Dayang Research Release

DAYANG

Windows Server 2008 R2 SP1域策略

配置手册

文档信息：

Windows Server 2008 R2 SP1 域策略 配置手册				
版本编号	**版本日期**	**修改者**	**语言**	**更 新 说 明**
V.1.0	2011-12-06	孙轶玮	中文	创建新文档

一、 版权说明

关于本手册的版权归属

Windows Server 2008 R2 SP1 域策略 配置手册

目　录

一 背景描述

在很多大洋项目具体实施中，都需要域策略的支持。基于 windows 2003 所部署的域策略，已经是大洋比较成熟稳定的域策略方案，如今，服务器操作系统已经升至 windows2008 平台，所以，我们迫切需要一套基于 windows2008 平台的域策略部署方案。本文主要介绍如何在 Windows Server 2008 R2 SP1 服务器进行一些常规域策略的部署，达到抛砖引玉的作用，帮助实施工程师根据项目具体需求，进行针对性的域策略的部署；

二 功能描述

Windows Server 2008 R2 SP1 平台下的域策略，较 windows 2003 平台，有了更多完善的功能，在安全性方面，也得到了进一步得到了提高,通过本文档，我们可以实现如下一些安全域策略配置：

1. 基于网络驱动器域策略管理；
2. 基于应用程序域策略管理（重定向开始菜单）；
3. 基于桌面隐藏等域策略管理；

三 配置前的准备

a) 建立 1—2 台域控制器；

b) 安装操作系统：安装下述任一版本均可

Windows Server 2008 R2 SP1 标准版 64bit（安装时请选择完全安装）

Windows Server 2008 R2 SP1 企业版 64bit（安装时请选择完全安装）

c) 关闭本机的防火墙：

注：加域前如果禁用防火墙，加域后需要再禁用一次，否则防火墙默认是被打开

四 windows 2008 域控 安装配置

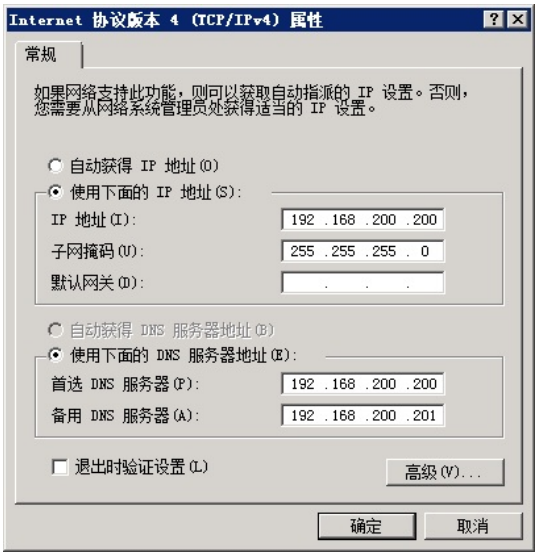
4.1 安装操作系统

安装 Win2008 R2 SP1 的方法此处不再赘述，但是对于此系统，操作系统在安装过程中需要注意以下几点问题：

- 主机的硬件驱动识别正确
- 正确关闭防火墙

4.2 配置网卡

对于网卡的 IP 地址划分如图：



其中涉及到的 IP 地址如下表：

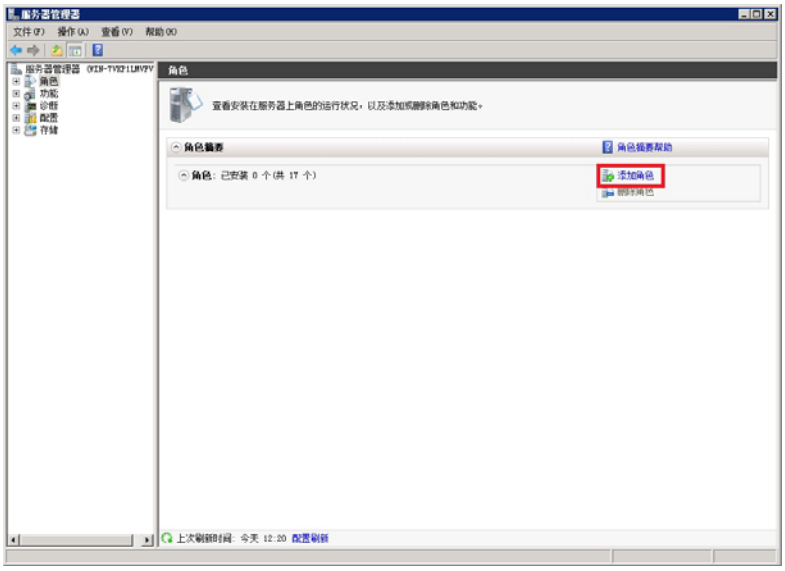
主机	公网 IP	心跳 IP	虚拟 IP
主服务器	192.168.200.200/24	10.10.10.10/24	192.168.200.202/24
备服务器	192.168.200.201/24	10.10.10.11/24	192.168.200.202/24

4.3 建立域控

建立域控时需要注意以下几点：

- **域控最好使用主备模式，即域控使用两台服务器来承担，一台为主域控，另一台为从域控。**

首先来建立主域控服务器，进入服务器管理器，点击左侧树状菜单中的角色按钮，在右面的窗口中点击“添加角色”按钮，如下图所示：

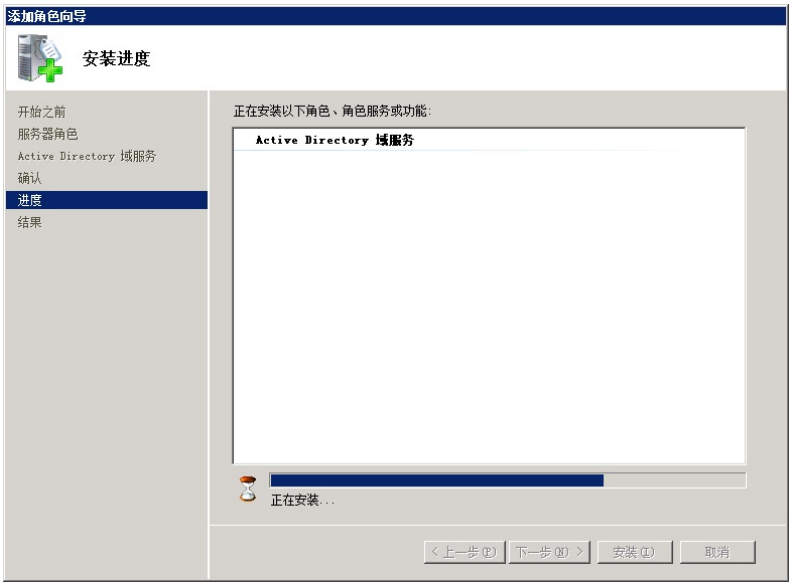


在弹出的对话框中，选择“域服务”，点击“下一步”，如下图：

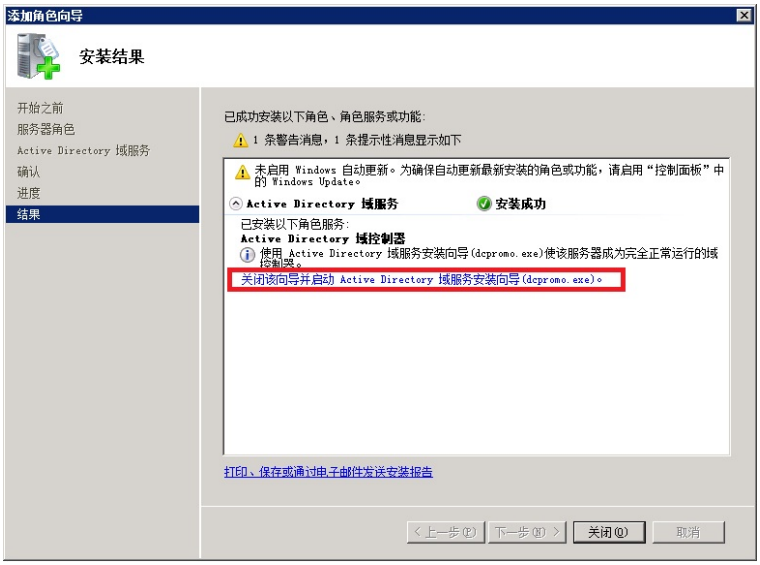
点击“下一步”，如下图：

点击“安装”，如下图：

开始进行角色的安装，如下图：

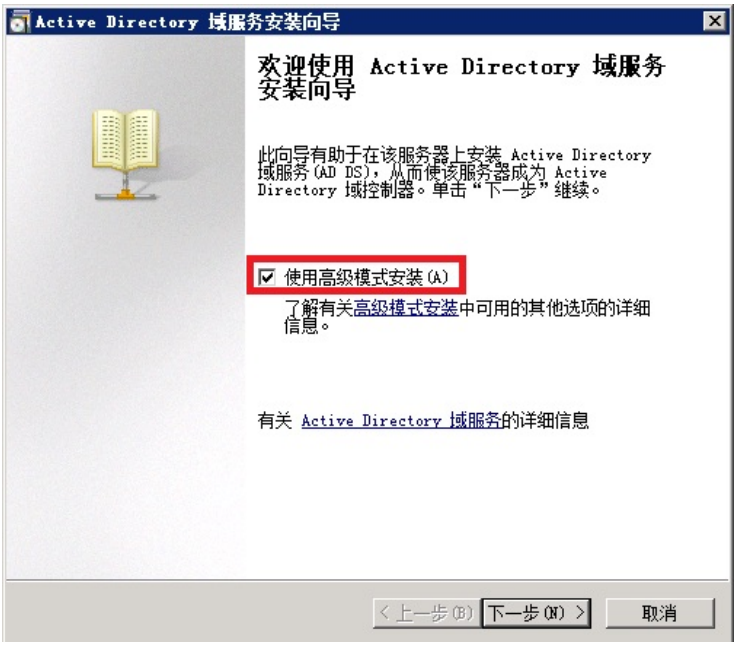


在安装结束后回弹出如下对话框，点击红色框图圈中的连接，窗口会自动关闭，进入到配置阶段，如下图：

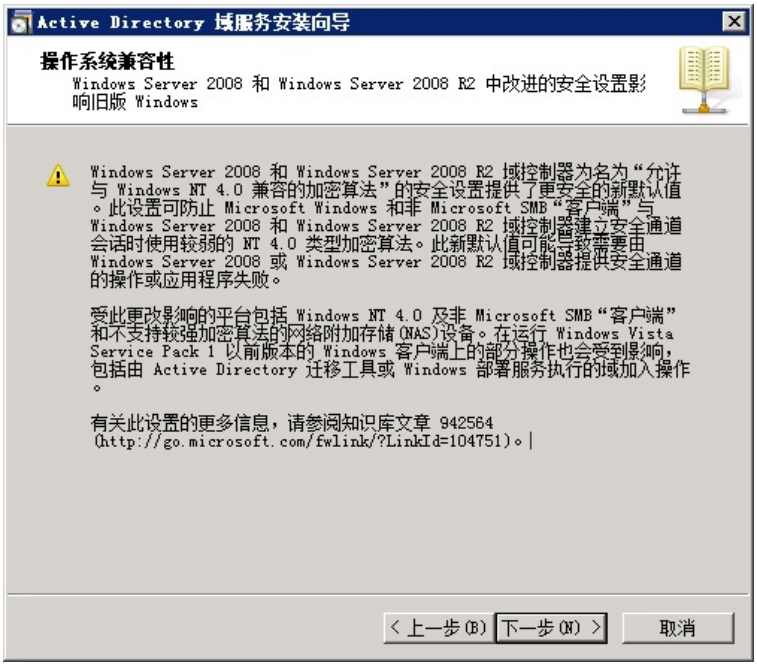


下面开始对域控服务进行配置，此操作在主域控服务器上进行

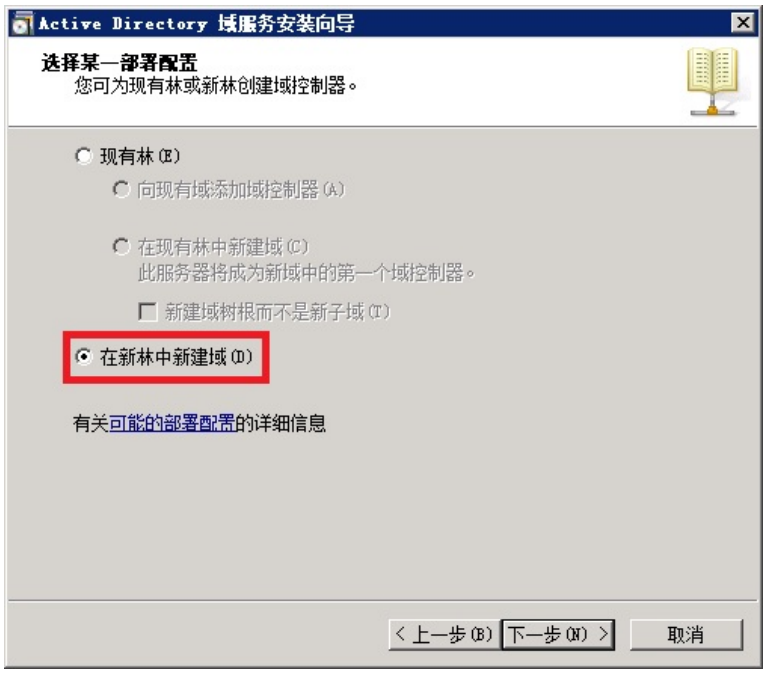
勾选“使用高级模式安装”，点击“下一步”，如下图：



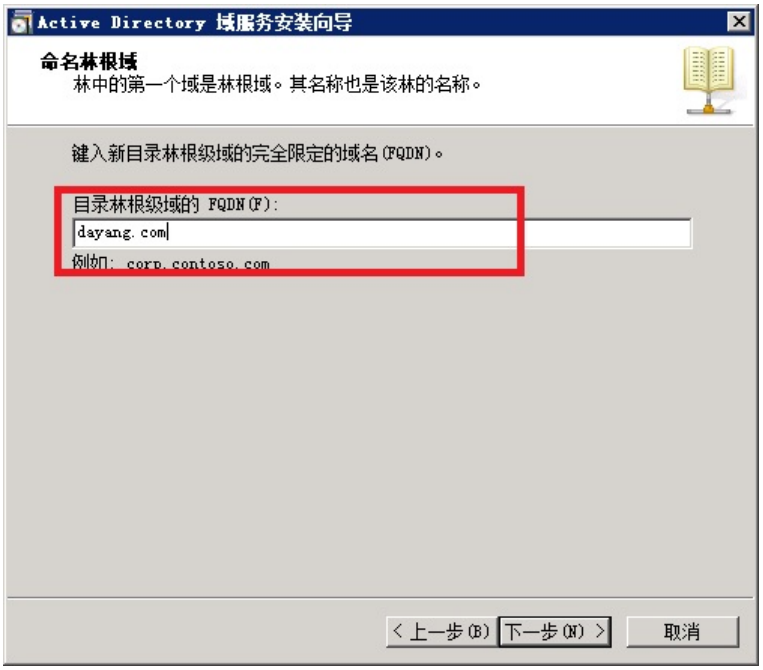
保持默认，点击“下一步”，如下图：



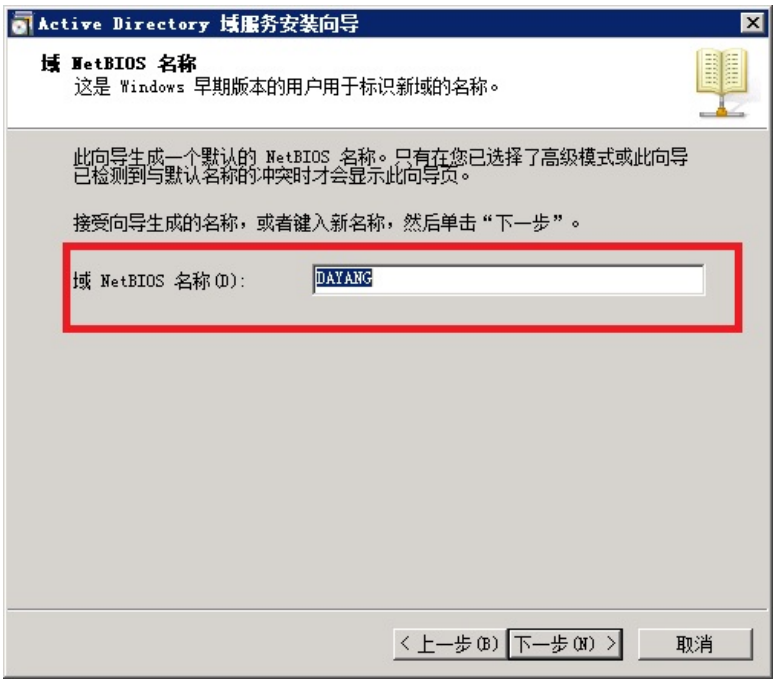
选择“在新林中新建域”，点击“下一步”，如下图：



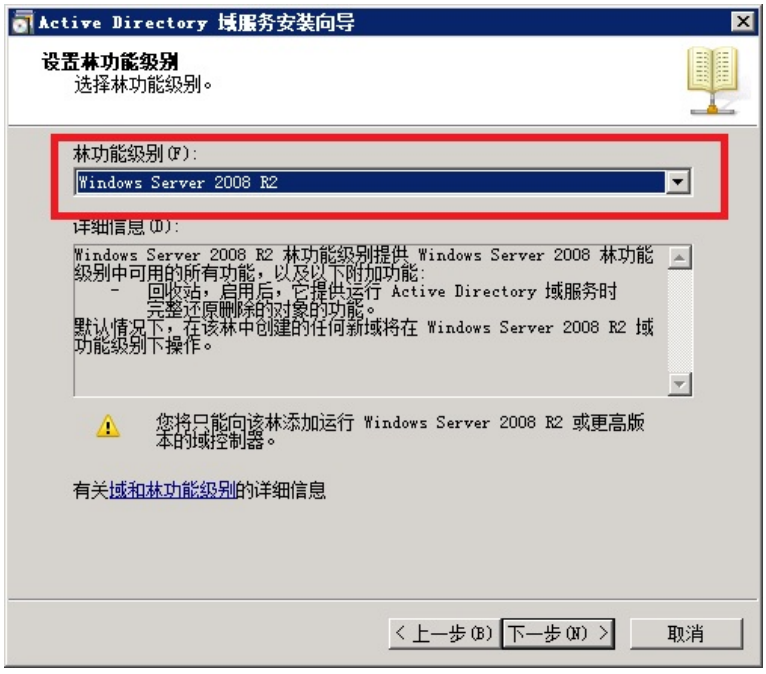
在输入框中输入域名称，此处输入的是“dayang.com”，点击“下一步”，如下图：



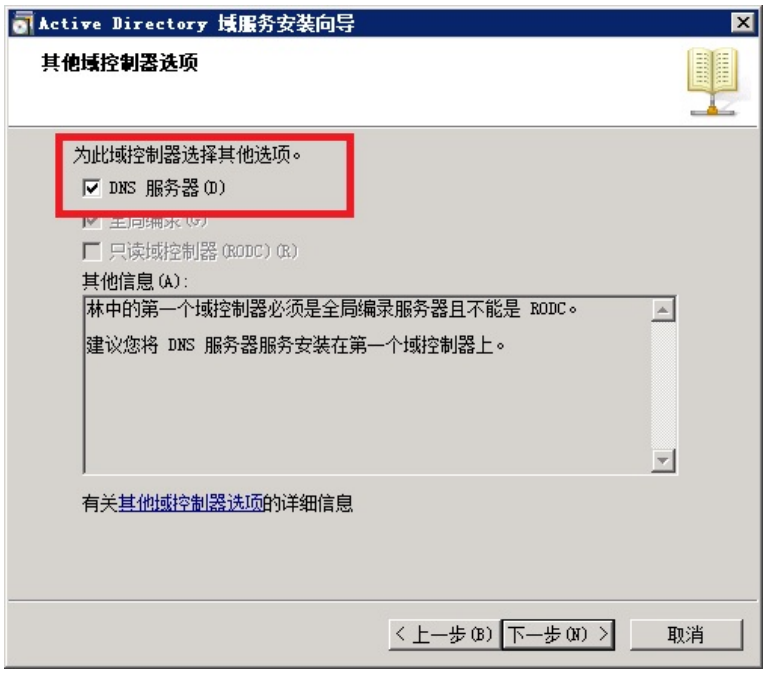
如下图：点击“下一步”



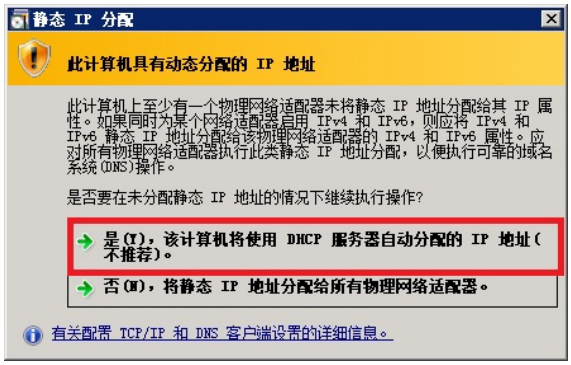
在“林功能级别”选项中选择“Win2008 R2”，点击“下一步”如下图：



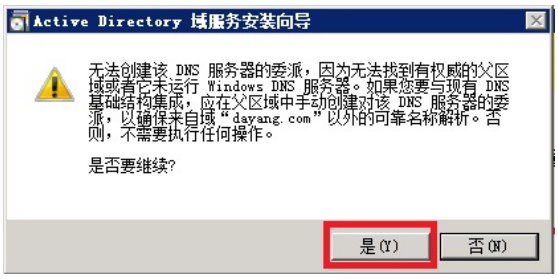
勾选“DNS 服务器”，点击“下一步”



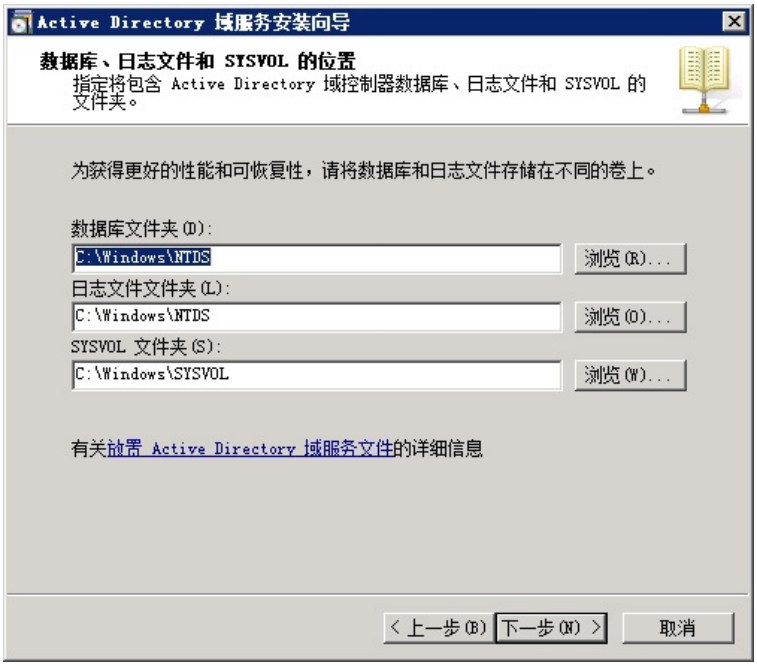
在弹出的对话框中，选择“是”选项，



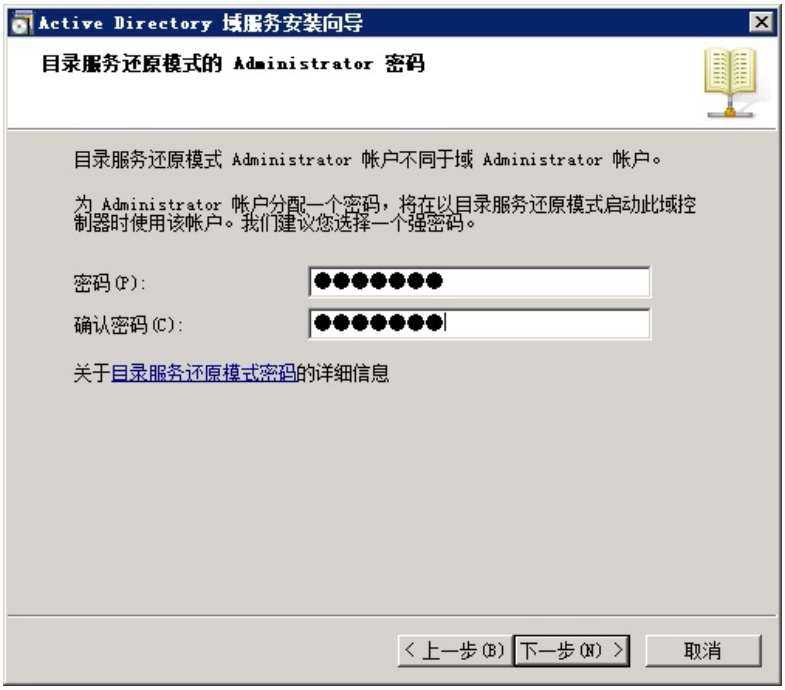
如下图，点击“是”



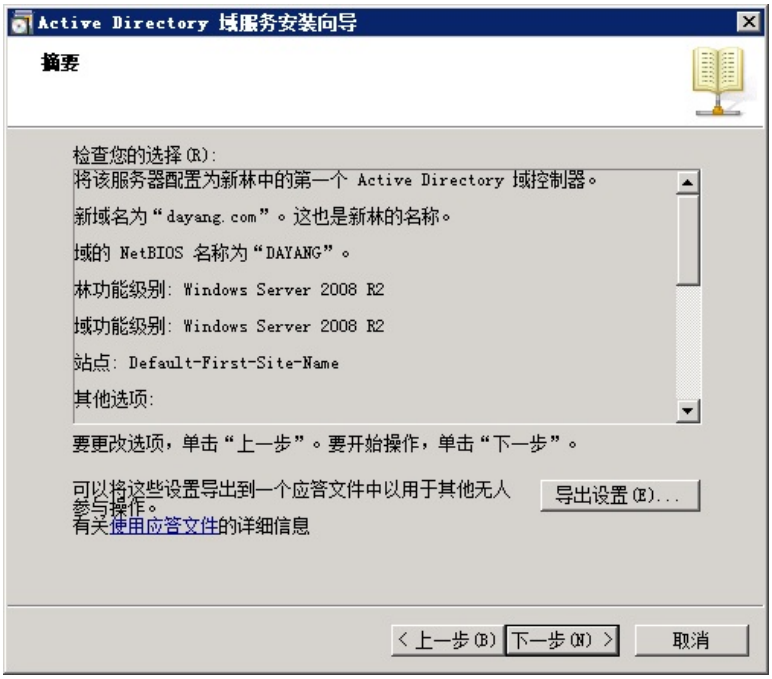
保持默认，点击“下一步”如下图：



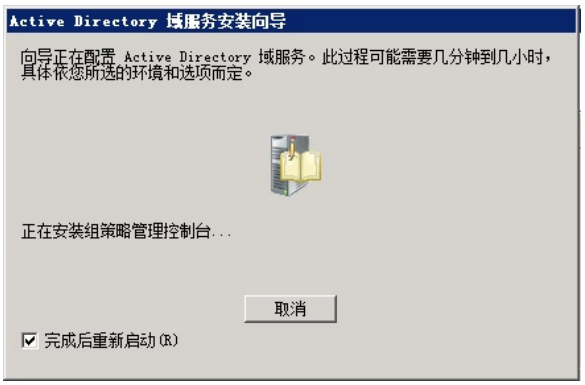
为目录服务还原模式的 Administrator 设置一个新密码，如下图：



保持默认，点击“下一步”



系统开始配置域控

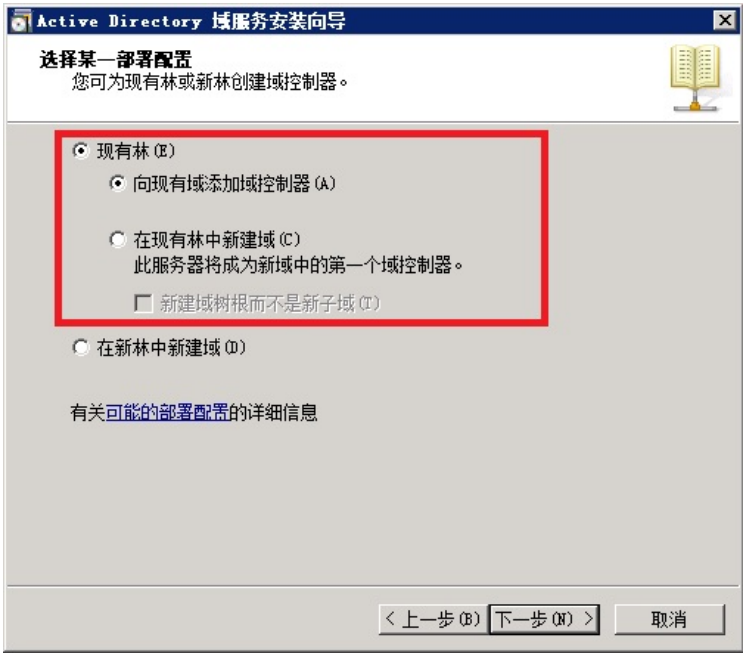


域控服务配置完成之后，系统会重新启动。

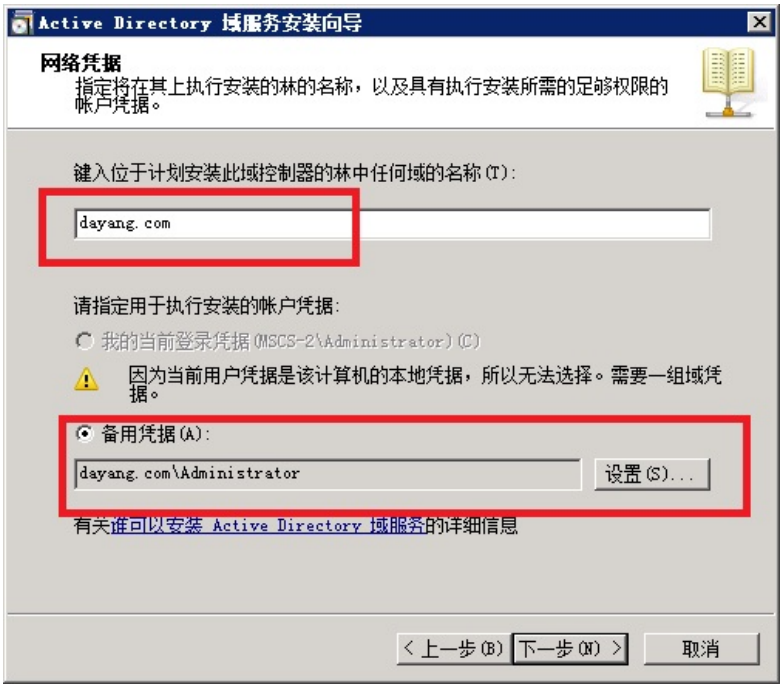
下面开始配置备用域控，以下操作在备服务器上操作：

安装域控角色的步骤与前面一样，下面介绍配置备用域控的方法：

如下图：选择“向现有域添加域控制器”，点击“下一步”



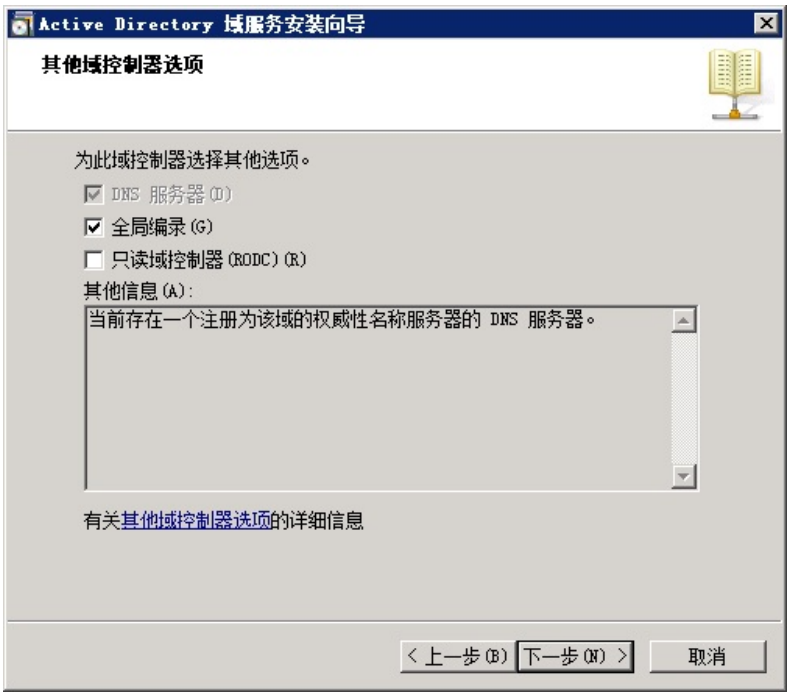
在输入栏中添加域的名称，前面建立域的名称是“dayang.com”这里也输入相应的名称，如下图：点击使用“备用凭据”，输入域管理员的用户名密码，点击“下一步”



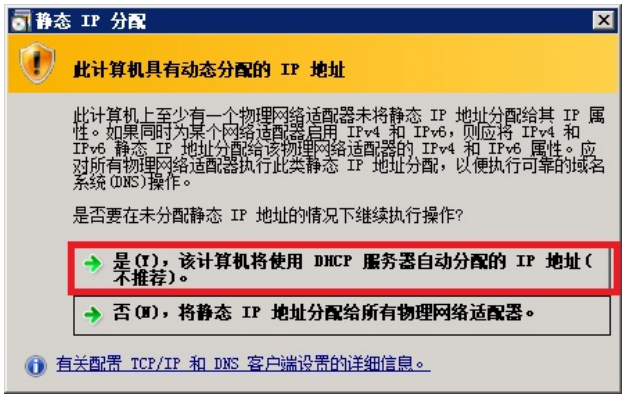
系统找到域，点击“下一步”，如下图：

保持默认，如下图，点击“下一步”

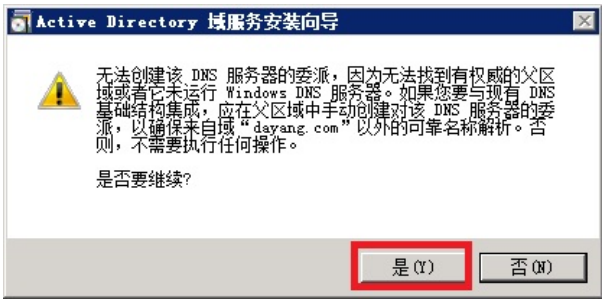
保持默认，如下图，点击“下一步”



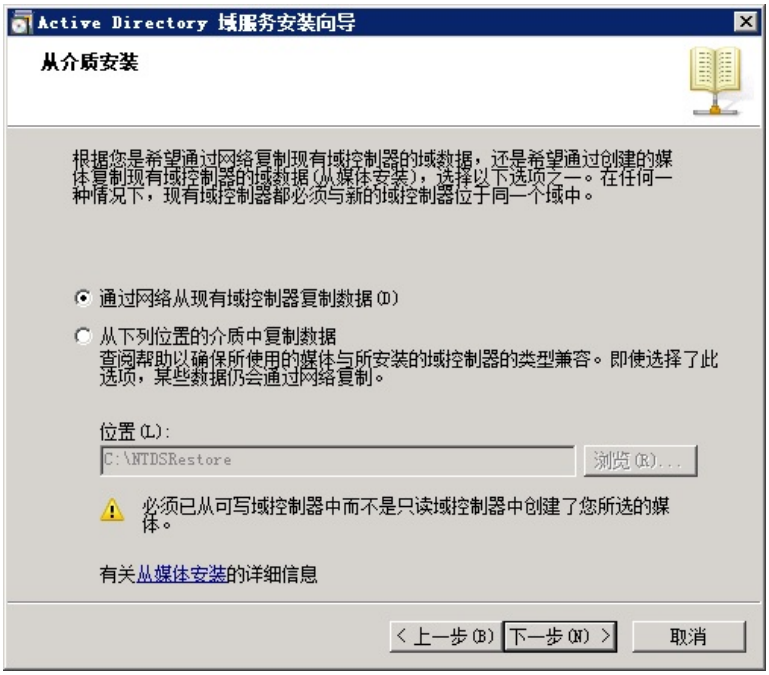
如下图：选择“是”



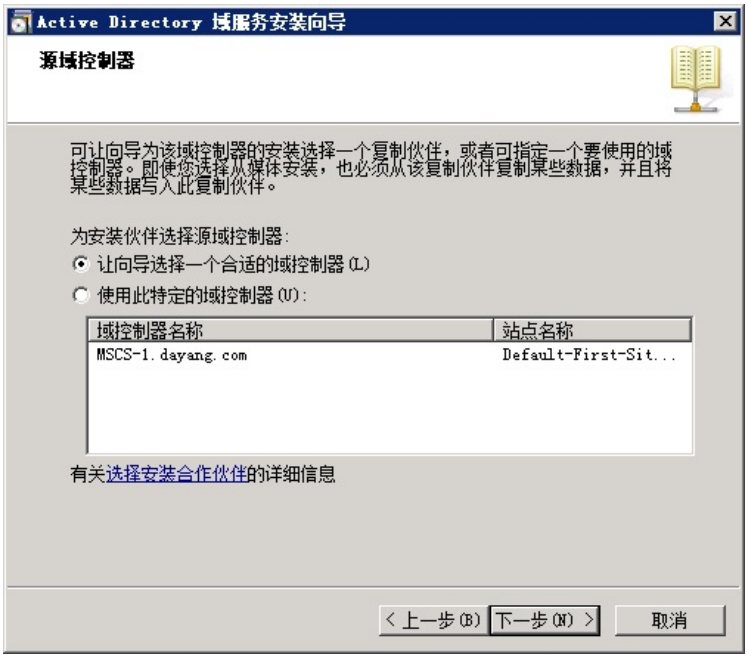
如下图：选择“是”



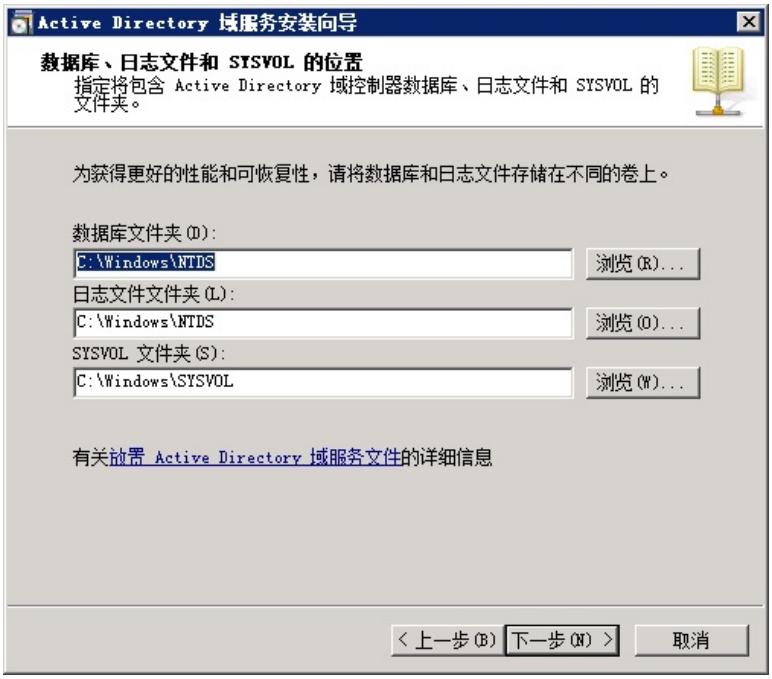
保持默认，如下图：点击“下一步”



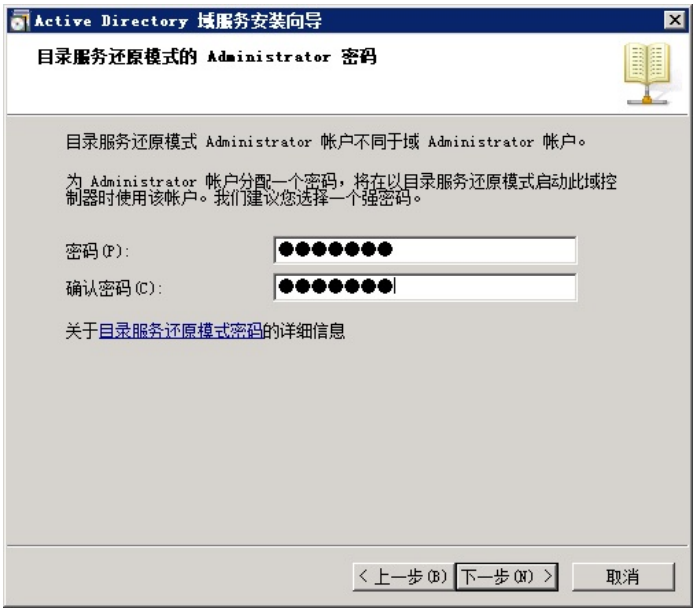
保持默认，如下图：点击“下一步”



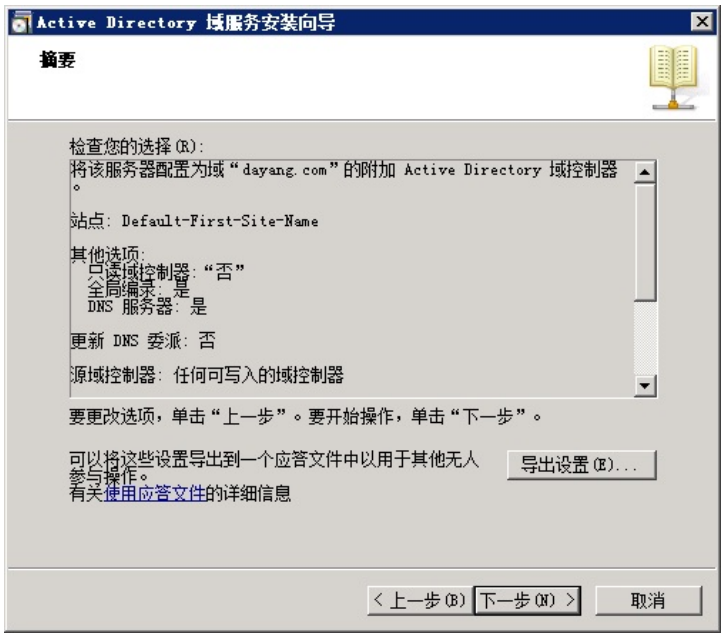
保持默认，如下图：点击“下一步”



输入一个新密码，如下图，点击“下一步”



保持默认，如下图，点击“下一步”



勾选“完成后重新启动”，系统在配置完成之后会自动重启服务器的操作系统

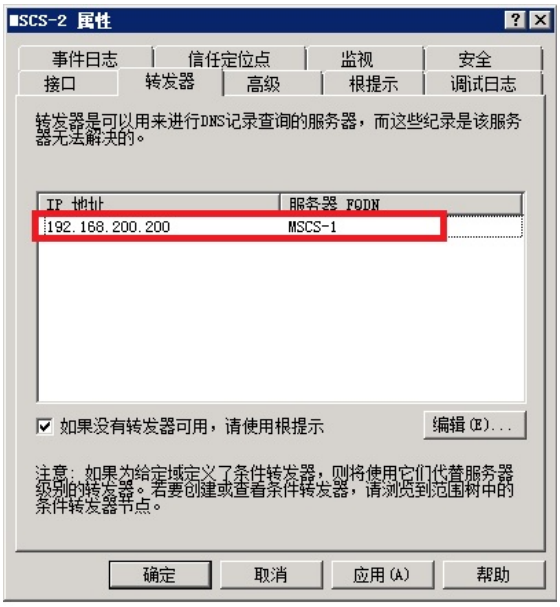
到此，主备域控的配置就完成了。

4.4 配置辅助 DNS

在建立完成主备域控之后，我们需要对两台 DNS 服务器进行 DNS 记录的自动同步的配置，具体方法如下：

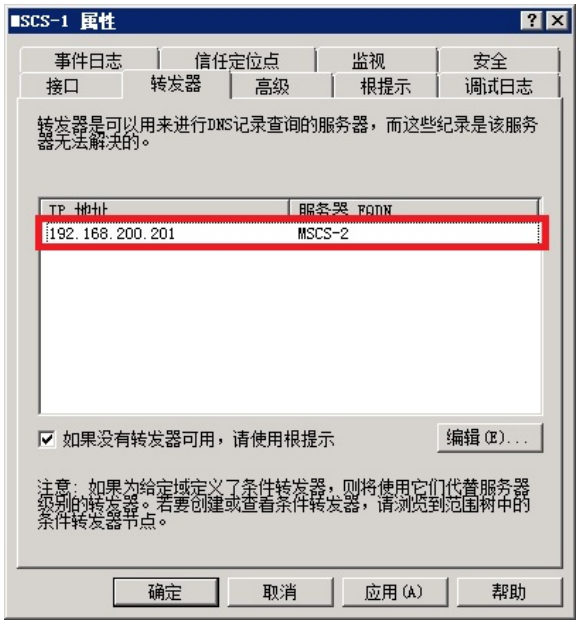
首先在第二台服务器，即备域控服务器上点击“开始---管理工具---DNS”，在根节点即机器名上点击鼠标右键，选择“属性”，出现如下对话框，选择“转发器”页签，点击“编辑”按钮，添加主域控的 IP 地址，等待系统进行网络扫描。

完成之后，点击确定，退出。



此时就完成了辅助 DNS 的配置，为了验证配置生效，我们登陆到第一台服务器上，按照上述方法，打开主 DNS 的“转发器”页签，可以看到如下图：

在未进行配置的情况下，主 DNS 服务自动进行了识别，可以看到窗口中已经有 MSCS-2 的机器在，说明辅助 DNS 配置成功。



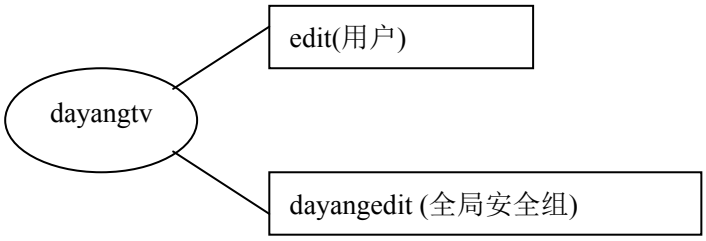
五 部署域策略：

在完成了域控与 DNS 的主备系统部署之后，我们开始在主域控上进行域的部署。为了顺利完成配置任务，我们需要在配置之前验证下面的准备工作是否已经完成并没有出现报错：

- **防火墙已经关闭。**

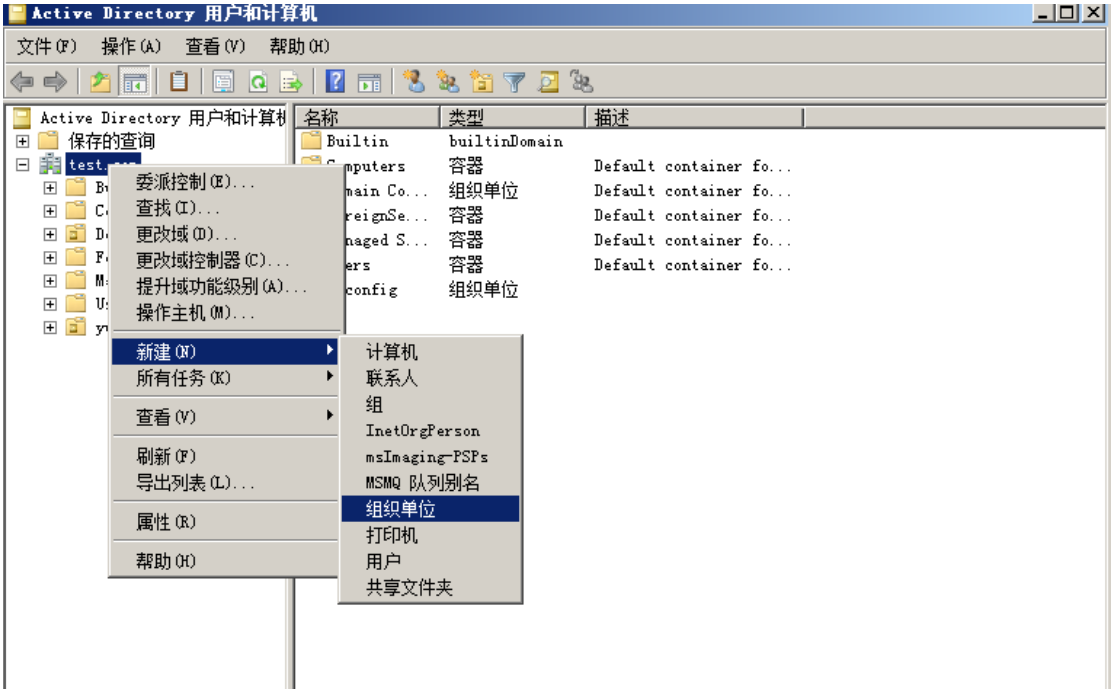
使用 windows 2008 R2 域策略，可以实现所有站点有统一的界面；可以使用户没有任何设置涉及系统安全性方面的权力，所有对安全性的设置大部分都在服务器端只设置一次，只有很少量的设置需要在各客户端设置，接下来，开始介绍如何安装部署域策略功能：

5.1 创建 OU 并新建用户和组

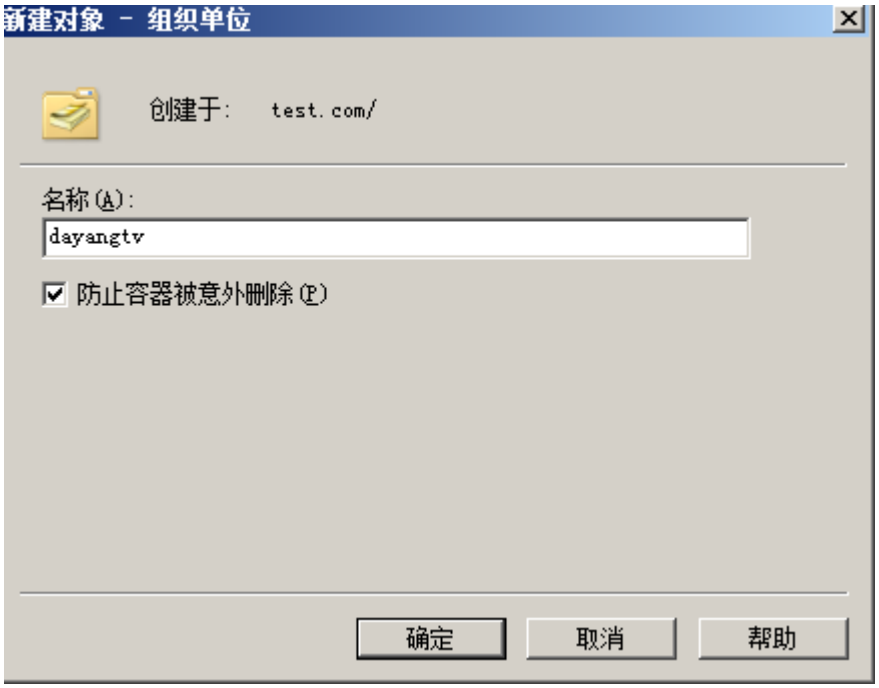


其中，dayangtv 是 OU，即一个域中的组织单位，edit 是一个用户，即在客户端登陆 windows 2008 R2 的用户名，dayangedit 是一个全局安全组，具体创建过程如下：

开始－所有程序－管理工具－Active Directory 用户和计算机，展开左边树，如图所示：



选中 test.com 右键－新建－组织单位，如下图：



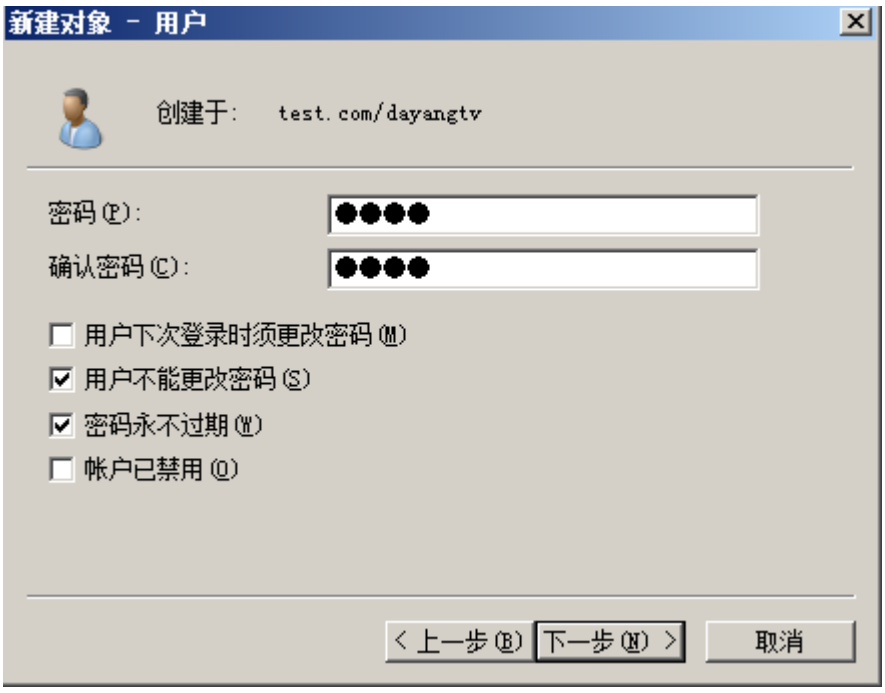
输入组织单位名称：dayangtv，确定，创建 OU 结束。

然后在 OU 上创建组，在 dayangtv－右键－新建－组，如下图

输入组名：dayangedit，组作用域：全局，组类型：安全式，确定，创建组完成。

同样，创建用户，在 dayangtv－右键－新建－用户，如下图：

输入需要创建的用户名登陆名：edit，姓名：edit，点击下一步：



输入密码，并选中：用户不能更改密码；密码永不过期，点击下一步：

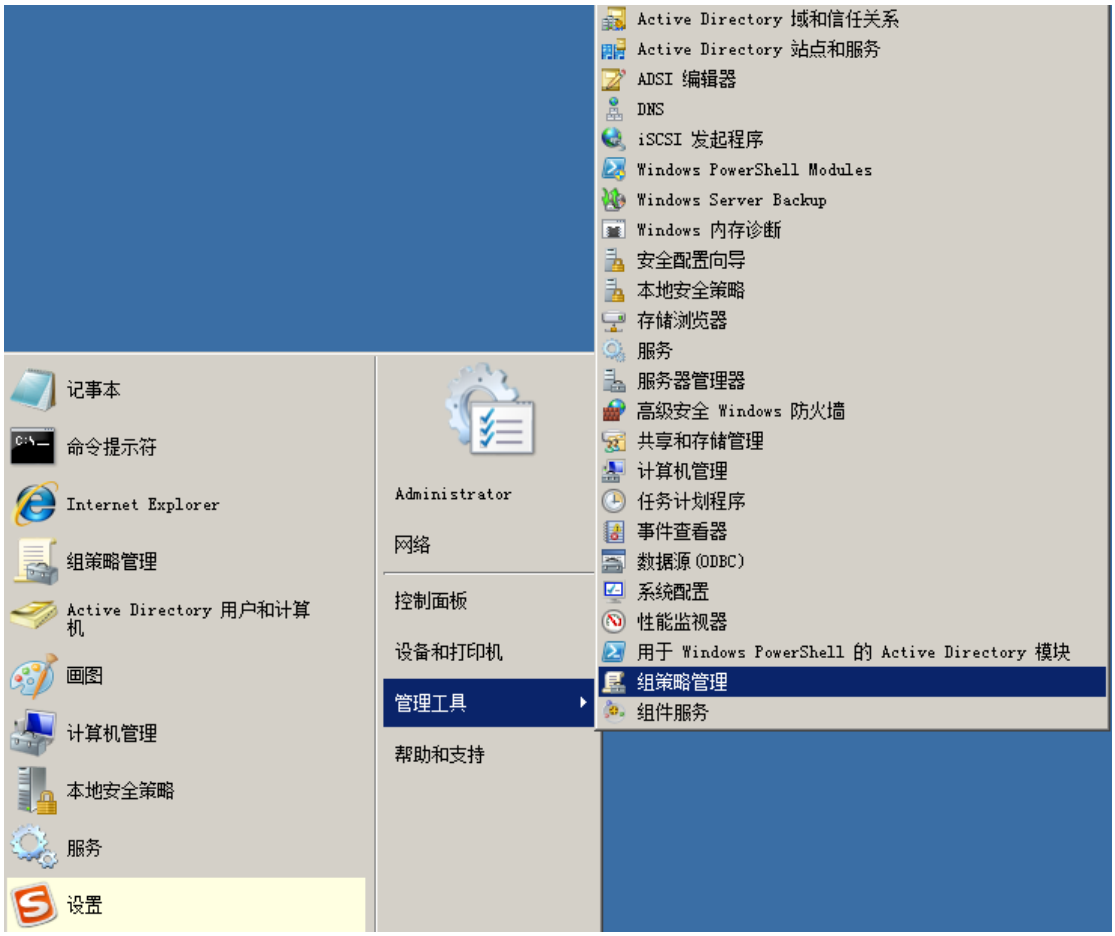
创建完成，点击确定。

然后修改用户属性，使其加入到 edit 组中，在新建的用户名上右键－属性－隶属于－添加－选中 dayangedit－添加，这样把用户添加到 dayangedit 全局安全组。

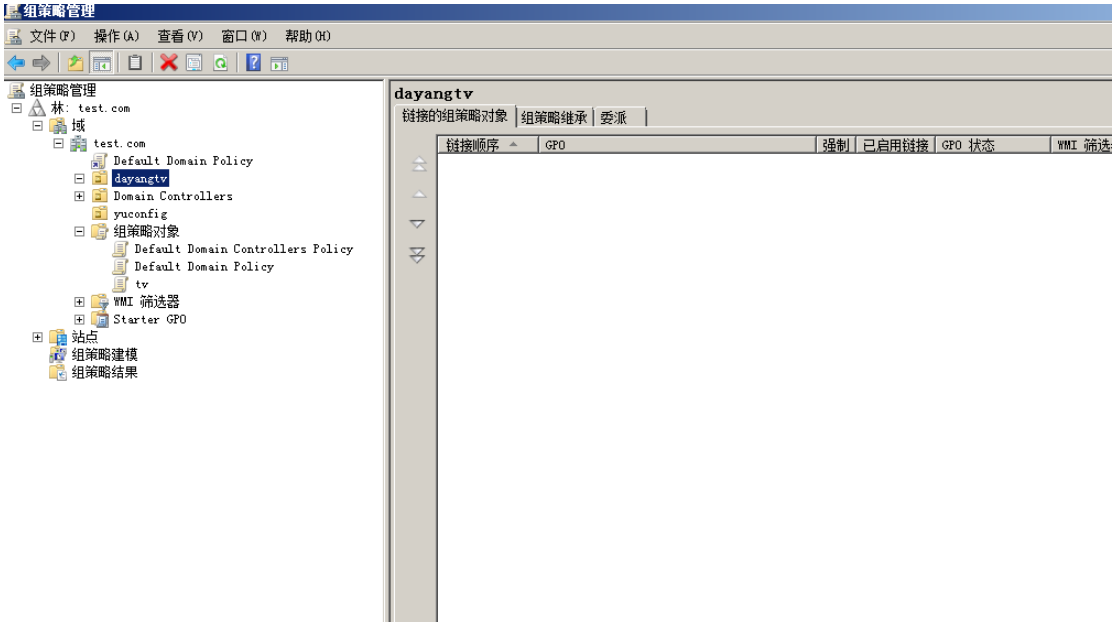
若需要建立其它帐号，可依上样建立，如 edit1、edit2、edit3 三个用户。

5.2 创建策略组：

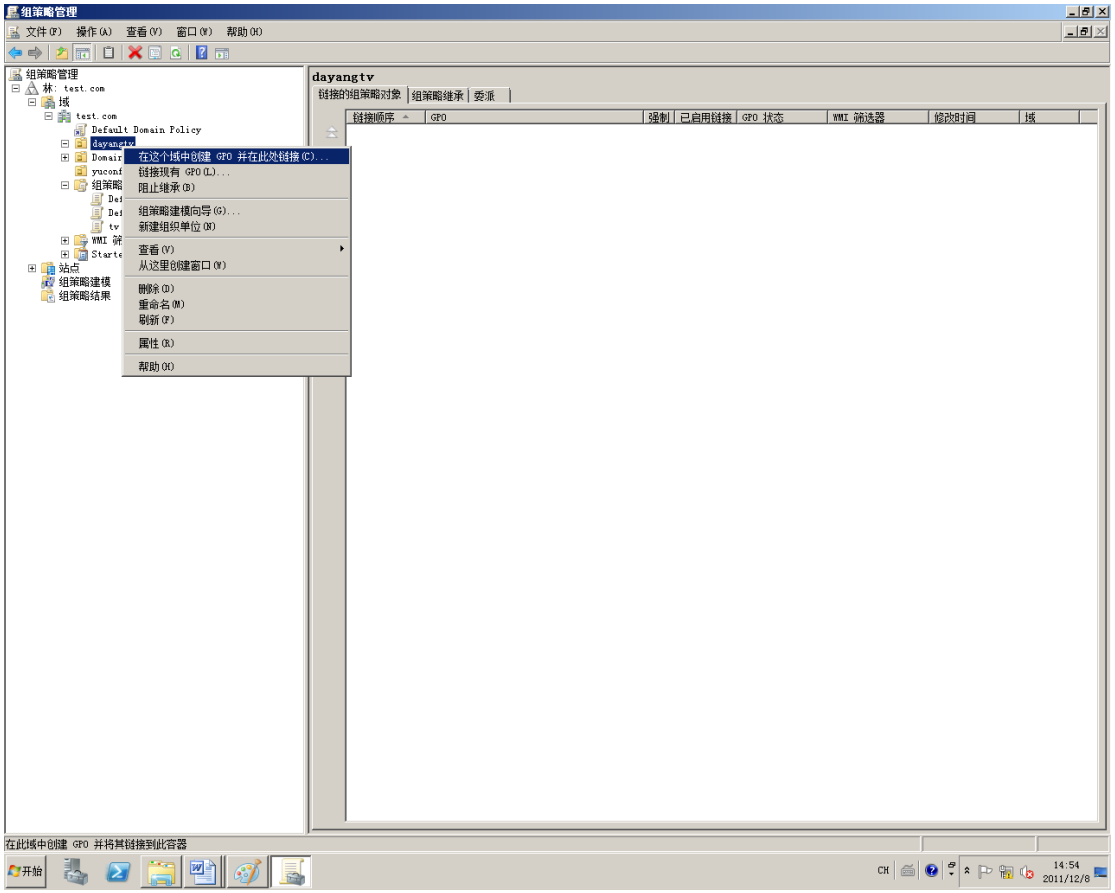
组策略使用来设置 windows 登陆安全的策略，比如屏蔽客户端左面右键，开始菜单，资源管理器等，组策略针对 OU，所有设置只涉及“用户配置”中的“windows 设置”和“管理模板”。



开始－所有程序－管理工具－组策略管理，展开左边树，如图所示：

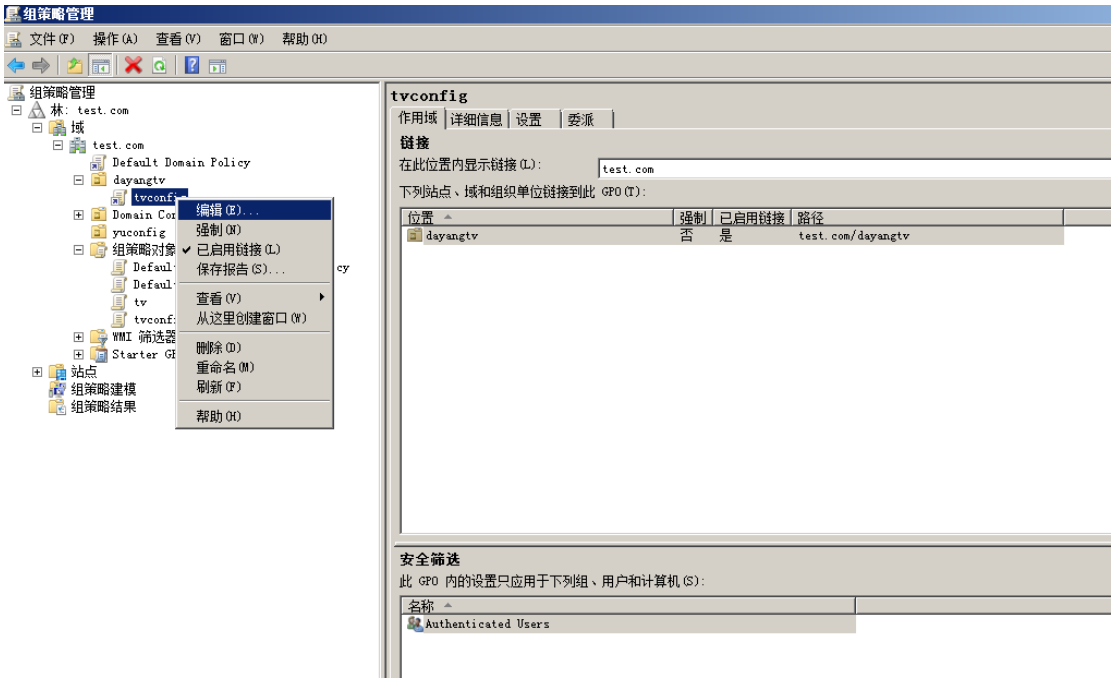


右键，选择在这个域中创建 GPO 并在此处链接：

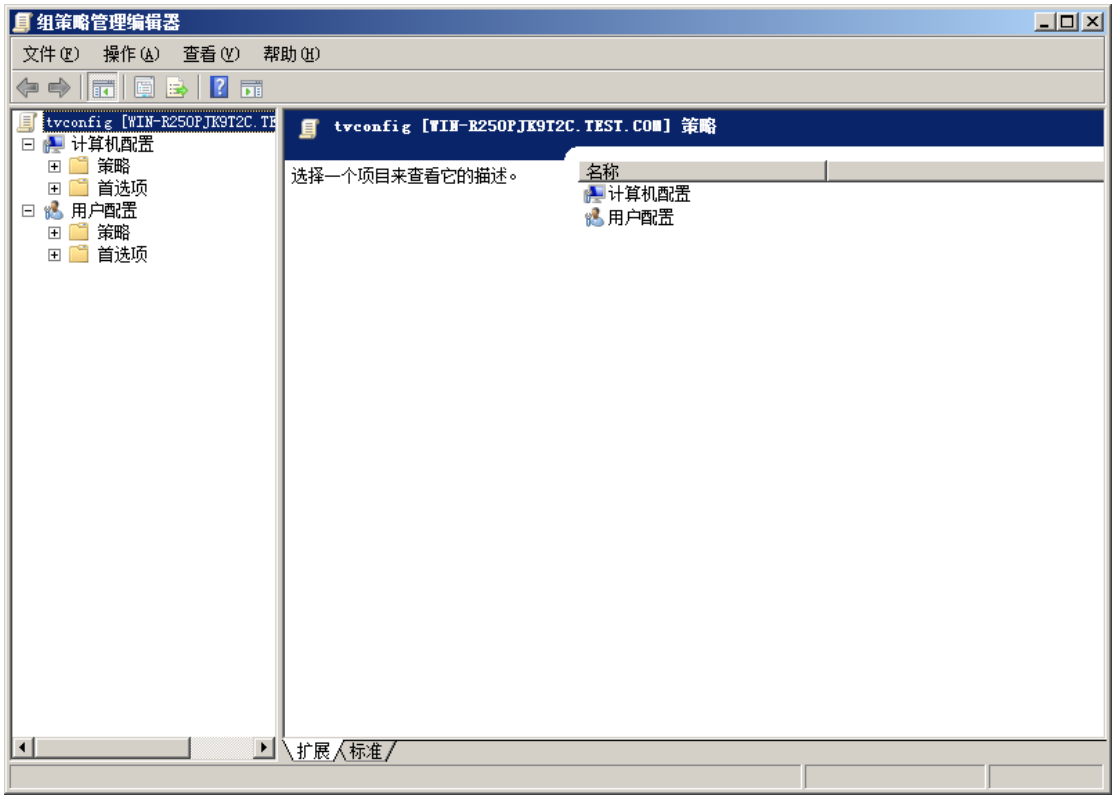


弹出的对话框中“新建 GPO”中，输入 tvconfig，建立策略组，点击确定；

选中 tvconfig，右键选择编辑，如下图：



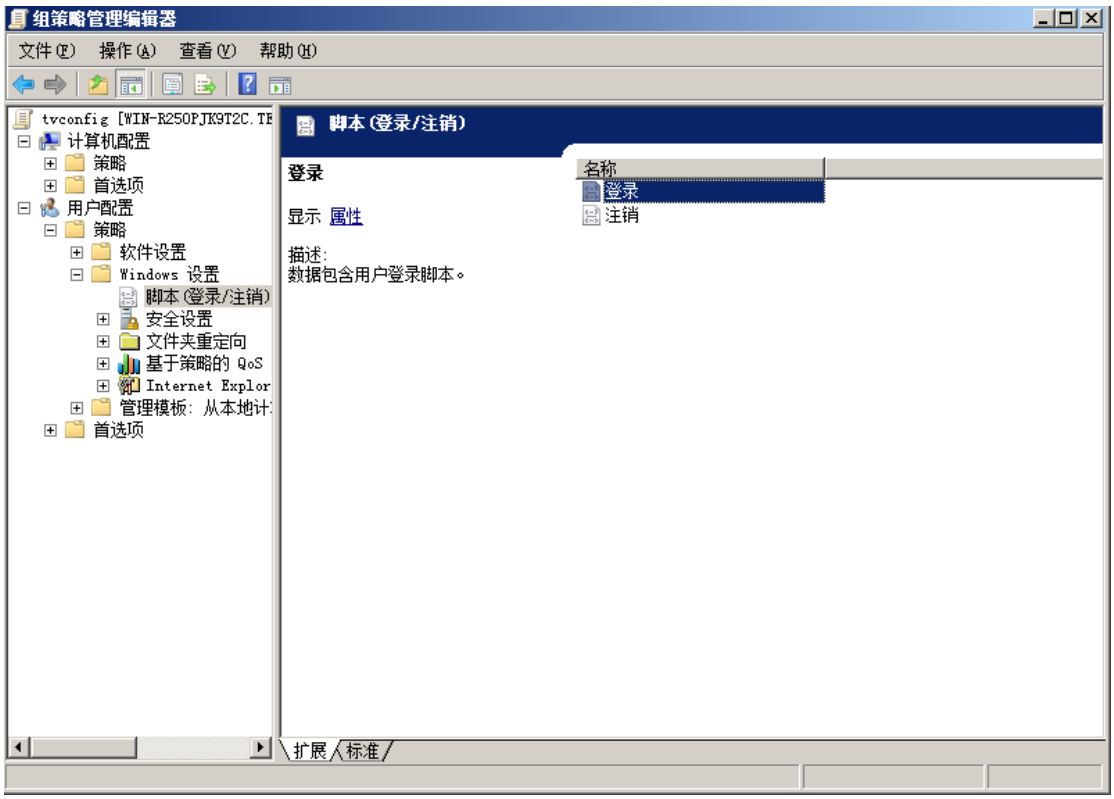
在弹出的组策略管理编辑中，根据项目要求，进行相应编辑



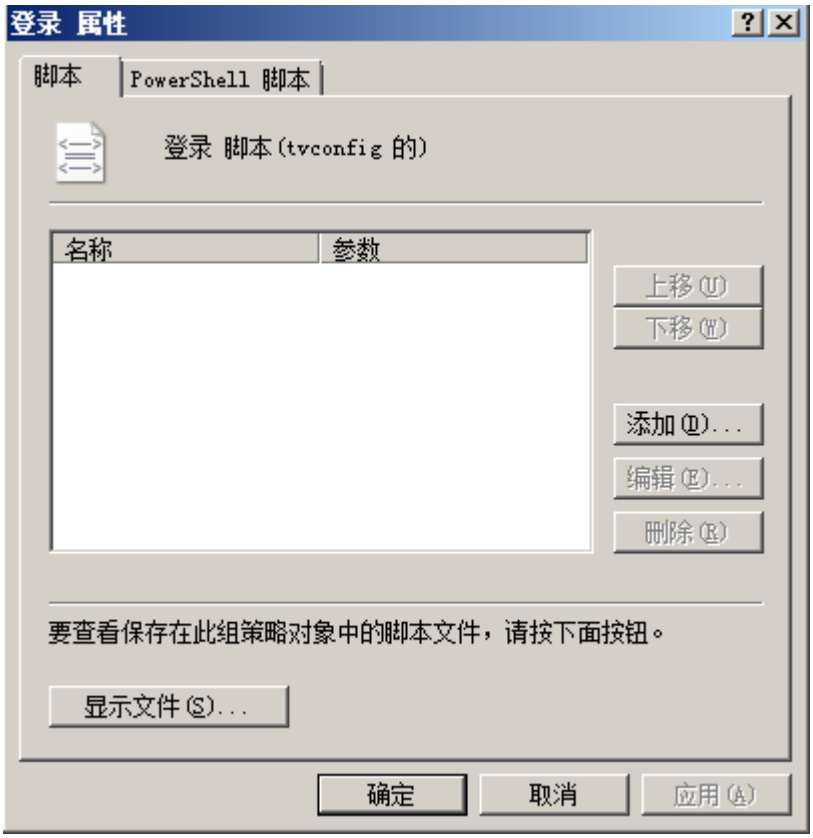
六 域策略具体应用场景：

6.1 基于网络驱动器域策略管理

点“编辑”该组策略对象链接名，策略组－用户配置－windows 设置－脚本（登陆/注销），如下图：



双击登录，如下图：



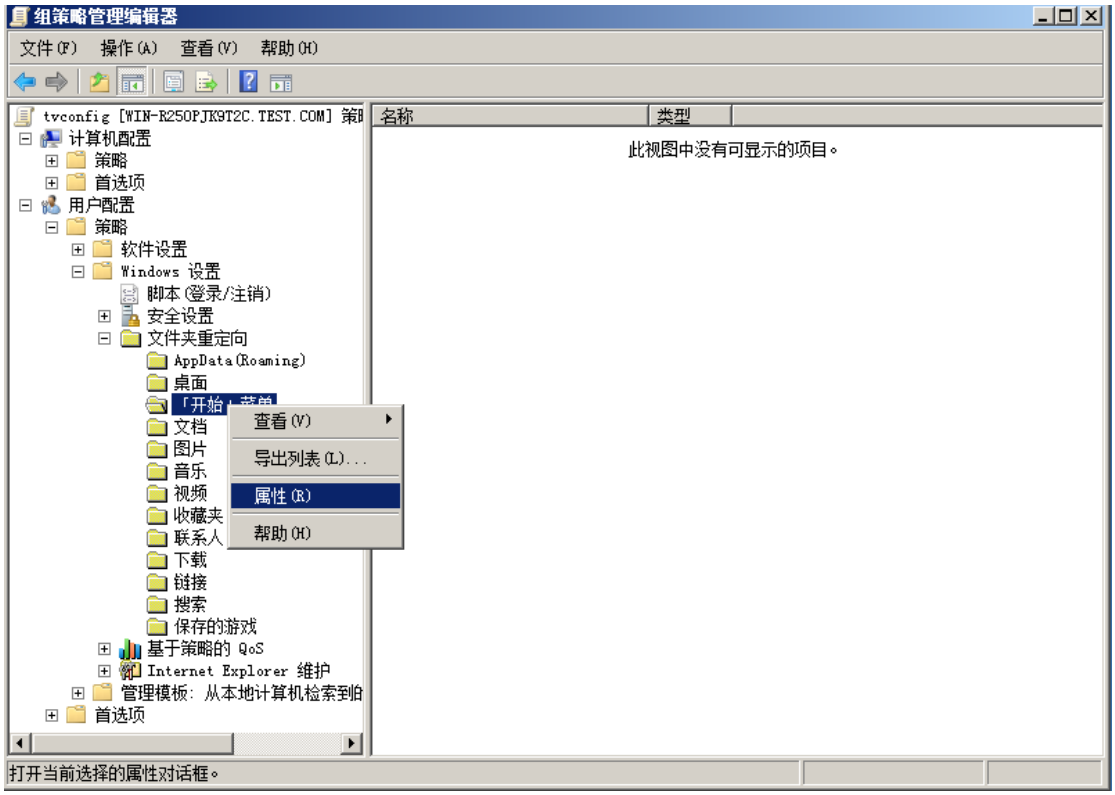
点击显示文件，将展开浏览器，然后在该文件夹中新建登陆脚本文件（登陆脚本针对磁盘阵列的盘符映射），如下例：

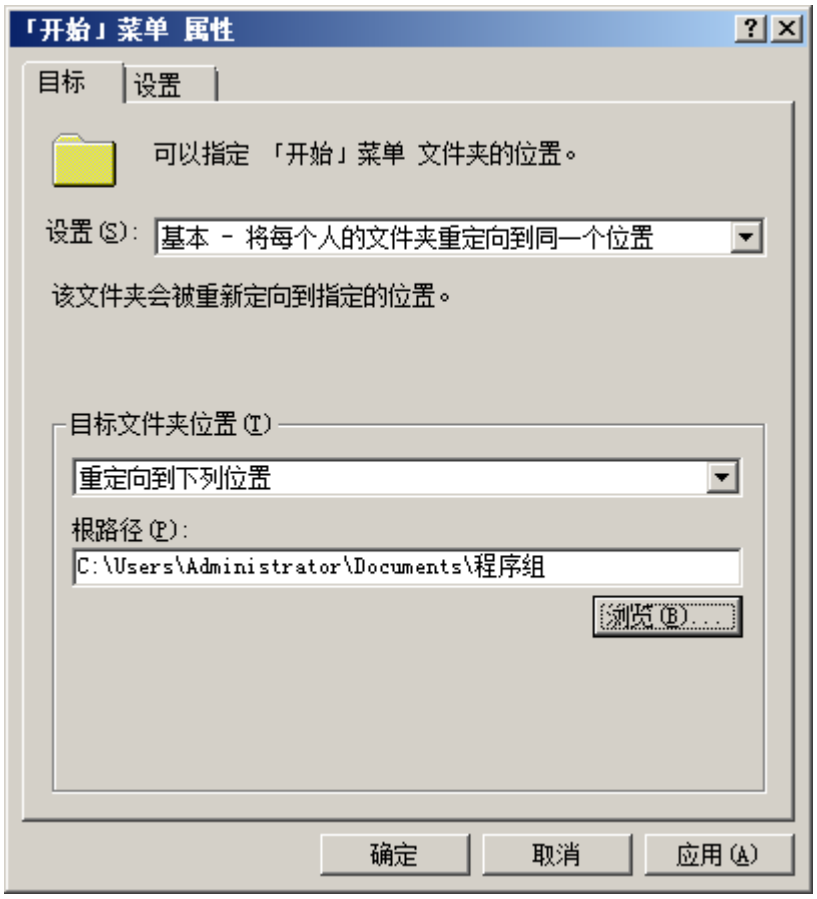
将该文件保存为 disk.bat，这样用户登陆时在本地工作站映射共享盘符。

然后在登录属性中点击添加－浏览－选中 disk .bat－确定，这样就配置完成了用户登陆脚本。

6.2 基于应用程序域策略管理（重定向开始菜单）：

策略组－用户配置－windows 设置－文件夹重定向－[开始]菜单－属性，如下图：





配置说明：我们将目标文件夹设置为：C:\Users\Administrator\Documents\程序组，这样我们需要在每个工作站上用 administrator 登陆后，在 C 盘我的文档中建立文件夹“程序组”，把我们需要的软件快捷方式如：Xedit，Newsmanage 拷贝到该文件夹，这样，用户登陆后在开始菜单中只出现我们需要的快捷方式。**注意：**在设置该项后，要在所有站点上以某个 edit 组用户登录，然后删除系统在程序组中自动生成的快捷方式。

6.2 基于桌面隐藏等域策略管理：

管理模板策略主要是用来屏蔽桌面等设置，在组策略－用户配置－管理模板中，对相应的策略设置启用。

1．桌面的设置（位置在“管理模板”→“桌面”）

1)启用“隐藏桌面上的所有图标”

2)启用“禁止添加、托、放和关闭任务栏的工具栏”

3)启用“禁用调整着桌面工具栏”

2．任务栏和开始菜单的设置(位置在“管理模板”→“任务栏和开始菜单”)

1) 启用“从开始菜单上删除‘文档’菜单”
2) 启用“从开始菜单中删除‘搜索’菜单”
3) 启用“从开始菜单中删除‘收藏夹’菜单”
4) 启用“从开始菜单中删除‘运行’菜单”
5) 启用“从开始菜单删除‘帮助’命令”(可选)
6) 启用“从开始菜单删除‘网络和拨号连接’”(可选)
7) 启用“禁用并删除‘Windows Update’的链接”
8) 启用“禁用开始菜单上的拖放上下文菜单”
9) 启用“在设置菜单上禁用程序”
10) 启用“将‘注销’添加到开始菜单”(可选)
11) 启用“禁止更改‘任务栏和开始菜单’设置”
12) 启用“禁用任务栏的上下文菜单” 注：在设置该项前，要在所有站点上以该用户登录，然后在任务栏右击，在“工具栏”中取消“快速启动”。(这样可以更加提高安全性，但此项设置也可以做为可选项)本项设置最好删除程序组里自动生成的快捷方式，这样可以减少工作量。
13) 启用“从开始菜单删除公用程序组”

3．限制用户网络设置权限（在“管理模板”→“网络”→“网络及拨号连接”）

1) 启用“禁止启用/停用 LAN 连接”
2) 启用“禁止访问 LAN 连接的属性”

最后在工作站本地登录，并在本地 Administrators 组中添加 test.com/edit 这个组，这样做可以使登陆用户仅能使用 edit 用户所配置的权限。

这样网络权限安全性设置完成。