**windows服务器管理学习要点注意事项**

**1. Windows Server 2012 R2服务器安装与配置**

要求：掌握网络操作系统的定义，功能，了解常见网络操作系统。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 性能 | Foundation | Essentials | Standard | Datacenter |
| 处理器（CPU）上限 | 1 | 2 | 64 | 64 |
| 授权用户限制 | 1 | 25 | 无限 | 无限 |
| 文件服务限制 | 1个独立DFS根目录 | 1个独立DFS根目录 | 无限 | 无限 |
| 网络策略和访问控制 | 50个RRAS连接以及1个IAS连接 | 250个RRAS连接、50个IAS连级以及2个IAS服务组 | 无限 | 无限 |
| 远程桌面服务限制 | 20个连接 | 250个连接 | 无限 | 无限 |
| 虚拟化 | 无 | 1个虚拟机或者物理服务器，两者不能同时存在 | 2个虚拟机 | 无限 |
| 服务器核心模式 | 无 | 无 | 有 | 有 |
| Hyper-V | 无 | 无 | 有 | 有 |

安装注意事项：选择带GUI的服务。

基本配置：

更改计算机名和工作组的步骤：单击任务栏左下角的“服务器管理器”图标，打开“服务器管理器”窗口，单击窗口左侧“本地服务器”，单击右侧“本地服务器属性”窗口中“计算机名”后面的默认计算机名“WIN-EJERBD8B3JE”打开“计算机名/域更改”窗口，输入计算机名单击“确定”按钮。按照提示重新启动计算后，这些更改才会生效。

在Windows Server 2012 R2中配置TCP/IP协议的步骤如下：

（1）依次选择“开始控制面板查看网络状态和任务更改适配器设置单击“Ethernet0（以太网）”选项，即可打开“Ethernet0（以太网）状态”对话框；

（2）单击“属性”按钮，打开“本地连接Ethernet0（以太网）属性”对话框，如果服务器安装有多块网卡应当分别选择并一一进行设置。

（3）在“此连接使用下列项目”列表框中选中“Internet协议版本4（TCP/IPv4）”选项，单击“属性”按钮，打开“Internet协议版本4（TCP/IPv4）属性”对话框。可以选择“自动获取IP地址”或用户指定IP地址，对于DNS服务器也可以选择自动获取或由用户指定。

（4）选中“使用下面的IP地址”单选按钮，分别输入为该服务器分配的IP地址（在这里输入192.168.100.100）、子网掩码（在这里输入255.255.255.0）和默认网关（在这里输入192.168.100.1），并指定DNS服务器的IP地址（在这里输入：首选DNS：192.168.100.100）。

（5）单击“确定”按钮，保存所作的修改。

在Windows Server 2012 R2中，可以为每块网卡设置多个IP地址，在“Internet协议（TCP/IP）属性”对话框中，单击 “高级”按钮，打开“高级TCP/IP 设置”对话框，单击“IP地址”框下方的“添加”按钮，弹出“TCP/IP地址”对话框，添加IP地址（如IP地址为192.168.100.101，子网掩码为255.255.255.0），添加完后单击“添加”按钮，既可为网卡设置第二个IP地址。

应用测试命令验证网络连接：

（1）在桌面上，单击“开始运行”命令，打开“运行”对话框，在“打开”文本框中输入cmd命令。单击“确定”按钮，打开“命令提示符”窗口。

（2）在命令提示符后输入ipconfig/all命令，按下回车键，即可查看当前TCP/IP的配置信息。

（3）在命令提示符后输入ping 192.168.100.1命令，按下回车键，测试当前计算机和10.8.25.101之间的网络是否能够正常通信。

启用与关闭Windows防火墙：

系统默认已经启用Windows防火墙，它会阻挡其他计算机与此台计算机通信。启用与关闭Windows防火墙步骤：单击“开始”菜单->“控制面板”->“系统和网络安全”->“Windows防火墙”­->“启用或关闭Windows防火墙”-> “自定义设置”进行设置即可。

Windows防火墙会阻挡所有的传入连接，不过可以通过单击如图1.32左上方的“允许应用或功能通过Windows防火墙”命令，打开 “允许的应用”窗口来解除对某些程序的封锁。

如果要进一步设置Windows防火墙的规则，可以通过“高级安全Windows防火墙”设置。单击左侧的“高级设置”命令，打开 “高级安全Windows防火墙”窗口。高级安全Windows防火墙设置可以同时针对传入连接与传出连接来设置访问规则（图中的“入站规则”与“出站规则”）。

例如实验项目一中windows server2012可以ping通windows server2003，而03ping12时收不到ICMP回答报文，则需要在windows server2012入站规则中开启ICMP回答报文。

创建MMC管理控制台：

步骤1：在服务器桌面单击【开始】→【运行】→输入“mmc”命令→【确定】→打开MMC控制台。

步骤2：在菜单栏单击【文件】→【添加/删除管理单元】→【添加】。

步骤3：在打开的【可用的独立管理单元】列表框中选定需要的管理单元→【添加】。

步骤4：在打开的“选择计算机”对话框中选择要管理的计算机，若管理本地的计算机，单击“这台计算机”；若管理单元指向远程计算机，则单击“以下计算机”，并输入该项目管理的计算机的名称→【完成】。

步骤5：返回，继续添加其他管理单元，添加完后单击【关闭】，返回【可用的独立管理单元】对话框→单击【确定】。

步骤6：返回MMC控制台，在菜单栏单击【文件】→【保存】→确定控制台保存的位置（如：桌面、“开始”菜单或“管理工具”中）→输入控制台名称（如：我的控制台）→单击【确定】。

步骤7：如果要删除管理单元，可以先选择要删除的管理单元，然后单击【删除】按钮。

**2.磁盘管理**

基本磁盘规定一块硬盘最多可以创建四个分区，可以是4个主分区或最多三个主磁盘分区加上一个扩展分区。一块硬盘至少要有一个主分区；最多只能有一个扩展分区。Windows 操作系统一般建议安装在主分区上。在扩展分区内可以创建多个逻辑分区（逻辑驱动器）。

动态磁盘支持多种类型的动态卷，它们之中有的可以提高访问效率、有的可以提供除错功能、有的可以扩大磁盘的使用空间，这些卷包含简单卷（simple volume）、跨区卷（spanned volume）、带区卷（striped volume）、镜像卷（mirrored volume）和 RAID-5（RAID-5 volume）。其中简单卷为动态磁盘的基本单位，其他4中分别具备不同特性。



FAT和NTFS文件系统的转换

如果需要将文件系统由原来的FAT32格式转换为NTFS格式，并且不希望数据丢失，可以利用命令“convert 盘符/FS:NTFS”，就可以将特定分区由FAT32转换为BTFS。

例如，将F盘由FAT32格式转换为NTFS格式，命令为：

**convert F:/FS:NTFS**

在此注意正确输入卷标。

项目具体实施，各种卷的创建详见课件。

**3.本地用户和组**

Windows Server 2012支持两种用户账户：本地账户和域账户。

Windows Server 2012在系统安装完成时，就提供了两个内置账户供使用，分别是Administrator和Guest。

用户通过帐户名和密码来登录系统，因此，创建用户账户要遵循账户命名规则。

帐户名必须唯一：本地帐户必须在本地计算机上唯一，不区分大小写。

帐户名不能包含以下字符：?+\*/\[]=<>等特殊字符。

帐户名最长不能超过20个字符，输入时可超过20个字符，但只识别前20个。

不能与用户组的组名相同。

在Windows Server 2012系统中，系统会为每一个用户帐户建立一个惟一的安全标识码（Security Identifier，SID），Windows Server 2012系统都是利用这个SID来代表该用户，有关的权限设置等都是通过SID来设置的，而不是利用用户的账户名称。

查看当前用户账户的SID，可以使用如下命令：

whoami /logonid

系统默认账户密码要符合复杂性要求，具体如下：

请勿包含使用者账户名称的全部或任何超过两个字符的部分。

密码最多可由128个字符组成，推荐最小长度为6个字符。

包含下列四种字符中的三种：

英文大写字符 (A 到 Z)。

英文小写字符 (a 到 z)。

10 进位数字 (0 到 9)。

非英文字母字符 (例如 !、$、#、%)、扩充型 ASCII、符号或语音字符。

本地用户账户和组的创建过程详见课件。

**4.文件系统与共享资源管理**

用户对磁盘内的文件和文件夹拥有适当的权限后，才可以访问这些资源。通过对Windows Server 2012 文件系统的管理，理解NTFS和FAT32文件系统的区别，理解文件和文件夹权限与共享权限的区别，掌握使用NTFS控制资源访问的方法和设置共享资源和访问共享资源的方法。

**FAT、FAT32、NTFS是目前Windows系统中最常见的三种文件系统**。只有在NTFS格式的磁盘可以设置NTFS权限，FAT16和FAT32格式的磁盘上不能使用NTFS权限。

分配文件权限：管理员创建张三用户，创建文件file1.txt，管理员设置zhangsan对file1.txt只具有读取的权限，并阻断继承权，然后以zhangsan的身份登录，发现zhangsan对此文件只具有读取权限。

给用户分配文件夹权限步骤：鼠标右键单击要设权限的文件夹->属性->安全标签。之后的步骤和分配文件的步骤雷同。

注意：首先，只有Administrators组内的成员、文件/文件夹的所有者、具备完全控制权限的用户，才有权限为其他用户来分配这个文件/文件夹的权限。

其次，文件/文件夹从父项继承来的权限，不能直接将其灰色对勾删除，仅仅可以增加勾选。如果要修改继承权限，则需先删除继承。删除继承的步骤：单击 “高级”按钮，单击随后打开的对话框的左下方底部的“禁用继承”按钮，即可断开文件夹的继承。单击 “高级”按钮，单击随后打开的对话框的左下方底部的“禁用继承”按钮，即可断开文件的继承。

Windows中任何一个对象都有所有者，所有者与其他权限是彻底分开的。对象的所有者拥有一项特殊的能力即更改对象的权限设置。

默认情况下，创建文件和文件夹的用户是该文件和文件夹的所有者，拥有对象的所有权。除了用户自行新建的对象外，Windows Server 2012 R2中其他对象的所有者都是本地Administrator组的成员。

Administrator组的成员可以取得系统中任意对象的所有权，这是操作系统为了管理的需要，而给予管理员组成员的特权。

权限的累加规则：

实际演示：

1、创建“销售部”和“技术支持部”组和“zhangsan”用户；

2、设置zhangsan属于两组成员；

3、设置zhangsan对zsfile2.txt有写入的权限，阻断继承权。

4、注销以zhangsan进入，验证张三对zsfile2.txt的权限情况。

5、注销以Administrator进入，设置技术部和销售部对zsfile2.txt文件的权限分别为读取，读取和运行。

6、注销以zhangsan进入，验证张三对zsfile2.txt的权限情况。

权限的拒绝规则：

1、创建“销售部”和“技术支持部”组和“zhangsan”用户；

2、设置zhangsanm属于两组成员；

3、设置zhangsan对zsfile3.txt有写入的权限；阻断继承权。

4、注销以zhangsan进入，验证张三对zsfile3.txt的权限情况。

5、注销以Administrator进入，设置技术部和销售部对zsfile3.txt文件的权限分别为拒绝写入，读取。

6、注销以zhangsan进入，验证张三对zsfile3.txt的权限情况。

权限的继承规则：

1、在E盘新建TEST文件夹，在TEST文件夹中建立file1.txt~file5.txt;

2、对用户zhangsan 设置对TEST文件夹设置“读取和运行+读取”权限；

3、删除其它用户和组对该文件的权限；

4、注销以zhangsan进入，对TEST文件夹下的文件进行操作，查看结果。

5、注销以administrator进入，取消“file1.txt”的继承权，然后设置zhangsan对其file1.txt文件具有“读取和运行+读取+写入” 的权限。

6、注销以zhangsan进入，对TEST文件夹下的文件进行操作，查看结果并作比较。

权限的优先规则：

1、在E盘新建TEST文件夹，在TEST文件夹中建立file1.txt~file3.txt;

2、设置zhangsan对文件夹E:/TEST 有“读取”权限；

3、设置zhangsan对文件夹E:/TEST/file3.txt 有“修改”权限；

4、注销以zhangsan进入，查看张三对file4.txt最终有效权限是？

移动和复制操作对权限操作的影响：

① 在同一个分区内移动文件或文件夹时，此文件和文件夹会保留在原位置的一切NTFS权限；在不同的NTFS分区之间移动文件或文件夹时，文件或文件夹会继承目的分区中文件夹的权限。

② 在同一个分区内复制文件或文件夹时，文件和文件夹会继承目的位置中的文件夹的NTFS权限；在不同的NTFS分区之间复制文件或文件夹时，文件或文件夹将继承目的位置中文件夹的权限。

③ 当从NTFS分区向FAT分区中复制或移动文件和文件夹都将导致文件和文件夹的权限丢失。

位于NTFS、FAT32、FAT或exFAT磁盘内的文件夹，都可以被设置为共享文件夹，然后通过共享权限来设置网络用户的访问权限。

**共享权限只有三种：读取、更改和完全控制。**

新建共享文件夹：

步骤1：鼠标右键单击需要共享的文件夹->选择“共享”->选择“特定用户”；

步骤2：单击向下箭头选择要共享的用户或组（此处选择用户“zhangsan”）->单击“添加”按钮，则被选择的用户或组被添加到共享用户或组列表中，被选择的用户“张三”的默认共享权限为“读取”，如果要更改，单击用户右边向下的箭头，然后从显示的列表中进行选择，完成后单击“共享”按钮。

步骤3：如果此计算机的网络位置为“公用网络”，则出现对话框。选择是否要在所有公用网络启用网络发现和文件共享的对话框。如果选择“否”，此计算机的网络位置被更改为“专用网络”。

步骤4：出现“你的文件夹已共享”界面是单击“完成”按钮。

详细实施过程见课件。

**5.域的创建与管理**

**活动目录**

活动目录是Windows Server 2012系统中提供的目录服务，用于存储网络上各种对象的相关信息，以便于管理员查找和使用。特点：结构化的数据存储方法，通过登陆验证及目录中对象的访问控制将安全性集成到活动目录中。

**域控制器**是运行活动目录的Windows Server 2012服务器；成员服务器是运行Windows Server 2012的域成员服务器；**成员服务器**安装活动目录后即可成为域控制器。

Windows Server 2012更改计算机名为server1，Windows Server 2003更改计算机名为xcm-2，将Windows Server 2012升级为域控制器：

Windows Server 2012可通过添加角色和功能的方式来拥有服务器管理工具：

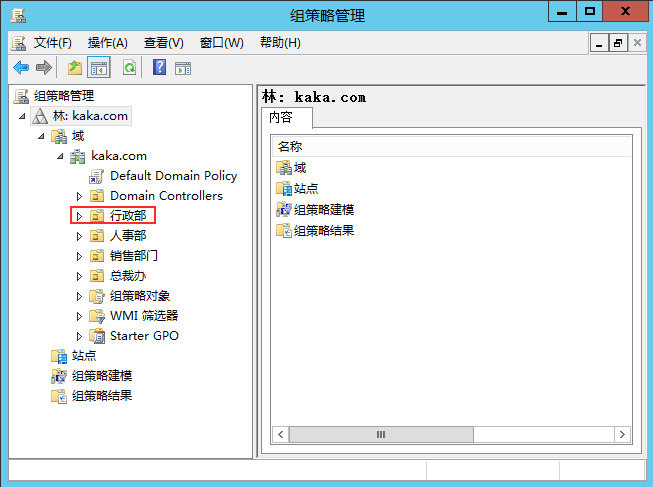
打开服务器管理器，单击添加角色和功能，持续单击下一步按钮，在选择功能界面中勾选DNS, AD，新建林，域名可为study.cn，先决条件检查时可能出出现一些情况，建议分情况搜索解决，比较常见的状况为administrator空密码不符合密码复杂性要求的问题，可在命令提示符窗口输入命令行：net user administrator /passwordreq:yes，然后给administrator设置一个符合要求的密码即可。

Windows Server2003确认设置正确的的DNS服务器，然后打开系统属性对话框，选择加入域“study.cn”，弹出需要身份认证的时候输入administrator及密码即可收到欢迎加入study.cn域的窗口。

至此域环境升级成功。

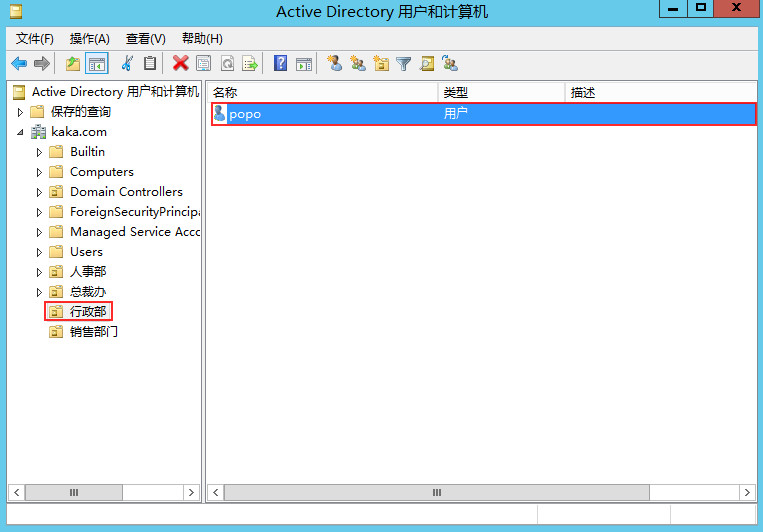
创建域用户和域组用户的实施过程详见课件。

域组策略：AD域的组策略添加有助于管理AD域中的用户使用的client端的环境。组策略依附于AD域的OU构成，使用“gpmc.msc”在运行里面打开，或者是在“开始—管理工具”里面打开，或者在仪表板管理中找到域组策略打开，在打开的组策略管理界面里面，林kaka下的DefaultDomain Policy为全局策略。如下图所示。

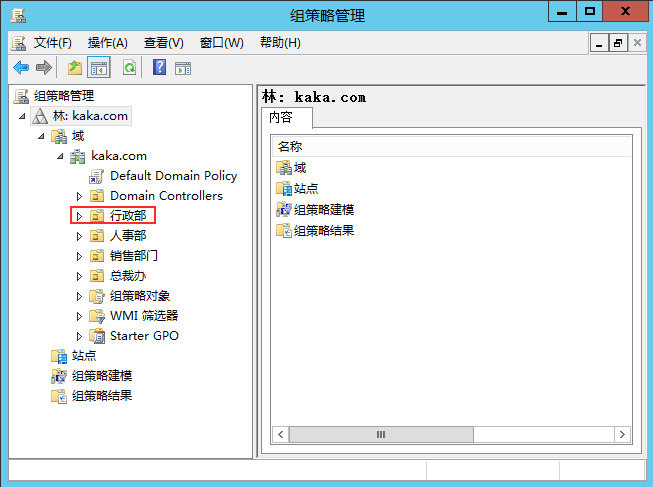


操作实例：简单组策略的建立实现，要求:更改行政部门的用户 popo 在登录后的浏览器主页锁定为：www.baidu.com,则实现步骤如下:

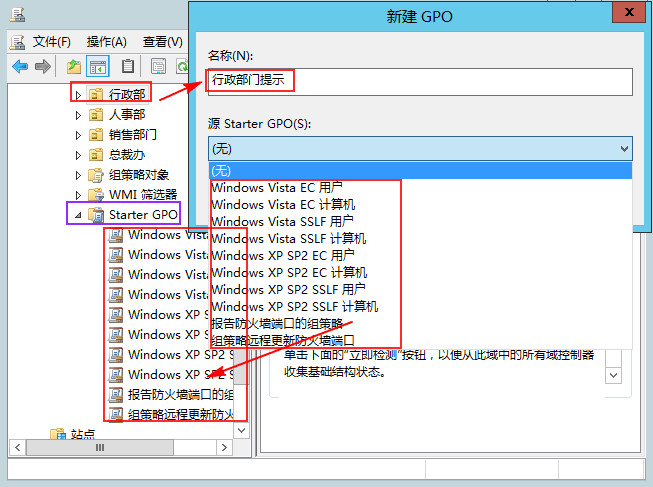
首先在AD域下要有行政部门的OU且已建立有popo的用户。如下图:



接下来使用运行打开组策略管理器“gpmc.msc”并依次展开，如下图：

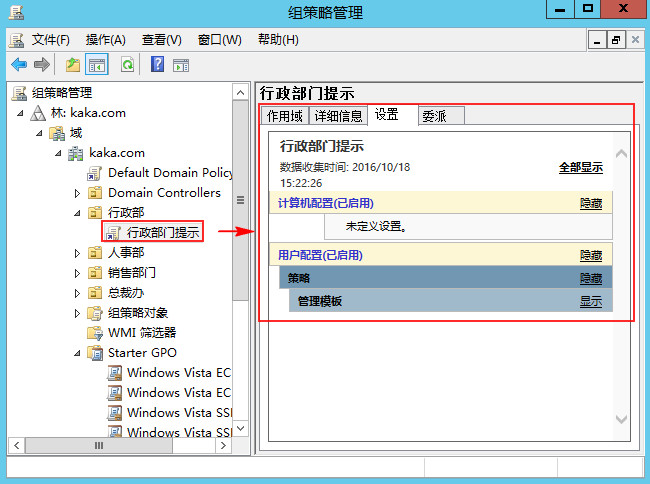


右键点开行政部，点击“在这个域中创建GPO并在此处链接…”新建行政部下的组策略，如下图：

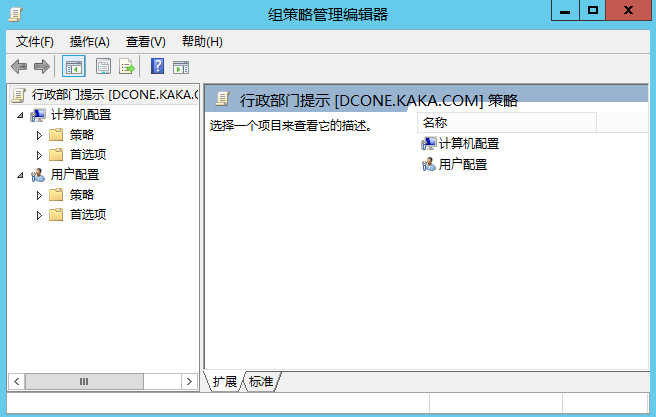


在名称里面填写要创建的组策略的名称，而在源这里可以选择“无”进行自己自定义的组策略配置，或者选择下拉列表中已经是系统默认新建好的模版策略，而这些模版策略都存放在“StarterGPO”下面，如果方便的话，建议可以直接在“StarterGPO”下面建立配置模版，然后在组织OU下面调用就可以了，这样不用每次需要重复查找配置策略。

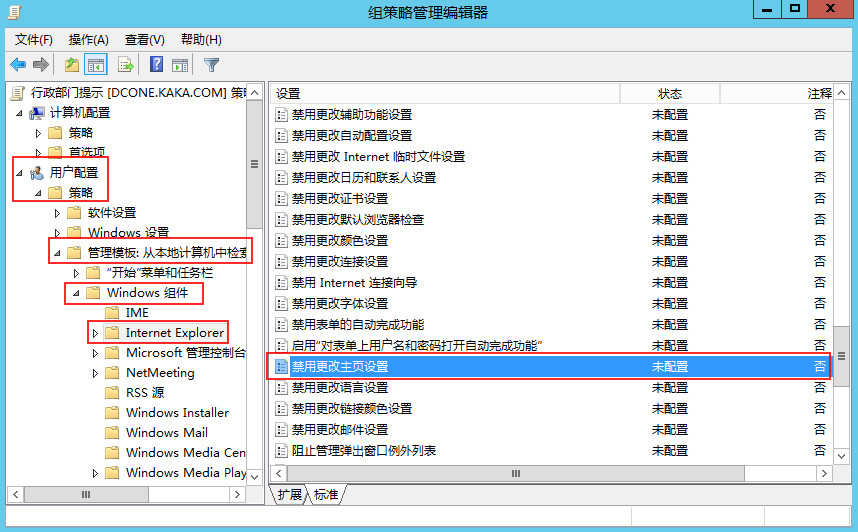
这样在行政部的OU下面就会有一条组策略的记录刚建立好的，而在设置里面可以看到当前都配置的条目，点击右边的显示可以逐条向下显示：



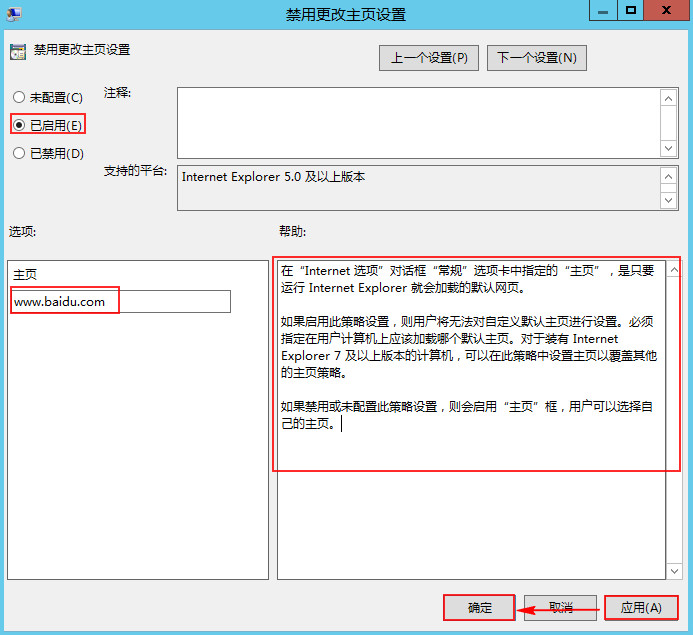
右键点击“行政部门提示”-----“编辑”可以对这个策略的具体项进行配置，如下图：



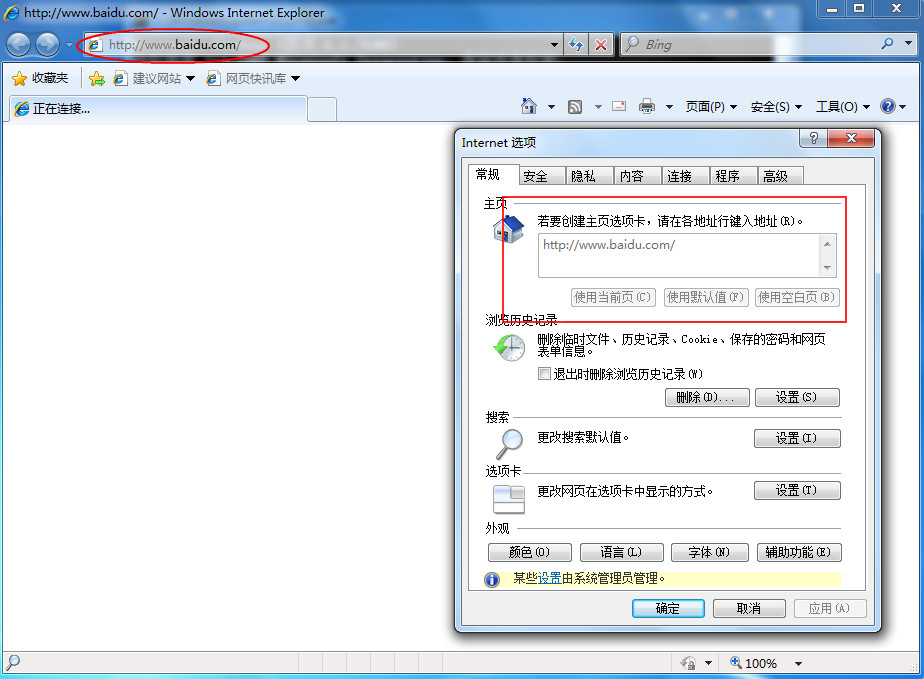
可以分别针对计算机配置或者用户进行配置，这个跟计算机本地策略配置一样。所以根据要求去修改就可以了。此处找到修改浏览器的默认主页项进行修改，如下图：



双击“禁用更改主页设置”的条目进行修改，如下图：



进行客户端“popo”账户的验证，如下图这样就表示组策略生效了。可以在命令提示符界面使用更新组策略命“gpupdate /force”。



可以注意看，这张图里面开始就是百度的首页，然后在主页设置这里是灰白色的显示。

至此，简单的组策略就建立并生效完成了。

注意：对于用户的组策略配置项的更新，只要用户注销后再登录就可以应用，对于计算机的配置需要重启计算机后才会被应用。

除此之外还可以利用组策略建立统一的桌面，对文件夹重定向，分发软件等。

**6.DHCP服务器的配置**

通过安装和配置DHCP服务器，理解DHCP的工作原理，掌握使用DHCP进行网络管理的基本方法。DHCP是网络服务的一种，其他网络服务的安装配置与DHCP有许多相同之处，通过实训，理解网络服务的概念，掌握在Windows Server 2012操作系统中安装配置网络服务的一般性方法。

**IP地址的设置有以下两种方法：（1）手工静态设置；（2）自动向DHCP服务器索取。**

注意：在使用DHCP服务时，整个网络至少有一台服务器上安装了DHCP服务，其他要使用DHCP功能的客户机则必须设置为利用DHCP获得IP地址。客户机在向服务器请求一个IP地址时，如果还有IP地址没有使用，则在数据库中登记该IP地址已被该客户机使用，然后回应这个IP地址以及相关的选项给客户机。

了解DHCP基本术语，比如作用域，排除范围，地址池，保留，选项类型等。

了解DHCO的工作原理。

当作为DHCP客户端的计算机第一次启动时，它通过一系列的步骤以获得其TCP/IP配置信息，并得到IP地址的租期。DHCP客户端从DHCP服务器上获得完整的TCP/IP配置需要经过以下几个过程：

① DHCP发现：DHCP工作过程的第一步是DHCP发现（DHCP Discover），该过程也称之为IP发现。以下几种情况需要进行DHCP发现：

 当客户端第一次以DHCP客户端方式使用TCP/IP协议栈时，即第一次向DHCP服务器请求TCP/IP配置时。

 客户端从使用固定IP地址转向使用DHCP动态分配IP地址时。

 该DHCP客户端所租用的IP地址已被DHCP服务器收回，并已提供给其他的DHCP客户端使用时。

② DHCP提供：DHCP工作的第二个过程是DHCP提供（DHCP offer），是指当网络中的任何一个DHCP服务器（同一个网络中可能存在多个DHCP服务器时）在收到DHCP客户端的DHCP发现信息后，该DHCP服务器若能够提供IP地址，就从该DHCP服务器的IP地址池中选取一个没有出租的IP地址，然后利用广播方式提供给DHCP客户端。在还没有将该IP地址正式租用给DHCP客户端之前，这个IP地址会暂时保留起来，以免再分配给其他的DHCP客户端。

如果网络中有多台DHCP服务器，且这些DHCP服务器都收到了DHCP客户端的DHCP发现信息，同时这些DHCP服务器都广播一个应答信息给该DHCP客户端时，则DHCP客户端将从收到应答信息的第一台DHCP服务器中获得IP地址及其配置。

提供应答信息是DHCP服务器发给DHCP客户端的第一个响应，它包含了IP地址、子网掩码、租用期（以小时为单位）和提供响应的DHCP服务器的IP地址。

③ DHCP请求：DHCP工作的第三个过程是DHCP请求（DHCP request），一旦DHCP客户端收到第一个由DHCP服务器提供的应答信息后，就进入此过程。当DHCP客户端收到第一个DHCP服务器响应信息后就以广播的方式发送一个DHCP请求信息给网络中所有的DHCP服务器。在DHCP请求信息中包含所选择的DHCP服务器的IP地址。

④ DHCP应答：DHCP工作的最后一个过程便是DHCP应答（DHCP ACK）。一旦被选择的DHCP服务器接收到DHCP客户端的DHCP请求信息后，就将已保留的这个IP地址标识为已租用，然后也以广播方式发送一个DHCP应答信息给DHCP客户端。该DHCP客户端在接收DHCP应答信息后，就完成了获得IP地址的过程，便开始利用这个已租到的IP地址与网络中的其他计算机进行通信。

DHCP服务器的授权：必须在AD DS域环境中，DHCP服务器才可以被授权。

**注意：**若利用虚拟环境来练习，请将这些计算机所连接的虚拟网络的DHCP服务器功能禁用；如果利用物理机练习，请将网络中其他DHCP服务器关闭或禁用，例如停用IP共享设备或宽带路由器内的DHCP服务器功能。这些DHCP服务器都会干扰实验。

**7.DNS服务器的配置**

DNS的查询方式：当DNS客户端向DNS服务器查询IP地址时，或DNS服务器向另外一台DNS服务器查询IP地址时，它有递归查询和迭代查询两种查询模式。

域名系统的对象类型

|  |  |  |
| --- | --- | --- |
| 类型 | 意义 | 内容 |
| SOA | 授权开始 | 标识一个资源记录集合（称为授权区段）的开始 |
| A | 主机地址 | IP地址（标识一个主机名与其所对应的IP地址的映射） |
| MX | 邮件交换 | 邮件服务器名及优先级（标识一个邮件服务器与其所对应的IP地址的映射）。 |
| NS | 域名服务器 | 域的授权名字服务器 |
| CNAME | 别名 | 别的规范名字 |
| PTR | 指针 | 对应于IP地址的主机名 |
| SRV | 服务 | 用来记录提供特殊服务的服务器的相关数据。 |
| HINFO | 主机描述 | ASCII字符串，用于CPU和OS描述 |
| TXT | 文本 | ASCII字符串 |

可以在DNS服务器内建立以下三种类型的DNS区域：

主要区域，辅助区域，存根区域。

思考：通常在DNS区域内建立哪些常用的资源记录？

扩展技能：DNS泛域名解析

企业想要为很多员工建立了个人网站，为了节省费用，可以采用虚拟主机技术，即在同一web服务器上架设多个网站，员工使用二级域名访问这些站点（将在随后的项目10中实现）。然而，维护这些二级域名的工作量非常大，因此，可以采用DNS泛域名解析技术来解决这个难题。详细操作步骤见ppt。

客户端测试DNS服务器

（1）使用ping命令测试DNS解析情况

若实验机器直接连接物理外网，或由虚拟机桥接的方式连接外网，则还可利用Ping命令去解析www.sina.com.cn、www.baidu.com、 www.sohu.com等网站域名的IP地址。需要调整各实验机器的IP配置，这里不做详述。仅以百度为例，给出解析结果.

反向解析测试主要是测试DNS服务器是否能够提供名称解析功能。在命令状态下输入ping –a 192.168.11.250，以检测DNS服务器是否能够将IP地址解析成主机名。

（2）使用nslookup命令测试DNS服务器

① 使用nslookup

在命令提示符下，键入：nslookup，进入Nslookup 交互模式，出现“>”提示符，这时输入域名或IP 地址等资料，回车可得到相关信息。

② nslookup 中的其他常用命令及说明

所有的命令需在“>”提示符后面输入，常用命令有：

help：显示有关帮助信息

exit：退出nslookup 程序。

server IP：将默认的服务器更改到指定的DNS域。IP为指定DNS服务器的IP地址。

set q=A：由域名、主机名查询IP地址。为默认设定值。

set q=CNAME：查询别名的规范名称。

set q=ANY：查询所有数据类型。

set q=PTR：如果查询是IP地址，则为计算机名；否则为指向其他信息的指针。

set q=MX：查询邮件交换器。

set q=NS：查询用于命名区域的 DNS 名称服务器。

（3）查看主机高速缓存区

为了提高主机的解析效率，主机常常采用高速缓冲区来存储检索过的域名与其IP地址的映射关系。Unix、Linux、Windows等操作系统都提供命令，允许用户查看域名高速缓冲区中的内容。在Windows Server2012中，可以使用“ipconfig／displaydns”命令将高速缓冲区中的域名与其IP地址映射关系显示在屏幕上，包括域名、类型、TTL、IP地址等。

**8.WEB服务器的配置**

URL是与因特网相连的机器上的任何可访问对象的一个指针。由于对不同对象的访问方式不同（如通过WWW、FTP等），所以URL还指出读取某个对象时所使用的访问方式。URL的一般形式为：

<URL的访问方式>：//<主机域名>:<端口>/<路径>

使用HTTP的URL

对于万维网网站的访问要使用HTTP协议。HTTP的URL的一般形式如：

http://<主机域名>：<端口>／<路径>

http的默认端口号是80，通常可以省略。若再省略文件的<路径>项，则URL就指到因特网上的某个主页（Home Page）。

例如，要查有关邢台职业技术学院的信息，就可先进入到邢台职业技术学院的主页，其URL为：

http://www.xpc.edu.cn

更复杂一些的路径是指向层次结构的从属页面。例如：

http://www.xpc.edu.cn/xxzx/index.htm

HTTP会话过程包括四个步骤：连接、请求、应答、关闭。

客户端测试网站可以使用以下方式：

（1）利用DNS网址http://www.xpc.edu.cn来连接网站，此时测试计算机的IE浏览器会先通过DNS服务器来得知网站www.xpc.edu.cn的ip地址，然后连接此网站。

（2）利用IP地址http://192.168.11.250来连接网站。

（3）利用计算机名来连接网站，这种方法适合于局域网内计算机，并需要先将WEB服务器的windows防火墙关闭或放行，否则可能会连接失败。

主目录

网站的主目录，既可以是本机的默认文件夹，也可以是本机的其他文件夹或其他计算机的共享文件夹。

默认文档

访问网站时，用户只输入IP地址或域名就能打开主页文件，而并不需要输入主页的绝对URL路径，这实际上是因为网站设置了默认文档。一旦用户访问网站域名，则默认打开该页面。网站的主页文件，一般存放在网站主目录下。单击IIS界面的站点名称，选择“默认文档”可以查看到当前可以自动识别的默认主页文件名，条目类型为“继承”，表示这些设置是从计算机设置继承来的。以后添加的新站点都会继承这些默认值。如果网站主页文件名在此列表中，就可以直接被识别。

物理目录

网站主目录内可以创建不同的子文件夹，用于管理和归类不同的网站文件。那么这些子文件夹，可以依照标准的URL路径格式来访问，目录名就是磁盘上实际存在的文件夹名，因此称之为物理目录（Physical Directory）。访问方法是：

<URL的访问方式>：//<主机域名>:<端口>/路径/<子目录名>

物理目录和后面将要介绍的虚拟目录，均可以像网站主目录一样设置默认文档，当我们访问到该路径下，自动打开默认的页面。

虚拟目录

在网站的管理工作中经常出于各类需要，网站资源并不一定只放在一个磁盘的一个文件夹内，甚至不一定只放在同一台服务器上。在这里，我们就要用到虚拟目录（Virtual Directory）这种目录组织形式了。我们完全可以将网页文件存储到其他位置，然后通过虚拟目录映射到网站的主目录之下，每一个虚拟目录都使用别名（Alias），用户通过标准URL路径格式访问该别名，而不需要知道这个目录实际的文件夹名称。访问方法是：

<URL的访问方式>：//<主机域名>:<端口>/路径/<别名>

每个Internet服务可以从多个目录中发布。通过以通用命名约定(UNC)名、用户名及用于访问权限的密码指定目录，可将每个目录定位在本地驱动器或网络上。虚拟服务器可拥有一个宿主目录和任意数量的其它发布目录。其它发布目录称为虚拟目录。

IIS支持在同一个WEB服务器上架设多个网站。需要方便识别各个网站，可以设置网站的名称。网站的名称可以在创建网站时设置，也可以在创建后更改。更改的方法是在IIS界面右击网站的名称，在快捷菜单内单击“重命名”，之后录入新的网站名称即可。

另外，WEB服务器也需要正确区分各个网站的服务请求。那么，**区分的方法有三种，分别是：主机名、IP地址和TCP端口号。**

**利用不同的主机名架设网站**

**利用TCP端口号来架设多个网站**

**利用不同的IP地址来架设网站**

详细操作方法见ppt。

**9.FTP服务器的配置**

在Internet和Intranet中，FTP是除Web之外最为广泛的一种应用，大量的软件及音、视频等大容量文件的上传和下载多使用FTP方式。

FTP（File Transfer Protocol）就是文件传输控制协议，是用于TCP/IP网络及Internet的最简单、广泛的协议之一。FTP的主要作用就是让用户连接上一个远程计算机（这些计算机运行着FTP服务进程，并且存储着各种格式的文件，包括计算机软件、声音文件、图像文件、重要资料、电影等），查看远程计算机上有哪些文件，然后把文件从远程计算机上复制到本地计算机，或把本地计算机的文件传送到远程计算机去。前者称为“下载”，后者称为“上传”。

**FTP的工作原理**

客户端和服务器端使用TCP进行连接，在连接时，都必须各自打开一个TCP端口。FTP服务器预置两个端口21和20，其中端口21用来发送和接收FTP的控制信息，一旦建立FTP会话，端口21的连接在整个会话期间始终保持打开状态：端口20用于发送和接收FTP数据，只有在传输数据时才打开，一旦传输结束就断开。FTP客户端激发FTP客户端服务之后，动态分配自己的端口（端口号为122465535）。

用户对FTP服务的访问有两种方式：匿名FTP和用户FTP。

根据FTP数据连接建立方法，可将FTP客户端对FTP服务器的访问分为两种模式：主动模式（又称标准模式）和被动模式。

FTP命令

用户可以使用FTP命令来进行文件传输，这种称为交互模式。当用户交互使用FTP时，FTP发出一个提示，用户输入一条命令，FTP执行该命令并发出下一提示。FTP允许文件沿任意方向传输，即文件可以上传与下载，在交互方式下，也提供了相应的文件上传与下载的命令。如在windows 2000操作系统下可使用如下形式的FTP命令。

FTP [-d-g-i-n-t-v] [host]

其中：

Host：代表主机名或者主机对应的IP地址

-d：表示允许调试。

-g：表示不允许在文件名中出现“\*”和“?”等通配符。

-i：表示多文件传输时，不显示交互信息。

-n：表示不利用$HOME/netrc文件进行自动登录

-t：表示允许分组跟踪。

-v：显示所有从远程服务器上返回的信息。

[]：表示其中的内容为命令的可选参数。

用户输入FTP 命令如“ftp://192.168.174.128”后，屏幕就会显示“FTP >”提示符，表示用户进入FTP交互模式，在该模式下用户可输入FTP操作的子命令。常见的FTP子命令及其功能如下：

ASCII：进入ASCII方式，传送文本文件；

BINARY：传送二进制文件；进入二进制方式；

BYE或QUIT：结束本次文件传输，退出FTP程序；

CD dir：改变当前工作目录；

LCD dir：改变本地当前目录；

DIR或LS [remote-dir] [local-file]：列目录 ；

GET remote-file [local-file]：获取远地文件；

MGET remote-files：获取多个远地文件，可以使用通配符；

PUT local-file [remote-file]：将一个本地文件传递到远地主机上；

MPUT local-files：将多个本地文件传到远地主机上；可用通配符；

DELETE remote-file：删除远地文件 ；

MDELETE remote-files：删除远地多个文件；

MKDIR dir-name：在远地主机上创建目录；

RMDIR dir-name：删除远地目录；

OPEN host：与指定主机的FTP服务器建立连接 ；

CLOSE：关闭与远地FTP程序的连接；

PWD：查询当前目录；

STATUS：显示FTP程序的状态；

USER user-name [password] [account]：向FTP服务器表示用户身份；

另外有许多工具软件被开发出来用于实现FTP的客户端功能，如NetAnts、Cute FTP、WSFTP等，另外Internet Explorer和Netscape Navigator也提供FTP客户软件的功能。这些软件的共同特点是采用直观的图形界面，通常还实现了文件传输过程中的断点再续和多路传输功能。

对FTP站点属性配置的方法详见ppt。

一台计算机内可以建立多个FTP站点，为了区分需要给予每一个站点唯一的标识信息，**即虚拟主机名、IP地址和TCP端口号。**

**补充：证书颁发机构（CA）作为PKI的核心，主要用于证书颁发、证书更新、证书吊销、证书和证书吊销列表的公布、证书状态的在线查询、证书认证等。**

**NAT的实现方式有三种，即静态转换Static Nat、动态转换Dynamic Nat和端口多路复用OverLoad。**

**VPN:**虚拟专用网络，可以把它理解成虚拟的企业内部专线。它可以通过特殊的加密的通讯协议在连接在Internet上的位于不同地方的两个或多个企业内部网之间建立一条专有的通讯线路。

**Windows Server 2012支持PPTP、L2TP(L2TP/IPsec)、SSTP(SSL)与IKEv2（VPV Reconnect）等VPN通信协议。**