**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。

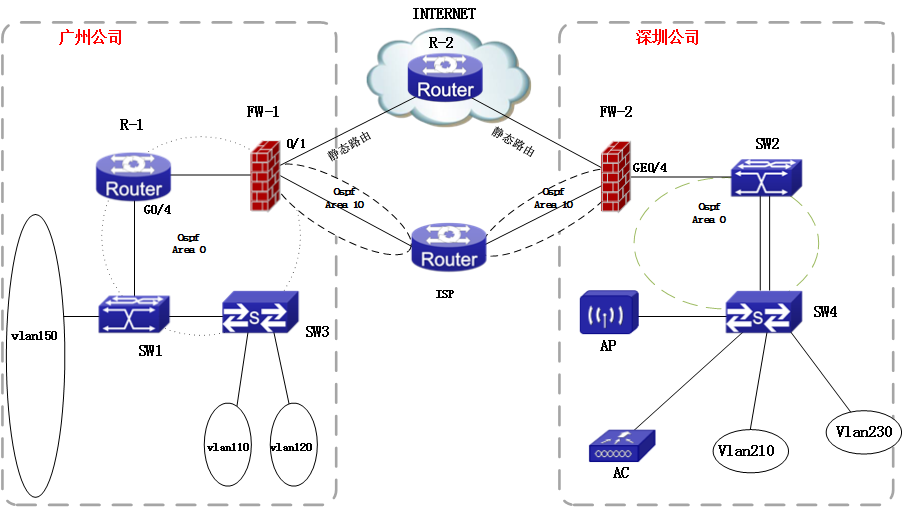
由于深圳公司业务发展迅速，在原有的有线架构实现与总公司互联的基础上，增加了无线接入方式，更方便来访人员访问网络资源。

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 |  |
| FW1 | Ethernet0/2 |  |
| 防火墙 | 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 R2 | IP: 10.1.5.101 |
| 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](ftp://ftp.jnds.net)  [ftp1.jnds.net](ftp://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：
   1. 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
   2. 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。
3. **物理连接与IP地址划分**
4. 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。
5. 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。
6. **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。

1. 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。

1. **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l2tp 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。

1. **无线配置**
2. 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”。
3. 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。
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。
5. 保障无线信息的覆盖性，无线AP的发射功率设置为90%。
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。

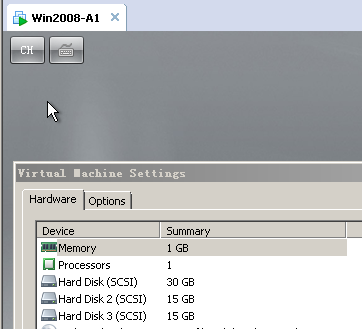
（3）所有系统镜像文件及试题所需的其它软件均存放在每台主机的D:\soft文件夹中，并将题目要求的截图内容以.jpg格式存储于各物理机桌面BACKUP\_X（X为组号）文件夹中，文件名、扩展名和存放位置错误，涉及到的所有操作分值记为0分。

（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。

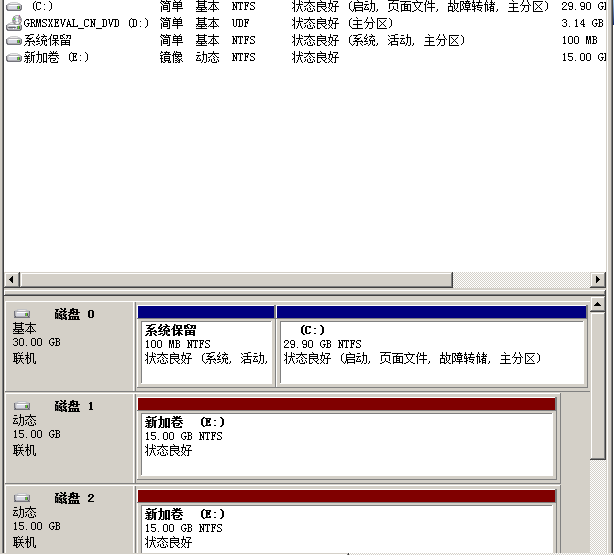
**一、在PC 1上完成如下操作:**

**（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；

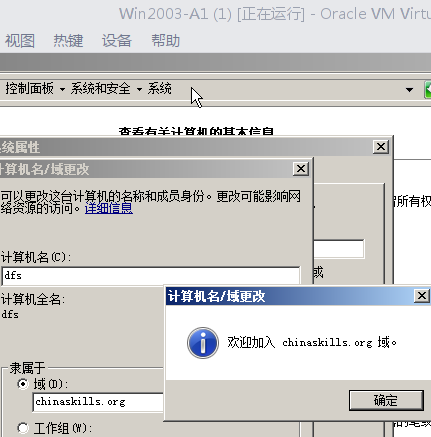


2、在虚拟机“Win2008-A1”中添加SCSI控制器，添加二块SCSI虚拟硬盘，其每块硬盘的大小为15G；将二块硬盘制作成RAID1，磁盘盘符为e:\；



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“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；

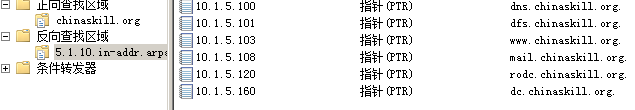


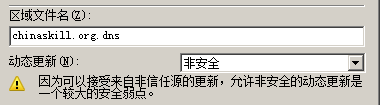


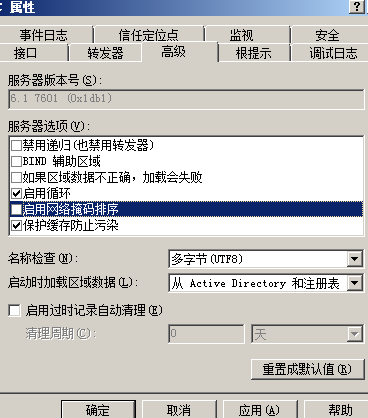
**（二）在主机Win2008-A1中完成DNS服务器的部署**

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；

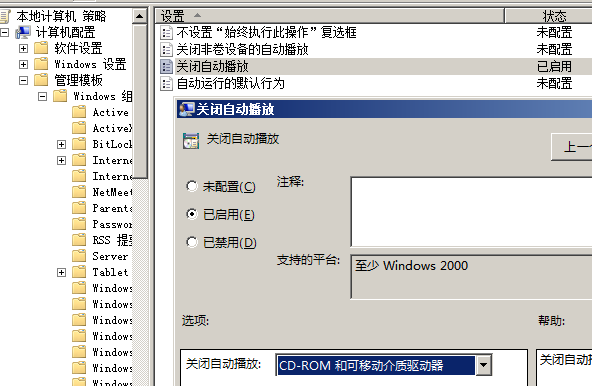


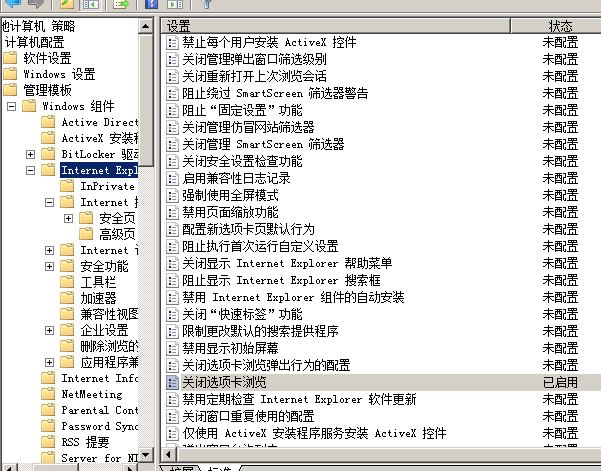






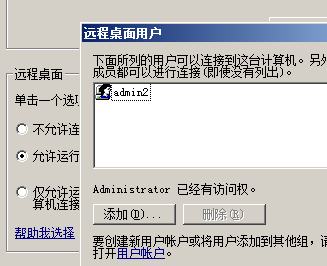
2、配置组策略，要求所有域内计算机禁用光盘自动播放，不在桌面显示网上邻居图标，禁用IE的安全选项卡。；



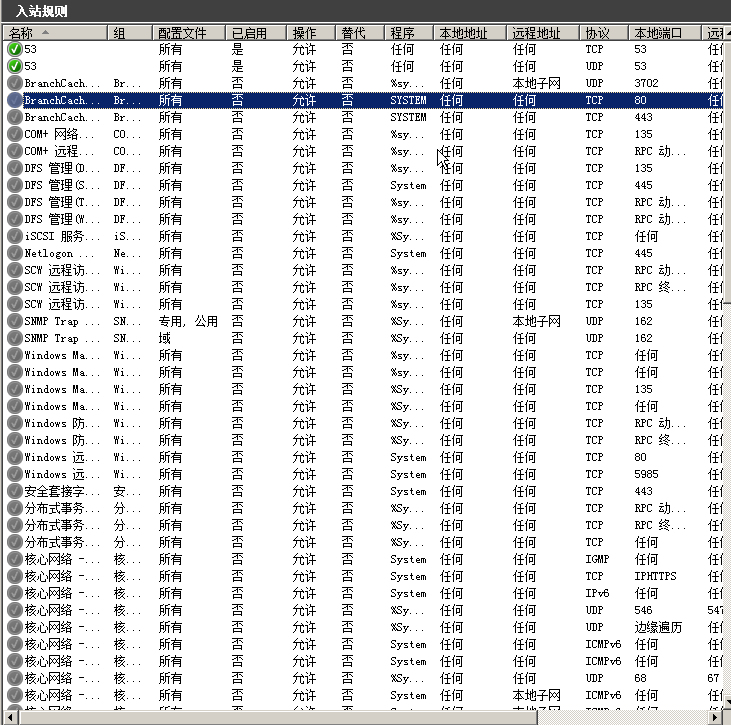


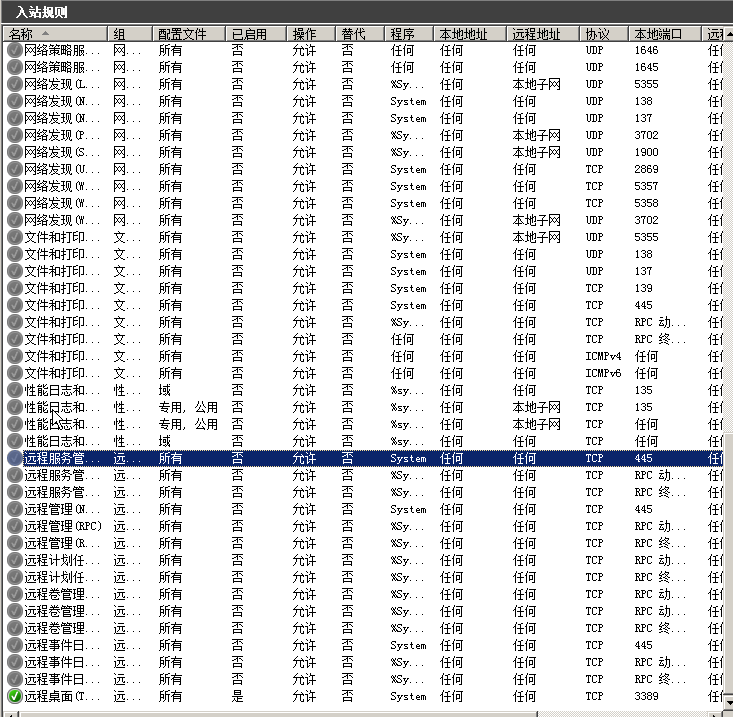


3. 打开远程桌面功能，允许使用admin2登录；



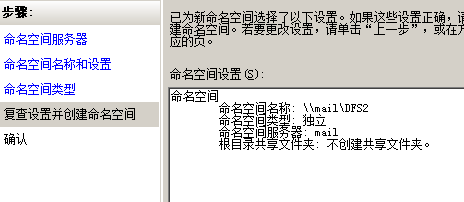
4. 开启系统防火墙，关闭除服务端口外的其他端口；

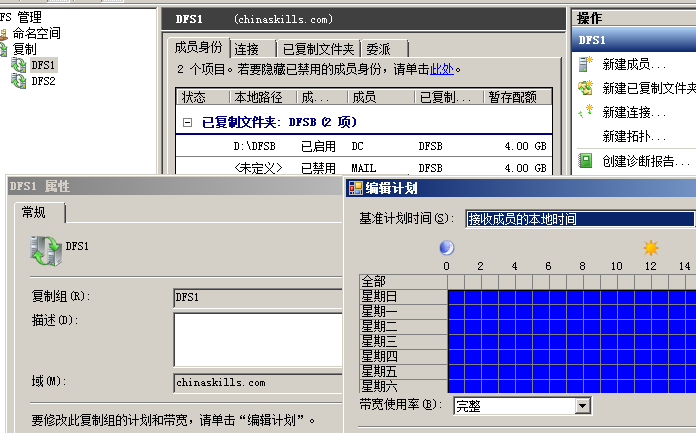




**（三）在主机Win2003-A1中完成DFS服务器的部署**

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]；



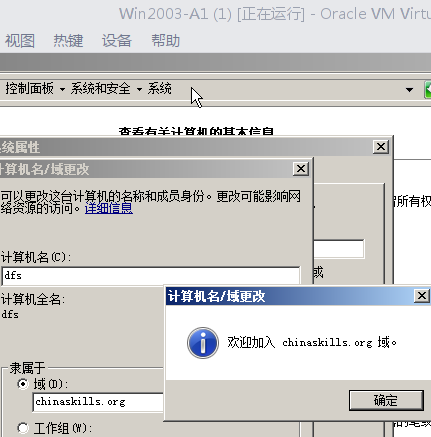


**二、在PC2上完成如下操作:**

**（一）完成虚拟主机的创建**

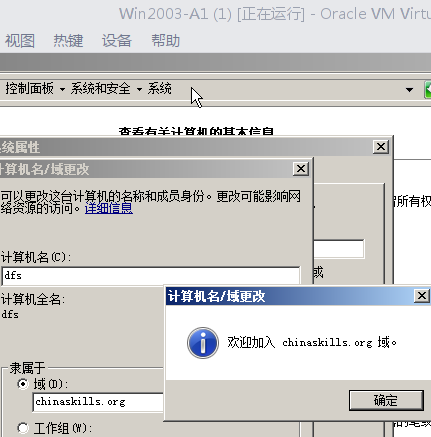
1、安装虚拟机“Win2008-B1”，其内存为1G，硬盘20G，并将服务器加入到Windows域环境；





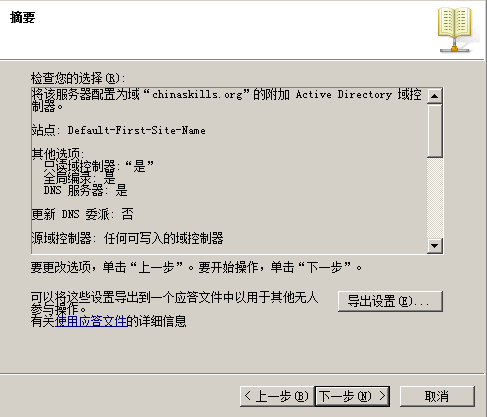
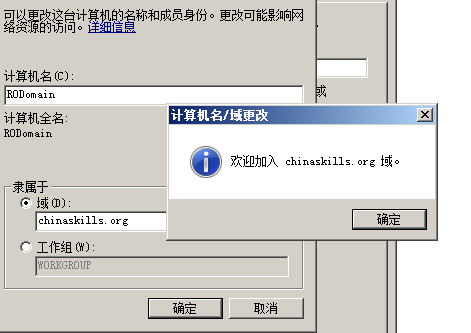
1. 安装虚拟机“Win2008-B2”， 其内存为512M，硬盘20G，将服务器加入至Windows域中；

****



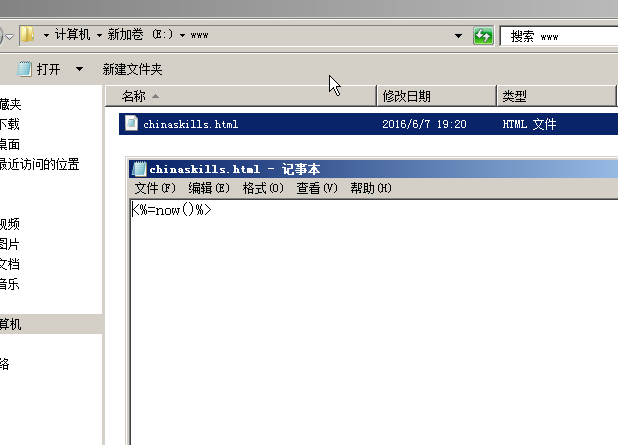
**（二）在主机Win2008-B1中完成RODC的部署**

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）**



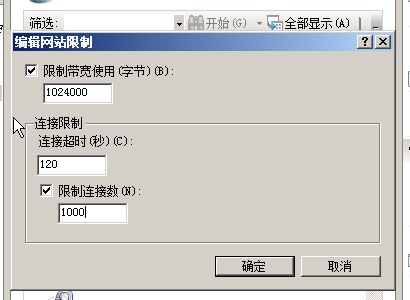
**（三）在主机Win2008-B2中完成web及DFS服务器的部署**

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；

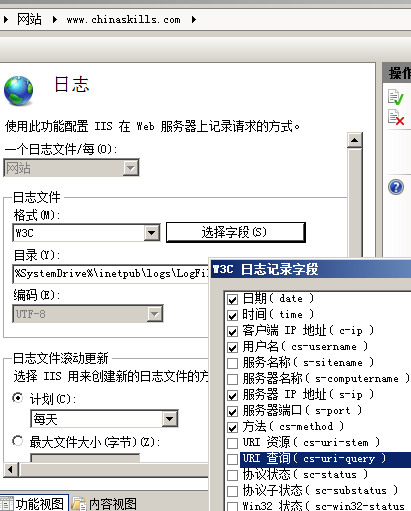


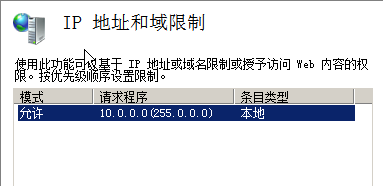


1. 设置网站的最大连接数为1000，网站连接超时为120s，网站的带宽为1000KB/S，使用W3C记录日志；禁用父路径；每天创建一个新的日志文件，使用当地时间作为日志文件名；日志只允许记录日期、时间、客户端IP地址、用户名、服务器IP地址、服务器端口号和方法；设置IP列表只允许IP为10.0.0.0/255.0.0.0的用户访问。

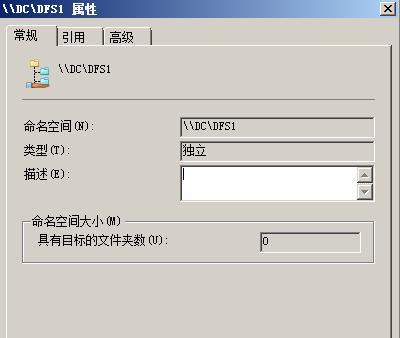


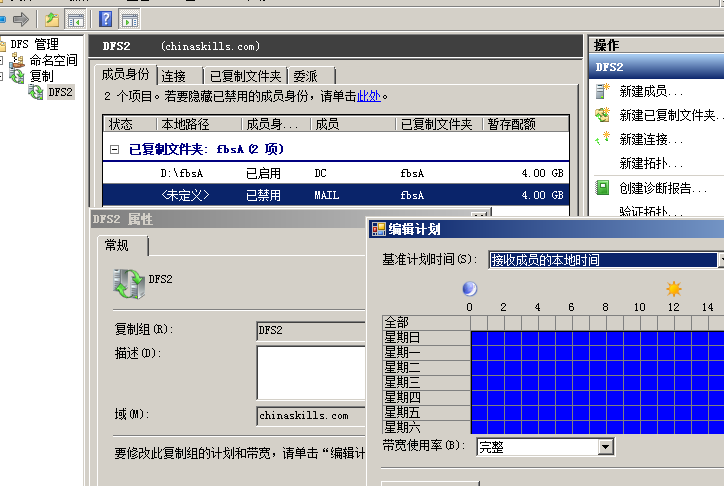
9





1. 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；



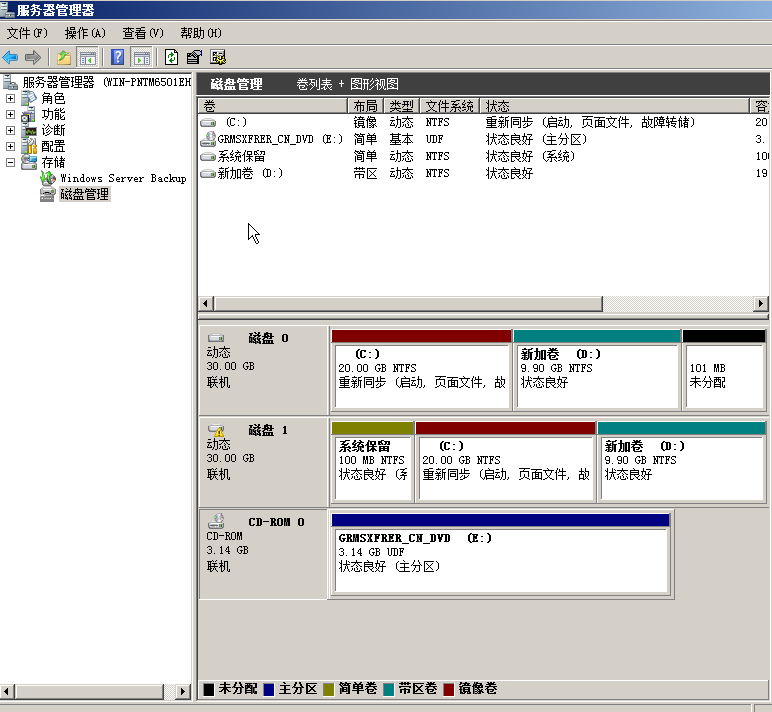


**三、在PC3上完成如下操作:**

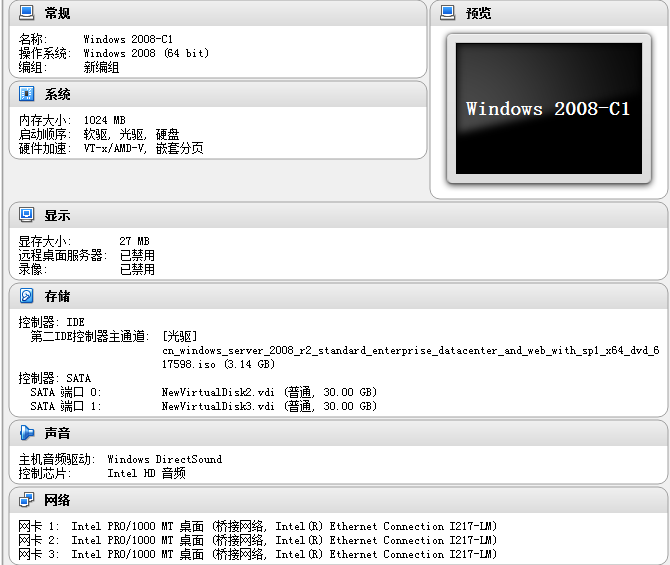
**（一）完成虚拟主机的创建**

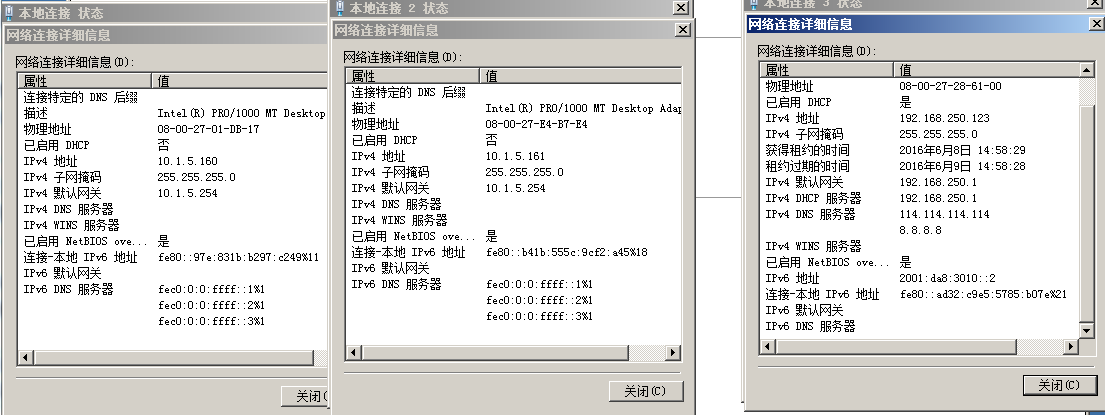
1、安装虚拟机“Win2008-C1”，其内存为1G，系统有两个30G的硬盘，系统分区使用20G，**需要支持容错功能。其余为数据分区，要提高分区的访问速度。**





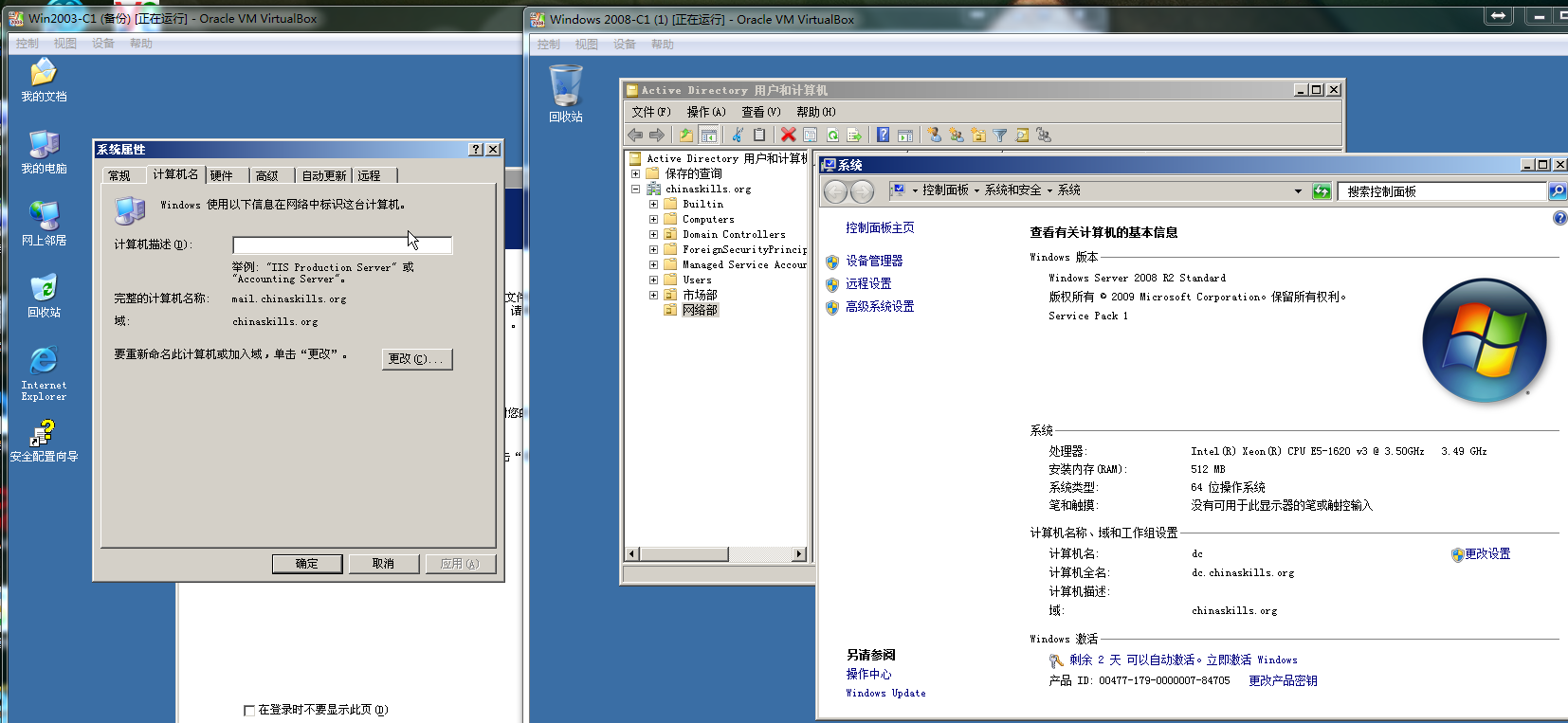
1. 在虚拟机“Win2008-C1”中配置三个网卡，IP地址如表所示。并将服务器加入到Windows域环境；；





（二）完成域的升级和迁移

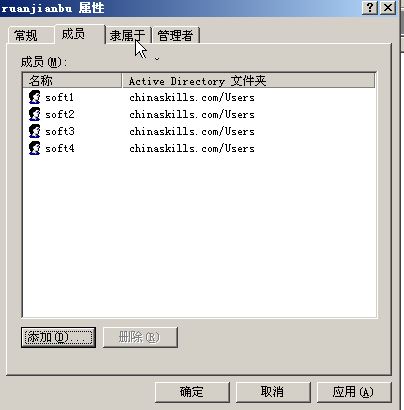
1、将标识为“PC3”的计算机上的已有虚拟机Win2003-C1启动。对其进行滚动升级，将原用chinaskills.org域的域控制器Win2003-C1升级到新安装的Windows Server 2008服务器Win2008-C1。

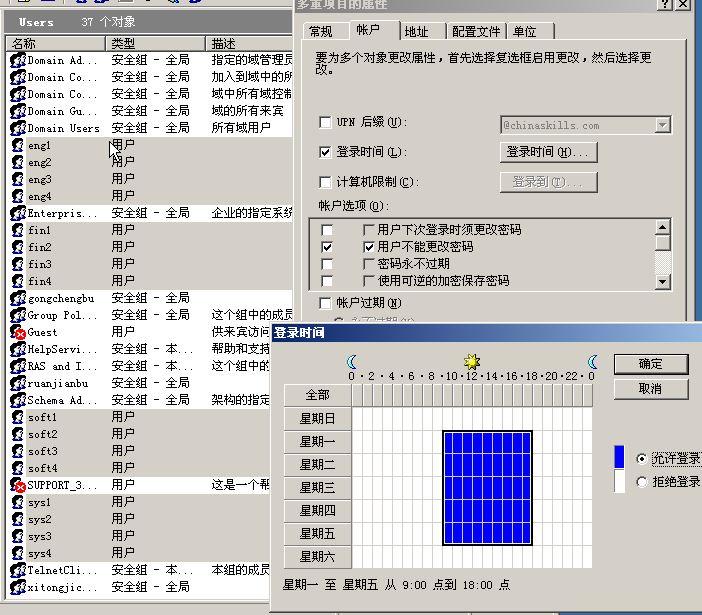


1. 将已有虚拟机Win2003-C1的DHCP服务和DNS服务迁移到Win2008-C1服务器上。

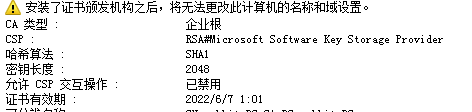
（三）在主机Win2008-C1上完成域控制器的基本配置

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。；



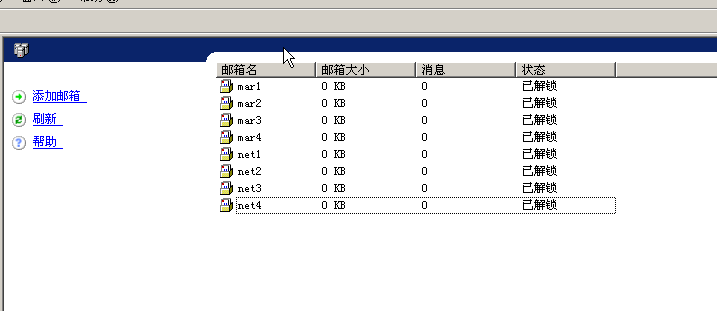


1. 安装证书服务，设置为企业根，有效期为6年，为企业内部自动回复证书申请；

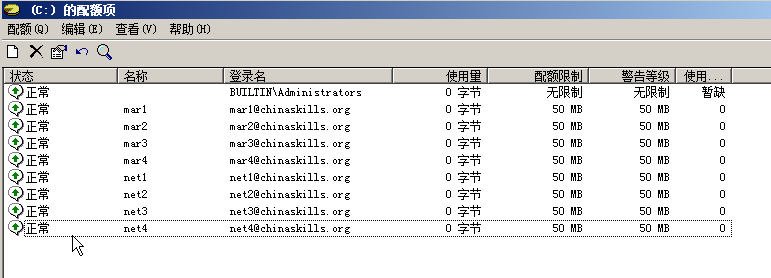


1. **在主机Win2003-C1中完成E-MAIL服务器的部署**

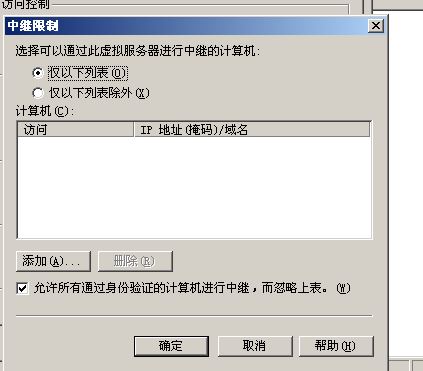
1、安装E-mail服务，采用Active Directory集成的身份验证方式为内网市场部和网络部的用户创建邮箱；

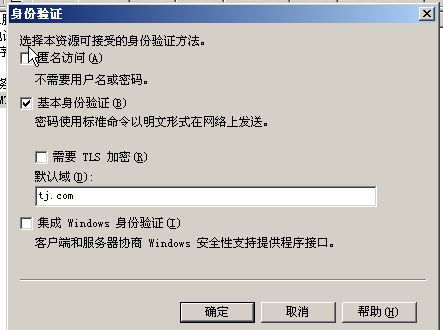


1. 限定市场部和网络部每个用户的邮箱大小为50MB；

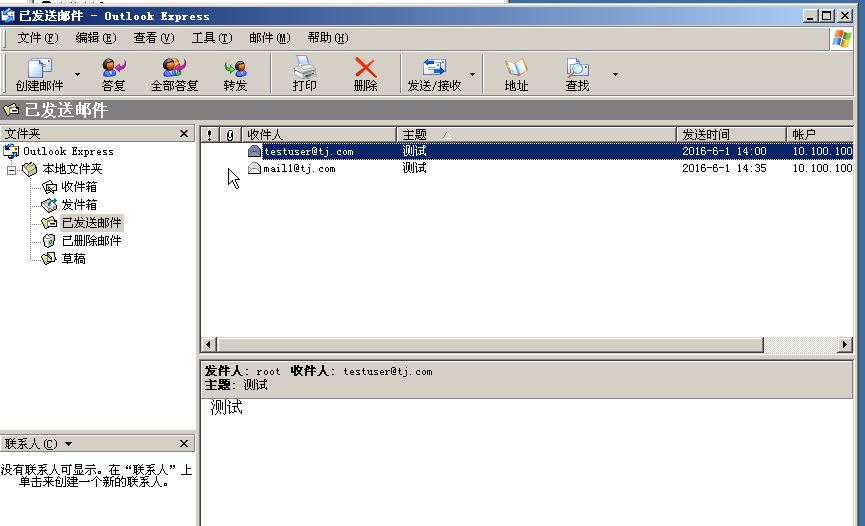


1. 完成对smtp服务的配置，只允许通过验证的用户进行中继，身份验证使用基本认证方式；





1. 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；

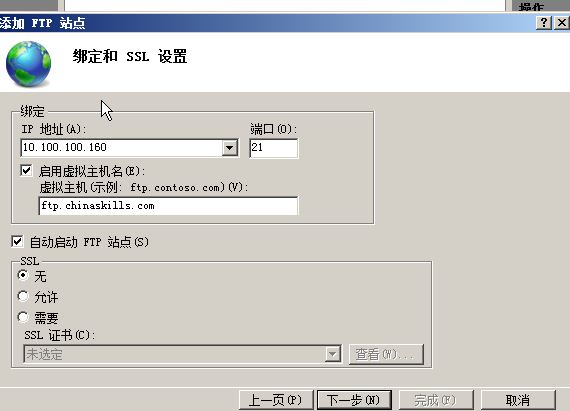


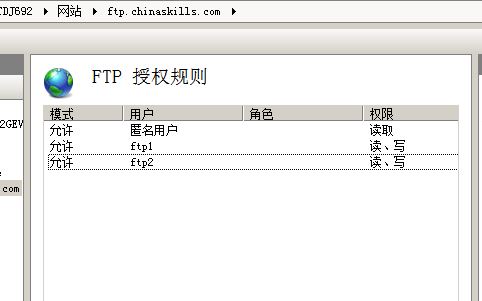
**（五）在主机Win2003-C1中完成FTP服务器的部署**

1、安装FTP服务。

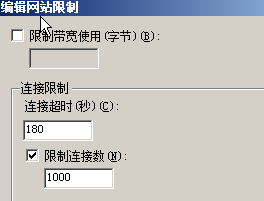
2、使用隔离用户创建名为ftp.chinaskills.com的FTP站点，FTP主目录为c:\inetpub\ftproot。使用ftp.chinaskills.com可访问该FTP站点。域用户ftp1、ftp2及匿名用户均可登录，但匿名用户权限只读，ftp1,ftp2可以读写。

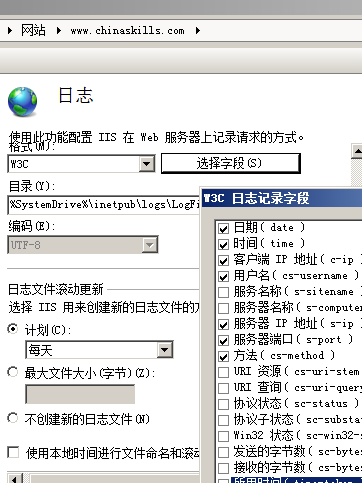






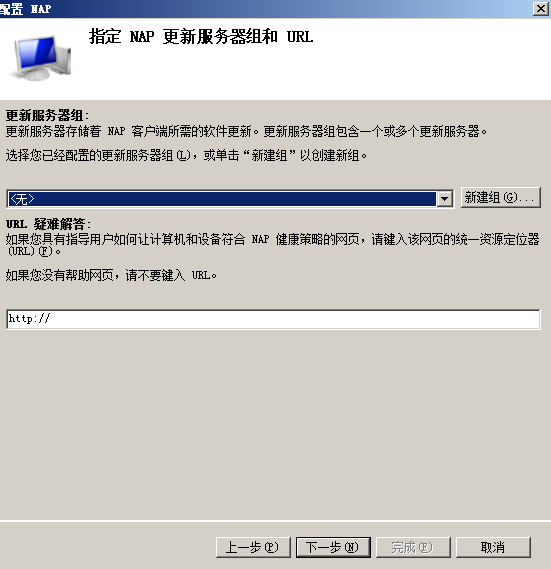
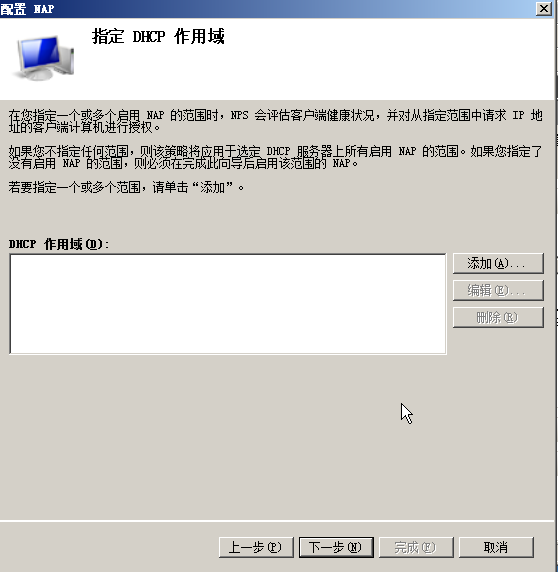
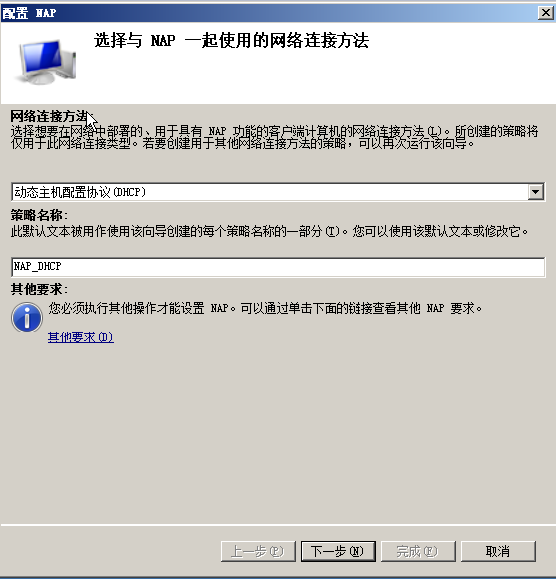
3、限制站点的最大连接数为1000，连接超时180s；使用W3C记录日志；每天创建一个新的日志文件，使用当地时间作为日志文件名；日志只允许记录日期、时间、客户端IP地址、用户名、服务器IP地址、服务器端口号和方法。

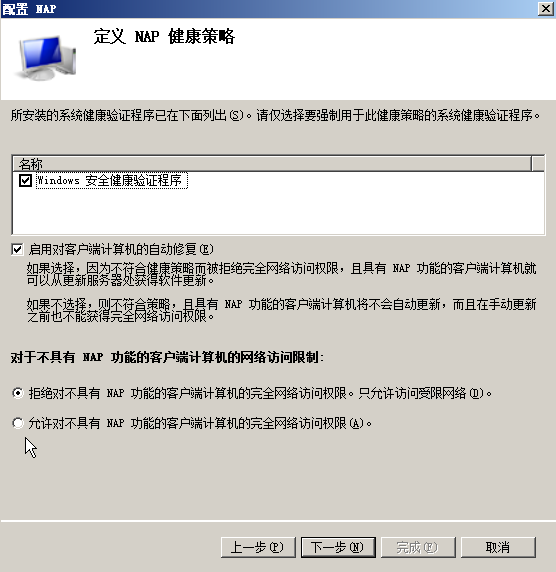




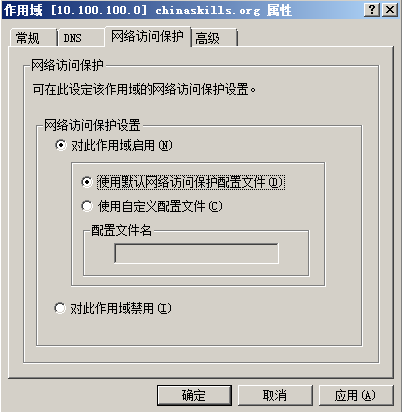
**（六）在主机Win2008-C1中完成NAP服务器的部署**

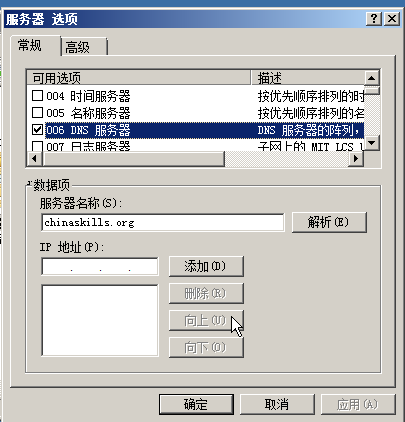
1. 将**Win2008-C1**配置成为网络访问策略的服务器（NPS）。将DHCP设置为与NAP一起使用的网络连接方法，策略名称为NAP\_DHCP。NAP应用于DHCP上所有的作用域和域中的所有用户。不使用跟新服务器组。启动客户端计算机自动更新，拒绝对不具有NAP功能的客户端计算机完全访问网络，只允许访问受限网络。

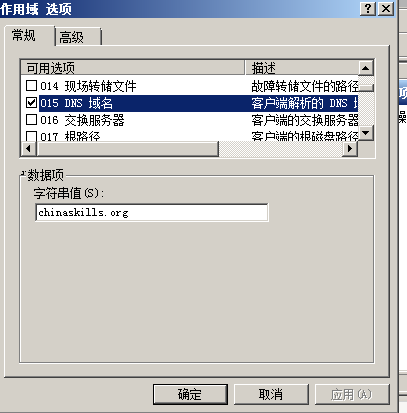


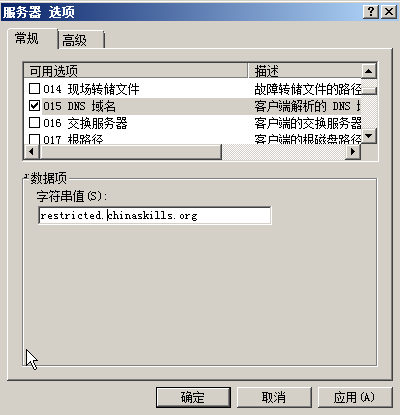


1. 修改DHCP服务设定，对chinaskills.org域启用网络访问保护。默认用户通过检查后可以完全访问网络的客户端获取的DNS域名为chinaskills.org。默认的访问保护级别的用户获取的DNS域名为restricted. chinaskills.org。

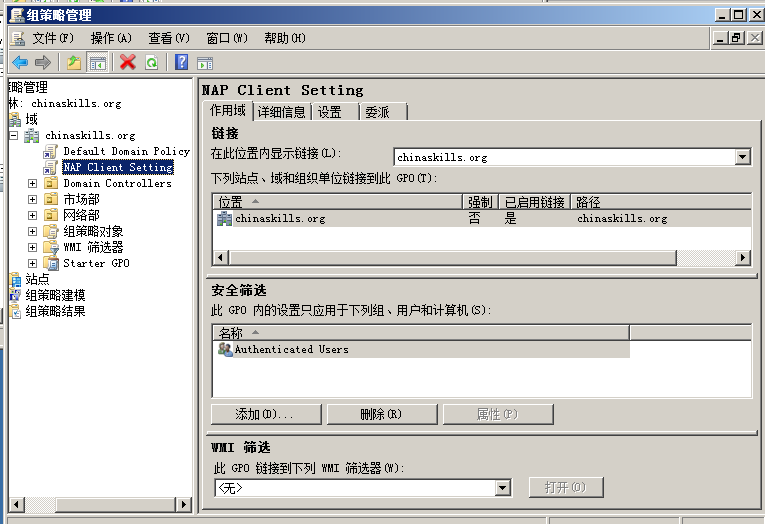




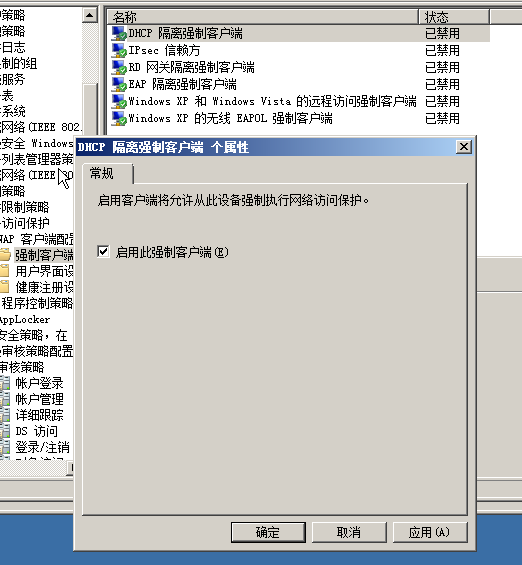


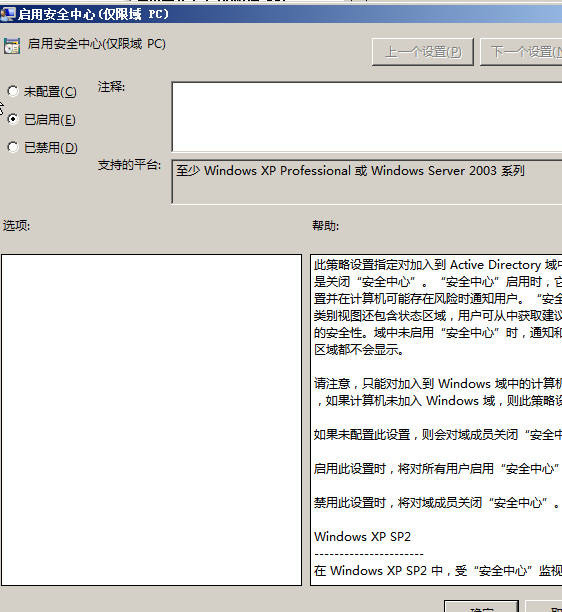


1. 在**Win2008-C1**中创建chinaskills.org域的组策略对象，命名为“NAP Client Setting”。



1. 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。

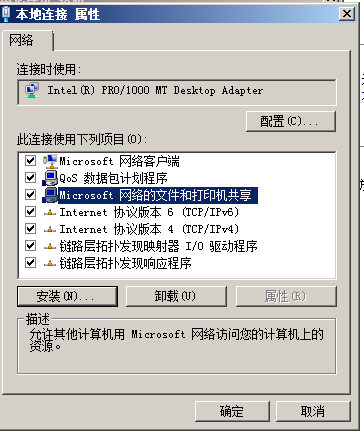




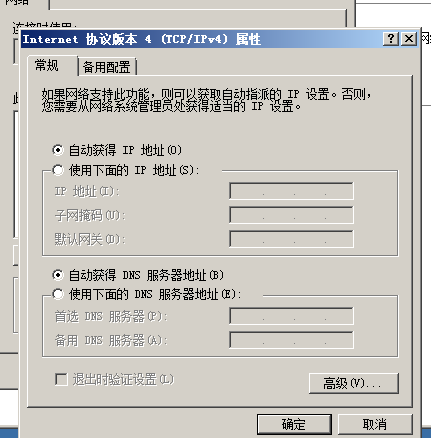
1. 删除NAP Client Setting策略安全筛选中原有的内容，添加NAP Client Computers。



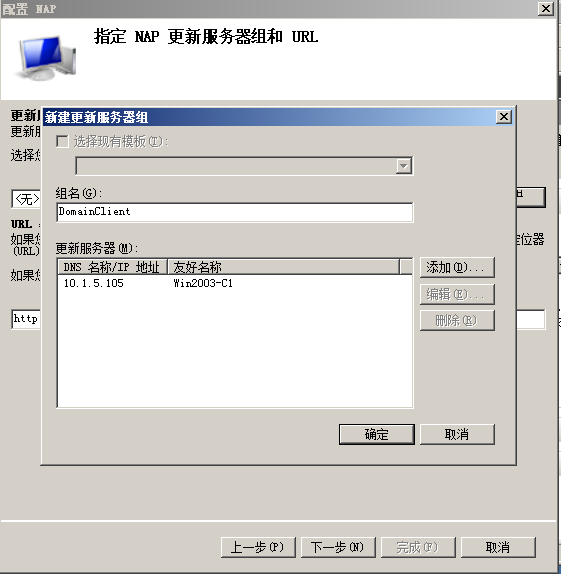
1. 在**Win2008-C1**中启动网络共享和文件发现功能。



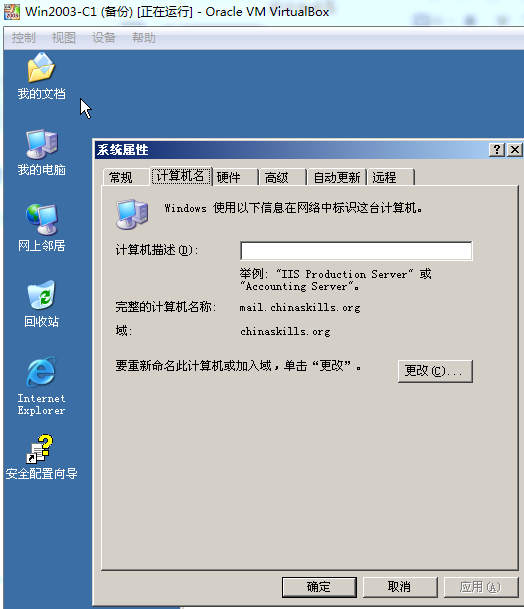
1. 将Win2003-C1的网卡设置为自动获取IP地址。

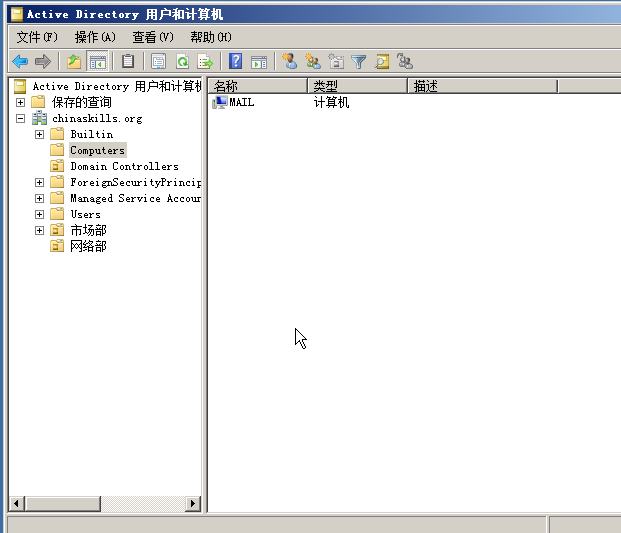


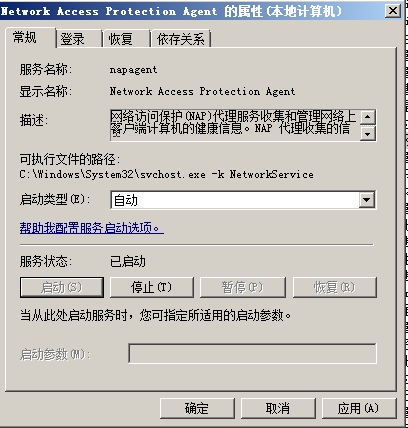
1. 修改**Win2008-C1**中的网络策略，在DHCP不支持NAP情况下，添加NAP强制更新服务器组，组名DomainClient，将Win2003-C1获取的IP作为组中的好友。



1. 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。







**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。

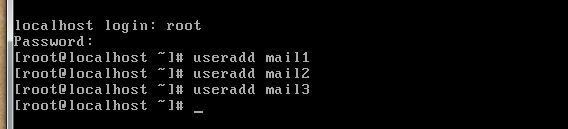
**一、在PC1上完成如下操作:**

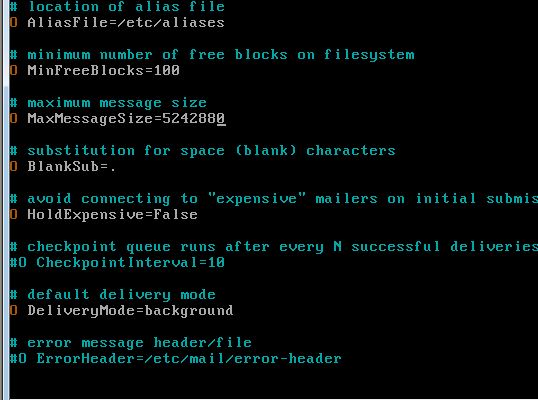
**（一）完成虚拟主机的创建**

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。

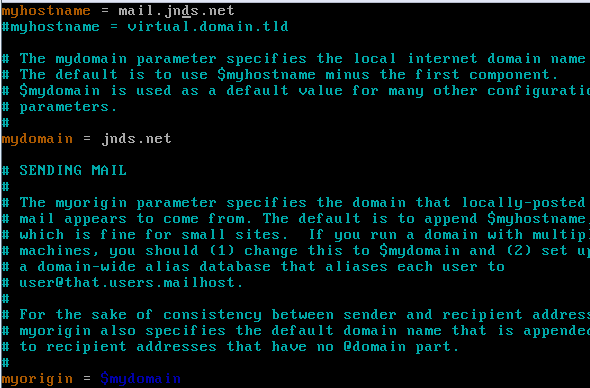
**（二）在主机Centos-A1中完成E-MAIL服务器的部署**

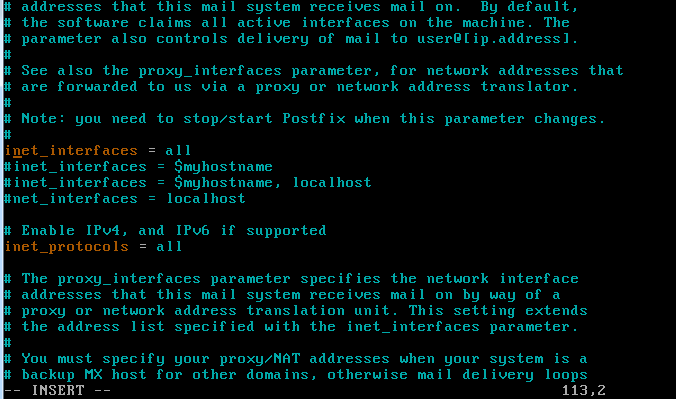
1、在此服务器上配置基于SMTP认证的postfix邮件服务，创建创建三个用户mail1,mail2,mail3；每个用户的邮箱大小为20MB，限定用户发邮件时，附件大小为5MB；





1. 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；

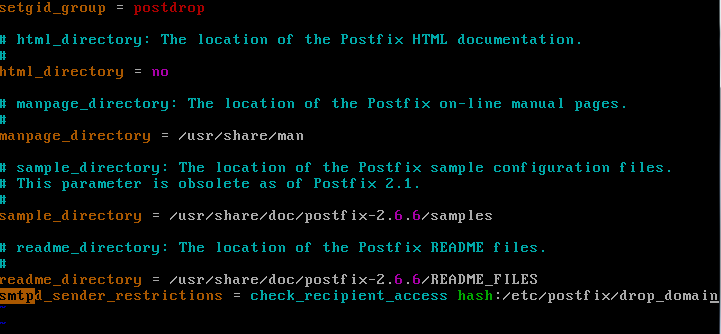




3、设置postfix服务需要运行级别3和5级别开机自动启动，其它运行级别必须为关闭；



1. 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。

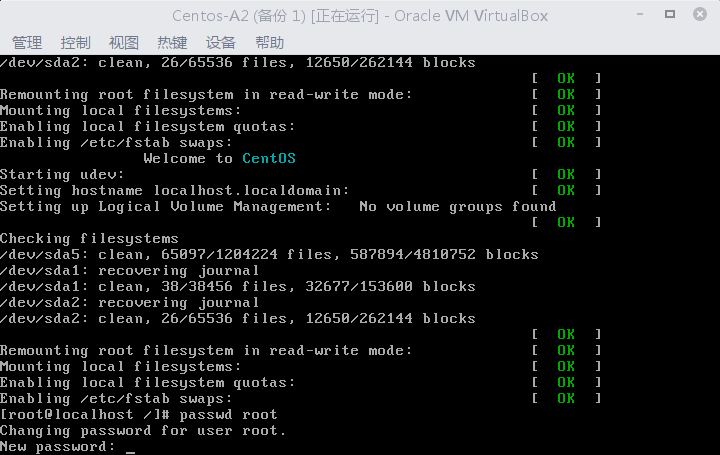




**（三）在主机Centos-A2中完成密码的清除和yum的部署**

**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。

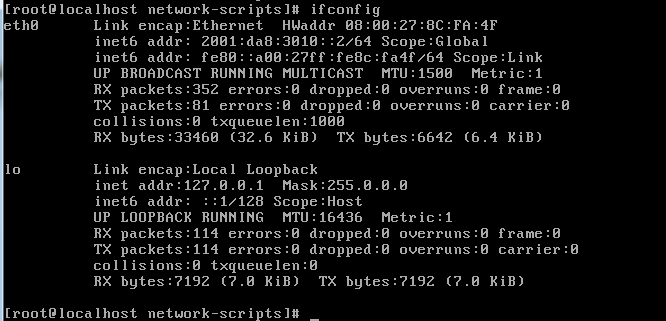
1. 将标识为“PC1”的计算机上的已有虚拟机Centos-A2启动，请破解Root的密码，并将新密码设置为nvsc.com；



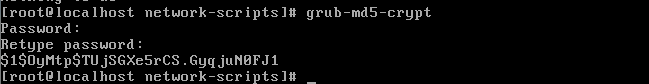
1. 配置Centos-A2的yum，并通过yum安装setup工具包，截图为yum；

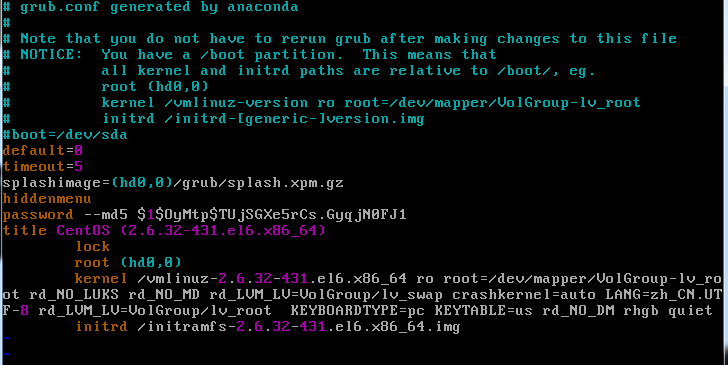


1. 配置Centos-A2的IPv6地址为：2001:DA8:3010::2/64，截图为ipv6；



1. 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；





**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；



1. 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();

?>。



1. 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。



1. 配置使得用户只能使用域名访问网站，不能使用ip地址。

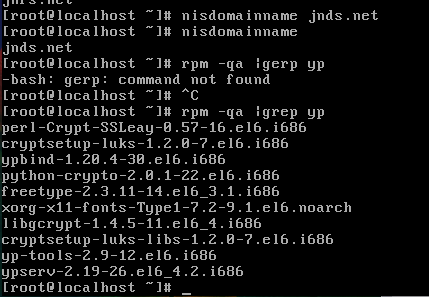


1. 将/home目录打包并压缩成gzip格式，文件名为var.tar.gz，保存到/tmp目录下。

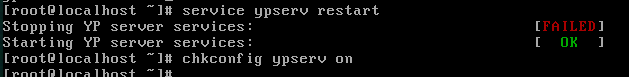


**（三）在主机Centos-B1中完成NIS客户端的部署**

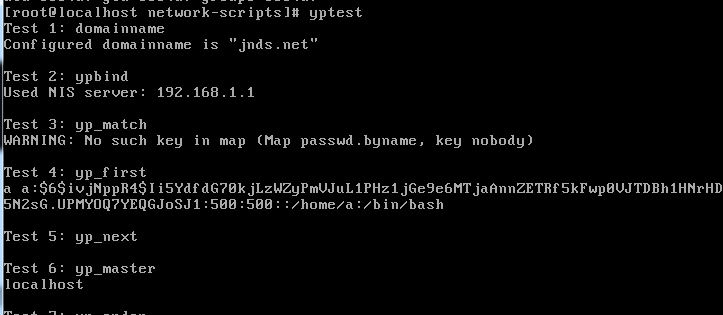
1、安装NIS服务，设置NIS域名为jnds.net，指定通过NIS进行身份认证。



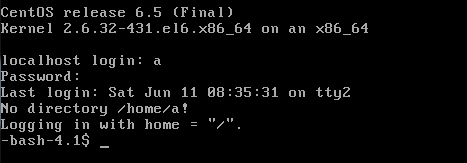
1. 启动服务，并设置开机自动启动。



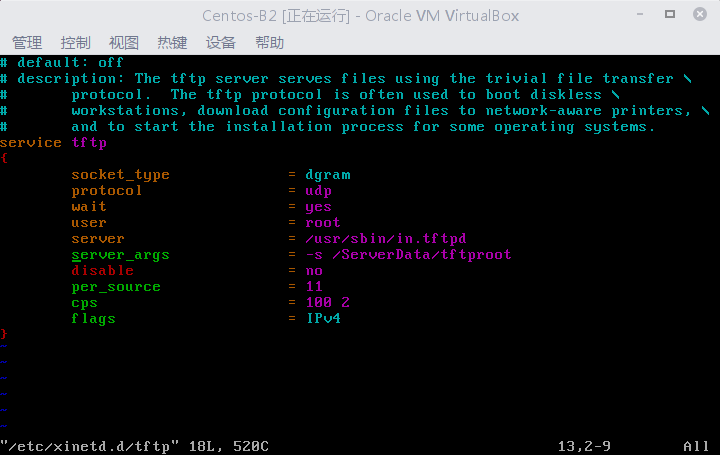
1. 使用yptest进行测试，将测试结果截图为yptest。



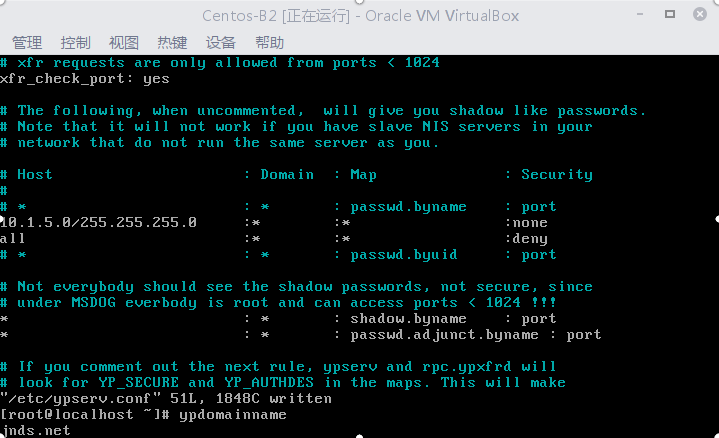
4、使用用户a登录，要求显示登录成功的界面，并截图为suc。



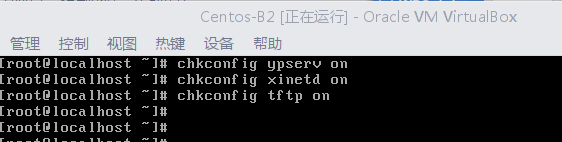
**（四）在主机Centos-B2中完成TFTP和NIS服务器的部署(20分)**

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

1. 安装NIS服务，设置NIS域名为jnds.net，只允许本网段可以访问。



1. 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。

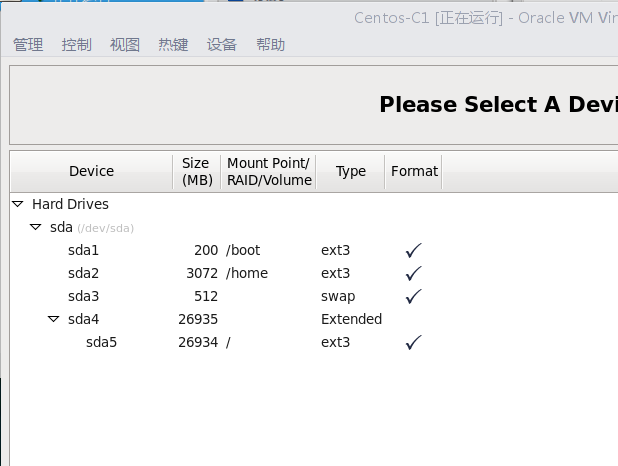


1. **在PC 3上完成如下操作：**

**（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。





1. 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**

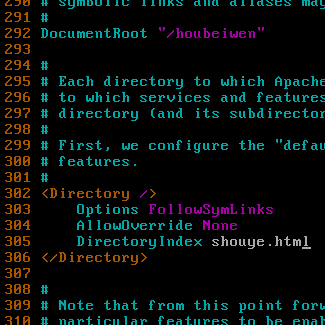
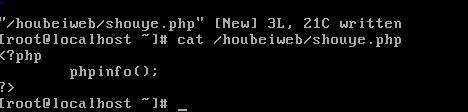
1、在Centos-C1上搭建WEB服务器。站点根目录在/houbeiweb，首页文件命名为shouye.php，内容为

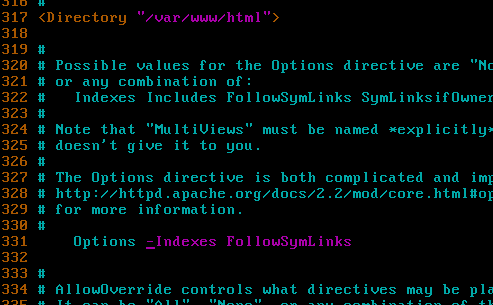
<?php

phpinfo();

?>。

，修改配置文件禁止目录浏览。

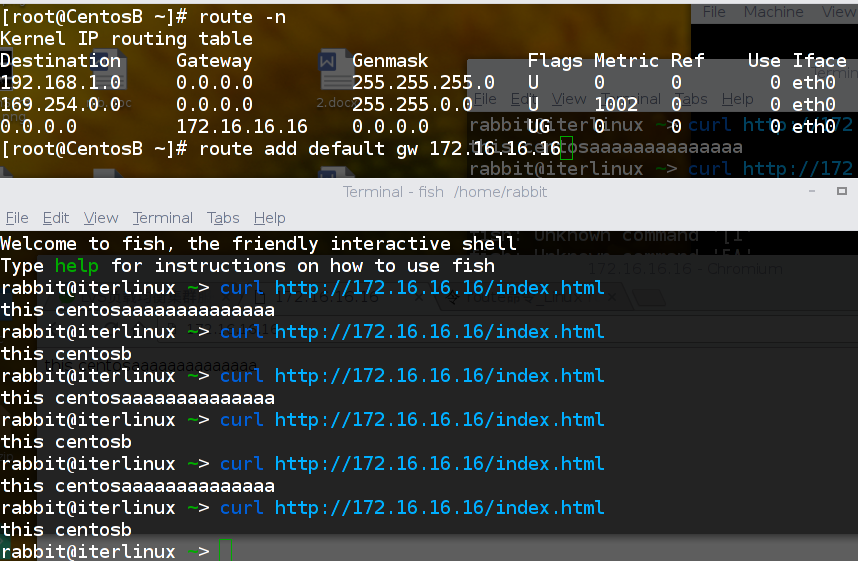




1. 借助自签名证书完成web服务的配置，结合ssl实现安全传输，复制一个CA服务器认证证书, 在win7-D1安装此证书，实现安全的访问；

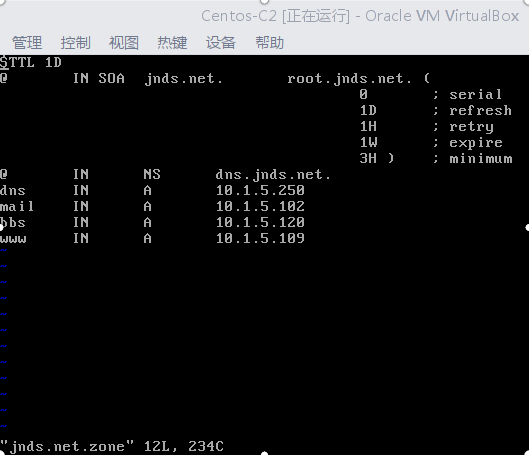


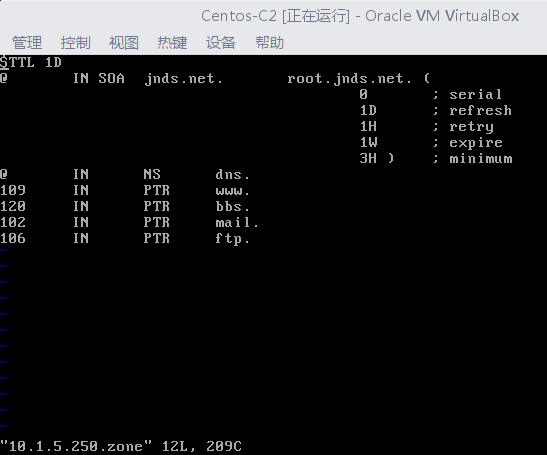
1. 将**Centos-B1**与Centos-C1提供负载平衡的Web服务。其中虚拟地址为10.10.100.250/24，**Centos-B1**作为均衡管理主机。将**Centos-B1**设置完成IP地址的界面截屏保存命名为3-1，将Centos-C1设置完成IP地址的界面截屏保存为3-2。(有文档，类似这张图。按文档做)



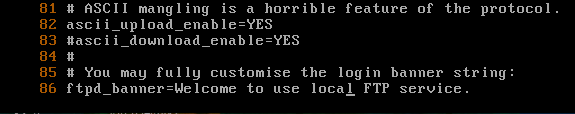
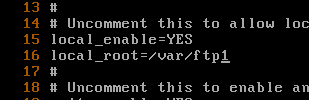
**（三）在主机Centos-C2中完成bind、 FTP服务器的部署**

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](http://www.jnds.net)、bbs.jnds.net、ftp.jnds.net以及mail.jnds.net,做好正反向DNS服务解析；



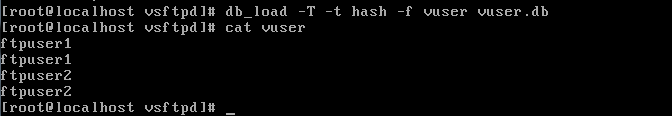


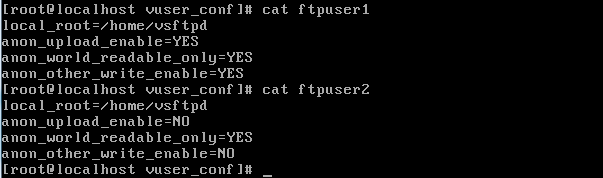
1. 配置FTP服务，创设FTP服务站点，域名为[ftp.jnds.net](ftp://ftp.jnds.net)，站点主目录分别为 /var/ftp1，登录后显示banner文字说明为“欢迎使用本ftp服务器”，开启ASCII 模式上传数据；



1. 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；







1. **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；

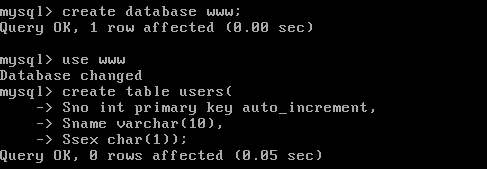
1. 开启系统防火墙，只对该系统服务的端口进行监听，截图为4-1；

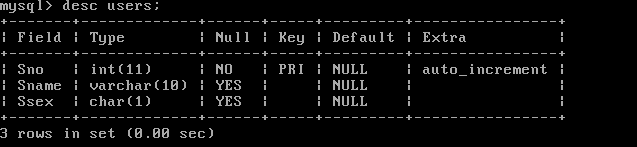


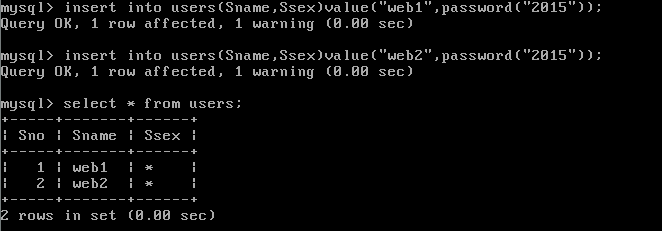
**（二）在主机Cent**OS**-D1中完成MySQL数据库服务器的部署**

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 |







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]。

