘贴到竞赛结果文件指定位置；



②在 Win2003-A1 的 DNS 管理器中，右键点击正向查询区域中 tj.com，选择属性，将其“区域复制”属性页截图，确保截图可以看到允许复制的 IP 地址。将截图粘贴到竞赛结果文件指定位置；



③在 Win2003-A2 的 DNS 管理器中，右键点击正向查询区域中 tj.com，选择属性，将其“常规”属性页截图，确保截图可以看到 IP 地址。将截图粘贴到竞赛结果文件指定位置；

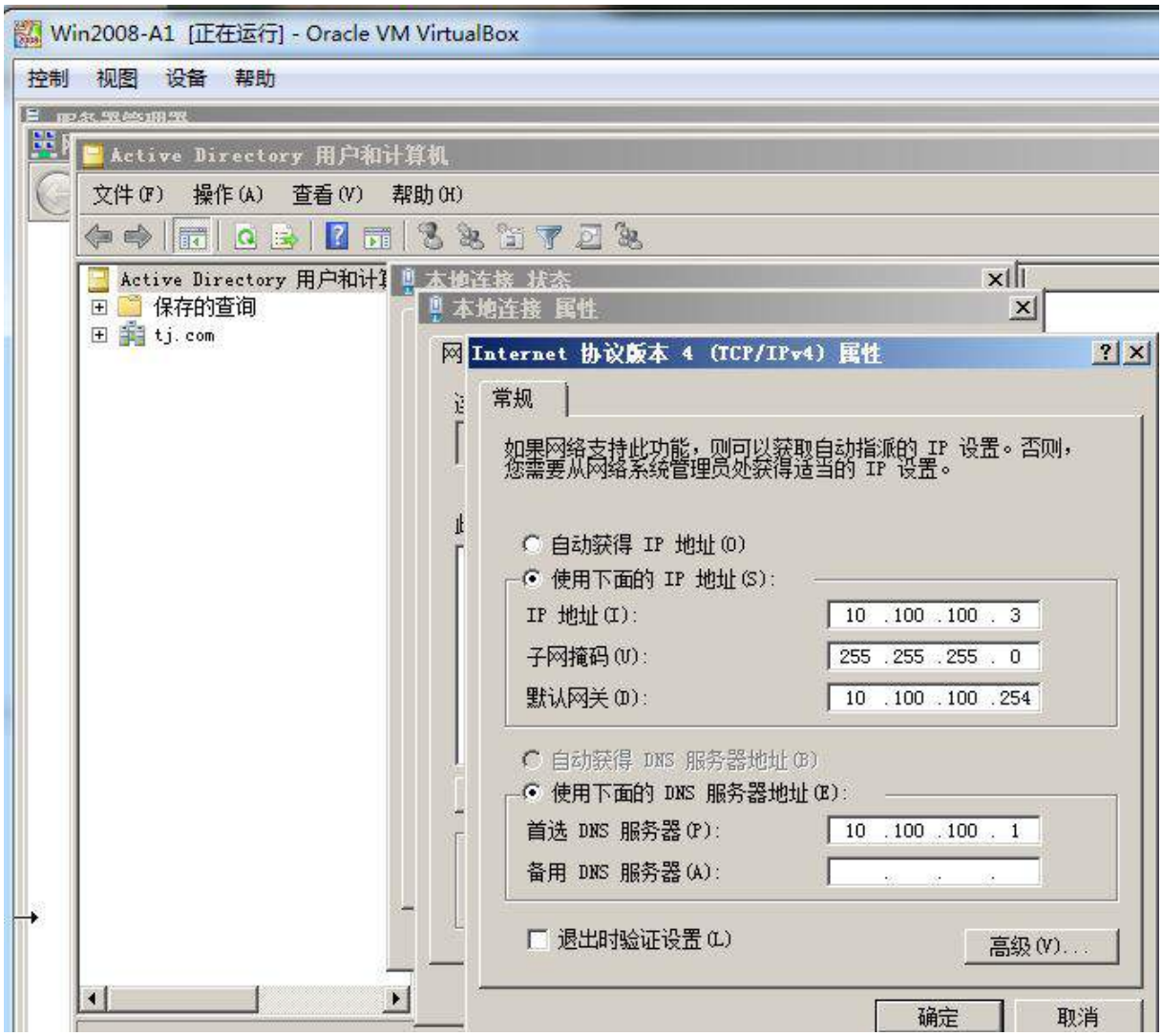
④在 Win2003-A1 的“网络负载平衡管理器”中，通过“加载主机列表文件”（赛场选手可自行制作该“服务器负载均衡.txt”文件），待 2 台负载均衡主机完全导入后，将“网络负载平衡管理器”截图，将截图粘贴到竞赛结果文件指定位置；

⑤在 PC-A 的操作系统桌面中，配置网卡的 DNS 地址为（IP 地址参见分配表 1-5 自行规划内容）利用 IE 浏览器，访问 http://erp.tj.com，将 IE 浏览器显示内容截图，确保截图包含地址栏，将截图粘贴到竞赛结果文件指定位置，然后关闭 IE 浏览器浏览页面显示的那台 Windows 2003 虚拟主机，待该主机关闭后，重新浏览 http://erp.tj.com 地址，经过多次刷新，检查该网页服务是否依然有效，如果确认有效，请将将 IE 浏览器显示内容截图，确保截图包含地址栏，将截图粘贴到竞赛结果文件指定位置。

（已测试）

4. 在主机 Win2008-A1 中完成 DC 域控制器的部署

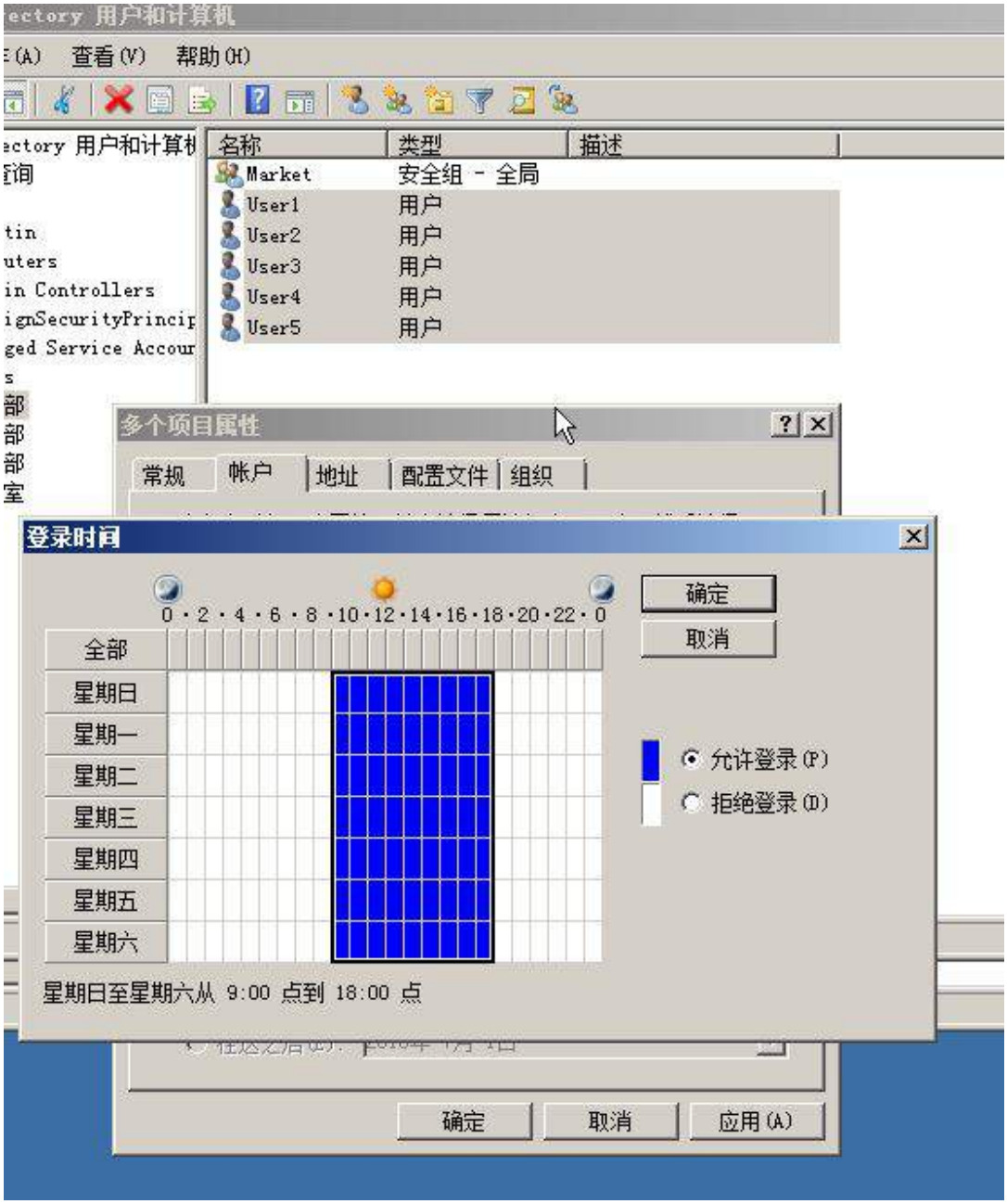
（1）将此服务器升级为域控，DNS 域名解析服务由服务器 Win2003-A1 提供，域名为 tj.com；将截图粘贴到竞赛结果文件指定位置；

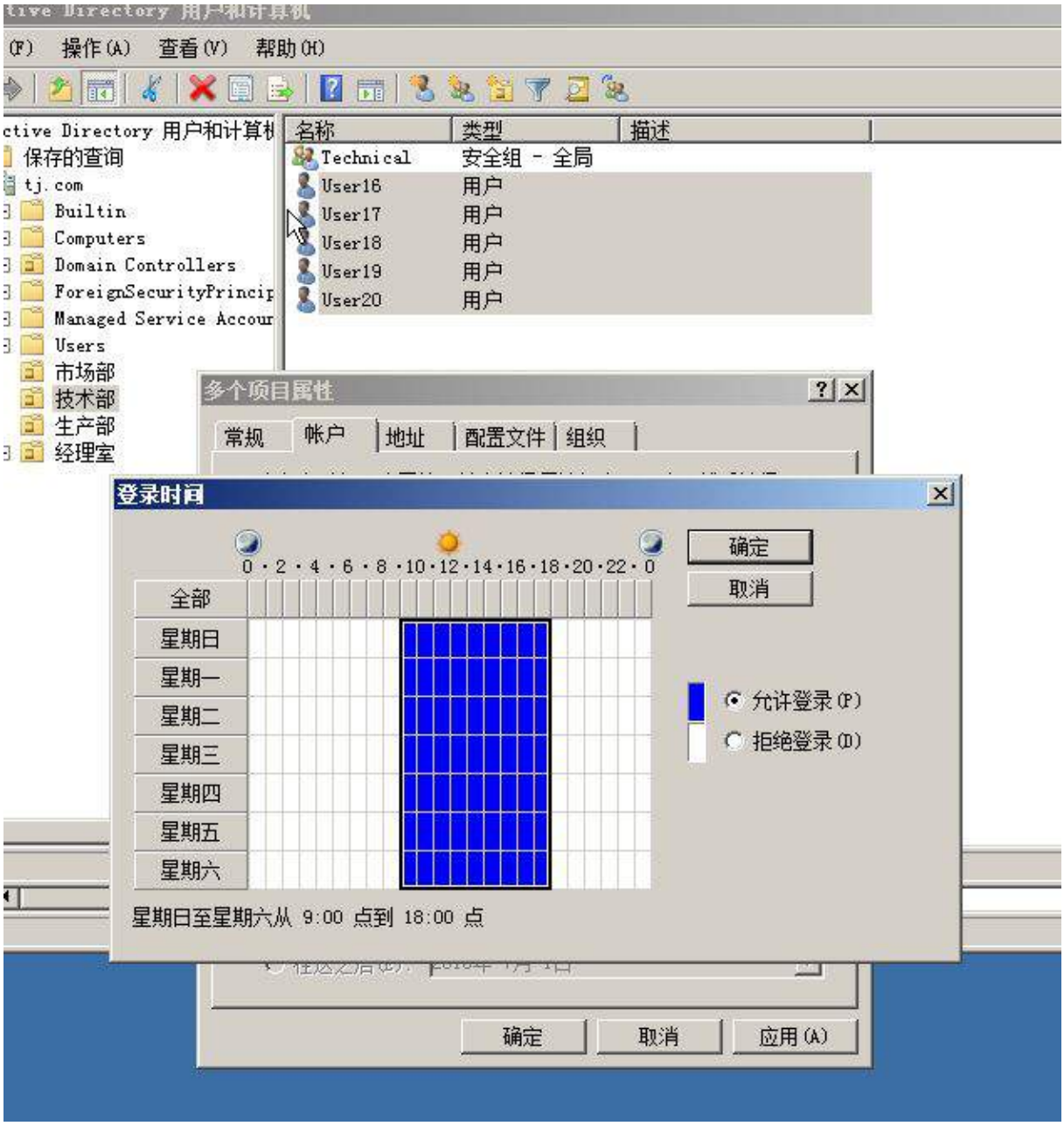


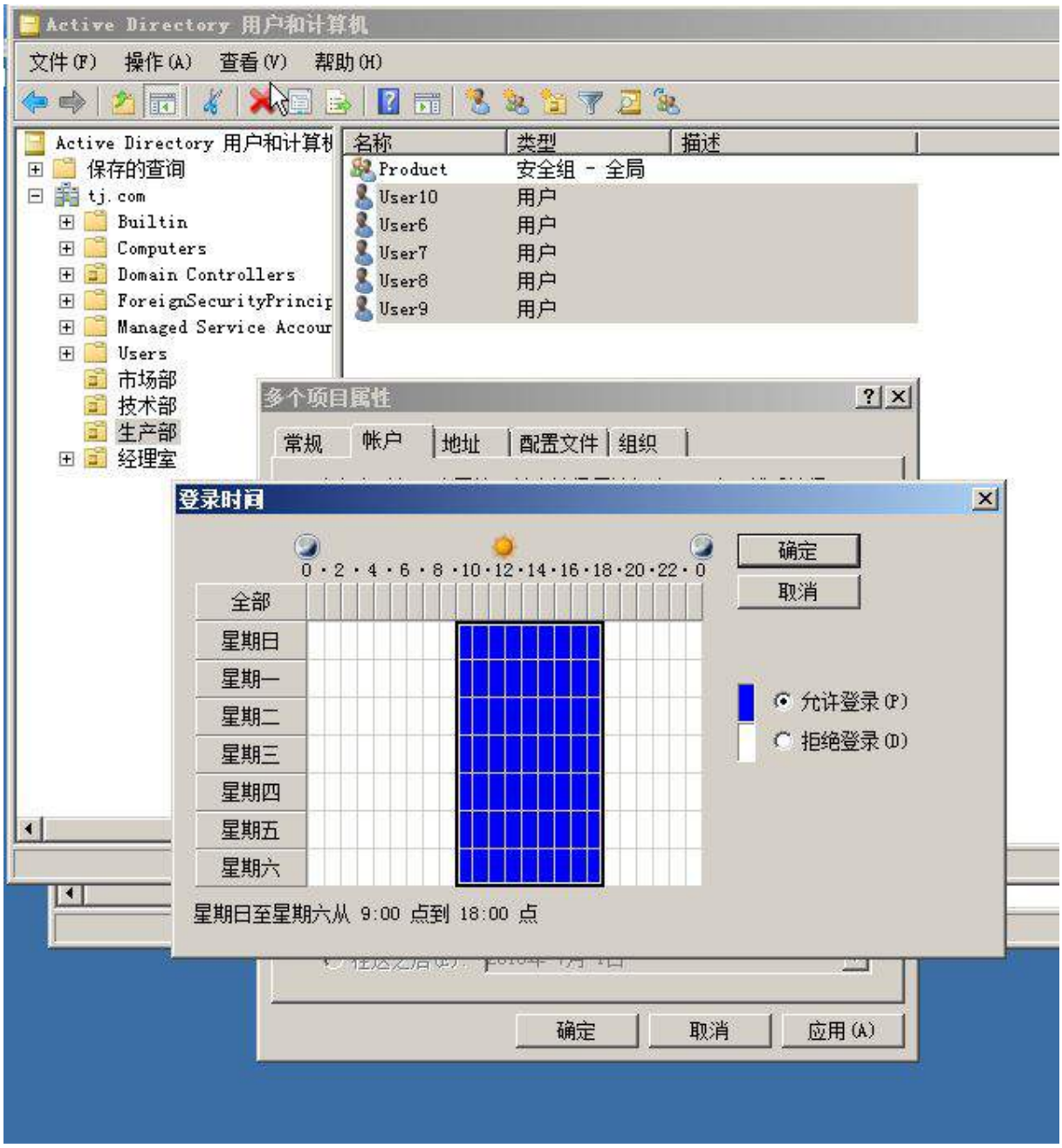
（2）以下用户工作时间为 9:00~18:00；

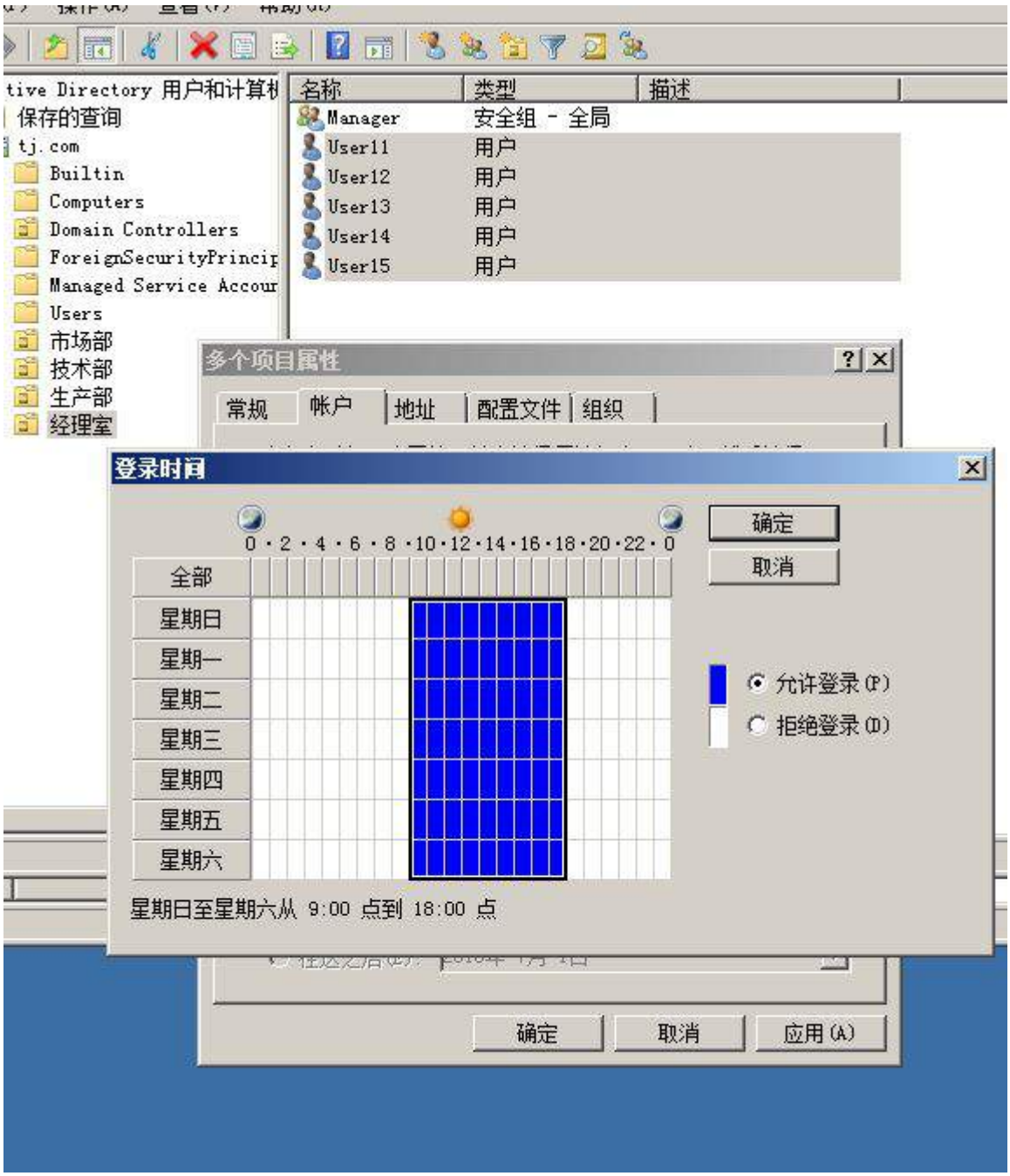
表 2-1 域用户信息表

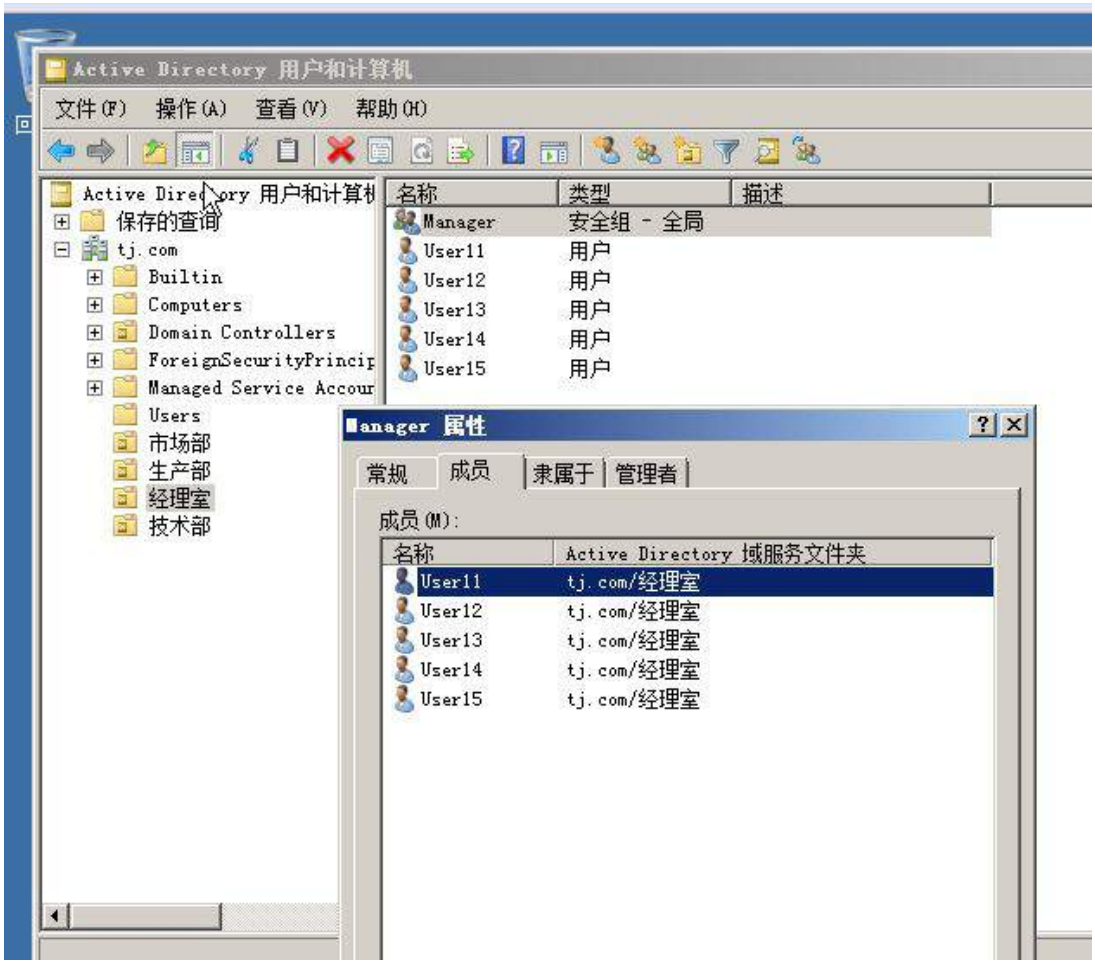
组织单位	全局组	用户
市场部	Market	User1-user5
生产部	Product	User6- user10
经理室	Manager	User11- user15
技术部	Technical	User16- user20

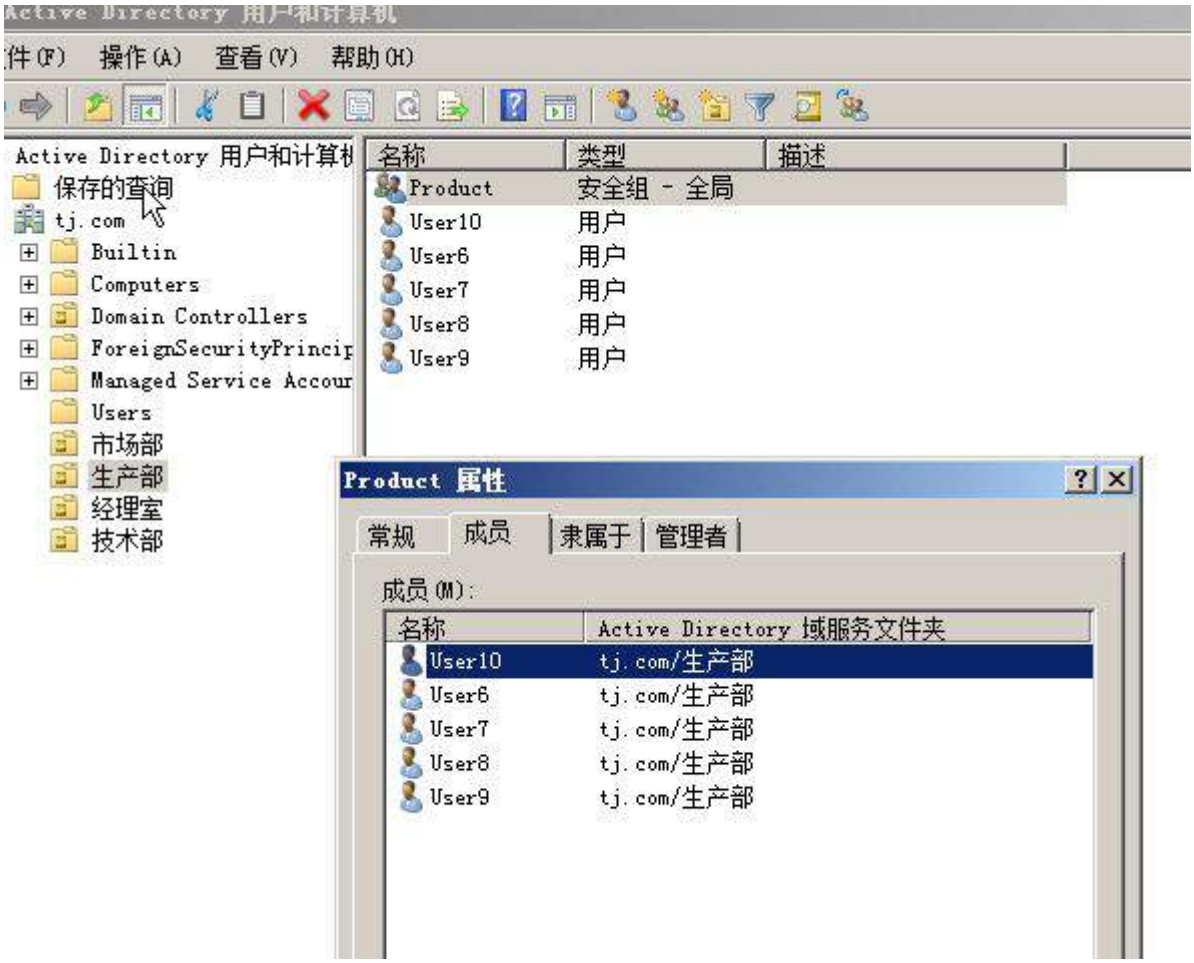

ectory 用户和计算机
(A) 查看(V) 帮助(H)
名称 类型 描述
Market 安全组 - 全局
User1 用户
User2 用户
User3 用户
User4 用户
User5 用户
多个项目属性
常规 帐户 地址 配置文件 组织
登录时间
0 · 2 · 4 · 6 · 8 · 10 · 12 · 14 · 16 · 18 · 20 · 22 · 0
全部
星期日
星期一
星期二
星期三
星期四
星期五
星期六
确定
取消
允许登录(P)
拒绝登录(D)
星期日至星期六从 9:00 点到 18:00 点
确定
取消
应用(A)

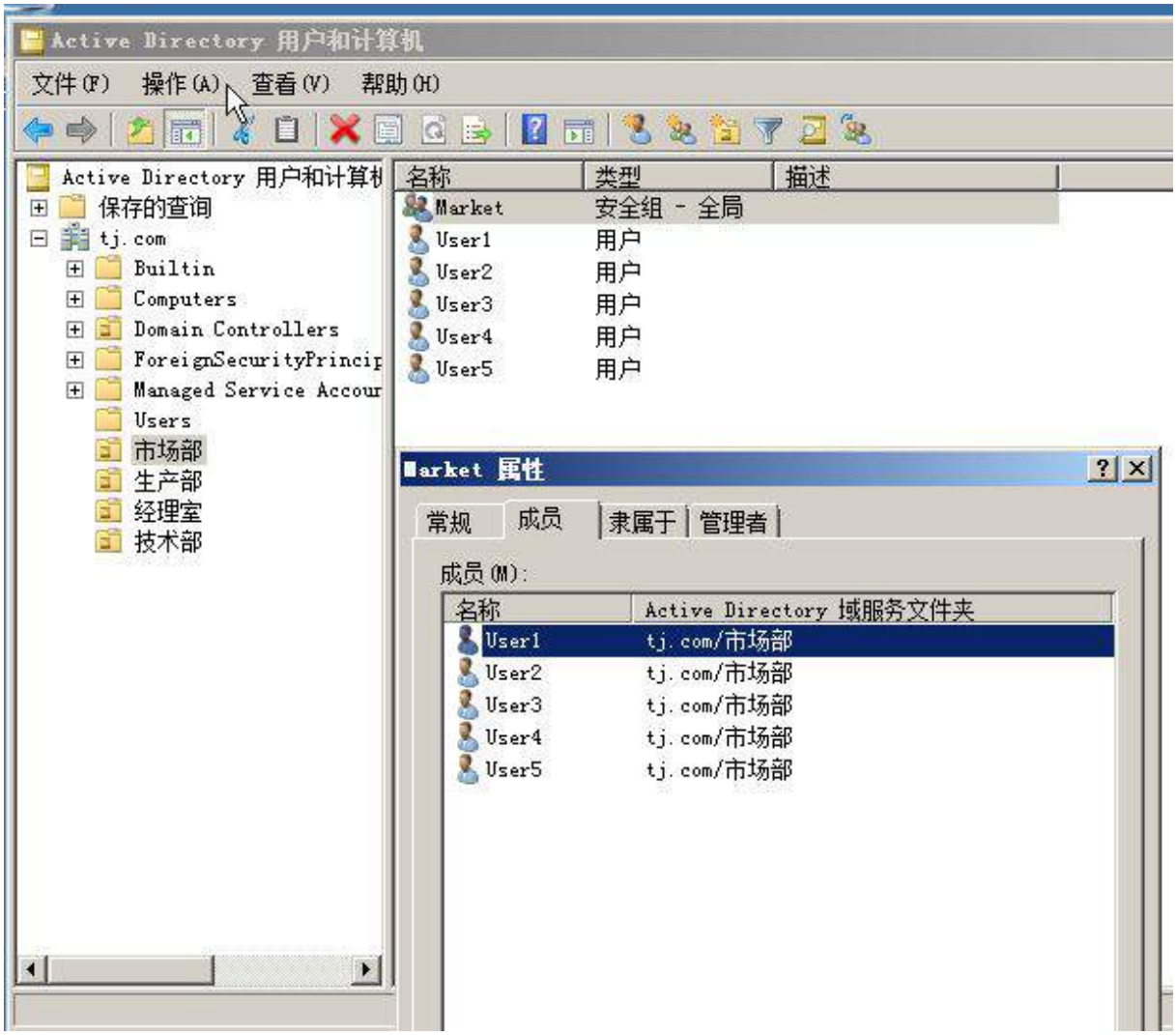

(F) 操作(A) 查看(V) 帮助(H)
ctive Directory 用户和计算机
保存的查询
tj.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincip
Managed Service Accour
Users
市场部
技术部
生产部
经理室
名称
类型
描述
Technical 安全组 - 全局
User16 用户
User17 用户
User18 用户
User19 用户
User20 用户
多个项目属性
常规
帐户
地址
配置文件
组织
登录时间
0 · 2 · 4 · 6 · 8 · 10 · 12 · 14 · 16 · 18 · 20 · 22 · 0
全部
星期日
星期一
星期二
星期三
星期四
星期五
星期六
确定
取消
允许登录(P)
拒绝登录(D)
星期日至星期六从 9:00 点到 18:00 点
确定
取消
应用(A)

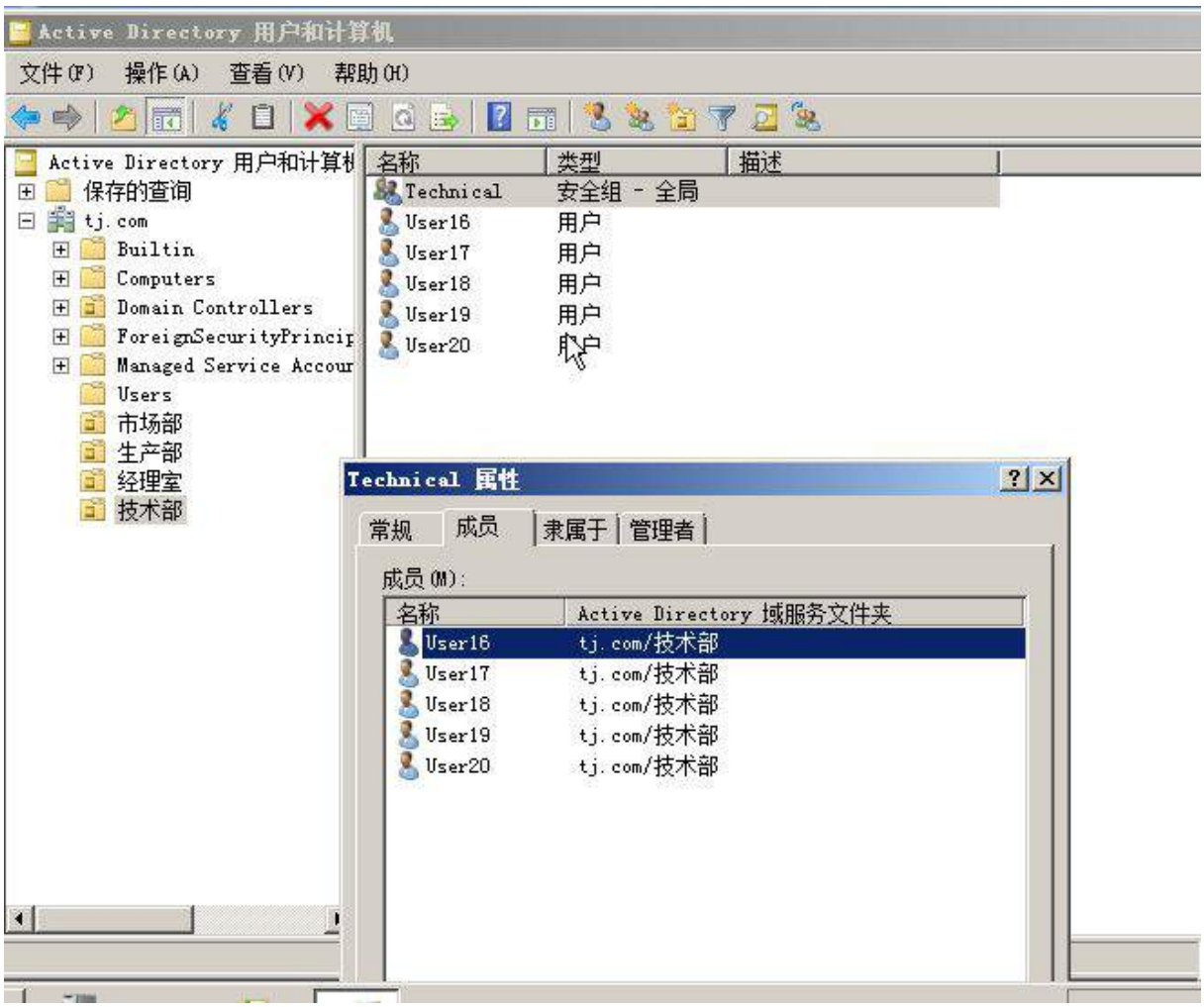

Active Directory 用户和计算机
文件(F) 操作(A) 查看(V) 帮助(H)
Active Directory 用户和计算机
保存的查询
tj.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincip
Managed Service Accour
Users
市场部
技术部
生产部
经理室
名称 类型 描述
Product 安全组 - 全局
User10 用户
User6 用户
User7 用户
User8 用户
User9 用户
多个项目属性
常规 帐户 地址 配置文件 组织
登录时间
0 · 2 · 4 · 6 · 8 · 10 · 12 · 14 · 16 · 18 · 20 · 22 · 0
全部
星期日
星期一
星期二
星期三
星期四
星期五
星期六
确定
取消
允许登录(P)
拒绝登录(D)
星期日至星期六从 9:00 点到 18:00 点
确定
取消
应用(A)


tive Directory 用户和计算机
保存的查询
tj.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincip
Managed Service Accour
Users
市场部
技术部
生产部
经理室
名称
类型
描述
Manager
安全组 - 全局
User11
用户
User12
用户
User13
用户
User14
用户
User15
用户
多个项目属性
常规
帐户
地址
配置文件
组织
登录时间
0 · 2 · 4 · 6 · 8 · 10 · 12 · 14 · 16 · 18 · 20 · 22 · 0
全部
星期日
星期一
星期二
星期三
星期四
星期五
星期六
确定
取消
允许登录(P)
拒绝登录(D)
星期日至星期六从 9:00 点到 18:00 点
确定
取消
应用(A)


Active Directory 用户和计算机
文件(F) 操作(A) 查看(V) 帮助(H)
Active Directory 用户和计算机
保存的查询
tj.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincip
Managed Service Accour
Users
市场部
生产部
经理室
技术部
名称 类型 描述
Manager 安全组 - 全局
User11 用户
User12 用户
User13 用户
User14 用户
User15 用户
anager 属性
常规 成员 隶属于 管理者
成员(M):
名称 Active Directory 域服务文件夹
User11 tj.com/经理室
User12 tj.com/经理室
User13 tj.com/经理室
User14 tj.com/经理室
User15 tj.com/经理室


Active Directory 用户和计算机
件(F) 操作(A) 查看(V) 帮助(H)
Active Directory 用户和计算机
保存的查询
tj.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincip
Managed Service Accour
Users
市场部
生产部
经理室
技术部
名称 类型 描述
Product 安全组 - 全局
User10 用户
User6 用户
User7 用户
User8 用户
User9 用户
Product 属性
常规 成员 隶属于 管理者
成员(M):
名称 Active Directory 域服务文件夹
User10 tj.com/生产部
User6 tj.com/生产部
User7 tj.com/生产部
User8 tj.com/生产部
User9 tj.com/生产部

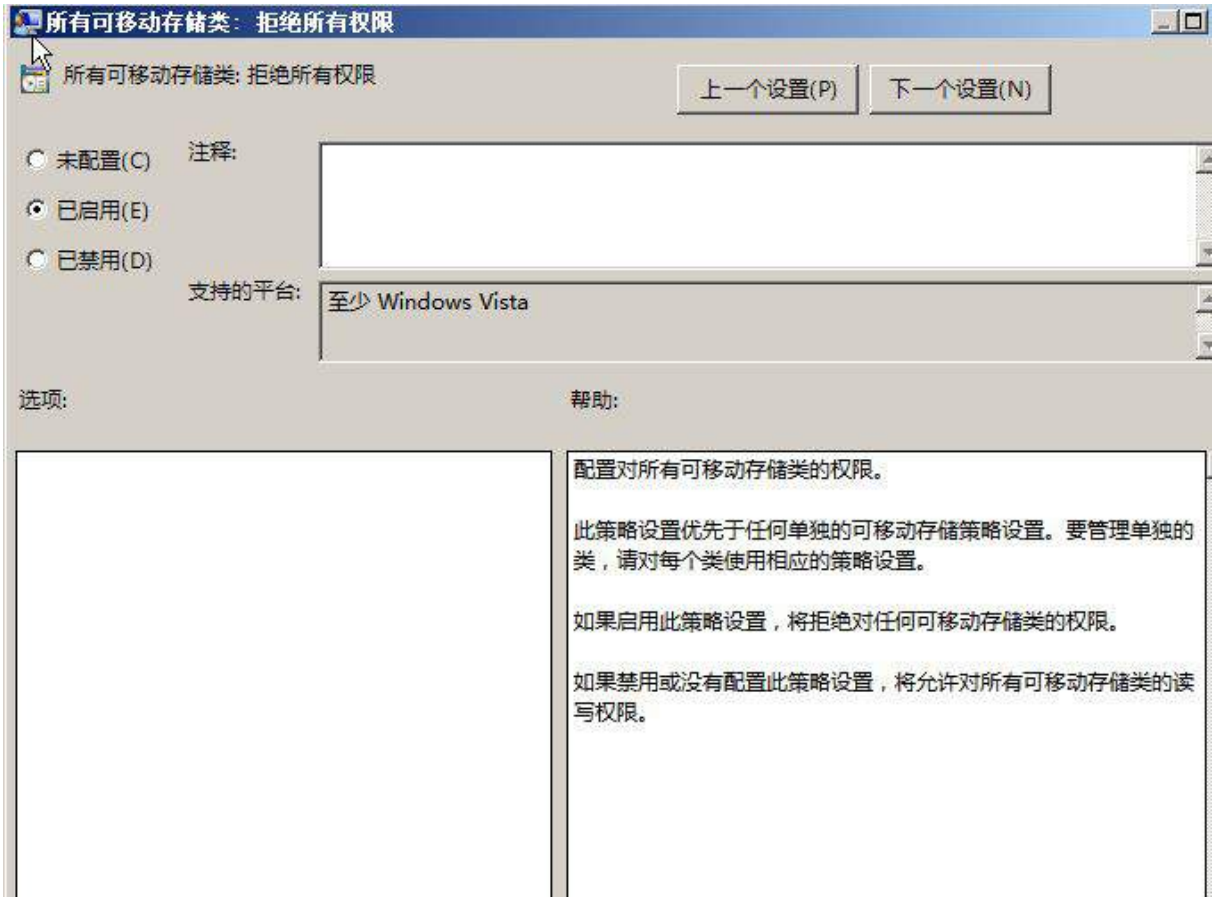

Active Directory 用户和计算机
文件(F) 操作(A) 查看(V) 帮助(H)
Active Directory 用户和计算机
保存的查询
tj.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincip
Managed Service Accour
Users
市场部
生产部
经理室
技术部
名称 类型 描述
Market 安全组 - 全局
User1 用户
User2 用户
User3 用户
User4 用户
User5 用户
arket 属性
常规 成员 隶属于 管理者
成员(M):
名称 Active Directory 域服务文件夹
User1 tj.com/市场部
User2 tj.com/市场部
User3 tj.com/市场部
User4 tj.com/市场部
User5 tj.com/市场部



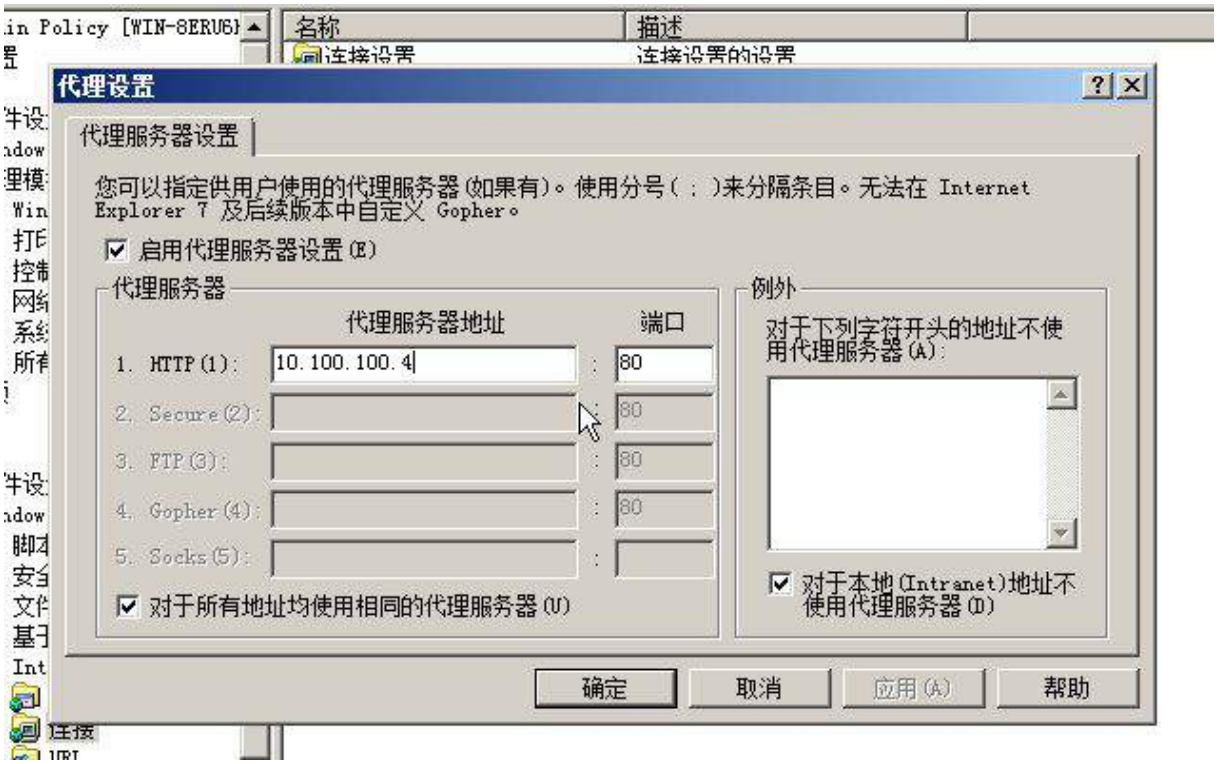
（3）为了减轻管理负担，委派用户 user6 组织单元“生产部”有新建删除用户和组的权限；

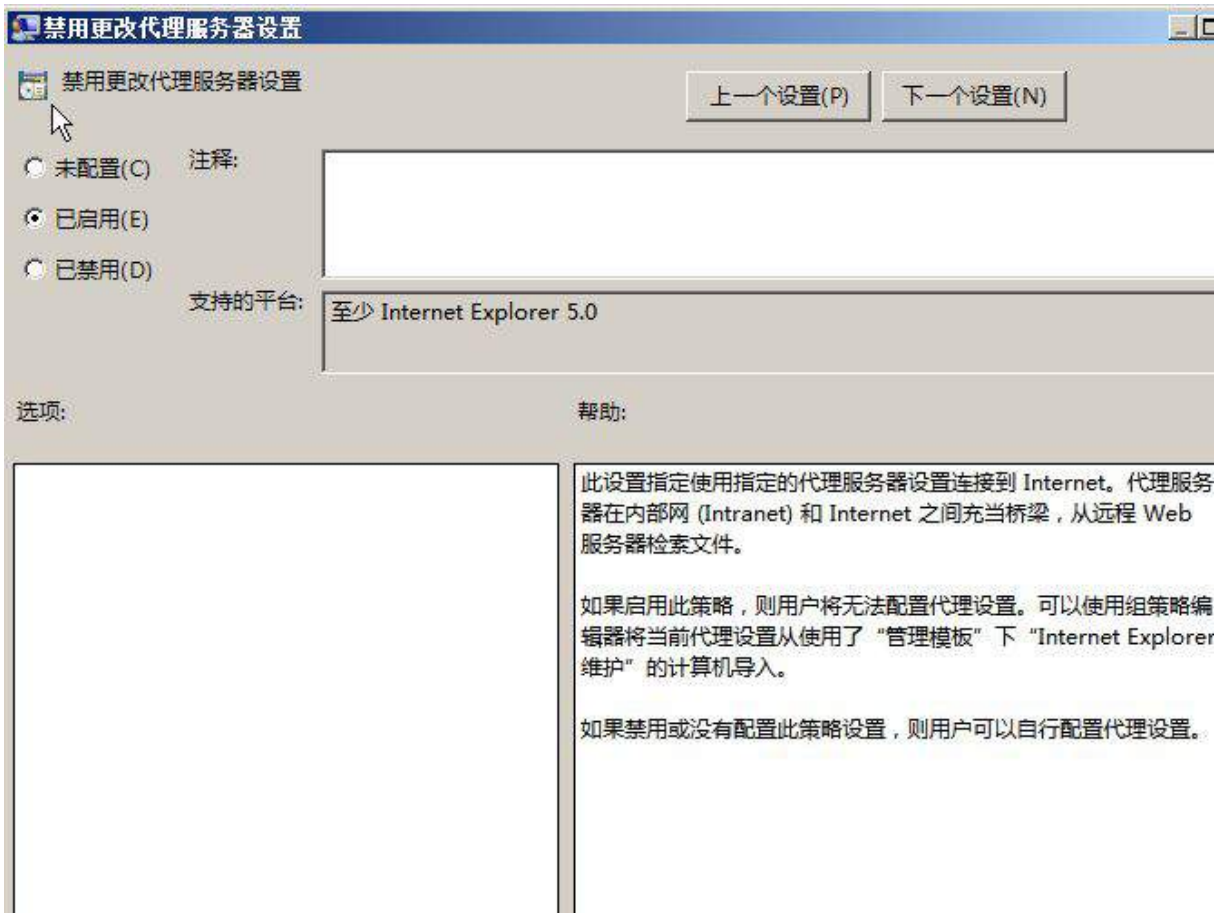
（4）配置组策略：

①禁止用户使用可移动存储类策略；

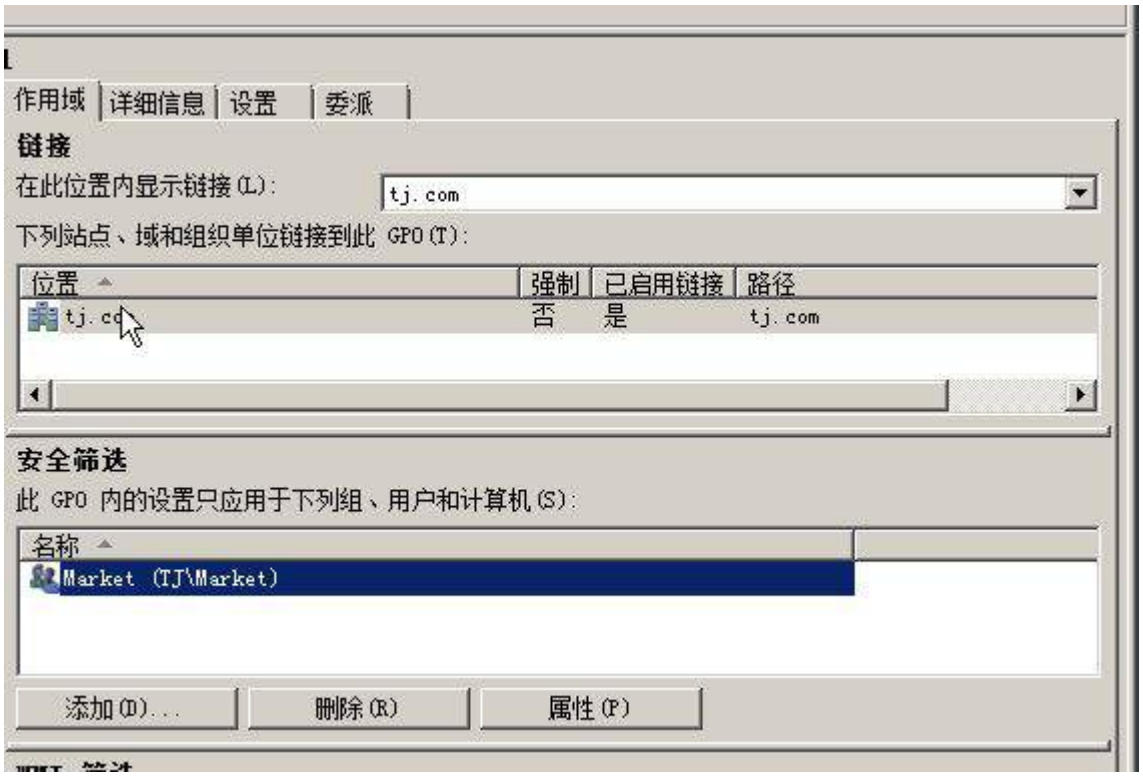


②设置 IE 代理服务器地址为:（参见 IP 地址分配表 1-5 自行规划内容），禁止客户端更改代理服务器地址；

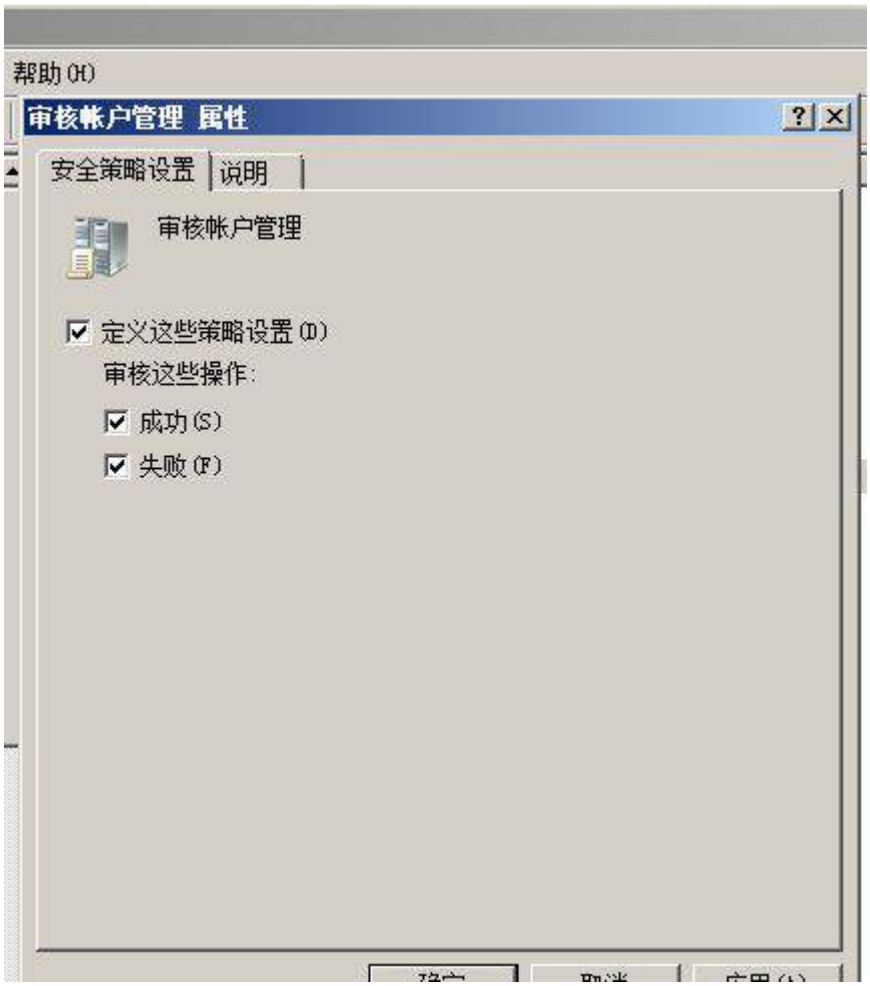




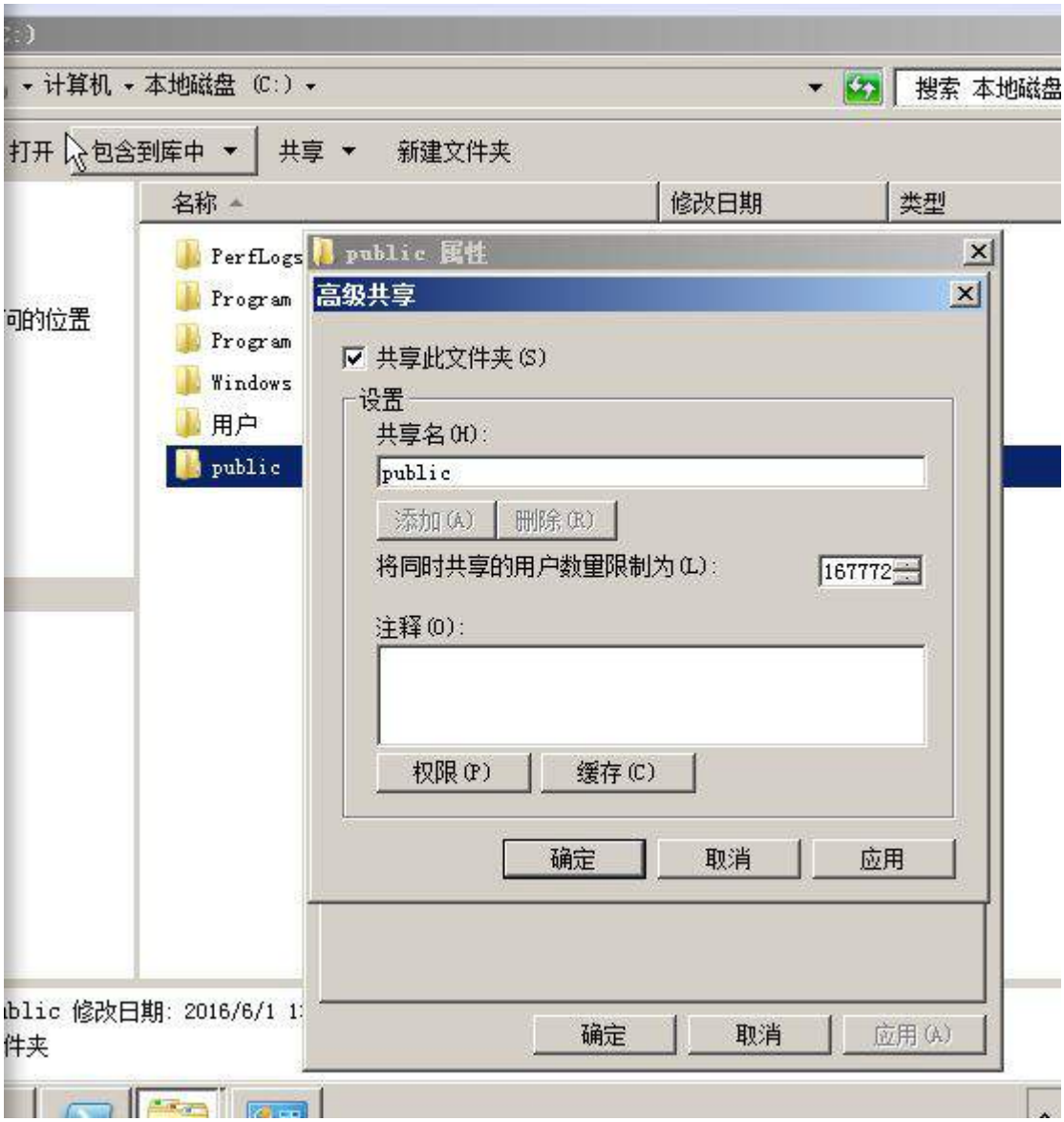
③当市场部用户登录时，自动在登入的计算机桌面上建立一个 www.tj.com 网址快捷方式，但不应用于 User11-user15 用户；

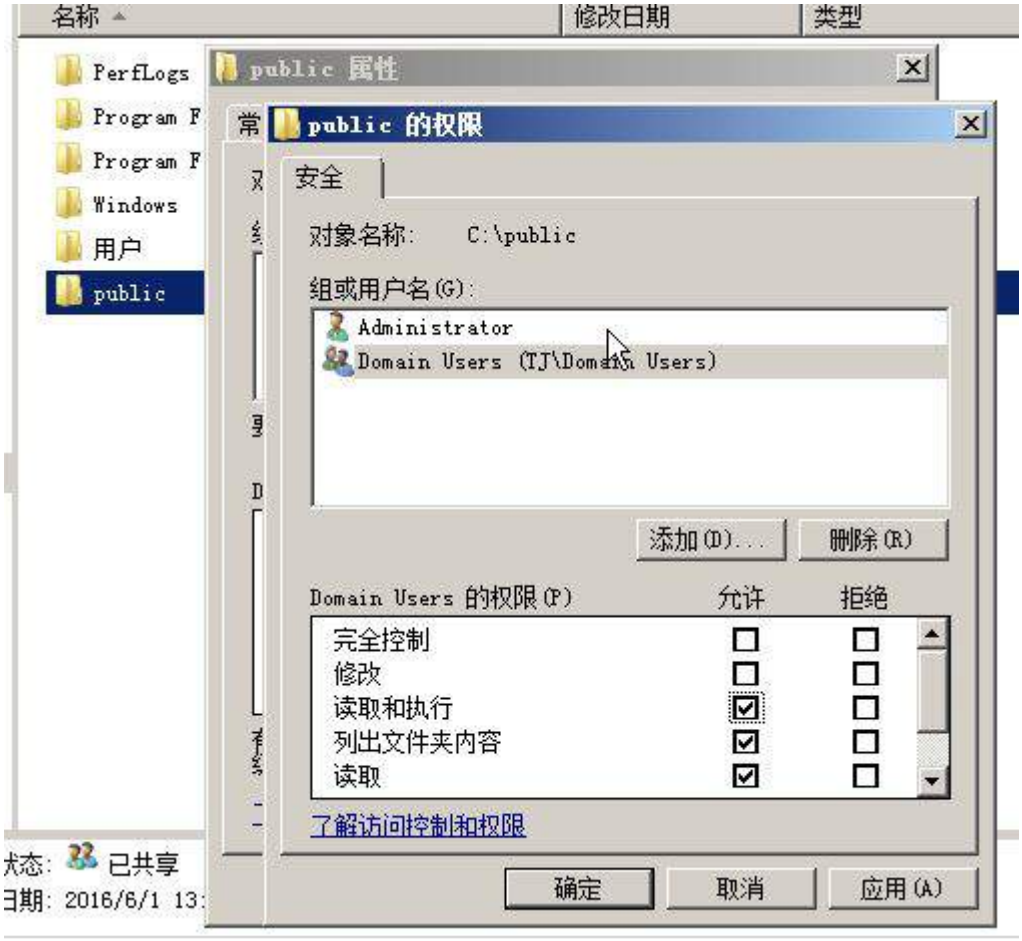


④开启审核账户管理策略，成功失败均审核；



⑤将该域控制器作为文件服务器，禁止默认C&共享。在该服务器上创建共享名为public的共享文件夹，存放内网的公共资料，希望域中所有用户均能访问该共享，并且要求只赋予只读权限；

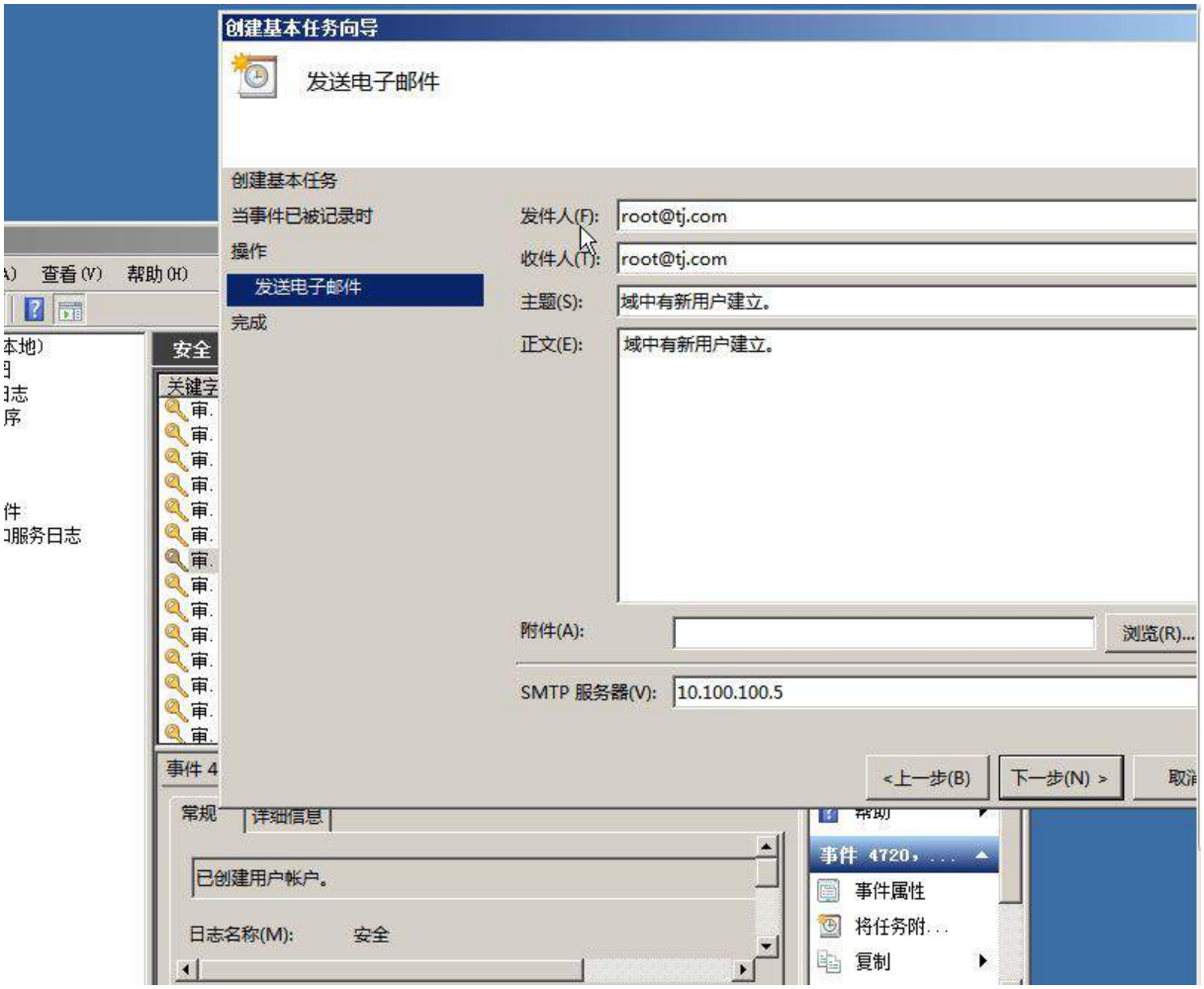

计算机 本地磁盘 (C:)
搜索 本地磁盘
打开
包含到库中
共享
新建文件夹
名称
修改日期
类型
PerfLogs
Program
Program
Windows
用户
public
public 属性
高级共享
共享此文件夹(S)
设置
共享名(H):
public
添加(A)
删除(R)
将同时共享的用户数量限制为(L):
167772
注释(O):
权限(P)
缓存(C)
确定
取消
应用
确定
取消
应用(A)



⑥为方便网络管理员远程管理域控制器，请开启域控制器远程桌面管理功能，允许账户 Administrator 的用户远程登录；

⑦将客户机 PC-B 加入到域中，并使用 PC-B 登录，更改密码为 01234567；

（5）利用域中新建用户时，root@tj.com 给自己发送一封电子邮件，内容为：“域中有新用户建立。”，邮件服务器使用 Win2003-B1；



（6）安装 IIS 服务，配置 IIS，以使访问者在浏览器中输入 tj.com，也可以正确访问到 Win2008-B1 上的 www.tj.com；

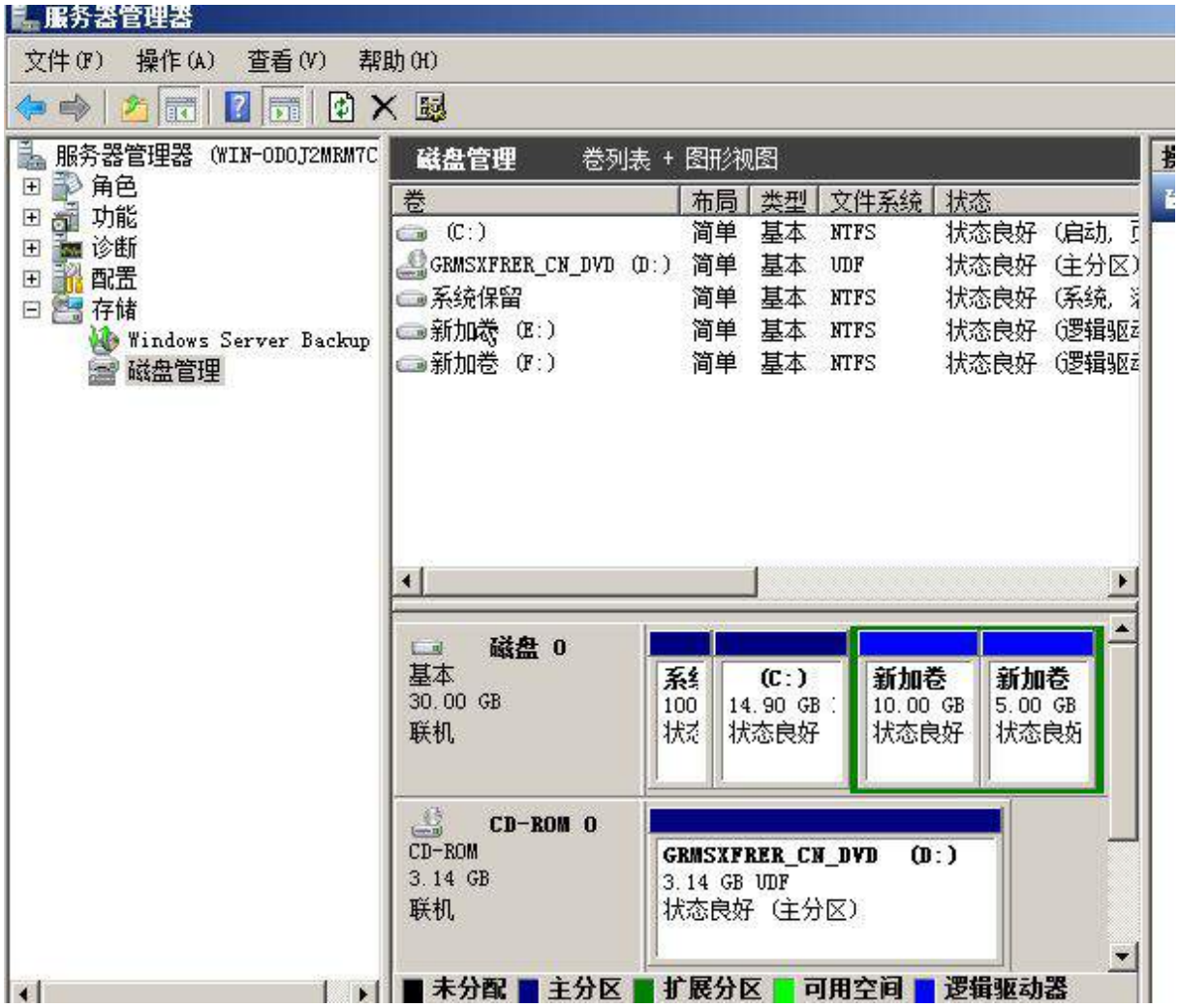
（7）将上面所有配置点截图粘贴到竞赛结果文件指定位置。

二、在 PC-B 上完成如下操作

1. 完成虚拟主机的创建

（1）创建虚拟机 Win2008-B1,具体要求为内存 1024MB,硬盘 30GB,主分区 15GB,扩展分区 15GB,分为两个逻辑分区,大小分别为 10GB 和 5GB；并将主机加入到 tj.com 域；


常规
名称: Win2008-B1
操作系统: Windows 2008 (64 bit)
预览
系统
内存大小: 1024 MB
启动顺序: 软驱, 光驱, 硬盘
硬件加速: VT-x/AMD-V, 嵌套分页
显示
显存大小: 27 MB
远程桌面服务器: 已禁用
录像: 已禁用
存储
控制器: IDE
第二IDE控制器主通道: [光驱]
cn_windows_server_2008_r2_standard_enterprise_datacenter_and_web_with_sp1_x64_dvd_617598.iso (3.14 GB)
控制器: SATA
SATA 端口 0: Win2008-B1.vdi (普通, 30.00 GB)
声音
主机音频驱动: Windows DirectSound
控制芯片: Intel HD 音频
网络
网卡 1: Intel PRO/1000 MT 桌面 (桥接网络, Intel(R) Ethernet Connection I217-LM)


服务器管理器
文件(F) 操作(A) 查看(V) 帮助(H)
服务器管理器 (WIN-ODOJ2MRM7C
角色
功能
诊断
配置
存储
Windows Server Backup
磁盘管理
磁盘管理 卷列表 + 图形视图
卷 布局 类型 文件系统 状态
(C:) 简单 基本 NTFS 状态良好 (启动,
GRMSXFRER_CN_DVD (D:) 简单 基本 UDF 状态良好 (主分区)
系统保留 简单 基本 NTFS 状态良好 (系统,
新加卷 (E:) 简单 基本 NTFS 状态良好 (逻辑驱
新加卷 (F:) 简单 基本 NTFS 状态良好 (逻辑驱
磁盘 0
基本
30.00 GB
联机
(C:)
14.90 GB
状态良好
新加卷
10.00 GB
状态良好
新加卷
5.00 GB
状态良好
CD-ROM 0
CD-ROM
3.14 GB
联机
GRMSXFRER_CN_DVD (D:)
3.14 GB UDF
状态良好 (主分区)
未分配 主分区 扩展分区 可用空间 逻辑驱动器

（2）创建虚拟机 Win2003-B1,具体要求为内存 512MB,硬盘 10GB；并将主机加入到 tj.com 域；

（3）在 PC-B 上，使用虚拟机安装 Windows XP 操作系统，设备名为 Windows-XP-B1，其内存为 512M，硬盘 10G，将计算机加入到域中，其合法域名为 pc.tj.com，ip 地址为（参见 IP 地址分配表 1-5 自行规划内容）。检测是否正常访问 www.tj.com；

常规

名称: Windows-XP-B1
操作系统: Windows XP (64 bit)

预览

系统

内存大小: 512 MB
启动顺序: 软驱, 光驱, 硬盘
硬件加速: VT-x/AMD-V, 嵌套分页

显示

显存大小: 18 MB
远程桌面服务器: 已禁用
录像: 已禁用

存储

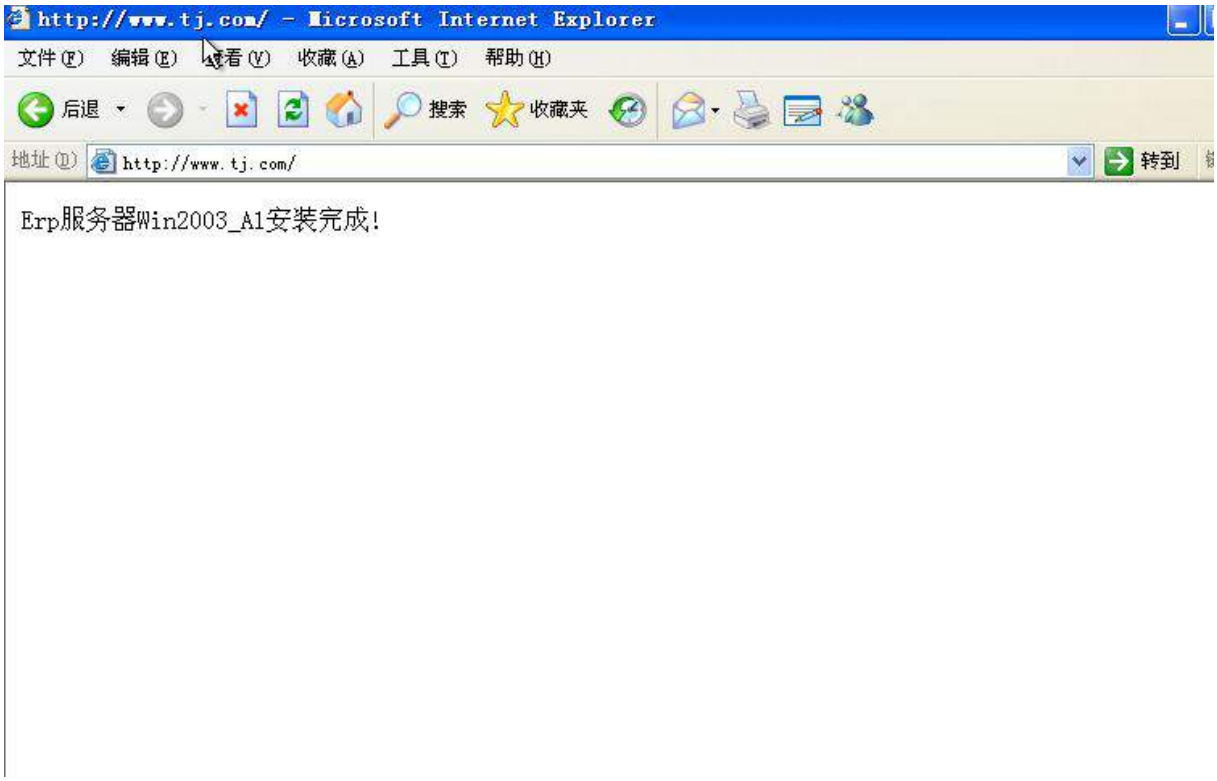
控制器: IDE
第一IDE控制器主通道: Windows-XP-B1.vdi (普通, 10.00 GB)
第二IDE控制器主通道: [光驱] windows_xp_sp3.iso (601.04 MB)

声音

主机音频驱动: Windows DirectSound
控制芯片: ICH AC97

网络

网卡 1: Intel PRO/1000 MT 桌面 (桥接网络, Intel(R) Ethernet Connection I217-LM)

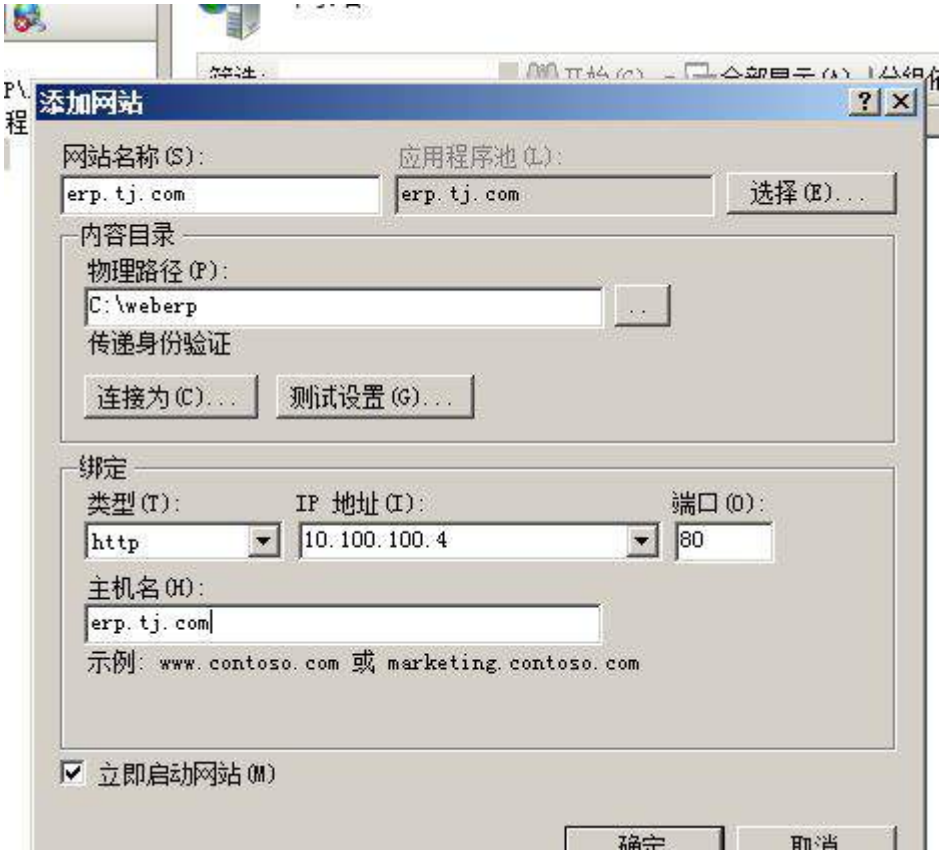


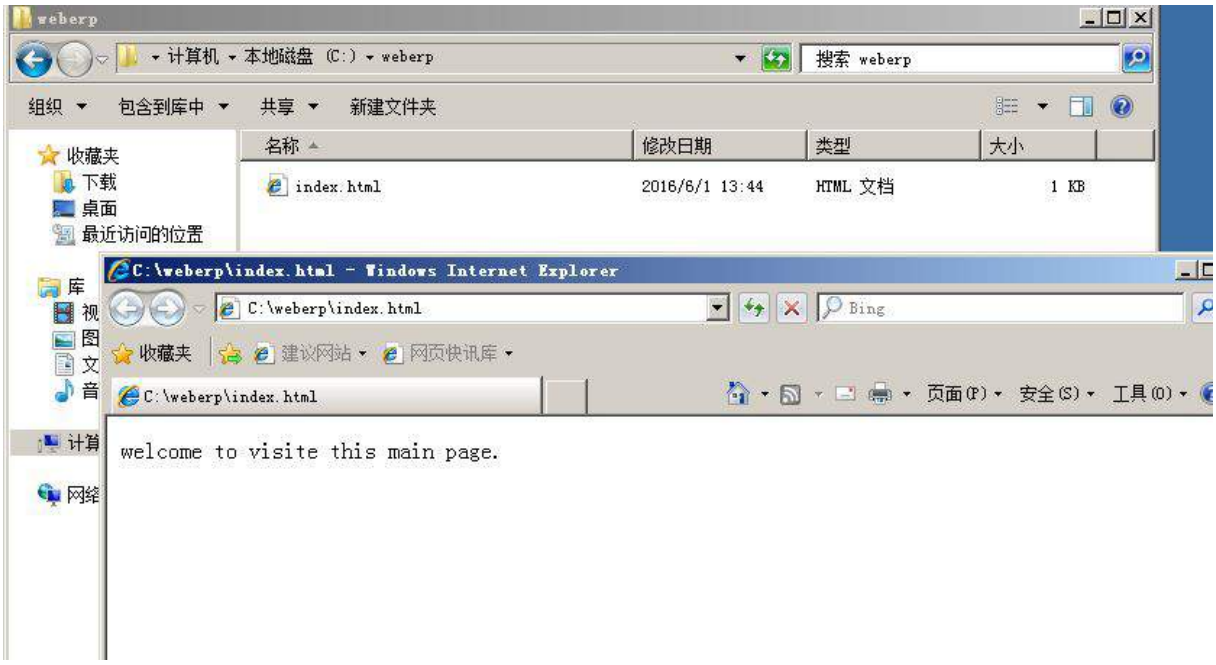
（4）根据拓扑结构图和网络系统规划表为 PC-B 物理主机及三台虚拟机配置正确的 IP 地址、子网掩码、网关和 DNS，将 PC-A 物理主机的 IP 地址配置界面截图保存，在 Windows 系统中使用 ipconfig/all 将显示所有结果的界面截图保存。

2. 在主机 Win2008-B1 中完成 Web 服务器以及 FTP 服务器的部署

（1）在此服务器中安装 IIS 以及 FTP 服务；

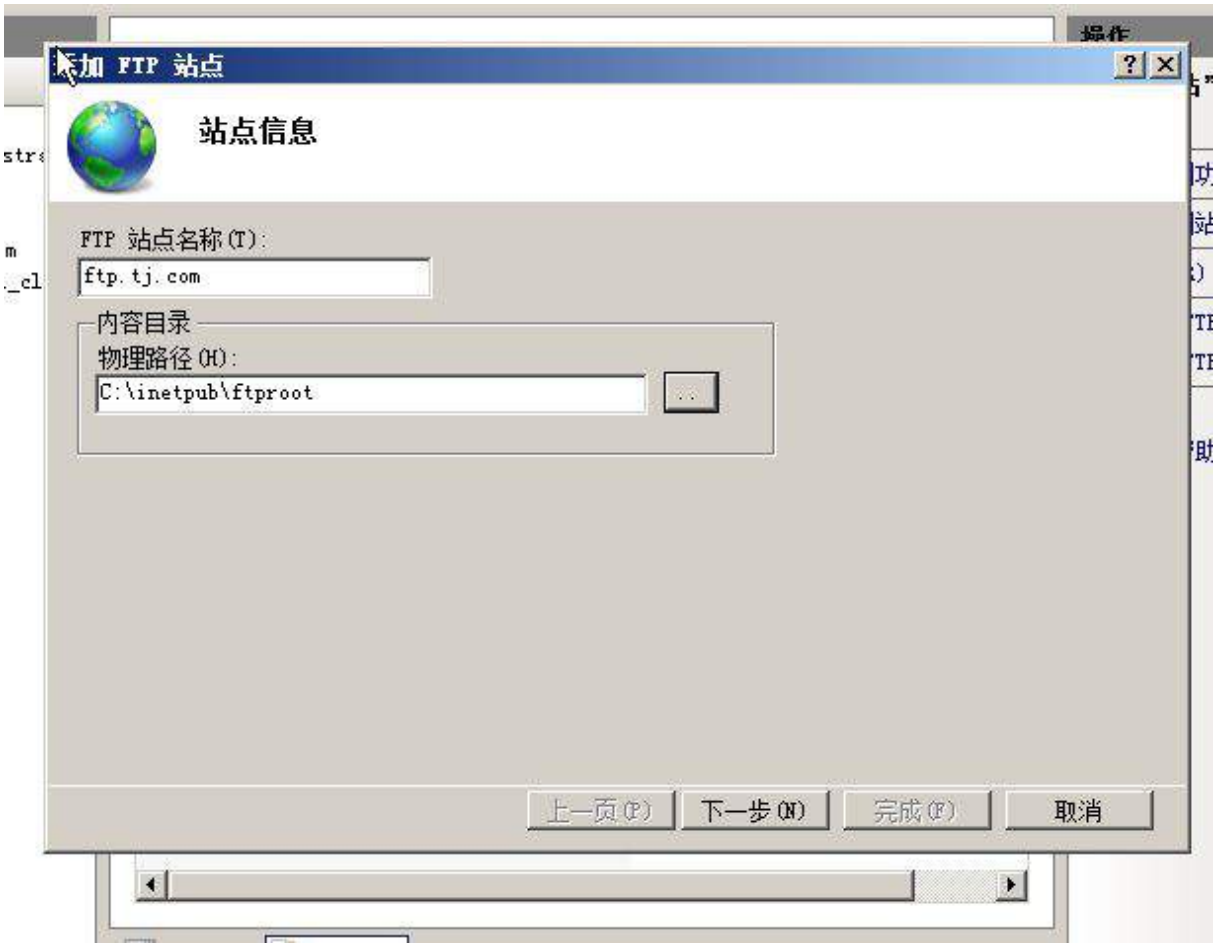
（2）配置 IIS 服务器，创建名为 weberp 的站点，主目录路径为 c:\weberp，并配置主机头 erp.tj.com 对应 IP 地址；此外，创建虚拟目录 web1，目录路径为 c:\web1，设置首页显示内容为”welcome to visit this main page.”；限制所有后缀为 linu.net 的主机均不能访问此网站；

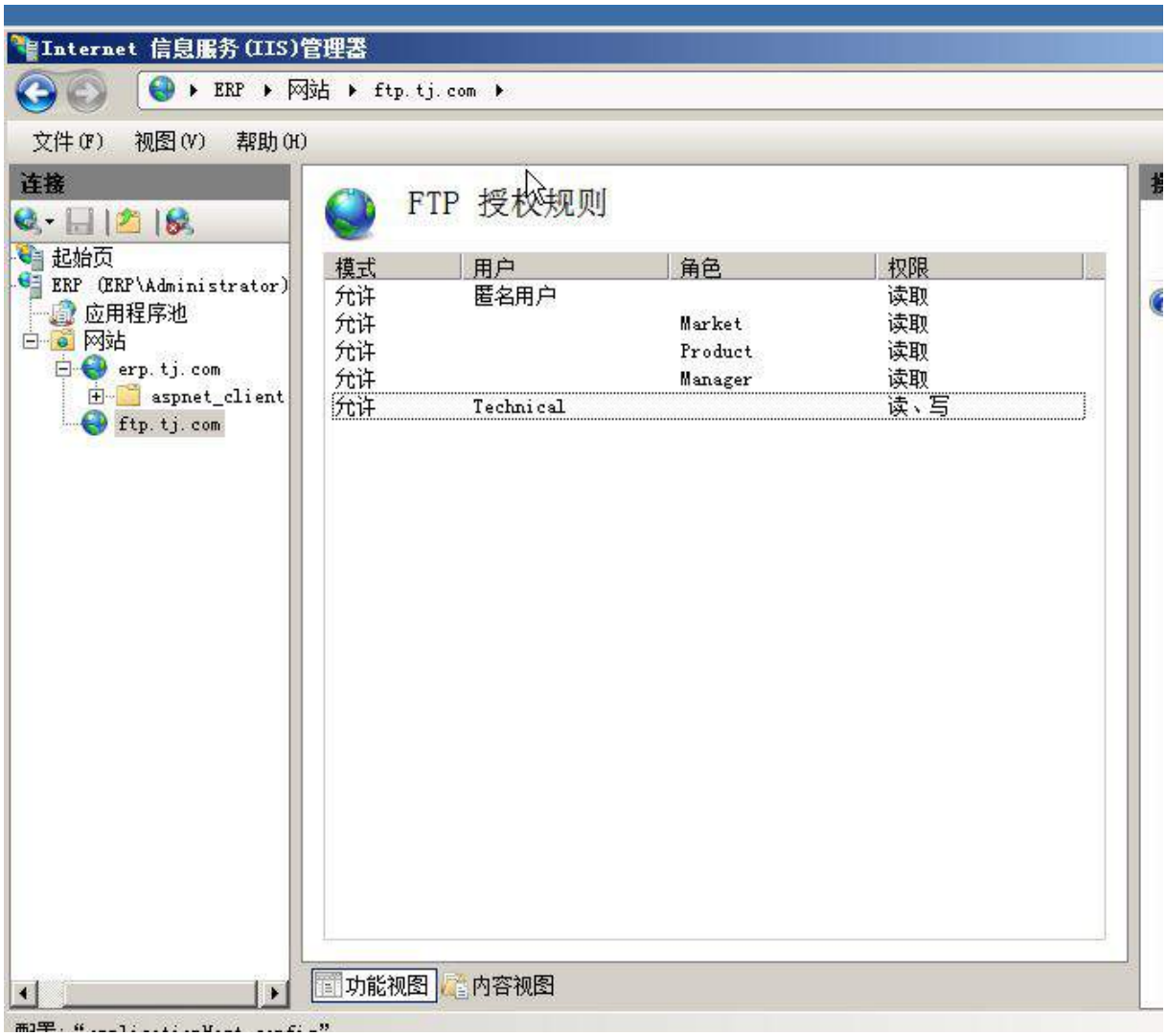




（3）设置网站应用摘要式身份验证方式，访问者必须输入正确的域用户和密码方可进行访问

（4）以隔离用户方式创建名为 ftp.tj.com 的 FTP 站点，FTP 主目录路径为 c:\inetpub\ftproot；域用户 User1- User20 及匿名用户均可登录，但匿名用户仅有只读权限，域用户 User16- User20 则能够完成读写操作；



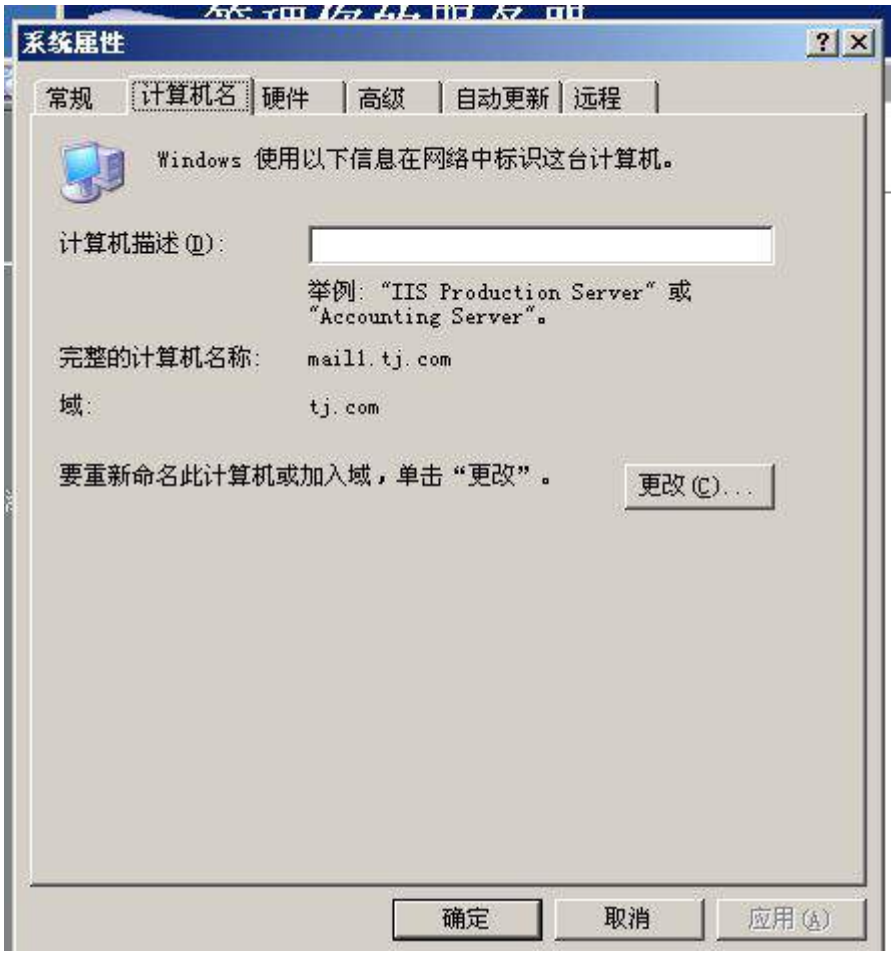


（5）创建模拟目录 PC-B，且只有客户端 PC-B 用户可以访问，可以实现文件的上传和下载，并启用日志记录功能；

（6）将上面所有配置点截图粘贴到竞赛结果文件指定位置。

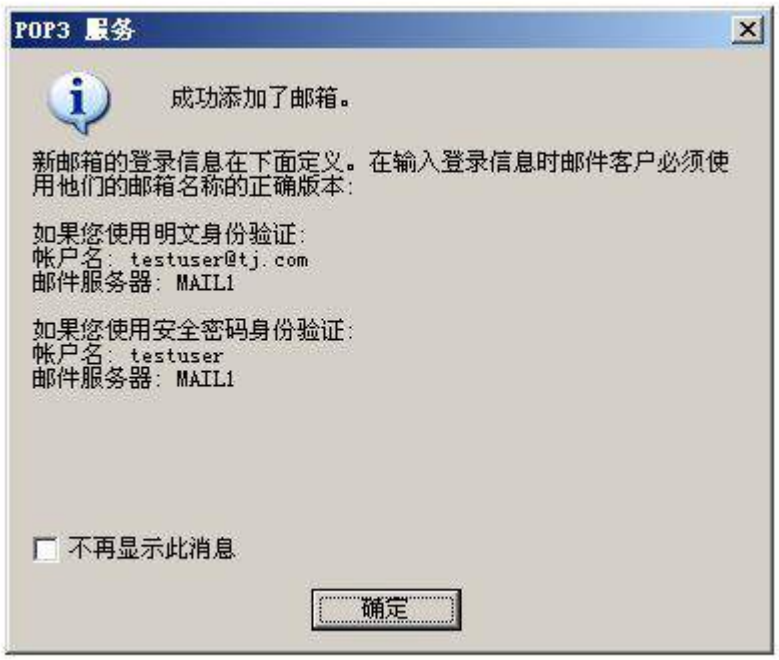
3. 在主机 Win2003-B1 中完成邮件服务器的部署

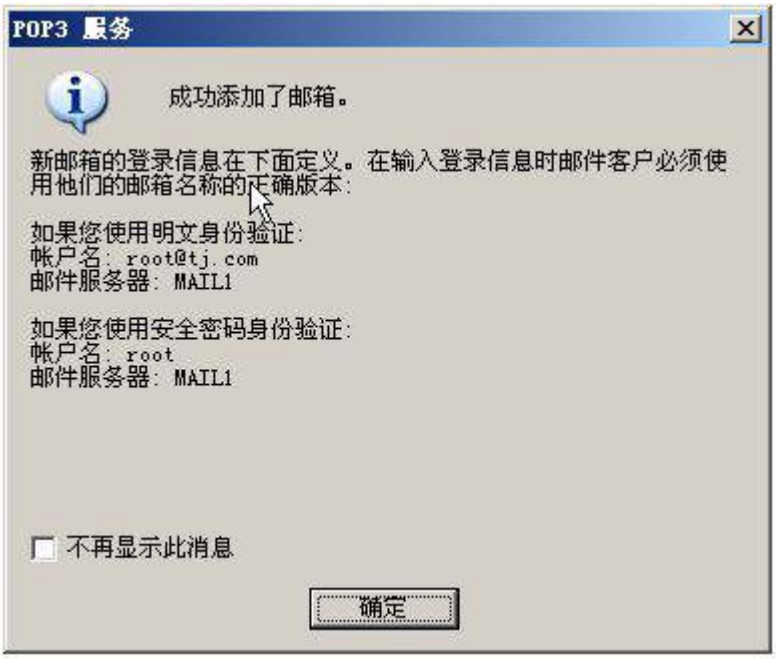
（1）在 Win2003-B1 上架设一台邮件服务器，邮件服务器域名为 Mail1.tj.com，为公司员工实现发送与接收邮件的功能；



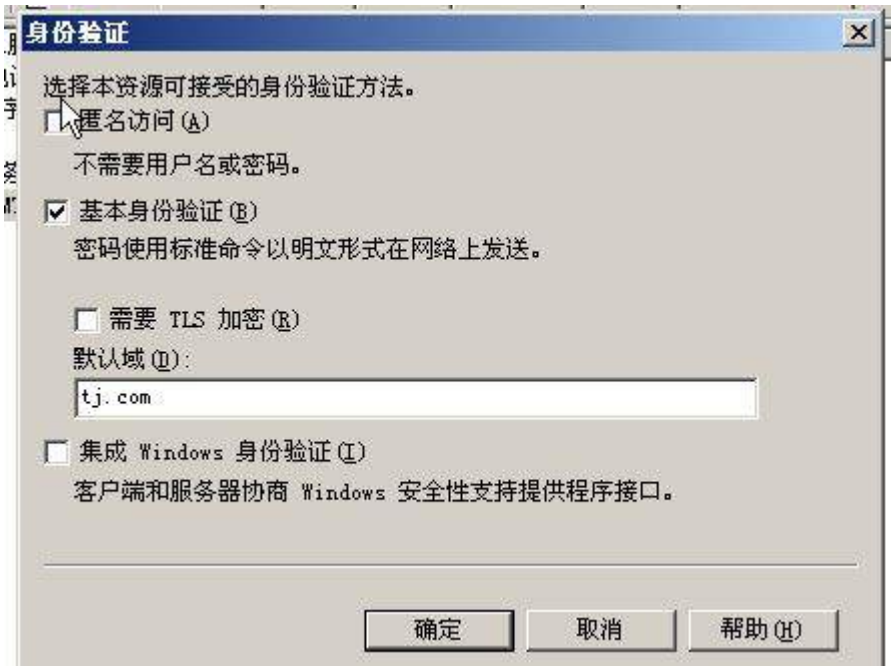
（2）安装 IIS，并配置服务器为邮件服务器。其邮箱域为 tj.com，为域中的所有用户分配邮箱；

（3）在当前服务器中设置电子邮件服务，并采用 Active Directory 集成的身份验证方式，创建 root@tj.com 及 testuser@tj.com 用户邮箱；

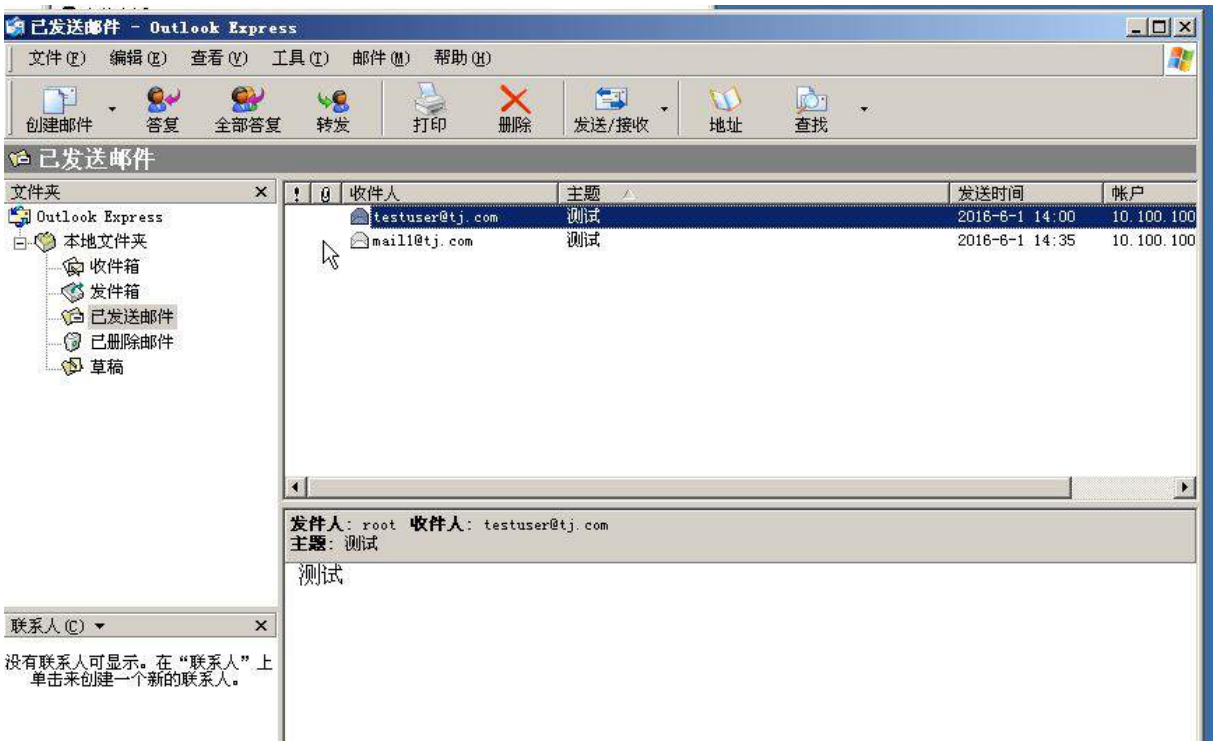




（4）完成对 smtp 服务的配置，只允许通过验证的用户进行中继，身份验证使用基本认证方式；



（5）以用户 root@tj.com 角色分别给用户 testuser@tj.com、mail1@jnds.net 发送一封邮件；

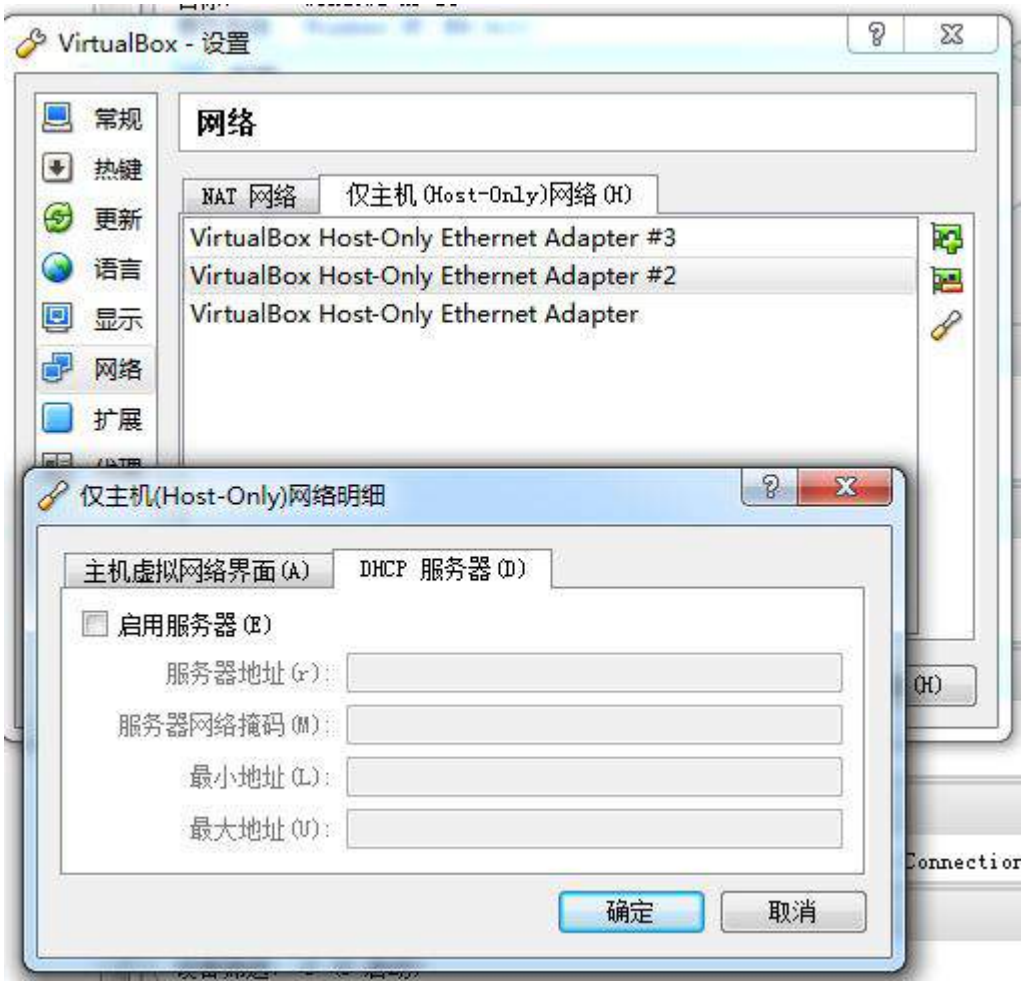


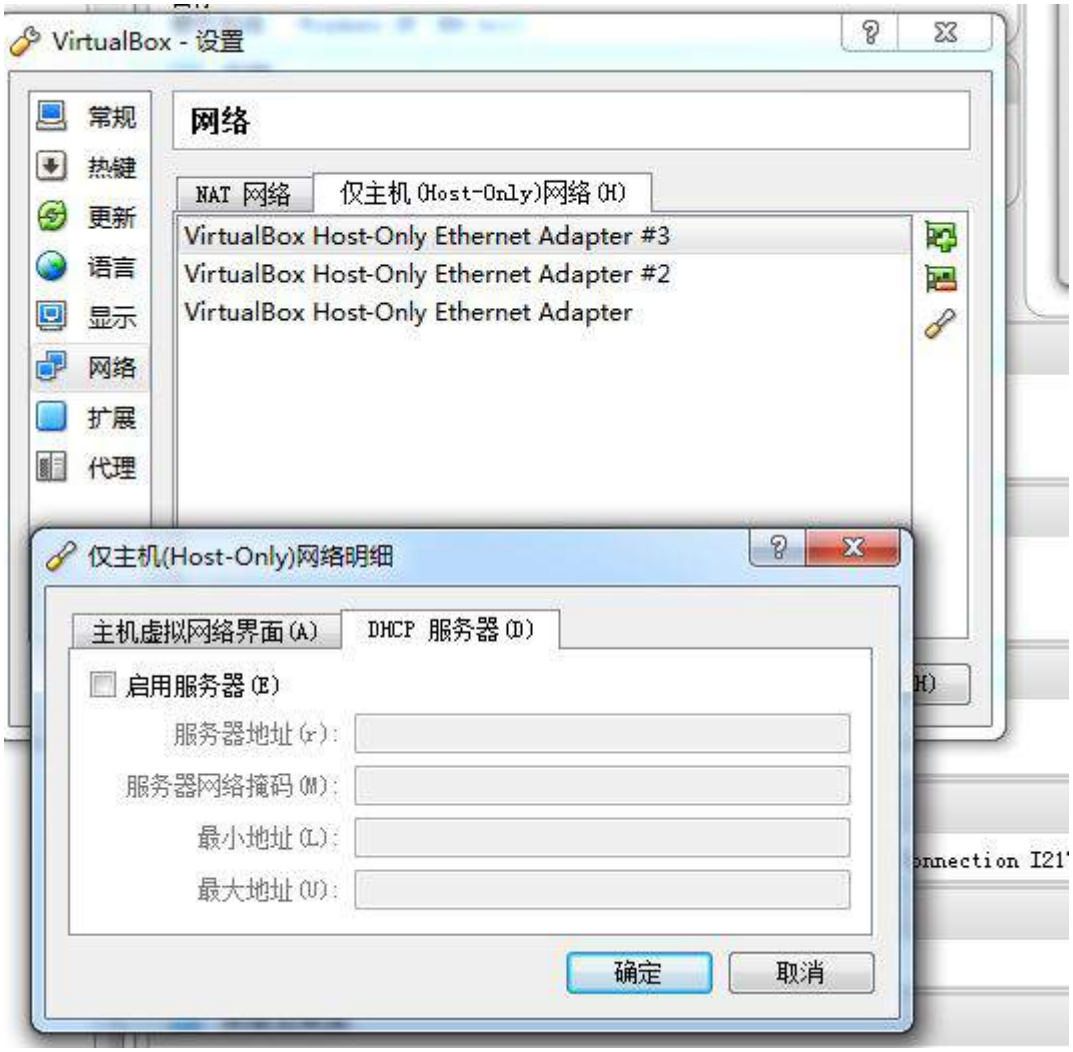
（6）将上面所有配置点截图粘贴到竞赛结果文件指定位置。

三、在 PC-C 上完成如下操作

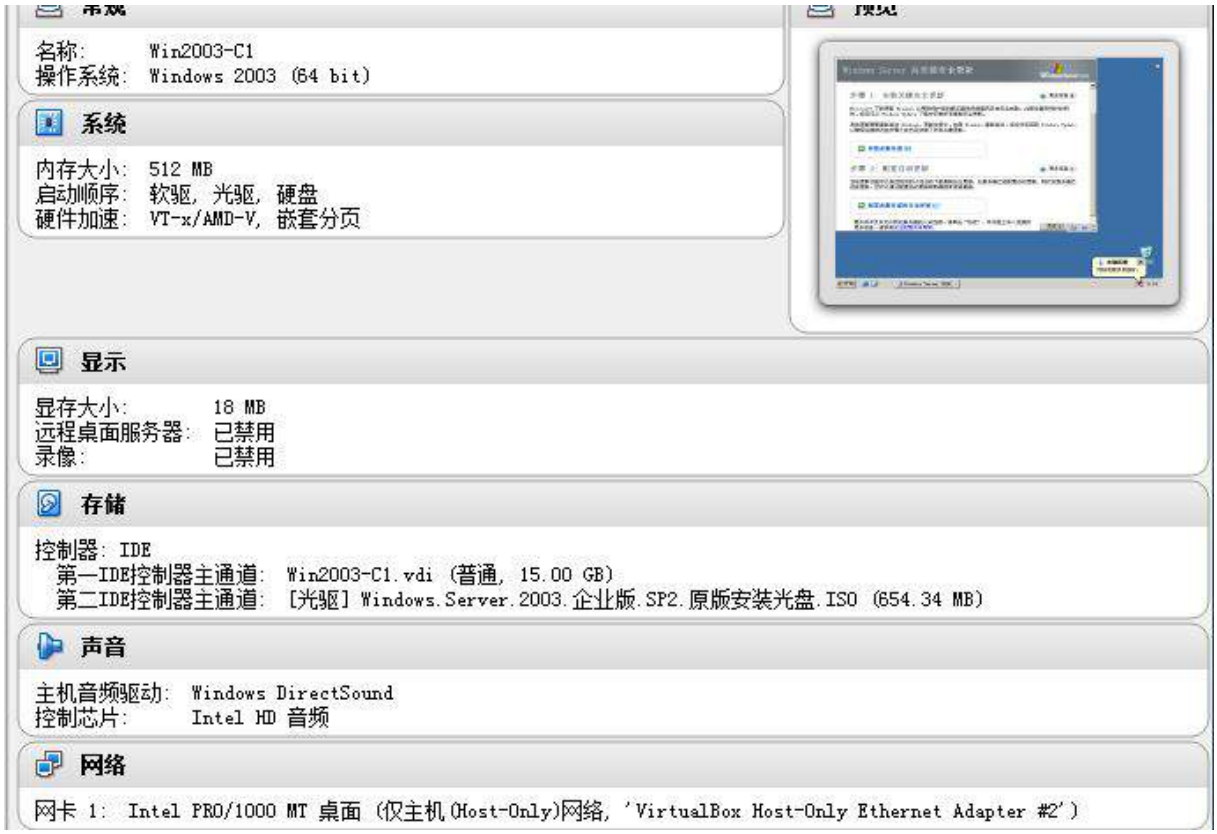
1. 完成虚拟主机的创建

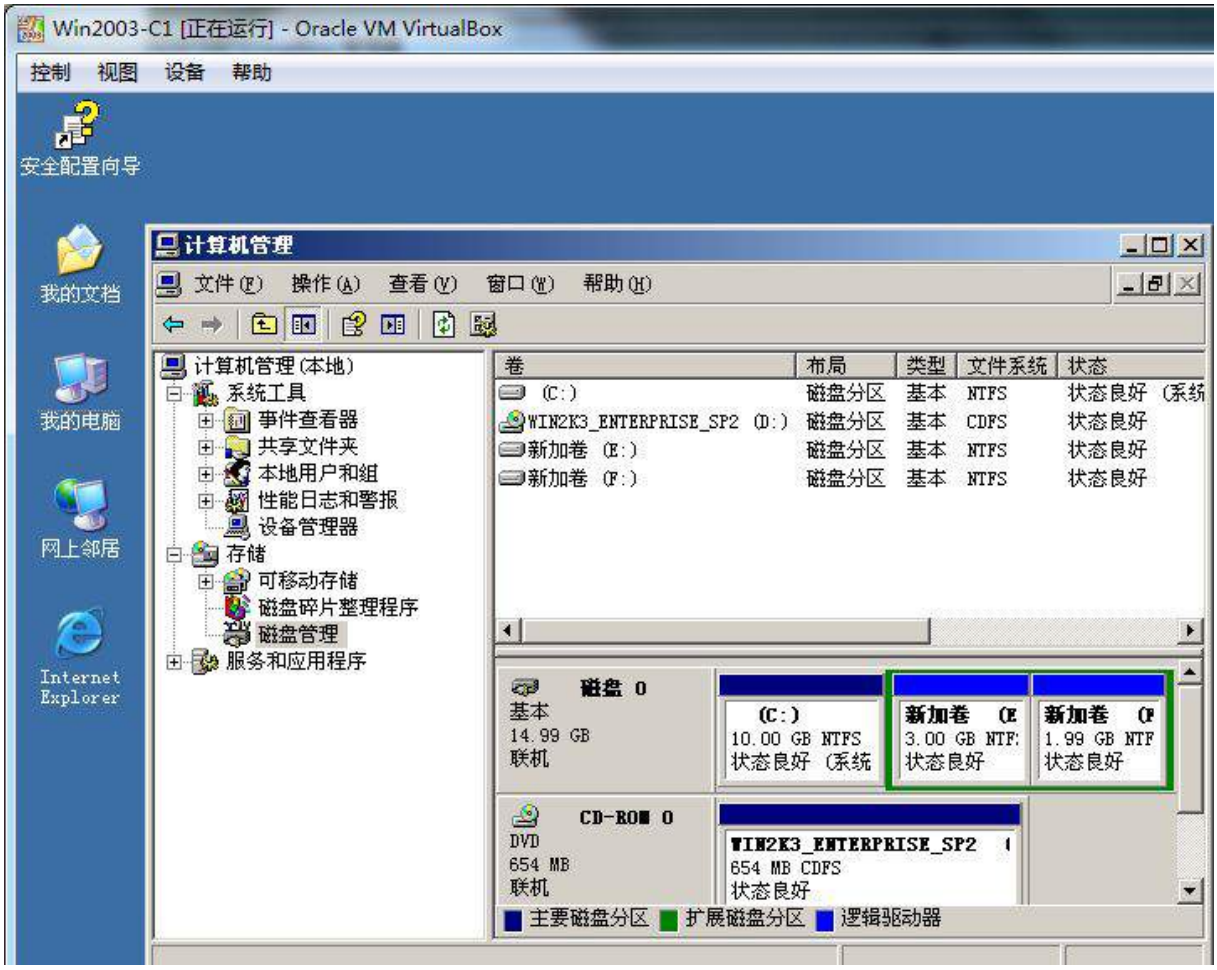
（1）创建两个“host-only”类型网络(虚拟机管理菜单—全局设定—网络),分别设置为#2 和#3,均禁用 dhcp 服务；以下 IP 均指在系统内网络静态地址，掩码默认设置；


VirtualBox - 设置
常规
热键
更新
语言
显示
网络
扩展
网络
NAT 网络
仅主机(Host-Only)网络(H)
VirtualBox Host-Only Ethernet Adapter #3
VirtualBox Host-Only Ethernet Adapter #2
VirtualBox Host-Only Ethernet Adapter
仅主机(Host-Only)网络明细
主机虚拟网络界面(A)
DHCP 服务器(D)
启用服务器(E)
服务器地址(r):
服务器网络掩码(M):
最小地址(L):
最大地址(U):
确定
取消



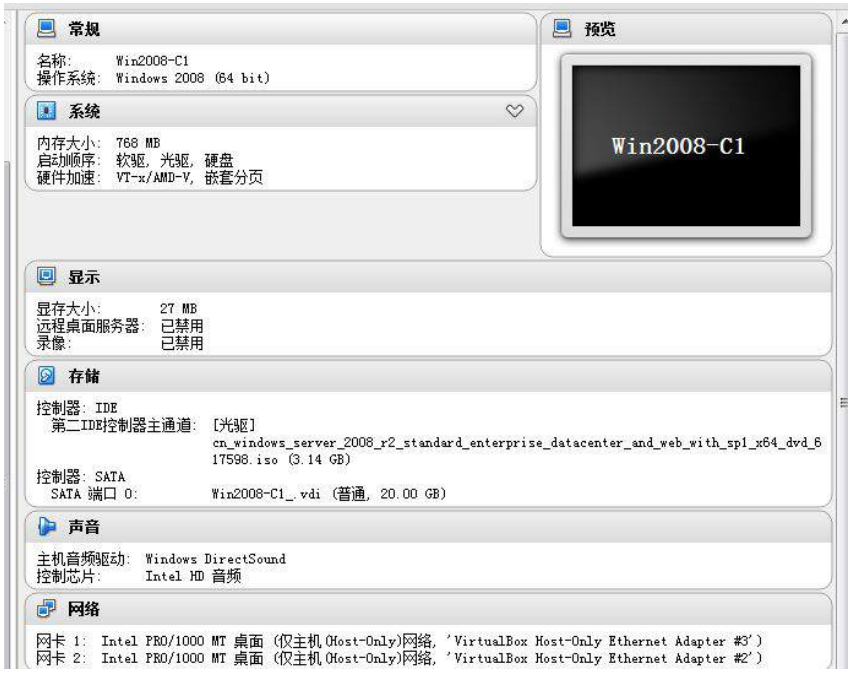
（2）创建虚拟机“win2003-C1”,具体要求为内存 512MB，硬盘 15GB，主分区 10GB，扩展分区 5GB，分为两个逻辑分区，大小分别为 3GB 和 2GB；网卡使用 host-only 连接方式，使用#2 网络接口 IP （参见 IP 地址分配表 1-5 自行规划内容）；





（3）创建虚拟机“Win2008-C1”，具体要求为内存 768M，硬盘 20G，主分区 15G，扩展

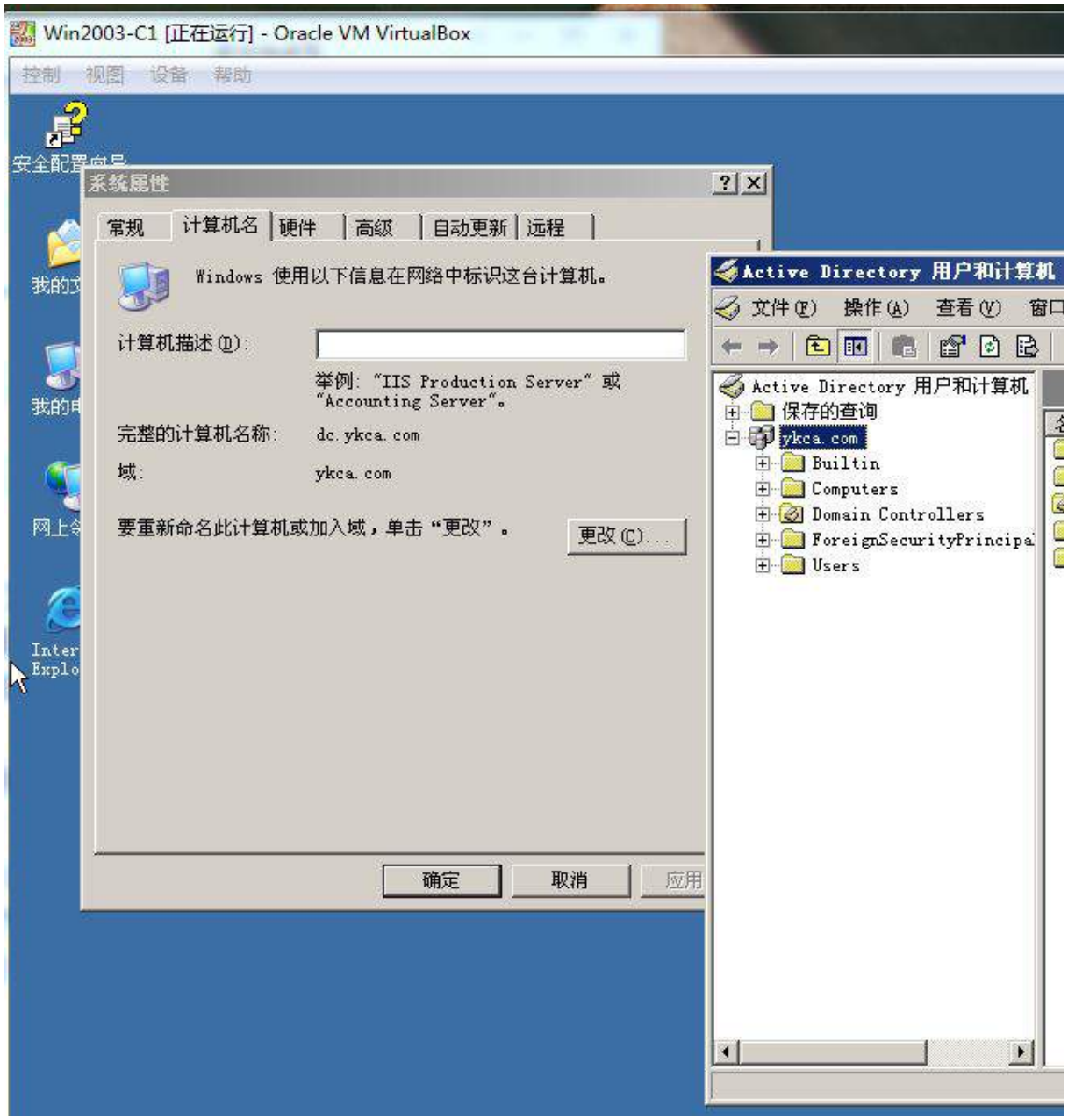
分区 5G，添加两块网卡，均使用 host-only 连接方式，网卡 1 使用#3 网络接口 IP（参见分配表 1-5 自行规划内容），网卡 2 使用#2 网络接口 IP：（参见分配表 1-5 自行规划内容）；



（4）将上面所有配置点截图粘贴到竞赛结果文件指定位置。

2. 在主机 Win2003-C1 中完成 DC 域控制器以及 CA 证书服务器的部署

（1）将此服务器升级为域控制器（dc.ykca.com），并安装配置 CA 证书服务，配置为企业根；

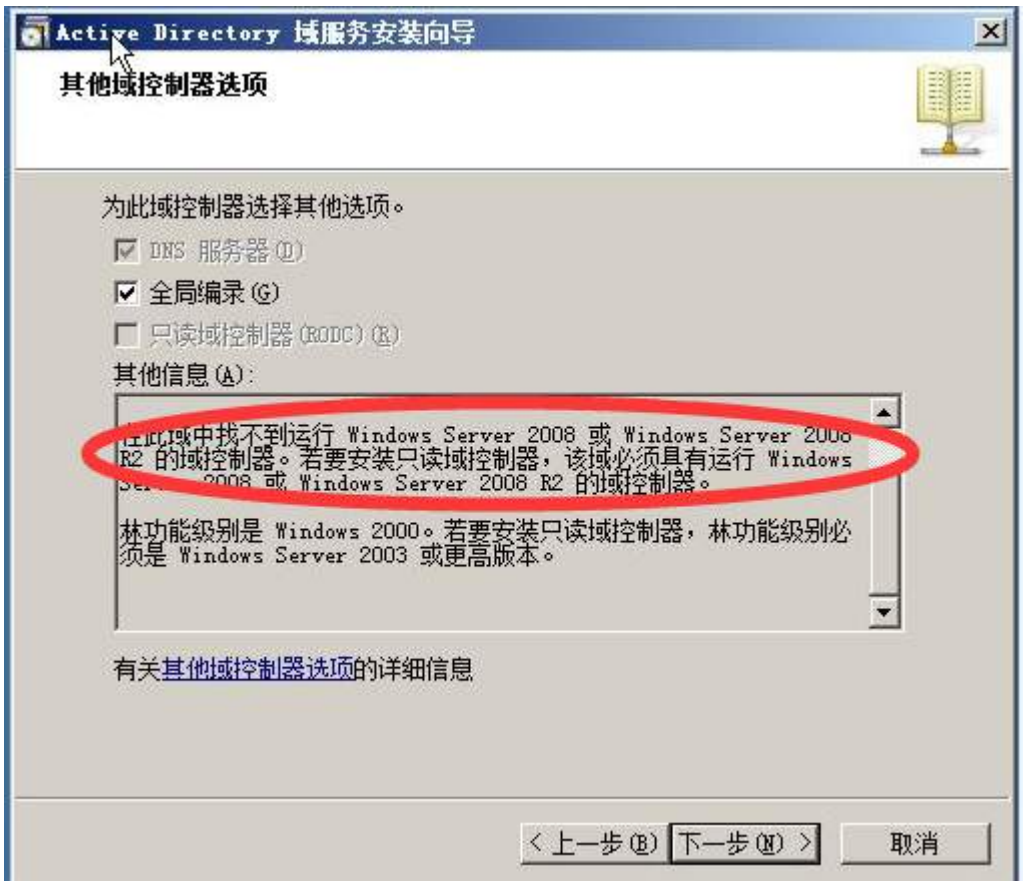

Win2003-C1 [正在运行] - Oracle VM VirtualBox
控制 视图 设备 帮助
系统属性
常规 计算机名 硬件 高级 自动更新 远程
Windows 使用以下信息在网络中标识这台计算机。
计算机描述(D):
举例: "IIS Production Server" 或 "Accounting Server"。
完整的计算机名称: dc.ykca.com
域: ykca.com
要重新命名此计算机或加入域，单击“更改”。
更改(C)...
确定
取消
应用
Active Directory 用户和计算机
文件(F) 操作(A) 查看(V)
Active Directory 用户和计算机
保存的查询
ykca.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipa
Users

（2）将证书请求提交的结果对话框、访问结果界面截图保存到竞赛结果文件指定位置。

3. 在主机 Win2008-C1 中完成 RODC 只读域控制器的部署

（1）将此服务器升级为 rodc.ykca.com 只读域控制器；进入“服务管理器”的“角色”菜单，展开“Active Directory 域服务”项后截图命名为 rodc.jpg 进行存储；


系统
控制面板 ▸ 系统和安全 ▸ 系统
搜索控制面板
控制面板主页
设备管理器
远程设置
高级系统设置
查看有关计算机的基本信息
Windows 版本
Windows Server 2008 R2 Standard
版权所有 © 2009 Microsoft Corporation。保留所有权利。
Service Pack 1
系统
处理器: Intel(R) Xeon(R) CPU E5-1620 v3 @ 3.50GHz 3.49 GHz
安装内存(RAM): 768 MB
系统类型: 64 位操作系统
笔和触摸: 没有可用于此显示器的笔或触控输入
计算机名称、域和工作组设置
计算机名: rodc
更改设置
计算机全名: rodc.ykca.com
计算机描述:
域: ykca.com
Windows 激活
剩余 2 天 可以自动激活。立即激活 Windows
产品 ID: 00477-179-0000007-84824 更改产品密钥
另请参阅
操作中心
Windows Update


Active Directory 域服务安装向导
其他域控制器选项
为此域控制器选择其他选项。
DNS 服务器(D)
全局编录(G)
只读域控制器(RODC)(R)
其他信息(A):
在此域中找不到运行 Windows Server 2008 或 Windows Server 2008 R2 的域控制器。若要安装只读域控制器，该域必须具有运行 Windows Server 2008 或 Windows Server 2008 R2 的域控制器。
林功能级别是 Windows 2000。若要安装只读域控制器，林功能级别必须是 Windows Server 2003 或更高版本。
有关其他域控制器选项的详细信息
< 上一步(B)
下一步(N) >
取消

（2）将域控制器升级提交的结果对话框、访问结果界面截图保存到竞赛结果文件指定位置。

二、Linux 操作系统部分

【注意事项】

（1）所有 Linux 操作系统的 root 用户的密码为 123456，若未按要求设置密码，涉及到该操作系统下的所有分值记为 0 分。

（2）系统主机及虚拟主机的 IP 属性设置请按照网络拓扑结构图以及（参见分配表 1-5 自行规划内容）的要求设定。

（3）除有特别规定外，其他未明确规定用户密码均与用户名相同。

（4）所有操作系统镜像文件及试题所需的其他软件均存放于每台计算机的/根目录下，并将题目要求的截图内容以.jpg 格式存储于计算机桌面以自己参赛工位号文件夹内。

（5）请各位选手按下列要求完成各项服务器配置，在完成配置后提交能反映各个配置项目结果的窗口截图，PC-C、PC-D 中 Linux 系统的所有截图按照试题顺序粘贴在文件名为：工位号_PC-C.doc、工位号_PC-D.doc（如 47 号工位在 PC-D 的文件命名为：47_PC-D.doc）的文档中，要求有试题的题号小标题，并对每个截图进行必要的说明，无截图的项目不得分，若缺少文件，涉及到该文件对应设备下的所有分值记为 0 分。，

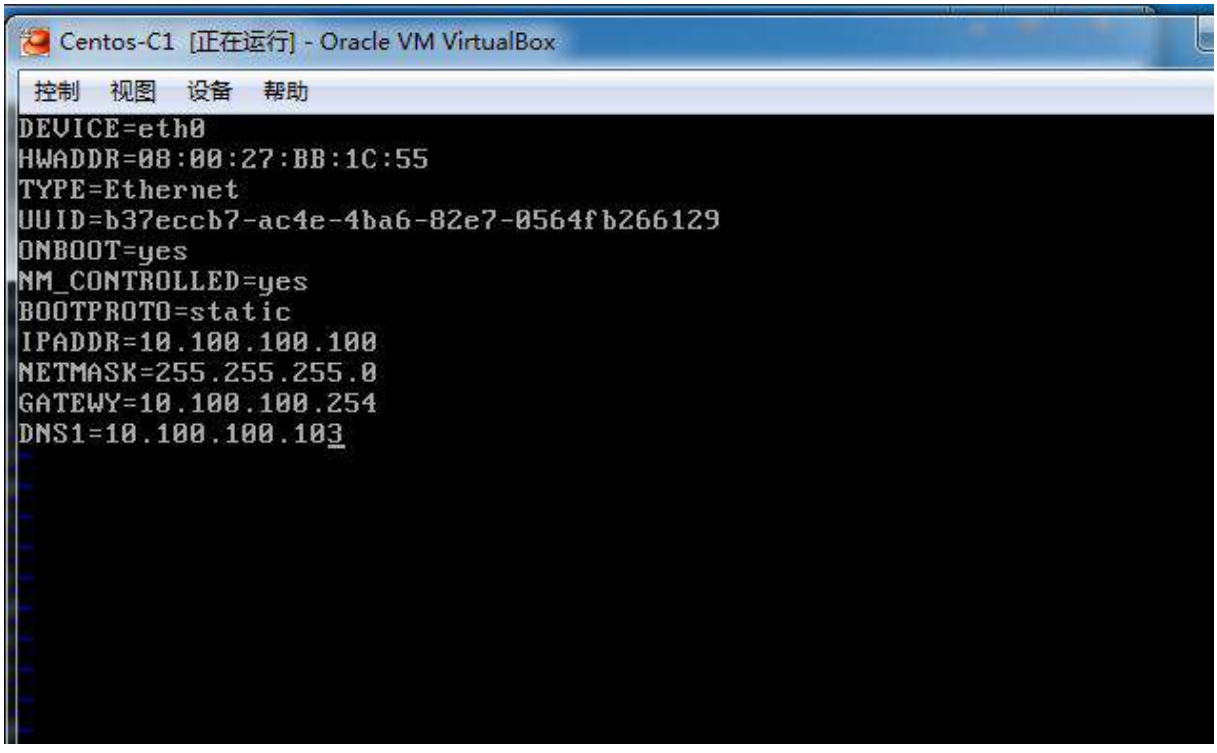
一、在 PC-C 上完成如下操作:

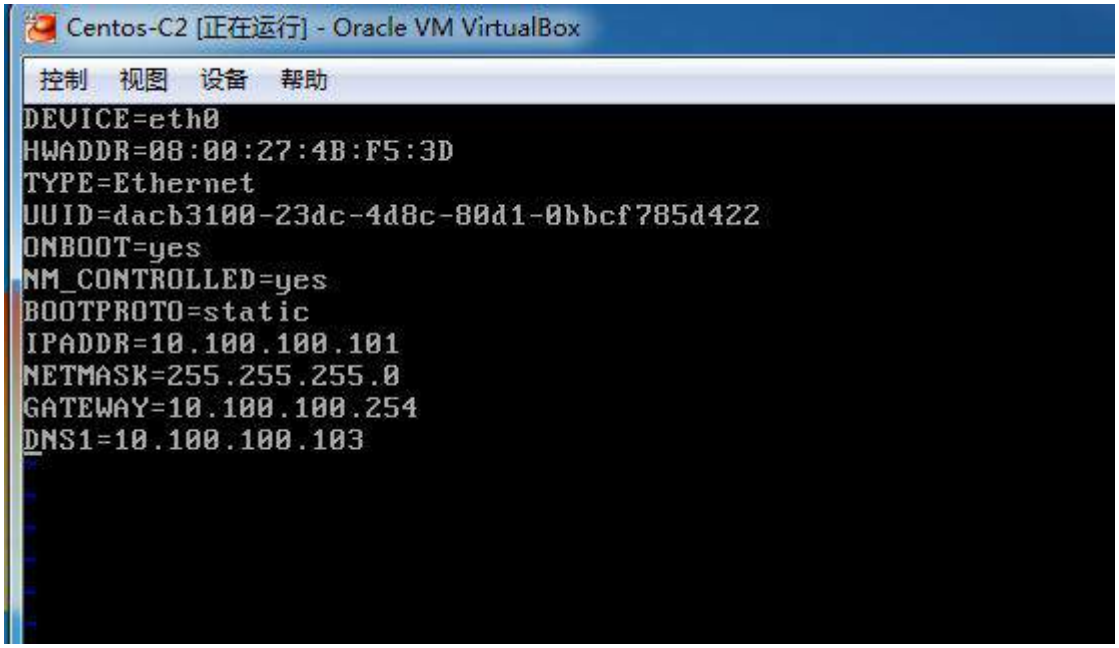
1、完成虚拟主机的创建

（1）安装虚拟机“Centos-C1”，具体要求为内存为 700MB,硬盘大小为 10GB;

（2）安装虚拟机“Centos-C2”，具体要求为硬盘大小为 10GB，内存为 700MB;

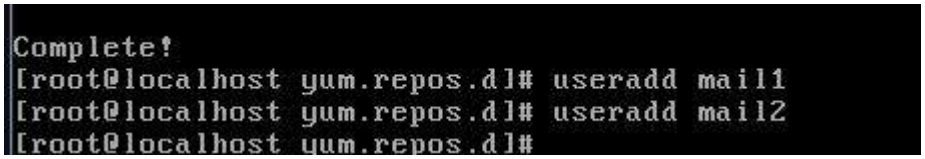
（3）将各虚拟机配置界面分别截图保存，内容有服务器的 IP 地址、子网掩码、网关和 DNS 等；



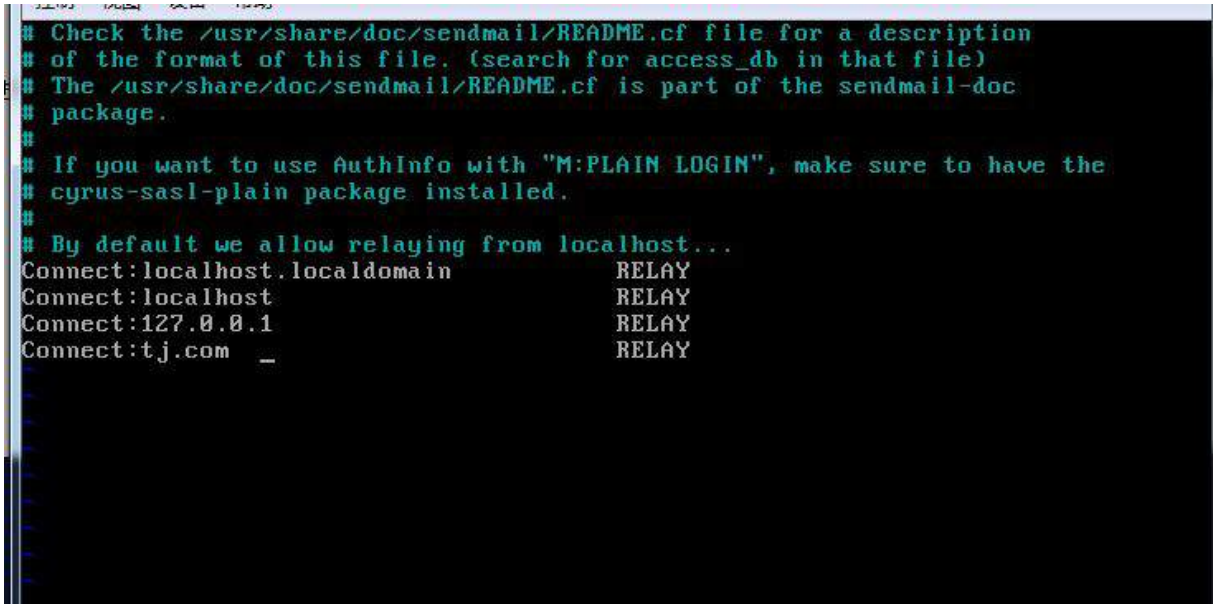


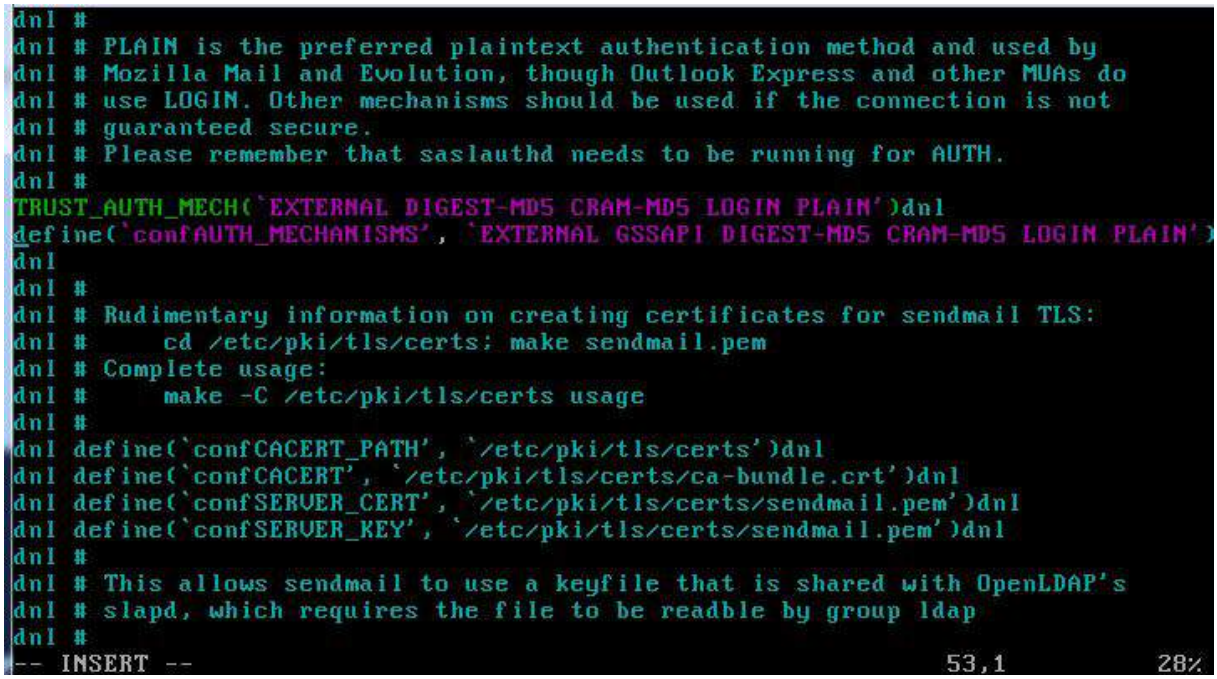
2、在主机 Centos-C1 中完成 Sendmail 邮件服务器的部署

（1）在此服务器中安装配置 Sendmail 服务，建立分别名为 mail1 及 mail2 的用户，并建立 linu.net 邮件域；



（2）允许来自 tj.com 域的邮件中继转发。开启 SMTP 的 SASL 验证，允许通过身份验证的用户转发邮件；

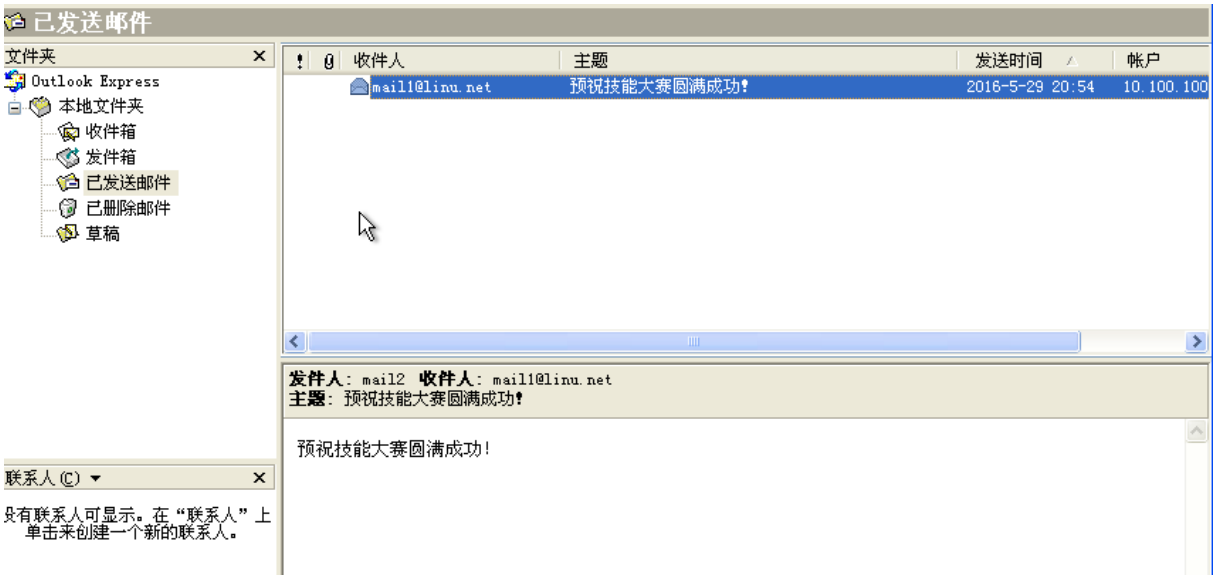




（3）限制单个邮件大小为 5M；

```
# wait for alias file rebuild (default units: minutes)
O AliasWait=10

# location of alias file
O AliasFile=/etc/aliases

# minimum number of free blocks on filesystem
O MinFreeBlocks=100

# maximum message size
O MaxMessageSize=5242880_

# substitution for space (blank) characters
O BlankSub=.

# avoid connecting to "expensive" mailers on initial submission?
O HoldExpensive=False

# checkpoint queue runs after every N successful deliveries
#O CheckpointInterval=10

# default delivery mode
O DeliveryMode=background

-- INSERT --                                          182,25        9%
```

（4）使用自带邮件客户端进行测试，用户 mail2@linu.net 向 mail1@linu.net 发送正文为“预祝技能大赛圆满成功!”的邮件，利用用户 mail1 进行接收；



（5）配置相关服务开机自启动；

```
[root@localhost network-scripts]#
[root@localhost network-scripts]# chkconfig sendmail on
[root@localhost network-scripts]#
[root@localhost network-scripts]# _
```

（6）创建用户 vncuser1 和 vncuser2,为 vncuser1 和 vncuser2 用户配置远程桌面，均使用 gnome 桌面环境，配置为开机自启动；

```
[root@localhost network-scripts]# useradd vncuser1
[root@localhost network-scripts]# [redacted]
[root@localhost network-scripts]# useradd vncuser2
[root@localhost network-scripts]# _
```

```
正在启动 VNC 服务器：1: vncuser1
New 'localhost.localdomain:1 (vncuser1)' desktop is localhost.localdomain:1

Starting applications specified in /home/vncuser1/.vnc/xstartup
Log file is /home/vncuser1/.vnc/localhost.localdomain:1.log

2: vncuser2
New 'localhost.localdomain:2 (vncuser2)' desktop is localhost.localdomain:2

Starting applications specified in /home/vncuser2/.vnc/xstartup
Log file is /home/vncuser2/.vnc/localhost.localdomain:2.log

                                                          [确定]
```

vncuser2@localhost:/home/vncuser1/.vnc

文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)

```
#!/bin/sh

[ -r /etc/sysconfig/i18n ] && . /etc/sysconfig/i18n
export LANG
export SYSFONT
vncconfig -iconic &
unset SESSION_MANAGER
unset DBUS_SESSION_BUS_ADDRESS
OS=`uname -s`
if [ $OS = 'Linux' ]; then
  case "$WINDOWMANAGER" in
    *gnome*)
      if [ -e /etc/SuSE-release ]; then
        PATH=$PATH:/opt/gnome/bin
        export PATH
      fi
      ;;
  esac
fi
if [ -x /etc/X11/xinit/xinitrc ]; then
  exec /etc/X11/xinit/xinitrc
fi
if [ -f /etc/X11/xinit/xinitrc ]; then
  exec sh /etc/X11/xinit/xinitrc
fi
[ -r $HOME/.Xresources ] && xrdb $HOME/.Xresources
xsetroot -solid grey
xterm -geometry 80x24+10+10 -ls -title "$VNCDESKTOP Desktop" &
gnome &
~
~
```

vncuser2@localhost:/home/vncuser2/.vnc

文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)

```
#!/bin/sh

[ -r /etc/sysconfig/i18n ] && . /etc/sysconfig/i18n
export LANG
export SYSFONT
vncconfig -iconic &
unset SESSION_MANAGER
unset DBUS_SESSION_BUS_ADDRESS
OS=`uname -s`
if [ $OS = 'Linux' ]; then
  case "$WINDOWMANAGER" in
    *gnome*)
      if [ -e /etc/SuSE-release ]; then
        PATH=$PATH:/opt/gnome/bin
        export PATH
      fi
      ;;
  esac
fi
if [ -x /etc/X11/xinit/xinitrc ]; then
  exec /etc/X11/xinit/xinitrc
fi
if [ -f /etc/X11/xinit/xinitrc ]; then
  exec sh /etc/X11/xinit/xinitrc
fi
[ -r $HOME/.Xresources ] && xrdb $HOME/.Xresources
xsetroot -solid grey
xterm -geometry 80x24+10+10 -ls -title "$VNCDESKTOP Desktop" &
gnome &
~
```

（7）将上面 6 个方面的主要配置关键点界面截图保存到竞赛结果文件指定位置。

3、在主机 Centos-C2 中完成 FTP 服务器的部署 （50 分）

（1）在 Centos-C2 上安装配置 FTP 服务，使得用户在客户端能通过域名 ftp.linu.net 访问服务器。该服务器允许匿名用户访问，但只允许其下载数据，不允许上传数据；

```
# Allow anonymous FTP? (Beware - allowed by default if you comment this
anonymous_enable=YES
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to
# if your users expect that (022 is used by most other ftpd's)
local_umask=022
#
# Uncomment this to allow the anonymous FTP user to upload files. This
# has an effect if the above global write enable is activated. Also, yo
# obviously need to create a directory writable by the FTP user.
#anon_upload_enable=YES
anon_world_readable_only=YES_
#
# Uncomment this if you want the anonymous FTP user to be able to creat
# new directories.
#anon_mkdir_write_enable=YES
```

（2）开启 vsftp 的 log 功能设置，文件名为/var/log/xferlog；

```
xferlog_enable=YES
#
# Make sure PORT transfer connections originate from port 20 (ftp-data).
connect_from_port_20=YES
#
# If you want, you can arrange for uploaded anonymous files to be owned by
# a different user. Note! Using "root" for uploaded files is not
# recommended!
#chown_uploads=YES
#chown_username=whoever
#
# The name of log file when xferlog_enable=YES and xferlog_std_format=YES
# WARNING - changing this filename affects /etc/logrotate.d/vsftpd.log
xferlog_file=/var/log/xferlog
#
# Switches between logging into vsftpd_log_file and xferlog_file files.
# NO writes to vsftpd_log_file, YES to xferlog_file
xferlog_std_format=YES
#
# You may change the default value for timing out an idle session.
#idle_session_timeout=600
```

（3）设置无任何操作的超时时间为两分钟,设置数据连接的超时时间为五分钟；

```
#
# You may change the default value for timing out an idle sess
idle_session_timeout=120
#
# You may change the default value for timing out a data conne
data_connection_timeout=300_
#
# It is recommended that you define on your system a unique us
# ftp server can use as a totally isolated and unprivileged us
#nopriv_user=ftpsecure
```

（4）设置 FTP 服务器最大支持连接数为 500 个，每个 IP 最多能支持 20 个链接；

（5）限制匿名用户以下载速度为不超过 256KB/S 速度下载,其他用户以 512KB/S 速度下载。将配置文件界面截图保存；

```
# You may activate the "-R" option to the builtin ls. This is disabled by
# default to avoid remote users being able to cause excessive I/O on large
# sites. However, some broken FTP clients such as "ncftp" and "mirror" assume
# the presence of the "-R" option, so there is a strong case for enabling it.
#ls_recurse_enable=YES
#
# When "listen" directive is enabled, vsftpd runs in standalone mode and
# listens on IPv4 sockets. This directive cannot be used in conjunction
# with the listen_ipv6 directive.
listen=YES
#
# This directive enables listening on IPv6 sockets. To listen on IPv4 and IPv6
# sockets, you must run two copies of vsftpd with two configuration files.
# Make sure, that one of the listen options is commented !!
#listen_ipv6=YES

pam_service_name=vsftpd
userlist_enable=YES
tcp_wrappers=YES
max_clients=500
max_per_ip=20
anon_rate=262144
local_rate=524288
```

（6）配置当系统启动时自动启动 FTP 服务；

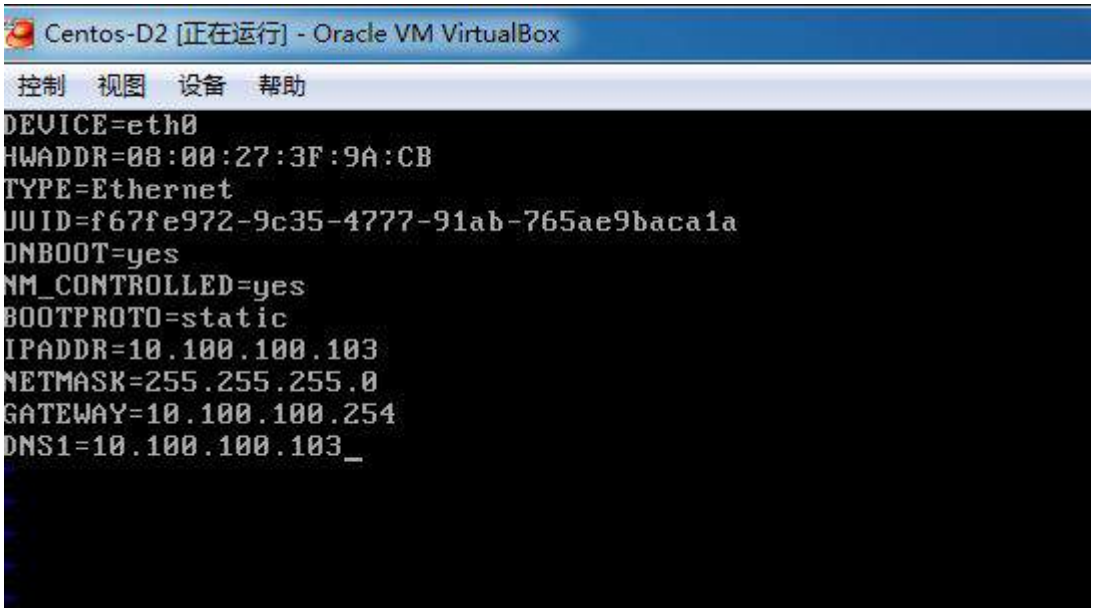
```
[root@localhost vsftpd]#
[root@localhost vsftpd]#
[root@localhost vsftpd]# chkconfig vsftpd on
[root@localhost vsftpd]#
```

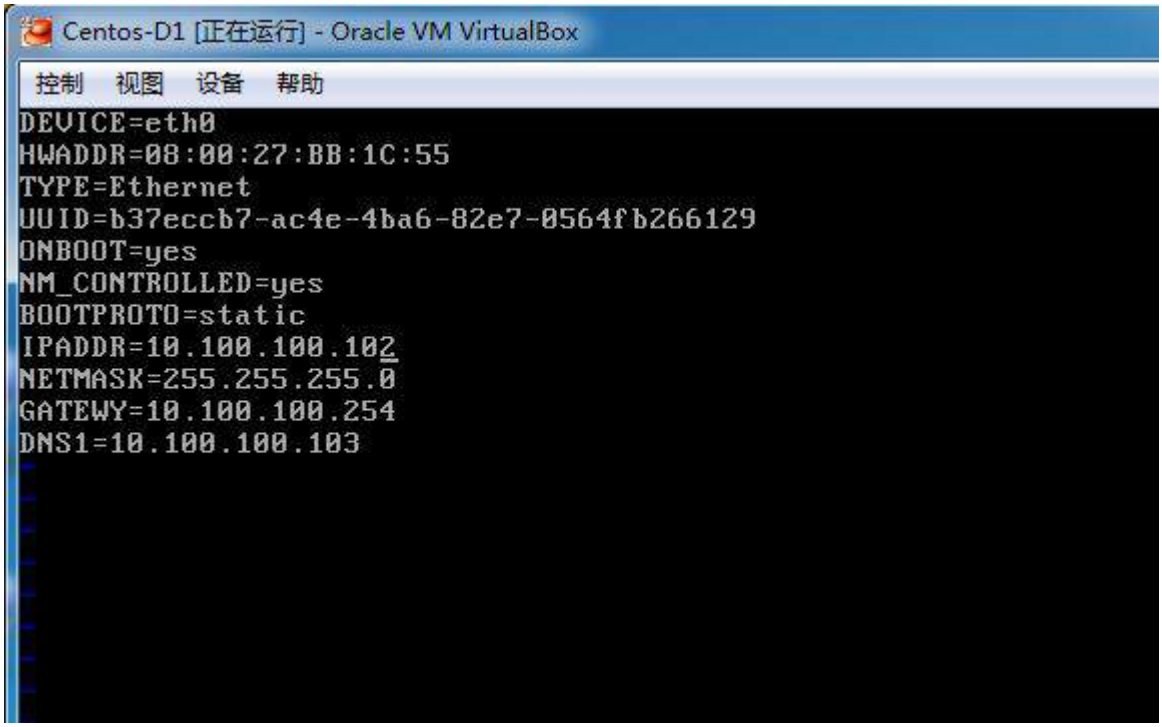
（7）在客户端 PC-D 桌面通过域名访问 FTP 服务器，将访问的结果窗口截图保存；
将上面 4 个方面的主要配置关键点界面截图保存到竞赛结果文件指定位置。

二、在 PC-D 上完成如下操作：
1、Server4 主机系统为 CentOS6.5，需要在此 Linux 平台上采用 KVM 方式安装以下虚拟机（小提示：如无法正确安装虚拟机 Centos-D1，下述题目中所涉及的虚拟机题目可在 Server4 真实主机中完成）。
（1）安装虚拟机“Centos-D1”，具体要求为内存 900MB，硬盘 5GB，分区大小为：SWAP 分区大小为 512M；/boot 分区大小为 500M，文件类型为 ext3；/home 分区大小为 1G，文件类型为 ext3，其余为/分区，文件类型为 ext3；

（2）安装虚拟机“Centos-D2”，具体要求为硬盘大小为 8GB，内存为 800MB；

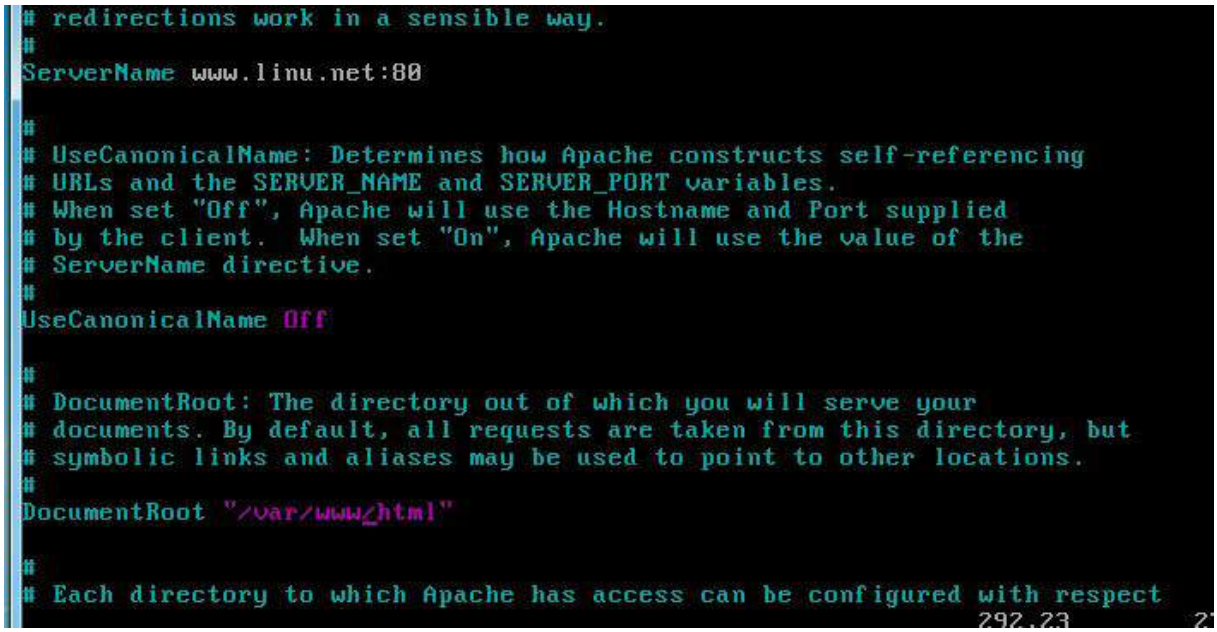
（3）将各虚拟机配置界面分别截图保存，内容有服务器的 IP 地址、子网掩码、网关和 DNS 等。

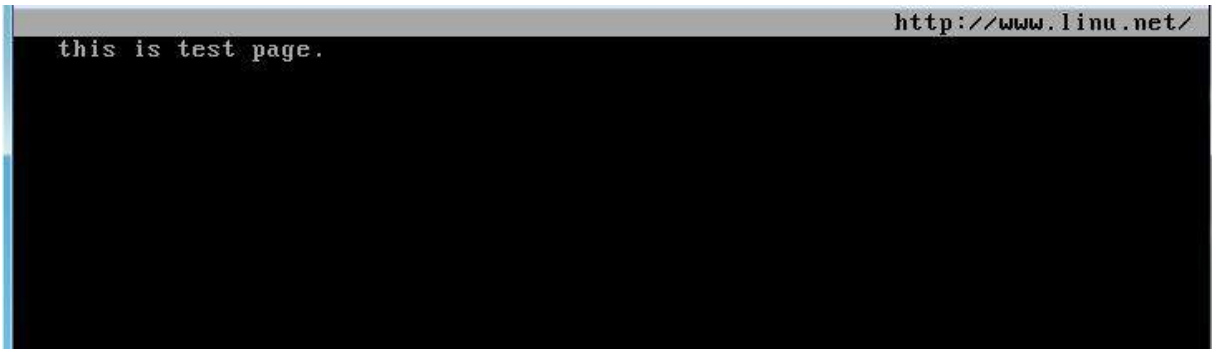




2、在主机 Centos-D1 中完成 Apache 服务器的部署

（1）在此服务器中安装 httpd 服务，为编辑 http.conf 配置文件的命令定义别名为 confighttp。建立网站 www. linu.net。网站主目录/var/www/html。首页内容为“this is test page.”;





（2）在网站目录下新建目录 https。创建自签名证书 server.crt 和私钥 server.key 以用于 SSL。私钥密码为“1234567”；

```
[root@localhost conf]# cd /etc/httpd/conf
[root@localhost conf]# ls
confighttp  httpd.conf  magic
[root@localhost conf]# mkdir /var/www/html/https
[root@localhost conf]#
```

```
[root@localhost certs]# openssl genrsa -des3 -out server.key 1024
Generating RSA private key, 1024 bit long modulus
..............++++++
.........................++++++
e is 65537 (0x10001)
Enter pass phrase for server.key:
Verifying - Enter pass phrase for server.key:
[root@localhost certs]#
```

```
[root@localhost certs]# openssl x509 -days 365 -req -in server.csr -signkey serv
er.key -out server.crt
Signature ok
subject=/C=XX/L=Default City/O=Default Company Ltd
Getting Private key
Enter pass phrase for server.key:
[root@localhost certs]#
```

（3）配置 http，使用自签名证书，使访问 www. linu.net/https 时必须使用 https 方式访问；此问须截图命名为 https.jpg 进行存储；

（4）配置只能使用域名访问网站，不能使用 ip 地址，httpd 服务开机自启动，不需要

输入私钥密码；


```
[root@localhost named]#
[root@localhost named]# chkconfig httpd on
[root@localhost named]# _
```

```
[root@localhost certs]# ls
ca-bundle.crt        localhost.crt    Makefile          server.crt  server.key
ca-bundle.trust.crt  make-dummy-cert  renew-dummy-cert  server.csr
[root@localhost certs]# openssl rsa -in server.key -out server.key
Enter pass phrase for server.key:
writing RSA key
[root@localhost certs]# _
```

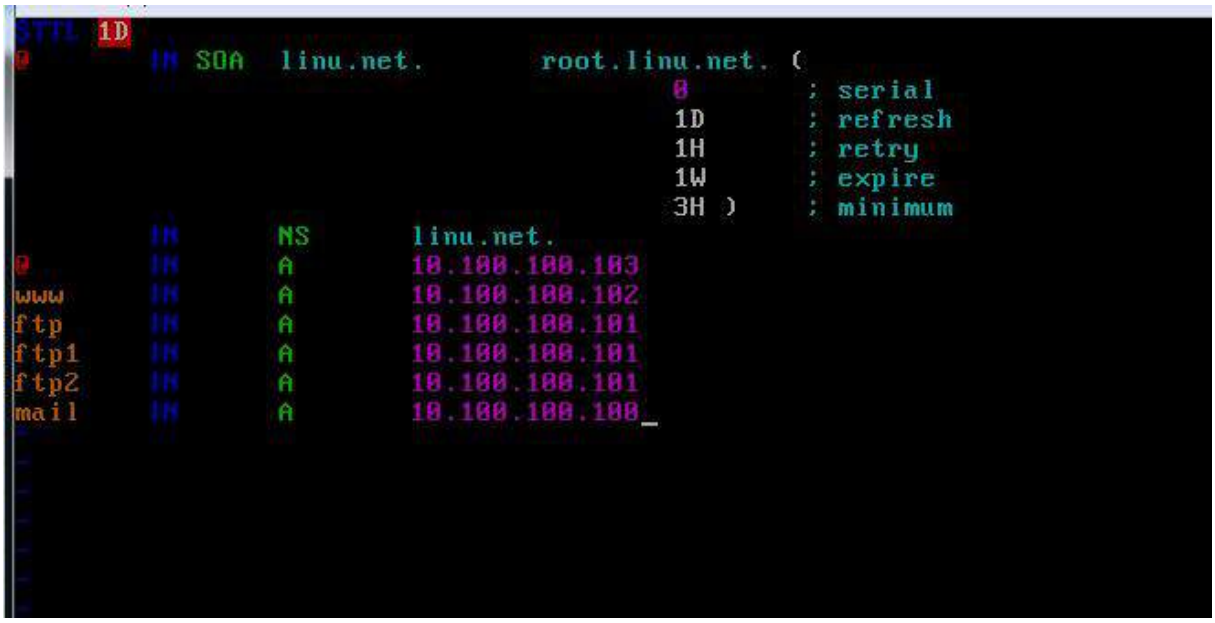
（5）将/var 目录打包并压缩成 gzip 格式，文件名为 var.tar.gz，保存到/tmp 目录下；

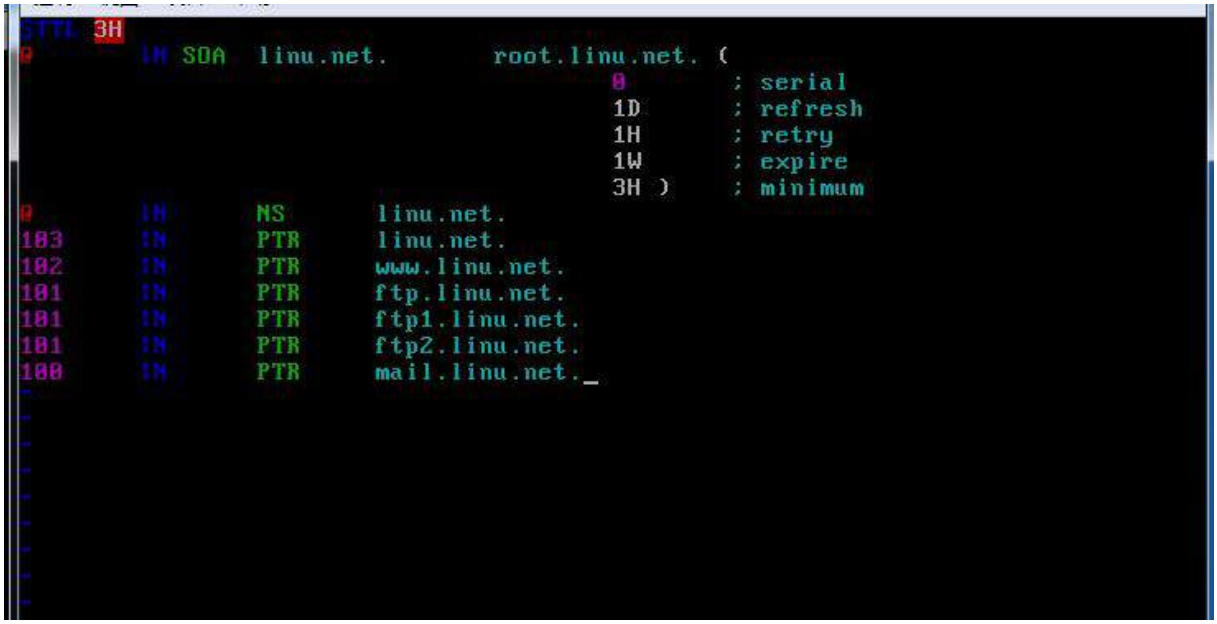
```
[root@localhost certs]# tar -zcvf /tmp/var.tar.gz /var_
```

（6）将上面 5 个方面的主要配置关键点界面截图保存到竞赛结果文件指定位置。

3、在主机 Centos-D2 中完成 BIND 域名服务器、MySQL 数据库服务器以及 NFS 共享服务器的部署

（1）在此服务器中安装配置 bind 服务，负责区域“linu.net”内主机解析，三台主机分别为 www. linu.net、ftp.linu.net、ftp1.jnds.net、ftp2.linu.net 以及 mail.linu.net，做好正反向 DNS 服务解析，对 tj.com 域的解析转发给 Win2003_A1；


$TTL 1D
@ IN SOA linu.net. root.linu.net. (
0 ; serial
1D ; refresh
1H ; retry
1W ; expire
3H) ; minimum
IN NS linu.net.
@ IN A 10.100.100.103
www IN A 10.100.100.102
ftp IN A 10.100.100.101
ftp1 IN A 10.100.100.101
ftp2 IN A 10.100.100.101
mail IN A 10.100.100.100


$TTL 3H
@ IN SOA linu.net. root.linu.net. (
0 ; serial
1D ; refresh
1H ; retry
1W ; expire
3H) ; minimum
@ IN NS linu.net.
103 IN PTR linu.net.
102 IN PTR www.linu.net.
101 IN PTR ftp.linu.net.
101 IN PTR ftp1.linu.net.
101 IN PTR ftp2.linu.net.
100 IN PTR mail.linu.net.

```
//
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//

options {
        listen-on port 53 { any; };
        listen-on-v6 port 53 { any; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        allow-query     { any; };
        recursion yes;
        foward only;
        forwarders{10.100.100.1;};_

        dnssec-enable yes;
        dnssec-validation yes;
        dnssec-lookaside auto;
-- INSERT --                                                    20,28-35      Top
```

（2）通过配置，在本机上可以使用 rndc 来控制域名服务运行；

```
        managed-keys-directory "/var/named/dynamic";
};

 key "rndc-key" {
        algorithm hmac-md5;
        secret "MqiAI5S33Gq8cYz11h5PeA==";
 };

 controls {
        inet 127.0.0.1 port 953
                allow { 127.0.0.1; } keys { "rndc-key"; };
 };
logging {
"named.conf" 53L, 1167C written
[root@localhost etc]#
[root@localhost etc]#
[root@localhost etc]#
[root@localhost etc]# service named restart
Stopping named: rndc .                                     [  OK  ]
Starting named:                                            [  OK  ]
[root@localhost etc]# rndc reload
WARNING: key file (/etc/rndc.key) exists, but using default configuration file (
/etc/rndc.conf)
server reload successful
[root@localhost etc]#
```

（3）在 CentOS 上安装 mysql 服务，配置 mysql 设置 root 口令为 tj2015，创建数据库 testdb，创建用户 test1，其对 testdb 数据库有完全控制权，仅可在本机登录。按如下结构创建 2-2 表 table1；

表 2-2 数据库表

字段名	数据类型	主键	自增
ID	int	是	是
name	varchar(10)	否	否
birthday	datetime	否	否
sex	cahr(1)	否	否

```
[root@localhost 桌面]# mysqladmin -u root password "tj2015"
[root@localhost 桌面]#
```

```
mysql> create database testdb;
Query OK, 1 row affected (0.00 sec)

mysql> creat user "test1"@"localhost" identified by "123456";
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for
the right syntax to use near 'creat user "test1"@"localhost" identified by "123456"' at line 1
mysql> create user "test1"@"localhost" identified by "123456";
Query OK, 0 rows affected (0.00 sec)

mysql> grant all on testdb.* to "testuser"@"localhost";
Query OK, 0 rows affected (0.00 sec)

mysql>
```

```
mysql> use testdb
Database changed
mysql> create table table1(
    -> ID int primary key auto_increment,
    -> name varchar(10),
    -> birthday datetime,
    -> sex char(1));
Query OK, 0 rows affected (0.03 sec)

mysql> desc table1;
+----------+-------------+------+-----+---------+----------------+
| Field    | Type        | Null | Key | Default | Extra          |
+----------+-------------+------+-----+---------+----------------+
| ID       | int(11)     | NO   | PRI | NULL    | auto_increment |
| name     | varchar(10) | YES  |     | NULL    |                |
| birthday | datetime    | YES  |     | NULL    |                |
| sex      | char(1)     | YES  |     | NULL    |                |
+----------+-------------+------+-----+---------+----------------+
4 rows in set (0.00 sec)

mysql>
```

（4）每周五凌晨 1：00 备份数据库 testdb 到/var/databak/testdb.sql；

```
[root@localhost /]# vim backup.sh
```

```
mysqldump -u root -ptj2015 testdb >/vardatabak/testdb.sql
~
~
~
~
~
~
~
~
~
```

```
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root
HOME=/

# For details see man 4 crontabs

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name command to be executed
 0   1  *  *  5 root /backup.sh
~
~
~
~
~
~
~
~
~
~
~
```

（5）配置 NFS 服务，服务开机自启动。按下表 2-3 要求共享目录；

表 2-3 共享目录表

共享目录	共享要求
/var/test	10.0.200.0/23 这个网段的用户具有读写权限，其它只读
/var/tmp	所有人都可以存取，root 写入的文件还具有 root 的权限

```
[root@localhost etc]# chkconfig nfs on
[root@localhost etc]#
```

```
/var/test       10.0.200.0/23(rw)       *(ro)
/var/tmp        *(ro,no_root_squash)
~
~
~
~
~
~
~
~
~
~
```

（6）创建用户 nfsuser，当 nfsuser 在终端登录时，自动 mount 共享的/var/test 目录到/home/nfsuser/t，退出时自动 umout；

```
[root@localhost etc]# useradd nfsuser
[root@localhost etc]# passwd nfsuser
更改用户 nfsuser 的密码 。
新的 密码：
无效的密码： 过于简单化/系统化
无效的密码： 过于简单
重新输入新的 密码：
passwd： 所有的身份验证令牌已经成功更新。
[root@localhost etc]#
```

```
# commands via sudo.
#
# Defaults   env_keep += "HOME"

Defaults    secure_path = /sbin:/bin:/usr/sbin:/usr/bin

## Next comes the main part: which users can run what software on
## which machines (the sudoers file can be shared between multiple
## systems).
## Syntax:
##
##      user    MACHINE=COMMANDS
##
## The COMMANDS section may have other options added to it.
##
## Allow root to run any commands anywhere
root    ALL=(ALL)       ALL

## Allows members of the 'sys' group to run networking, software,
## service management apps and more.
# %sys ALL = NETWORKING, SOFTWARE, SERVICES, STORAGE, DELEGATING, PROCESSES, LOCATE, DRIVERS

## Allows people in group wheel to run all commands
# %wheel        ALL=(ALL)       ALL

## Same thing without a password
# %wheel        ALL=(ALL)       NOPASSWD: ALL

## Allows members of the users group to mount and unmount the
## cdrom as root
# %users  ALL=/sbin/mount /mnt/cdrom, /sbin/umount /mnt/cdrom

## Allows members of the users group to shutdown this system
# %users  localhost=/sbin/shutdown -h now

## Read drop-in files from /etc/sudoers.d (the # here does not mean a comment)
#includedir /etc/sudoers.d
nfsuser         ALL=(ALL)       NOPASSWD: ALL
```

```
# .bash_profile

# Get the aliases and functions
if [ -f ~/.bashrc ]; then
        . ~/.bashrc
fi

# User specific environment and startup programs

PATH=$PATH:$HOME/bin

export PATH
sudo    mount 10.100.100.103:/var/test /home/nfsuser/t
~
~
~
~
```

```
# ~/.bash_logout
sudo umount /home/nfsuser/t
~
~
~
~
~
~
~
~
~
~
```

（7）将上面 6 个方面的主要配置关键点界面截图保存到竞赛结果文件指定位置。

4、在主机 Centos-D2 中完成 Samba 共享服务器的部署

（1）在此服务器中安装配置 Samba 服务，创建三个用户 m1,m2,m3。分别建立共享 m1，m2，m3，public，本地目录分别为/opt/a1、/opt/a2、/opt/a3、/opt/public；

```
[root@localhost nfsuser]# useradd m1
[root@localhost nfsuser]# useradd m2
[root@localhost nfsuser]# useradd m3
[root@localhost nfsuser]# smbpasswd -a m1
New SMB password:
Retype new SMB password:
Added user m1.
[root@localhost nfsuser]# smbpasswd -a m2
New SMB password:
Retype new SMB password:
Added user m2.
[root@localhost nfsuser]# smbpasswd -a m3
New SMB password:
Retype new SMB password:
Added user m3.
[root@localhost nfsuser]# mkdir /opt/a1
[root@localhost nfsuser]# mkdir /opt/a2
[root@localhost nfsuser]# mkdir /opt/a3
[root@localhost nfsuser]# mkdir /opt/public
[root@localhost nfsuser]# chmod 777 /opt/a1
[root@localhost nfsuser]# chmod 777 /opt/a2
[root@localhost nfsuser]# chmod 777 /opt/a3
[root@localhost nfsuser]# chmod 777 /opt/public/
[root@localhost nfsuser]#
```

（2）默认以匿名访问，可以对 public 有读权限。进入其它文件夹时需要对其身份认证；

```
#
# Scurity can be set to user, share(deprecated) or server(deprecated)
#
# Backend to store user information in. New installations should
# use either tdbsam or ldapsam. smbpasswd is available for backwards
# compatibility. tdbsam requires no further configuration.

        security = user
        map to guest=bad user
        passdb backend = tdbsam
```

（3）其中，m1 用户属于 manager 组，对 m1、m2、m3 共享有读写权限。m2,m3 为同一项目组 m2 的成员，可以互相对彼此文件有读的权限。/opt/a1 的共享只有 manager 组用户

可以访问；

```
[m1]
path = /opt/a1
writable=no
write list = m1
valid user=@manager
[m2]
path = /opt/a2
writable=no
write list = m1,m2
valid user=m1,m2,m3
[m3]
path = /opt/a3
writable=no
write list = m1,m3
valid user=m1,m2,m3
[public]
path = /opt/a1
public =yes
```

（4）将目录/var/www/liun.net 共享，共享名为 linu.net，配置当系统启动时自动启动 Samba 服务；

```
[linu.net]
path = /var/www/liun.net
public =yes
~
~
~

[root@localhost samba]# chkconfig smb on
[root@localhost samba]#
```

（5）提取本机 eth0 网卡 IPv4 地址，如（参见 IP 地址分配表 1-5 自行规划内容）；

```
[root@localhost samba]#
[root@localhost samba]# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:3F:9A:CB
          inet addr:10.100.100.103  Bcast:10.100.100.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe3f:9acb/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3459 errors:0 dropped:0 overruns:0 frame:0
          TX packets:687 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:635855 (620.9 KiB)  TX bytes:50665 (49.4 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:860 errors:0 dropped:0 overruns:0 frame:0
          TX packets:860 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:74974 (73.2 KiB)  TX bytes:74974 (73.2 KiB)

[root@localhost samba]#
```

（6）将上面 4 个方面的主要配置关键点界面截图保存到竞赛结果文件指定位置。

2015 年全国职业院校技能大赛
网络搭建与应用竞赛
（总分 1000 分）

赛题说明

一、竞赛内容分布

“网络搭建与应用”竞赛共分二个部分，其中：

第一部分：网络搭建及安全部署项目，占总分的比例为 45%；

第二部分：服务器配置及应用项目，占总分的比例为 55%；

二、竞赛注意事项

（1）禁止携带和使用移动存储设备、计算器、通信工具及参考资料。

（2）请根据大赛所提供的比赛环境，检查所列的硬件设备、软件清单、材料清单是否齐全，计算机设备是否能正常使用。

（3）本试卷共有两个部分。请选手仔细阅读比赛试卷，按照试卷要求完成各项操作。

（4）操作过程中，需要及时保存设备配置。比赛结束后，所有设备保持运行状态，不要拆、动硬件连接。

（5）比赛完成后，比赛设备、软件和赛题请保留在座位上，禁止将比赛所用的所有物品（包括试卷和草纸）带离赛场。

（6）所有需要提交的文档均放置在桌面的 PC1 “比赛文档”文件夹中，禁止在纸质资料上填写与竞赛无关的标记，如违反规定，可视为 0 分。

（7）裁判以各参赛队提交的竞赛结果文档为主要评分依据。所有提交的文档必须按照赛题所规定的命名规则命名，文档中有对应题目的小标题，截图有截图的简要说明，否则按无效内容处理。

（8）与比赛相关的工具软件放置在 D 盘的 tools 文件夹中。

三、竞赛项目背景及网络拓扑

1. 项目描述

下图是某集团公司在天津设有总公司，在上海设有分公司，为了实现信息交流和资源共享，需要构建一个跨越两地的集团网络。总公司采用节点和链路冗余的网络架构及双出口的网络接入模式，采用防火墙接入互联网络，保护内网用户资源，采用路由器接入城域网专用链路来传输业务数据流。

总公司为了安全管理每个部门的用户，使用 VLAN 技术将每个部门的用户划分到不同的 VLAN 中。上海分公司采用路由器接入互联网络和城域网专用线路，分公司的内网用户接入采用无线接入方式访问网络资源。为了保障总公司与分公司业务数据传输的高可用性，租用广域网专用线路 ISP 为主链路，采用基于 IPSEC-VPN 技术作为因特网链路的备份链路，以实现业务流量的高可用性。总公司与分公司网络采用 OSPF 路由协议；而总公司防火墙与内网路由器的连接采用 RIP 路由协议，集团网络具体拓扑结构如图 1 所示。

2. 网络拓扑规划

网络拓扑结构规划如图 1 所示。

图1 集团网络拓扑-结构图

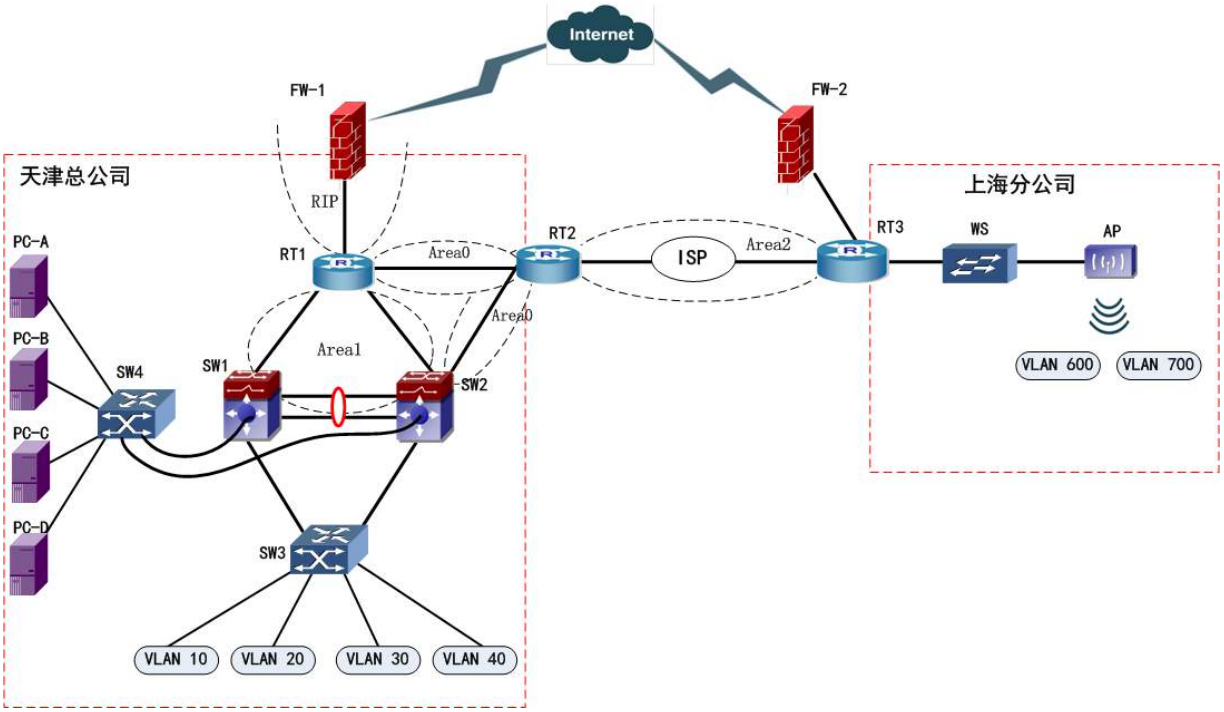


图 1　网络拓扑结构图

本次公司的网络构建包括总公司和分公司的两个部分。总公司局域网核心采用双交换机的构架，通过 VRRP 结合 MSTP 技术实现负载均衡和链路备份。两台核心交换机分别连接到核心路由器，核心路由器连接到网络出口防火墙，同时核心路由器通过 ISP 专线

连接到分公司的出口路由器。总公司的网络出口使用防火墙分别连接到 ISP 和 VPN 设备，通过配置防火墙来实现内网用户访问 Internet 以及保护内网的安全。总公司和分公司之间的办公用户通过 VPN 建立的隧道相互通信，有效的保证了数据传输的安全性。

服务器集中放置在网络中心机房，直接连接到核心交换机。分公司的网络的出口路由器分别连接到 ISP 和 VPN 设备，通过部署防火墙来保护内网的安全，内网的用户分别通过专网或 VPN 建立的安全隧道来访问总公司的资源。

四、工程建设的内容

本工程项目主要建设内容为：

1. 总公司与分公司布线系统建设

总公司与分公司内部局域网的布线系统搭建，包括数据及语音的布线系统。

2. 总公司局域网建设

总公司网络构建（有线双核心网络）、可用性及安全规则部署。

3. 分公司局域网建设

分公司网络构建（无线网络）、可用性及安全规则部署。

4. 总公司与分公司广域网互联建设

总公司与分公司之间采用数据专线、VPN 方式互联。

5. 总公司应用平台建设

在总公司的网络中心机房，部署 Windows 2003 Server、Windows2008 Server 及 LINUX 服务器系统，并在此之上架设 DNS、WEB、DHCP、FTP、MAIL、CA 认证、Apache、NFS、KVM 安装等应用服务。

第一部分 网络配置项目(450 分)

【注意事项】

1、设备 console 线有两条。交换机， AC，防火墙使用同一条 console 线，路由器使用另外一条 console 线。

2、设备配置完毕后，保存最新的设备配置。保存文档方式分为两种：

a) 交换机和路由器要把 show running-config 的配置保存在 PC1 桌面的相应文档中，文档命名规则为：设备名称.doc,例如：RT1 路由器文件命名为：RT1.doc，然后放入到 PC1 桌面上“比赛文档”文件夹中

b) 防火墙等截图方式的设备，把截图的图片放到同一 word 文档中，文档命名规则为：设备名称.doc,例如：防火墙 FW1 文件命名为：FW1.doc, 保存后放入到 PC1 桌面上“比赛文档”文件夹中。

一、网络设备配置要求

1. 设备连接关系:

表 1-3 网络设备 1 连接到设备 2 表

设备一	设备二	设备一端口	设备二端口	线缆类型
RT1	FW1	GE0/5	E0/1	双绞线
RT1	RT2	GE 0/4	GE 0/4	双绞线
RT1	SW1	GE0/2	E1/0/1	双绞线
RT1	SW2	GE0/3	E1/0/1	双绞线
RT2	RT3	S0/1	S0/2	V35
RT2	SW2	GE0/2	E1/0/2	双绞线
RT3	FW2	GE0/3	E0/1	双绞线
RT3	WS	GE0/4	E1/0/1	双绞线
SW1	SW2	E1/0/14-15	E1/0/14-15	双绞线
SW1	SW3	E1/0/21	E1/23	双绞线
SW1	SW4	E1/0/23	E1/23	双绞线
SW2	SW3	E1/0/21	E1/24	双绞线
SW2	SW4	E1/0/24	E1/24	双绞线
SW4	PC-A	E1/1	NIC	双绞线
SW4	PC-B	E1/2	NIC	双绞线
SW4	PC-C	E1/3	NIC	双绞线
SW4	PC-D	E1/4	NIC	双绞线
WS	AP	E1/0/2	LAN 口	双绞线

2．网络设备 IP 地址自行分配表。

表 1-4 网络设备 IP 地址表

设备	设备名称	设备接口	IP 地址/
路由器	RT1	GigaEthernet0/2	
		GigaEthernet0/3	
		GigaEthernet0/4	
		GigaEthernet0/5	
	RT2	Serial0/1	
		GigaEthernet0/2	
		GigaEthernet0/4	
	RT3	Serial0/2	
		GigaEthernet0/3	
		GigaEthernet0/4	
三层交换机	SW1	VLAN1000 (Ethernet1/0/1)	
		VLAN3000 (Ethernet1/0/14-15)	
		VLAN10 SVI	
		VLAN20 SVI	
		VLAN30 SVI	
		VLAN40 SVI	
		管理 VLAN50 SVI	
		服务器群 VLAN100 (Ethernet1/0/10-13)	
	SW2	VLAN2000 (Ethernet1/0/1)	
		VLAN3000 (Ethernet1/0/14-15)	
		VLAN10 SVI	
		VLAN20 SVI	
		VLAN30 SVI	
		VLAN40 SVI	
		管理 VLAN50 SVI	
二层交换机	SW3	管理 VLAN50 SVI	
	SW4	管理 VLAN50 SVI	
防火墙 1	FW1	Ethernet0/1	
		Ethernet0/3	139.4.17.1/24
防火墙 2	FW2	Ethernet0/1	
		Ethernet0/3	139.4.17.2/24
无线控制器	WS	VLAN600 SVI	
		VLAN700 SVI	

3. 服务器 IP 地址自行分配表:

表 1-5 服务器 IP 地址分配表

宿主机	虚拟 主机名称	域名信息	服务角色	系统及 版本信息	IPv4 地址信息
PC-A	Win2003-A1	web.tj.com	WWW 服务器 CA 服务器	Windows Server 2003 R2	10.100.100.1
	Win2003-A2	web2.tj.com	WWW 服务器	Windows Server 2003 R2	10.100.100.2
	Win2008-A1	dc.tj.com	DC 域控制器	Windows Server 2008 R2	10.100.100.3
PC-B	Win2008-B1	ftp.tj.com	FTP 服务器	Windows Server 2008 R2	10.100.100.4
	Win2003-B1	Dhcp.tj.com	DHCP 服务器	Windows Server 2003 R2	10.100.100.5
	WindowsXP	pc.tj.com	工作站	WindowsXP	10.100.100.6
PC-C	Win2003-C1	dc.ykca.com	DNS 服务器	Windows Server 2003 R2	10.100.100.7
	Win2008-C1	rodc.ykca.com	只读 域控制器	Windows Server 2008 R2	10.100.100.8
	Centos-C1	www.linunet.tj.com	Apache 服务器	Centos 6.5	10.100.100.100
	Centos-C2	dns. linu.net	BIND 域名服务器 NFS 共享 服务器	Centos 6.5	10.100.100.101
PC-D	Centos-D1	ftp. linu.net	FTP 服务器	Centos 6.5	10.100.100.102
	Centos-D2	Mail. linu.net	MAIL 服务器	Centos 6.5	10.100.100.103

二、网络搭建部分：

1. 物理连接与 IP 地址划分

（1）按照网络拓扑图制作以太网网线跳线，用于 SW1、SW2、RT1、SW3 设备的连接，并增加标识。要求符合 T568A 和 T568B 的标准，其线缆长度适中；

（2）根据“拓扑结构图”和“表 1-4:网络设备 IP 地址分配表”和“表 1-5：服务器 IP 地址分配表”所示，请对网络中的所有网络设备接口和服务器分别规划部署 IP 地址。

总公司中整个网络互联地址规划使用 172.16.0.0/16 地址段，为了节省 IP 资源，请按下面需求做到合理分配，目前市场部有 91 名员工、工程部有 110 名员工、软件部和系统集成部两个部门都有 121 名员工，服务器的网段为 172.16.100.0/24。上

海分公司使用 172.16.200.0/23 地址段,保证上海分公司行政部至少有 100 台主机，销售部至少有 40 台主机。天津总公司与上海分公司所有设备互联地址使用/30 的掩码进行分配。并把分配后的地址填入上述表 1-4 及表 1-5 分配表中的空白处。

注意：

- 要求网络地址根据上述题目要求合理规划；
- 网关地址规划为本网段的最后一个地址。

2.交换机配置

（1）为交换机设备命名，命名规则参考为表 1 中的“设备名称”，设备名称的命名规则与拓扑图图示名称相符；

（2）在两台三层交换设备上开启 telnet 管理功能，使用安全 IP 技术，只允许管理 VLAN 的主机对三层交换设备进行管理，同时要求每台网络设备只允许 6 条线路管理网络设备，管理设备使用 telnet 用户，口令为 2015telnet，enable 密码为 2015network；

（3）依据“拓扑结构图”和 1-6 表，在交换机上完成 VLAN 配置和端口分配，不允许不必要的 VLAN 通过；

表 1-6VLAN 接口地址表

设备	VLAN 名称	VLAN ID	接口
SW1	Link_to_管理 vlan	50	Ethernet1/20
	Link_to_RT1	1000	Ethernet1/0/1
	Link_to_SW2	3000	Ethernet1/0/14-15
SW2	Link_to_管理 vlan	50	Ethernet1/20
	Link_to_RT1	2000	Ethernet1/0/1
	Link_to_SW1	3000	Ethernet1/0/14-15
SW3	Link_to_管理 vlan	50	任意
	Link_to_ SW1/SW2	trank	Ethernet 1/23-24
	SCB（市场部）	10	Ethernet 1/0/1-5
	GCB（工程部）	20	Ethernet 1/0/6-10
	RJB（软件部）	30	Ethernet 1/0/11-15
	XTJCB（系统集成部）	40	Ethernet 1/0/16-20
SW4	Link_to_管理 vlan	50	任意
	Link_to_PC-A、PC-B、PC-C、PC-D	100	Ethernet 1/1-4
	Link_to_ SW1	trunk	Ethernet 1/23
	Link_to_ SW2	trunk	Ethernet 1/24

（4）天津总公司两个核心交换机 SW1 和 SW2 之间使用双线路连接，分别下联到接入交换机 SW3，采用基于 VLAN 生成树协议，实现网络中的二层的负载均衡和冗余备份。交换机创建两个实例：分别为 Instance 10 和 Instance 20，其中 Instance 10 关联

VLAN 10 和 VLAN20，Instance 20 关联 VLAN 30 和 VLAN40。SW1 为缺省 Instance0 和 Instance10 的根交换机，为 Instance20 备份交换机；SW2 为 Instance20 根交换机，为缺省 Instance0 和 Instance10 的备份交换机，按需求设置 STP 优先级为 8192。同时结合 VRRP 技术实现 VLAN10、VLAN20、VLAN30、VLAN40 内的用户网关的冗余备份。设置 SW1 为 VLAN10、20 的 Master 路由器，设置 SW2 为 VLAN30、40 的 Master 路由器。要求 VRRP 组中高优先级设置为 120，同时开启抢占特性。将各 VLAN 的虚拟 IP 地址规划填入下表 1-7 所示：

表 1-7 VLAN 虚拟 IP 地址表

VLAN-ID	VRRP 备份组号（VRID）	VRRP 虚拟 IP 地址
VLAN10	10	
VLAN20	20	
VLAN30	30	
VLAN40	40	

（5）将 SW1 三层交换机 Ethernet 1/0/14 和 Ethernet 1/0/15 接口与 SW2 三层交换机 Ethernet1/0/14 和 Ethernet1/0/15 接口配置为动态模式的端口聚合；

（6）总部服务器群直接连接在交换机 SW4 的 Ethernet1/1-4 端口上，需要在两个端口上限制接入服务器的数量，Ethernet1/3 限制为 2 台，Ethernet1/4 限制为 4 台，超过后将关闭该端口；

（7）在所有交换设备上，使用系统登录标题：“welcome login guoshai2015!”。在 10 分钟内，没有任何输入信息，网络设备连接超时。

3. 路由器配置

（1）为路由设备命名，命名规则参考为表 1 中的“设备名称”，设备名称的命名规则与拓扑图图示名称相符；

（2）在每个路由器设备与其它网络设备连接的接口都要进行描述；

（3）根据网络拓扑图所示，为了保障专用线路的链路安全，需要在 ISP（RT2 与 RT3 之间）连接的链路上配置 PPP 协议，采用双向 CHAP 的验证方式，速率为 1024000bps，用户名分别为 RT2 和 RT3，密码均为 7654321；

（4）天津总公司内网采用 OSPF 动态路由协议，防火墙 FW1 与路由器 RT1 之间采用 RIP 协议，通过专线实现与分公司的互联互通，请自行规划设备 RouterID，并填入下表 1-8：

表 1-8VLAN 虚拟 IP 地址表

设备名称	RouterID
RT1	
RT2	
RT3	
SW1	
SW2	

（5）集团公司网络采用了 OSPF 和 RIP 两种动态路由协议，合理规划开销值，实现集团总公司访问外网数据流主走 RT1，备走 RT2；到分公司内网数据流主走 RT2，备走 RT1；

（6）在 RT2 上使用队列拥塞管理技术，使内网访问分公司的正常数据流优先级最高，Telnet 数据流优先级最低；

（7）在 RT3 上配置上海分公司网段访问集团公司资源的下载速率最大为 2Mbps；并为分公司访问集团公司时设置 QOS，分别为 VLAN600 保留 20%的带宽、VLAN700 保留 10%的带宽。

4. 无线配置

（1）上海分公司用户采用无线接入方式，其中 VLAN600 用户的 SSID 为 SH001，协议为 802.11b，信道为 1；无线控制器做为 DHCP 服务器为 VLAN600 用户动态分配 IP 地址，地址租约时长为 1 天。用户接入无线网络时采用 WEP 认证方式，其口令为 012345678；

（2）VLAN700 用户的 SSID 为 SH002，协议为 802.11g，信道为 6；使用无线控制器做为 DHCP 服务器，为 VLAN700 用户动态分配 IP 地址和网关，地址租约时长为 3 天。用户接入无线网络时需要采用 WPA-personal 加密方式，其口令为 1234567890；

（3）配置 AP 下可以连接的无线用户数是 20，用户的老化时间为 6 分钟；

（4）激活无线网络的二层隔离，实现同一个 AP 下无线局域网内用户不能互相访问，配置该 AP 下可以连接的无线网络用户数为 20；

（5）配置无线局域网用户上行速度为 512Kbps，下行速度为 2Mbps，突发速度为 4Mbps；

（6）将 MAC 地址为 C417.C417.C417 的无线客户端加入黑名单；

（7）黑名单过滤策略之前，MAC 地址 0D03.0D03.0D03 的无线客户已经加入无线网，配置 AC 删除这个非法用户。

注意：新建参赛号+无线. doc 文件，将无线配置后的关键步骤界面截图保存，并存放在主机 F 盘上以自己参赛号命名文件夹中。

提交的截图：

- 将截图粘贴到“工位号_网络无线配置文档.doc”中，标记为“(1)网络无线相关配置截图”，并对截图进行必要的说明，保存到指定位置。

三、网络安全部分：

1. 防火墙配置

（1）集团公司内网 VLAN20、VLAN30 用户可以通过防火墙 FW-1 做 NAT 访问 Internet，并将总公司内网 WWW 服务器映射到外网接口。上海分公司所有用户可以通过防火墙 FW-2 做 NAT 访问 Internet；

（2）集团公司和上海分公司内网的 Web 服务器分别需要对外提供服务；

（3）为了保障总公司内网的安全性，在 FW-1 上做以下防护部署：

- 端口扫描攻击防护功能，在 3 秒时间内，有 5 个以上相同 IP 地址的 TCP SYN 包请求，则发出警报，但允许数据包通行；
- 在防火墙的在安全网关上配置在安全网关上配置网页关键字规则，禁止公司工程部网段，访问含“X”和“S”两个词汇的网页，并对试图访问的行为进行记录；
- IP 地址欺骗攻击防护功能；
- 配置 Ping of Death 攻击防护功能；
- 配置 Land 攻击防护功能；
- 配置 WinNuke 攻击防护功能；

（5）在防火墙上创建允许从管理网段地址到任意地址的 ICMP 服务的策略规则；

（6）在 FW1 中禁止 UDP 的 4500 端口以及 TCP 的 6300 端口的双向数据包通信。

- 防火墙提交的截图:用户配置防火墙的所有关键配置点信息(包括 FW1 和 FW2)。
- 将截图粘贴到“工位号_防火墙配置文档.doc”中，标记为“防火墙配置相关截图”，并对截图进行必要的说明。

2、VPN 配置

（1）为了保障总公司与分公司之间传输业务数据流，当总公司与分公司之间的 ISP 专线中断后，需要采用互联网链路为备份链路，在天津总公司与上海分公司的两端防火墙上配置 VPN，采用置 GRE over IPSec 功能，采用 esp-md5-3des-g2 提议部署实现总部与分公司之间信息通过 Internet 的安全传输；

（2）在天津总公司出口防火墙上配置 SSL 方式远程接入 VPN，允许远程办公用户可以访问服务群 WWW、FTP 资源，其使用的合法用户名为 vpn10、vpn11 和 vpn12，其共同口令为 2015SEC，其拨入的计算获取的 IP 地址段为 172.16.150.0/24。

- VPN 提交截图：用户配置 VPN 的所有信息(包括 VPN1 和 VPN2)，包含配置过程中出现的每一个界面都需要截图；
- 将截图粘贴到“工位号_VPN 配置文档.doc”中，标记为“VPN 配置相关截图”，并对截图进行必要的说明。

---

3. 网络系统安全配置

（1）所有启用 OSPF 协议的接口上都使用 MD5 认证，认证密钥为：1234567。为了加快路由协议的收敛时间以及故障恢复时间。调整 RIP 时钟的更新时间为 15 秒，失效时间 70 秒，刷新时间 100 秒；

（2）为了规范总公司员工的上网行为，规定总公司办公区员工（vlan12 网段）在周一到周五上班时间 (8:30---17:30) ，除了和总公司以及分公司的内部网络通信之外，只能使用公网的 http、ftp、mail 和 dns 服务，其它时间不进行限制，请在 RT1 上配置访问控制列表；

（3）分别在 RT1 上配置访问控制列表，用于禁止外网访问内网的 138、139 和 445 端口；

（4）在 SW3 上设置，配置 VLAN20 端口安全功能，每个接口的最大连接数为 5，如果违规则关闭接口；

（5）请将软件部某开发终端主机 IP 地址与 MAC 地址绑定（该终端的 MAC 地址为：47-01-39-04-17-ff,IP 地址可参考表 1-4 中软件部的一个可用 IP 地址）；

（6）请配置 SW4 交换机的 Ethernet 1/10-20 端口为 802.1X 认证端口，交换机的管理地址、终端的 IP 地址、认证服务器的地址请根据前面规划进行设置；

（7）对服务器群资源进行震荡波、SQL 蠕虫病毒的防护。

【结果文件的提交】

在 RT1、RT2、RT3、SW1、SW2、SW3、SW4 上运行 show running-config，将运行结果粘贴到“工位号_网络配置文档.doc”中（如 47 号工位的文件命名为：47_网络配置文档.doc），此时文档已经包含有：

（1）无线网络相关配置截图，

（2）VPN 配置相关截图，

（3）防火墙配置相关截图，

（4）请将路由器和交换机的 show running-config 信息接着写入：

①RT1 的 show running-config 信息；

②RT2 的 show running-config 信息；

③RT3 的 show running-config 信息；

④SW1 的 show running-config 信息；

⑤SW2 的 show running-config 信息；

⑥SW3 的 show running-config 信息；

⑦SW4 的 show running-config 信息

所有设备需要通过文档的方式保存，名称与设备名称一致。并将所有文档保存到计算机桌面以自己参赛工位号文件夹内，若缺少文件，涉及到该文件对应设备下的所有分值记为 0 分。

第二部分服务器配置及应用项目

项目实施 Windows 操作系统部分

【注意事项】

（1）题目中所涉及 Windows 操作系统的 administrator 管理员用户密码为 2015Net（注意区分大小写），若未按照要求设置密码，涉及到该操作的所有分值记为 0 分。

（2）系统主机及虚拟主机的 IP 属性设置请按照网络拓扑结构图以及“表 1-5：IP 地址自行规划表”的要求设定。

（3）除非作特殊说明，在同一主机下需要安装相同操作系统版本的虚拟机时，可采用 VM VirtualBox 软件自带的克隆系统功能实现。

（4）所有系统镜像文件及试题所需的其它软件均存放在每台主机的 D:\soft 文件夹中，并将题目要求的截图内容以.jpg 格式存储于桌面 Backup 文件夹中。

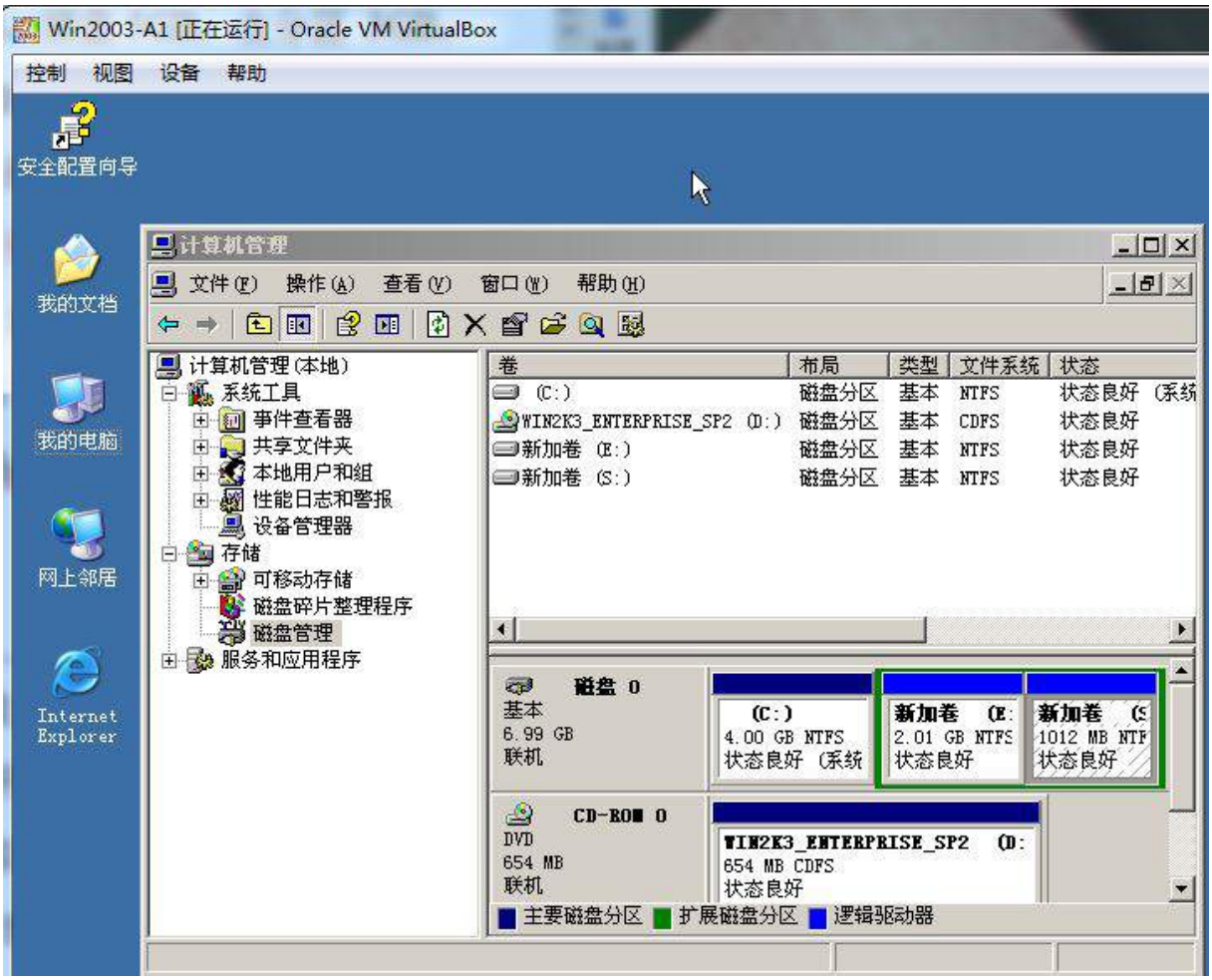
（5）请各位选手按下列要求完成各项服务器配置，在完成配置后提交能反映各个配置项目结果的窗口截图，比如 PC-A 中 Windows2003 系统的所有截图按照试题顺序粘贴在文件名为：工位号_PC-A.doc（如 47 号工位的文件命名为：47_PC-A.doc）的文档中。文档中要求有试题的题号小标题，并对每个截图进行必要的说明，无截图的项目不得分。

一、在 PC-A 上完成如下操作

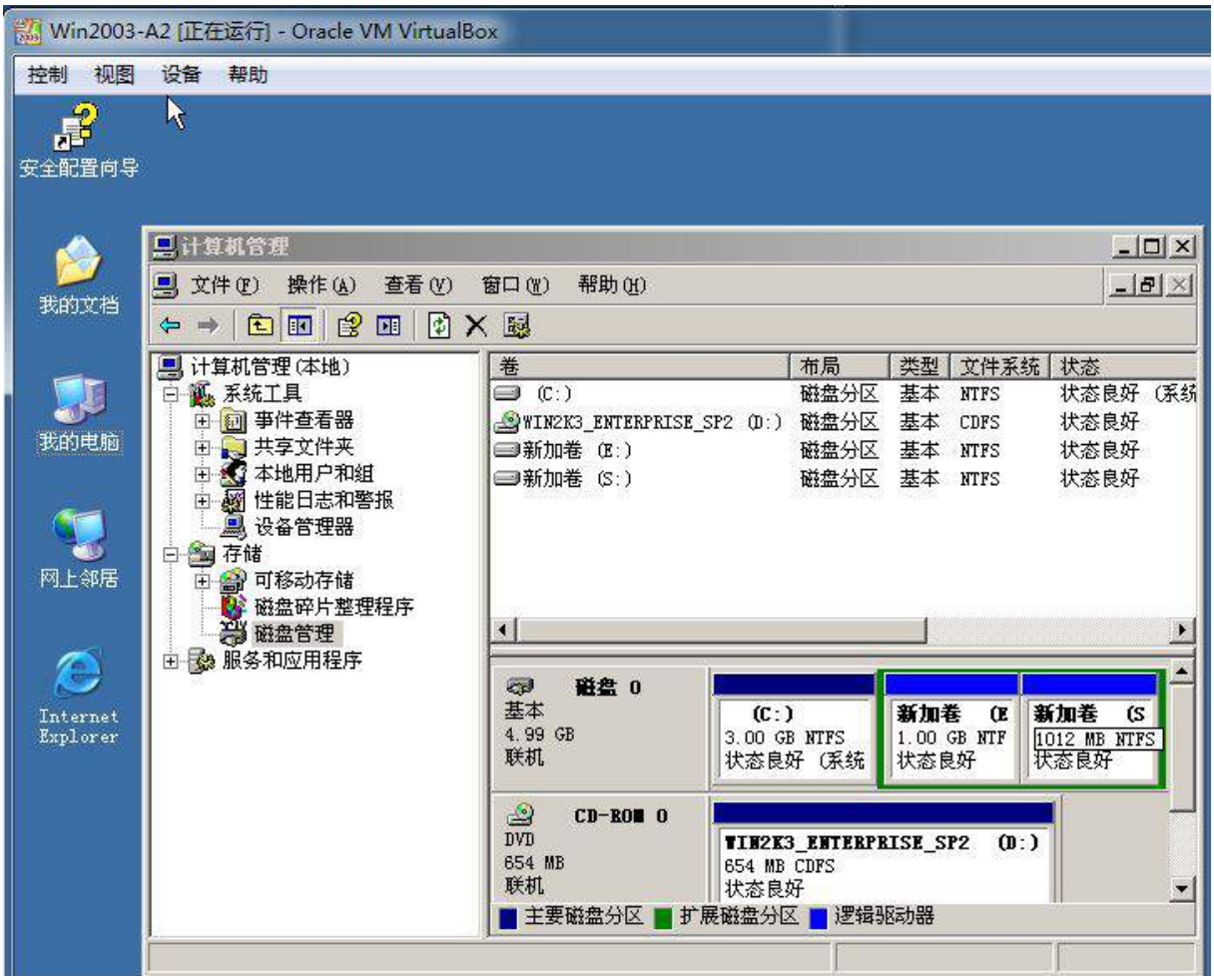
1. 完成虚拟主机的创建

（1）创建虚拟机“Win2003-A1”，具体要求为内存 512MB，硬盘 7GB，主分区 4GB，扩展分区 3GB；分为两个逻辑分区,大小分别为 2GB 和 1GB；


常规
名称: Win2003-A1
操作系统: Windows 2003 (64 bit)
预览
Windows Server 2003
系统
内存大小: 512 MB
启动顺序: 软驱, 光驱, 硬盘
硬件加速: VT-x/AMD-V, 嵌套分页
显示
显存大小: 18 MB
远程桌面服务器: 已禁用
录像: 已禁用
存储
控制器: IDE
第一IDE控制器主通道: Win2003-A1.vdi (普通, 7.00 GB)
第二IDE控制器主通道: [光驱] Windows.Server.2003.企业版.SP2.原版安装光盘.ISO (654.34 MB)
声音
主机音频驱动: Windows DirectSound
控制芯片: Intel HD 音频
网络
网卡 1: Intel PRO/1000 MT 桌面 (桥接网络, Intel(R) Ethernet Connection I217-LM)

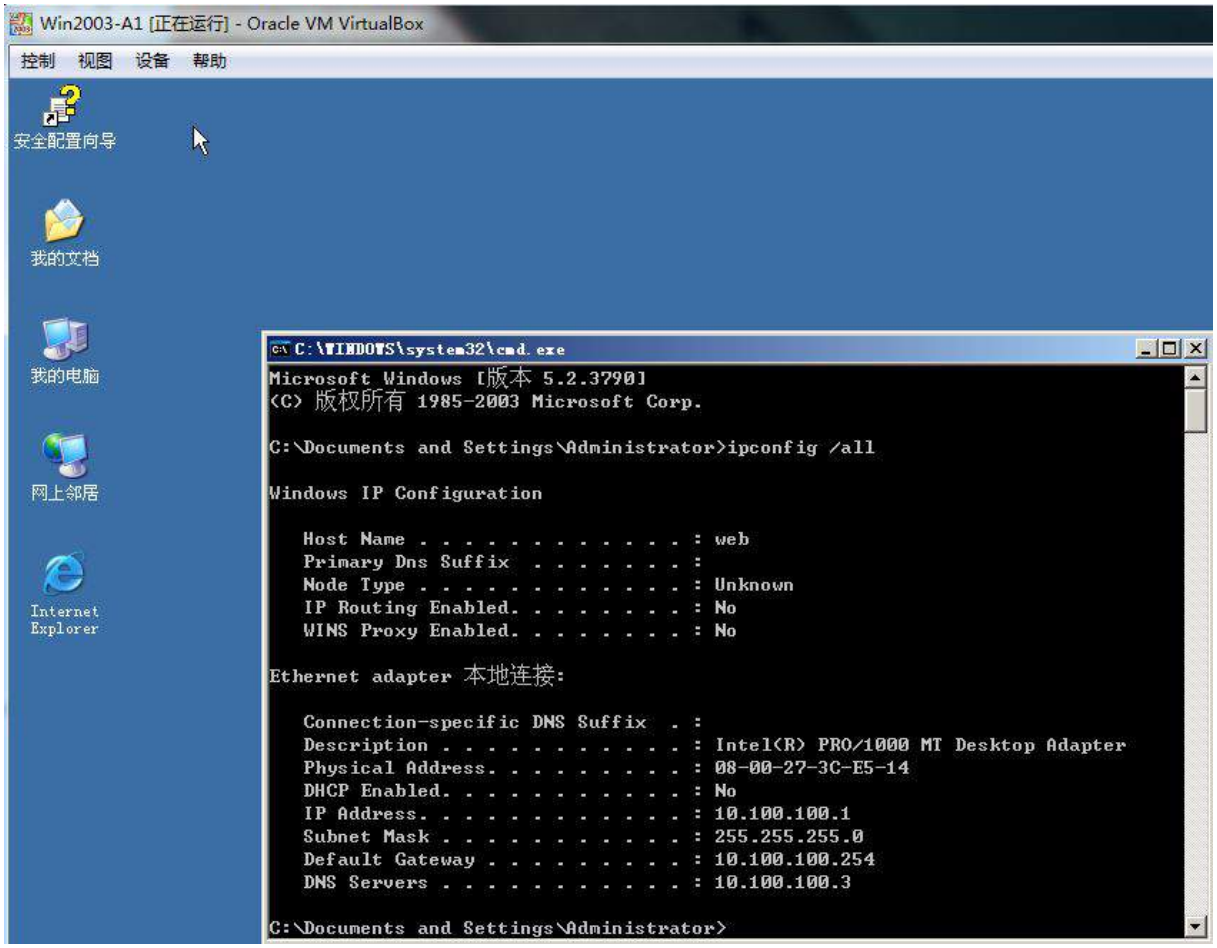

Win2003-A1 [正在运行] - Oracle VM VirtualBox
控制 视图 设备 帮助
安全配置向导
我的文档
我的电脑
网上邻居
Internet Explorer
计算机管理
文件(F) 操作(A) 查看(V) 窗口(W) 帮助(H)
计算机管理(本地)
系统工具
事件查看器
共享文件夹
本地用户和组
性能日志和警报
设备管理器
存储
可移动存储
磁盘碎片整理程序
磁盘管理
服务和应用程序
卷 布局 类型 文件系统 状态
(C:) 磁盘分区 基本 NTFS 状态良好 (系统
WIN2K3_ENTERPRISE_SP2 (D:) 磁盘分区 基本 CDFS 状态良好
新加卷 (E:) 磁盘分区 基本 NTFS 状态良好
新加卷 (S:) 磁盘分区 基本 NTFS 状态良好
磁盘 0
基本
6.99 GB
联机
(C:)
4.00 GB NTFS
状态良好 (系统
新加卷 (E:
2.01 GB NTFS
状态良好
新加卷 (S
1012 MB NTF
状态良好
CD-ROM 0
DVD
654 MB
联机
WIN2K3_ENTERPRISE_SP2 (D:
654 MB CDFS
状态良好
主要磁盘分区
扩展磁盘分区
逻辑驱动器

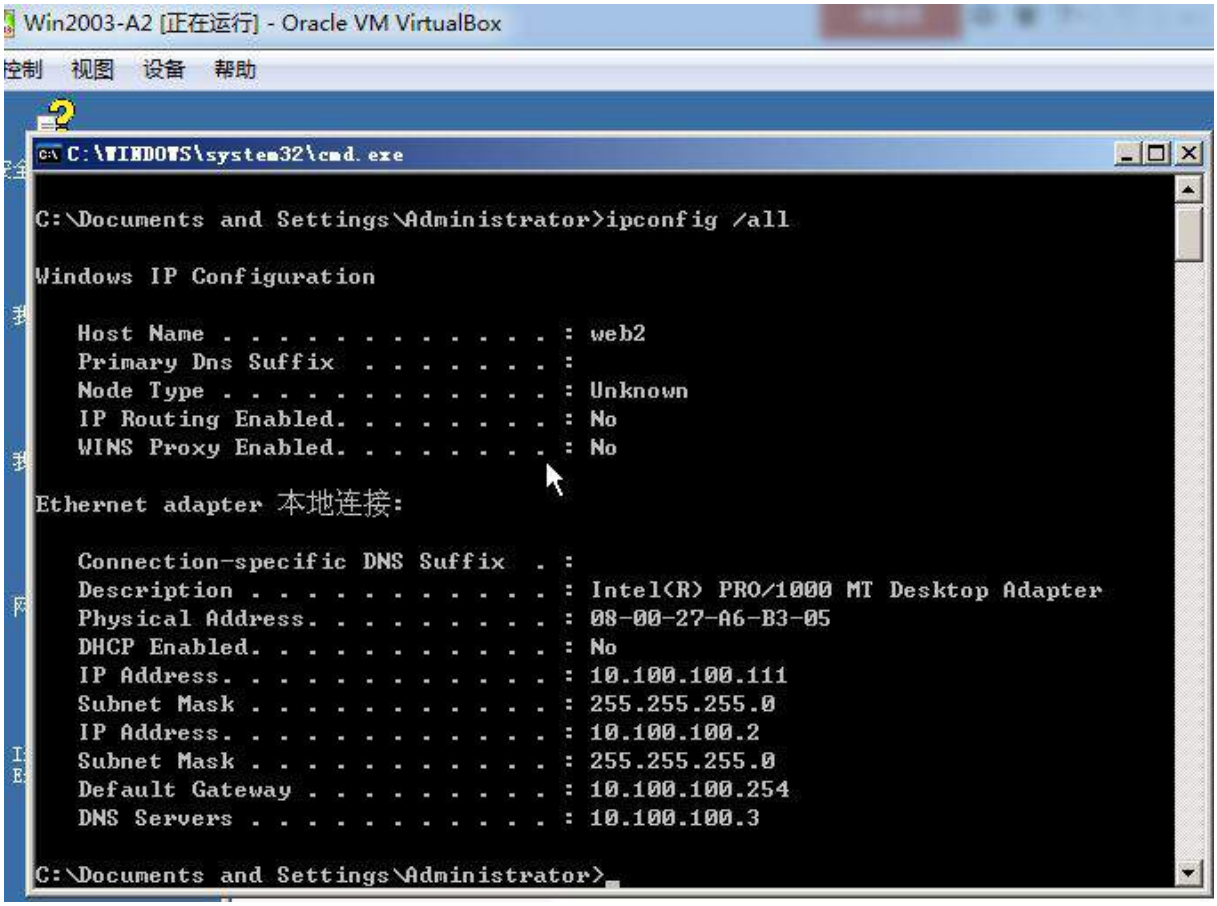
（2）创建虚拟机“Win2003-A2”，具体要求为内存 512MB，硬盘 5GB，主分区 3GB，扩展分区 2GB；分为两个逻辑分区,大小分别为 1GB 和 1GB；

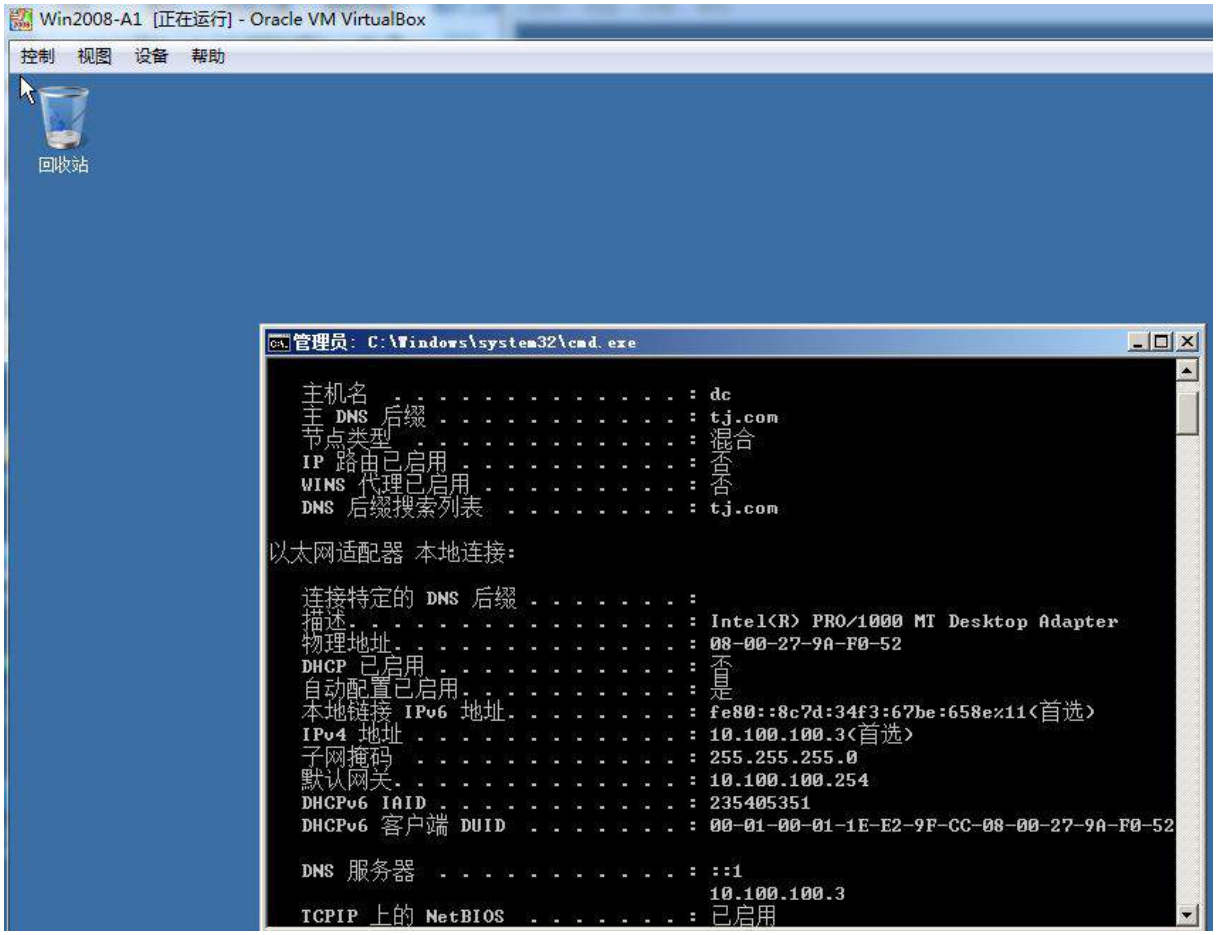


（3）创建虚拟机“Win2008-A1”,具体要求为内存 768MB,硬盘 10GB,主分区 5GB,扩展分区 5GB，分为两个逻辑分区,大小分别为 3GB 和 2GB； 无法分主分区(大小不够)

（4）根据“拓扑结构图”和自行规划的“表 1-4”和“表 1-5”所示内容为 PC-A 物理主机及三台虚拟机配置正确的 IP 地址、子网掩码、网关和 DNS，将 PC-A 物理主机的 IP 地址配置界面截图保存，在 Windows 系统中使用 ipconfig/all 将显示所有结果的界面截图保存。


Win2003-A1 [正在运行] - Oracle VM VirtualBox
控制 视图 设备 帮助
安全配置向导
我的文档
我的电脑
网上邻居
Internet Explorer
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [版本 5.2.3790]
(C) 版权所有 1985-2003 Microsoft Corp.
C:\Documents and Settings\Administrator>ipconfig /all
Windows IP Configuration
Host Name . . . . . : web
Primary Dns Suffix . . . . . :
Node Type . . . . . : Unknown
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
Ethernet adapter 本地连接:
Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Physical Address. . . . . : 08-00-27-3C-E5-14
DHCP Enabled. . . . . : No
IP Address. . . . . : 10.100.100.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.100.100.254
DNS Servers . . . . . : 10.100.100.3
C:\Documents and Settings\Administrator>


Win2003-A2 [正在运行] - Oracle VM VirtualBox
控制 视图 设备 帮助
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>ipconfig /all
Windows IP Configuration
Host Name . . . . . : web2
Primary Dns Suffix . . . . . :
Node Type . . . . . : Unknown
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
Ethernet adapter 本地连接:
Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Physical Address. . . . . : 08-00-27-A6-B3-05
DHCP Enabled. . . . . : No
IP Address. . . . . : 10.100.100.111
Subnet Mask . . . . . : 255.255.255.0
IP Address. . . . . : 10.100.100.2
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.100.100.254
DNS Servers . . . . . : 10.100.100.3
C:\Documents and Settings\Administrator>

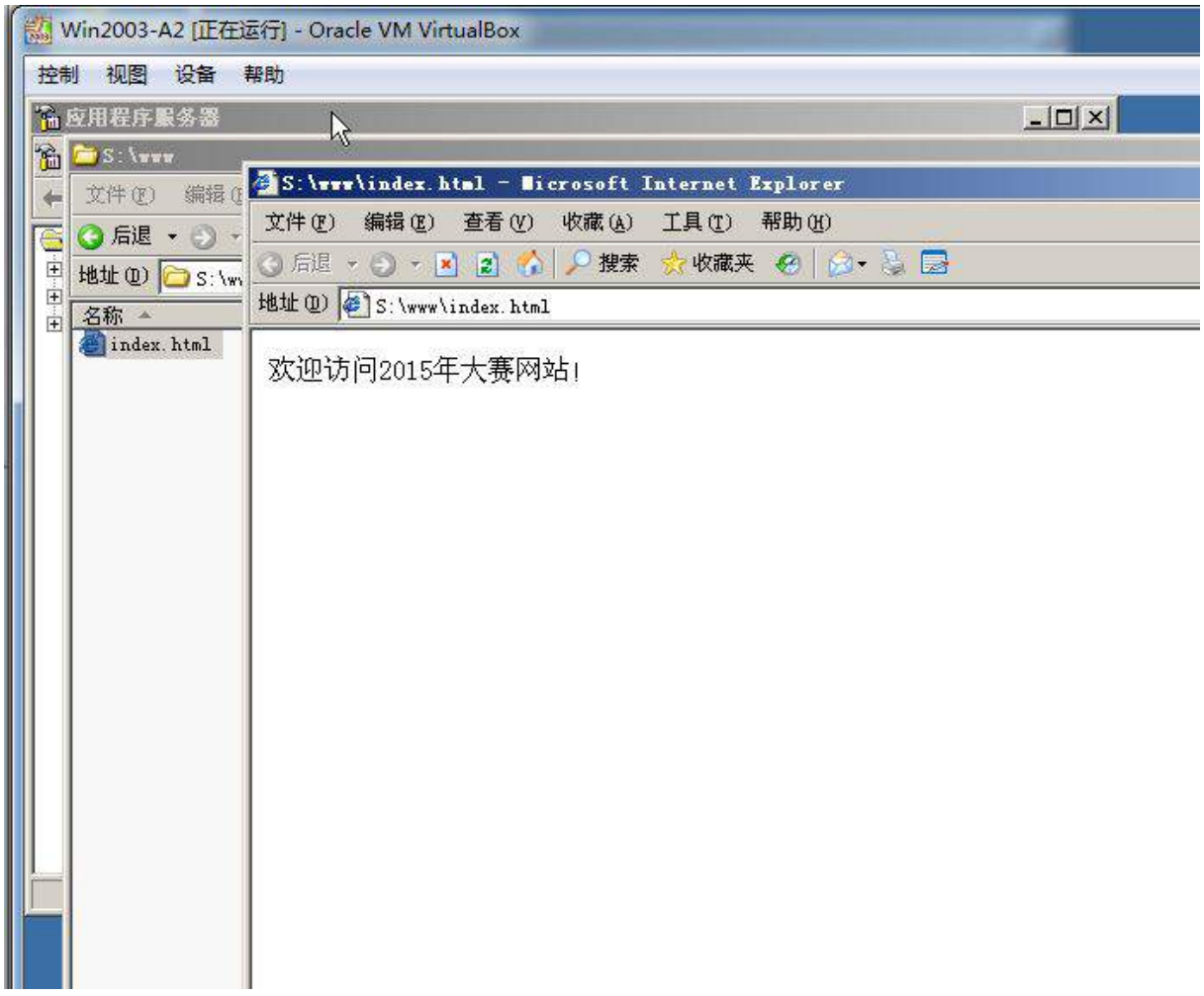


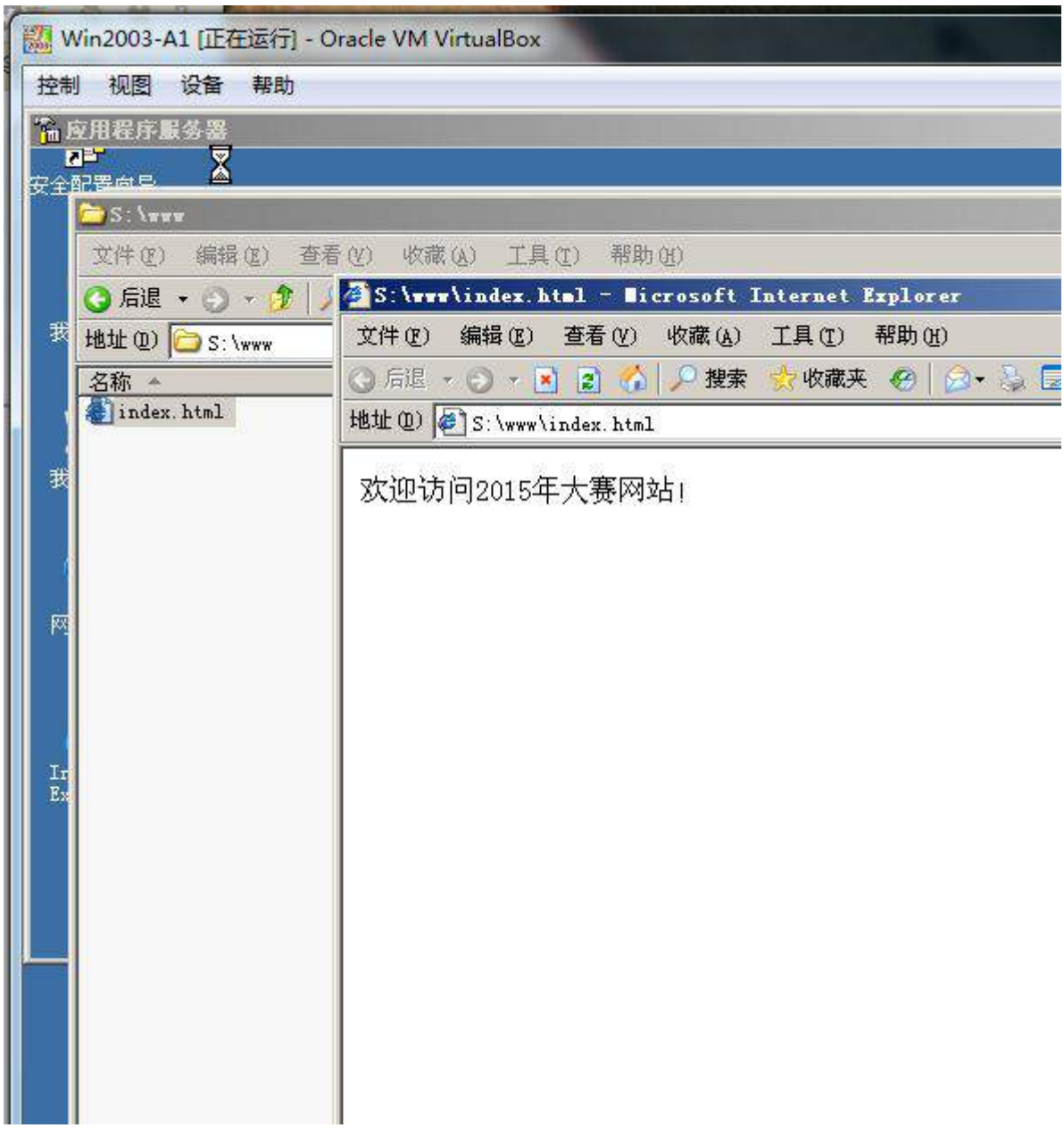
2. 在主机 PC-A 中部署 WEB 服务器应用

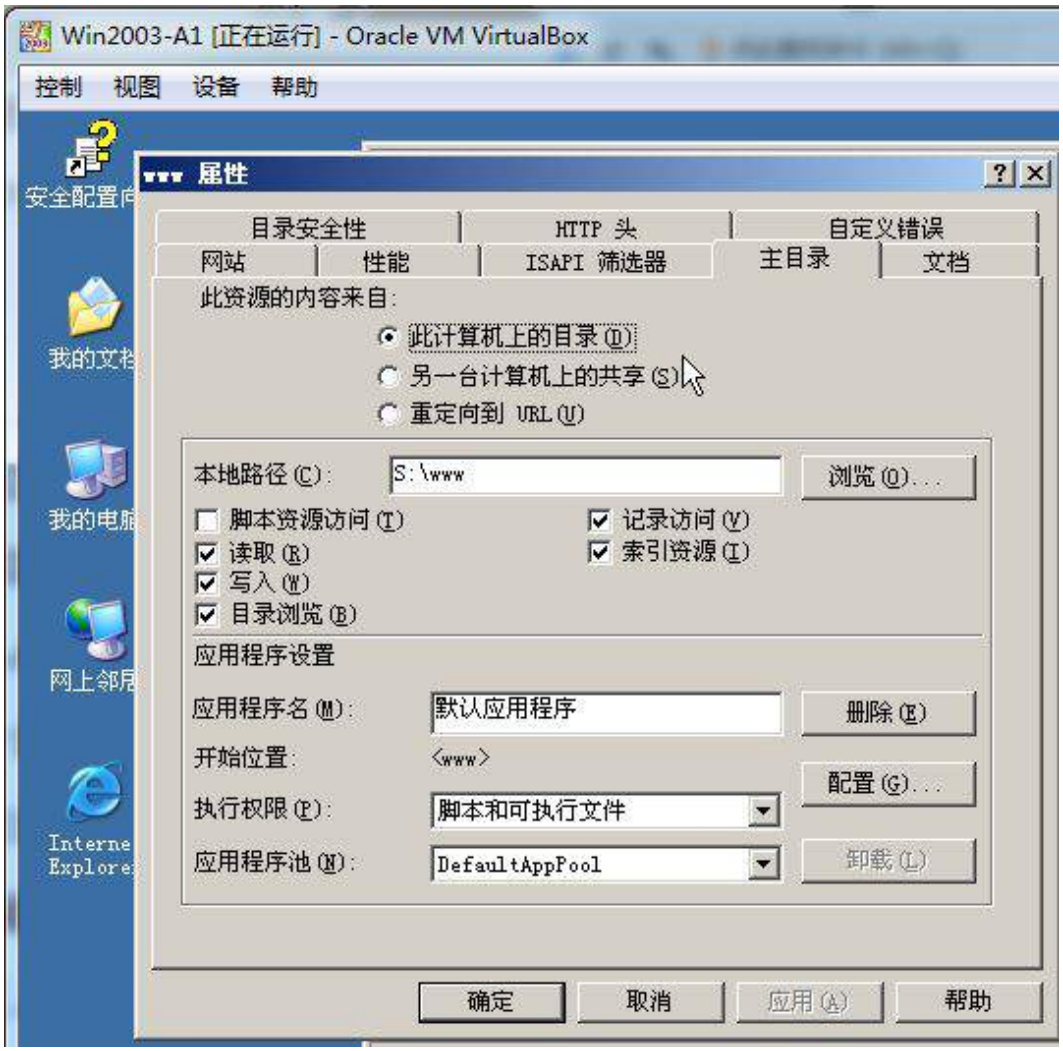
为了满足公司发布一些新闻、公司介绍、经营项目、技术支持等信息的需要，需要搭建一个公司网站，给用户提供一个了解公司信息和网上开展业务的一个平台。

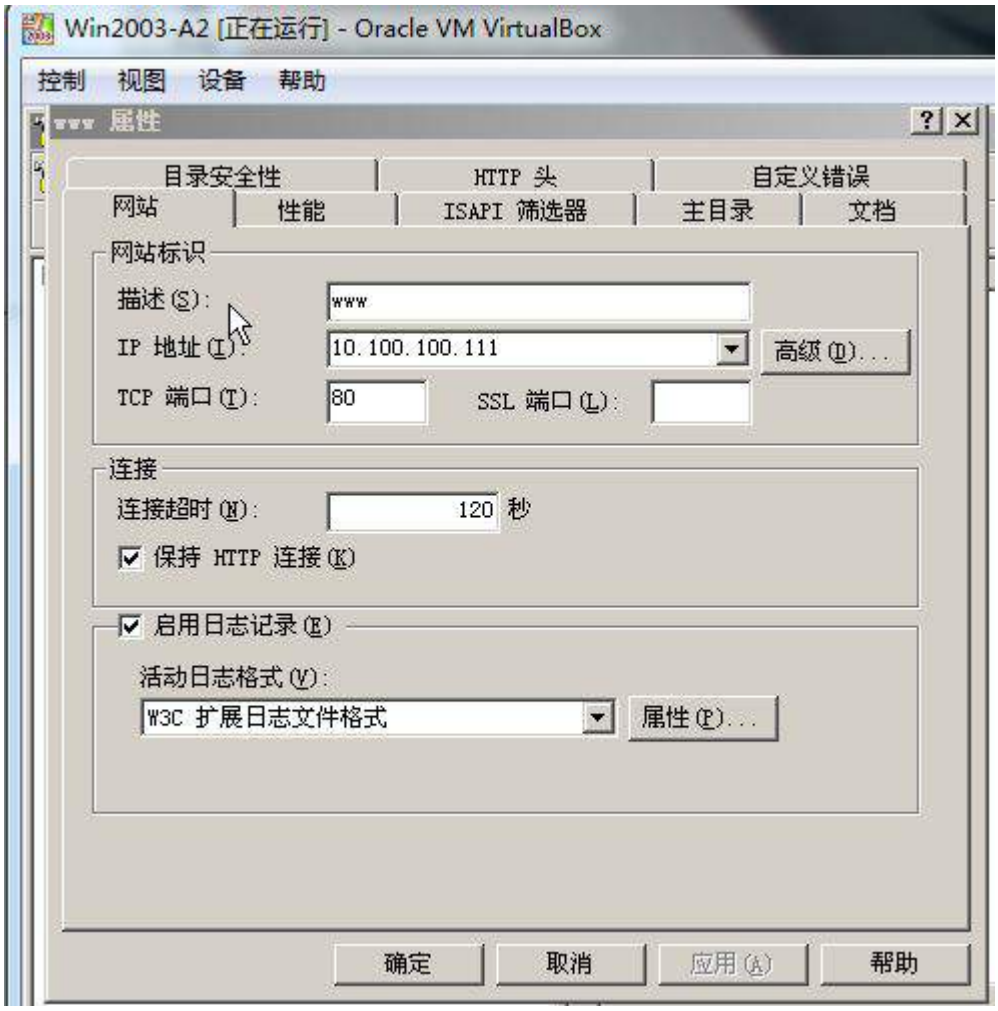
（1）在 PC-A 中 Win2003-A1 和 Win2003-A2 两个虚拟机系统中，分别使用 IIS 启用 WEB 服务，建立网站 IP 地址为群集公共 IP 地址（参考表 1-5 规划），TCP 端口号为 80，网站主目录的本地路径为 S:\www。要求网站主页文档为 index.html，其内容为“欢迎访问 2015 年大赛网站!”将配置对话框分别截图保存，在 PC-A 物理机的 Windows 7 系统中使用 IE 浏览器通过域名访问该站点主页，将浏览器窗口截图保存；

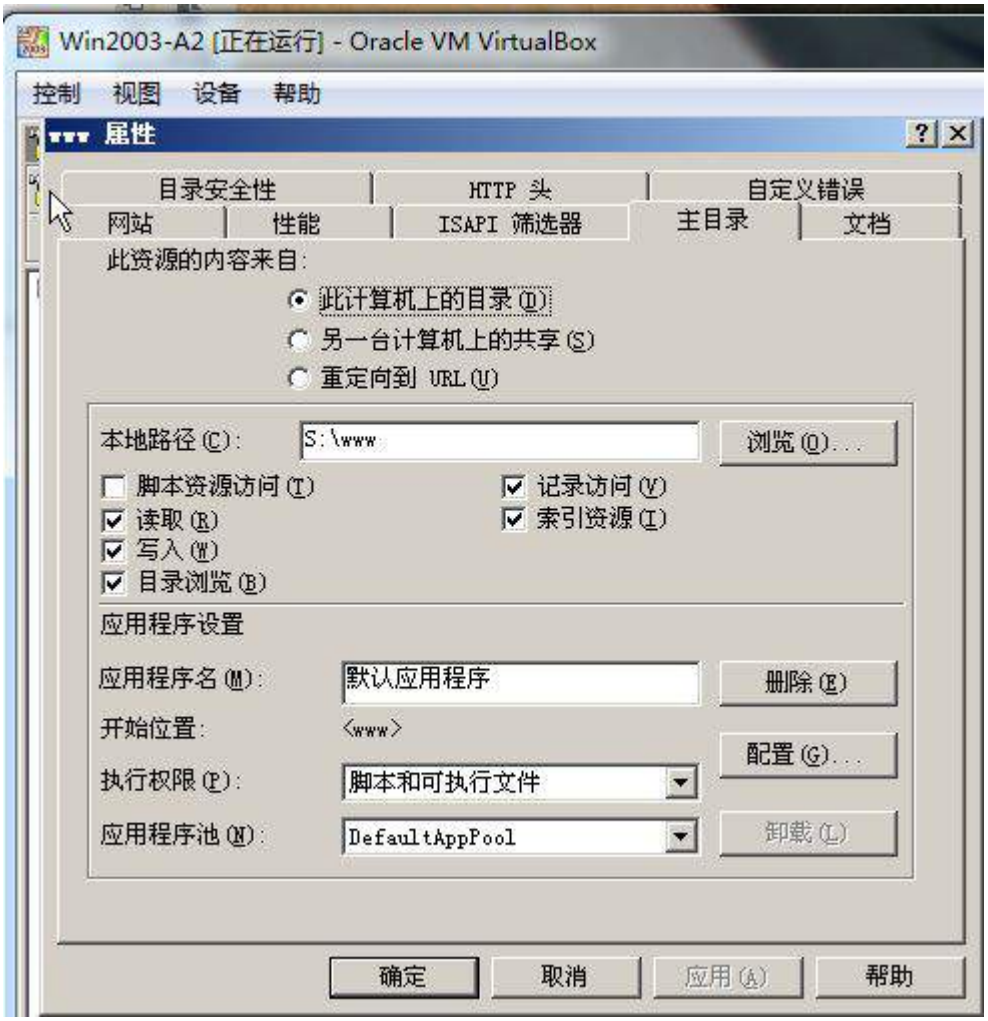

网络负载平衡管理器
文件(F) 群集(C) 主机(O) 选项(P) 帮助(H)
网络负载平衡群集
www.tj.com (10.100.100.111)
WEB(本地连接)
WEB2(本地连接)
在群集 www.tj.com (10.100.100.111) 的主机配置信息
主机(接口) 状态 专用 IP 地址
WEB(本地连接) 已聚合 10.100.100.1
WEB2(本地连接) 已聚合 10.100.100.2
群集 属性
群集参数 群集 IP 地址 端口规则
定义的端口规则(D):
群集 IP 地址 开始 结束 协议 模式 优... 加载 相似性
所有 80 80 两者 多重 -- 相等 单一
添加(A)... 编辑(E)... 删除(R)
端口规则描述
日志项目 日期 时间
0001 2016-6-3 9:28:
0002 2016-6-3 9:28:

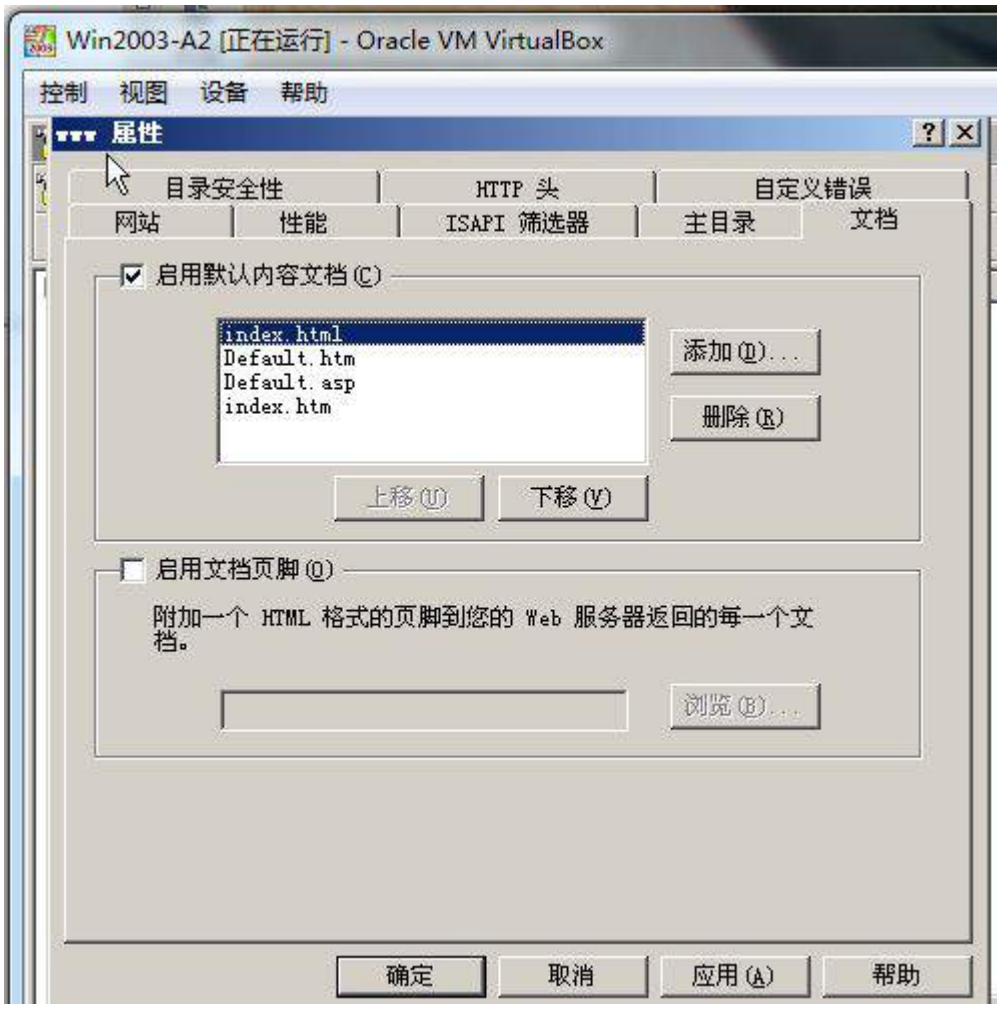

Win2003-A2 [正在运行] - Oracle VM VirtualBox
控制 视图 设备 帮助
应用程序服务器
S:\www
S:\www\index.html - Microsoft Internet Explorer
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
后退 搜索 收藏夹
地址(D) S:\www\index.html
名称
index.html
欢迎访问2015年大赛网站!

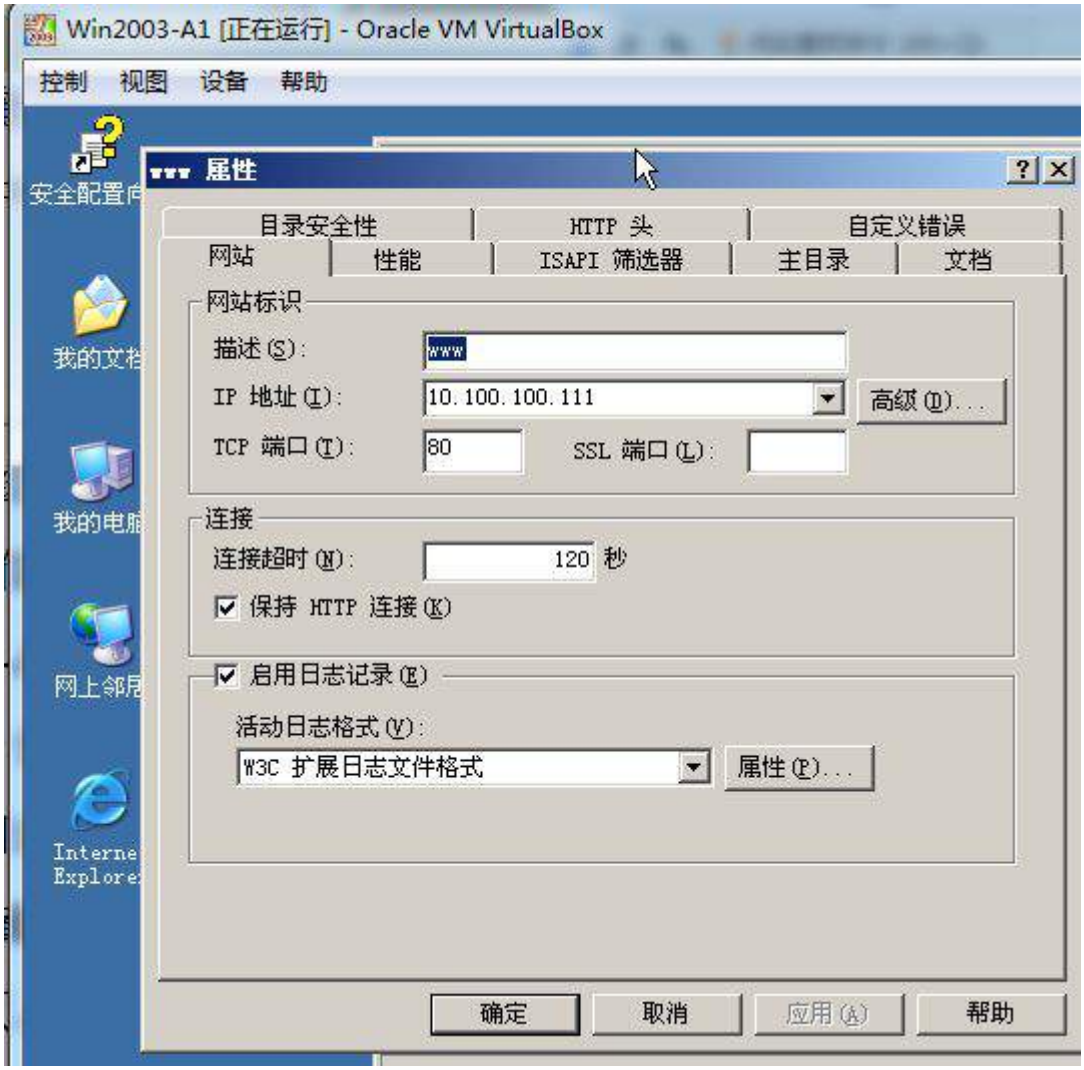

Win2003-A1 [正在运行] - Oracle VM VirtualBox
控制 视图 设备 帮助
应用程序服务器
S:\www
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
后退
地址(D) S:\www
名称
index.html
S:\www\index.html - Microsoft Internet Explorer
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
后退 搜索 收藏夹
地址(D) S:\www\index.html
欢迎访问2015年大赛网站!

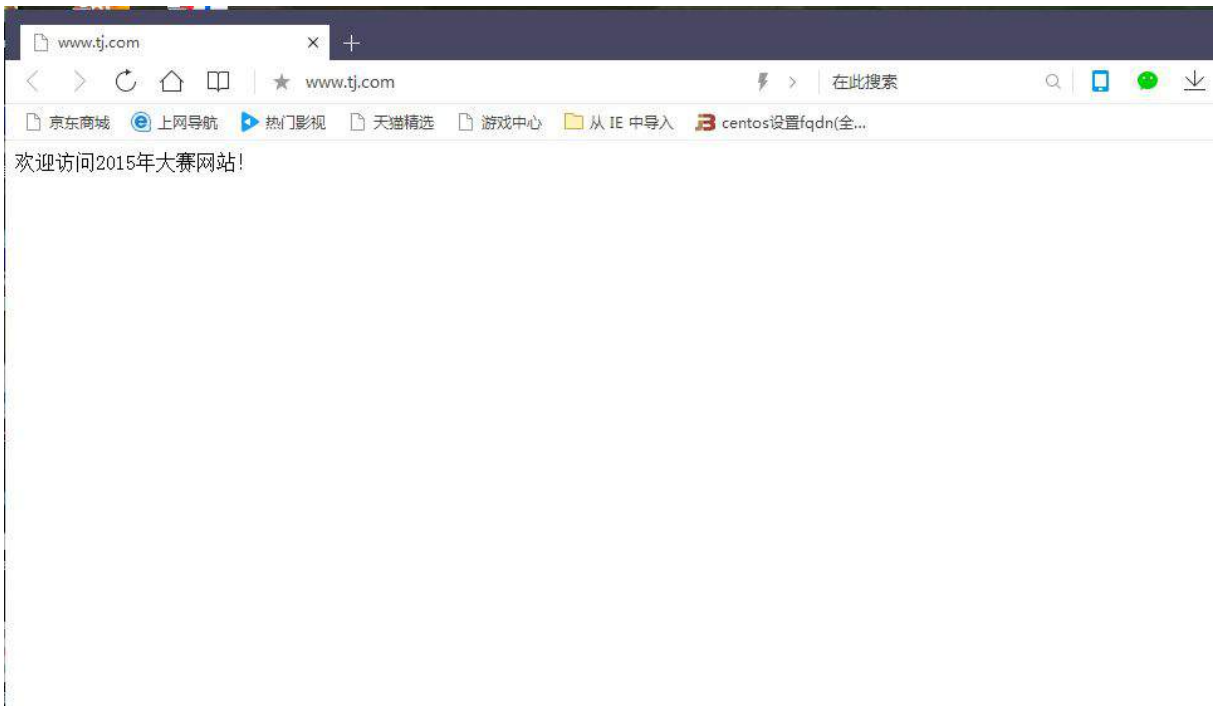

Win2003-A1 [正在运行] - Oracle VM VirtualBox
控制 视图 设备 帮助
属性
目录安全性
HTTP 头
自定义错误
网站
性能
ISAPI 筛选器
主目录
文档
此资源的内容来自:
此计算机上的目录(D)
另一台计算机上的共享(S)
重定向到 URL(U)
本地路径(C):
S:\www
浏览(O)...
脚本资源访问(T)
记录访问(V)
读取(R)
索引资源(I)
写入(W)
目录浏览(B)
应用程序设置
应用程序名(M):
默认应用程序
删除(E)
开始位置:
<www>
配置(G)...
执行权限(P):
脚本和可执行文件
应用程序池(N):
DefaultAppPool
卸载(L)
确定
取消
应用(A)
帮助


Win2003-A2 [正在运行] - Oracle VM VirtualBox
控制 视图 设备 帮助
属性
目录安全性
HTTP 头
自定义错误
网站
性能
ISAPI 筛选器
主目录
文档
网站标识
描述(S):
www
IP 地址(I):
10.100.100.111
高级(D)...
TCP 端口(T):
80
SSL 端口(L):
连接
连接超时(N):
120
秒
保持 HTTP 连接(K)
启用日志记录(E)
活动日志格式(V):
W3C 扩展日志文件格式
属性(P)...
确定
取消
应用(A)
帮助


Win2003-A2 [正在运行] - Oracle VM VirtualBox
控制 视图 设备 帮助
属性
目录安全性
HTTP 头
自定义错误
网站
性能
ISAPI 筛选器
主目录
文档
此资源的内容来自:
此计算机上的目录(D)
另一台计算机上的共享(S)
重定向到 URL(U)
本地路径(C):
S:\www
浏览(O)...
脚本资源访问(T)
记录访问(V)
读取(R)
索引资源(I)
写入(W)
目录浏览(B)
应用程序设置
应用程序名(M):
默认应用程序
删除(E)
开始位置:
<www>
配置(G)...
执行权限(P):
脚本和可执行文件
应用程序池(N):
DefaultAppPool
卸载(L)
确定
取消
应用(A)
帮助


Win2003-A2 [正在运行] - Oracle VM VirtualBox
控制 视图 设备 帮助
属性
目录安全性
HTTP 头
自定义错误
网站
性能
ISAPI 筛选器
主目录
文档
启用默认内容文档(C)
index.html
Default.htm
Default.asp
index.htm
添加(D)...
删除(R)
上移(U)
下移(V)
启用文档页脚(O)
附加一个 HTML 格式的页脚到您的 Web 服务器返回的每一个文档。
浏览(B)...
确定
取消
应用(A)
帮助


Win2003-A1 [正在运行] - Oracle VM VirtualBox
控制 视图 设备 帮助
属性
目录安全性
HTTP 头
自定义错误
网站
性能
ISAPI 筛选器
主目录
文档
网站标识
描述(S):
www
IP 地址(I):
10.100.100.111
高级(D)...
TCP 端口(T):
80
SSL 端口(L):
连接
连接超时(N):
120
秒
保持 HTTP 连接(K)
启用日志记录(E)
活动日志格式(V):
W3C 扩展日志文件格式
属性(P)...
确定
取消
应用(A)
帮助


www.tj.com
www.tj.com
在此搜索
京东商城
上网导航
热门影视
天猫精选
游戏中心
从 IE 中导入
centos设置fqdn(全...
欢迎访问2015年大赛网站!

（2）为保证服务器的性能，要求限制网站使用的最大带宽为 1024KB/s，网站最大连接限制为 1000。将配置对话框分别截图保存；

（3）要求服务器启用日志功能，记录每天的访问日志，以时间作为文件名，日志目录为 C:\www\log 日志文件只记录以下信息：客户端 IP 地址及用户名、服务器 IP 地址及端口、服务名、URI 资源及查询、发送与接收的字节数及所用时间。将配置对话框截图保存。

3．在 Windows 2003-A1 配置 CA 证书(30 分)

为了保证内部网站 web.tj.com 安全，总公司用户与内部网站 WEB 服务器建立加密通信。

（1）在 Win2003-A1 系统中安装证书 CA 服务；

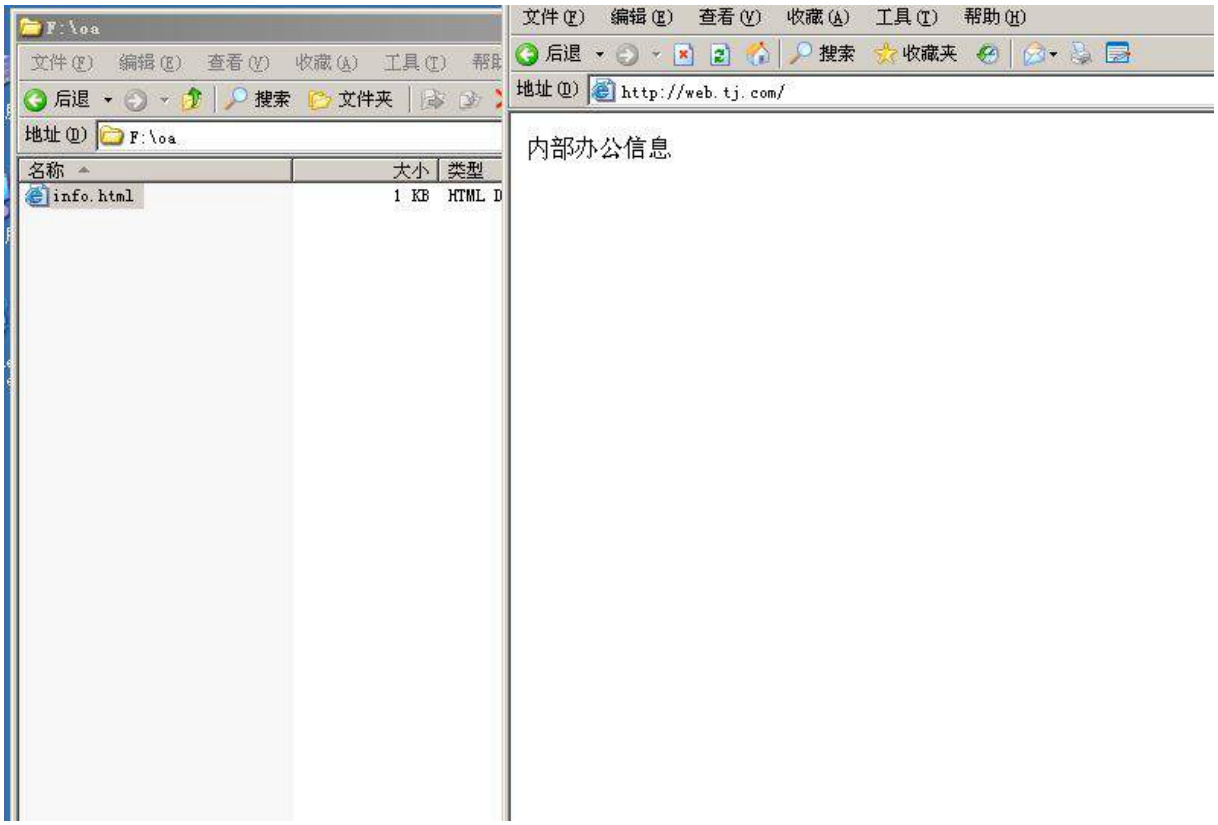
①CA 类型选择“独立根 CA”；将配置界面截图保存；

②CA 的公用名称使用“TJ-CA”；将配置界面截图保存；

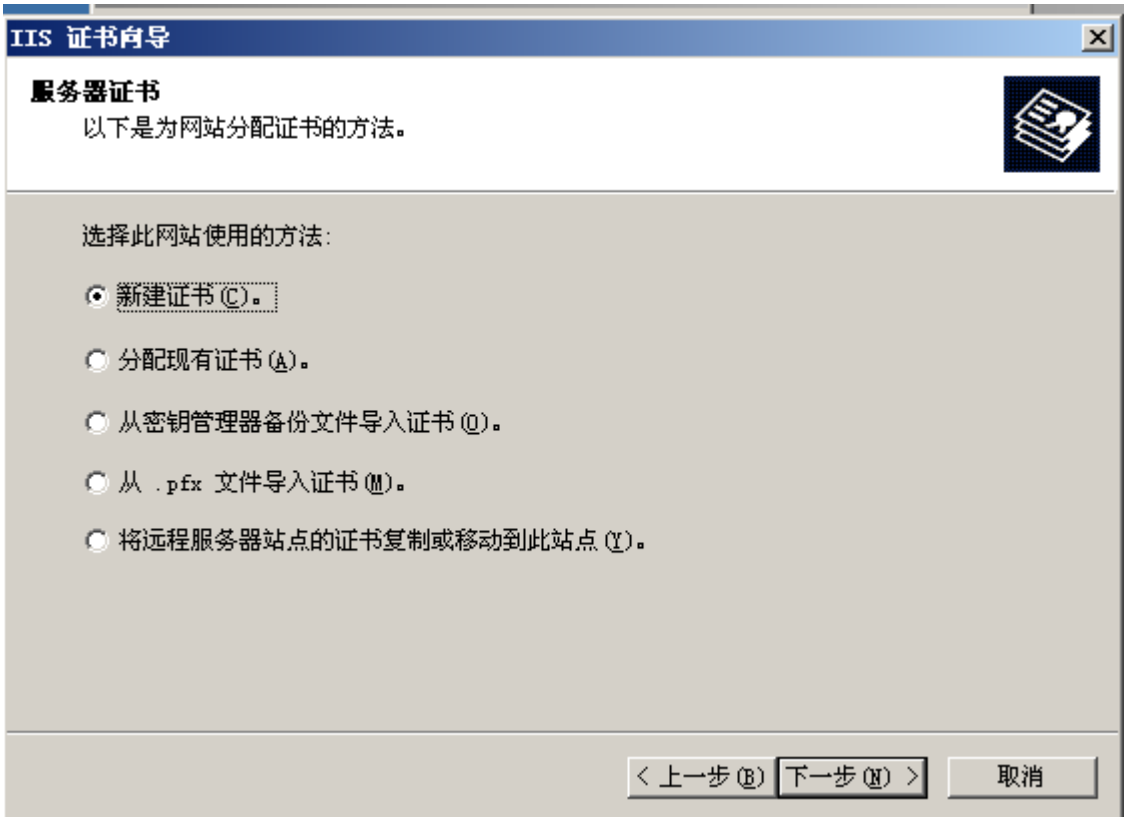
③安装完毕后，启动证书服务。

（2）为 WEB 站点申请和颁发证书；

在 Win2003-A1 服务器上再搭建一个内部网站，IP 地址为（参考表 1-5 规划），域名为 web.tj.com，主目录的本地路径为 F:\oa，网站主页文档为 info.html，其内容为“内部办公信息”，并为“web.tj.com”申请和颁发 CA 服务证书，实现 WEB 站点的 SSL 加密功能（SSL 端口号为 443），要求：



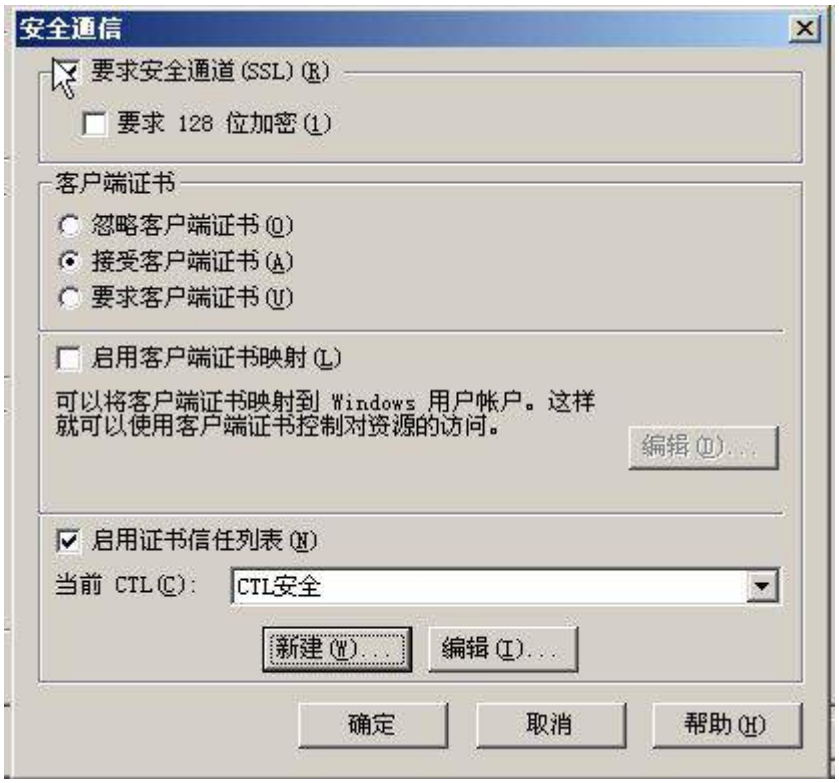
①服务器证书采用新建证书方式为网站分配证书；



②证书名称为：bangong，单位为 tianjing，部门为 OA，公用名称为 TJ-OA，将证书请求提交的结果对话框截图保存；

③安全通信要求开启 SSL 安全通道，客户端证书采用接受客户端证书，选择 CA 证

书添加至 CTL 中的证书，名称为 CTL 安全，将安全通信对话框截图保存

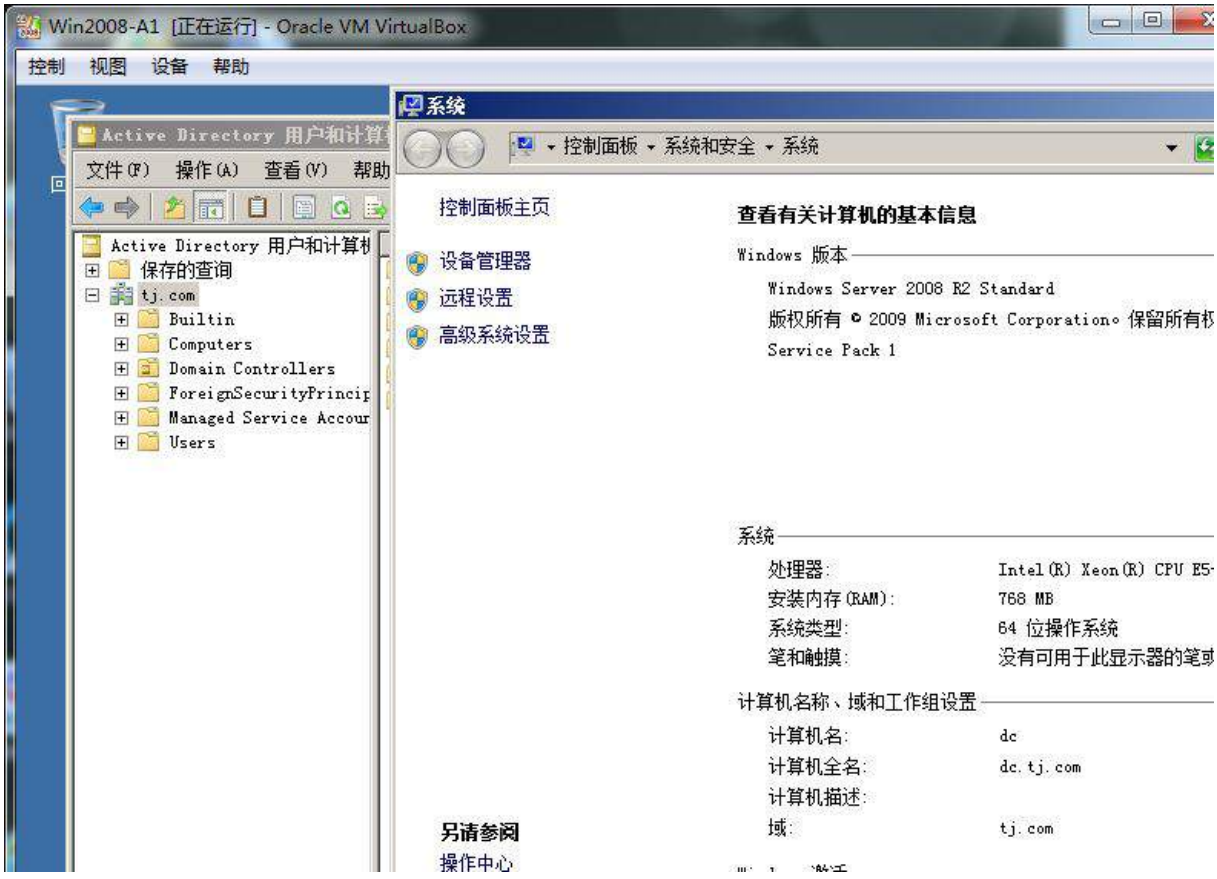


（3）申请并安装客户端证书；

在客户端 Client2 使用 https:// web.tj.com 访问内部网站首页。将访问结果界面截图保存。

4. 在主机 Win2008-A1 中完成 DC 域控制器的部署

（1）将此服务器升级为域控，DNS 域名解析服务由服务器 Win2003-A1 提供，域名为 tj.com；将截图粘贴到竞赛结果文件指定位置；

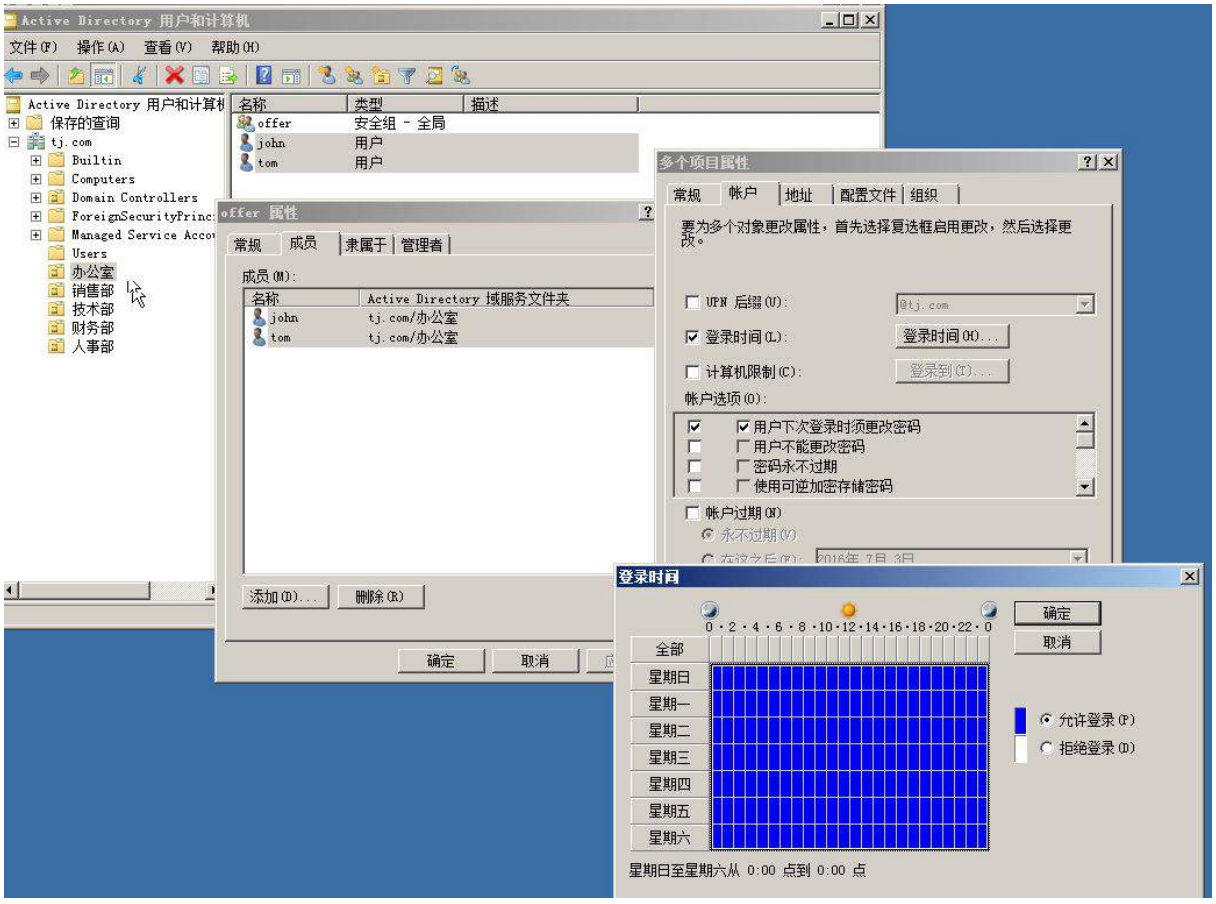


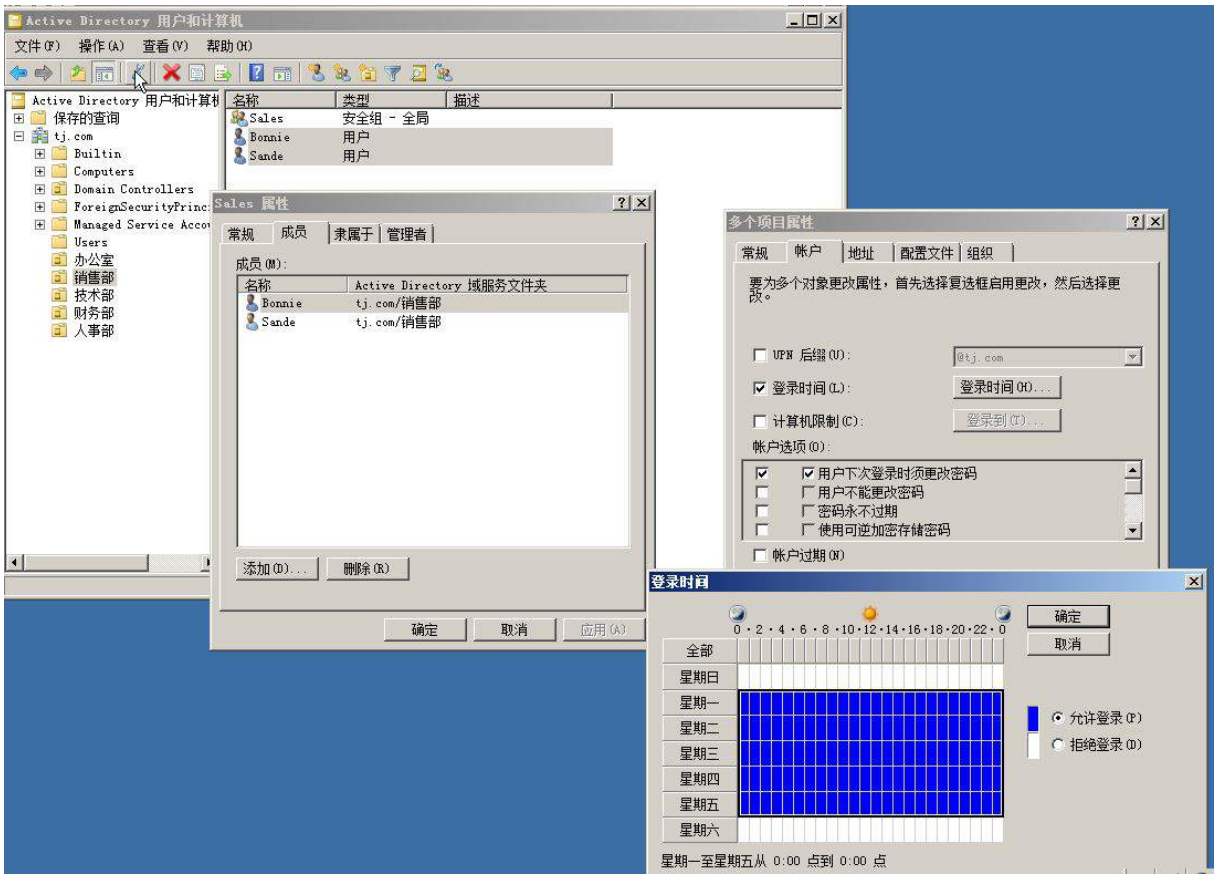
（2）创建组织单位和用户：在 dc.tj.com 域中创建 5 个组织单位、5 个全局组和 10 个域

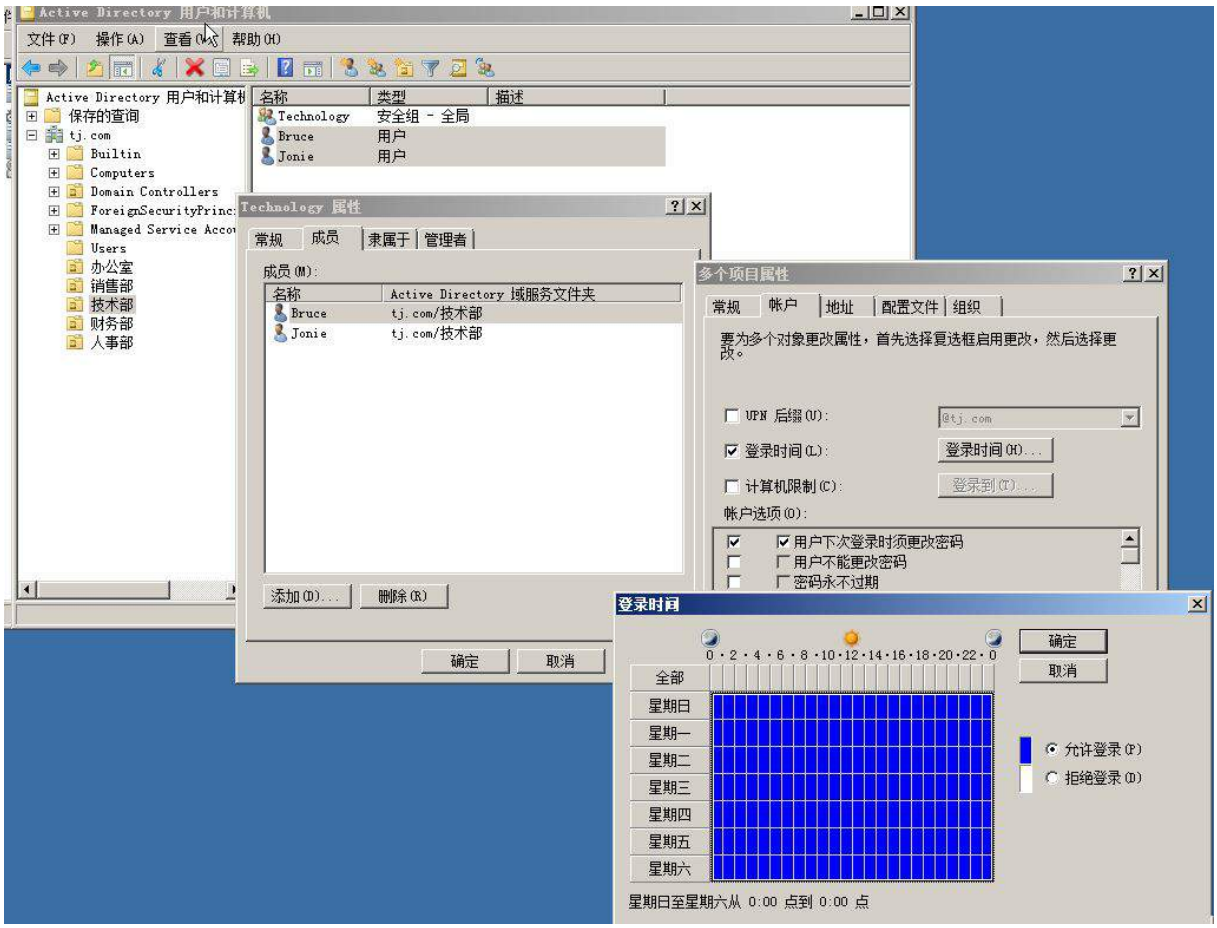
用户，域用户的初始密码为 User123，要求域用户在首次登录时更改密码，具体如下表 2-1 所示；

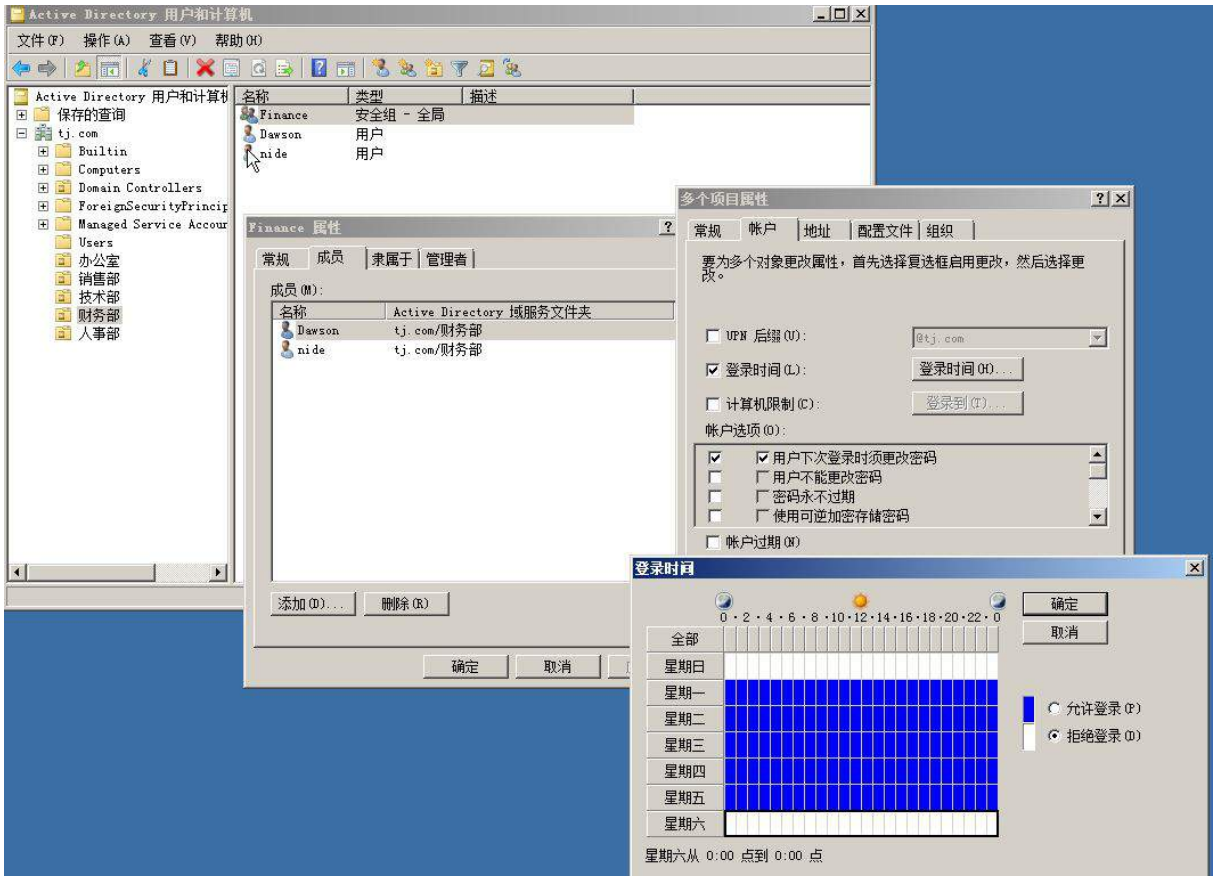
表 2-1 域用户信息表

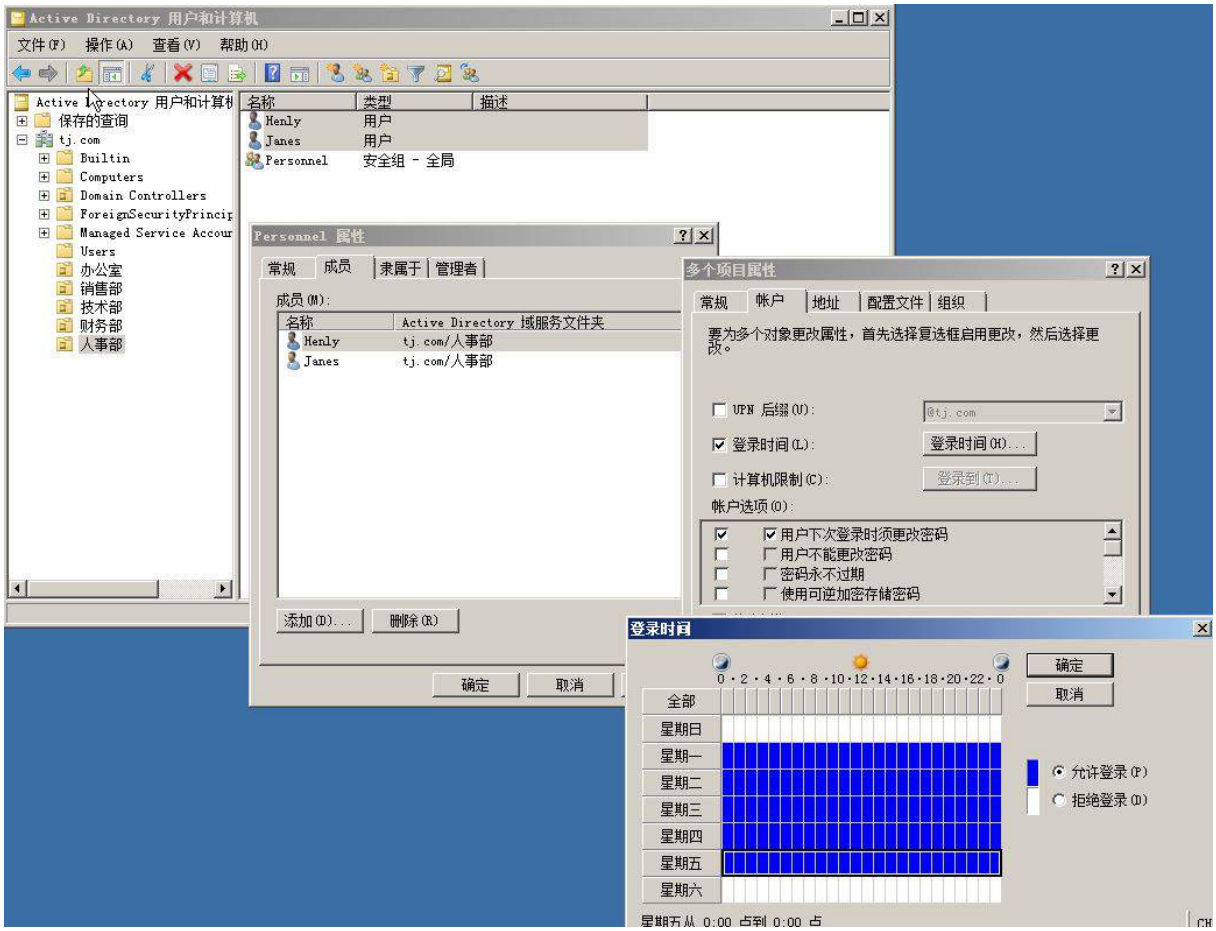
部门	组织单位	全局组	隶属用户	登录时间
办公室	办公室	offer	john、tom	全部
销售部	销售部	Sales	Bonnie、Sande	周一到周五
技术部	技术部	Technology	Jonie、Bruce	全部
财务部	财务部	Finance	nide、Dawson	周一到周五
人事部	人事部	Personnel	Janes、Henly	周一到周五




Active Directory 用户和计算机
文件(F) 操作(A) 查看(V) 帮助(H)
Active Directory 用户和计算机
保存的查询
tj.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrinc
Managed Service Accou
Users
办公室
销售部
技术部
财务部
人事部
名称 类型 描述
Sales 安全组 - 全局
Bonnie 用户
Sande 用户
Sales 属性
常规 成员 隶属于 管理者
成员(M):
名称 Active Directory 域服务文件夹
Bonnie tj.com/销售部
Sande tj.com/销售部
添加(D)... 删除(R)
确定 取消 应用(A)
多个项目属性
常规 帐户 地址 配置文件 组织
要为多个对象更改属性，首先选择复选框启用更改，然后选择更改。
UPN 后缀(U):
登录时间(L):
登录时间(H)...
计算机限制(C):
登录到(T)...
帐户选项(O):
用户下次登录时须更改密码
用户不能更改密码
密码永不过期
使用可逆加密存储密码
帐户过期(N)
登录时间
0 · 2 · 4 · 6 · 8 · 10 · 12 · 14 · 16 · 18 · 20 · 22 · 0
全部
星期日
星期一
星期二
星期三
星期四
星期五
星期六
确定
取消
允许登录(P)
拒绝登录(D)
星期一至星期五从 0:00 点到 0:00 点


Active Directory 用户和计算机
文件(F) 操作(A) 查看(V) 帮助(H)
Active Directory 用户和计算机
保存的查询
tj.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrinc
Managed Service Accou
Users
办公室
销售部
技术部
财务部
人事部
名称 类型 描述
Technology 安全组 - 全局
Bruce 用户
Jonie 用户
Technology 属性
常规 成员 隶属于 管理者
成员(M):
名称 Active Directory 域服务文件夹
Bruce tj.com/技术部
Jonie tj.com/技术部
添加(D)... 删除(R)
确定 取消
多个项目属性
常规 帐户 地址 配置文件 组织
要为多个对象更改属性，首先选择复选框启用更改，然后选择更改。
UPN 后缀(U):
登录时间(L):
登录时间(H)...
计算机限制(C):
登录到(T)...
帐户选项(O):
用户下次登录时须更改密码
用户不能更改密码
密码永不过期
登录时间
0 · 2 · 4 · 6 · 8 · 10 · 12 · 14 · 16 · 18 · 20 · 22 · 0
全部
星期日
星期一
星期二
星期三
星期四
星期五
星期六
确定
取消
允许登录(P)
拒绝登录(D)
星期日至星期六从 0:00 点到 0:00 点





（3）为了减轻管理负担，委派用户 Jonie 组织单元“技术部”有新建删除用户和组的权

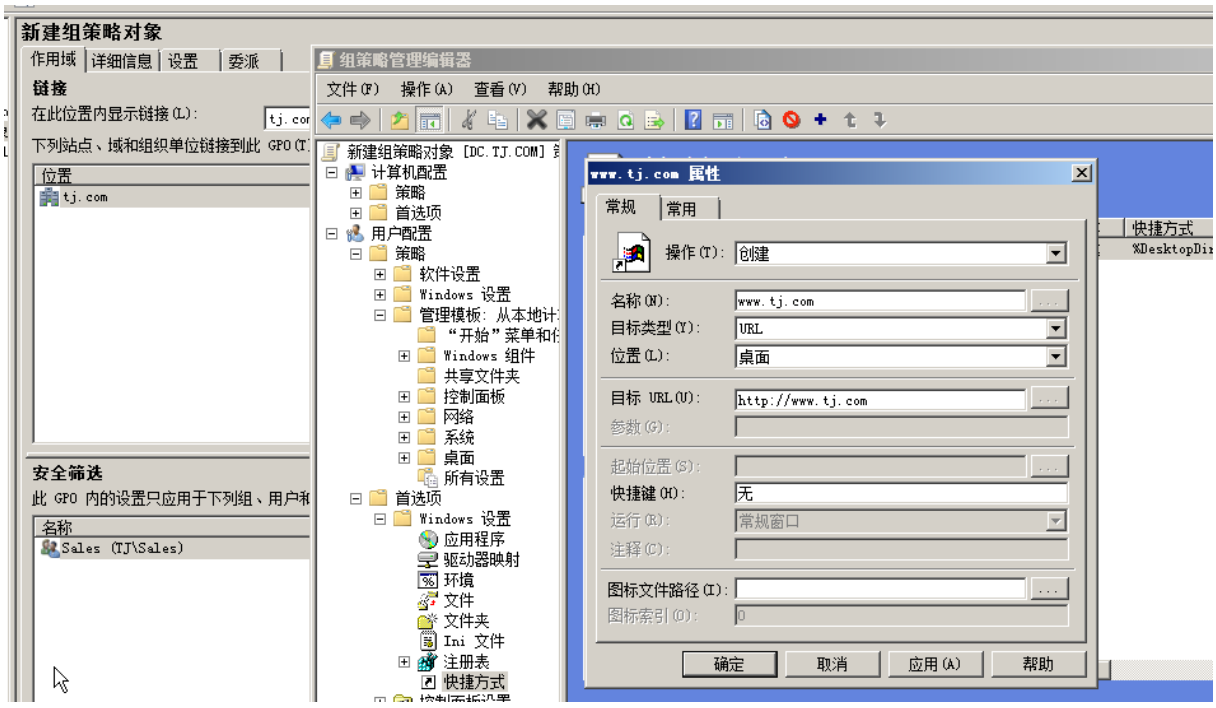
限；

（4）配置组策略：

①每个组织用户只能在周一至周五 8:00-17:30 登录；

②让 Bruce 在域中的任何一台计算机上都可以实现相同的桌面；

③当市场部用户登录时，自动在登入的计算机桌面上建立一个 www.tj.com 网址快捷方式，但不应用于技术部和财务部用户；



④配置域安全策略，账户锁定阈值为 4 次，如果超过此阈值该账号将被锁定的时间为 60 分钟；

（5）当在域中新建用户时，root@tj.com 给自己发送一封电子邮件，内容为：“域中有新用户建立。”；

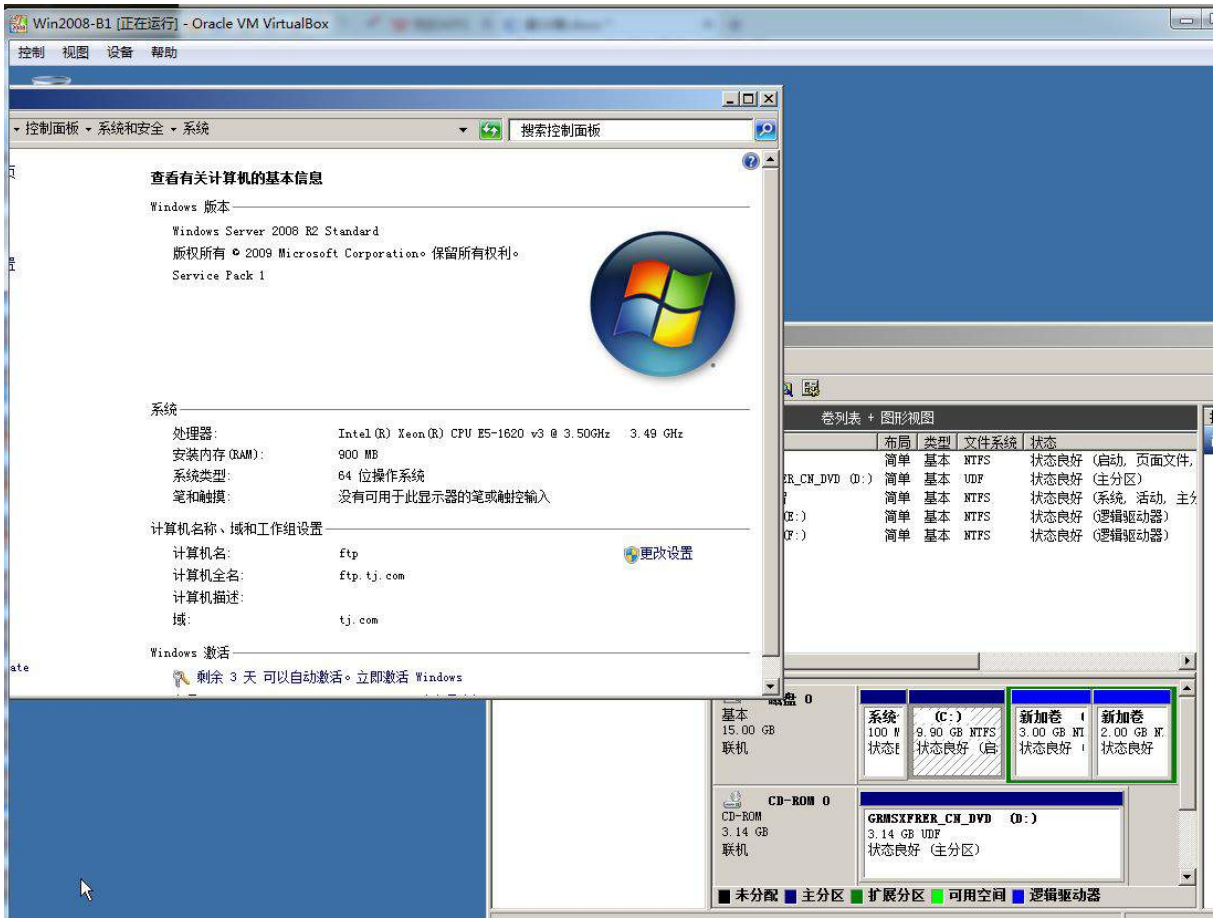
（6）安装 IIS 服务，配置 IIS，以使访问者在浏览器中输入 tj.com，也可以正确访问到 Win2008-A1 上的 www.tj.com；

（7）将上面所有配置点截图粘贴到竞赛结果文件指定位置。

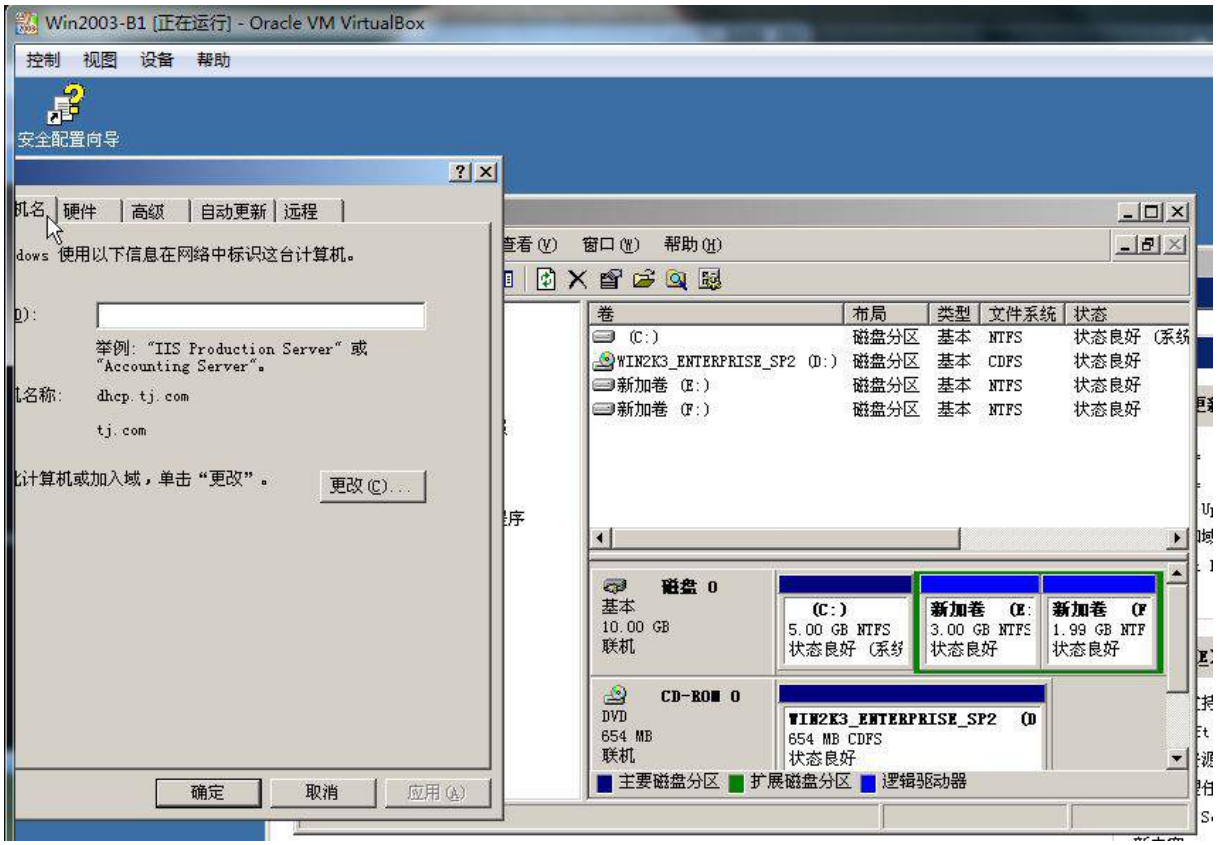
二、在 PC-B 上完成如下操作

1、完成虚拟主机的创建

（1）创建虚拟机 Win2008-B1,具体要求为内存 900MB,硬盘 15GB；主分区 10GB,扩展分区 5GB,并将主机加入到 tj.com 域，分为两个逻辑分区,大小分别为 3GB 和 2GB；

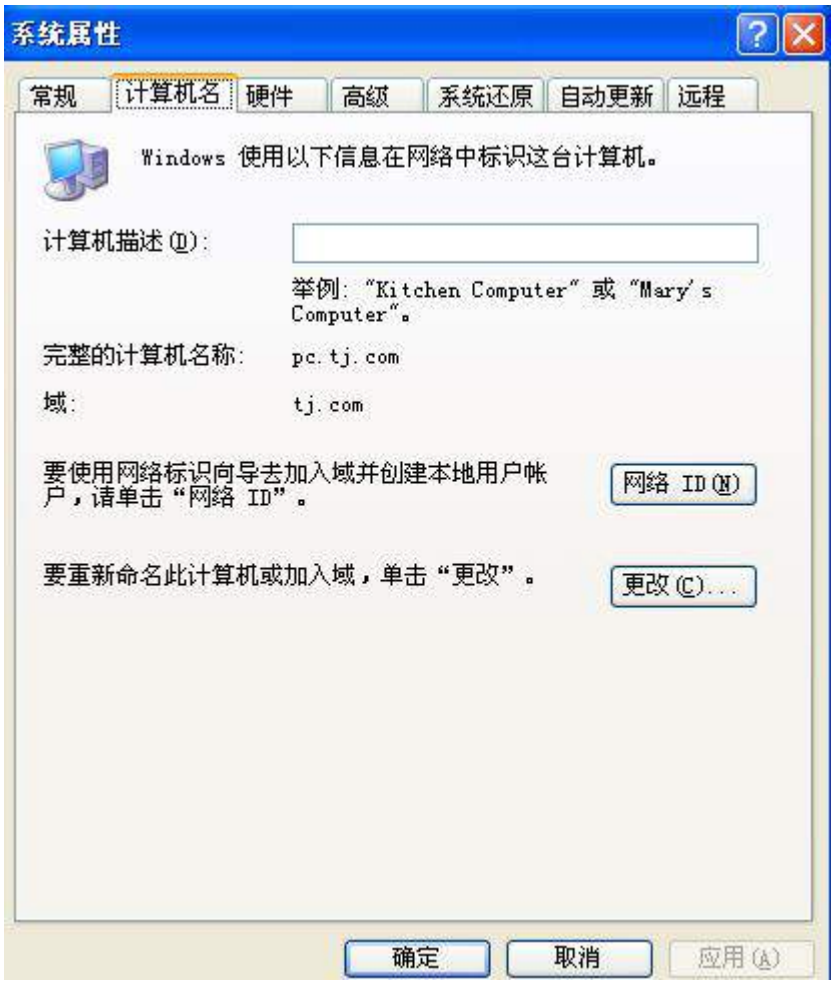


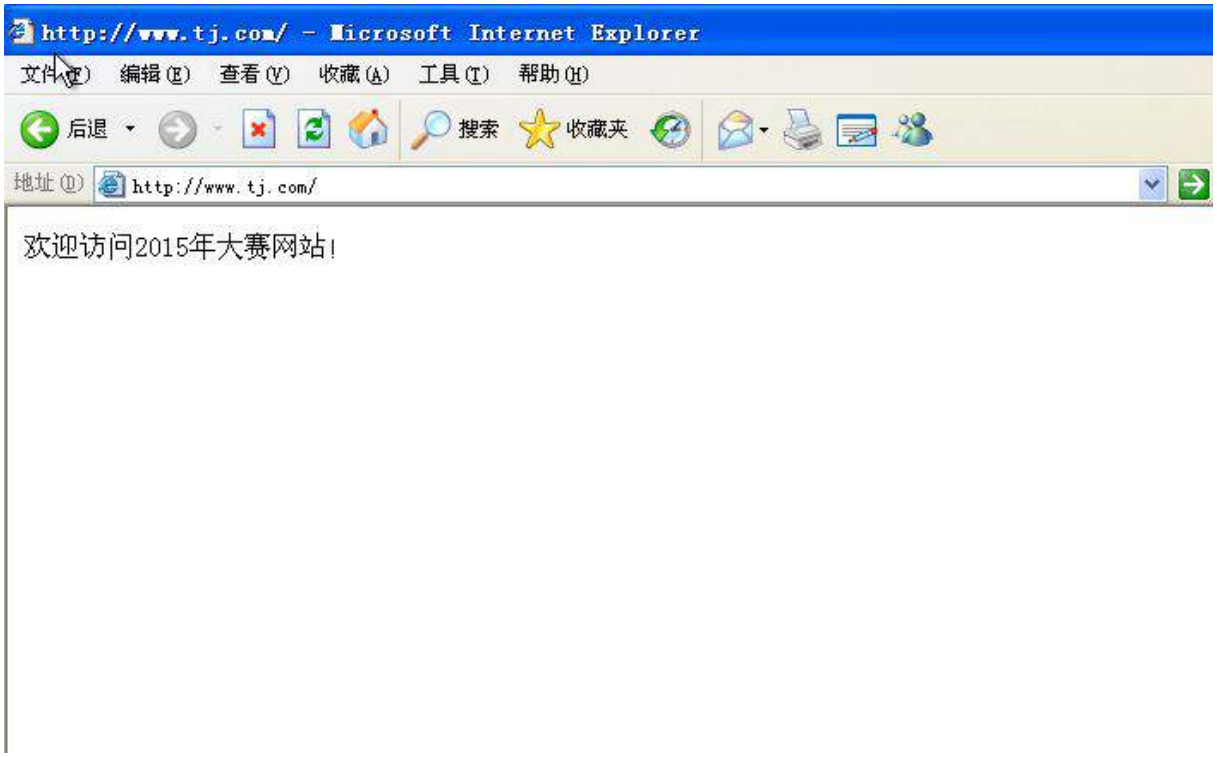
（2）创建虚拟机 Win2003-B1,具体要求为内存 512MB,硬盘 10GB,主分区 5GB,扩展分区 5GB,分为两个逻辑分区,大小分别为 3GB 和 2GB；并将主机加入到 tj.com 域；



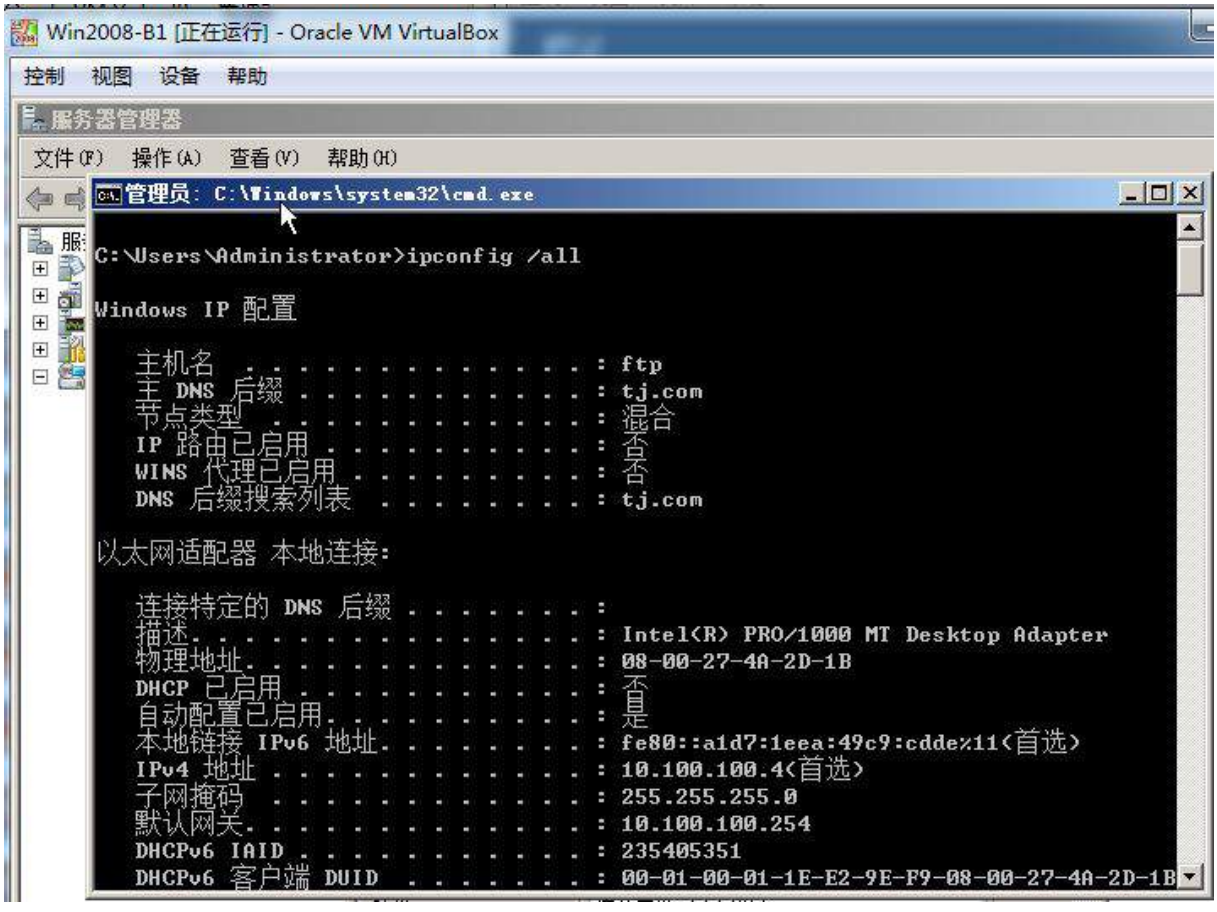
（3）在 PC-B 上，使用虚拟机安装 Windows XP 操作系统，设备名为 PC-B，其内存为 512M，硬盘 10G，将计算机加入到域中，其合法域名为 pc.tj.com，ip 地址为（参见 IP 地址分配表 1-5 自行规划内容）。检测是否正常访问 www.tj.com；

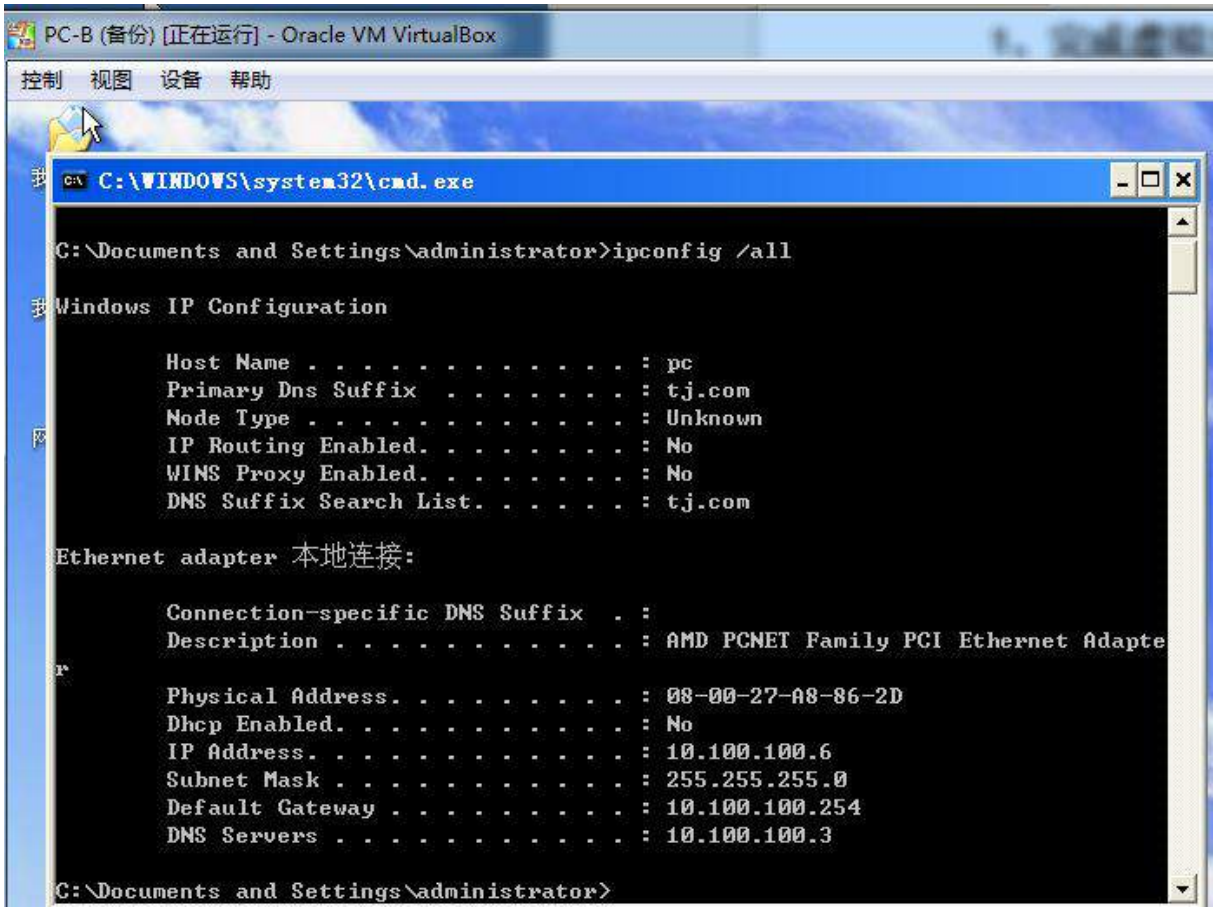

常规
名称: PC-B
操作系统: Windows XP (64 bit)
编组: 新编组
预览
PC-B
系统
内存大小: 512 MB
启动顺序: 软驱, 光驱, 硬盘
硬件加速: VT-x/AMD-V, 嵌套分页
显示
显存大小: 18 MB
远程桌面服务器: 已禁用
录像: 已禁用
存储
控制器: IDE
第一IDE控制器主通道: Windows XP.vdi (普通, 10.00 GB)
第二IDE控制器主通道: [光驱] windows_xp_sp3.iso (601.04 MB)
声音
主机音频驱动: Windows DirectSound
控制芯片: ICH AC97
网络
网卡 1: PCnet-PCI II (桥接网络, Intel(R) Ethernet Connection I217-LM)

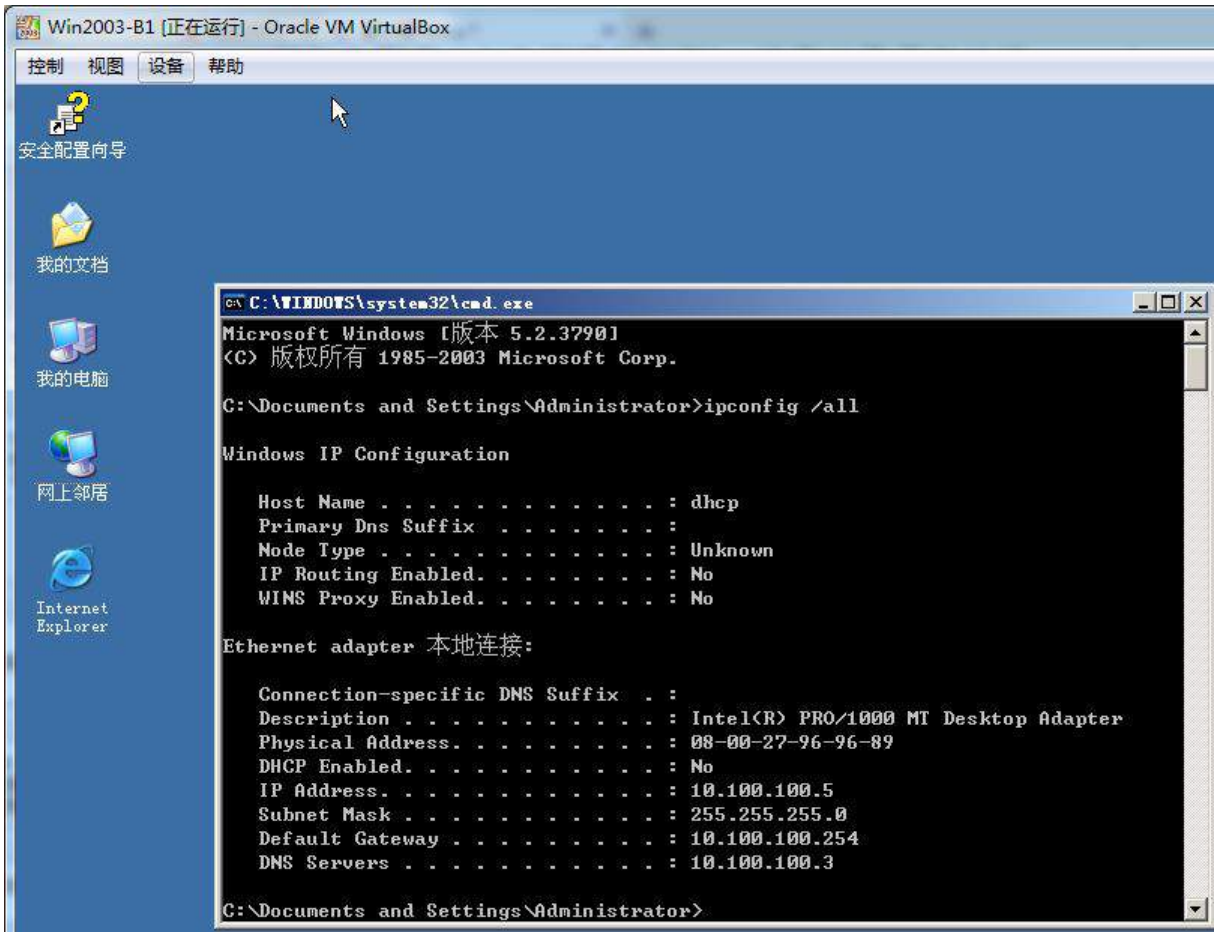

系统属性
常规
计算机名
硬件
高级
系统还原
自动更新
远程
Windows 使用以下信息在网络中标识这台计算机。
计算机描述(D):
举例: “Kitchen Computer” 或 “Mary's Computer”。
完整的计算机名称: pc.tj.com
域: tj.com
要使用网络标识向导去加入域并创建本地用户帐户，请单击“网络 ID”。
网络 ID(N)
要重新命名此计算机或加入域，单击“更改”。
更改(C)...
确定
取消
应用(A)



（4）根据拓扑结构图和网络系统规划表为 PC-B 物理主机及三台虚拟机配置正确的 IP 地址、子网掩码、网关和 DNS，将 PC-A 物理主机的 IP 地址配置界面截图保存，在 Windows 系统中使用 ipconfig/all 将显示所有结果的界面截图保存。



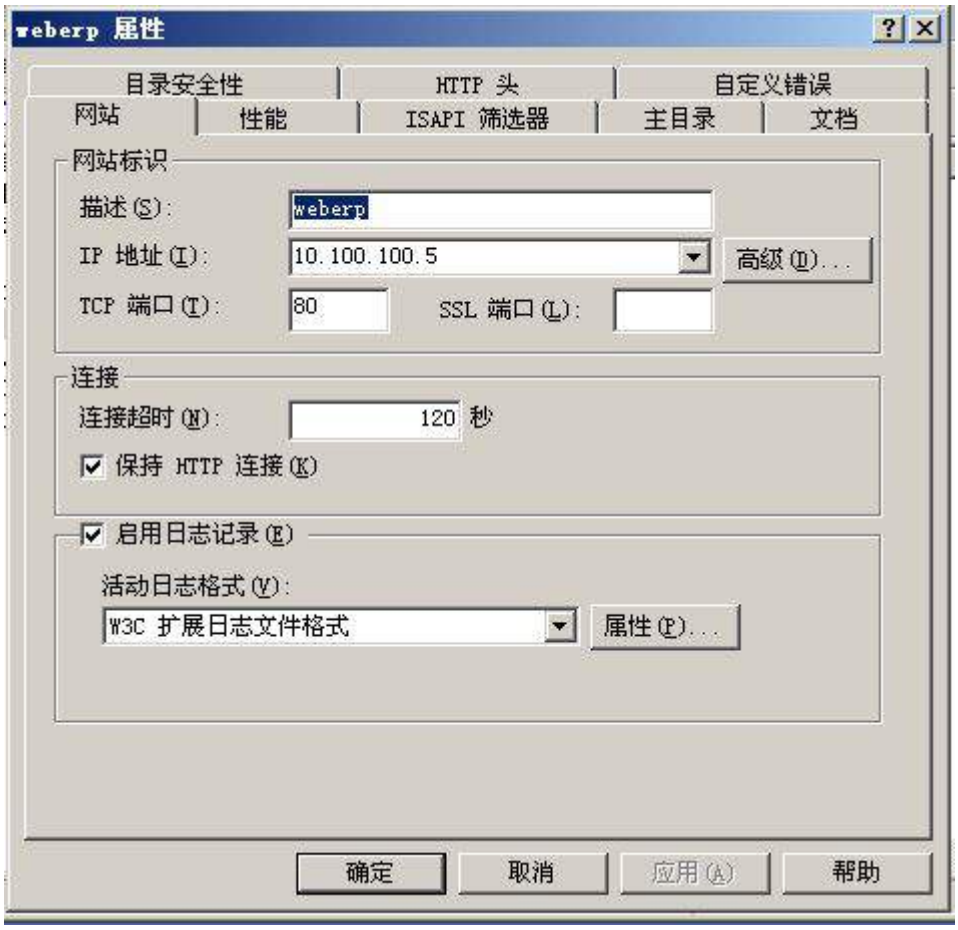

PC-B (备份) [正在运行] - Oracle VM VirtualBox
控制 视图 设备 帮助
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\administrator>ipconfig /all
Windows IP Configuration
Host Name . . . . . : pc
Primary Dns Suffix . . . . . : tj.com
Node Type . . . . . : Unknown
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : tj.com
Ethernet adapter 本地连接:
Connection-specific DNS Suffix . :
Description . . . . . : AMD PCNET Family PCI Ethernet Adapte
r
Physical Address. . . . . : 08-00-27-A8-86-2D
Dhcp Enabled. . . . . : No
IP Address. . . . . : 10.100.100.6
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.100.100.254
DNS Servers . . . . . : 10.100.100.3
C:\Documents and Settings\administrator>


Win2003-B1 [正在运行] - Oracle VM VirtualBox
控制 视图 设备 帮助
安全配置向导
我的文档
我的电脑
网上邻居
Internet Explorer
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [版本 5.2.3790]
(C) 版权所有 1985-2003 Microsoft Corp.
C:\Documents and Settings\Administrator>ipconfig /all
Windows IP Configuration
Host Name . . . . . : dhcp
Primary Dns Suffix . . . . . :
Node Type . . . . . : Unknown
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
Ethernet adapter 本地连接:
Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Physical Address. . . . . : 08-00-27-96-96-89
DHCP Enabled. . . . . : No
IP Address. . . . . : 10.100.100.5
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.100.100.254
DNS Servers . . . . . : 10.100.100.3
C:\Documents and Settings\Administrator>

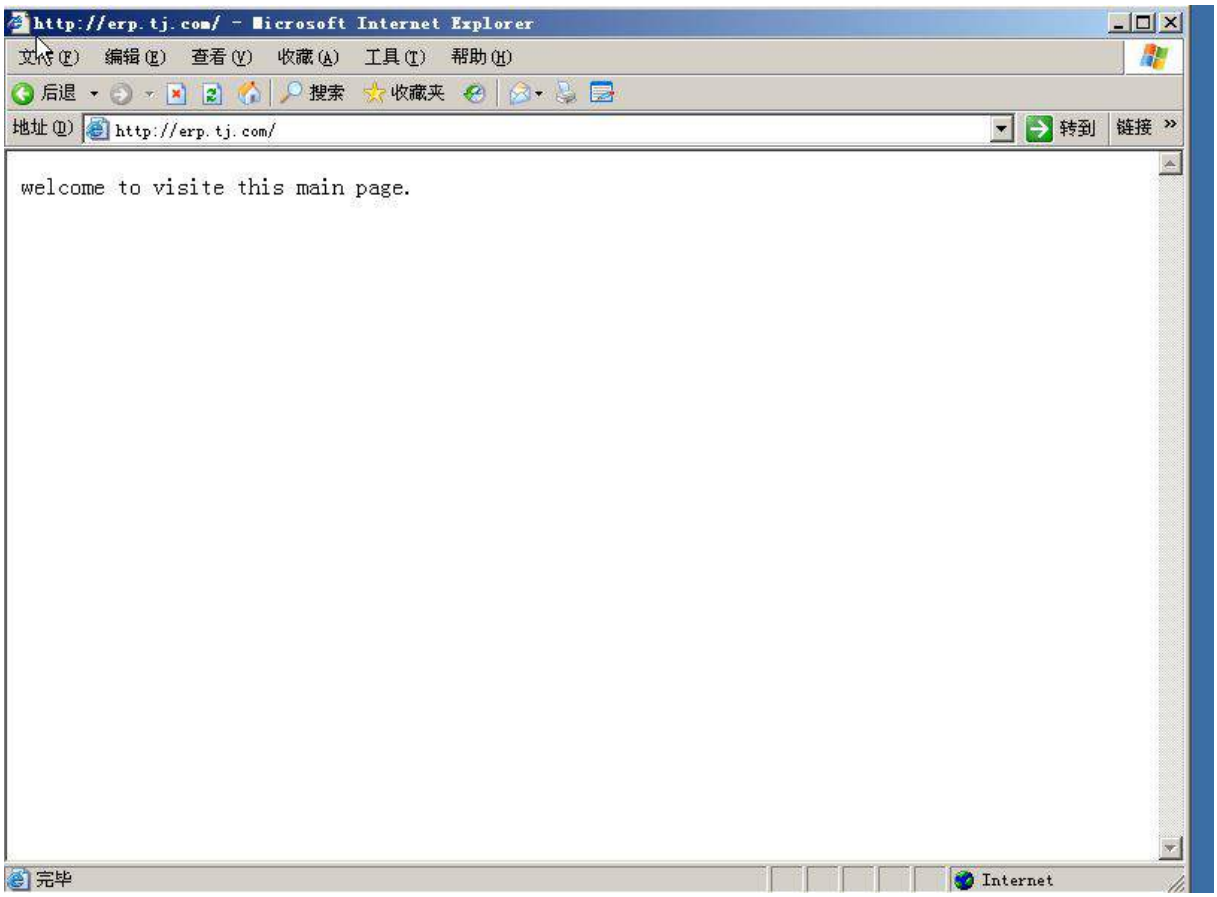
2. 在主机 Win2003-B1 中完成 Web 服务器以及 FTP 服务器的部署

（1）在此服务器中安装 IIS 以及 FTP 服务；

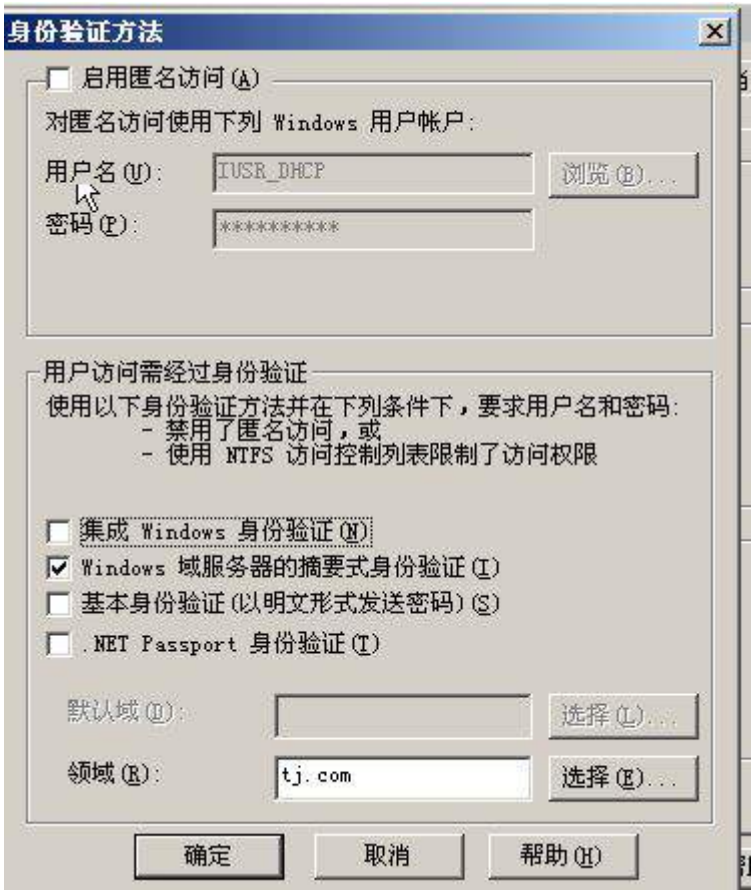
（2）配置 IIS 服务器，创建名为 weberp 的站点，主目录路径为 c:\weberp，并配置主机头 erp.tj.com 对应 IP 地址；此外，创建虚拟目录 web1，目录路径为 c:\web1，设置首页显示内容为”welcome to visit this main page.”；限制所有后缀为 linu.net 的主机均不能访问此网站；


weberp 属性
目录安全性
HTTP 头
自定义错误
网站
性能
ISAPI 筛选器
主目录
文档
网站标识
描述(S):
weberp
IP 地址(I):
10.100.100.5
高级(D)...
TCP 端口(T):
80
SSL 端口(L):
连接
连接超时(N):
120
秒
保持 HTTP 连接(K)
启用日志记录(E)
活动日志格式(V):
W3C 扩展日志文件格式
属性(P)...
确定
取消
应用(A)
帮助

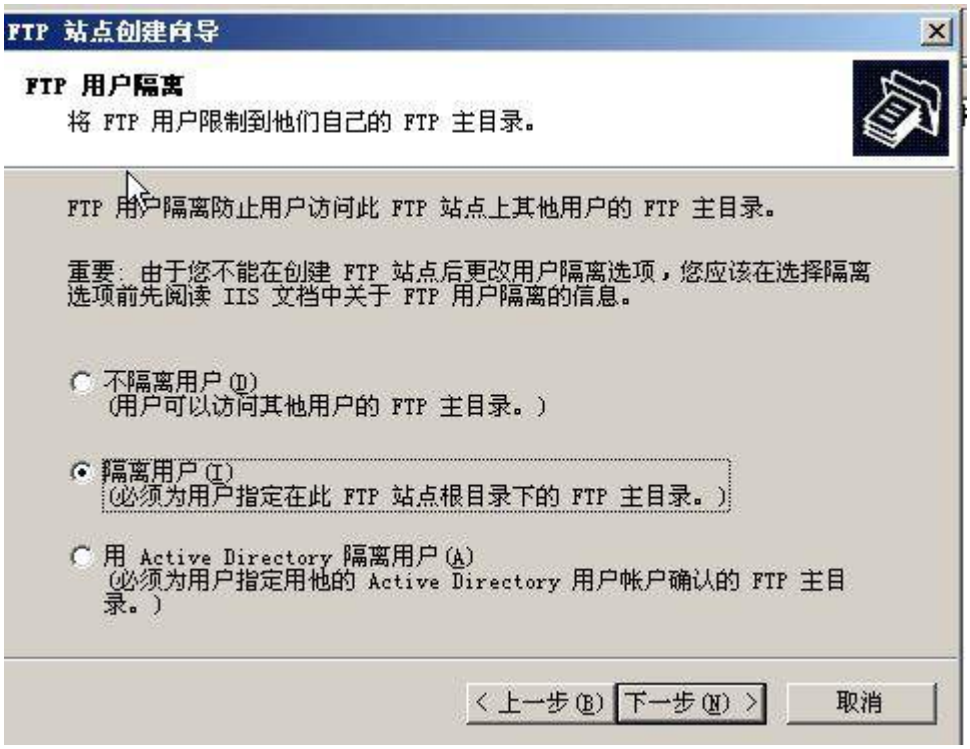

weberp 属性
目录安全性
HTTP 头
自定义错误
网站
性能
ISAPI 筛选器
主目录
文档
此资源的内容来自:
此计算机上的目录(D)
另一台计算机上的共享(S)
重定向到 URL(U)
本地路径(C):
C:\weberp
浏览(O)...
脚本资源访问(T)
记录访问(V)
读取(R)
索引资源(I)
写入(W)
目录浏览(B)
应用程序设置
应用程序名(M):
默认应用程序
删除(E)
开始位置:
<weberp>
配置(G)...
执行权限(P):
脚本和可执行文件
应用程序池(N):
DefaultAppPool
卸载(L)
确定
取消
应用(A)
帮助


http://erp.tj.com/ - Microsoft Internet Explorer
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
后退
搜索
收藏夹
地址(D) http://erp.tj.com/
转到
链接
welcome to visite this main page.
完毕
Internet

（3）设置网站应用摘要式身份验证方式，访问者必须输入的域用户和密码方可进行访问；



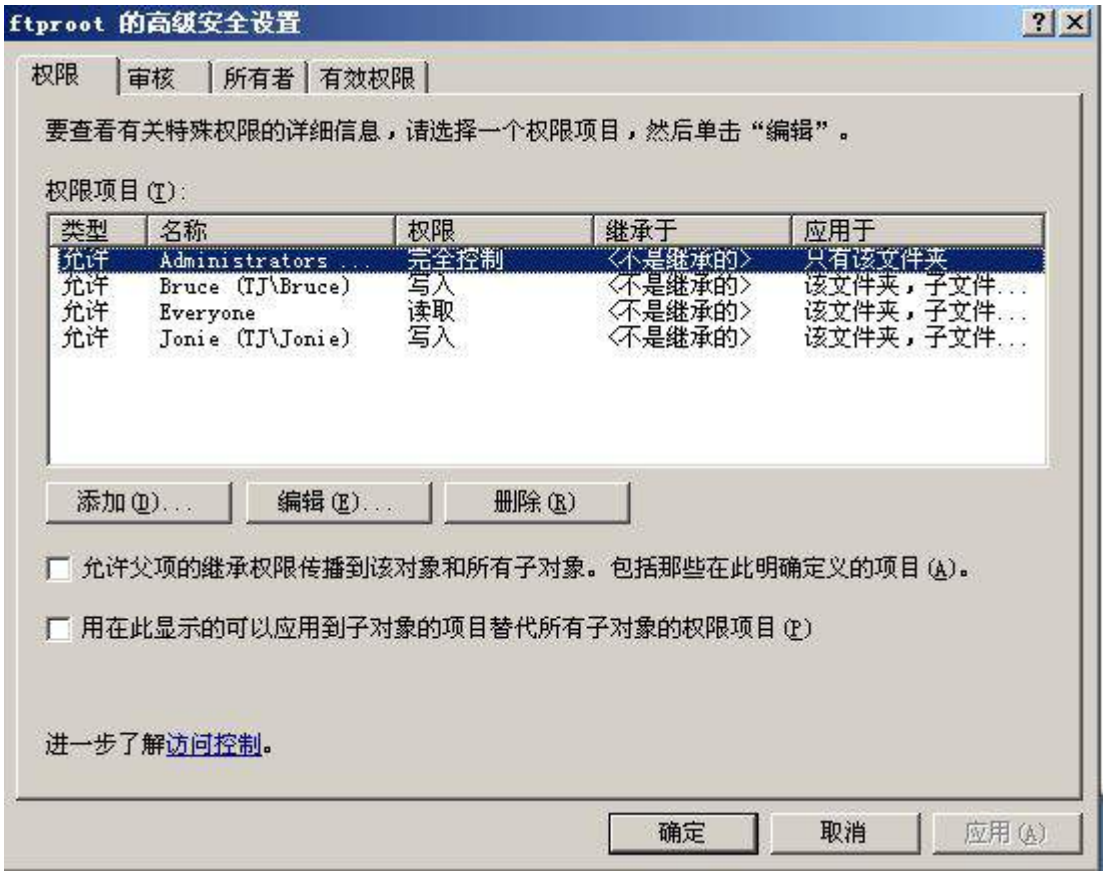
（4）以隔离用户方式创建名为 ftp.tj.com 的 FTP 站点，FTP 主目录路径为 c:\inetpub\ftproot；域用户及匿名用户均可登录，但匿名用户仅有只读权限，域用户 Jonie、Bruce 则能够完成读写操作；


FTP 站点创建向导
FTP 用户隔离
将 FTP 用户限制到他们自己的 FTP 主目录。
FTP 用户隔离防止用户访问此 FTP 站点上其他用户的 FTP 主目录。
重要：由于您不能在创建 FTP 站点后更改用户隔离选项，您应该在选择隔离选项前先阅读 IIS 文档中关于 FTP 用户隔离的信息。
不隔离用户(D)
(用户可以访问其他用户的 FTP 主目录。)
隔离用户(I)
(必须为用户指定在此 FTP 站点根目录下的 FTP 主目录。)
用 Active Directory 隔离用户(A)
(必须为用户指定用他的 Active Directory 用户帐户确认的 FTP 主目录。)
< 上一步(B)
下一步(N) >
取消


FTP 站点创建向导
FTP 站点描述
FTP 站点描述用于帮助管理员识别各个站点。
输入 FTP 站点的描述。
描述(D):
ftp.tj.com
< 上一步(B)
下一步(N) >
取消


FTP 站点创建向导
FTP 站点主目录
主目录是 FTP 内容子目录的根目录。
输入主目录的路径。
路径(P):
C:\Inetpub\ftproot
浏览(R)...
< 上一步(B)
下一步(N) >
取消


ftp.tj.com 属性
FTP 站点
安全帐户
消息
主目录
目录安全性
允许匿名连接(O)
对匿名访问使用下列 Windows 用户帐户:
用户名(U):
IUSR_DHCP
浏览(B)...
密码(P):
****
只允许匿名连接(L)
确定
取消
应用(A)
帮助

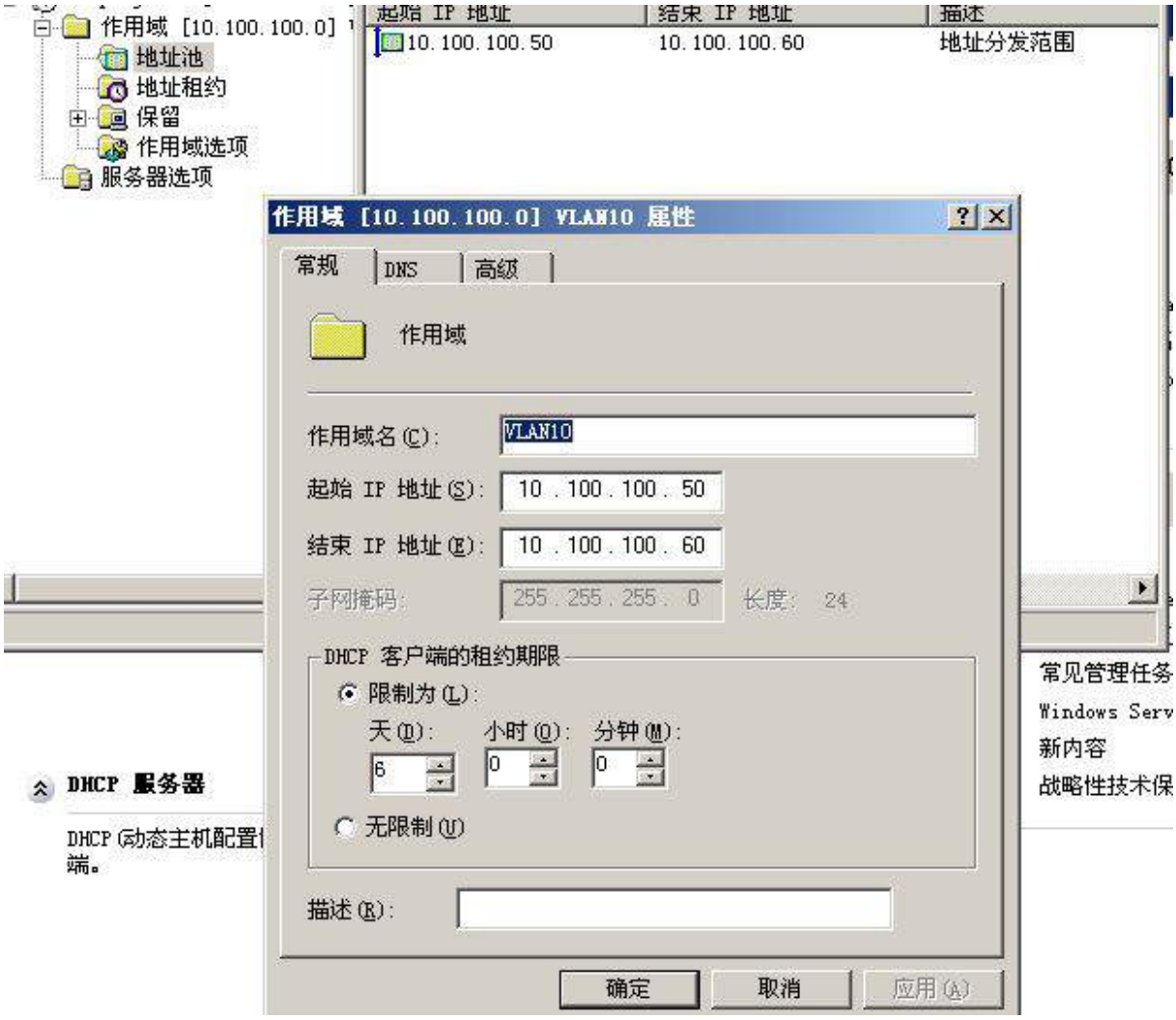


（5）创建模拟目录 PC-B，且只有客户端 PC-B 用户可以访问，可以实现文件的上传和下载，并启用日志记录功能；

（6）将上面所有配置点截图粘贴到竞赛结果文件指定位置。

3. 在主机 Win2003-B1 中完成 DHCP 服务器的部署

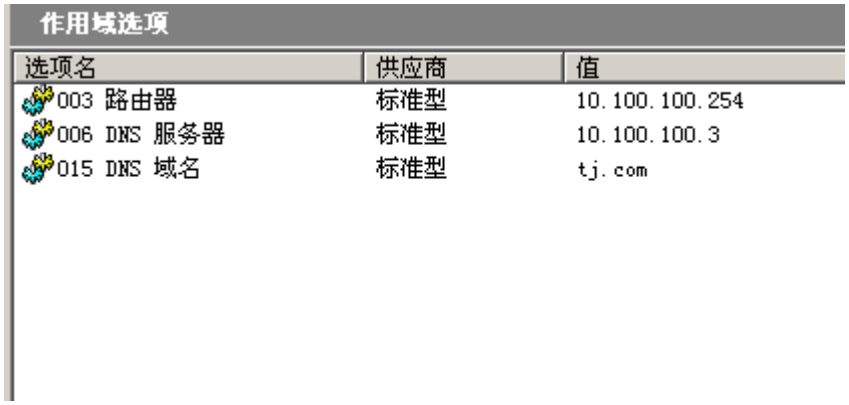
（1）安装 DHCP 服务器；创建作用域为集团公司 VLAN10 网段，地址范围、DNS 和网关根据表 1-4 规划需求指定，租约期限为 6 天。保留 IP 地址网关，给每个网段的 DHCP 客户端分配一个用户类别；



（2）通过用户类别使 DHCP 客户端获取正确的 IP 地址；

（3）客户地址的有效期为 24 小时；

（4）配置正确的网关，DNS 指向 Win2003-A1；

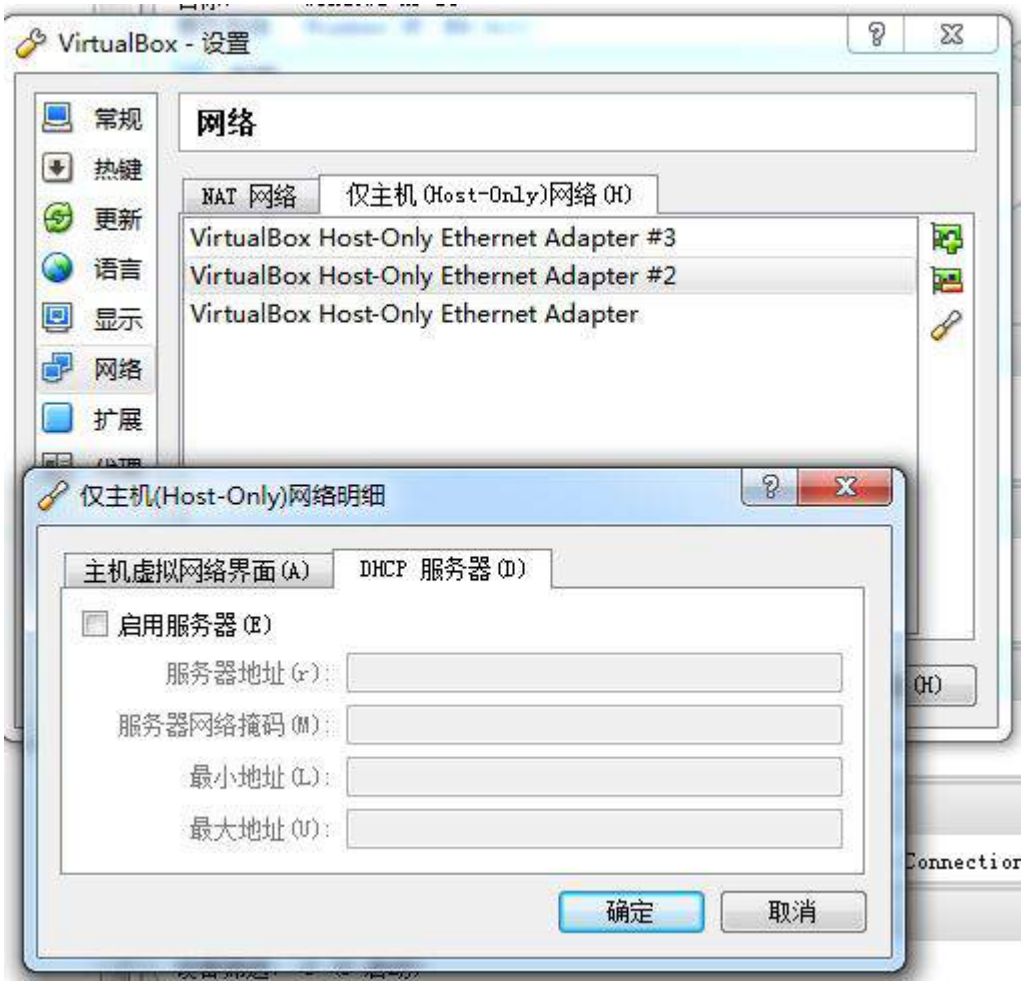


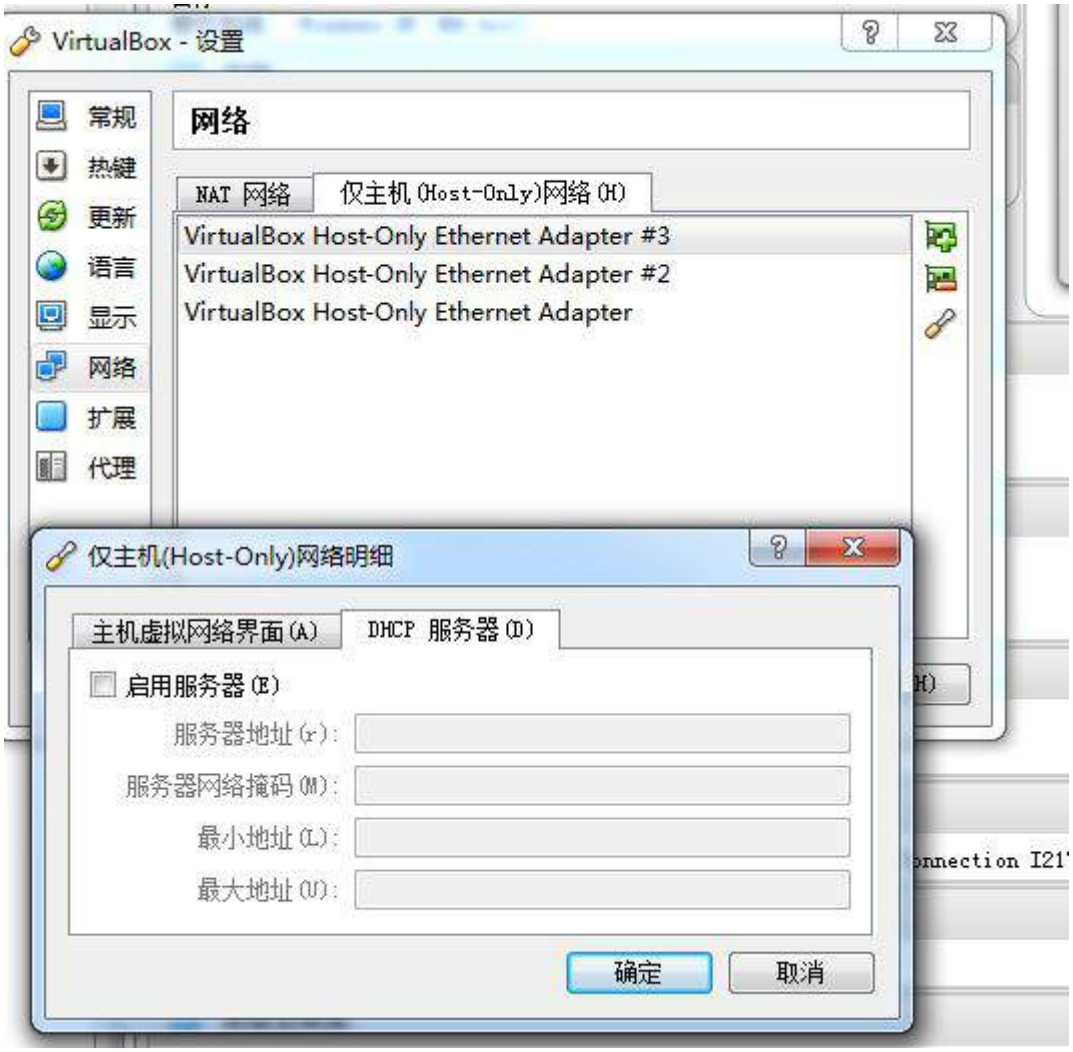
（5）将上面所有配置点截图粘贴到竞赛结果文件指定位置。

三、在 PC-C 上完成如下操作

1. 完成虚拟主机的创建

（1）创建 2 个“host-only”类型网络(虚拟机管理菜单—全局设定—网络),分别设置为#2 和#3 ,均禁用 dhcp 服务；以下 IP 均指在系统内网络静态地址，掩码默认设置；





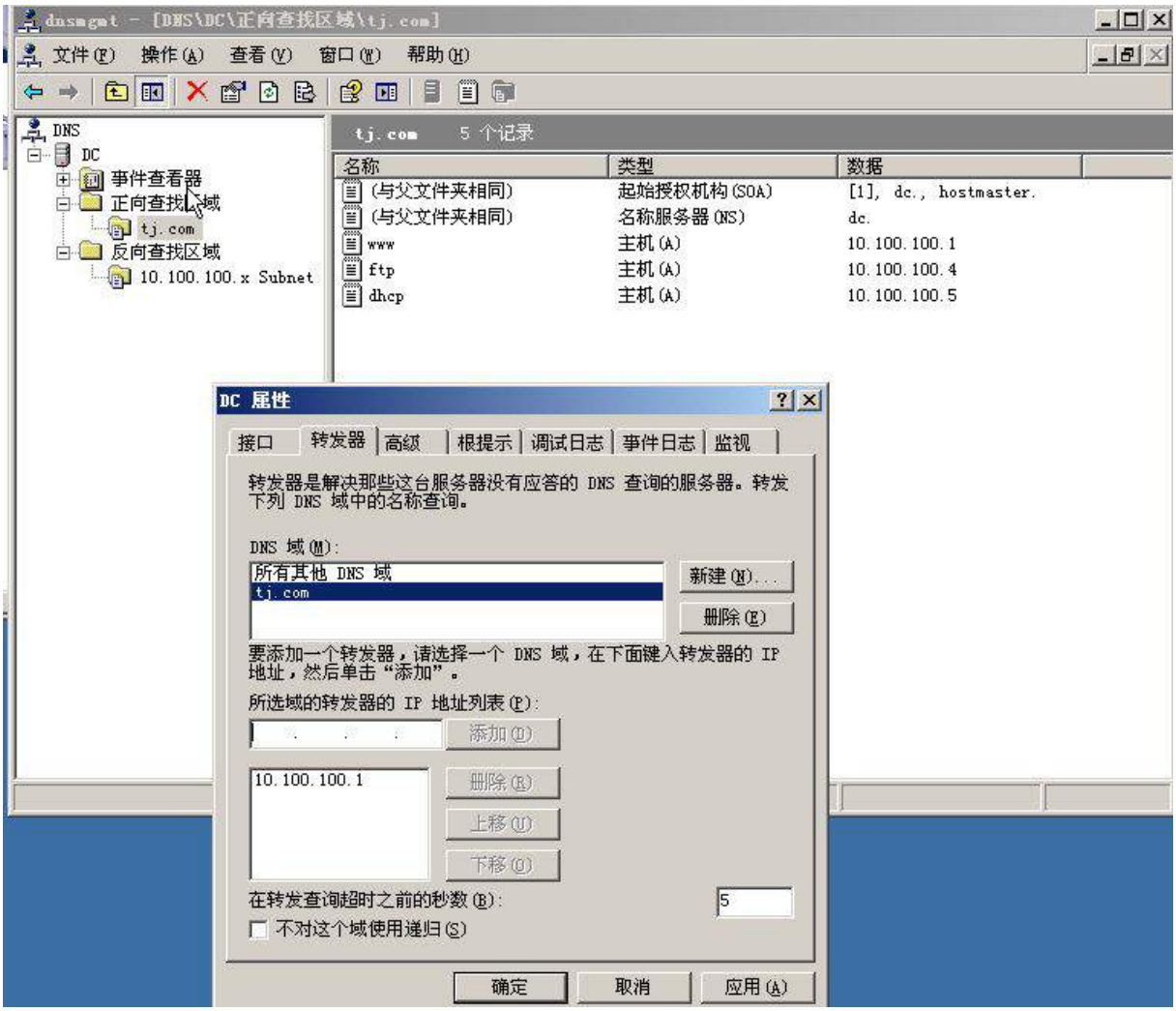
（2）创建虚拟机“Win2003-C1”，具体要求为内存 512MB，硬盘 15GB，主分区 10GB，扩展分区 5GB，分为两个逻辑分区，大小分别为 3GB 和 2GB；网卡使用 host-only 连接方式，使用#2 网络接口 IP（参见 IP 地址分配表 1-5 自行规划内容）；

（3）创建虚拟机“Win2008-C1”，具体要求为内存 768MB，硬盘 20GB，主分区 15GB，扩展分区 5GB.分为两个逻辑分区，大小分别为 3GB 和 2GB。网卡使用 host-only 连接方式，使用#3 网络接口 IP（参见 IP 地址分配表 1-5 自行规划内容）；

（4）将上面所有配置点截图粘贴到竞赛结果文件指定位置。

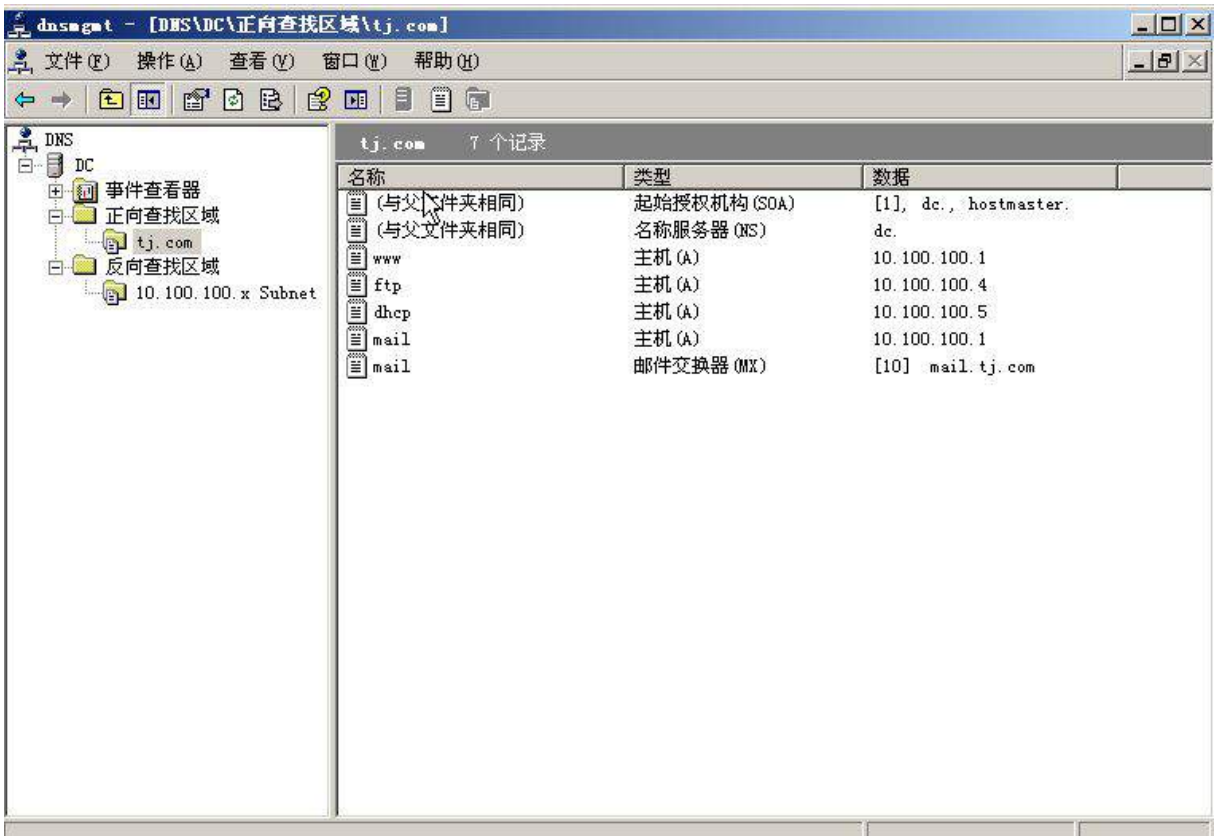
2、在主机 Win2003-C1 中完成 DNS 服务器的部署

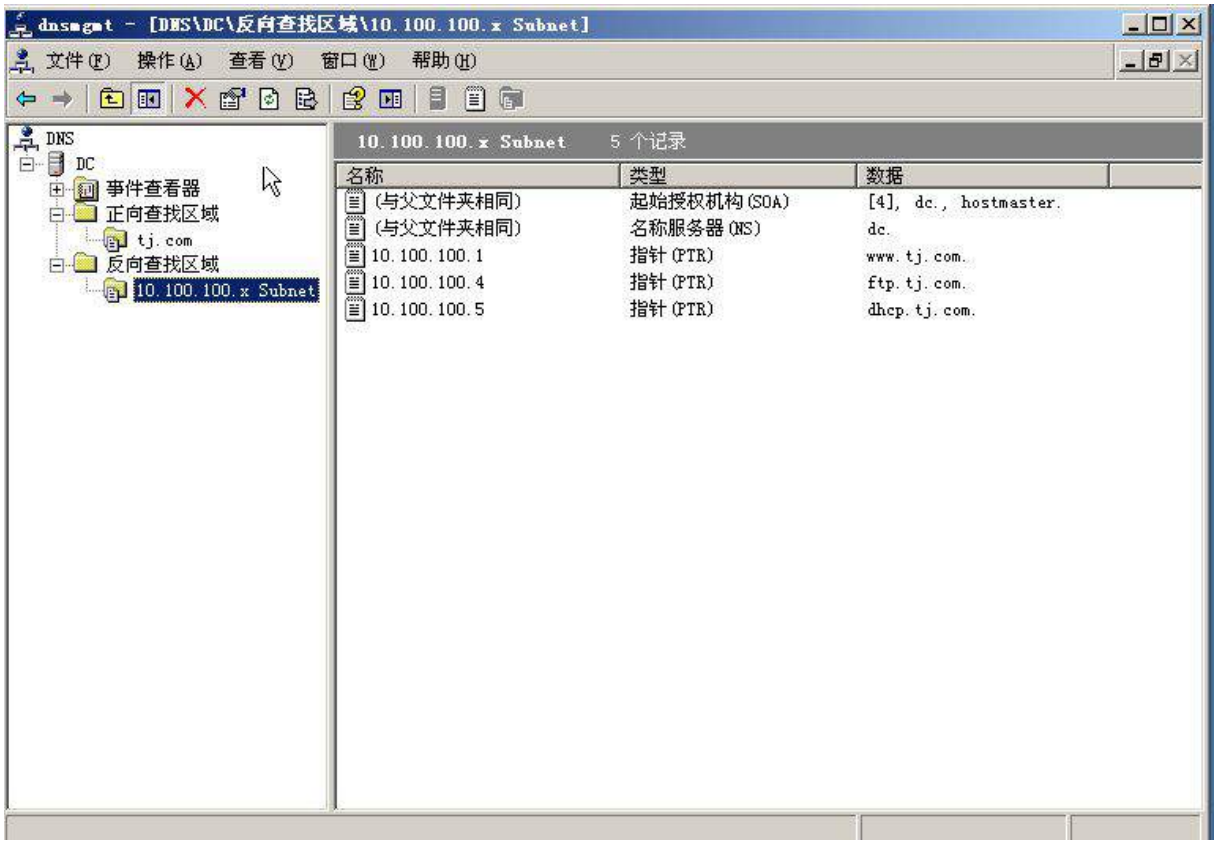
在 Win2003A 服务器上配置 DNS 服务，为单位内部用户提供域名解析服务，同时也负责向外部 DNS 服务器转发 DNS 请求，域名为 tj.com。



（1）能实现正向、反向域名解析服务；

（2）实现 www.tj.com、ftp.tj.com、dhcp.tj.com 域名解析服务；并为邮件服务器建立邮件交换器。将域 tj.com 的记录内容界面截图保存。

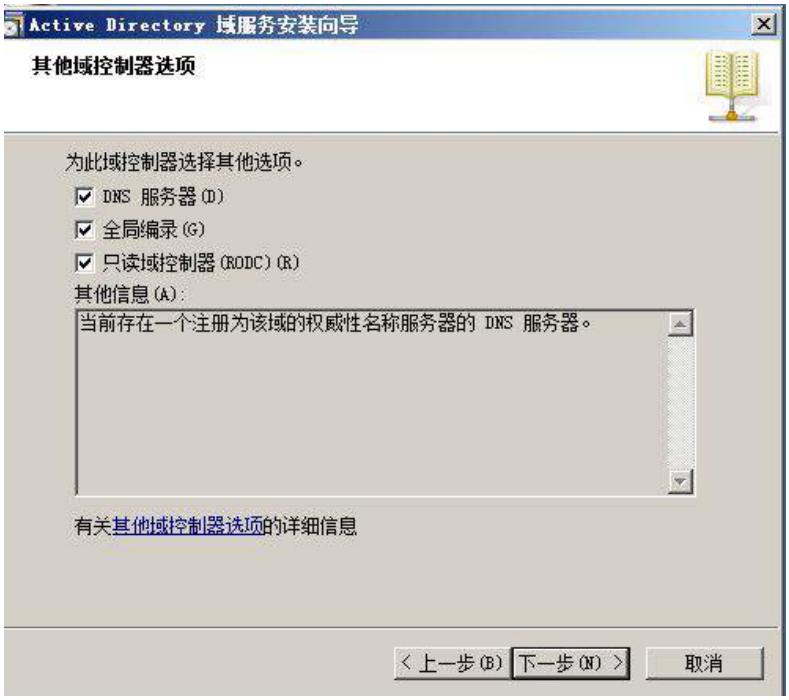




3. 在主机 Win2008-C1 中完成 RODC 只读域控制器的部署

（1）将此服务器升级为 ykca.com 只读域控制器；进入“服务管理器”的“角色”菜单，

展开“Active Directory 域服务”项后截图命名为 rodc.jpg 进行存储；



（2）将上面所有配置点截图粘贴到竞赛结果文件指定位置。

二、Linux 操作系统部分

【注意事项】

（1）所有 Linux 操作系统的 root 用户的密码为 123456，若未按要求设置密码，涉及到该操作系统下的所有分值记为 0 分。

（2）系统主机及虚拟主机的 IP 属性设置请按照网络拓扑结构图以及（参见分配表 1-5 自行规划内容）的要求设定。

（3）除有特别规定外，其他未明确规定用户密码均与用户名相同。

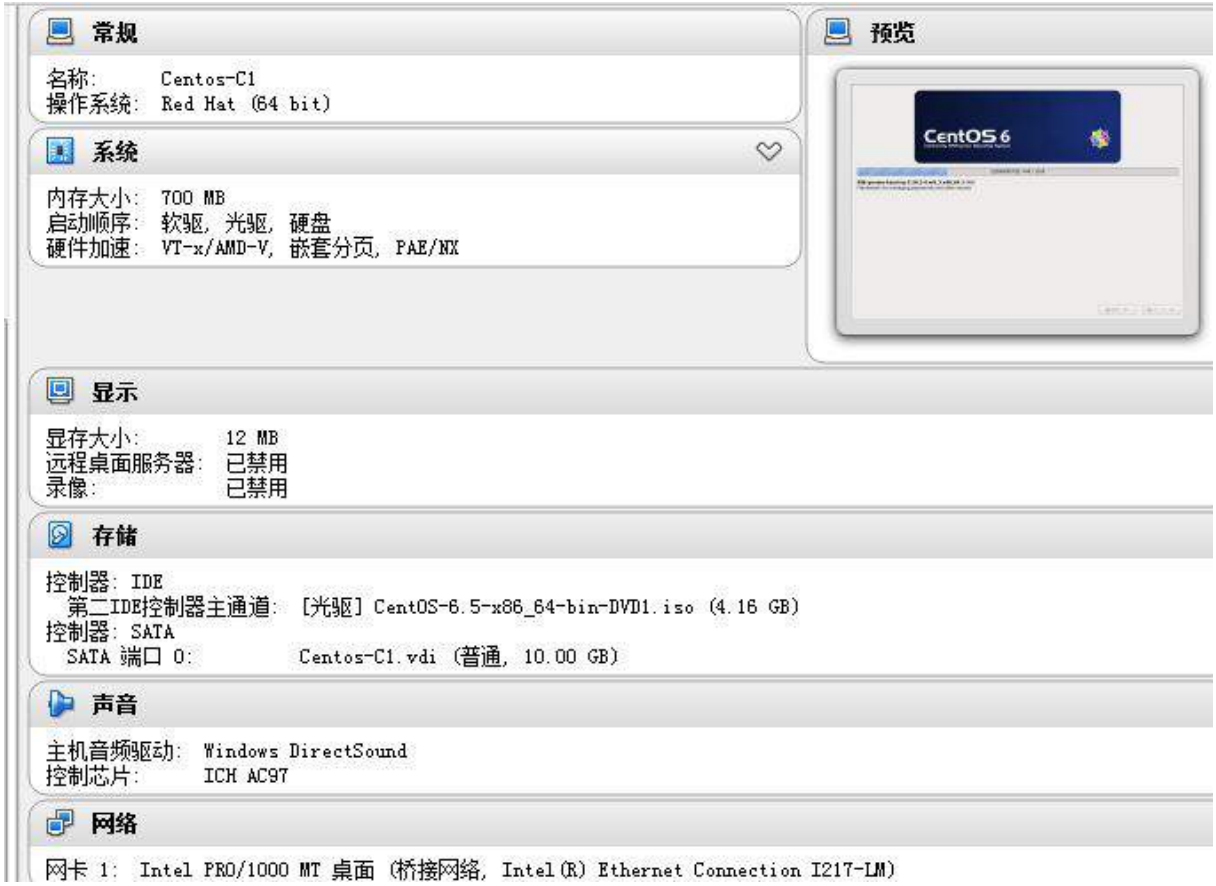
（4）所有操作系统镜像文件及试题所需的其他软件均存放于每台计算机的/根目录下，并将题目要求的截图内容以.jpg 格式存储于计算机桌面以自己参赛工位号文件夹内。

（5）请各位选手按下列要求完成各项服务器配置，在完成配置后提交能反映各个配置项目结果的窗口截图，PC-C、PC-D 中 Linux 系统的所有截图按照试题顺序粘贴在文件名为：工位号_PC-C.doc、工位号_PC-D.doc（如 47 号工位在 PC-D 的文件命名为：47_PC-D.doc）的文档中，要求有试题的题号小标题，并对每个截图进行必要的说明，无截图的项目不得分，若缺少文件，涉及到该文件对应设备下的所有分值记为 0 分。，

一、在 PC-C 上完成如下操作：

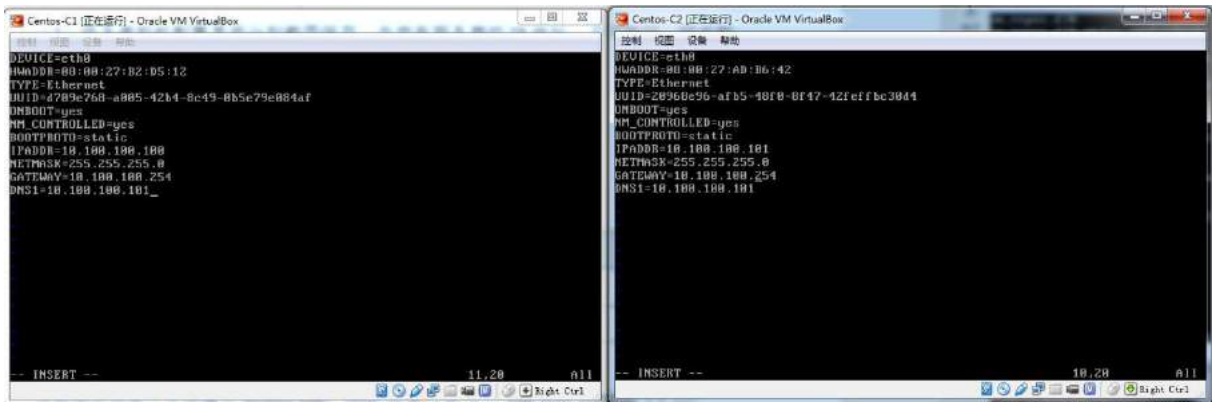
1. 完成虚拟主机的创建

（1）安装虚拟机“Centos-C1”，具体要求为内存 700MB，硬盘 10GB；



（2）安装虚拟机“Centos-C2”，具体要求为硬盘大小为 20GB，内存为 700MB；

（3）将各虚拟机配置界面分别截图保存，内容有服务器的 IP 地址、子网掩码、网关和 DNS 等



2. 在主机 Centos-C1 中完成 Apache 服务器的部署

（1）在 **Centos-C1 安装** Apache 服务；

①设置虚拟站点，将主文件设定成对应域名的默认首页；

表 2-2 域目录信息表

域名	目录	主文件
www1.linunet.tj.com	/web/http	Main.htm
www2.linunet.tj.com	/web/php	Default.php

```
#
# VirtualHost example:
# Almost any Apache directive may go into a VirtualHost container.
# The first VirtualHost section is used for requests without a known
# server name.
#
#<VirtualHost *:80>
#    ServerAdmin webmaster@dummy-host.example.com
#    DocumentRoot /www/docs/dummy-host.example.com
#    ServerName dummy-host.example.com
#    ErrorLog logs/dummy-host.example.com-error_log
#    CustomLog logs/dummy-host.example.com-access_log common
#</VirtualHost>
<VirtualHost *:80>
    DocumentRoot /web/http
    ServerName www1.linunet.tj.com
    DirectoryIndex main.htm
</VirtualHost>
<VirtualHost *:80>
    DocumentRoot /web/php
    ServerName www2.linunet.tj.com
    DirectoryIndex default.php
</VirtualHost>
                                                    1018,1        Bot
```

②在站点目录下分别建立 main.htm，body 标签内容为 success；

③在站点目录下分别建立 default.php，body 标签内容为:<? php echo phpinfo（）;?>

```
                                                                phpinfo() (1/27)
   PHP Logo

   PHP Version 5.3.3

   System                  Linux localhost.localdomain 2.6.32-431.el6.x86_64 #1
                           SMP Fri Nov 22 03:15:09 UTC 2013 x86_64
   Build Date              Nov 22 2013 11:00:06
                           './configure' '--build=x86_64-redhat-linux-gnu'
                           '--host=x86_64-redhat-linux-gnu'
                           '--target=x86_64-redhat-linux-gnu' '--program-prefix='
                           '--prefix=/usr' '--exec-prefix=/usr'
                           '--bindir=/usr/bin' '--sbindir=/usr/sbin'
                           '--sysconfdir=/etc' '--datadir=/usr/share'
                           '--includedir=/usr/include' '--libdir=/usr/lib64'
                           '--libexecdir=/usr/libexec' '--localstatedir=/var'
                           '--sharedstatedir=/var/lib' '--mandir=/usr/share/man'
                           '--infodir=/usr/share/info'
                           '--cache-file=../config.cache' '--with-libdir=lib64'
                           '--with-config-file-path=/etc'
                           '--with-config-file-scan-dir=/etc/php.d'
                           '--disable-debug' '--with-pic' '--disable-rpath'
                           '--without-pear' '--with-bz2'
                           '--with-exec-dir=/usr/bin' '--with-freetype-dir=/usr'
http://www.php.net/                                                    [------]
```

④只允许本网段的主机可以访问该网站；

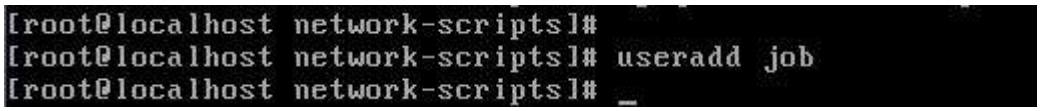
```
#
# "/var/www/cgi-bin" should be changed to whatever your ScriptAliased
# CGI directory exists, if you have that configured.
#
<Directory "/web/http">
    AllowOverride None
    Options None
    Order allow,deny
    Allow from 10.100.100.*
</Directory>
<Directory "/web/php">
    AllowOverride None
    Options None
    Order allow,deny
    Allow from 10.100.100.*
</Directory>

#
# Redirect allows you to tell clients about documents which used to exist in
# your server's namespace, but do not anymore. This allows you to tell the
# clients where to look for the relocated document.
# Example:
# Redirect permanent /foo http://www.example.com/bar
-- INSERT --                                              585,28        57%
```

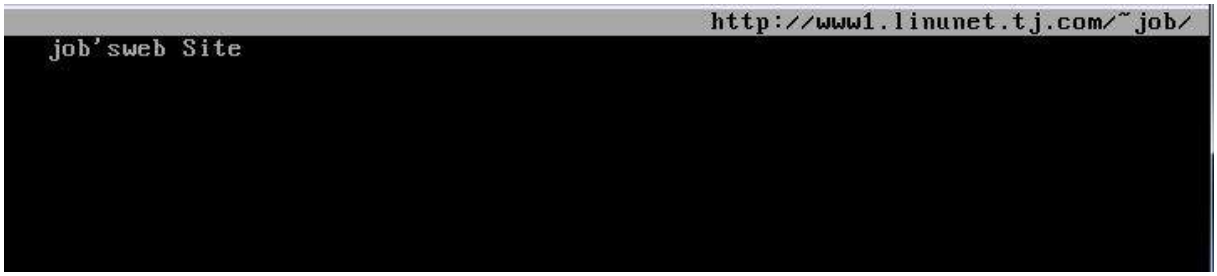
⑤将 MySQL 数据库的管理员 root 的密码设置为 mysql417，并新建一个数据库，命名为 offer；

```
[root@localhost network-scripts]# mysqladmin -u root password "mysql1417"
[root@localhost network-scripts]#
[root@localhost network-scripts]#
```

```
mysql> create database offer;
Query OK, 1 row affected (0.01 sec)
```

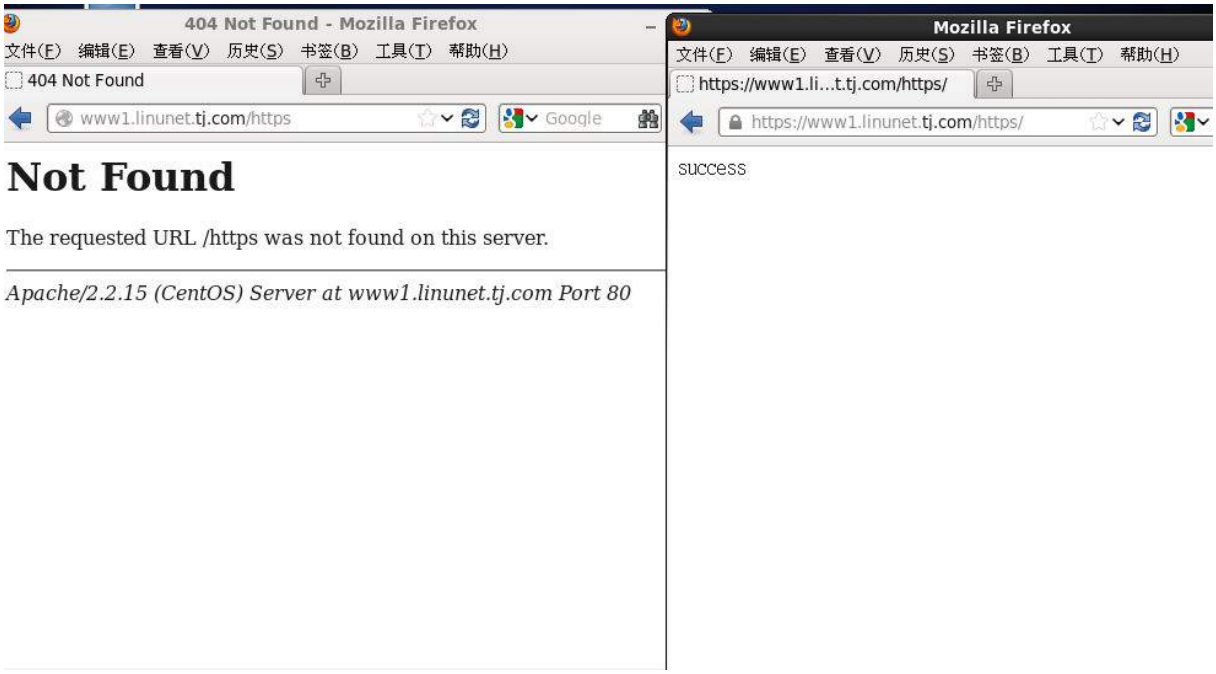
⑥新建用户 job，实现该用户的个人主页，内容为 job'sweb Site；



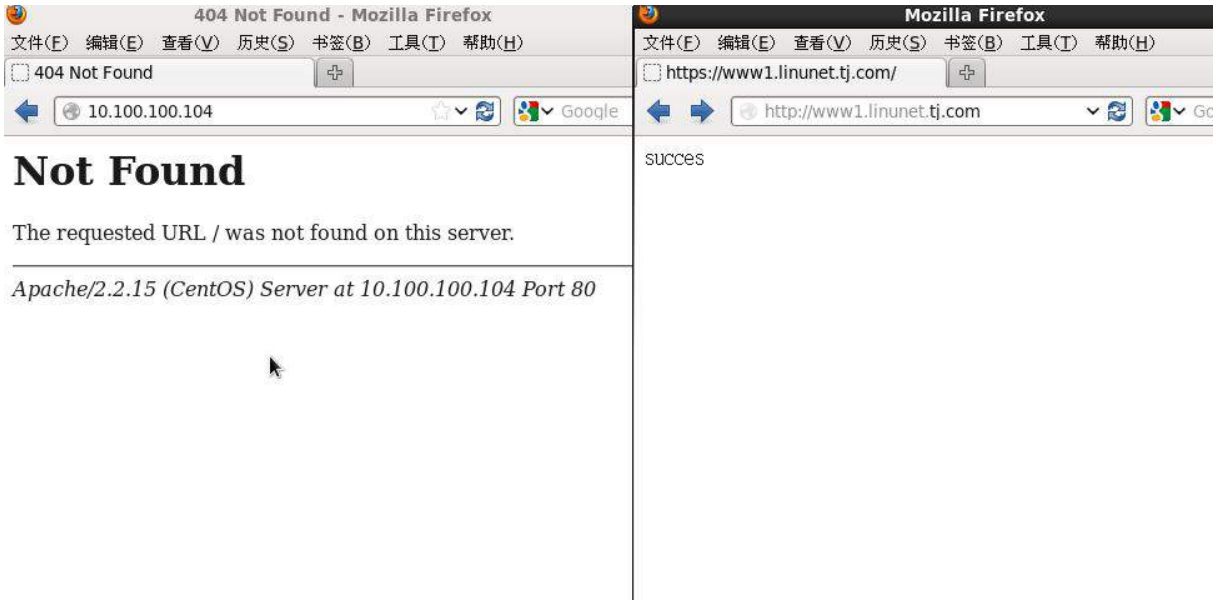


⑦实现 www1 的 ssl 访问。

（2）配置 http，使用自签名证书，使访问 www1. linu.net/https 时必须使用 https 方式访问；此问须截图命名为 https.jpg 进行存储；



（3）配置只能使用域名访问网站，不能使用 ip 地址，httpd 服务开机自启动，不需要输入私钥密码；




```
[root@localhost conf.d]# chkconfig httpd on
```

```
[root@localhost conf]# openssl rsa -in server.key -out server.key
Enter pass phrase for server.key:
writing RSA key
[root@localhost conf]#
```

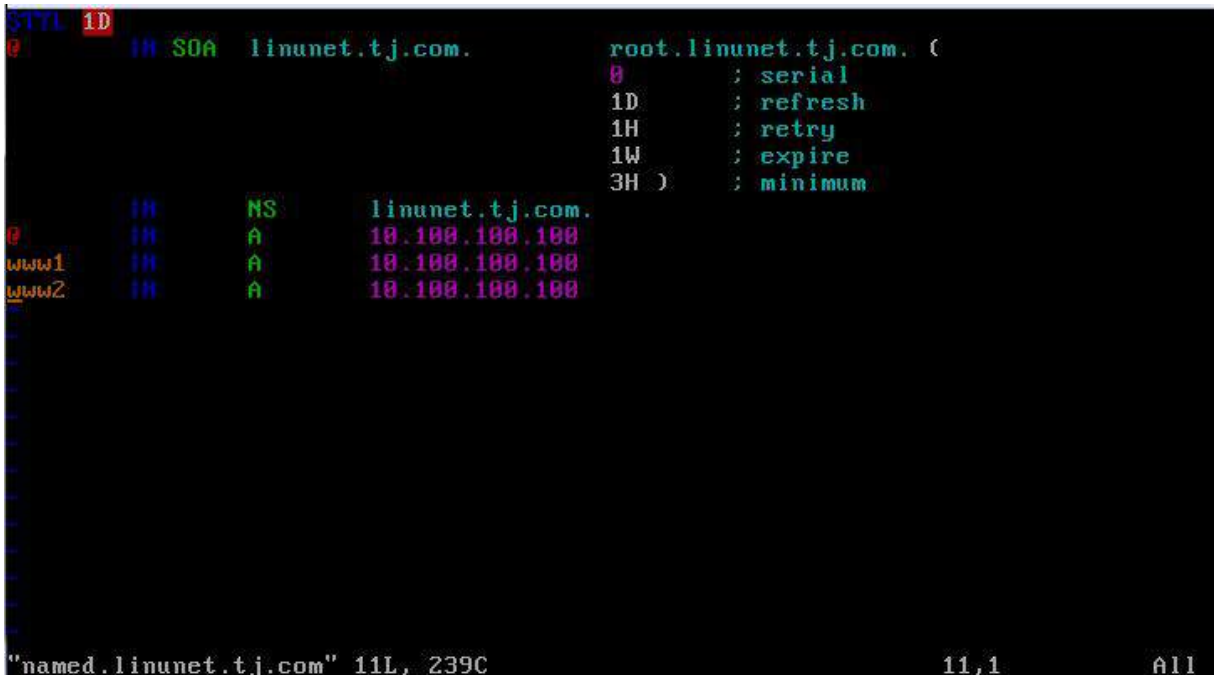
（4）将/var 目录打包并压缩成 gzip 格式，文件名为 var.tar.gz，保存到/tmp 目录下；

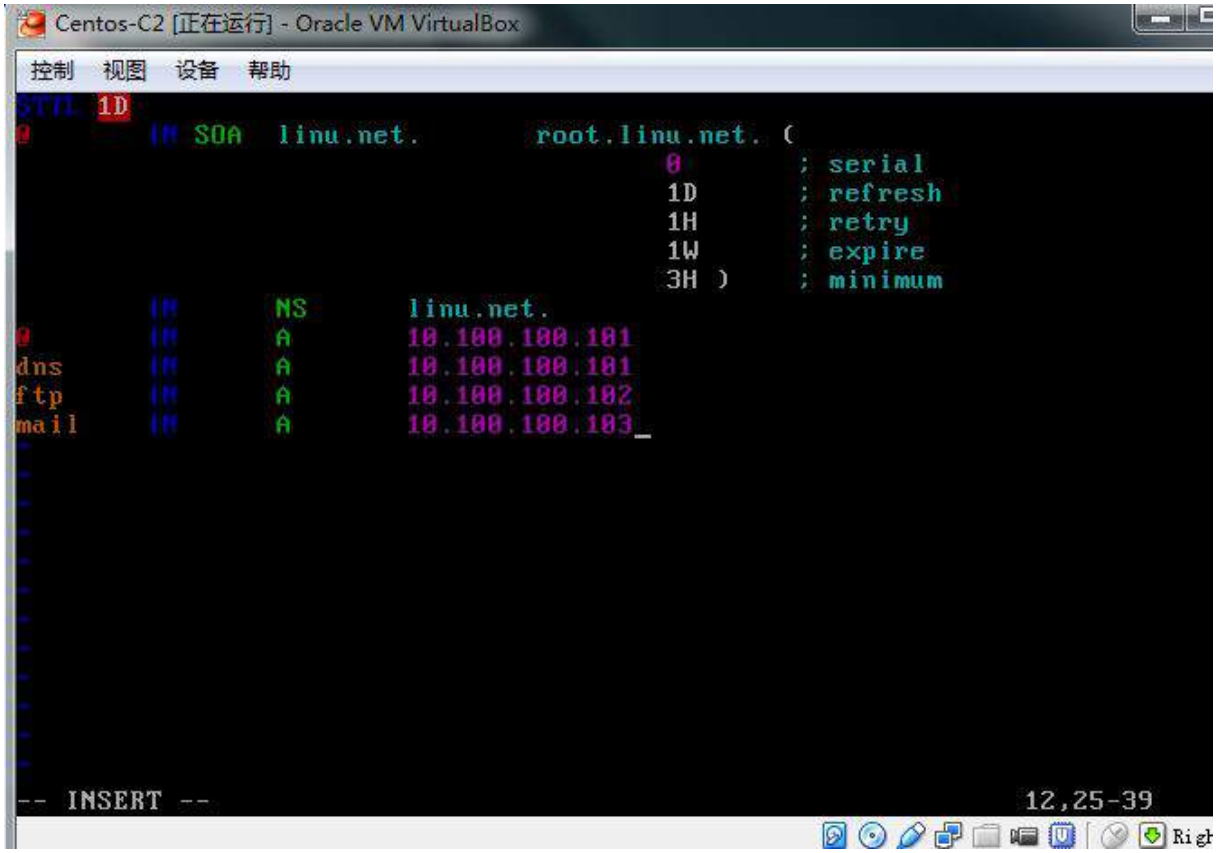
```
[root@localhost conf]# tar -zcvf /tmp/var.tar.gz /var
```

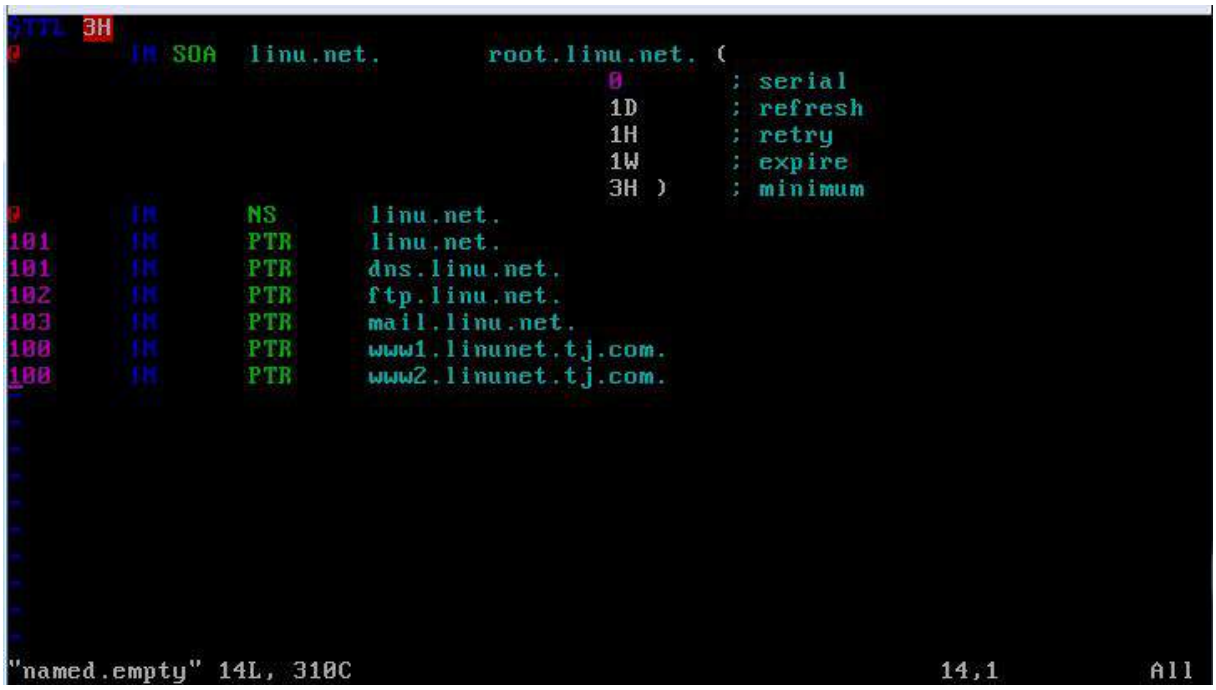
（5）将上面 5 个方面的主要配置关键点界面截图保存到竞赛结果文件指定位置。

3. 在主机 Centos-C2 中完成 BIND 域名服务器、MySQL 数据库服务器以及 NFS 共享服务器的部署

（1）在此服务器中安装配置 bind 服务，负责区域“linu.net”内所有主机解析；







（2）在 Centos-C2 上安装 mysql 服务，并新创建一个数据库名为 newstaff；创建一个数据表为 s-table；字段类型为 Username Char(10)，Sex Char(6)，Age int；并将下表中的总公司部门员工信息插入到 s-table 表中，将查询数据表 s-table 的结果截图保存。按如下表创建 2-3 表 s-table；

表 2-3 数据库表

序号	Username	Sex	Age
1	Janes	Male	33
2	Selire	Female	32
3	Bonnie	Male	24
4	Lesir	Female	23
5	Jonie	Male	27
6	Pense	Female	24

```
mysql> create database newstaff;
Query OK, 1 row affected (0.00 sec)
```

```
mysql> use newstaff
Database changed
mysql> create table stable(
    -> ID int primary key auto_increment,
    -> Username char(10),
    -> Sex char(6),
    -> Age int);
Query OK, 0 rows affected (0.06 sec)
```

```
mysql> insert into stable(Username,Sex,Age)value("Janes","Male","33");
Query OK, 1 row affected (0.00 sec)

mysql> insert into stable(Username,Sex,Age)value("Selire","Female","32");
Query OK, 1 row affected (0.00 sec)

mysql> insert into stable(Username,Sex,Age)value("Bonnie","Male","24");
Query OK, 1 row affected (0.00 sec)

mysql> insert into stable(Username,Sex,Age)value("Lesir","Female","23");
Query OK, 1 row affected (0.00 sec)

mysql> insert into stable(Username,Sex,Age)value("Jonie","Male","27");
Query OK, 1 row affected (0.00 sec)

mysql> insert into stable(Username,Sex,Age)value("Pense","Female","24");
Query OK, 1 row affected (0.00 sec)
```

```
mysql> select * from stable;
+----+----------+--------+------+
| ID | Username | Sex    | Age  |
+----+----------+--------+------+
|  1 | Janes    | Male   |   33 |
|  2 | Selire   | Female |   32 |
|  3 | Bonnie   | Male   |   24 |
|  4 | Lesir    | Female |   23 |
|  5 | Jonie    | Male   |   27 |
|  6 | Pense    | Female |   24 |
+----+----------+--------+------+
6 rows in set (0.00 sec)
```

（3）每周五凌晨 3：00 备份数据库 testdb 到/var/databak/testdb.sql；

```
[root@localhost /]# vim backup.sh
```

```
mysqldump -u root -pmysql1417 testdb >/var/databak/test.sql
```

```
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root
HOME=/

# For details see man 4 crontabs

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,f
ri,sat
# |  |  |  |  |
# *  *  *  *  * user-name command to be executed
  0  1  *  *  5 root /backup.sh_
~
~
~
~
```

（4）配置 NFS 服务，服务开机自启动。按下表 2-3 要求共享目录；

```
[root@localhost etc]# chkconfig nfs on
[root@localhost etc]#
[root@localhost etc]# _
```

表 2-3 共享目录表

共享目录	共享要求
/var/test	市场部这个网段的用户具有读写权限，其它只读
/var/tmp	所有人都可以存取，root 写入的文件还具有 root 的权限

```
/var/test       10.100.100.0/24(rw)     *(ro)
/var/tmp        *(rw,no_root_squash)
```

（4）创建用户 nfsuser，当 nfsuser 在终端登录时，自动 mount 共享的/var/test 目录到/home/nfsuser/t，退出时自动 umout；

```
[root@localhost etc]#
[root@localhost etc]#
[root@localhost etc]# useradd nfsuser
[root@localhost etc]#
[root@localhost etc]#
```

```
## Allow root to run any commands anywhere
root    ALL=(ALL)       ALL

## Allows members of the 'sys' group to run networking, software,
## service management apps and more.
# %sys ALL = NETWORKING, SOFTWARE, SERVICES, STORAGE, DELEGATING, PROCESSES, LOC
ATE, DRIVERS

## Allows people in group wheel to run all commands
# %wheel        ALL=(ALL)       ALL

## Same thing without a password
# %wheel        ALL=(ALL)       NOPASSWD: ALL

## Allows members of the users group to mount and unmount the
## cdrom as root
# %users  ALL=/sbin/mount /mnt/cdrom, /sbin/umount /mnt/cdrom

## Allows members of the users group to shutdown this system
# %users  localhost=/sbin/shutdown -h now

## Read drop-in files from /etc/sudoers.d (the # here does not mean a comment)
#includedir /etc/sudoers.d
nfsuser         ALL=(ALL)       NOPASSWD:ALL_
```

```
# .bash_profile

# Get the aliases and functions
if [ -f ~/.bashrc ]; then
        . ~/.bashrc
fi

# User specific environment and startup programs

PATH=$PATH:$HOME/bin

export PATH
sudo    mount 10.100.100.101:/var/test /home/nfsuser/t_
```

```
# ~/.bash_logout
sudo umount /home/nfsuser/t_
```

（5）将上面 6 个方面的主要配置关键点界面截图保存到竞赛结果文件指定位置。

二、在上完成如下操作:

1. PC-D 主机系统为 CentOS 6.5，需要在此 Linux 平台上采用 KVM 方式安装以下虚拟机

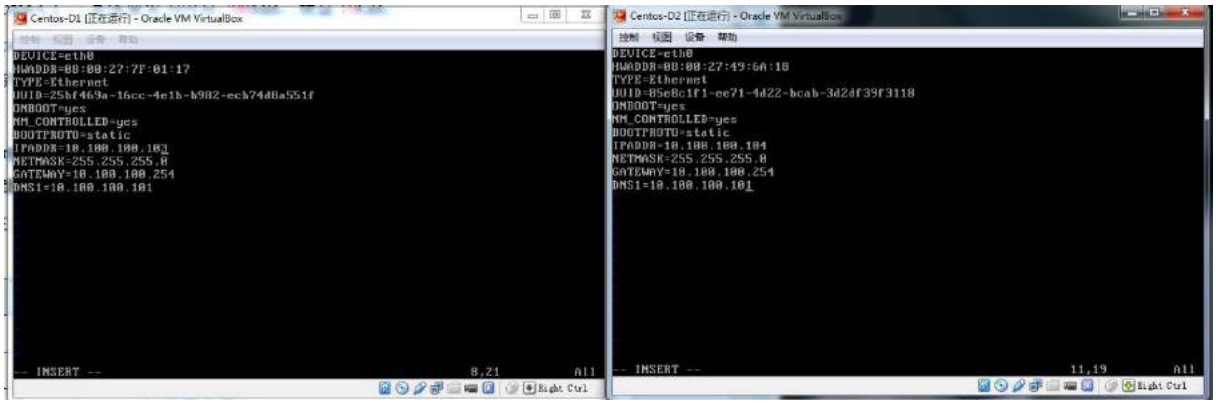
（小提示：如无法正确安装虚拟机 Centos-D1，下述题目中所涉及的虚拟机题目可在 Server4 真实主机中完成）

（1）安装虚拟机“Centos-D1”，具体要求为内存 900MB，硬盘 10GB，分区大小为：

SWAP 分区大小为 700M；/boot 分区大小为 512M，文件类型为 ext3；/home 分区大小为 1G，文件类型为 ext3，其余为/分区，文件类型为 ext3；

（2）安装虚拟机“Centos-D2”，具体要求为硬盘大小为 15GB，内存为 800MB；

（3）将各虚拟机配置界面分别截图保存，内容有服务器的 IP 地址、子网掩码、网关和 DNS 等。

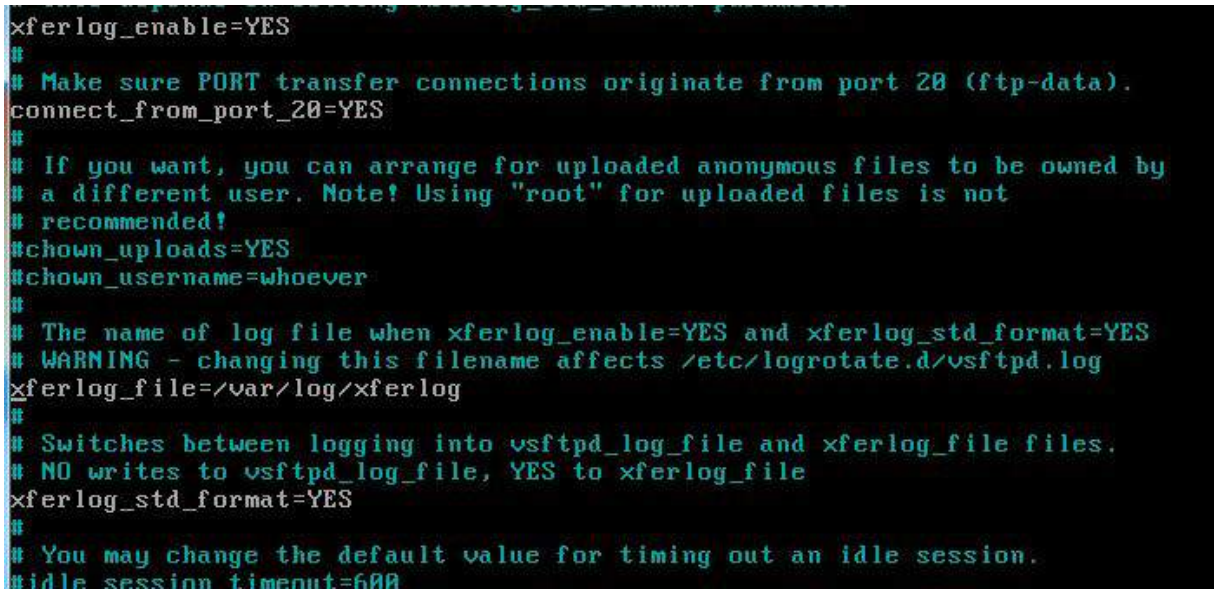


2. 在主机 Centos-D1 中完成 FTP 服务器部署

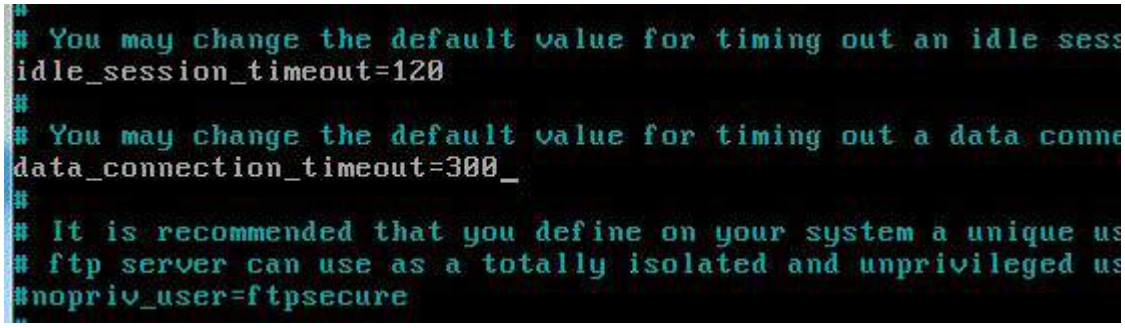
在 **Centos-D1** 上配置 FTP 服务，使得用户在客户端能通过域名 ftp.tj.com 访问服务器。该服务器允许匿名用户访问，但只允许其下载数据，不允许上传数据；

```
# Allow anonymous FTP? (Beware - allowed by default if you comment this
anonymous_enable=YES
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to
# if your users expect that (022 is used by most other ftpd's)
local_umask=022
#
# Uncomment this to allow the anonymous FTP user to upload files. This
# has an effect if the above global write enable is activated. Also, yo
# obviously need to create a directory writable by the FTP user.
#anon_upload_enable=YES
anon_world_readable_only=YES_
#
# Uncomment this if you want the anonymous FTP user to be able to creat
# new directories.
#anon_mkdir_write_enable=YES
```

（1）开启 vsftp 的 log 功能设置，文件名为/var/log/xferlog；



（2）设置无任何操作的超时时间为两分钟,设置数据连接的超时时间为五分钟；



（3）设置 FTP 服务器最大支持连接数为 500 个，每个 IP 最多能支持 20 个链接；

（4）限制匿名用户以下载速度为不超过 512KB/S 速度下载,其他用户以 2MB/S 速度下载。将配置文件界面截图保存；

```
# You may activate the "-R" option to the builtin ls. This is disabled by
# default to avoid remote users being able to cause excessive I/O on large
# sites. However, some broken FTP clients such as "ncftp" and "mirror" assume
# the presence of the "-R" option, so there is a strong case for enabling it.
#ls_recurse_enable=YES
#
# When "listen" directive is enabled, vsftpd runs in standalone mode and
# listens on IPv4 sockets. This directive cannot be used in conjunction
# with the listen_ipv6 directive.
listen=YES
#
# This directive enables listening on IPv6 sockets. To listen on IPv4 and IPv6
# sockets, you must run two copies of vsftpd with two configuration files.
# Make sure, that one of the listen options is commented !!
#listen_ipv6=YES

pam_service_name=vsftpd
userlist_enable=YES
tcp_wrappers=YES
max_clients=500
max_per_ip=20
anon_rate=262144
local_rate=524288
```

（5）在客户端 Client1 通过域名访问 FTP 服务器，将访问的结果窗口截图保存。

3. 在主机 Centos-D2 中完成 MAIL 服务器的部署

（1）在 Centos-D2 系统上，按照下列要求进行 MAIL 邮件服务器配置：

①完成相关软件包的安装与配置，设置邮件服务器，开启 SMTP、POP3、IMAP 服务，用 Telnet 进行端口测试，将测试结果窗口截图保存；

```
[root@localhost ~]# telnet 10.100.100.104 25
Trying 10.100.100.104...
Connected to 10.100.100.104.
Escape character is '^]'.
220 localhost.localdomain ESMTP Sendmail 8.14.4/8.14.4; Sun, 5 Jun 2016 14:17:45
 +0800
quit
221 2.0.0 localhost.localdomain closing connection
Connection closed by foreign host.
[root@localhost ~]# telnet 10.100.100.104 110
Trying 10.100.100.104...
Connected to 10.100.100.104.
Escape character is '^]'.
+OK Dovecot ready.
quit
+OK Logging out
Connection closed by foreign host.
[root@localhost ~]# telnet 10.100.100.104 143
Trying 10.100.100.104...
Connected to 10.100.100.104.
Escape character is '^]'.
* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE START
TLS AUTH=PLAIN] Dovecot ready.
```

②建立电子邮件帐号 bonnie 和 jonie、bruce，密码均为 Tj2015，将操作过程界面截图保存；

```
[root@localhost ~]# useradd bonnie
[root@localhost ~]# useradd jonie
[root@localhost ~]# useradd bruce
[root@localhost ~]# passwd bonnie
Changing password for user bonnie.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@localhost ~]# passwd jonie
Changing password for user jonie.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@localhost ~]# passwd bruce
Changing password for user bruce.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@localhost ~]#
```

③配置允许 MAIL 服务器所在网段进行中继操作，同时限制 bruce@mail.shengshi.com.cn 发送邮件，将操作过程界面截图保存；

```
# Check the /usr/share/doc/sendmail/README.cf file for a description
# of the format of this file. (search for access_db in that file)
# The /usr/share/doc/sendmail/README.cf is part of the sendmail-doc
# package.
#
# If you want to use AuthInfo with "M:PLAIN LOGIN", make sure to have the
# cyrus-sasl-plain package installed.
#
# By default we allow relaying from localhost...
Connect:localhost.localdomain                   RELAY
Connect:localhost                               RELAY
Connect:127.0.0.1                               RELAY
Connect:10.100.100                              RELAY
```

(2)在客户端 Client2 中以 bonnie@mail.sh.com.cn 帐户名向 jonie@mail.sh.com.cn 帐户发一份电子邮件，主题为“邀请函”，内容为“欢迎参加 2015 大赛新闻发布会!”。在此物理机上使用 outlook 发送、接收邮件，在收件箱中选中此点子邮件，将能够显示此邮件信息内容的活动窗口截图保持。