Active Directory 教程

岳雷的微软网络课堂

本文所有内容均出自岳雷老师博客

敬请关注 http://yuelei.blog.51cto.com/

51cto_bbs_Kirin 整理制作

目录

为什么需要域？

对很多刚开始钻研微软技术的朋友来说，域是一个让他们感到很头疼的对象。域的重要性毋庸置疑，微软的重量级服务产品基本上都需要域的支持，很多公司招聘工程师的要求中也都明确要求应聘者熟悉或精通 Active Directory。但域对初学者来说显得复杂了一些，众多的技术术语，例如 Active Directory，站点，组策略，复制拓扑，操作主机角色，全局编录....很多初学者容易陷入这些技术细节而缺少了对全局的把握。从今天开始，我们将推出 Active Directory 系列博文，希望对广大学习 AD 的朋友有所帮助。

今天我们谈论的第一个问题就是为什么需要域这个管理模型？众所周知，微软管理计算机可以使用域和工作组两个模型，默认情况下计算机安装完操作系统后是隶属于工作组的。我们从很多书里可以看到对工作组特点的描述，例如工作组属于分散管理，适合小型网络等等。我们这时要考虑一个问题，为什么工作组就不适合中大型网络呢，难道每台计算机分散管理不好吗？下面我们通过一个例子来讨论这个问题。

假设现在工作组内有两台计算机，一台是服务器 Florence，一台是客户机 Perth。服务器的职能大家都知道，无非是提供资源和分配资源。服务器提供的资源有多种形式，可以是共享文件夹，可以是共享打印机，可以是电子邮箱，也可以是数据库等等。现在服务器 Florence 提供一个简单的共享文件夹作为服务资源，我们的任务是要把这个共享文件夹的访问权限授予公司内的员工张建国，注意，这个文件夹只有张建国一个人可以访问！那我们就要考虑一下如何才能实现这个任务，一般情况下管理员的思路都是在服务器上为张建国这个用户创建一个用户账号，如果访问者能回答出张建国账号的用户名和密码，我们就认可这个访问者就是张建国。基于这个朴素的管理思路，我们来在服务器上进行具体的实施操作。

首先，如下图所示，我们在服务器上为张建国创建了用户账号。

然后在共享文件夹中进行权限分配，如下图所示，我们只把共享文件夹的读权限授予了用户张建国。

好，接下来张建国就在客户机 Perth 上准备访问服务器上的共享文件夹了，张建国准备访问资源\\Florence\人事档案，服务器对访问者提出了身份验证请求，如下图所示，张建国输入了自己的用户名和口令。

如下图所示，张建国成功地通过了身份验证，访问到了目标资源。

看完了这个实例之后，很多朋友可能会想，在工作组模式下这个问题解决得很好啊，我们不是成功地实现了预期目标嘛！没错，在这个小型网络中，确实工作组模型没有暴露出什么问题。但是我们要把问题扩展一下！现在假设公司不是一台服务器，而是 500 台服务器，这大致是一个中型公司的规模，那么我们的麻烦就来了。如果这 500 台服务器上都有资源要分配给张建国，那会有什么样的后果呢？由于工作组的特点是分散管理，那么意味着每台服务器都要给张建国创建一个用户账号！张建国这个用户就必须痛不欲生地记住自己在每个服务器上的用户名和密码。而服务器管理员也好不到哪儿去，每个用户账号都重新创建 500 次！如果公司内有 1000 人呢？我们难以想象这么管理网络资源的后果，这一切的根源都是由于工作组的分散管理！现在大家明白为什么工作组不适合在大型的网络环境下工作了吧，工作组这种散漫的管理方式和大型网络所要求的高效率是背道而驰的。

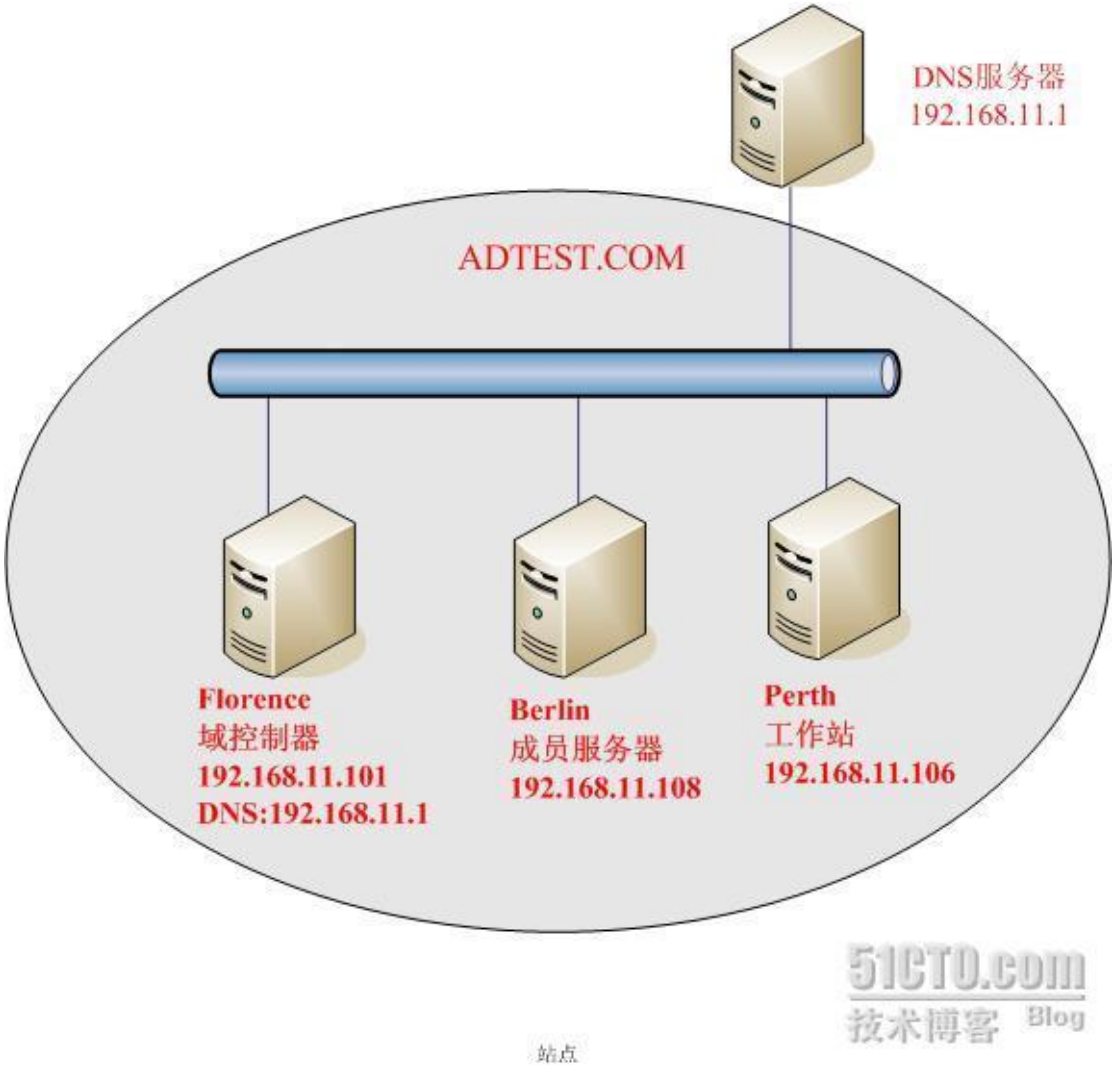
既然工作组不适合大型网络的管理要求，那我们就要重新审视一下其他的管理模型了。域模型就是针对大型网络的管理需求而设计的，域就是共享用户账号，计算机账号和安全策略的计算机集合。从域的基本定义中我们可以看到，域模型的设计中考虑到了用户账号等资源的共享问题，这样域中只要有一台计算机为公司员工创建了用户账号，其他计算机就可以共享账号了。这样就很好地解决刚才

我们提到的账号重复创建的问题。域中的这台集中存储用户账号的计算机就是域控制器，用户账号，计算机账号和安全策略被存储在域控制器上一个名为 Active Directory 的数据库中。

上述这个简单的例子说明的只是域强大功能的冰山一角，其实域的功能远远不止这些。从下篇博文我们将开始介绍域的部署以及管理，希望大家在使用过程中逐步增加感性认识，对域有更加深入及全面的了解，能够掌握好 Active Directory 这个微软工程师必备的重要知识点。

部署第一个域

在上篇博文中我们介绍了部署域的意义，今天我们来部署第一个域。一般情况下，域中有三种计算机，一种是域控制器，域控制器上存储着 Active Directory；一种是成员服务器，负责提供邮件，数据库，DHCP 等服务；还有一种是工作站，是用户使用的客户机。我们准备搭建一个基本的域环境，拓扑如下图所示，Florence 是域控制器，Berlin 是成员服务器，Perth 是工作站。



部署一个域大致要做下列工作：

1 DNS 前期准备

2 创建域控制器

3 创建计算机账号

4 创建用户账号

一 DNS 前期准备

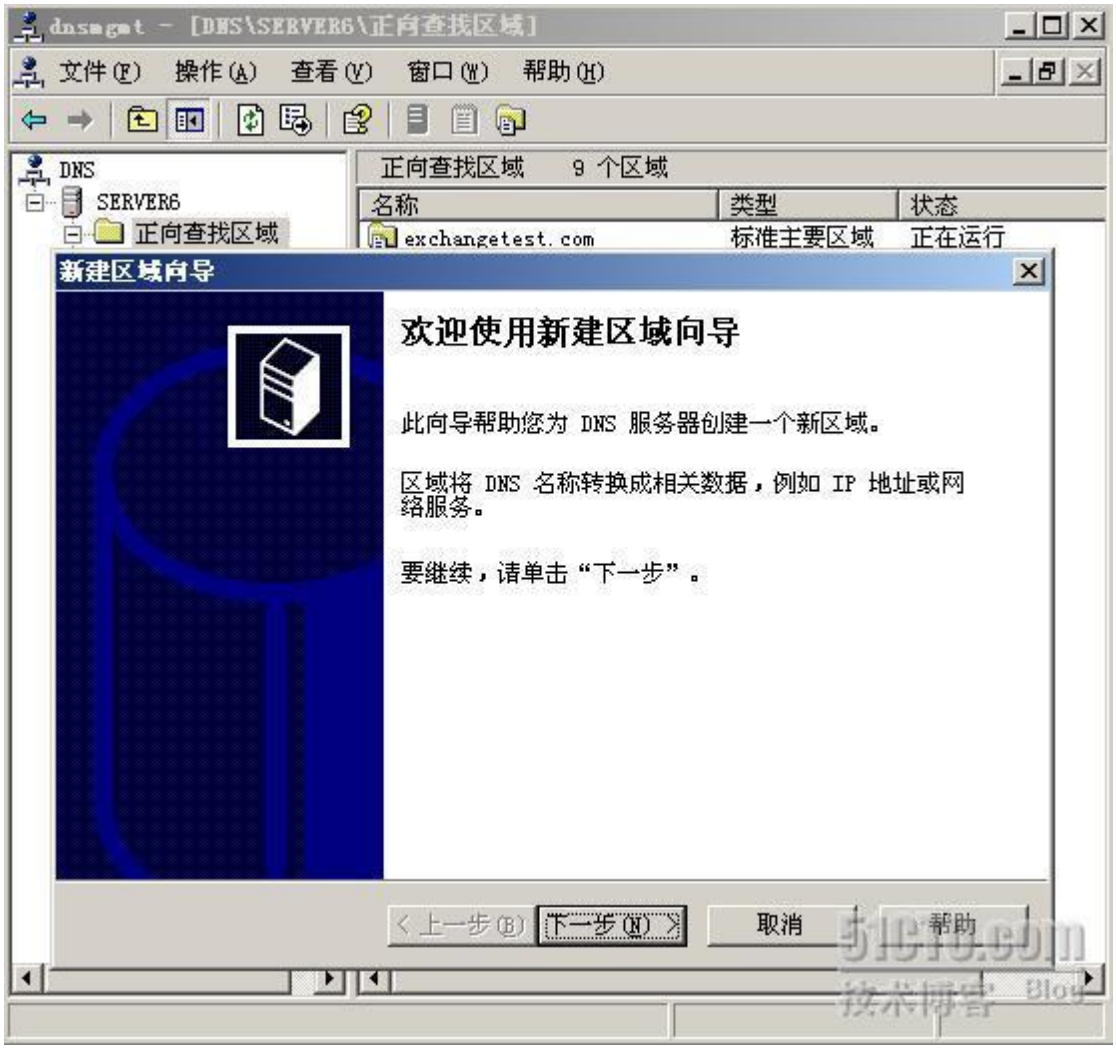
DNS 服务器对域来说是不可或缺的，一方面，域中的计算机使用 DNS 域名，DNS 需要为域中的计算机提供域名解析服务；另外一个重要的原因是域中的计算机需要利用 DNS 提供的 SRV 记录来定位域控制器，因此我们在创建域之前需

要先做好 DNS 的准备工作。那么究竟由哪台计算机来负责做 DNS 服务器呢？一般工程师有两种选择，要么使用域控制器来做 DNS 服务器，要么使用一台单独的 DNS 服务器。我一般使用一台独立的计算机来充当 DNS 服务器，这台 DNS 服务器不但为域提供解析服务，也为公司其他的业务提供 DNS 解析支持，大家可以根据具体的网络环境来选择 DNS 服务器。

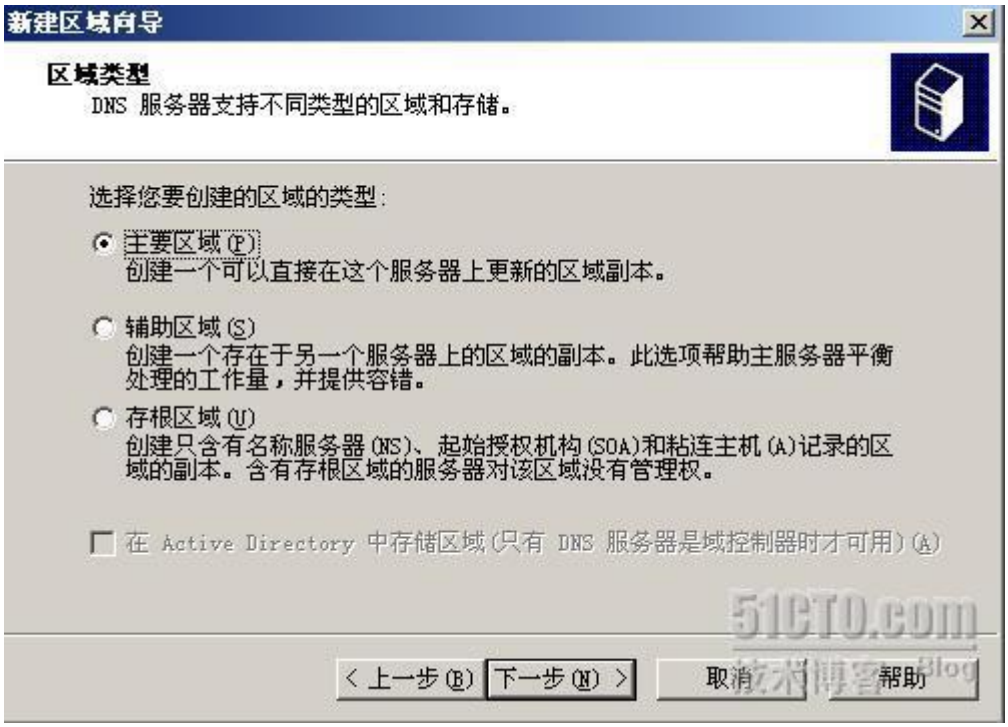
在创建域之前，DNS 服务器需要做好哪些准备工作呢？

1 创建区域并允许动态更新

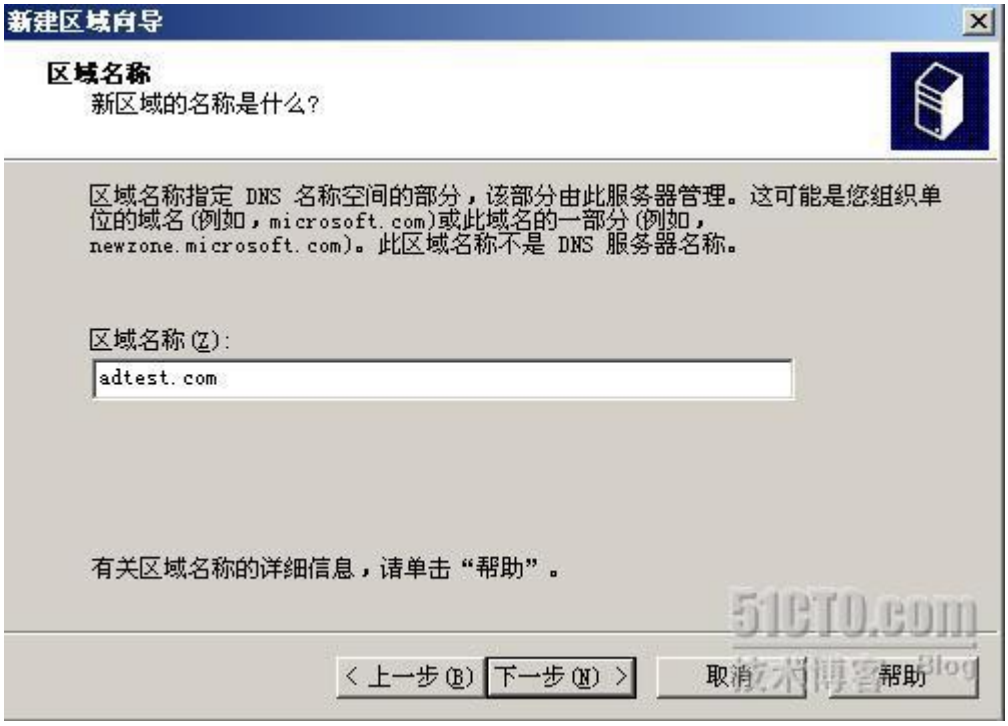
首先我们要在 DNS 服务器上创建出一个区域，区域的名称和域名相同，域内计算机的 DNS 记录都创建在这个区域中。我们在 DNS 服务器上打开 DNS 管理器，如下图所示，右键单击正向查找区域，选择新建一个区域。出现新建区域向导后，点击下一步继续。



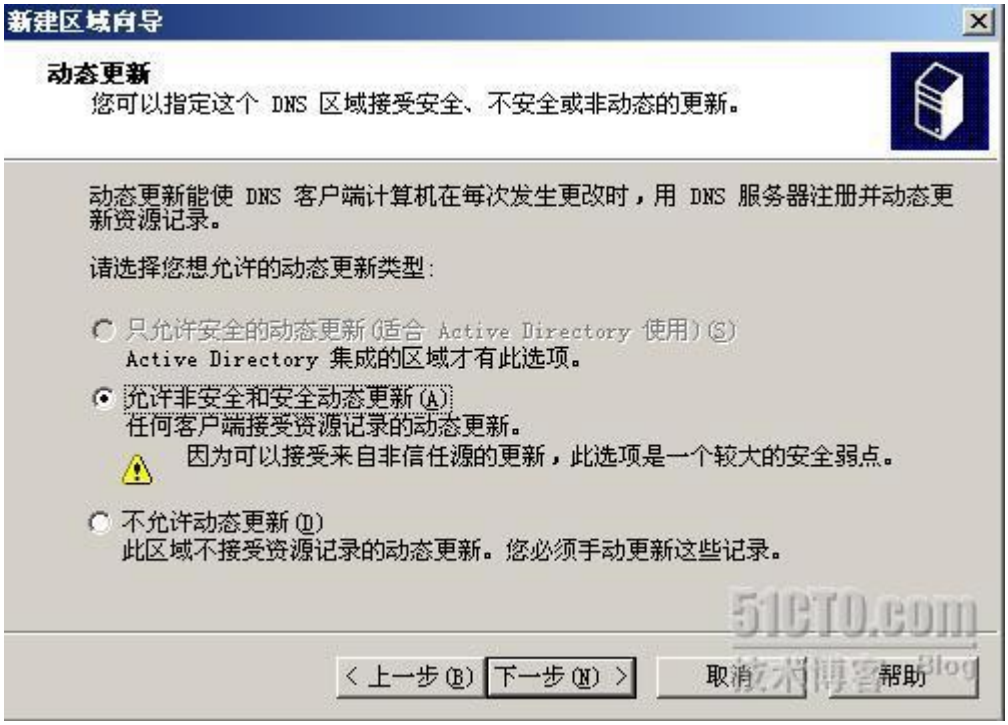
区域类型选择“主要区域”。



区域名称和域名相同，是 adtest.com。



区域一定要允许动态更新，因为在创建域的过程中需要向 DNS 区域中写入 A 记录，SRV 记录和 Cname 记录。

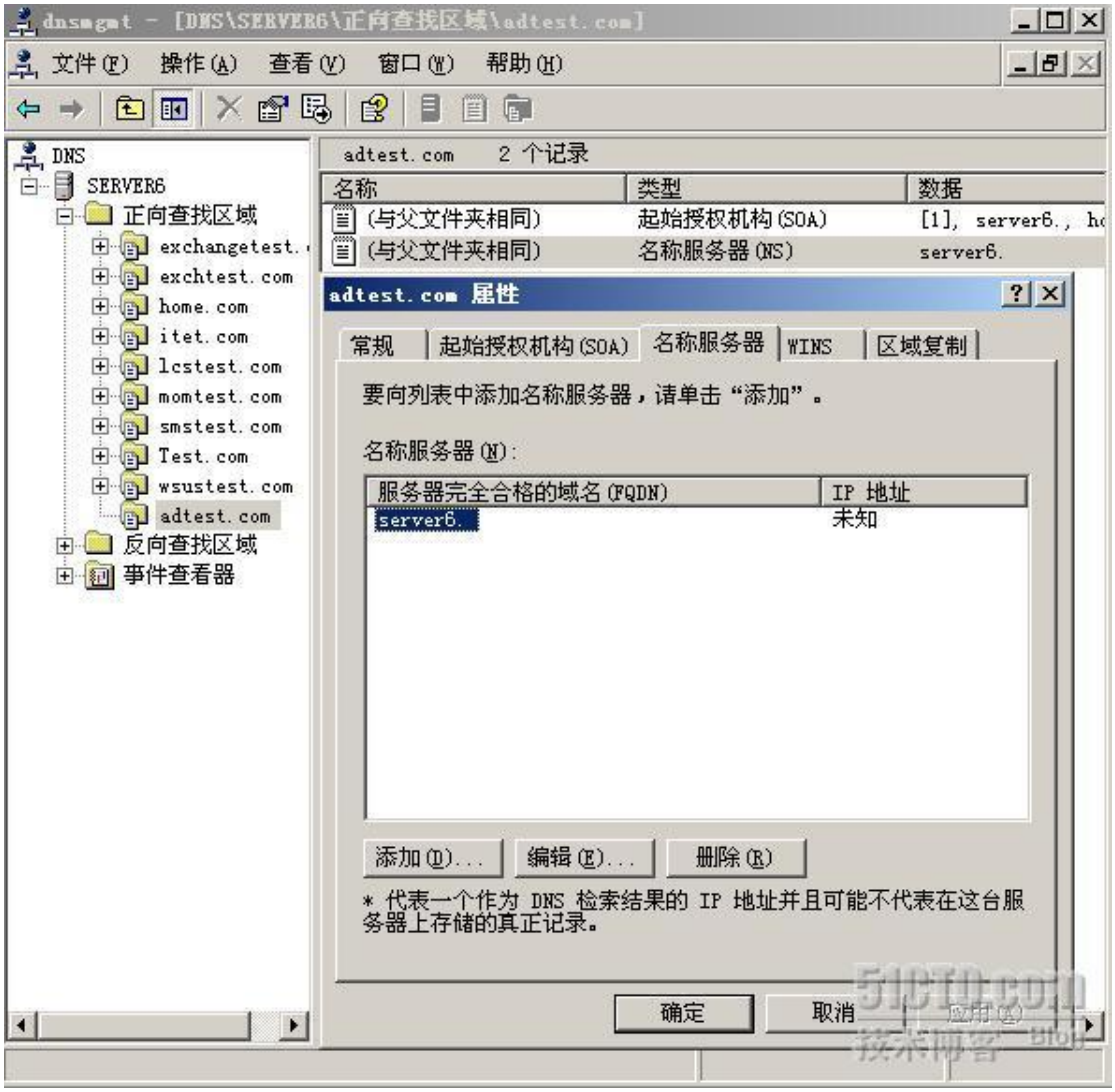


区域创建完毕，点击完成结束创建。

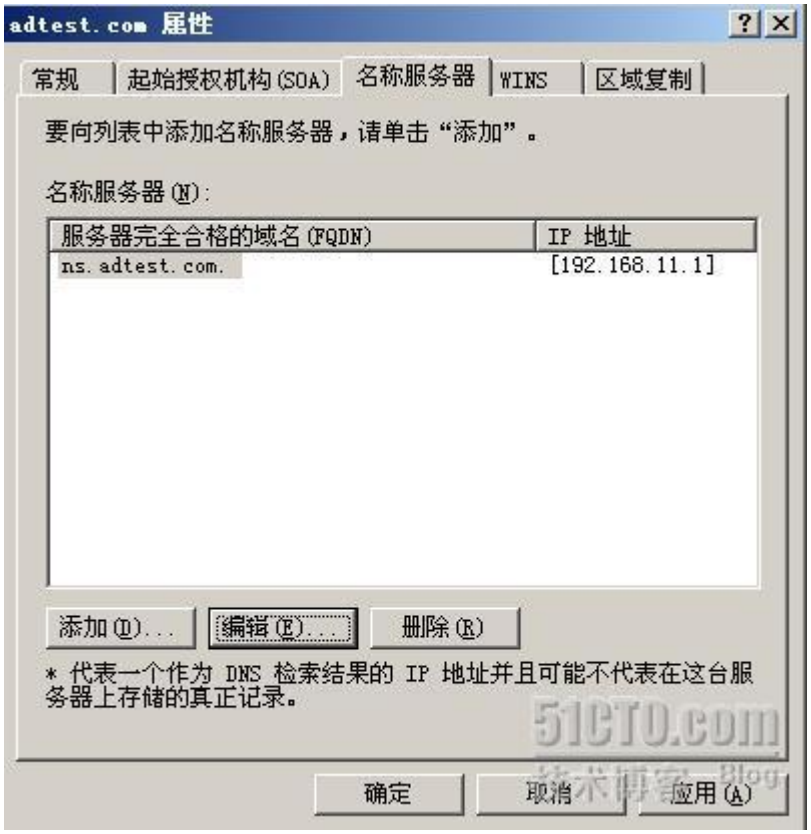
2 检查 NS 和 SOA 记录

区域创建完成后，一定要检查一下区域的 NS 记录和 SOA 记录。在前面的 DNS 课程中，我们已经介绍了 NS 记录和 SOA 记录的意义，NS 记录描述了有多少个 DNS 服务器可以解析这个区域，SOA 记录描述了哪个 DNS 服务器是区域

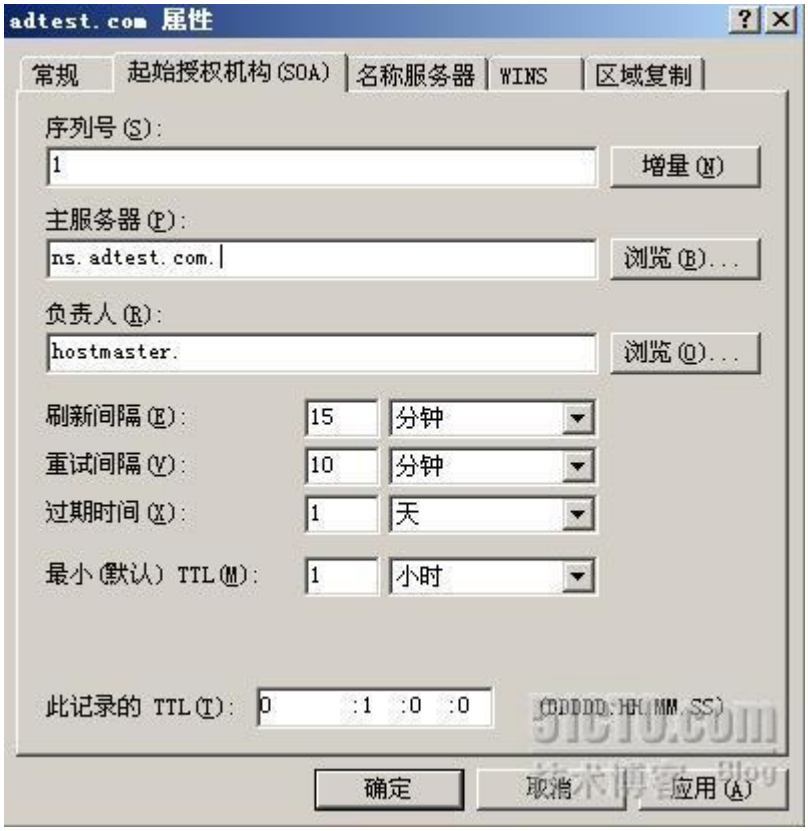
的主服务器。如果 NS 记录和 SOA 记录出错，域的创建过程中就无法向 DNS 区域中写入应有的记录。在 DNS 服务器上打开 DNS 管理器，在 adtest.com 区域中检查 ns 记录，如下图所示，我们发现 ns 记录不是一个有效的完全合格域名，我们需要对它进行修改。



如下图所示，我们把 ns 记录改为 ns.adtest.com.，解析出的 IP 地址和 DNS 服务器的 IP 是吻合的，这样我们就完成了 ns 记录的修改。



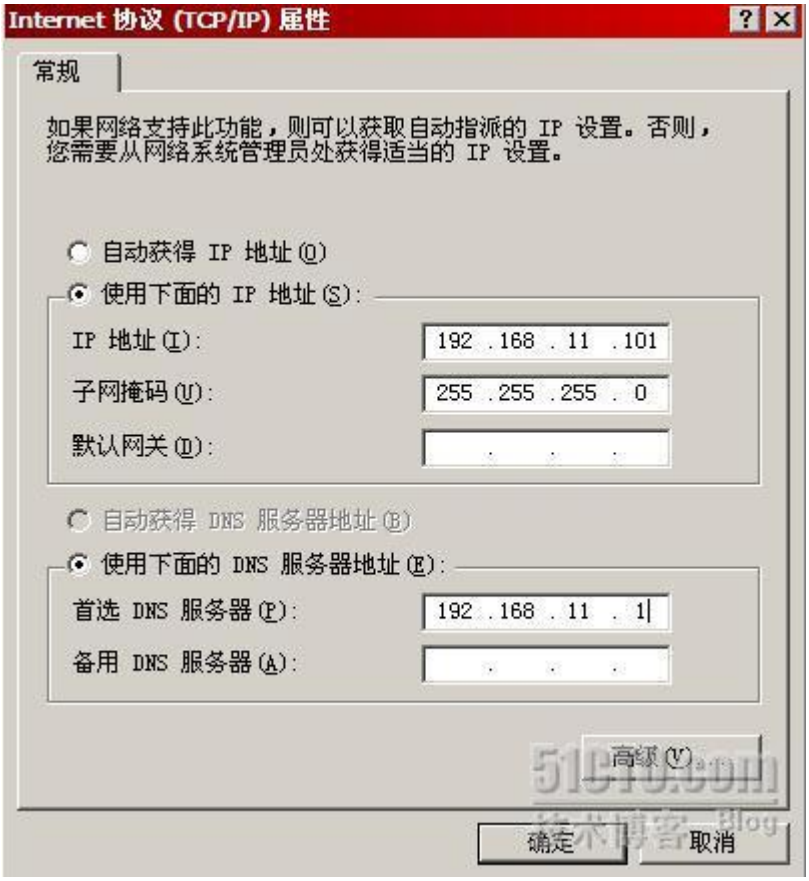
如下图所示，我们把区域的 SOA 记录也同样进行修改，现在区域的主服务器是 ns.adtest.com.，这样 SOA 记录也修改完毕了。



至此，DNS 准备工作完成，我们接下来可以部署域了。

二 创建域控制器

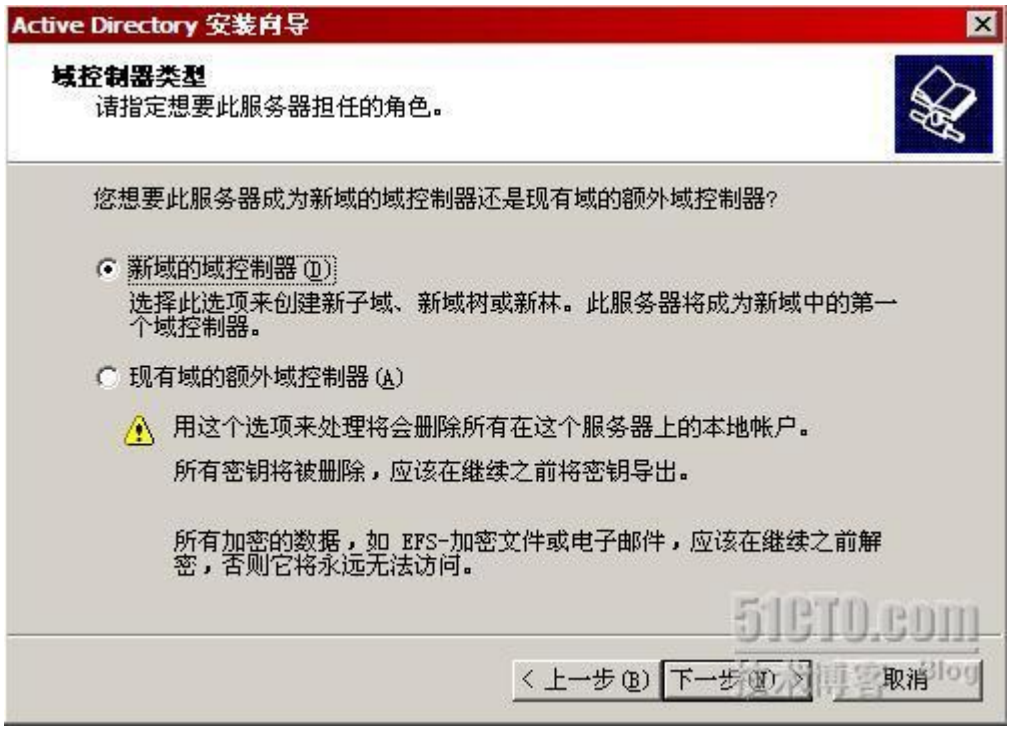
有了 DNS 的支持，我们现在可以开始创建域控制器了，域控制器是域中的第一台服务器，域控制器上存储着 Active Directory，可以说，域控制器就是域的灵魂。我们准备在 Florence 上创建域控制器，首先检查 Florence 网卡的 TCP/IP 属性，注意，Florence 应该使用 192.168.11.1 作为自己的 DNS 服务器。因为我们刚刚在 192.168.11.1 上创建了 adtest.com 区域。



如下图所示，在 Florence 上运行 Dcpromo，开始域控制器的创建。

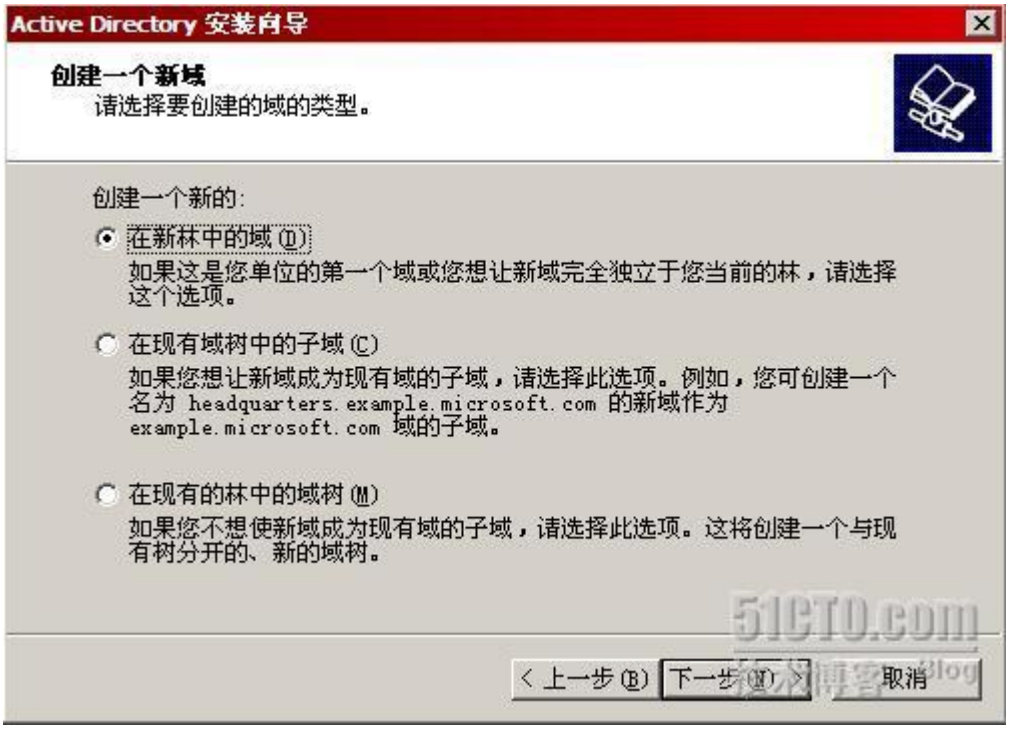
如下图所示，出现 Active Directory 安装向导，创建域控制器其实就是在 Florence 上安装一个 Active Directory 数据库，点击下一步继续。

Adtest.com 是一个新创建的域，因为我们选择创建“新域的域控制器”。



如下图所示，我们选择创建一个“在新林中的域”，这个选项是什么意思呢？我们虽然只是简单地创建了一个域，但其实从逻辑上讲是创建了一个域林。因为域

一定要隶属于域树，域树一定要隶属于域林。因为我们实际上是创建了一个域林，虽然这个域林内只有一棵域树，域树内只有一个树根。

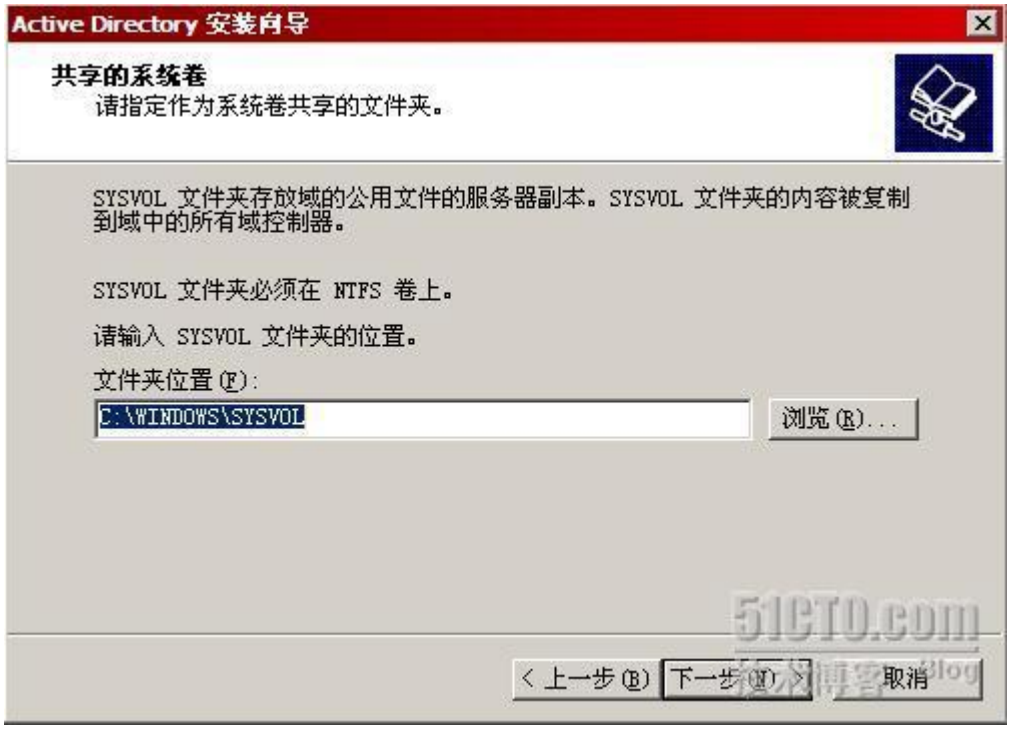


输入域的 DNS 名称，adtest.com。

域的 NETBIOS 名称是 ADTEST，由于.在 NETBIOS 名称中是非法字符，因为基本上域的 NETBIOS 名称就是域名中.之前的部分。

Active Directory 数据库的路径我们使用了默认值，如果在生产环境，可以考虑把数据库和日志部分分开存储

Sysvol 文件夹的路径我们也使用默认值，至于 Sysvol 文件夹是干嘛的，我们后续会有介绍。



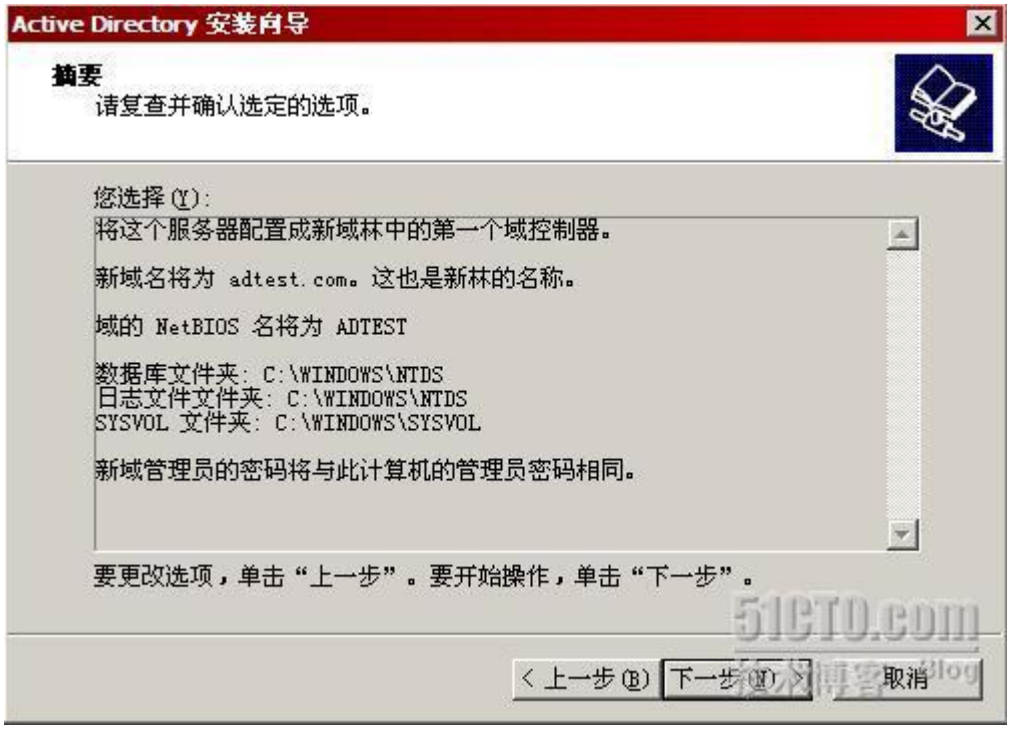
接下来 Active Directory 的安装向导会对 DNS 服务器进行检测，检查是否在 DNS 服务器上已经创建了和域名相同的区域，而且区域是否允许动态更新。如下图所示，DNS 检测通过。注意，如果 DNS 检测有问题，我们应该及时排除故障，而不应该继续向下进行。

接下来要选择用户和组的默认权限，我们选择了不允许匿名用户查询域中的信

息。

设置一下还原模式的管理员口令，我们从备份中恢复 Active Directory 时需要用到。

好，如下图所示仔细检查一下创建域的各项设置是否正确，如果没有问题我们就开工了！

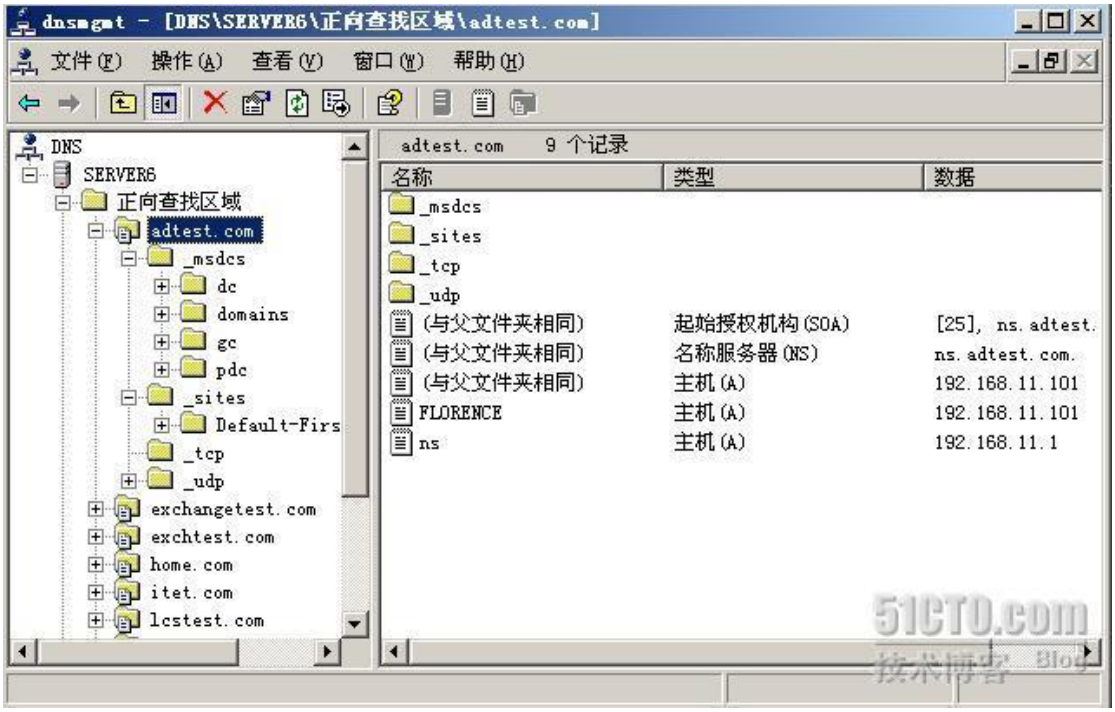


如下图所示，Active Directory 安装向导开始在 Florence 上安装 Active Directory。

如下图所示，重启计算机后即可完成 Active Directory 的安装。

重启 Florence 后我们发现已经可以用域管理员的身份登录了，adtest.com 域已经被成功创建了。

检查 DNS 服务器，我们发现 DNS 区域中已经自动创建了很多记录，这些记录的作用以后我们再来分析，现在大家只要注意检查一下创建域时有没有把这些记录创建出来，如果没有那就有问题了。

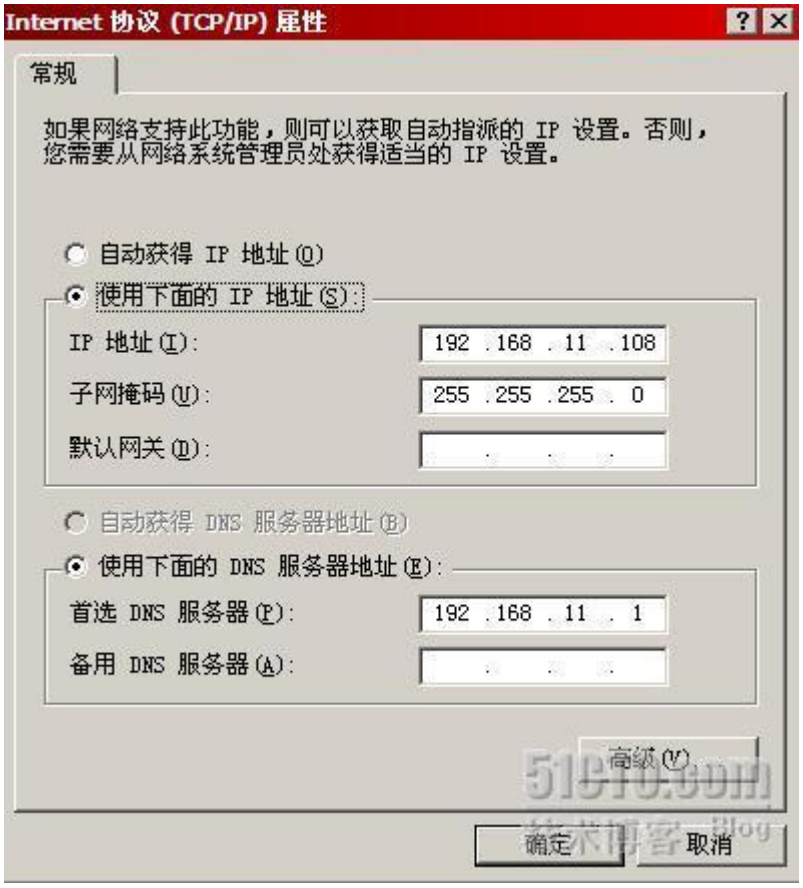


至此，我们完成了域控制器的创建，adtest.com 域诞生了！

三 创建计算机账号

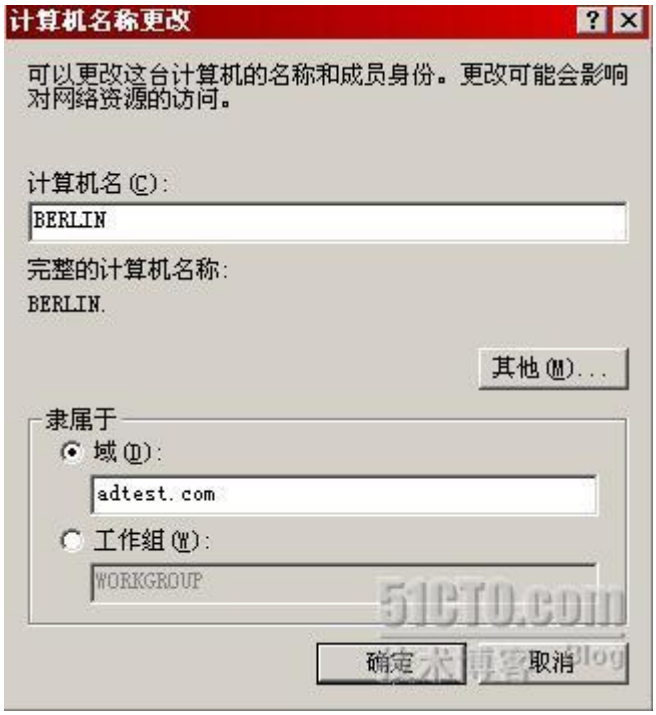
创建计算机账号就是把成员服务器和用户使用的客户机加入域，这些计算机加入域时会在 Active Directory 中创建计算机账号。创建计算机账号从操作上看非常简单，但其实背后涉及的东西很多，例如域控制器和加入域的计算机要共享一个密钥等等，这些内容我们在后期会为大家介绍。

以 Berlin 为例为大家介绍如何把计算机加入域，首先要确保 Berlin 已经使用了 192.168.11.1 作为自己的 DNS 服务器，否则 Berlin 无法利用 DNS 定位域控制器。



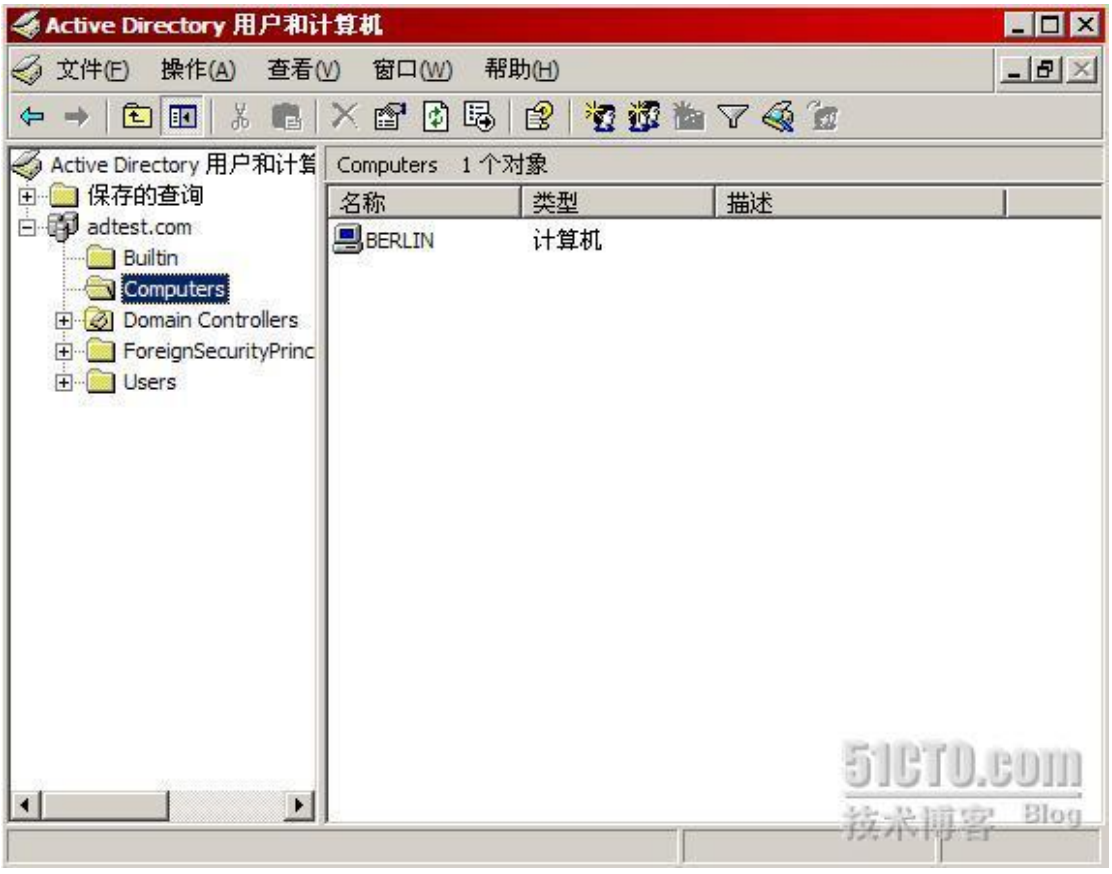
如下图所示，在 Berlin 的计算机属性中切换到“计算机名”标签，点击“更改”。

我们选择让 Berlin 隶属于域，域名是 adtest.com。



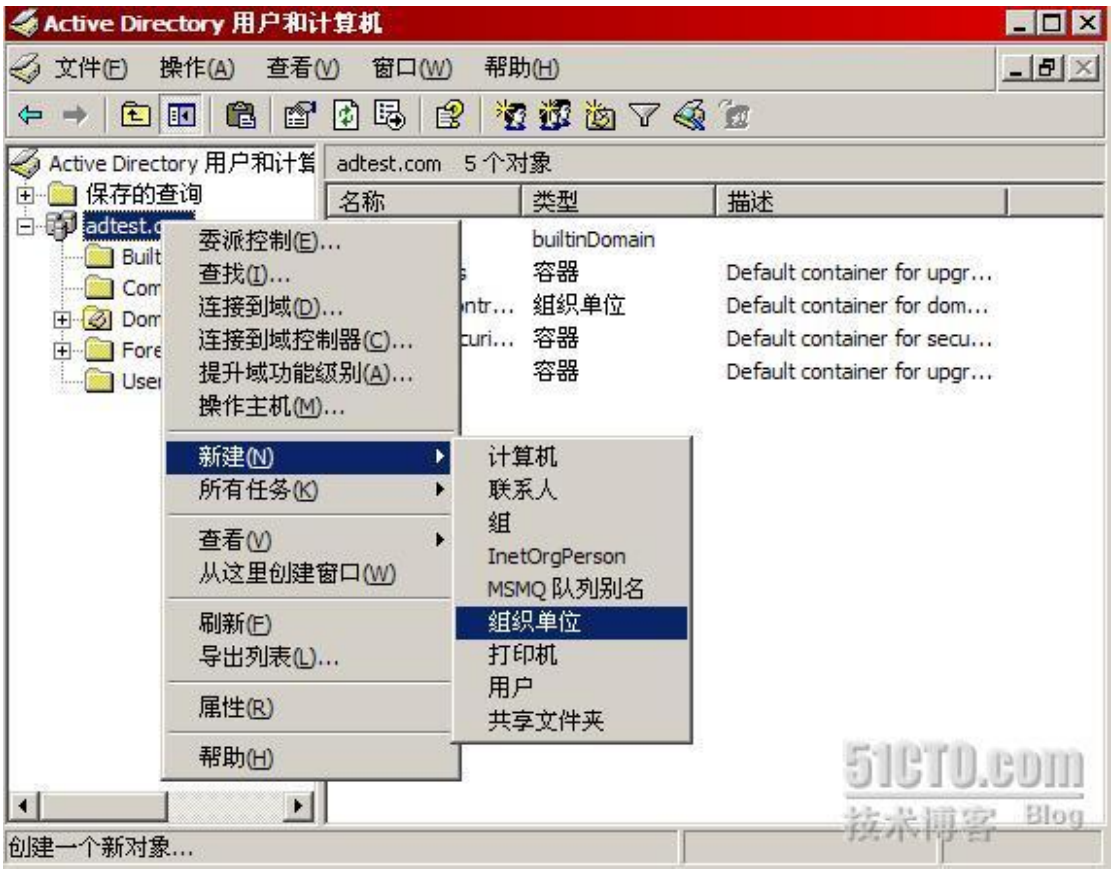
这时系统需要我们输入一个有权限在 Active Directory 中创建计算机账号的用户名和口令，我们输入了域管理员的用户名和密码。

系统弹出一个窗口欢迎 Berlin 加入域，这时在 Florence 上打开 Active Directory 用户和计算机，如下图所示，我们发现 Berlin 的计算机账号已经被创建出来了。



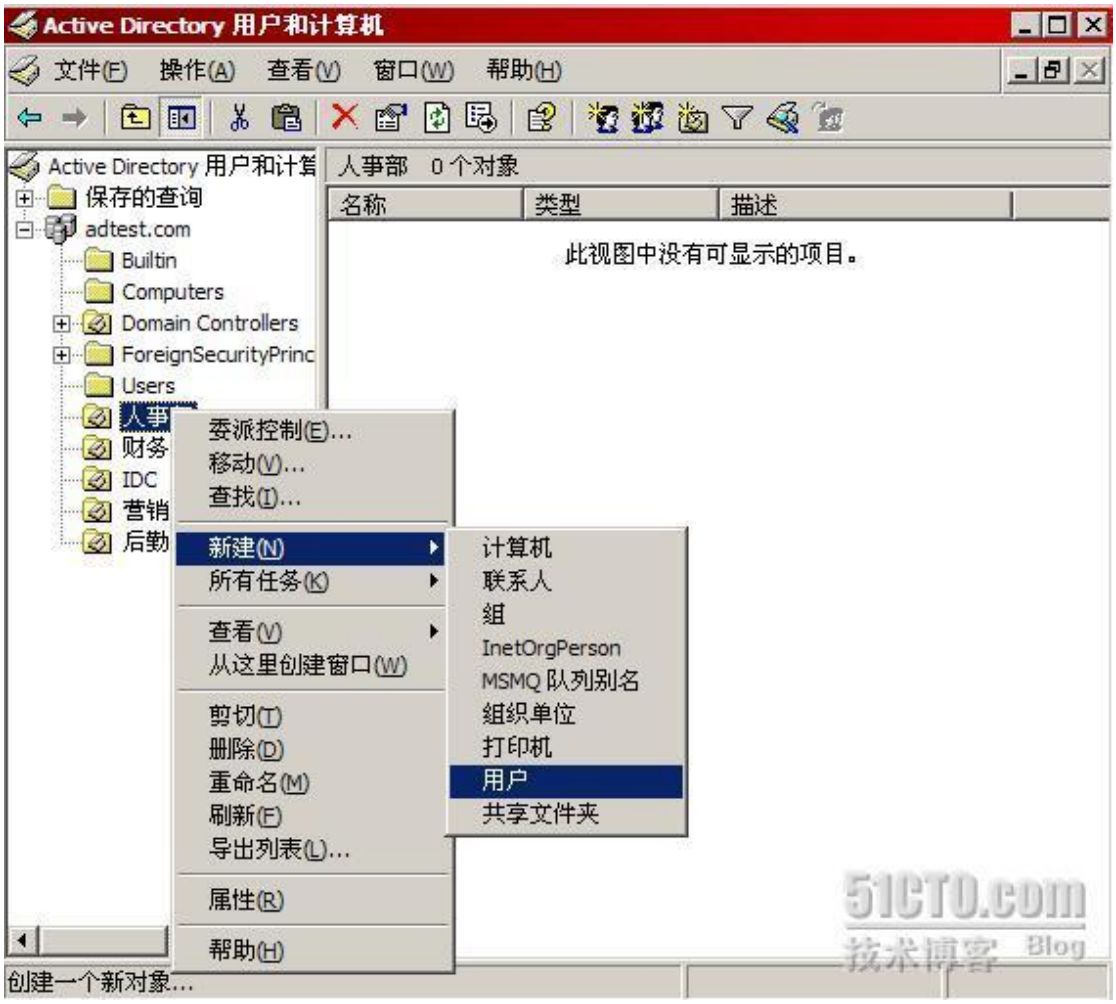
四 创建用户账号

创建完计算机账号后，我们需要为企业内的员工在 Active Directory 中创建关联的用户账号。首先我们应该在 Active Directory 中利用组织单位展示出企业的管理架构，如下图所示，我们为大家演示一下如何创建一个组织单位。打开 Active Directory 用户和计算机，选择新建组织单位。



输入组织单位的名称，点击确定后一个组织单位就创建完成了，是不是很简单呢。

创建了组织单位后，我们就可以在组织单位中创建用户账号了，如下图所示，我们在人事部的组织单位中选择新建一个用户。



输入用户的姓名及登录名等参数，点击下一步继续。

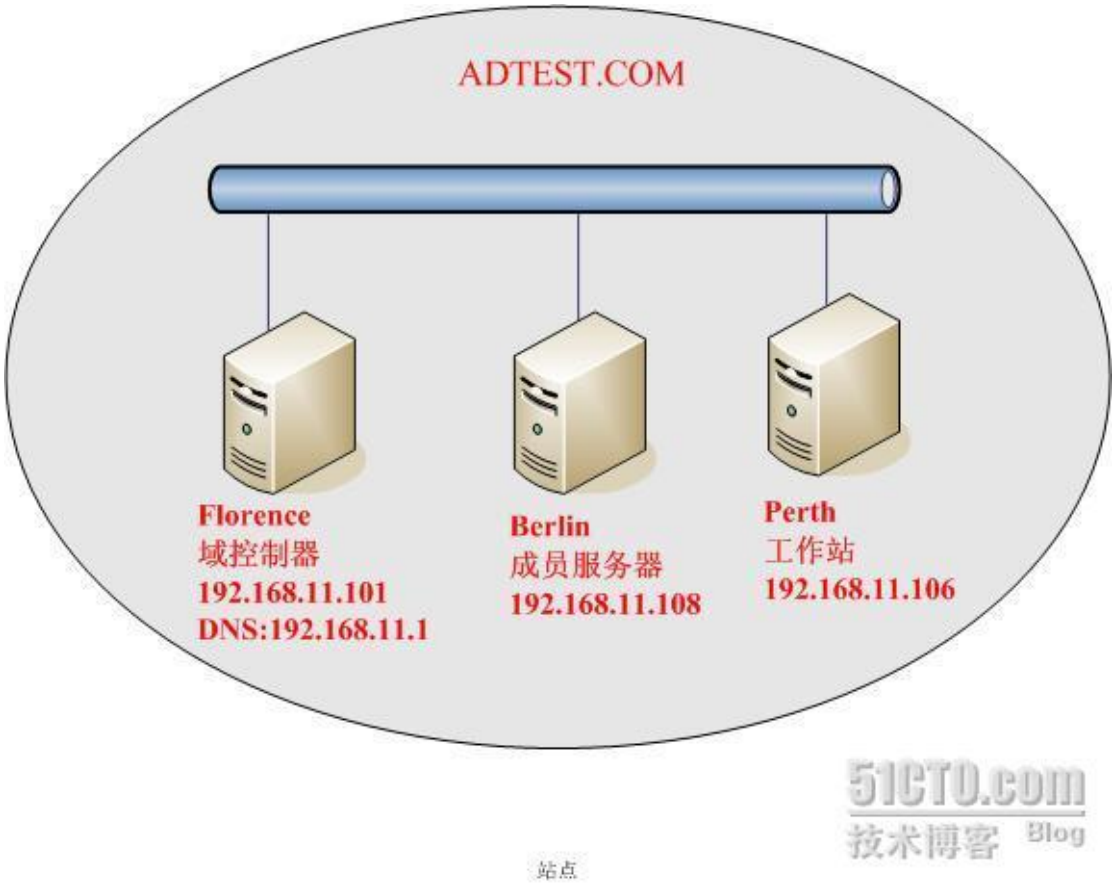
输入用户密码，选择“密码永不过期”。

点击完成后我们就可以轻松地创建出一个用户账号。其实，用户账号中有很多的配置工作需要做，我们在后续的课程中会有一个专题为大家介绍。

目前为止，我们已经创建了一个域，也在域中创建了计算机账号和用户账号。那么，域的管理优势如何能够加以体现，目前这个域模型有没有什么缺陷呢？我们在下篇博文中将解决这个问题。

用备份进行 ACTIVE DIRECTORY 的灾难重建

上篇博文中我们介绍了如何部署第一个域，现在我们来看看我们能够利用域来做些什么。域中的计算机可以共享用户账号，计算机账号和安全策略，我们来看看这些共享资源给我们在分配网络资源时带来了哪些改变。实验拓扑如下图所示，我们现在有个简单的任务，要把成员服务器 Berlin 上一个共享文件夹的读权限分配给公司的员工张建国。上次我们实验时已经为张建国创建了用户账号，这次我们来看看如何利用这个用户账号来实现资源分配的目标。



如下图所示，我们在成员服务器 Berlin 上右键点击文件夹 Tools，选择“共享和安全”，准备把 Tools 文件夹共享出来。

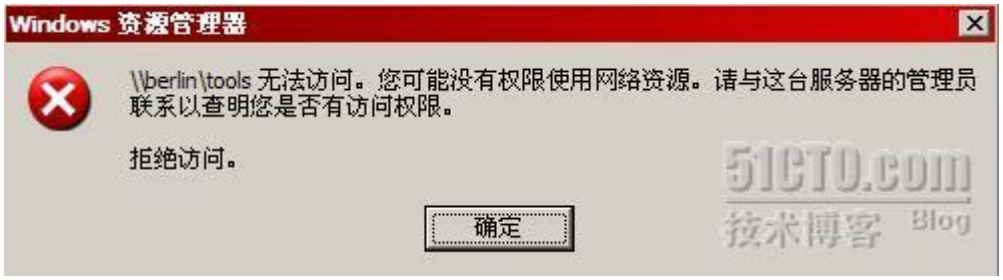
把 Tools 文件夹共享出来，共享名为 Tools，同时点击“权限”，准备把 Tools 文件夹的读权限只分配给张建国。

Tools 文件夹的默认共享权限是 Everyone 组只读，我们删除默认的权限设置，点击添加按钮，准备把文件夹的读权限授予张建国。

如下图所示，我们选择 adtest.com 域中的张建国作为权限的授予载体，这时我们要理解域的共享用户账号的含义，在域控制器上为张建国创建了用户账号后，成员服务器分配资源时就可以使用这些用户账号了。

我们把 Tools 文件夹的读权限授予了张建国。

我们先用域管理员登录访问一下 Berlin 上的 Tools 共享文件夹，如下图所示，域管理员没有访问共享文件夹的权限。这个结果和我们的权限分配是一致的，我们只把共享文件夹的权限授予了张建国。



如下图所示，在 Perth 上以张建国的身份登录。

张建国访问 Berlin 上的共享文件夹 Tools，如下图所示，张建国顺利地访问到了目标资源，我们的资源分配达到了预期的效果。

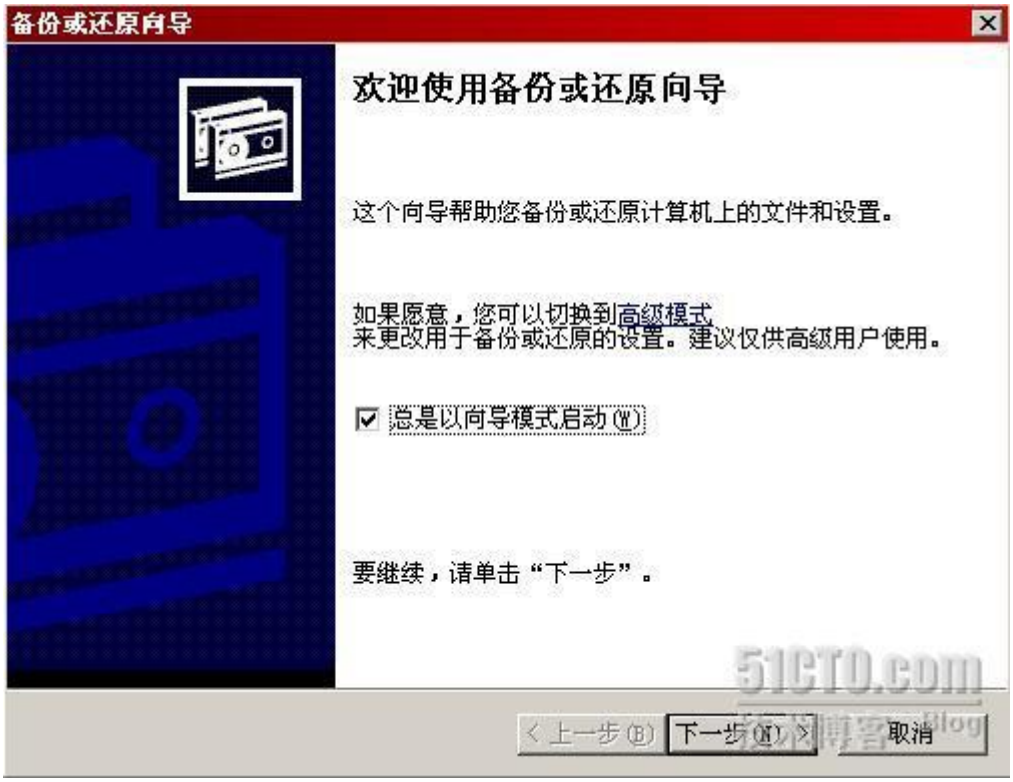
做完这个实验后，我们应该想一下，为什么张建国在访问共享文件夹时没有被要求身份验证呢？这是个关键问题，答案是这样的。当张建国登录时，输入的用户名和口令将送到域控制器请求验证，域控制器如果认可了张建国输入的用户名和口令，域控制器将为张建国发放一个电子令牌，令牌中描述了张建国隶属于哪些组等信息，令牌就相当于张建国的电子身份证。当张建国访问 Berlin 上的共享文件夹时，Berlin 的守护进程会检查访问者的令牌，然后和被访问资源的访问控制列表进行比较。如果发现两者吻合，例如本例中 Berlin 上的共享文件夹允许域中的张建国访问，而访问者的令牌又证明了自己就是域中的张建国，那么访问者就可以透明访问资源，无需进行其他形式的身份验证。

我们可以设想一下基于域的权限分配，每天早晨公司员工上班后，在自己的计算机上输入用户名和口令，然后域控制器验证后发放令牌，员工拿到令牌后就可以透明地访问域中的各种被授权访问的资源，例如共享打印机，共享文件夹，数据库，电子邮箱等。员工除了在登录时要输入一次口令，以后在访问资源时都不需要再输入口令了，这种基于域的资源分配方式是不是非常的高效灵活呢？

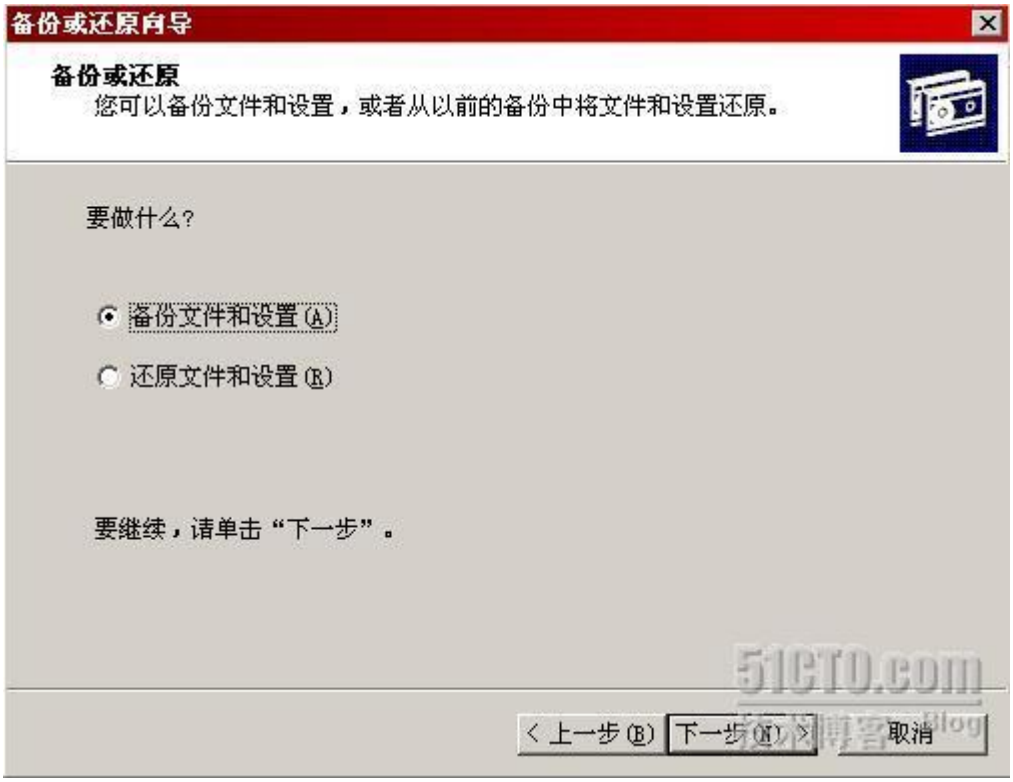
但是，我们要考虑一个问题，万一这个域控制器坏了怎么办？！如果这个域控制器损坏了，那用户登录时可就无法获得令牌了，没有了这个令牌，用户就没法向成员服务器证明自己的身份，嘿嘿，那用户还能访问域中的资源吗？结果不言而喻，整个域的资源分配趋于崩溃。这个后果很严重，那我们应该如何预防这种灾难性的后果呢？我们可以考虑对活动目录进行备份以及部署额外域控制器，今天我们先看如何利用对 Active Directory 的备份来实现域控制器的灾难重建。

如果只有一个域控制器，那么我们可以利用 Windows 自带的备份工具对 Active directory 进行完全备份，这样万一这个域控制器有个三长两短，备份可以帮助我们从困境中解脱出来。

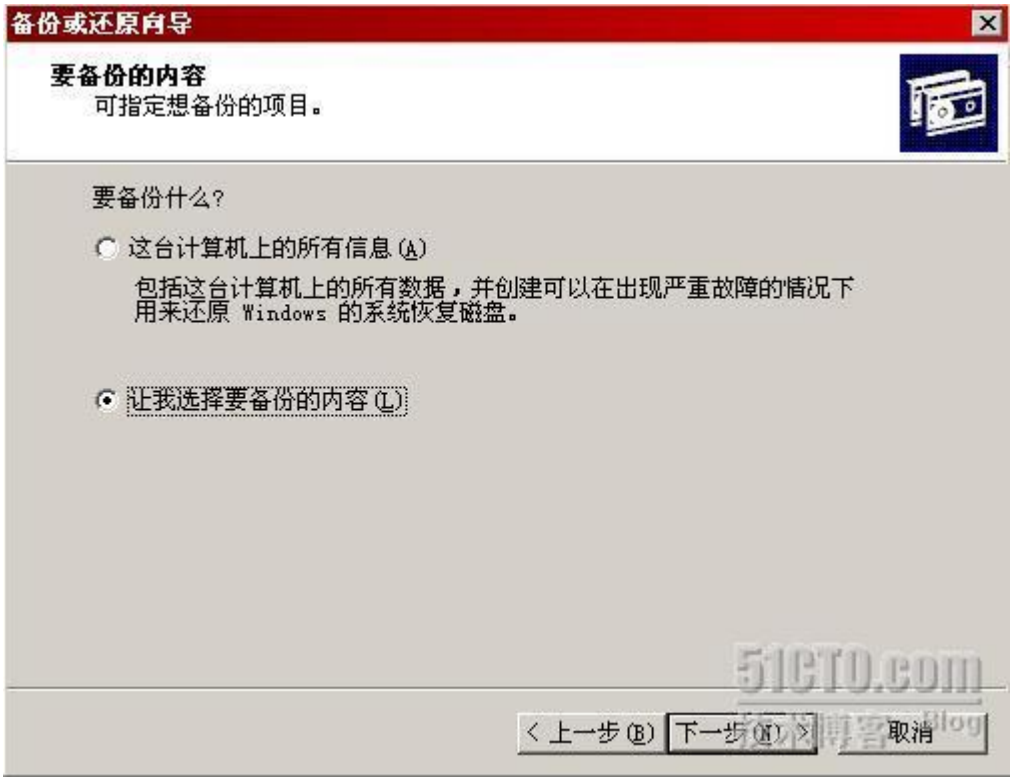
在 Florence 上依次点击 开始－程序－附件－系统工具－备份，如下图所示，出现了备份还原向导，点击下一步继续。



选择备份文件和设置。



不用备份计算机上的所有信息，我们只备份 Active Directory，因此我们手工选择要备份的内容。



如下图所示，我们选择备份 System State，System State 中包含了 Active Directory。其实我们只需要 System State 中的 Active Directory，Registry 和 Sysvol 就够了，但备份工具中不允许再进行粒度更细致的划分，因此我们选择备份整个 System State。

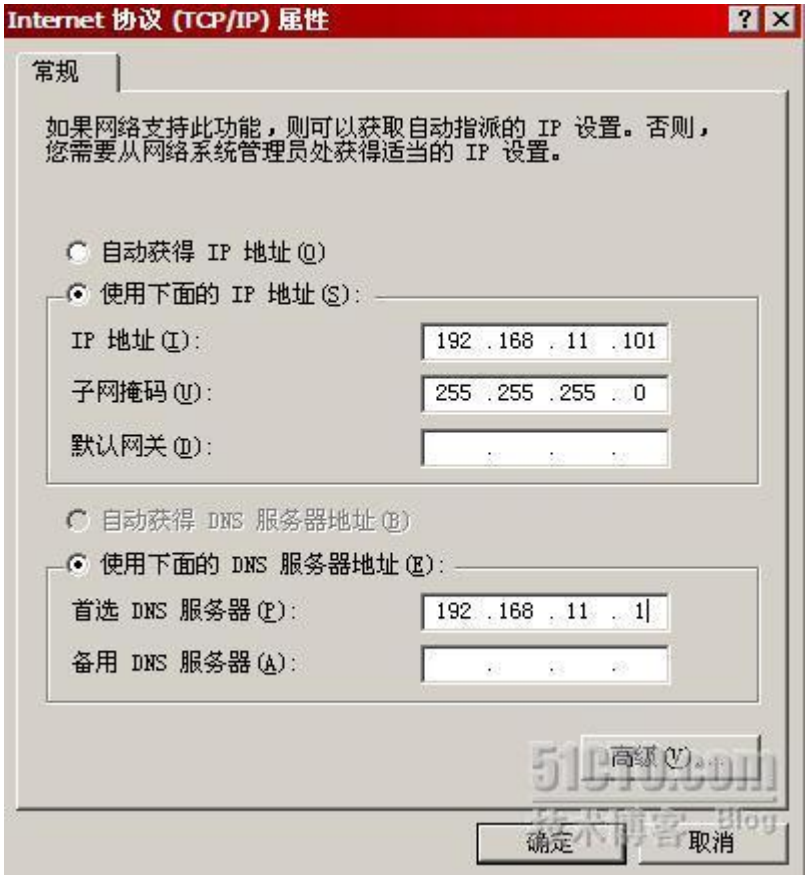
我们把 System State 备份在 C:\ADBAK 目录下。

点击完成结束备份设置。

如下图所示，备份开始，等备份完成后我们把备份文件复制到文件服务器进行保存即可。

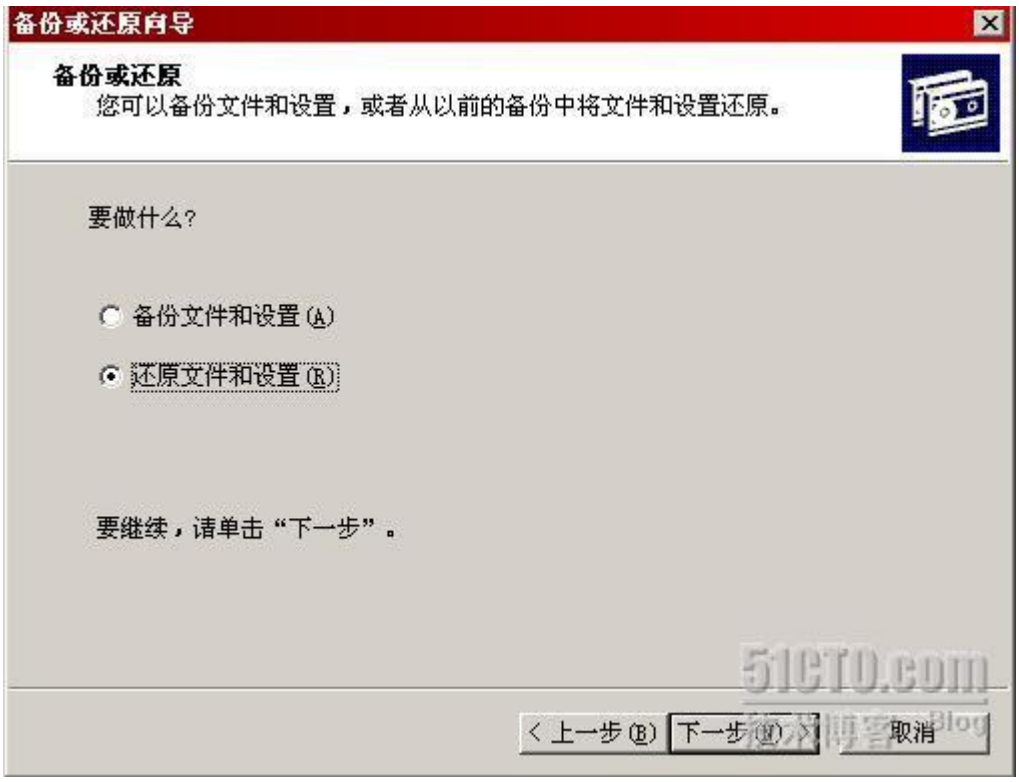
好，备份完成后，我们假设域控制器 Florence 发生了物理故障，现在我们用另外一台计算机来接替 Florence。如下图所示，我们把这台新计算机也命名为 Florence，IP 设置和原域控制器也保持一致，尤其是一定要把 DNS 指向为 ADTEST.COM 提供解析支持的那个 DNS 服务器，在此例中就是 192.168.11.1。而且新的计算机不需要创建 Active Directory，我们从备份中恢复 Active Directory 即可。


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: FLORENCE.
工作组: WORKGROUP
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)



从文件服务器上把 System State 的备份复制到新的 Florence 上，然后启动备份工具，如下图所示，选择下一步继续。

这次我们选择还原文件和设置。



如下图所示，通过浏览按钮选择要还原的文件是 C:\ADBAK\BACKUP.BKF，备份工具显示出了 BACKUP.BKF 的编录内容，勾选要还原的内容是 System State，选择下一步继续。

还原设置完毕，点击完成结束。

如下图所示，还原开始，还原结束后我们重新启动计算机即可 Active Directory 的重建工作。

重新启动 Florence 后，如下图所示，我们发现 Active Directory 已经恢复了。

Florence 的角色也发生了改变。

尝试让域用户进行登录，一切正常，至此，Active Directory 恢复完成！

如果域中唯一的域控制器发生了物理故障，那整个域的资源分配就要趋于崩溃，因此我们很有必要居安思危，未雨绸缪。使用用备份工具对 Active Directory 数据库进行备份，然后在域控制器崩溃时利用备份内容还原 Active Directory 是工程师经常使用的灾难恢复手段。这种方案简单易行，很适合小型企业使用，希望大家都能掌握这种基础手段。下次我们将介绍通过部署额外域控制器来解决 Active Directory 的容错和性能问题。

部署额外域控制器

在前面的博文中我们介绍了域控制器在进行网络资源分配时的核心作用，而且我们分析了一下一旦域控制器崩溃会导致的灾难场景，上篇博文中我们提出使用对 AD 数据备份的方法来进行域控制器的灾难重建，今天我们介绍使用额外域控制

器来避免域的崩溃。

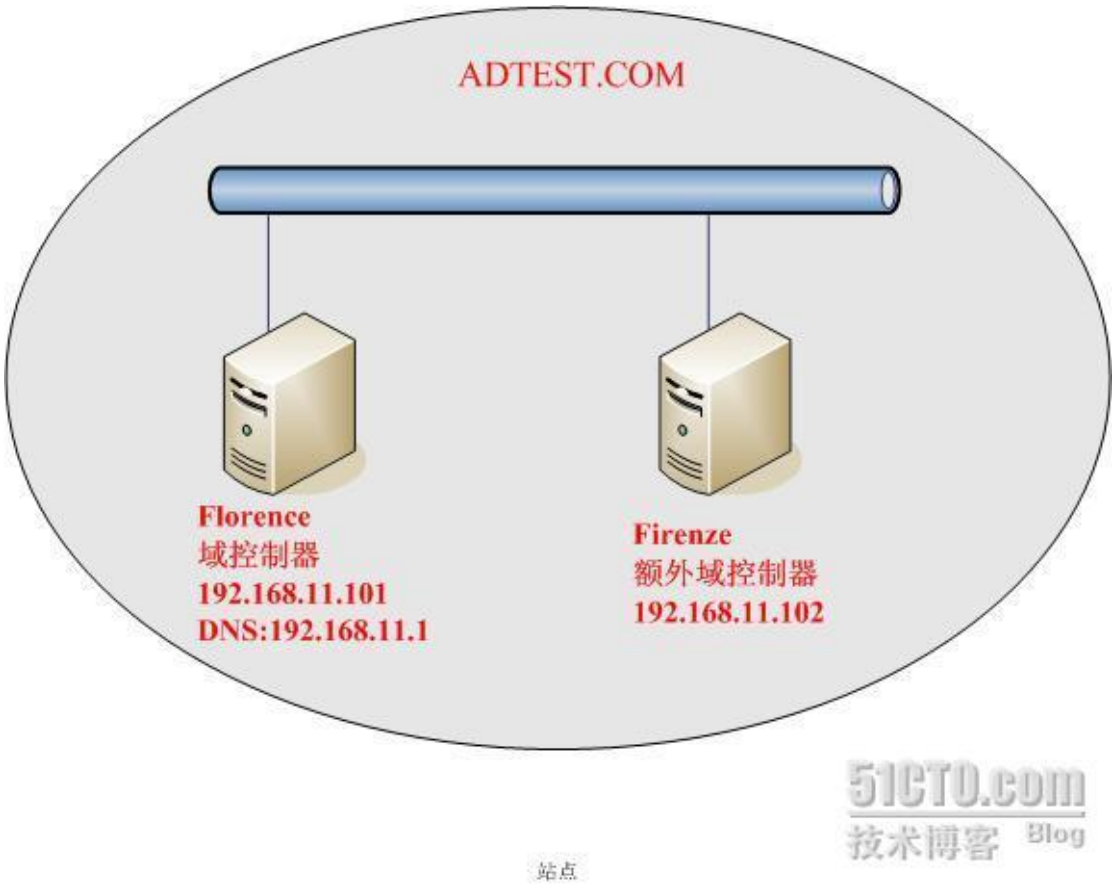
如果域中只有一台域控制器，一旦出现物理故障，我们即使可以从备份还原 AD，也要付出停机等待的代价，这也就意味着公司的业务将出现停滞。部署额外域控制器，指的是在域中部署第二个甚至更多的域控制器，每个域控制器都拥有一个 Active Directory 数据库。使用额外域控制器的好处很多，首先是避免了域控制器损坏所造成的业务停滞，如果一个域控制器损坏了，只要域内其他的域控制器有一个是工作正常的，域用户就可以继续完成用户登录，访问网络资源等一系列工作，基于域的资源分配不会因此停滞。使用域控制器还可以起到负载平衡的作用，如果公司内只有一个域控制器，而公司用户达到上万人，假设域控制器处理一个用户登录的时间是 0.1 秒，那最后一个用户登录进入系统肯定要遭遇一定的延迟。如果有额外域控制器，那么每个额外域控制器都可以处理用户的登录请求，用户就不用等待那么长时间了。尤其是如果域的地理分布跨了广域网，例如域内的计算机有的在北京，有的在上海，有的在广州，那么显然上海用户的登录请求通过低速的广域网提交到北京的域控制器上进行验证不是一个效率高的办法，比较理想的办法是在北京，上海，广州都部署额外域控制器以方便用户就近登录。

域中如果有多个域控制器，那么每个域控制器上都拥有 Active Directory 数据库，而且域控制器上的 Active Directory 内容是动态同步的，也就是说，任何一个域控制器修改了 Active Directory，其他的域控制器都要把这个修改作用到自己的 Active Directory 上，这样才能保证 Active Directory 数据的完整性和唯一性。否则如果每个域控制器的 Active Directory 内容不一致，域控制器的权威性就要受到质疑了。

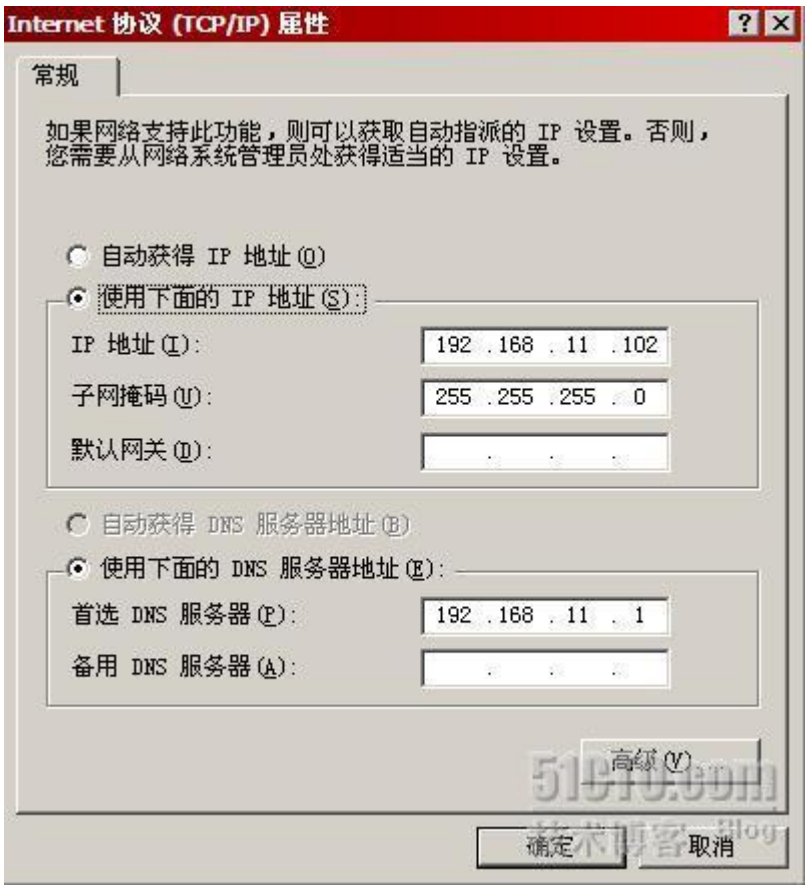
提到这里，顺便说一下主域控制器这个名词，很多朋友喜欢把域内的第一台域控制器称为主域控制器，其他的额外域控制器称为辅域控制器，严格来说这种说法并不严谨。主域控制器这个术语在 NT4 的环境下是成立的，因为 NT4 的域把域控制器分为两类，主域控制器和备份域控制器。两者的区别在于只有主域控制器才能修改域内的数据，而备份域控制器只有读取域内数据的权限，类似于 DNS 的主服务器和辅助服务器的区别。NT4 的这种结构我们称之为单主复制，而自从 Win2000 使用了 Active Directory 之后，所有的域控制器都可以自主地修

改 Active Directory 数据库的内容，现在的域结构我们称之为多主复制。因此，Win2003 域中的第一台域控制器我们称之为主域控制器是不太严谨的，虽然事实上第一台域控制器比其他的域控制器承担了更多的任务。

这次实验我们准备在域中部署一个额外域控制器，额外域控制器的角色由 Firenze 来承担，拓扑如下图所示，DNS 服务器仍然是由一台单独的计算机 192.168.11.1 来承担。



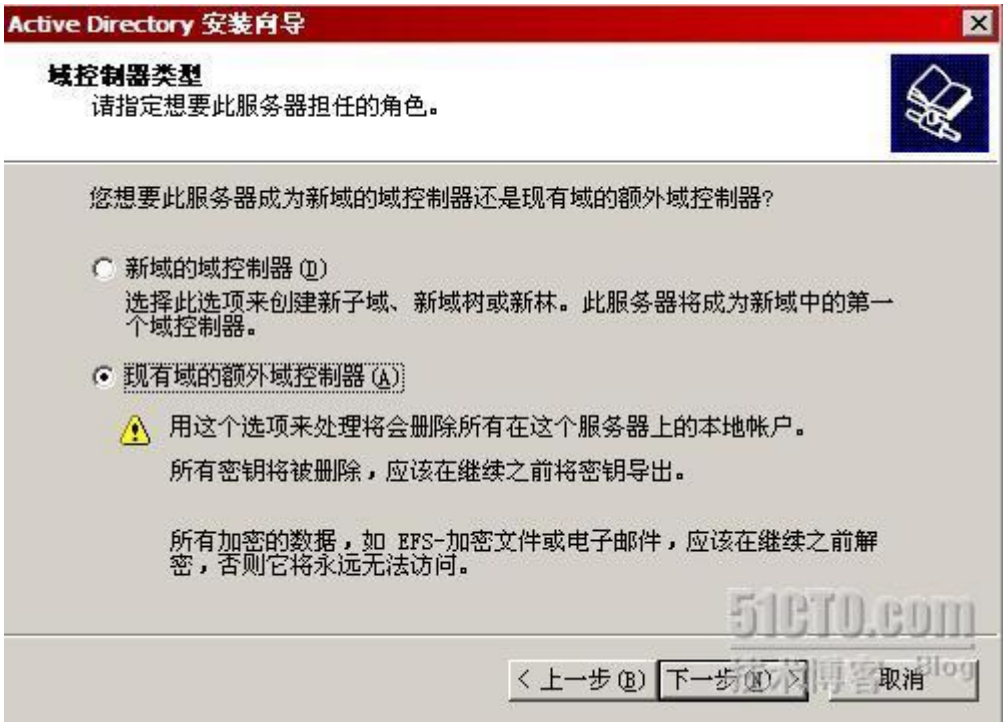
首先我们要在 Firenze 上设置 TCP/IP 的属性，如下图所示，我们要确保 Firenze 使用的 DNS 服务器是正确的，因为 Firenze 要依靠 DNS 服务器来定位域控制器。Firenze 不用先加入域，Firenze 是工作组内的一台独立计算机也是可以的。



在 Firenze 上运行 Dcpromo，如下图所示。

出现 Active Directory 的安装向导，点击下一步继续。

这次我们选择创建现有域的额外域控制器，点击下一步继续。

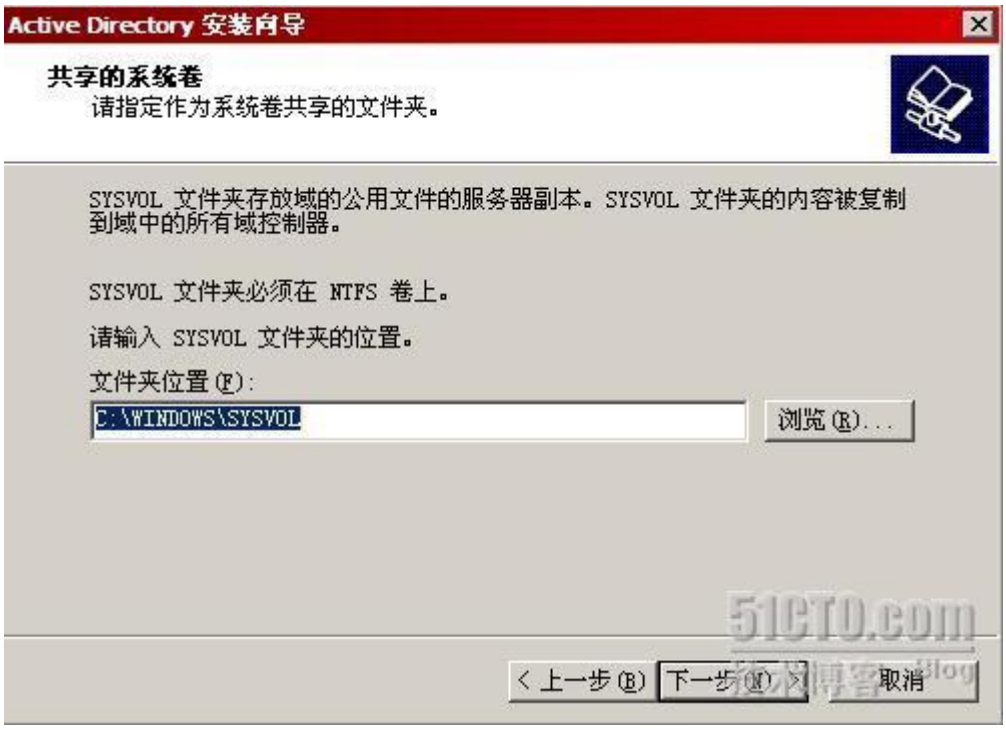


输入域管理员账号，用以证明自己有权限完成额外域控制器的部署。

Firenze 将成为 adtest.com 域的额外域控制器。

Active Directory 数据库的存储路径使用默认值即可。

Sysvol 文件夹的存储路径也可以使用默认值。



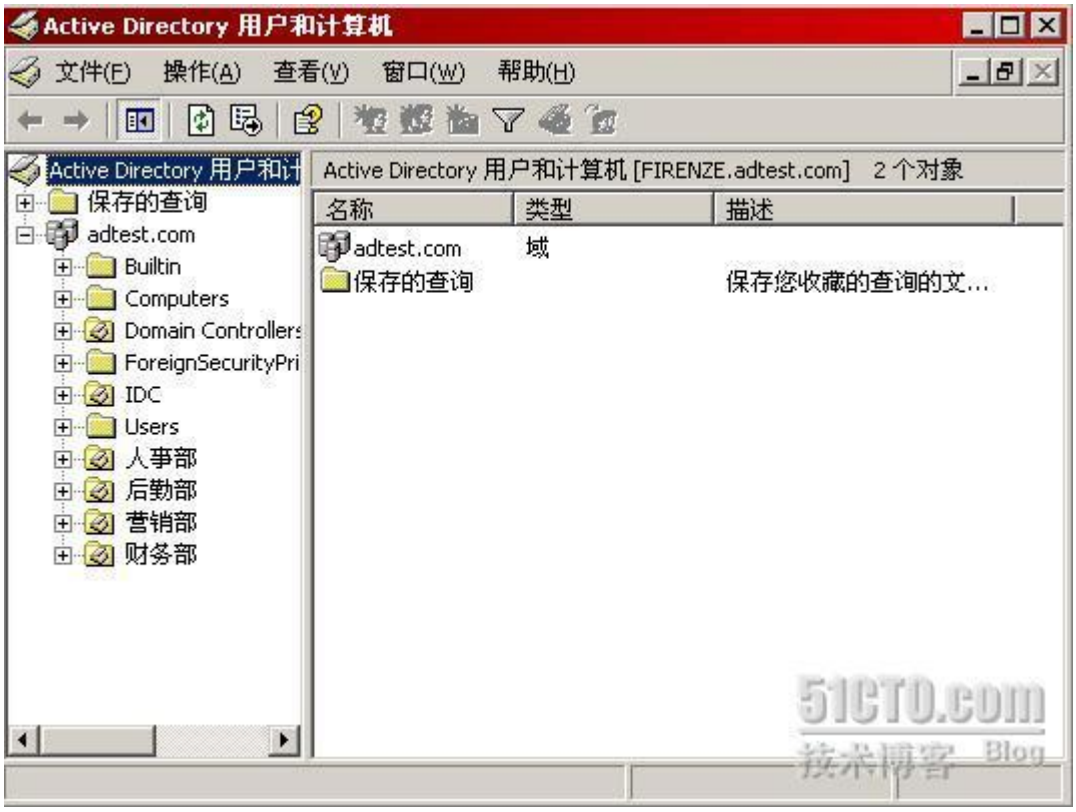
输入目录服务还原模式的管理员密码，以后我们从备份还原 Active Directory 时可以用到。

确认所有的设置无误，点击下一步继续。

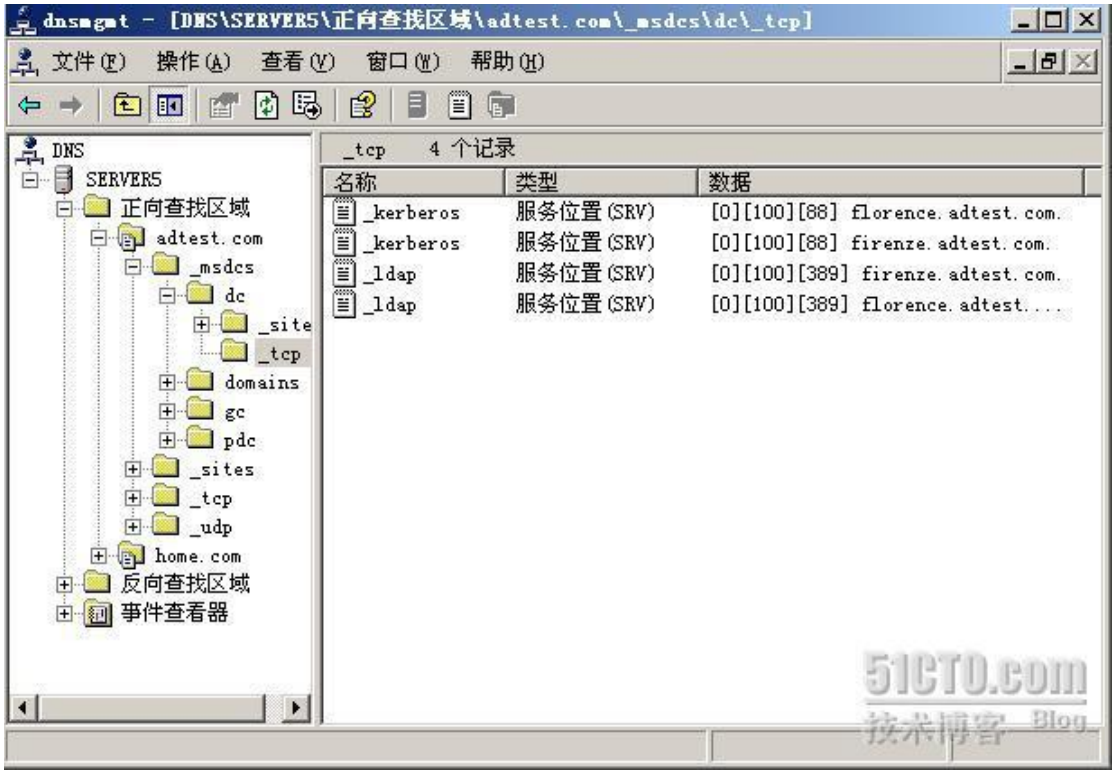
如下图所示，Firenze 通过网络从第一个域控制器 Florence 那里复制 Active Directory 到本机。

Active Directory 安装完毕，点击完成后 Firenze 会重新启动，至此，额外域控制器部署结束。

Firenze 部署完毕后，我们打开 Firenze 上的 Active Directory 用户和计算机，如下图所示，我们可以看到 Firenze 已经把 Florence 的 Active Directory 内容复制了过来。



检查 DNS 服务器，可以看到 DNS 中已经有了 Firneze 的 SRV 记录。



至此，部署 **Firenze** 作为额外域控制器成功完成，从过程来看并不复杂。现在

我们请大家考虑一个问题，**Florence** 和 **Firenze** 是现在域中的两个域控制器，**Florence** 和 **Firenze** 的 **Active Directory** 内容应该完全一致，但如果现在 **Florence** 和 **Firenze** 的 **Active Directory** 内容出现了差异，那应该以哪个域控制器的内容为主呢？问题的答案将在下篇博文中揭晓。

ACTIVE DIRECTORY 的授权还原

在上篇博文中我们介绍了如何在域中部署额外域控制器，额外域控制器有很多好处，例如可以平衡用户对 AD 的访问压力，有利于避免唯一的域控制器损坏所导致域的崩溃。从上篇博文中我们得知，域内所有的域控制器都有一个内容相同的 Active Directory，而且 Active Directory 的内容是动态平衡的，也就是说任何一个域控制器修改了 Active Directory，其他的域控制器都会把这个 Active Directory 的变化复制过去。

今天我们要考虑这么一个问题，如果域中有多个域控制器，但他们所拥有的 Active Directory 内容不一致，那么应该以哪个域控制器的 Active Directory 内容为准？有的朋友可能会疑惑，怎么会出现这种情况呢？其实假如有个域控制器由于更换硬件导致有几天时间没有在线，而其他的域控制器在这段时间对 Active Directory 进行了修改，那么当这个域控制器重新上线时就会出现我们所提到的这种情形。

当域控制器们发现彼此的 Active Directory 的内容不一致，他们就需要分析一下 Active Directory 的优先级，从而决定以哪个域控制器的 Active Directory 内容为准。Active Directory 的优先级比较主要考虑三方面因素，分别是：

1 版本号

2 时间

3 **GUID**

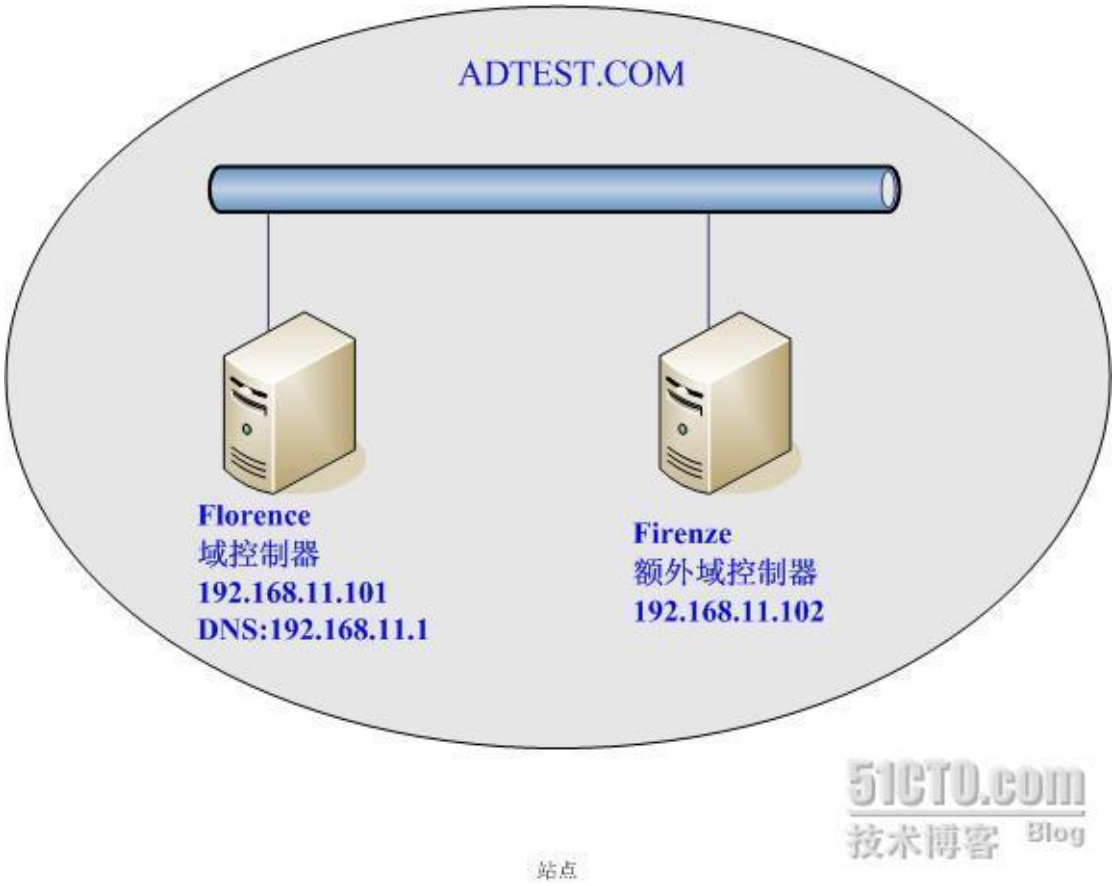
版本号指的是 Active Directory 对象的修改次数，版本号高者优先。例如域中

有两个域控制器 A 和 B，A 域控制器上的用户 administrator 口令被修改了 4 次，最后被改为 12345；B 域控制器上的用户 administrator 口令被修改了 5 次，最后被改为 123456。那么 A 和 B 发现他们的 Active Directory 中 administrator 口令不一致，这时 A 和 B 会分析版本号，发现版本号分别是 4 和 5，这时 A 就会把 B 的 Active Directory 内容复制到本机的 Active Direcotry 中。经过这么一轮复制后，A 和 B 的 Active Directory 内容就达到了新的平衡，他们 Active Directory 中所有对象的版本号也都完全一致了。

如果 A 和 B 两个域控制器都是对 administrator 口令修改了 4 次，那么版本号就是相同的。这种情况下两个域控制器就要比较时间因素，看哪个域控制器完成修改的时间靠后，时间靠后者优先。这里我们顺便提及一下，Active Directory 中时间是个非常重要的因素，域内计算机的时间误差不能超过 5 分钟，而且 Active Directory 还有一个墓碑时间的限制，这些我们以后再详细加以说明。

如果 A 和 B 两个域控制器的版本号和时间都完全一致，这时就要比较两个域控制器的 GUID 了，显然这完全是个随机的结果。一般情况下时间完全相同的非常罕见，因此 GUID 这个因素只是一个备选方案。

说了这么多的 Active Directory 优先级原理，我们引入一个具体的例子让大家加深理解。如下图所示，域中有两个域控制器 Florence 和 Firenze。现在域中有一个用户张建国，我们在 Firenze 上对 Active Directory 已经进行了备份。现在我们在 Florence 上不小心把张建国误删除了，显然 Firenze 会很快把 Active Directory 中的张建国也删除，以便和 Florence 的 Active Directory 保持一致。那么我们应该怎么做才能把张建国给恢复回来呢？

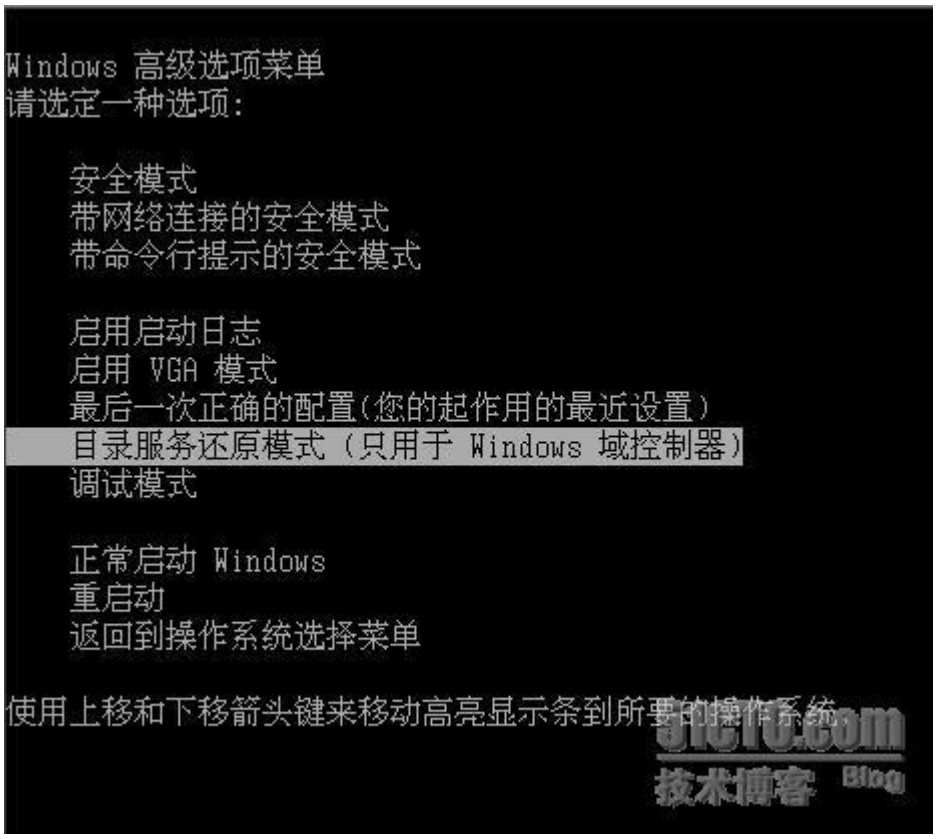


很多朋友会很自然地想到利用 Firenze 上的 Active Directory 备份来解决这个问题，既然备份中有张建国，那么把备份还原回来不就 OK 了吗？这个问题没这么简单，如果域中只有一个域控制器，那么用备份还原是成立的。但现在域中有两个域控制器，我们就要好好考虑一下了。Firenze 从备份还原后，Florence 和 Firenze 的 Active Directory 内容就不一样了，那么 Florence 和 Firenze 的 Active Directory 哪个优先级更高呢？哦，不对，似乎是 Florence 的版本号更高一些！那我们就可以从理论上得出结论，Firenze 从备份还原之后，Active Directory 中已经拥有了张建国的用户账号，但 Firenze 和 Florence 比较了 Active Directory 之后，Firenze 认为 Florence 的 Active Directory 比自己的优先级高，因此 Firenze 会把 Florence 的 Active Directory 复制过来，这样一来，刚被还原的张建国肯定会被重新删除掉！

难道我们对此就无能为力了吗？不是的，在 Firenze 从备份还原 Active Directory 之后，我们可以利用一个工具 NTDSUTIL.EXE 来修改 Active Directory

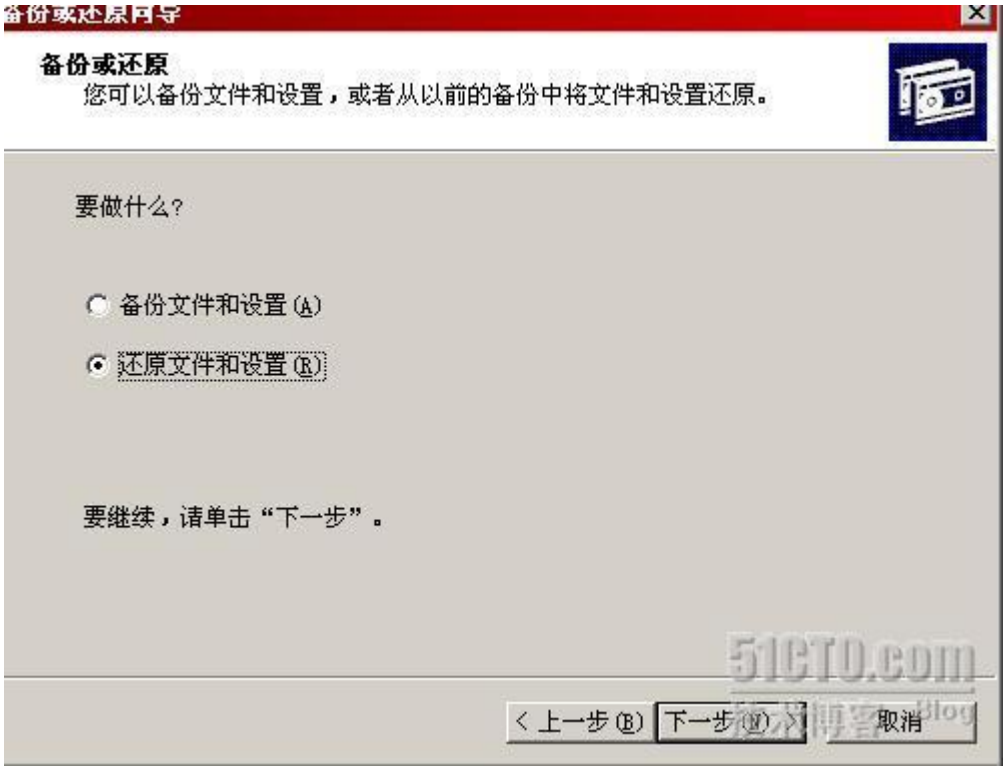
对象的版本号，让 Firenze 的版本号大于 Florence 的版本号，这样我们就可以利用游戏规则顺利地达到目的了。这种还原方式我们称为授权还原，下面我们通过一个实例为大家演示一下具体过程。

现在的场景是 Firenze 已经对 Active Directory 进行了备份，备份中包含了域用户张建国。在备份之后我们误删除了张建国，现在我们在 Firenze 上开始利用备份进行主要还原。首先在 Firenze 上重启计算机，BIOS 自检后按下 F8，如下图所示，选择进入目录服务还原模式。目录服务还原模式可以把 Active Directory 挂起，适合我们从备份还原 Active Directory。



进入目录服务还原模式后从附件中启动备份工具，如下图所示，选择下一步继续。

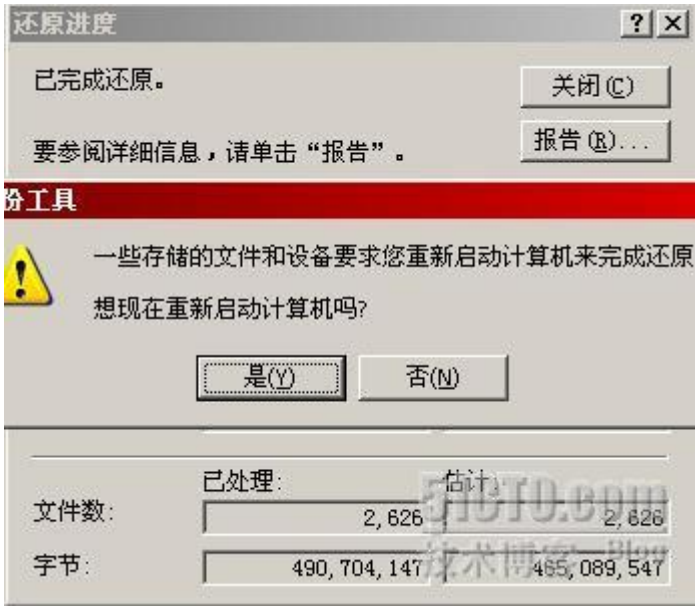
选择还原文件和设置。



选择从备份还原 Active Directory。

点击确定开始 Active Directory 的还原。

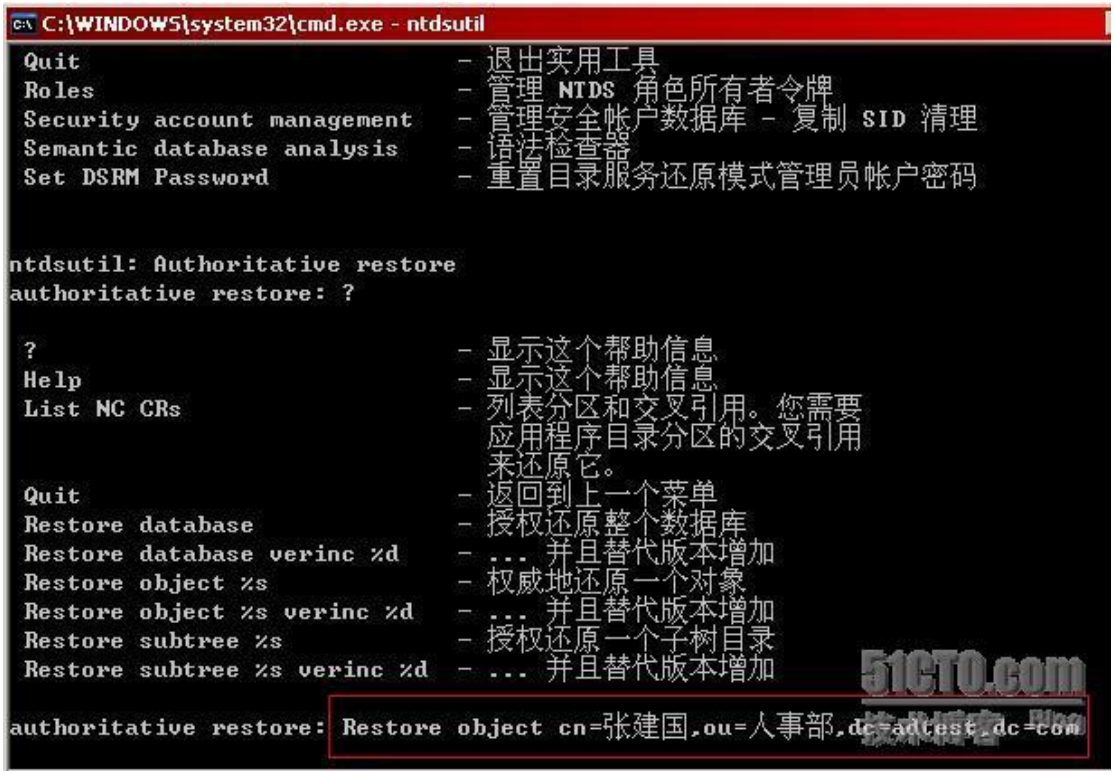
如下图所示，还原结束后，千万别选择重启计算机，我们还没有修改 Active Directory 的版本号呢，确保选择“否”。



还原结束后在 Firenze 的命令提示符下运行 NTDSUTIL，如下图所示。

运行了 NTDSUTIL 后，我们可以输入？来获取当前环境下的可执行命令帮助，如下图所示，我们运行 Authoritative restore 来修改 AD 对象的版本号。

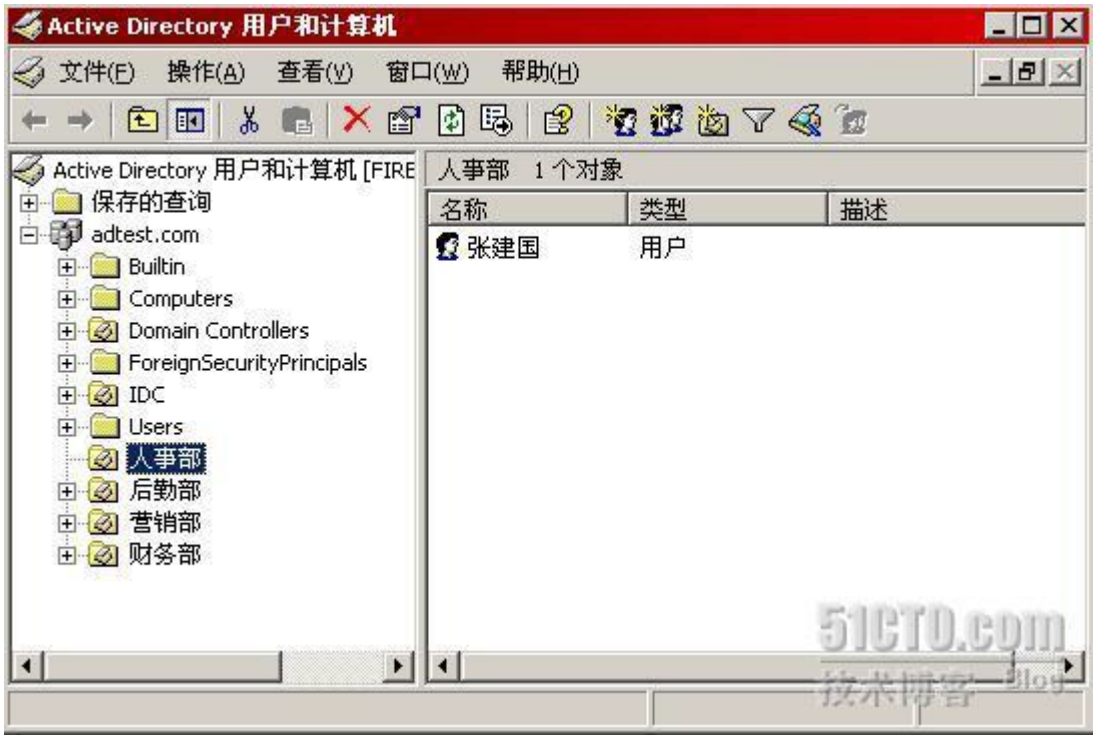
如下图所示，我们可以简单地运行 restore database，这样整个 AD 内所有对象的版本号都将加到最大，版本号加到最大是什么含义呢？微软规定，AD 对象的版本号每天最多可以增加 10 万。在本例中我们不需要把 AD 中所有对象的版本号都增加到最大，只要修改张建国的版本号就可以了。因此我们可以使用 Restore Object 命令只针对张建国的版本号进行修改，那如何在 AD 中表示张建国呢？按照目录对象的命名规范，张建国隶属于 ADTEST.COM 域中的人事部组织单位，那我们描述张建国就应该使用 cn＝张建国，ou＝人事部，dc＝adtest，dc＝com。如下图所示，我们输入修改指令后观察一下运行的效果。



系统询问是否执行授权还原，我们选择“是”。

如下图所示，授权还原成功完成，用 quit 命令退出 NTDSUTIL。

授权还原结束后我们重启 Firenze，如下图所示，Firenze 的 AD 中已经重新拥有了用户张建国，修改版本号成功了。

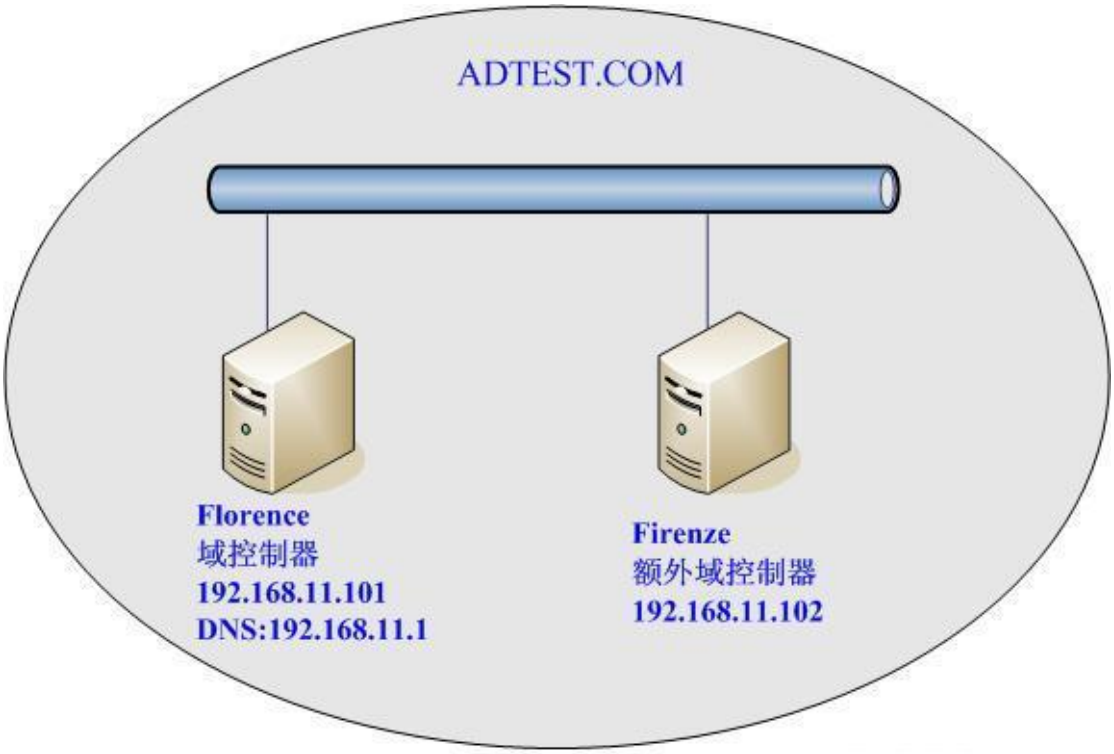


离线部署额外域控制器

在上篇博文中我们介绍了部署额外域控制器的意义，同时介绍了如何在线部署额外域控制器，也就是额外域控制器通过网络以在线方式从复制伙伴那里获取 Active Directory 数据。在线部署额外域控制器是我们部署额外域控制器时的首选，它方便易行，在拥有快速网络连接的环境下使用非常合适。但我们也要考虑另外一种场景，域控制器之间是通过低速网络连接的！如果域控制器之间的网络质量不理想，例如有的域控制器需要部署到非洲，那我们就不能希望获得一个高速，稳定，可靠的通讯网络。在这种情况下，如果我们还使用在线方式部署额外域控制器，就有可能事倍功半！那我们遇到这种情况应该如何解决呢？我们可以考虑使用离线方式来部署额外域控制器，也就是说额外域控制器在复制 Active Directory 时不通过网络从其他的域控制器复制，而是从 Active Directory 的离线文件复制，这样就可有效避免对网络环境的依赖。

那我们如何获得 Active Directory 的离线文件呢？我们可以从 Active Directory 的备份中得到。具体是这样的，我们对 Active Directory 备份之后，把离线部署额外域控制器所需要的文件从备份中提取出来，然后通过各种手段传送到需要部署额外域控制器的计算机上。例如我们可以把离线文件刻录到光盘上，然后在出差时带过去；或者可以放在一个支持断线续传下载的服务器上，让对方通过网络慢慢下载。对方得到了 Active Directory 的离线文件后，就可以通过 Dcpromo 来调用离线文件从而完成额外域控制器的部署。

我们通过一个具体实例加以说明，实验拓扑如下图所示，Florence 是域控制器，Firenze 是准备用离线方式部署的额外域控制器。



具体的部署过程分为下列两个阶段：

1、 获得 Active Directory 的离线文件

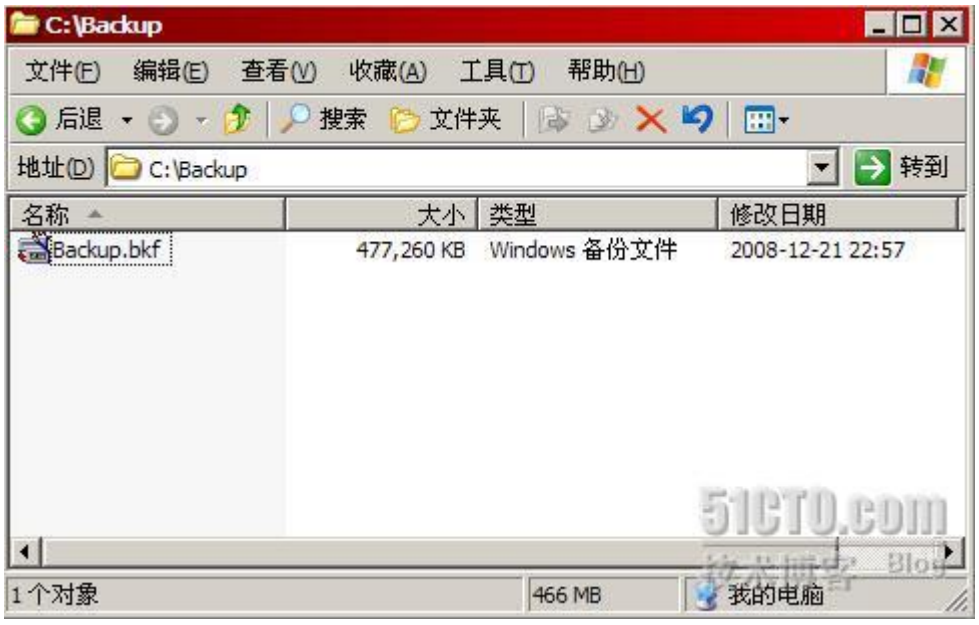
2、 离线部署额外域控制器

一 获得 Active Directory 的离线文件

首先我们在域控制器 Florence 上对 Active Directory 进行备份，备份工具使用系统自带的 NTBACKUP，具体的备份过程参见前期博文，在此不在赘述。Active Directory 的离线数据来源于对 Active Directory 的备份，但大家要注意的是，由于 NTBACKUP 备份的粒度并不太细致，因此我们对 System State 进行备份时，还备份了除 Active Directory 之外的其他内容。如下图所示，我们发现备份的 System State 的内容分为五部分，分别是 Active Directory，Boot Files，COM＋ Class Registration Database，Registry 和 SYSVOL。**其实我们用离线方式部署额外域控制器，只需要 Active Directory，Regis**

try 和 SYSVOL 三部分即可。

下图是备份 System State 后生成的备份文件，我们可以看到备份文件的大小是 480M 左右，其实其中只有少部分数据是我们需要的。



我们准备从备份中提取 Active Directory 的离线数据，我们使用的工具还是 NTBACKUP－系统自带的备份工具，如下图所示，我们在 Florence 上启动 NTBACKUP 后，选择“还原文件和设置”。

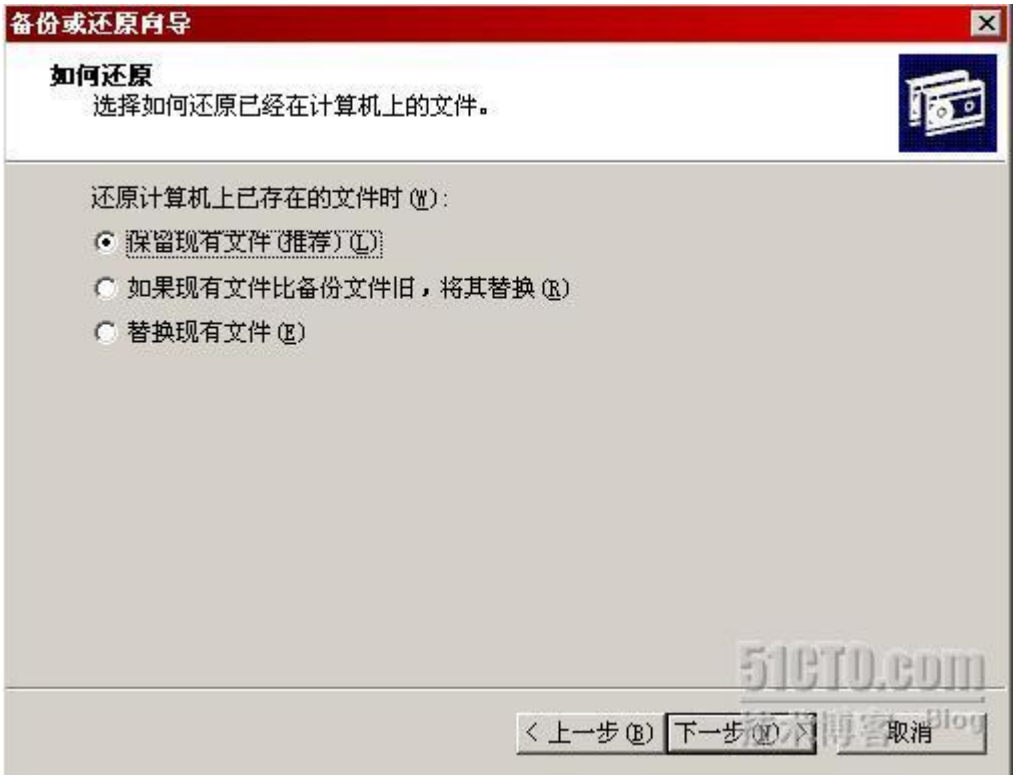
选择对 System State 的备份文件进行还原，从编录结果中我们可以看到 System State 的备份中包含了五部分内容。

如下图所示，千万不要选择完成，一定要点击“高级”按钮进行设置，否则系

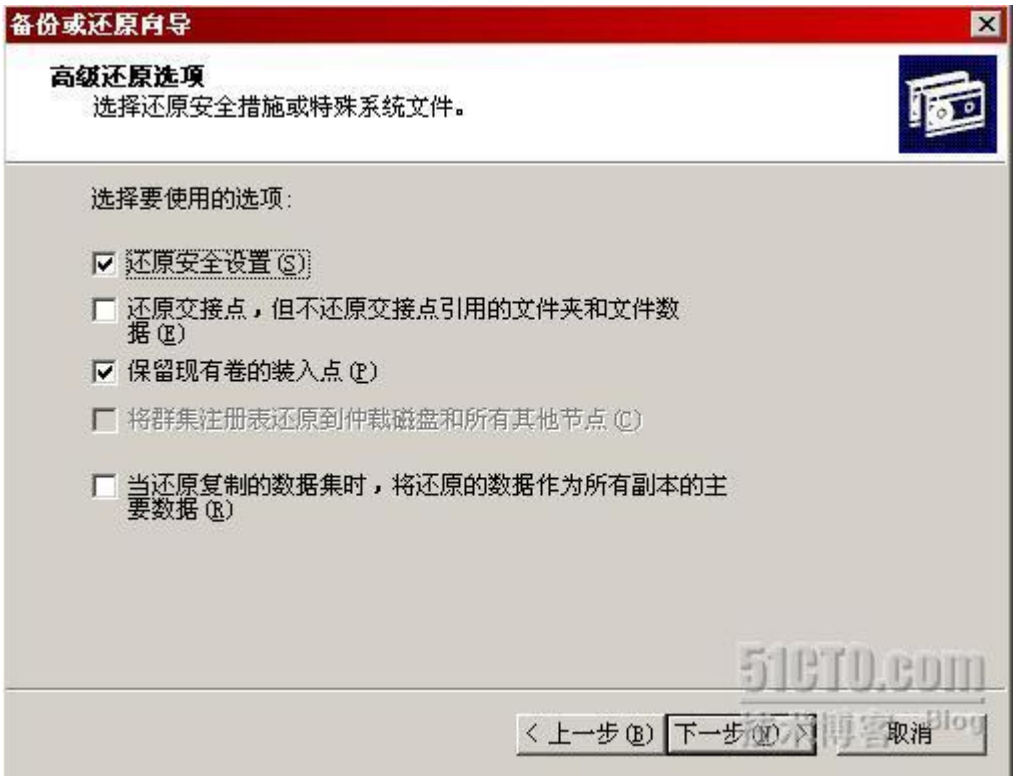
统会把备份文件还原到原位置。

我们不能把备份还原到原位置，而是应如下图所示还原到备用位置，我们选择的备用位置是 C:\ADBAK，这其实就是把备份文件中的内容展开到 C:\ADBAK 中。

还原选项使用默认值即可。



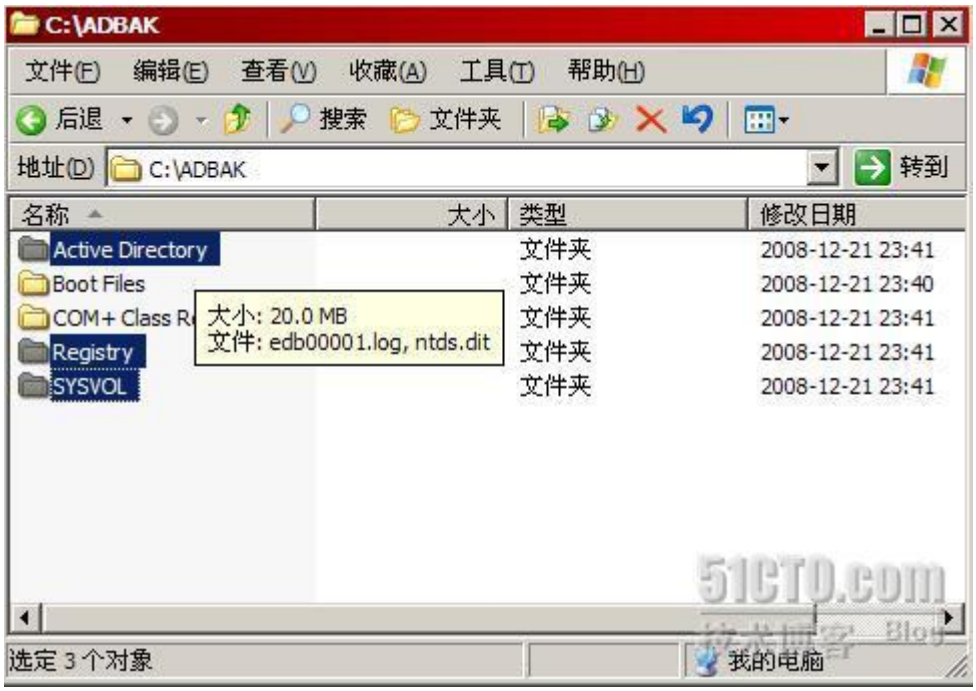
仍然保留默认设置。



如下图所示，还原顺利完成。

看看展开后的备份文件是什么内容，如下图所示，我们可以看到备份文件被展开成了五个目录，每个目录存储备份中的一部分内容。离线部署其实只需要 Active Directory，Registry 和 SYSVOL 三个文件夹的内容，这三个文件夹的数据大概是 40M 左右，相比较备份文件的 480M 体积确实缩水了不少。我们把这三个文件夹的内容传送到要部署成额外域控制器的计算机上，至此结束了 Active

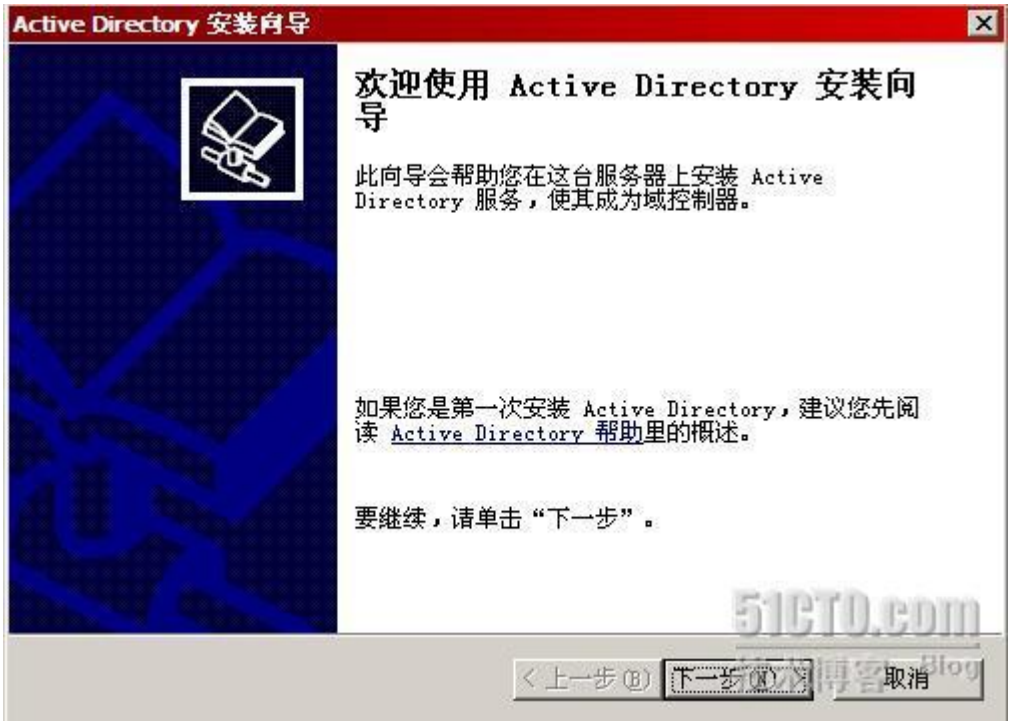
Directory 离线文件的准备。



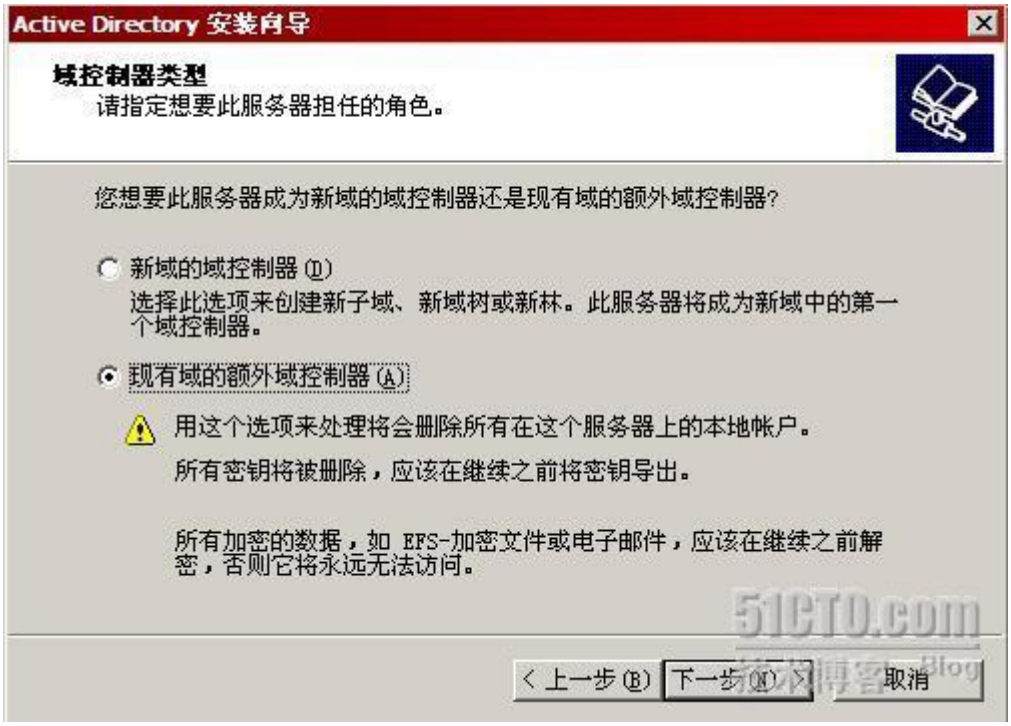
二 离线部署额外域控制器

拿到了 Active Directory 的离线文件后，我们就可以在 Firenze 上部署额外域控制器了，如下图所示，我们在 Firenze 上运行 Dcpromo /adv。

出现 Active Directory 安装向导，点击下一步继续。

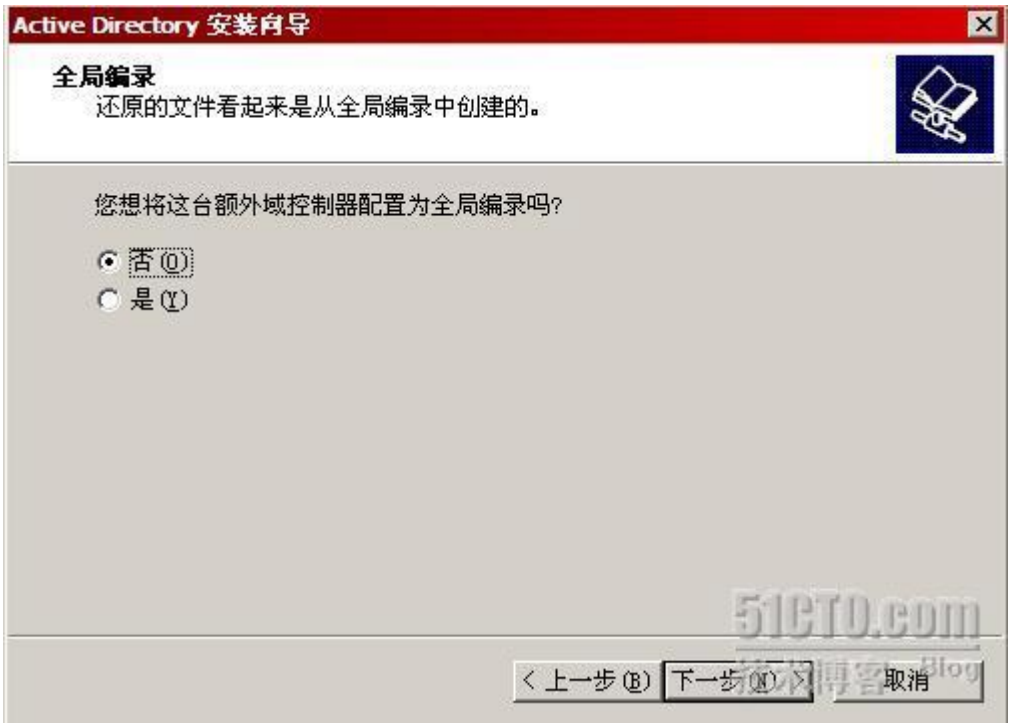


选择成为额外域控制器。



选择从备份文件复制 Active Directory，备份文件的路径是 C:\ADBAK，里面包括了从 Florence 复制来的三个文件夹，Active Directory，Registry 和 SYSVOL。

是否将 Firenze 设置成全局编录取决于实际需求，在此实验中我们不需要把 Firenze 配置成全局编录服务器。

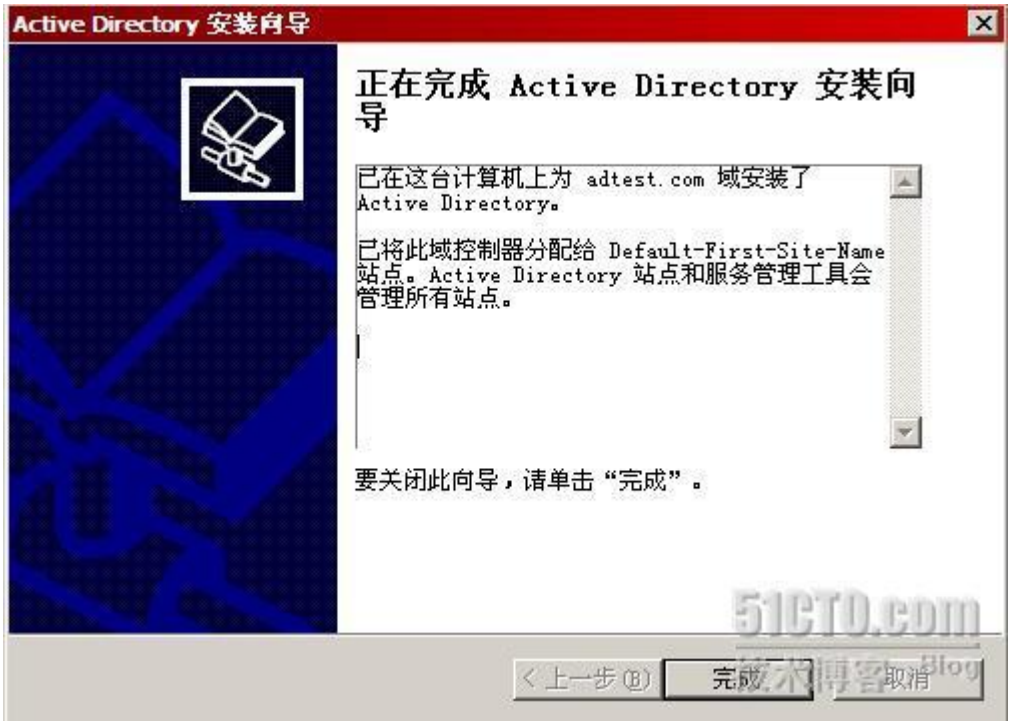


输入域管理员的口令用以在 Firenze 上创建 Active Directory。

输入还原模式口令，下一步继续。

如下图所示，Firenze 上开始离线部署额外域控制器。

Active Directory 创建完成，重启后就可以发现 Firenze 已经成为了域控制器，至此，利用备份离线部署额外域控制器顺利完成！

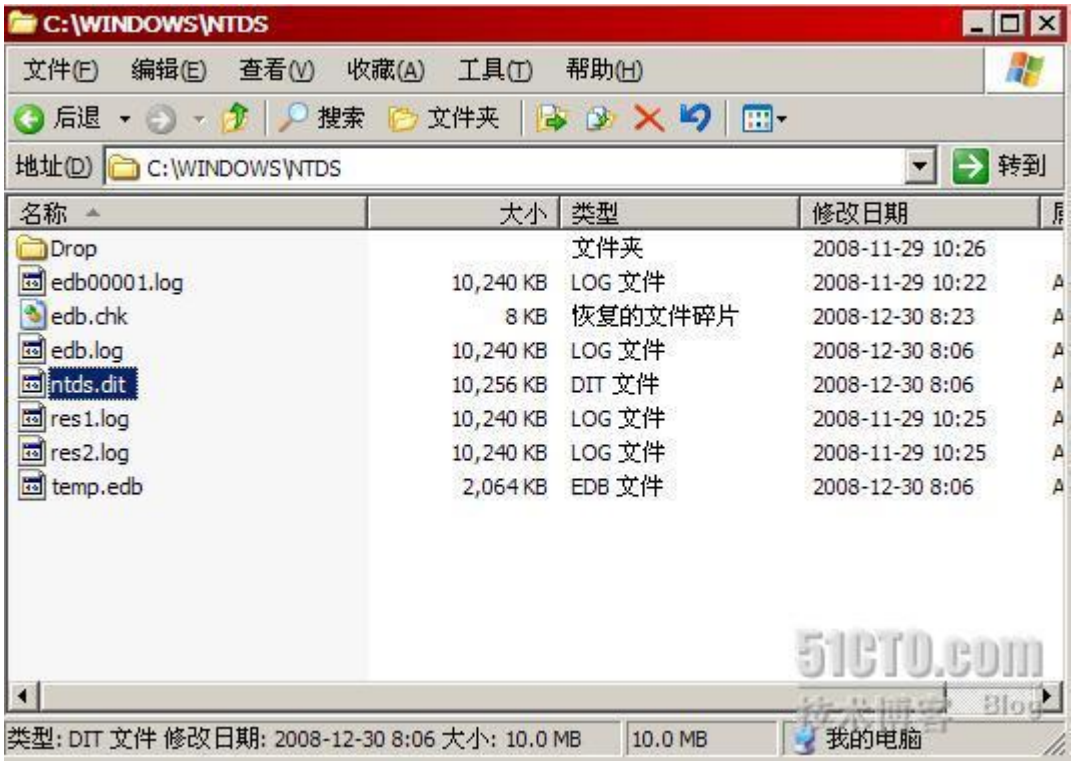


ACTIVE DIRECTORY 的脱机碎片整理

Active Directory 是一个被设计用于查询的非关系型数据库，Active Directory 使用一段时间后，需要对数据库内容进行维护，以减少数据碎片及提高查询效率，今天我们就为大家介绍一下如何对 Active Directory 的数据库进行离线维护。

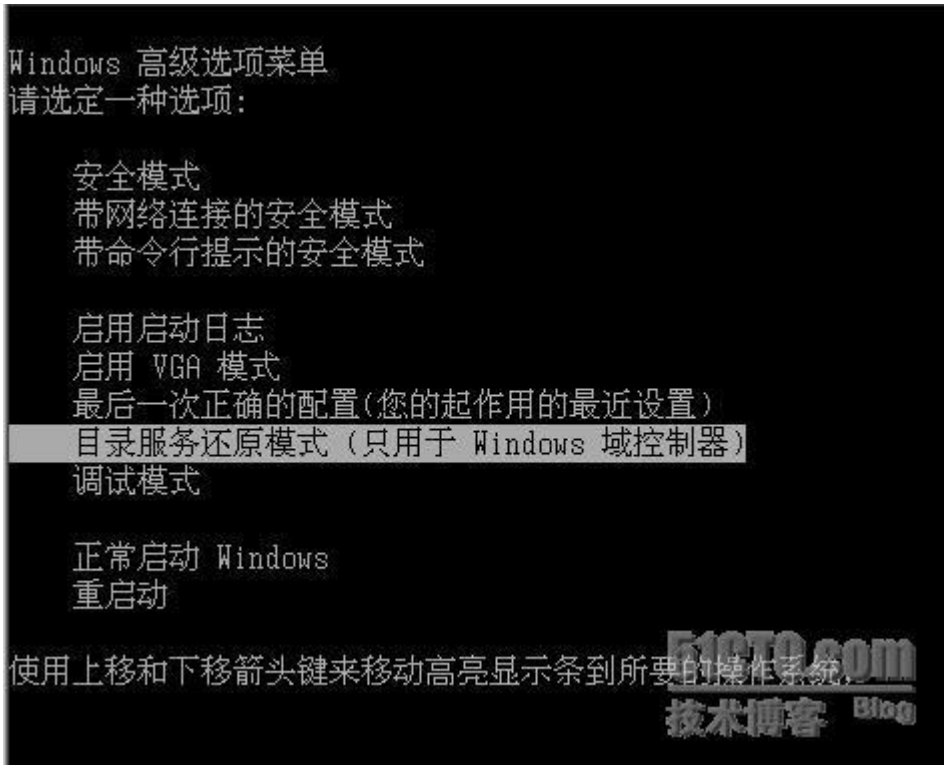
Active Directory 创建时默认的数据库及事务日志的存放路径是 C:\Windows\NTDS，我们打开前文中创建的域控制器 Florence，定位到 C:\Windows\NTDS 目录下，先来了解一下下图中各文件的作用。其中的 NTDS.DIT 是 Active Directory 的数据库文件，EDB.LOG 是事务日志文件，事务日志文件记录了数据库内容的变更，非常重要。默认的事务日志文件大小只有 10M，如果事务日志文件已经记录满了，系统就会自动地生成 edb00001.log 用以继续存储事务日志，如果 edb00001.log 也存满了，就会接下来生成 edb00002.log，以此类推。顺便提一下，在生产环境下，我们应该把数据库文件和事务文件分开存储，这样既可以提高性能，也可以增加数据安全性，但 Win2003 要求 Active Directory 的数据库和事务日志都存储在同一个硬盘上，不像 Win2000 中 Active Directory 的数据库和事务日志可以存储在不同的硬盘上。

EDB.CHK 是事务日志的检查点文件，记录了硬盘上的 Active Directory 和内存中 Active Directory 在内容上的差异，一般此文件用于 Active Directory 的初始化或还原。RES1.LOG 和 RES2.LOG 是系统保留的事务日志文件，这两个文件一共占用了 20M 空间，主要目的就是为了给 Active Directory 的事务日志预留 20M 空间，避免当硬盘空间用光后无法正常关机。

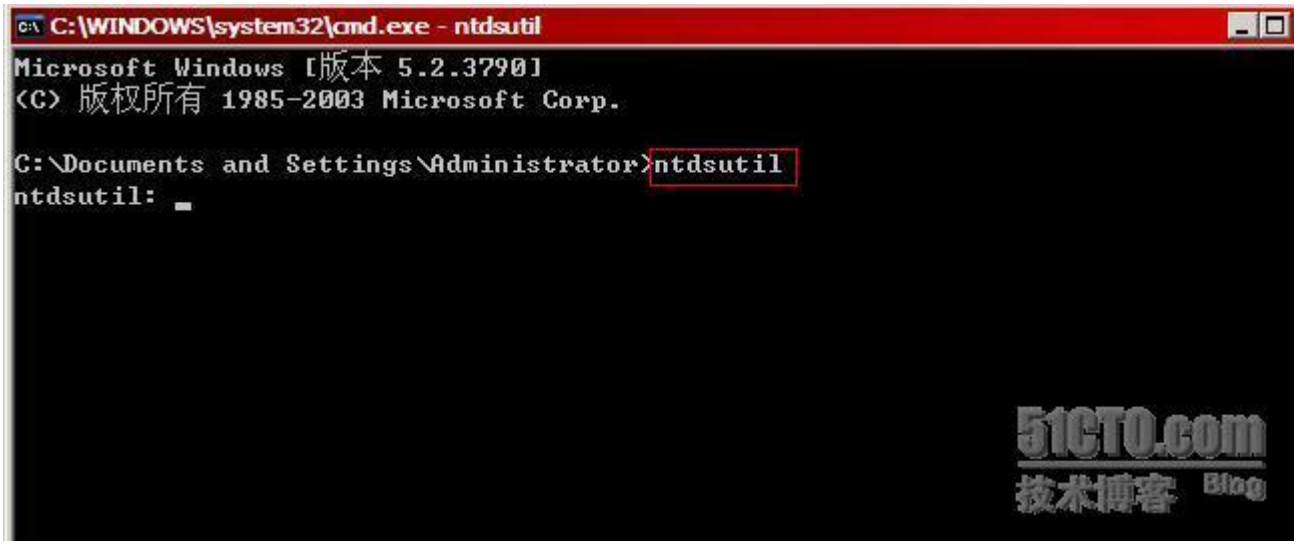


Active Directory 使用一段时间后，会产生数据碎片，表现为 Active Directory 占用的空间增大，响应速度降低，这时就需要对 Active Directory 做一些碎片整理了。Active Directory 的碎片整理分为在线和离线两部分，默认情况下在线整理会 12 小时进行一次。在线整理的好处是在数据库维护的过程中不需要关闭 Active Directory，用户不会受到影响；缺点是在线整理只能在已分配的数据库空间内进行碎片整理，无法减少数据库占用的空间。如果 Active Directory 的规模不大，数据变更不频繁，我们使用默认的在线整理也就可以了。如果 Active Directory 的数据库很大，达到上 G 的规模，而且数据频繁更改，这时我们就要使用今天提到的离线维护了。离线维护需要对 Active Directory 进行脱机处理，然后再进行 Active Directory 的碎片整理，这个过程中 Active Directory 无法使用，基于 AD 的业务系统会受到影响，因此建议在工作空闲时间例如晚上进行。Active Directory 进行脱机碎片处理后，可以有效地减少 Active Directory 数据库的大小，提高查询速度，有的单位经过第 Active Directory 进行脱机碎片处理后，可以把 Active Directory 的大小从 11G 降为 6 G！因此对 Active Directory 更新频繁，而且 Active Directory 内包含海量数据的单位来说，离线维护还是很有必要做的。

如何才能对 Active Directory 进行离线的脱机碎片整理呢？我们以域控制器 Florence 举例为大家演示应该如何操作，首先我们在 Florence 上要进入目录服务还原模式，在这个模式下，Active Directory 将被脱机挂起，然后我们就可以对离线的 Active Directory 数据库进行处理了。如下图所示，我们重启 Florence，然后在自检结束后按 F8 键选择进入“目录服务还原模式”。



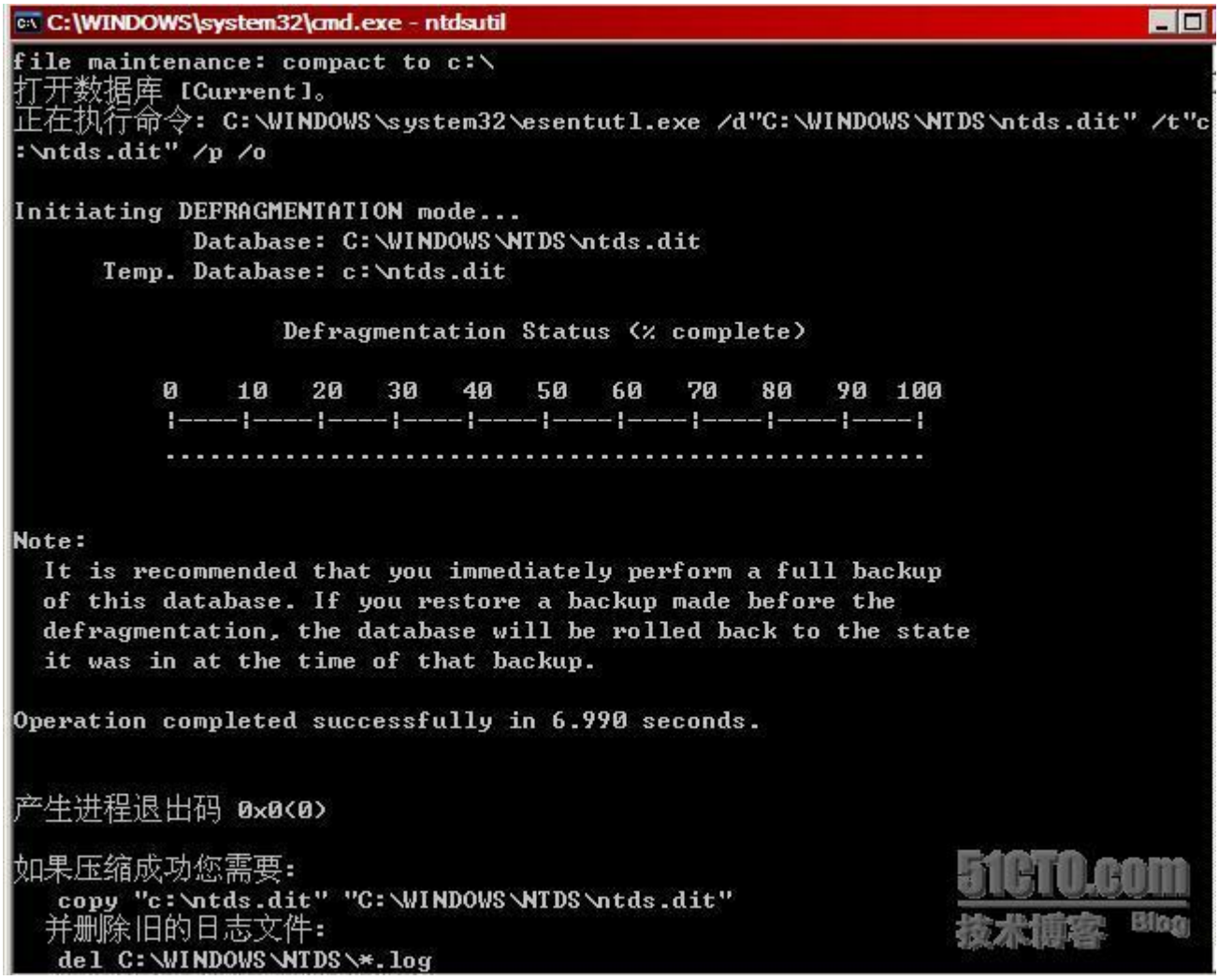
进入目录服务恢复模式后，我们输入命令 NTDSUTIL，如下图所示，我们将使用 NTDSUTIL 对 Active Directory 进行碎片整理。



如下图所示，我们在 NTDSUTIL 中输入 Files。

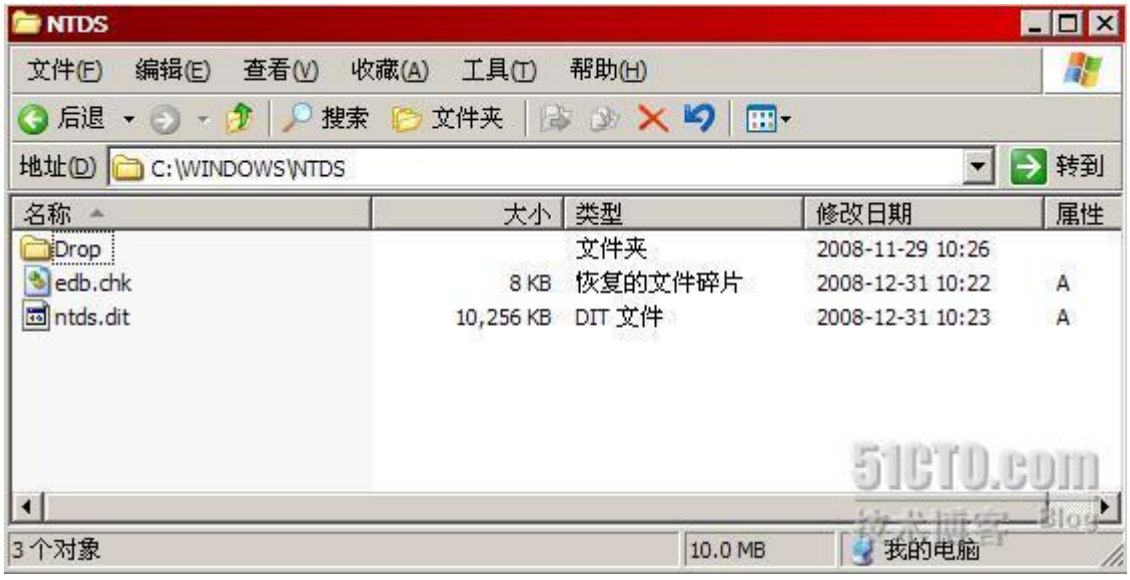
如下所示，我们输入 Compact To C:\，意思是对 Active Directory 数据库清理碎片后压缩到 C 盘的根目录下，这样我们将在 C 盘的根目录下得到一个消除了 Active Directory 碎片的 Ntds.dit。

如下图所示，大家可以发现真正压缩 Active Directory 的是 esentutl.exe，这个工具大家以后也会经常使用，而且大家会在 Exchange 中发现有类似的工具，这主要是因为 Active Directory，Exchange，WINS 等服务器都使用了类似的非关系型数据库引擎。



如下图所示，压缩成功后我们用新的 ntds.dit 覆盖了原来的 Active Directory 数据库文件，同时删除了原有的日志文件，但仍然保留 edb.chk 文件。

如下图所示，这就是我们进行碎片整理后的 Active Directory 文件，如果在一个大型网络中，经过这种离线整理后可以很明显地看出对磁盘空间的释放。



对 Active Directory 进行脱机碎片处理只能在单台域控制器上分别进行，对 Active Directory 压缩不会影响 Active Directory 现有数据，也不会影响 Acti

ve Directory 的复制。

ACTIVE DIRECTORY 的复制拓扑

在前面的博文中我们在域中部署了额外域控制器，而且我们已经知道每个域控制器都有一个内容相同的 Active Directory 数据库，今天我们要讨论一下额外域控制器在进行 Active Directory 复制时所使用复制拓扑。

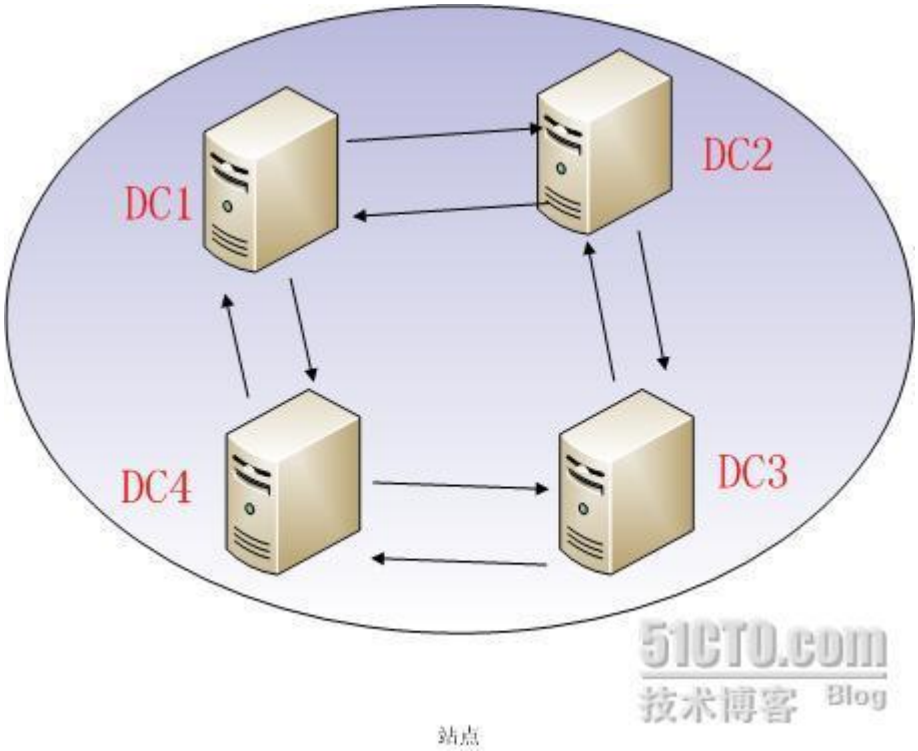
在 NT4 的时代，域控制器被分为两类，PDC 和 BDC。PDC 是主域控制器的缩写，BDC 是备份域控制器的缩写。每个域中只能有一个 PDC，BDC 可以有多个，BDC 的目录数据是从 PDC 复制而来。只有 PDC 才可以更改域中的用户账号，计算机账号等目录数据，BDC 的内容是只读的！这种复制模型我们称为单主复制，这种模型我们并不陌生，类似于 DNS 服务器的辅助服务器和主服务器的关系。单主复制模型比较简单，管理难度不大，但较容易构成单点故障。

从 Win2000 开始，Active Directory 开始使用多主复制的模型，也就是说每个域控制器都可以自主地修改 Active Directory 的内容，域中不再有 PDC 和 BDC 的区别了。Win2003 使用了和 Win2000 同样的多主复制模型，而 Win2008 则在多主复制的基础上又增加了一个 RODC，也就是只读域控制器，可以看出 Win2008 试图在多主复制模型中增加一些单主复制的元素，因为 RODC 的设计理念显然和 BDC 是有些关联的。

现在我们知道了 Win2003 的 Active Directory 中使用了多主复制的模型，也就是任何一个域控制器都可以修改 Active Directory。为了维护 Active Directory 的权威性，显然所有域控制器上的 Active Directory 内容应该都相同。那么，如果一个域控制器修改了自己的 Active Directory，修改的的内容是如何复制到其他域控制器上的呢？这就是我们今天要讨论的内容，Active Directory 的复制拓扑！

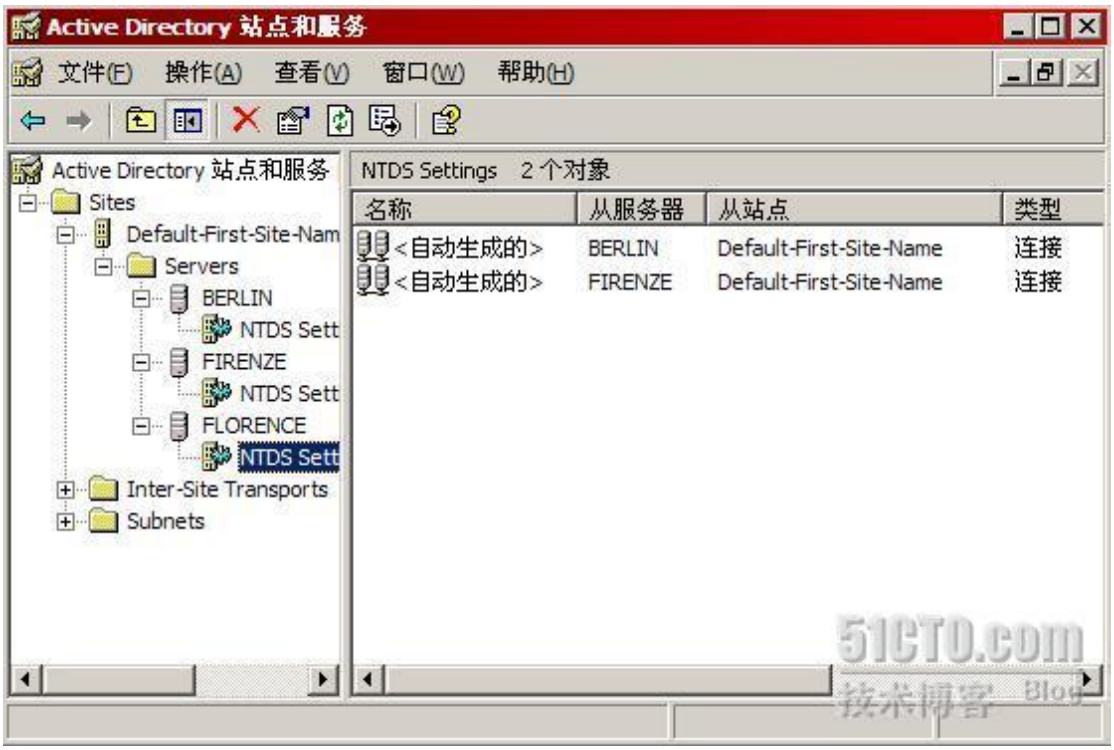
Active Directory 的复制拓扑是一个比较复杂的问题，今天我们只讨论在同一域中域控制器之间的复制拓扑。当域中的域控制器数量发生变化，例如增加或减少了域控制器，域控制器上的进程 KCC 就会进行 Active Directory 复制拓扑的计

算。KCC 被翻译为知识一致性验证器，我们在任务管理器的进程列表中看不到 KCC，因为它属于 LSACC 进程的一部分。KCC 可以自动计算出域控制器进行复制时所使用的拓扑，当域控制器数量较少时，KCC 倾向于在域中使用环形拓扑进行 Active Directory 复制，也就是说当一个域控制器的 Active Directory 内容发生变化时，这个更改不会同时传递给其他所有的域控制器，而是要沿着 KCC 设计的环形拓扑一一传递下去。而且为了实现冗余以及提高效率，KCC 设计的拓扑还是双环拓扑，下图就是一个域控制器的复制拓扑示意图，从图中可以看到，每个域控制器都有两个复制伙伴，Active Directory 的复制沿着顺时针和逆时针两个方向进行。

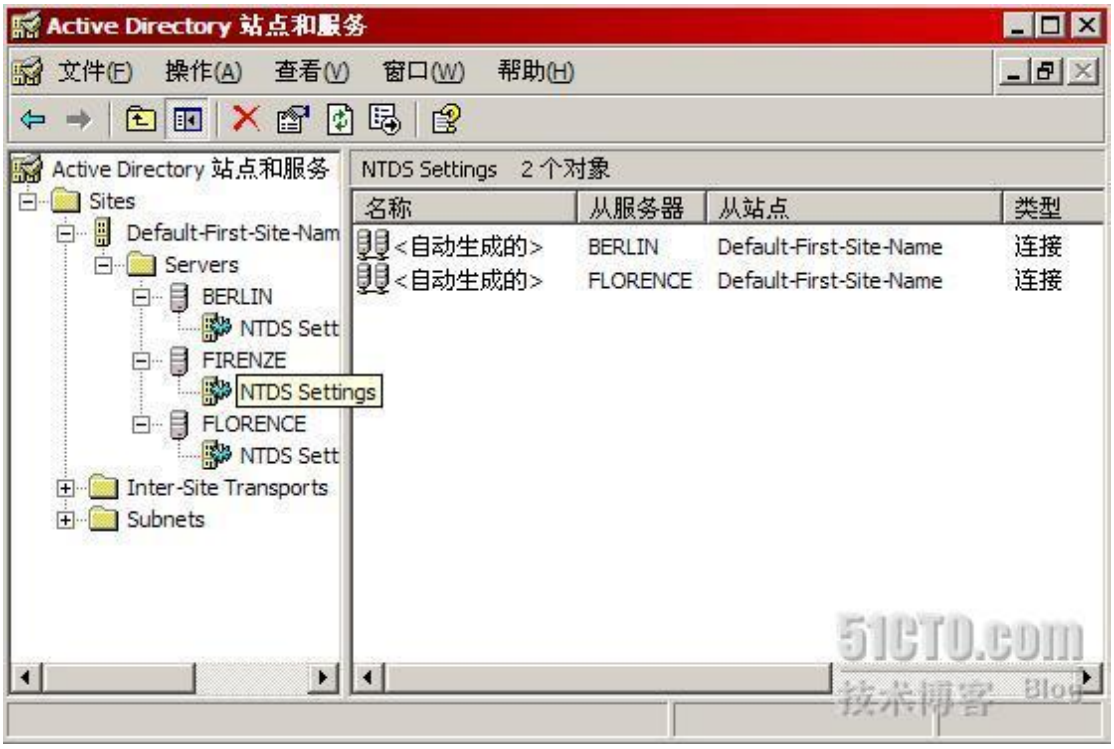


域控制器复制 Active Directory 时，一般会使用“带通知的拉复制”，也就是说，当 DC1 修改了 Active Directory 后，DC1 会在 5 分钟内通知自己的复制伙伴 DC2，“快来，我的 AD 中有些新内容”。DC2 收到通知后，会启动一个 Active Directory 的复制请求，以增量复制的方式从 DC1 把 Active Directory 复制到 DC2。如果 Active Directory 中发生了一些紧急事件，例如用户口令被修改，那么此时域控制器将不受 5 分钟的时间限制，而是在最短时间内把 Active Directory 复制给 PDC 操作主机。如果一个域控制器在一个小时之内都没有收到复制伙伴发来的通知，它就会向复制伙伴发出一个查询，询问复制伙伴是否在线。

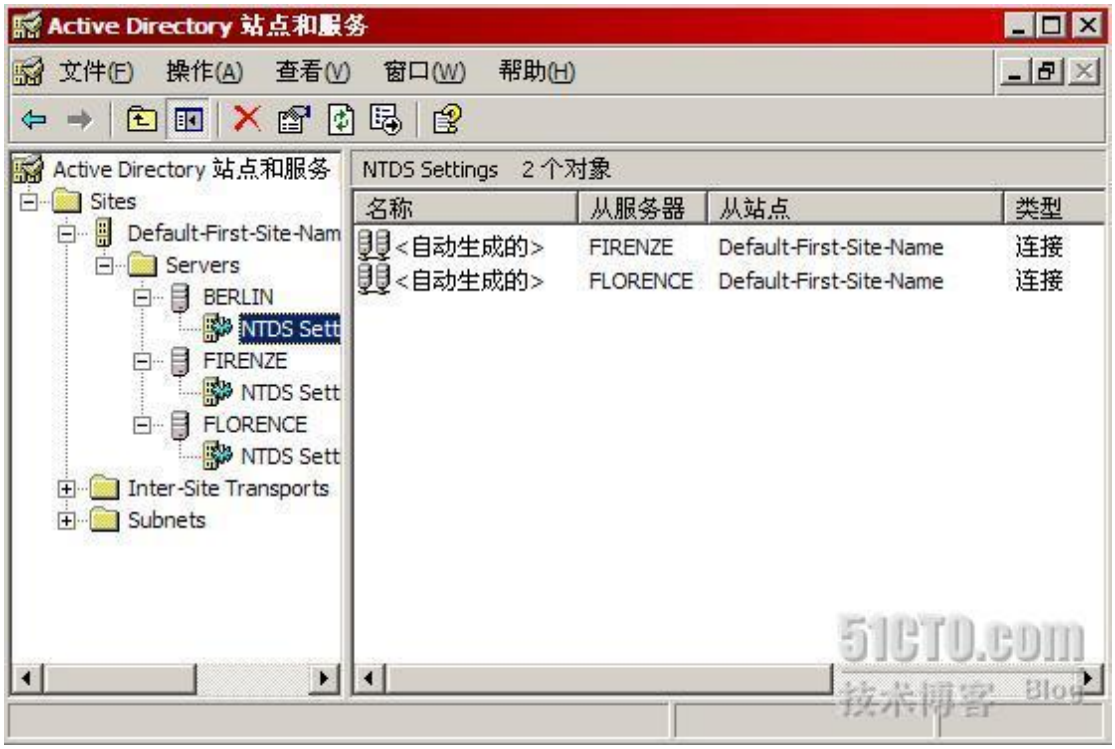
我们通过一个实例来观察一下域控制器的复制拓扑，Adtest.com 域中有 Florence，Firenze 和 Berlin 三个额外域控制器，我们在 Florence 打开 Active Directory 站点和服务，可以看到每个域控制器的复制伙伴。如下图所示，Florence 的复制伙伴是 Berlin 和 Firenze。



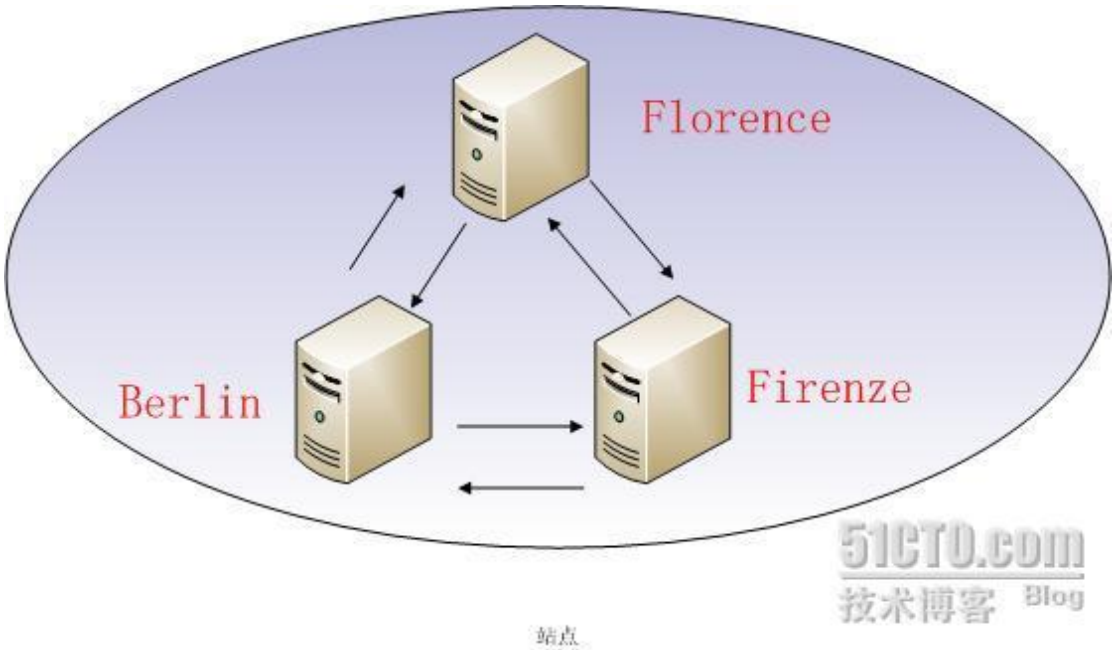
而 Firenze 的复制伙伴是 Florence 和 Berlin。



Berlin 的复制伙伴是 Florence 和 Firenze。



看完三个域控制器的复制伙伴，我们很容易勾勒出 Active Directory 的复制拓扑，这是一个标准的双环拓扑，拓扑如下图所示。



站点

双环拓扑非常优美，但并非适合所有场合！在域控制器较多的网络中，标准的环形拓扑就不太合适，因为域控制器复制 Active Directory 时有个严格的限制，那就是从源域控制器到目标域控制器不能超过三个域控制器的间隔。具体来说就

是如果 DC1 的 Active Directory 发生了变化，那么 DC1 可以复制给 DC2，DC2 可以接着复制给 DC3，DC3 还可以复制给 DC4，但 DC4 就不能再复制给 DC5 了！因为这时从 DC1 到 DC5 中间间隔的域控制器已经超过了三个。微软进行这个限制，估计是为了避免在大型网络中进行 Active Directory 复制时环形拓扑导致的延迟问题，试想一下，如果一个大型网络中有 100 个域控制器，域控制器复制的平均间隔为 5 分钟，那么从第一个域控制器复制到最后一个域控制器可能需要大约 500 分钟！这种延迟是不可接受的，因此在大型网络中 KCC 会使用网状拓扑，网状拓扑就不像环形拓扑那样有规律了，每个域控制器可能会有多个复制伙伴，看起来并不像环形拓扑那样有规律。域控制器的复制拓扑最好由 KCC 来规划，当然，也可以自己指定域控制器的复制伙伴，例如我们想指定 Florence 的复制伙伴，我们可以如下图所示，在 Florence 上选择“新建 Active Directory 连接”。

如下图所示，Florence 可以从域控制器列表中选择自己的复制伙伴。这样一来，我们就完成了对 Florence 复制伙伴的手工指定。

域控制器的复制拓扑最好由 KCC 来自动计算，域控制器一旦复制拓扑出现问题，处理时需要相当的耐心，而且要结合 DNS 的 SRV 记录来进行排错，可能还需要对 Active Directory 数据进行手工处理。以后有机会我们会介绍一些 Active Directory 排错的高级工具以及实际案例供大家参考，希望大家都能够处理好这个问题。

ACTIVE DIRECTORY 操作主机详解

在前面的博文中，我们已经了解到每个域控制器都能自主修改 Active Directory，而且修改后的结果会被其他的域控制器所承认。从这个角度讲，域控制器之间的地位是平等的，但我们决不能认为域控制器之间是没有区别的！事实上，域中的第一个域控制器往往比其他的域控制器承担了更多的任务。

有些企业中部署了多个域控制器之后，就开始忽略第一个域控制器的作用，有时甚至可能会一不经意间把第一个域控制器给处理掉了。但这些企业的用户很

快就会发现域中会出现一些异常现象，例如无法创建域用户账号，无法安装 Exchange，无法部署子域等等。原因很简单，第一个域控制器承担的任务并没有被转嫁到其他的域控制器上，而这些任务对一个域来说又是不可或缺的，因此我们才会面临如此多的问题。那么，究竟第一个域控制器和其他的域控制器相比承担了哪些更多的任务呢？这就是我们今天要讨论的话题，操作主机！

操作主机是由域控制器来扮演的一种角色，**操作主机角色共有五种，分别是 PDC 主机，RID 主机，结构主机，域命名主机和架构主机**，今天的这篇博文将分别介绍五种操作主机的用途。

我们先来介绍 PDC 主机，PDC 是主域控制器的缩写，在 NT4 时代，域控制器被分别 PDC（主域控制器）和 BDC（备份域控制器），只有 PDC 才可以修改目录数据库，BDC 的数据库是从 PDC 复制而来的。从 Win2000 开始，所有的域控制器都可以修改 Active Directory 了，那为什么 Win2003 的操作主机中还有 PDC 主机这个角色呢？原因是这样的，微软为了保护用户的前期投资，允许 NT4 服务器称为 Win2003 域中的额外域控制器，但 NT4 充当域控制器时一定要和域中的 PDC 联系，这种情况下 PDC 主机就要挺身而出，以主域控制器的身份和 NT4 的域控制器通讯。这就是 PDC 主机的第一个用途，兼容 NT4 服务器。

PDC 主机的第二个用途是可以优先成为主浏览器，这里说的浏览器可不是上网冲浪用的浏览器，而是网络中的一种计算机角色。我们都知道打开网上邻居后可以看到当前网络中有多少台计算机，双击计算机名还可以看到这台计算机提供的共享资源。这些网络资源列表是由谁来提供呢，在微软网络中被一种称为主浏览器的计算机来提供。那么哪些计算机可以成为主浏览器呢？只要操作系统的版本在 Windows workgroup 3.1 以上的计算机都有机会成为主浏览器。如果一个网络中的多台计算机都希望成为主浏览器，那么这些计算机就会通过“选举”来解决问题，我们有时用抓包工具可以抓到电子选举包就和这个过程有关。每台计算机选举时首先比较操作系统版本，版本新的优先成为主浏览器，例如 Win2003 优于 Win2000。如果操作系统版本相同，再比较谁是域控制器，域控制器比普通的计算机优先。如果参与选举的有多个域控制器，那么 PDC 主机会优先。最后再多说一句，如果一个广播域内有多个域，而且有多个 PDC 操作主机，那么它们之间又如何进行主浏览器的选举呢？它们之间会通过 GUID 来选出最后的胜利

者。

PDC 主机的第三个用途就是 Active Directory 的优先复制权，正常情况下，Active Directory 的复制周期是 5 分钟，但如果 Active Directory 中发生了一些紧急事件，例如修改了用户口令。这种情况下源域控制器就会在最短时间内通知 PDC 主机，由 PDC 主机来统一管理这些 Active Directory 的紧急事件。如果一台域控制器发现用户输入的口令和 Active Directory 中存储的口令不一致，域控制器考虑到有两种可能性，一种可能是用户输入错误，一种可能是用户输入的口令是正确的，但是自己的 Active Directory 还没有接收到最新的变化。域控制器为了避免自己判断错误，就会向 PDC 主机发出查询，请 PDC 主机来验证口令的正确与否，因为前面已经提到，任意一个域控制器修改了用户口令，都会在最短时间内通知 PDC 主机。

PDC 主机除了上述的几种用途，还可用于充当域内的权威时间源，同时 PDC 主机也是组策略的首选存储地点。顺便提一下，PDC 主机的作用级别是域级别，也就是说，在一个域中只能有一台域控制器充当 PDC 主机。

介绍完 PDC 主机的作用后，我们来介绍 RID 主机。RID 是 SID 的一部分，什么是 SID 呢？SID 是安全标识符（**S**ecurity **Id**entify）的缩写，当我们在域中创建用户账号或计算机账号时，操作系统会为被创建的账号建立一个对应的 SID，也就是说，SID 真正对应了用户账号或计算机账号。一个域用户对应的 SID 格式是这样的，S-1-5-21-D1-D2-D3-RID，S 是 SID 的缩写，1 是 SID 的版本号，5 代表授权机构，21 代表子授权，D1-D2-D3 是三个数字，代表对象所在的域或计算机，RID 是对象在域中或计算机中的相对号码。以大家熟悉的管理员账号为例，管理员的 SID 就是 S-1-5-21-3855104193-3464347045-3256418734-500，其中的 RID 是 500。

RID 是 SID 的组成部分，RID 主机的作用就是为 Active Directory 提供一个可用的 RID 池（默认 500 个），而且当池中的 RID 被消耗到一定程度后再自动补充满。如果 RID 主机出现故障，显然会对我们创建大量的用户账号造成麻烦。和 PDC 主机类似，RID 主机的作用级别也是域级别。

结构主机的作用是负责对跨域对象的引用进行更新，假如 A 域的一个用户加入了 B 域的一个组，B 域的结构主机就会负责关注 A 域的这个用户是否发生了什

么变化，例如是否被删除了，结构主机的工作可以确保域间对象引用的可操作性。如果是一个单域，基本上用不着结构主机做什么工作。如果在一个多域的林环境，有一点要切记，结构主机不要和 GC（全局编录）放在同一台域控制器上，否则结构主机无法正常工作。结构主机的作用级别也是域级别。

下一个要介绍的操作主机是域命名主机，这个操作主机的作用级别是林级别的！域命名主机主要负责控制域林内域的添加或删除，也就是说如果在域林内添加一个新域，必须由域命名主机判断域名合法，操作才可以继续。如果域命名主机不在线，我们就无法完成域林内新域的创建。除了对域名做出诠释，域命名主机还要负责添加或删除描述外部目录的交叉引用对象。

最后我们要介绍的是架构主机，架构主机的作用级别同样是林级别。架构主机的作用非常重要，如果要修改 Active Directory 的架构，我们只能从架构主机上进行操作。微软的很多高级服务器产品在部署时都需要修改 Active Directory 的架构，例如 Exchange，Office Communications Server，SMS 等。以最著名的 Exchange 为例，如果我们在域中部署 Exchange 时无法在线联系上架构主机，那 Exchange 的部署就无法继续，MCSE 的考题中曾经考过这个知识点。

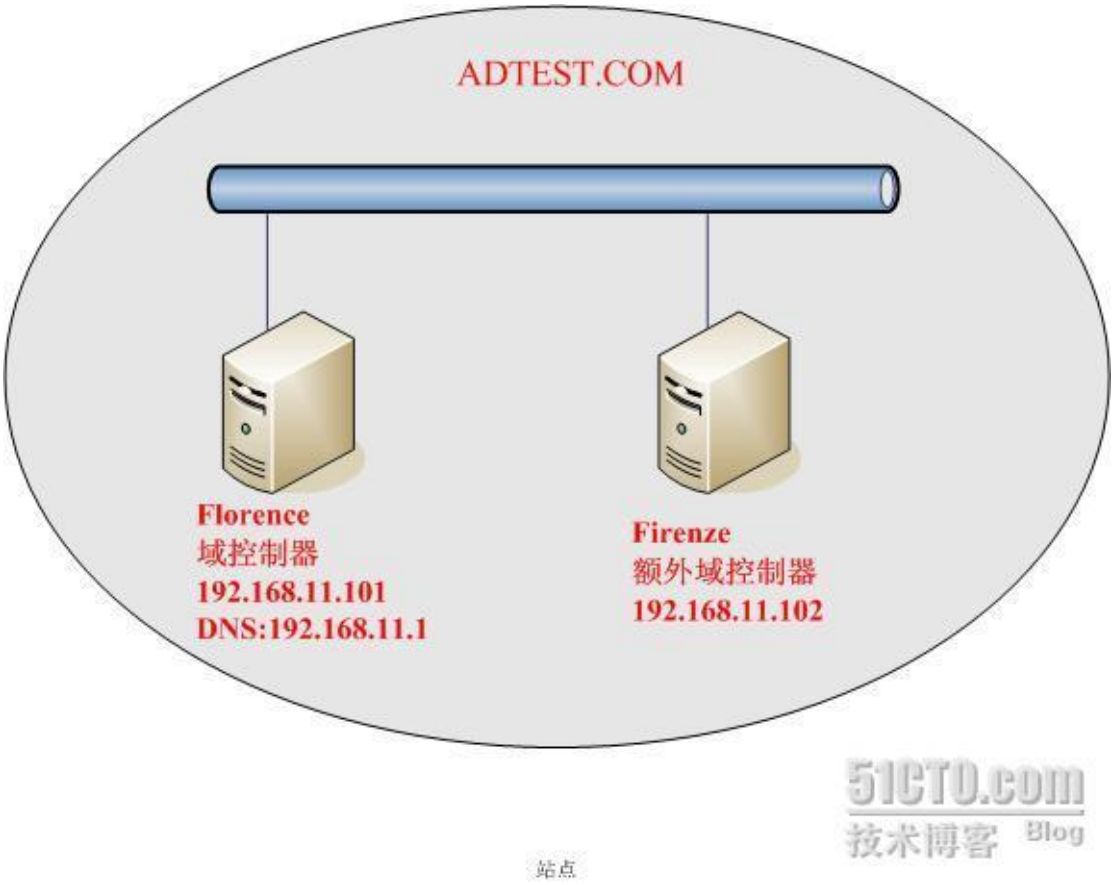
从上面的介绍中我们可以看出，操作主机都有各自的职能，一旦操作主机有问题我们就会遇到种种麻烦，因此我们在下篇博文中将介绍如何转移操作主机角色以及如何夺取操作系统角色，敬请期待。

实战操作主机角色转移

上篇博文中我们介绍了操作主机在 Active Directory 中的用途，今天我们通过一个实例为大家介绍如何实现操作主机角色的转移，这样如果 Active Directory 中操作主机角色出现了问题，我们就可以用今天介绍的知识来进行故障排除。

我们首先要明确一个重要原则，那就是操作主机角色有且只能有一个！如果操作主机角色工作在林级别，例如架构主机和域命名主机，那在一个域林内只能有一个架构主机和域命名主机。如果操作主机角色工作在域级别，例如 PDC 主机，结构主机和 RID 主机，那就意味着一个域内只能有一个这样的操作主机角色。

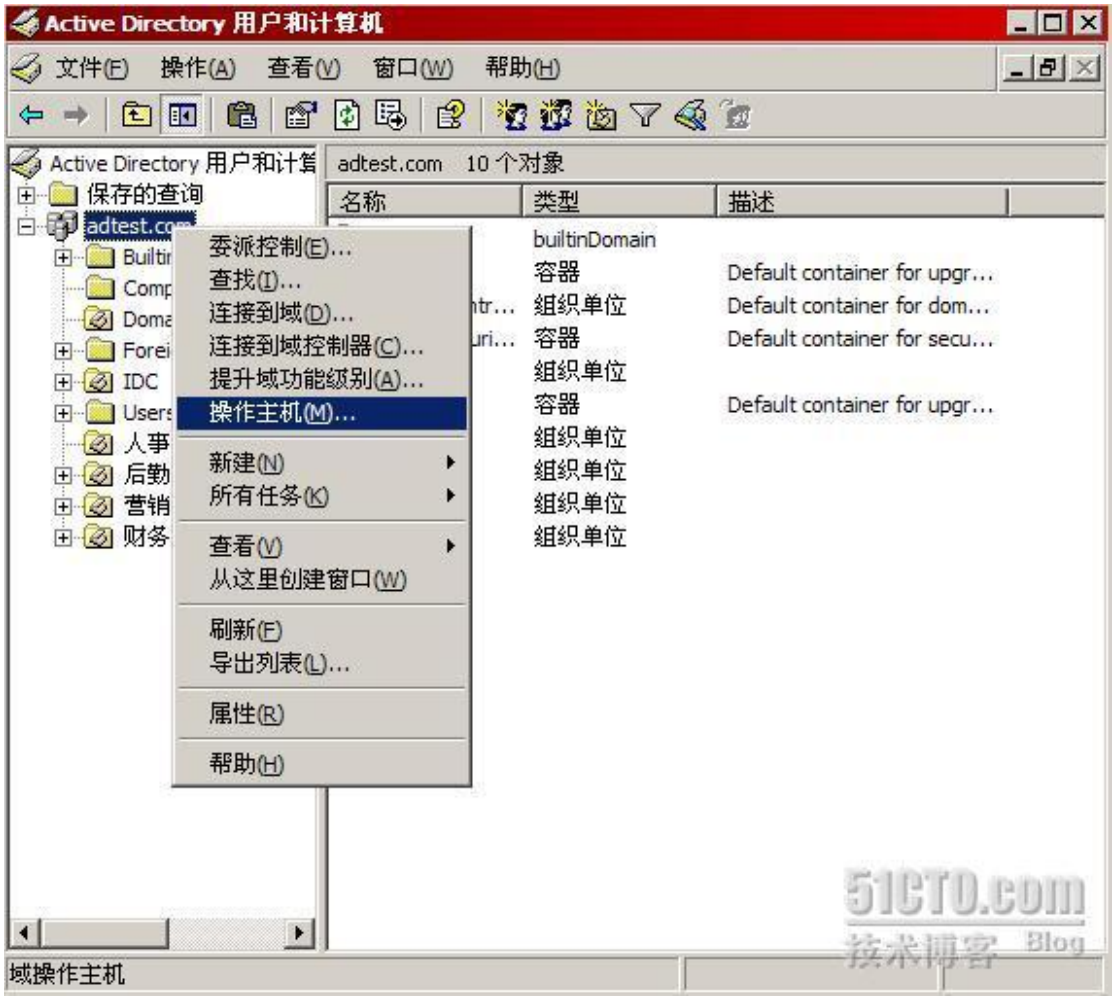
我们的实验拓扑如下图所示，Adtest.com 域内有两个域控制器，Florence 和 Firenze。Florence 是域内的第一个域控制器，目前所有的操作主机角色都在 Florence 上，我们通过实验来介绍如何在 Florence 和 Firenze 间切换操作主机角色。



其实当我们用 Dcpromo 卸载域控制器上的 Active Directory 时，这个域控制器会自动把自己所承担的操作主机角色转移给自己的复制伙伴，这个过程完全不需要管理员的干预。但如果我们希望指定一个域控制器来负责操作主机角色，我们就需要手工操作了。我们首先为大家介绍如何用 MMC 控制台把五个操作主机角色从 Florence 转移到 Firenze 上。

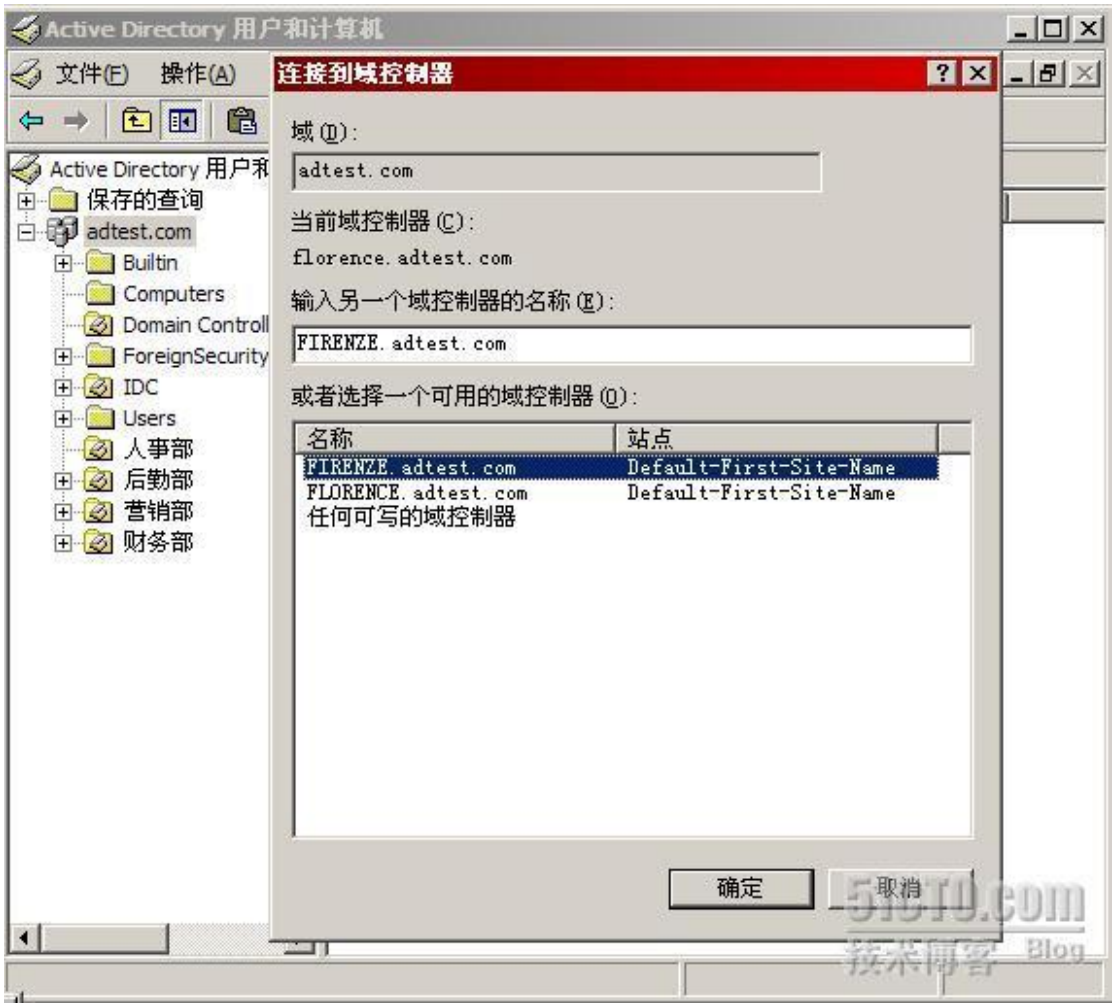
一 从 Florence 转移到 Firenze

在 Florence 上打开 Active Directory 用户和计算机，如下图所示，右键点击域名，在菜单中选择“操作主机”。



如下图所示，我们发现可以转移三个操作主机角色，分别是 PDC 主机，RID 主机和结构主机，但奇怪的是，我们希望把操作主机角色从 Florence 转移到 Firenze，但为何工具中显示的是我们只能把操作主机角色从 Florence 转移到 Florence 呢？

上述问题很容易解释，如果我们希望把 Firenze 作为操作主机角色转移的目标，那我们就需要把域控制器的焦点首先指向 Firenze。从下图所示，在 Active Directory 用户和计算机中右键单击 adtest.com，选择“连接到域控制器”，从域控制器列表中选择 Firenze 即可。



我们把域控制器的焦点指向 Firenze 后，接下来就发现可以把操作主机角色从 Florence 转移到 Firenze 了，如下图所示，我们点击“更改”，准备把 RID 主机角色从 Florence 转移到 Firenze。系统弹出窗口询问是否确定进行操作主机角色的转移，我们选择“是”。

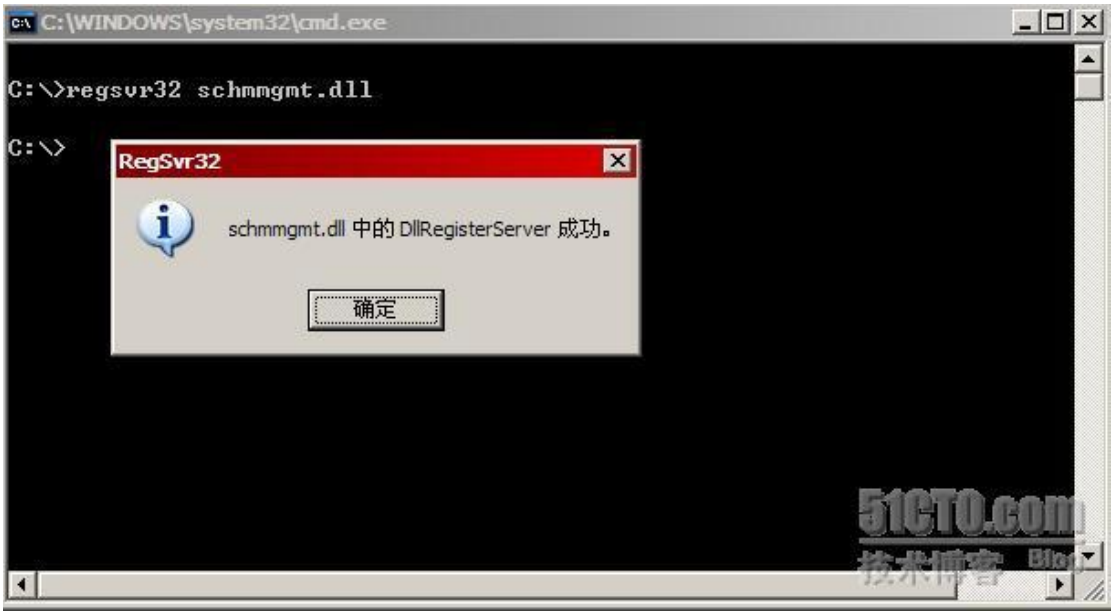
通过上述过程，我们可以非常轻松地把 RID 主机角色从 Florence 转移到 Firenze，如下图所示，操作主机角色的转移已经成功。用同样的方法，我们可以很轻松地把 PDC 和结构主机也转移到 Firenze 上。

转移了 RID 主机，PDC 主机和结构主机后，我们来尝试一下域命名主机。在 Florence 上打开 Active Directory 域和信任关系，注意先把域控制器的焦点指向 Firenze，然后如下图所示，右键单击 Active Directory 域和信任关系，从菜单中选择“操作主机”。

如下图所示，我们点击“更改”把域命名主机角色从 Florence 转移到 Firenze，整个过程实现起来非常简单。

如下图所示，域命名主机角色已经转移到 Firenze 上了。

最后我们要转移的操作主机角色是架构主机，架构主机由于角色非常重要，微软甚至没有为我们预设管理工具，因此我们首先要通过注册动态链接库来获得转移架构主机所需要的管理工具。如下图所示，我们运行 regsvr32 schmmgmt.dll，系统提示注册动态链接库成功。



注册了动态链接库后，我们运行 MMC，在文件菜单中选择“添加/删除管理单元”，这时我们会发现可以添加一个名为“Active Directory 架构”的管理单元，这就是注册了动态链接库的作用。使用这个 Active Directory 架构管理单元，如下图所示，选择“操作主机”进行架构主机的转移，同样不要忘记在之前把域控制器焦点指向 Firenze。

如下图所示，点击“更改”把架构主机角色转移到 Firenze 上。

从下图的结果来看，架构主机的转移是成功的，至此，我们完成了五个操作主机角色的转移。

二 从 Firenze 转移到 Florence

现在五个操作主机角色都集中在 Firenze 上，我们再为大家介绍一种方法把操作主机角色完璧归赵，还给 Florence，这种方法就是使用我们非常熟悉的工具 NTDSUTIL。如下图所示，运行 ntdsutil，然后输入 roles，准备进行操作主机角色的转移。

如下图所示，在 Roles 状态下，我们首先要使用 connections 命令来连接到特定的域控制器，连接到哪个域控制器呢？应该连接到操作主机转移的目标域控制器，在我们这个例子中应该是 Florence，如图所示，我们输入命令 connect to server Florence。

连接到 Florence 后，如下图所示，我们用 quit 命令返回上级菜单，用？列出当前状态下的所有可执行指令，我们发现转移五个操作主机角色只需要简单执行五条命令即可，这五条指令分别是：

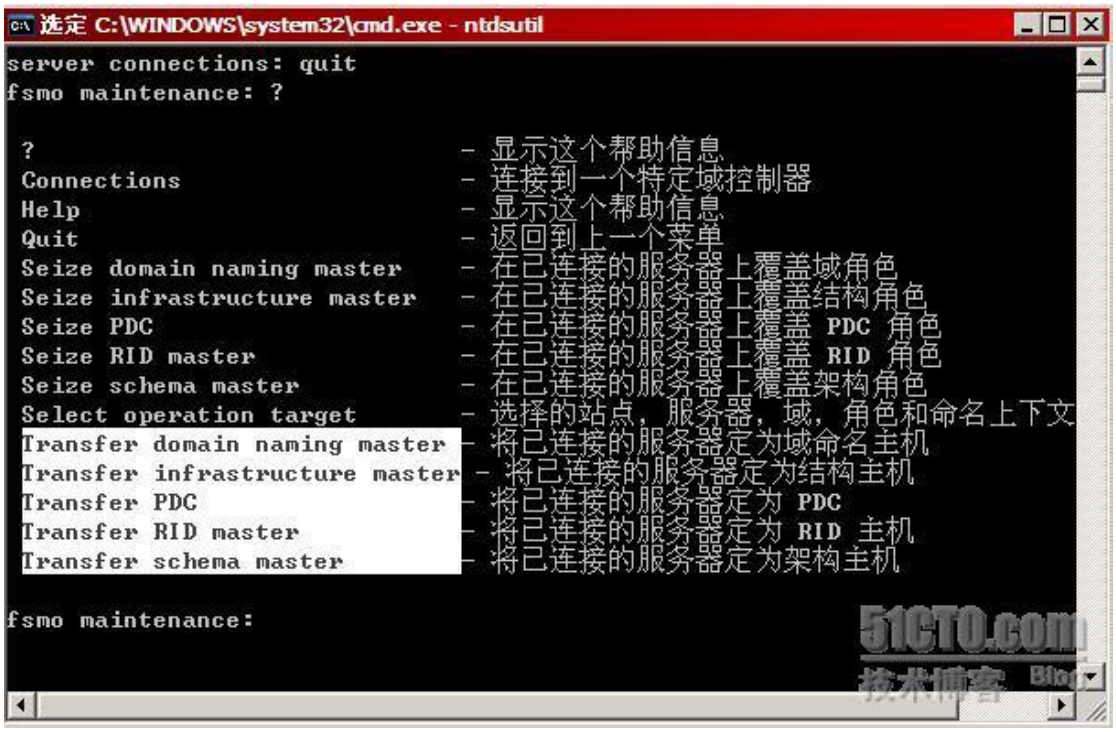
Transfer domain naming master 转移域命名主机

Transfer infrastructure master 转移结构主机

Transfer PDC 转移 PDC 主机

Transfer RID master 转移 RID 主机

Transfer schema master 转移架构主机



还有五条命令是强行把连接到的域控制器指定为操作主机角色，这个很适合在操作主机离线时进行操作，如果我们不小心把操作主机所在的域控制器给格式化了，我们就可以利用这些指令强行把一个域控制器指定为操作主机。这五条指令分别是：

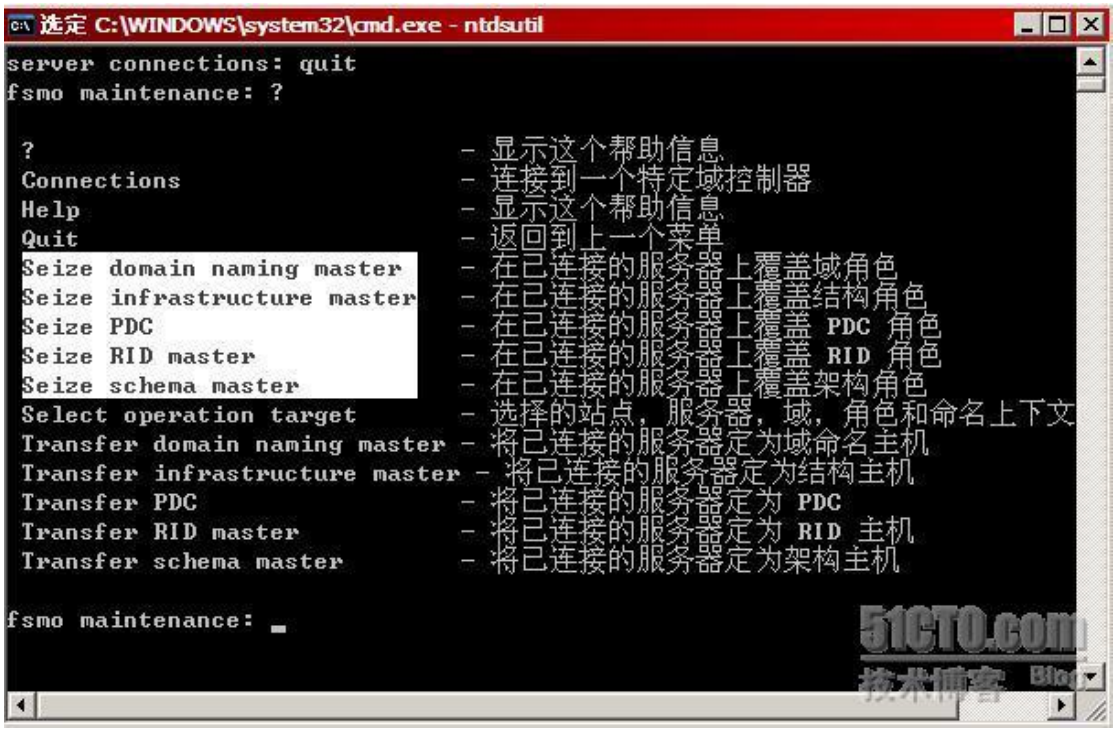
Seize domain naming master　指定域命名主机

Seize infrastructure master　指定结构主机

Seize PDC　指定 PDC 主机

Seize RID master　指定 RID 主机

Seize schema master　指定架构主机



如下图所示，我们执行转移操作主机角色的五条指令，很轻松地把操作主机角色从 Firenze 又转到了 Florence 上。

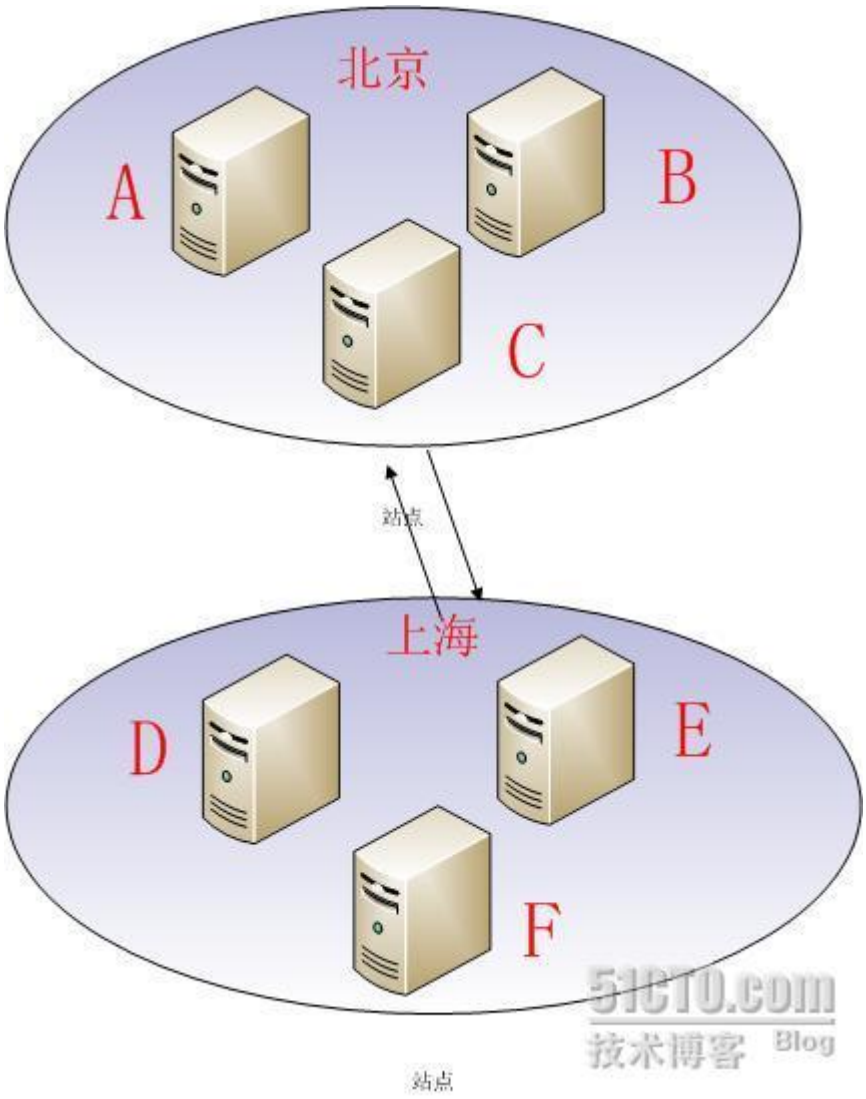
在本篇博文中，我们可以利用 MMC 和 NTDSUITL 进行操作主机角色的转移，也可以在操作主机离线的情况下进行操作主机角色的指定，掌握了这些，基本上

就可以应对工作中对操作主机的需求了。

什么是站点

谈到 Active Directory 中的站点，很多 Active Directory 的初学者都会深感头疼，为什么呢？搞不清楚这个站点究竟是起什么作用。有很多同学都问过这样的问题，站点和域有什么区别？到底是域大还是站点大？有了域为什么还要有站点？…..本文将尝试为大家介绍站点的概念及设计初衷，让大家能够更好地理解站点，运用站点。

域是共享用户账号，计算机账号及安全策略的一组计算机，这个定义是基于逻辑因素考虑的，只要用户和计算机在同一个 Active Directory 内，我们就认为他们都在域的安全边界之内。我们从域的定义中可以看到，域没有考虑网络速度等物理因素，无论计算机和域控制器之间是一个快速的物理连接还是一个慢速的物理连接，域都会一视同仁，完全把连接速度视若无物。但在实际的生产环境中我们就会发现如果不考虑网速这样的物理因素，我们会在管理域时遇到很多麻烦。我们通过一个例子加以说明，如下图所示，某域的域控制器分布在北京，上海两处，北京有 A,B,C 三台域控制器，上海有 D,E,F 三台域控制器。北京和上海的本地局域网都是千兆以太网，北京和上海之间是一条 128K 的专线。



站点

现在我们要考虑这么一个问题，如果域控制器 A 更改了 Active Directory，那么如果才能用最有效率的方法把这个 AD 的变化复制到其他五个域控制器上呢？显然域控制器 A 应该先把更改复制到同一高速局域网内的 B 和 C，然后再利用慢速的广域网链接复制到上海的一个域控制器上，例如复制到 D，最后再由 D 复制到 E 和 F。域控制器如果使用我们规划的这种复制拓扑，那当然好，在这种复制拓扑中数据只经过两地间的慢速链路传递了一次。但问题是域如果不考虑速度因素，未必能作出这种拓扑，万一 KCC 决定使用的复制拓扑是先从 A 到 D，再从 D 到 B，然后 B 到 E，再 E 到 C，最后从 C 到 F，那我们就要崩溃了。这样的话六个域控制器之间的 AD 复制要沿着两地间的慢速链路走五次，无论如何都让我们无法接受！从这个例子中我们已经看到了速度因素的重要性，再顺着这个例子引申一下，用户每天登录到域进行身份验证，显然北京的用户应该登录到北京的

域控制器，上海的用户应该登录到上海的域控制器，这样效率才会比较高，如果北京的用户每天都到上海的域控制器进行身份验证，显然不是一件好事。

从上面的例子中我们发现，在日常的运维工作中是不能把速度因素透明处理的，我们必须考虑到计算机之间的连接速度！正是基于这种考虑，微软才引入了站点对计算机进行管理。站点的概念其实很简单，站点就是高速相连的一组计算机！从这个概念来看，站点强调了速度这个物理因素，域则是强调要共享 Active Directory 这个逻辑因素，把站点和域结合起来对计算机从物理和逻辑两个角度进行管理，是微软的一个很好的构思。值得一提的是，微软这种管理思路并非罕见，例如 Exchange 中也有管理组和路由组的概念，管理组和路由组其实类似于域和站点的关系，也是一个从逻辑角度进行管理，另一个从物理角度进行管理。

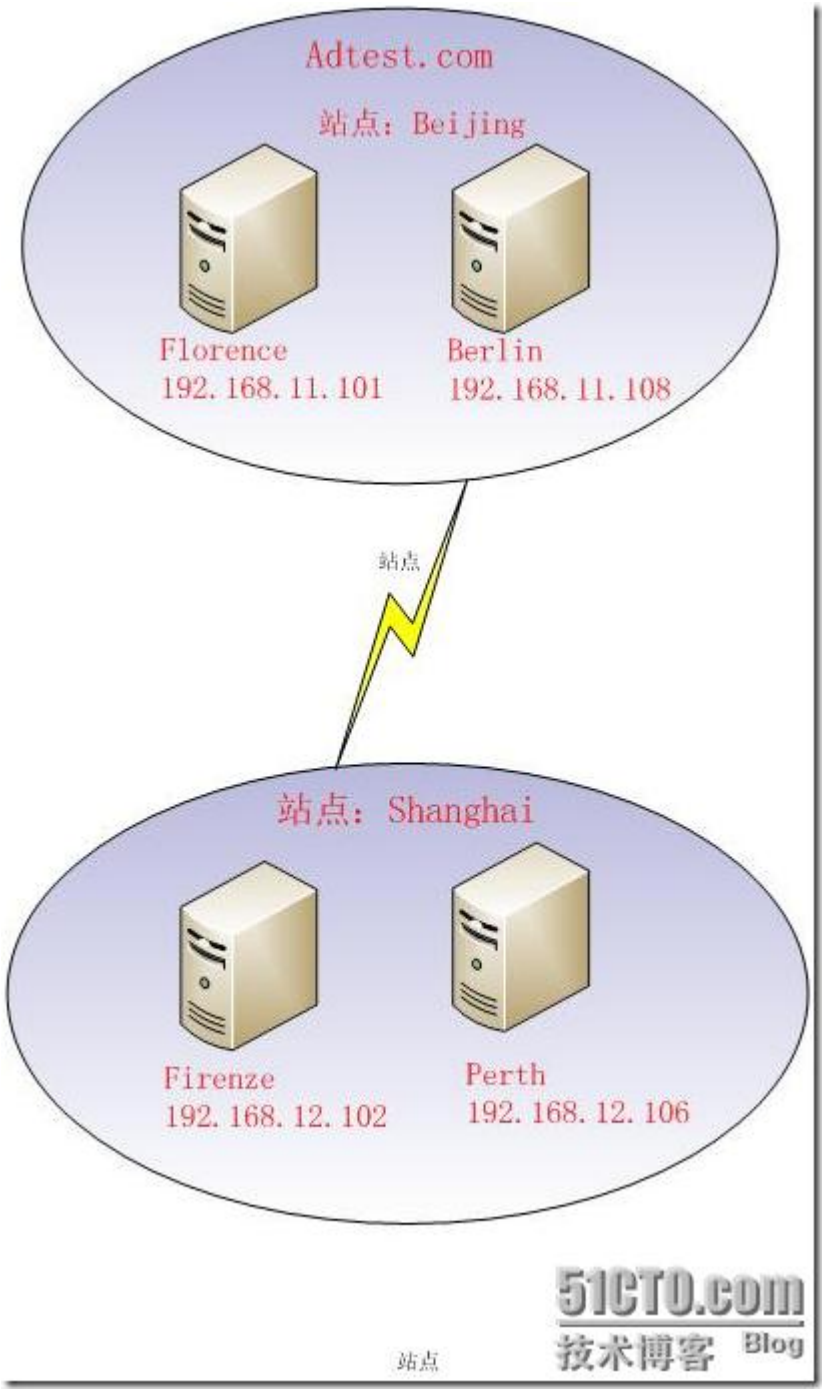
有了站点帮助管理，我们处理前面提到的那个例子就容易多了，从站点的定义来看，由于北京和上海之间存在一条慢速链路，因此我们应该把北京的计算机放到一个站点内，把上海的计算机放到另一个站点内。这样的话，北京和上海的用户在登录时会优先选择本站点内的域控制器登录，KCC 在规划复制拓扑时也会自动地优先考虑在本站点内的域控制器之间进行 AD 复制。更好的是，如果 AD 需要垮站点复制，AD 内容还可以经过压缩后再进行复制，显然站点在设计时已经充分考虑到了对带宽的充分利用。

从理论上证明了站点的必要性，我们在下篇博文中就要付诸实践了，我们将在下篇博文中通过实例为大家介绍如何进行站点的创建及管理，敬请关注！

实战 ACTIVE DIRECTORY 站点部署与管理

上篇博文中我们家介绍了站点的设计目的及大致原理，今天我们通过实战为大家介绍如何进行站点的部署以及管理。实验拓扑如下图所所示，adtest.com 域中有四个域控制器，分别是 Florence，Berlin，Firenze 和 Perth。其中 Florence 和 Berlin 在北京，隶属于 192.168.11 网段；Firenze 和 Perth 在上海，隶属于 192.168.12 网段。由于北京和上海之间使用了一条 64K 的 DDN 慢速链路，因

此我们有必要使用站点对域内的计算机进行合理规划，以便能够让域内的计算机在现有的带宽条件下能以最有效率的方式通讯。



目前四台域控制器都在一个站点中，如下图所示，就是默认的 Default-First-Site-Name。根据我们本次实验的具体情况，我们需要把北京和上海的域控制器分为两个站点，为完成这个任务，我们需要进行下列操作：

一 创建站点

二 定义站点子网

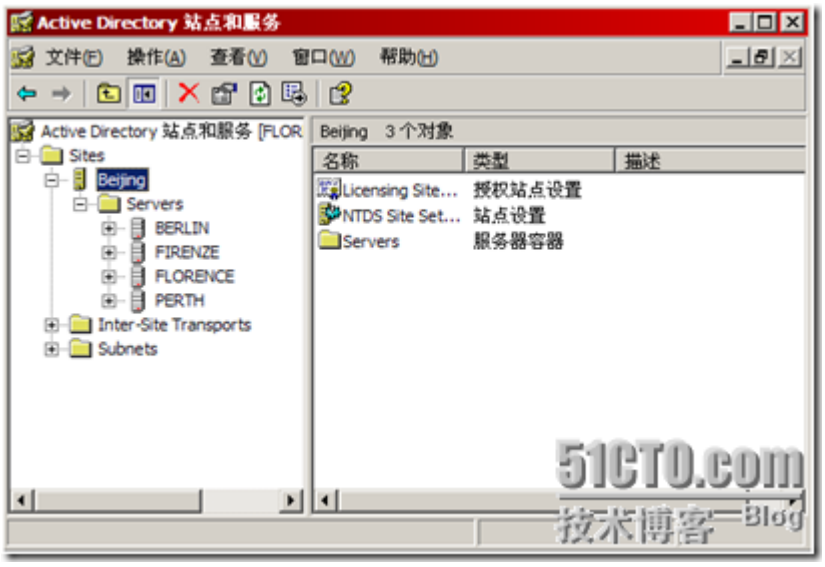
三 定位服务器

四 配置站点链接器

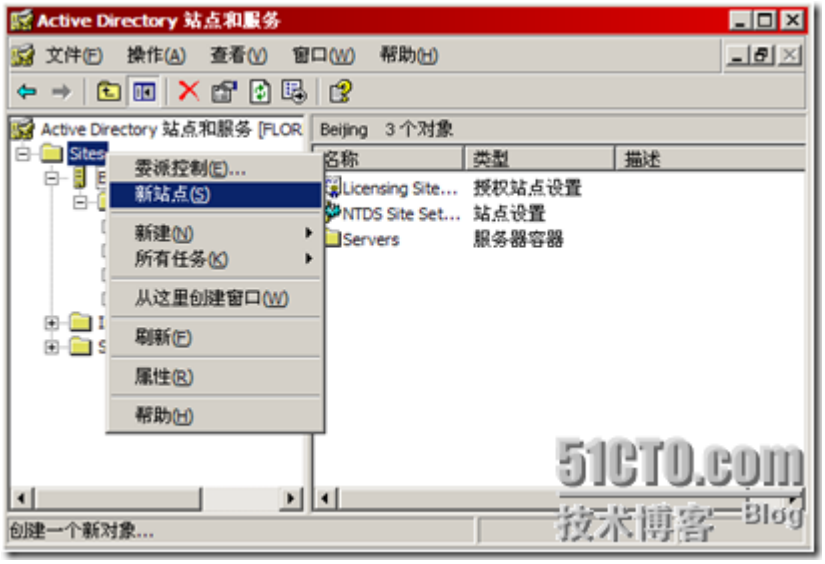
一 创建站点

默认情况下所有的域控制器都在一个站点内，但目前我们需要两个站点，一个用于管理北京的计算机，一个用于管理上海的计算机。因此我们需要创建一个新站点，同时把原先的默认站点改名即可。首先我们先把原来的默认站点 Default-First-Site-Name 改名为 Beijing，我们在域控制器 Florence 上打开 Active Directory 站点和服务，，如下图所示，右键点击原来的默认站点，选择“重命名”。

重命名后的结果如下图所示，默认站点已经改名为 Beijing。



接下来我们来创建一个新站点 Shanghai，如下图所示，右键点击“Sites”，选择新站点。



如下图所示，新站点取名为 Shanghai，我们为 Shanghai 站点选择了一个默认的站点链接器，关于这个站点链接器的作用我们将在后面的内容中予以介绍。

Shanghai 站点创建完毕后，系统提示我们要进行如下图所示的后续操作，我们接下来将按照提示实现对站点的配置。

二 定义站点子网

现在我们有了 Beijing 和 Shanghai 两个站点，接下来要考虑如何定义站点内的 IP 子网。如果不同的站点管辖了不同的 IP 子网，那么对域内的计算机来说是非常有利的，域控制器只要根据自己的 IP 地址就可以判断出自己应该隶属于哪个站点，域内的客户机登录到域时也会根据自己的 IP 地址来查询同一站点内的域控制器进行登录。

创建站点所属的子网并不难，如下图所示，右键单击 Subnets，选择“新建子网”。

如下图所示，我们创建了一个子网 192.168.11，然后把这个子网分配给了 Beijing 站点。

如法炮制，我们为 Shanghai 站点创建了 192.168.12 子网。这样以后如果有新的域控制器加进来，域控制器根据 IP 地址就可以自动加入相应的站点。

三 定位服务器

定义了站点子网后，我们接下来就要根据每个域控制器的 IP 地址来把它们加入不同的站点了。我们准备把 Florence 和 Berlin 放在 Beijing 站点，Firenze 和 Perth 放在 Shanghai 站点。如下图所示，右键单击 Firenze，选择“移动”。

然后我们选择把 Firenze 移动到 Shanghai 站点。

用同样的方法我们把 Perth 也移动到 Shanghai 站点，移动后的域控制器分布如下图所示，Beijing 和 Shanghai 站点各有两个。

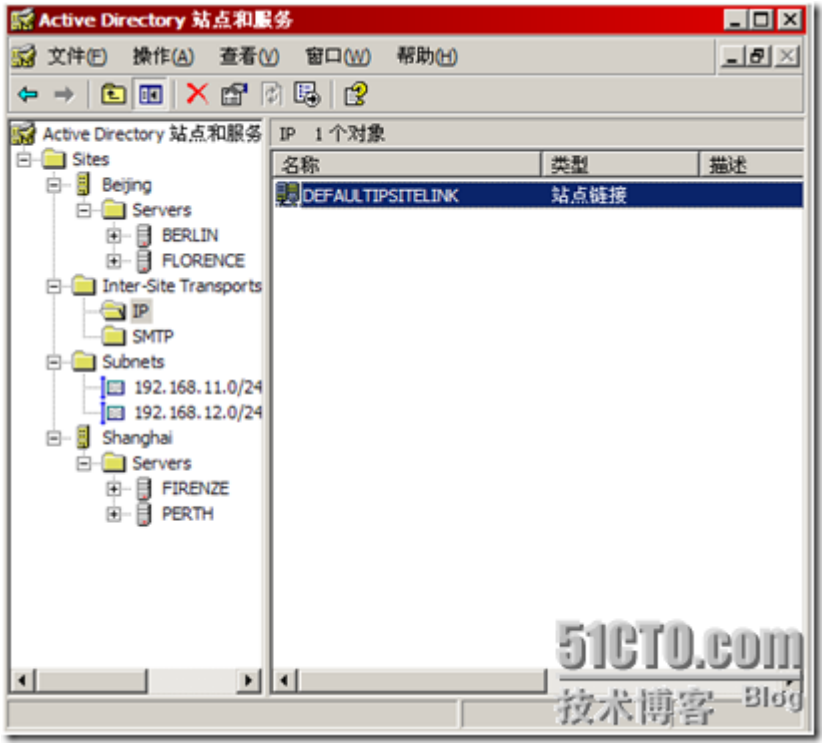
四 配置站点链接器

现在我们已经配置好了站点子网，然后把域控制器放到了相应的站点中，现在我们要考虑如何配置站点链接器了。站点链接器是一个逻辑控制单元，它并不负责域控制器之间的物理连接，那应该是电信部门负责的事情，即使没有站点链接器，

域内的这些处于不同城市的计算机也是可以在网络层实现联通的。链接器的作用是对不同站点间的数据传递进行控制，以便最大限度地利用好站点间的窄带链路。

有了站点之后，显然域控制器之间的 AD 复制应该优先在本站点内进行，然后站点会选出一个“桥头服务器”代表所在的站点和其他站点的“桥头服务器”进行通讯，这样 AD 的更改就可以通过两个站点间的“桥头服务器”进行跨越站点的传递。AD 复制在站点内的域控制器进行时是不压缩的，而 AD 复制如果跨站点进行则需要压缩。跨站点的 AD 复制拓扑也是由大家熟悉的 KCC 来设计的。

我们接下来看看如何利用站点链接器来控制站点间的数据传输，目前 Beijing 和 Shanghai 两个站点间使用的是一个默认的站点间链接。如下图所示，我们打开“Active Directory 站点和服务”，我们可以看到 Inter-Site-Transports 下面有 IP 和 SMTP 两个子项，这是告诉我们站点间数据复制可以使用 IP 协议或 SMTP 协议。一般我们都选择使用 IP，如果使用 IP，站点间的数据传输将使用 RPC 协议，这种协议可以传输 AD 的全部内容而 SMTP 则只能传输 AD 的部分内容。现在 Beijing 站点和 Shanghai 站点之间使用的就是基于 IP 的站点链接器。

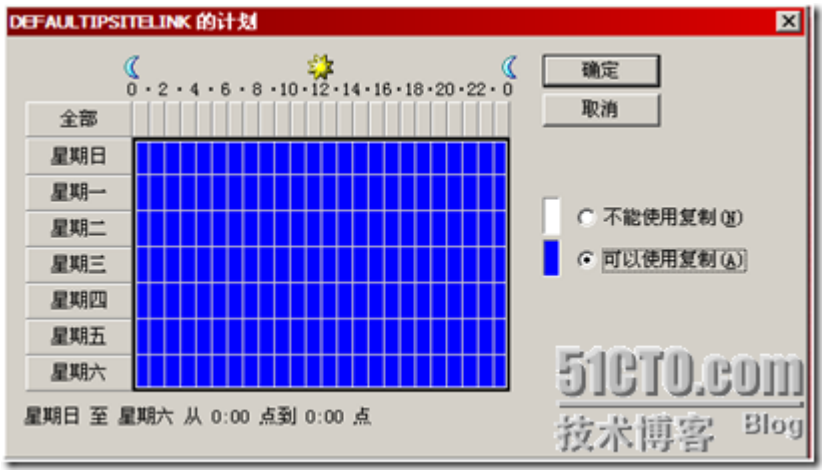


我们打开默认的站点链接器，查看属性，如下图所示，我们在常规属性中可以看到这个站点链接器连接了 Beijing 和 Shanghai 两个站点。然后我们可以看到站

点链接器的开销是 100，开销反映了站点间连接速度的快慢，开销值越小，速度越快。站点间的开销是个相对值，并不具体对应实际的连接速度，因此目前两个站点间的开销值并没有太多的讨论价值，因为没法和其他站点的开销值进行比较。如果有更多的站点，那站点开销的意义就凸显出来了。例如我们现在有北京，上海和广州三个站点，其中北京和上海之间是用 2M 的专线连接，北京和广州之间是用 64K 的专线连接，上海和广州之间则用的是 10M 的专线。那么北京的域控制器更改了 AD，如何传递给广州站点内的域控制器呢？从拓扑看，显然从北京直接传到广州就不如先从北京传到上海，再经过上海传到广州合算。我们怎么才能让 KCC 知道这个情况呢？通过站点开销就很容易做到，例如我们可以设置北京站点到广州站点的开销值是 100，而北京到上海的开销值是 20，上海到广州的开销值是 10。这样一来 KCC 在计算站点间链接时就可以通过开销值的量化指标判断出 100>10+5，因此 KCC 在安排北京站点和广州站点间的 AD 复制时会优先让 AD 数据先从北京站点复制到上海站点，再从上海站点复制到广州站点。值得注意的是，站点开销值是一个宏观上的相对值，并不具体对应传输速率。

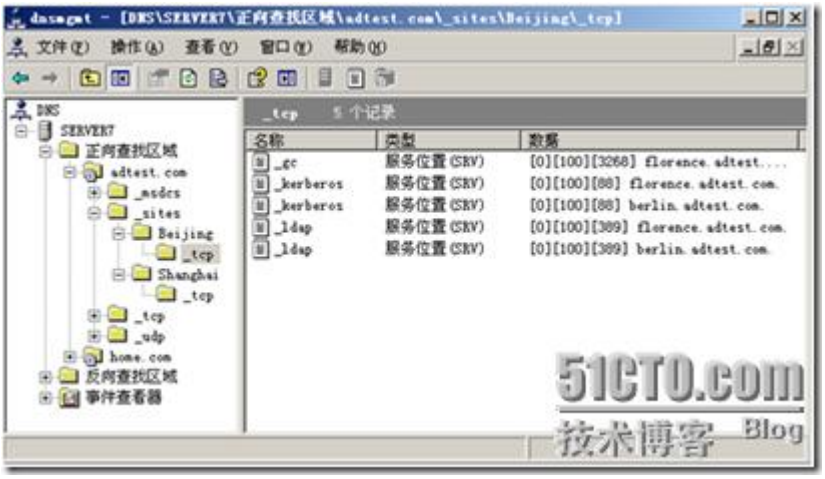
站点间的默认复制频率是 180 分钟，也就是默认情况下三个小时才跨站点复制一次，这个频率比站点内的 AD 复制低了很多，显然是为了适应广域网上的低速链路。

点击站点常规属性中的“更改计划”，我们可以设置站点间数据传输的时间段，这个设置显然有利于避开窄带利用的高峰期，在适当的时机用适当的节奏进行站点间的数据传递。



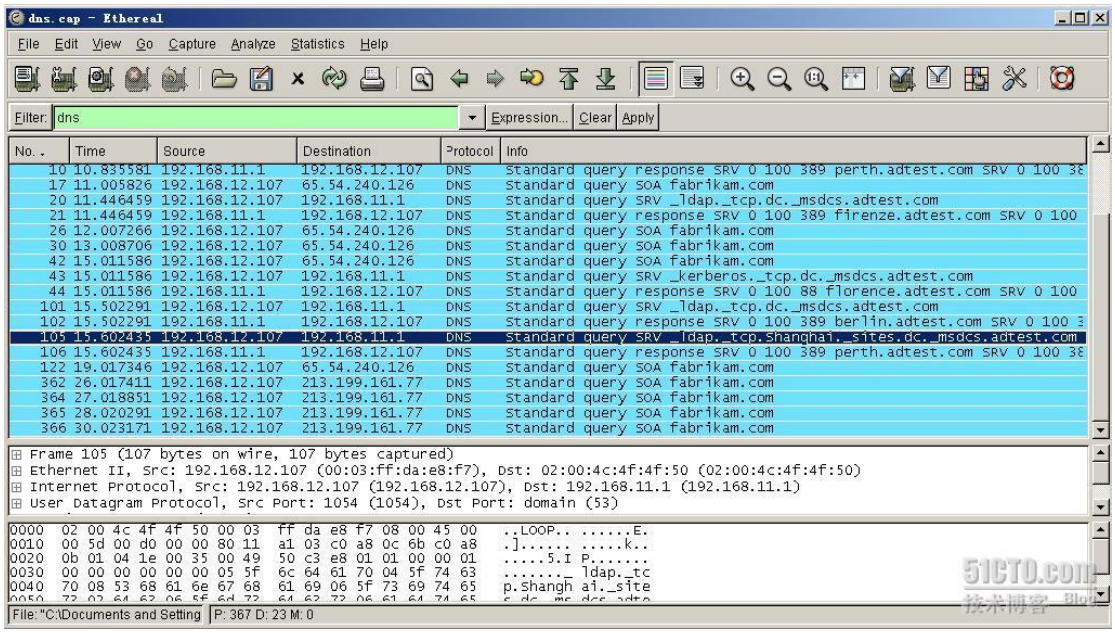
站点配置完毕后，我们检查 DNS 服务器，发现 DNS 中已经有了相关的 SRV 记录。如下图所示，我们发现 Beijing 和 Shanghai 两个站点的 SRV 记录已经出现在区域中了，这样的话有利于客户机通过查找 DNS 来定位出和自己所属站点内的域控

制器。



我们举个例子来说明 DNS 中和站点有关的 SRV 记录的作用，有一台客户机 Istanbul，IP 地址是 192.168.12.107。如下图所示，我们准备把它加入域，看看 Istanbul 加入域的过程。

我们用抓包器追踪 Istanbul 加入域的过程，如下图所示，我们可以看到 Istanbul 向 DNS 服务器发起查询，要求查询 shanghai 站点内的域控制器。显然 Istanbul 已经知道了自己属于 shanghai 站点,优先联系 shanghai 站点内的域控制器，这样我们设置站点的目的也就达到了。



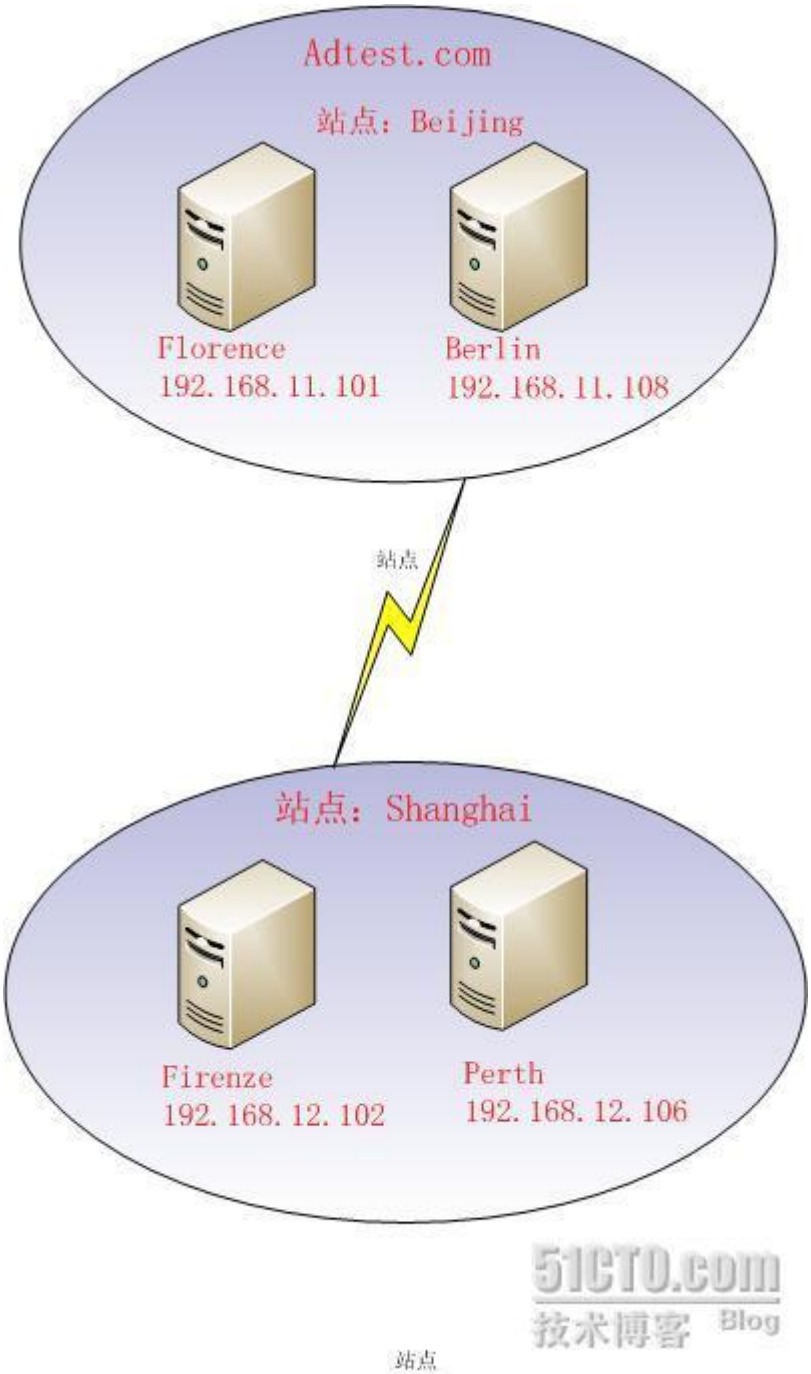
域控制器的常规卸载

我们现在已经有一些 Active Directory 的部署及管理经验了，今天我们要考虑一个问题，如果一个域控制器我们不需要了，那应该如何处理呢？直接把它砸了是不对的，这未免太暴力了，和当前的和谐环境有些格格不入哦。关键是，如果我们让这台域控制器直接消失，那么其他的域控制器就无法得知这个消息，每隔一段时间其他的域控制器还会试图和这个域控制器进行 AD 复制，客户机也有可能会把用户名和口令送到这个不存在的域控制器上进行验证。如果这个被暴力卸载的域控制器还承担着一些操作主机角色，我们就更麻烦了。因此，我们进行域控制器卸载时，一定要把工作做到位，优先使用常规卸载，争取不留后患。

有些朋友可能会说，我也希望用常规卸载，但有时就是不能正常卸载，没办法，只好…..我们要分析一下，为什么域控制器无法正常卸载呢？当域控制器进行常规卸载时，AD 的内容发生了变化，域控制器会把这个变化通知自己的复制伙伴，再由自己的复制伙伴通知其他域控制器。如果所有的域控制器都通知到了，那就肯定可以正常卸载，而且 DNS 记录，操作主机角色，AD 复制拓扑等问题都可以迎刃而解。因此，域控制器卸载和域控制器之间的 AD 复制其实是一个硬币的两面，域控制器卸载时也要进行 AD 复制。想知道一个域控制器是否可以正常

卸载，我们只要在 Active Directory 站点和服务中查看这个域控制器和它的复制伙伴是否可以 AD 复制就可以了，只要能进行 AD 复制，基本卸载域控制器时就没有问题。

我们举一个域控制器正常卸载的例子，拓扑如下图所示，我们准备卸载 shanghai 站点内的域控制器 perth。从拓扑可以看出，perth 的复制伙伴应该是 Firenze，只要 perth 和 Firenze 之间可以进行 AD 复制，perth 应该就可以进行域控制器卸载。



在 perth 上运行 Dcpromo，如下图所示，出现 Active Directory 安装向导，向导判断我们准备把 Active Directory 删除，点击“下一步”继续。

由于 perth 并不是域内的最后一个域控制器，因此我们不能勾选“这个服务器是域中的最后一个域控制器”。

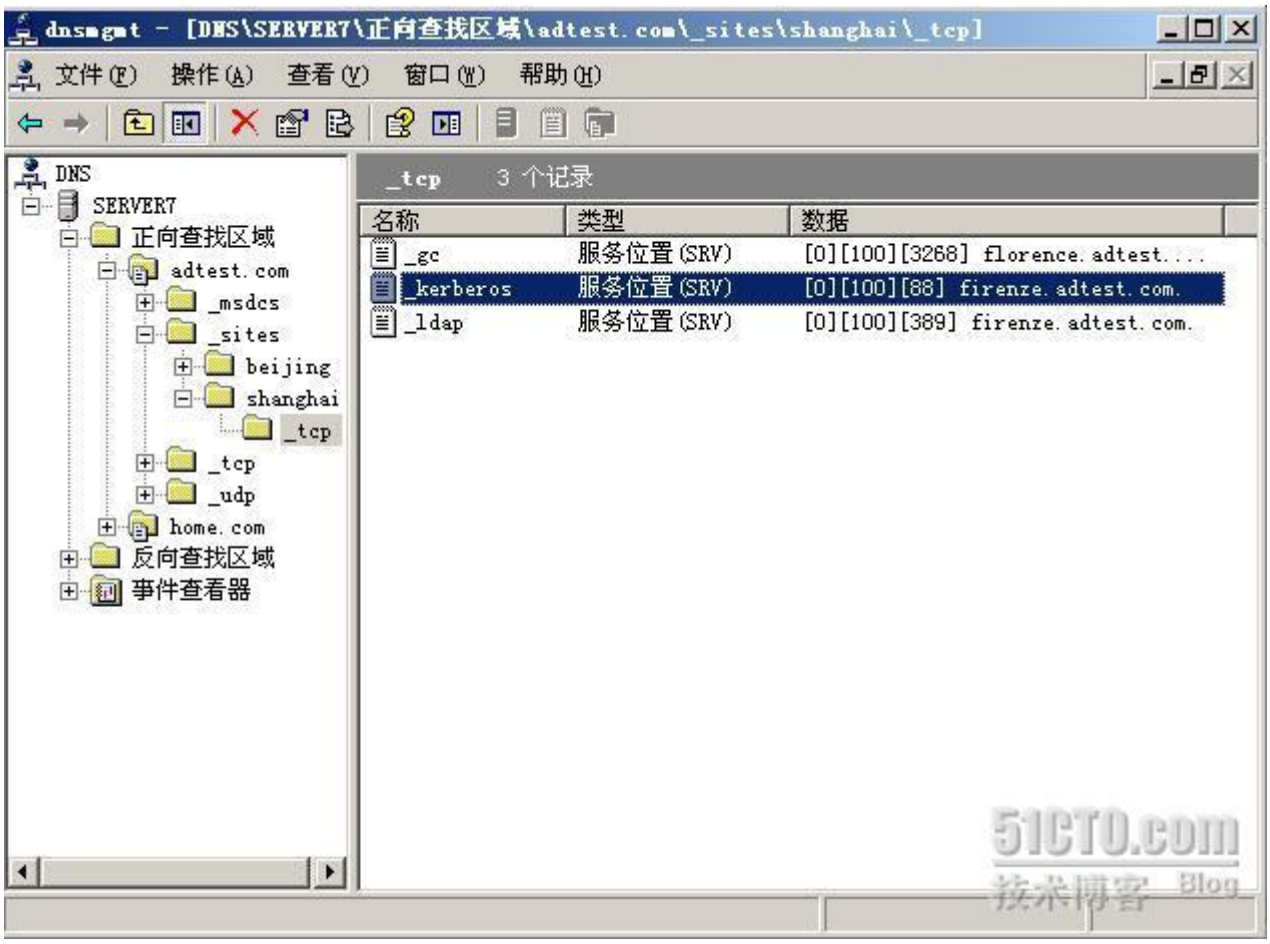
Perth 删除 Active Directory 后，需要我们设置本地管理员口令。

当 perth 上的 Active Directory 被删除后，perth 将成为一个成员服务器。

Perth 开始了卸载域控制器的操作，注意下图，perth 把 AD 的变化复制给了 Firenze，这和我们事先的分析是吻合的。

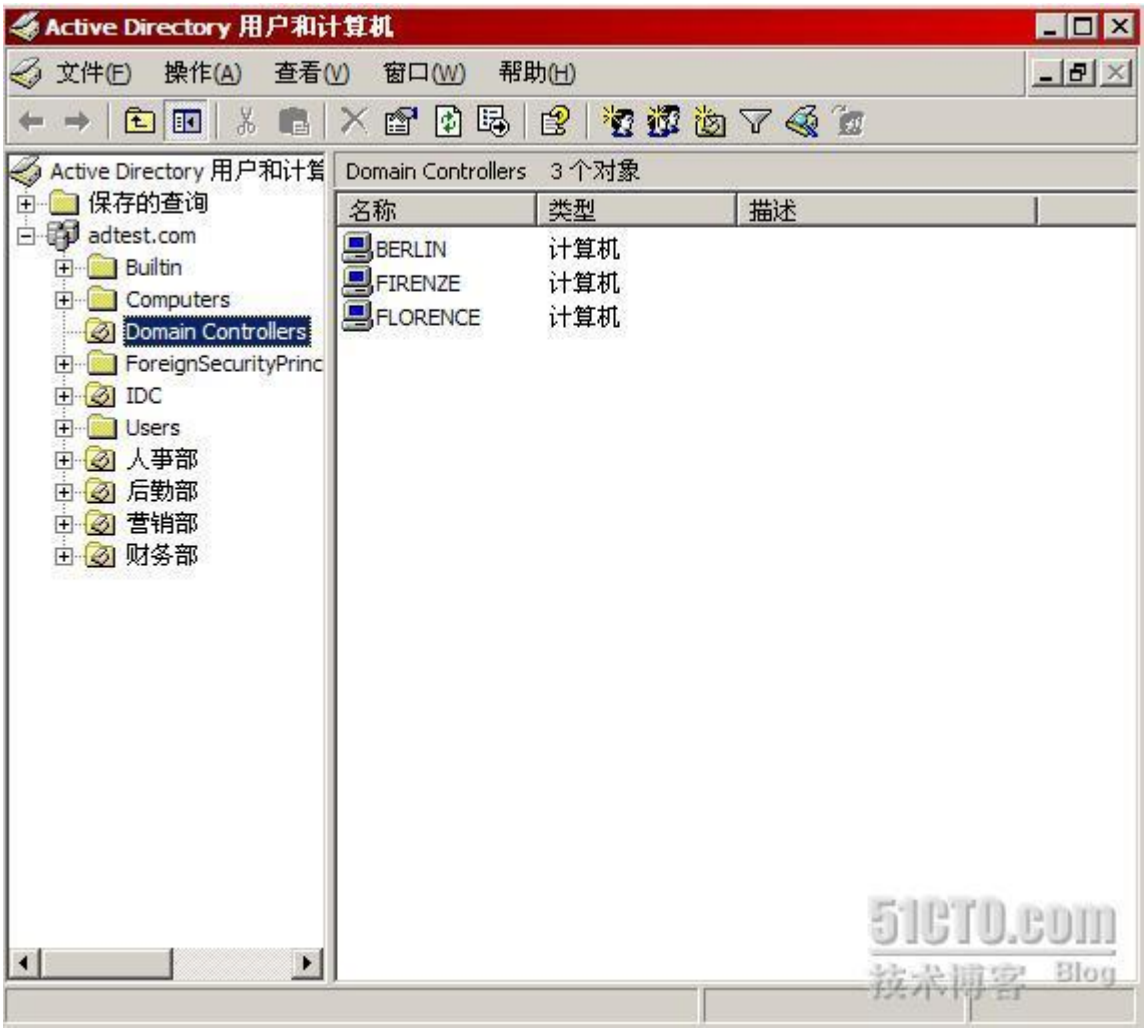
OK，perth 成功地完成了域控制器的卸载，删除了 Active Directory。

Perth 进行域控制器的卸载后，我们观察一下 DNS 服务器，如下图所示，我们发现 DNS 已经把 shanghai 站点的 SRV 记录自动更



如下图所示，shanghai 站点内的 Firenze 也把自己的复制伙伴从 Perth 改成了 Berlin。

域控制器的数量也发生了变化，Perth 已经不再是域控制器的一员。



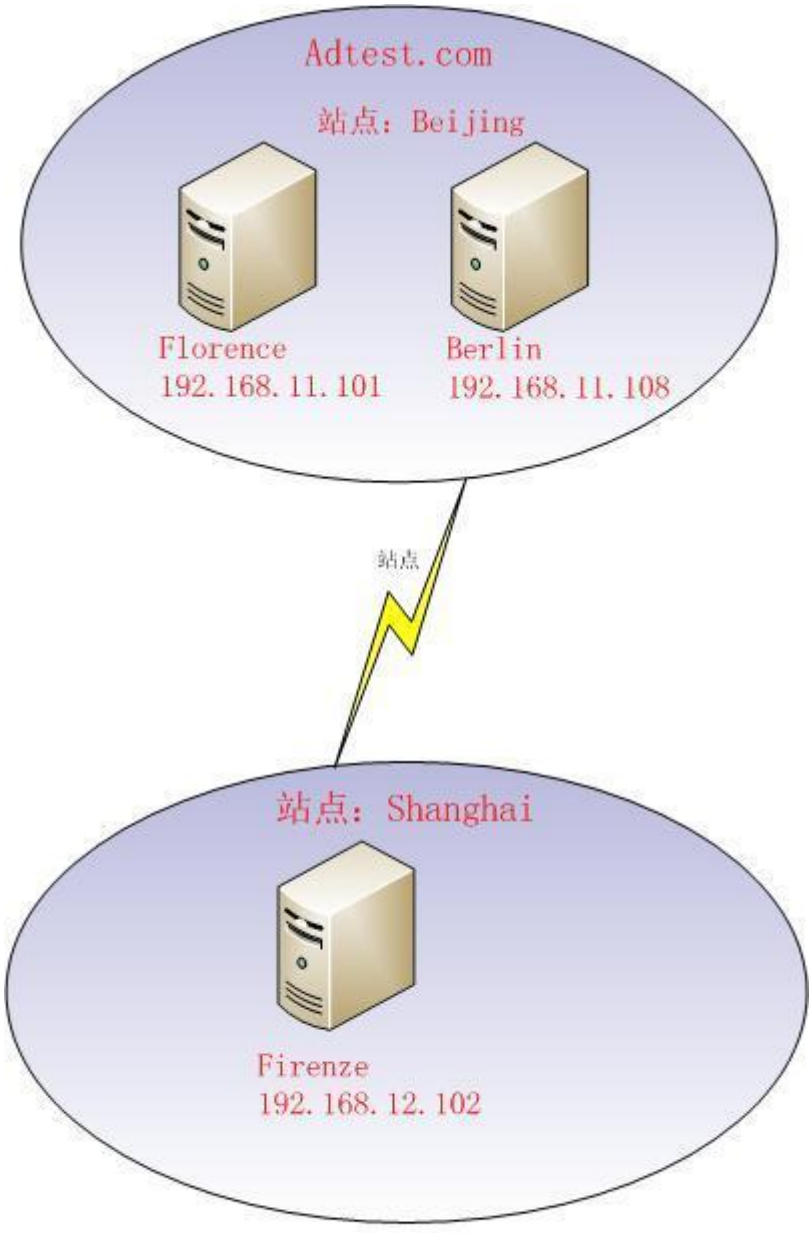
这样我们就在 Perth 上完成了域控制器的常规卸载，这种卸载方式是我们的首选方法。当然，如果实在无法正常卸载，我们也要想想其他办法，下篇博文中我们将介绍如何进行域控制器的强制卸载。

域控制器的强制卸载

上篇博文中我们介绍了如何对域控制器进行常规卸载，本文中我们将介绍如何对域控制器进行强制卸载。为什么需要对域控制器进行强制卸载呢？如果域控制器不能和复制伙伴正常通讯，而且更正无望，那我们就要考虑进行强制卸载了。例如我曾见过一个单位有 10 个域控制器，居然有 7 个不能相互复制，主要是管理员误以为域控制器越多越好....类似这样的情况，我们就可以果断出手，把域控

制器强行卸载掉。域控制器强行卸载的原理也很简单，那就是卸载时不再通知复制伙伴，直接把 AD 删除就好。这样的卸载方式是要相对简单一些，但其实后续的操作很麻烦，例如我们需要在 Active Directory 中手工清除被强制卸载的域控制器，手工清除 DNS 中的 SRV 记录等。因此，如果不是万不得已，还是用常规卸载比较好。

如下图所示，我们将利用如下图所示的拓扑为大家演示如何进行域控制器的强制卸载，我们进行强制卸载的目标是 shanghai 站点的 Firenze。



站点

一 强制卸载域控制器

首先我们在被卸载的域控制器 Firenze 上打开 cmd 命令提示符，执行 dcpromo/forceremoval，forceremoval 参数的作用就是执行强制卸载，如下图所示，卸载向导提示我们这种卸载方式将不对其他域控制器的 Active Directory 数据进行更新。

接下来我们需要设置 Firenze 本地管理员的口令。

强制卸载域控制器后，Firenze 将不再成为域内的成员服务器，而是会从域中脱离出去成为工作组中的独立服务器。

如下图所示，点击完成结束了域控制器的强制卸载。

二 手工清除 Active Directory 数据

Firenze 被强制卸载后，域内的其他域控制器并不知道这件事情，它们仍然认

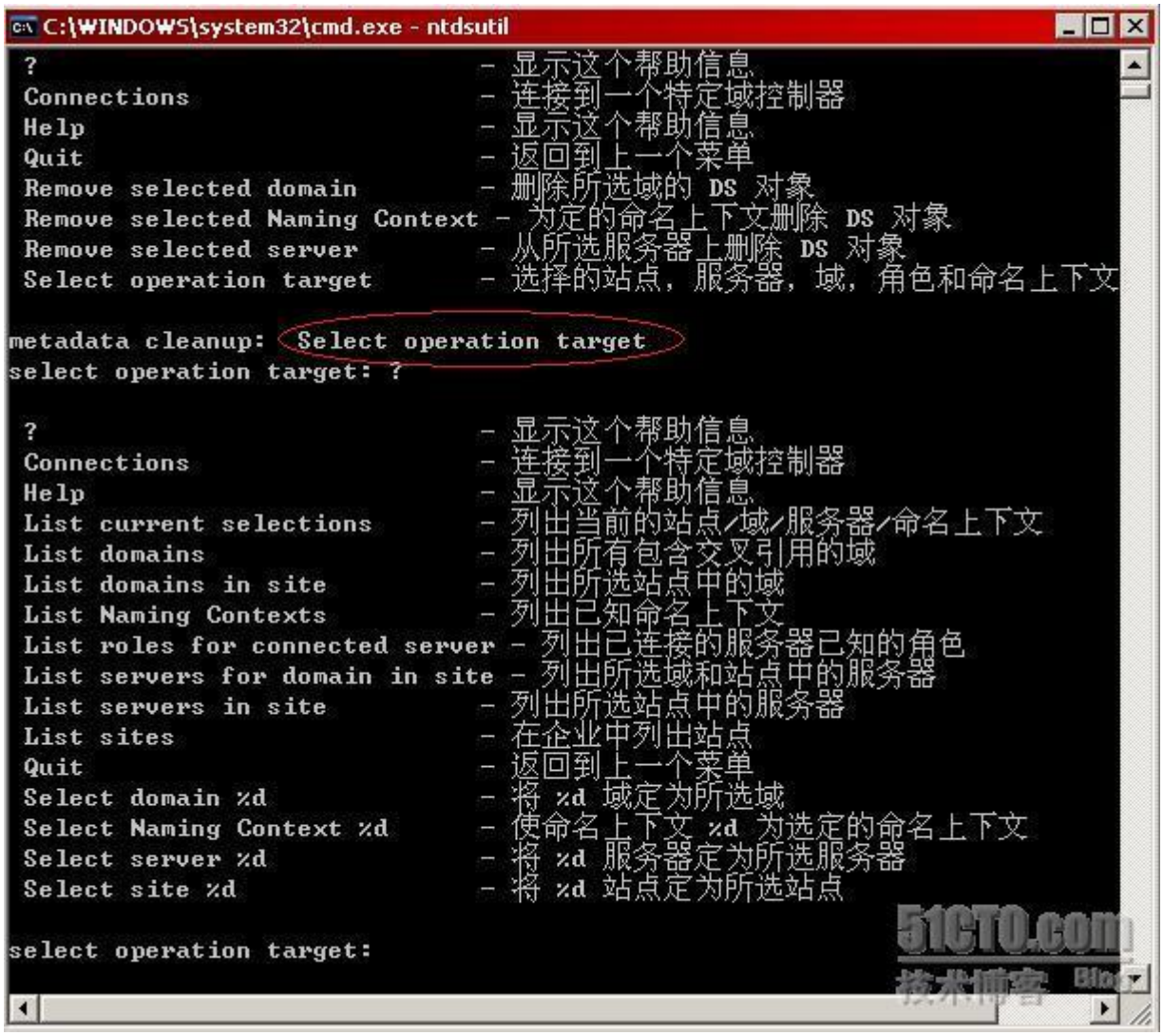
为 Firenze

是域控制器的一员，因此我们必须手工将 Firenze 从 Active Directory 中清除出去。我们准备在 Berlin 上对 Active Directory 进行手工清理，然后 Berlin 再把清理后的 Active Directory 复制到其他域控制器就可以了。

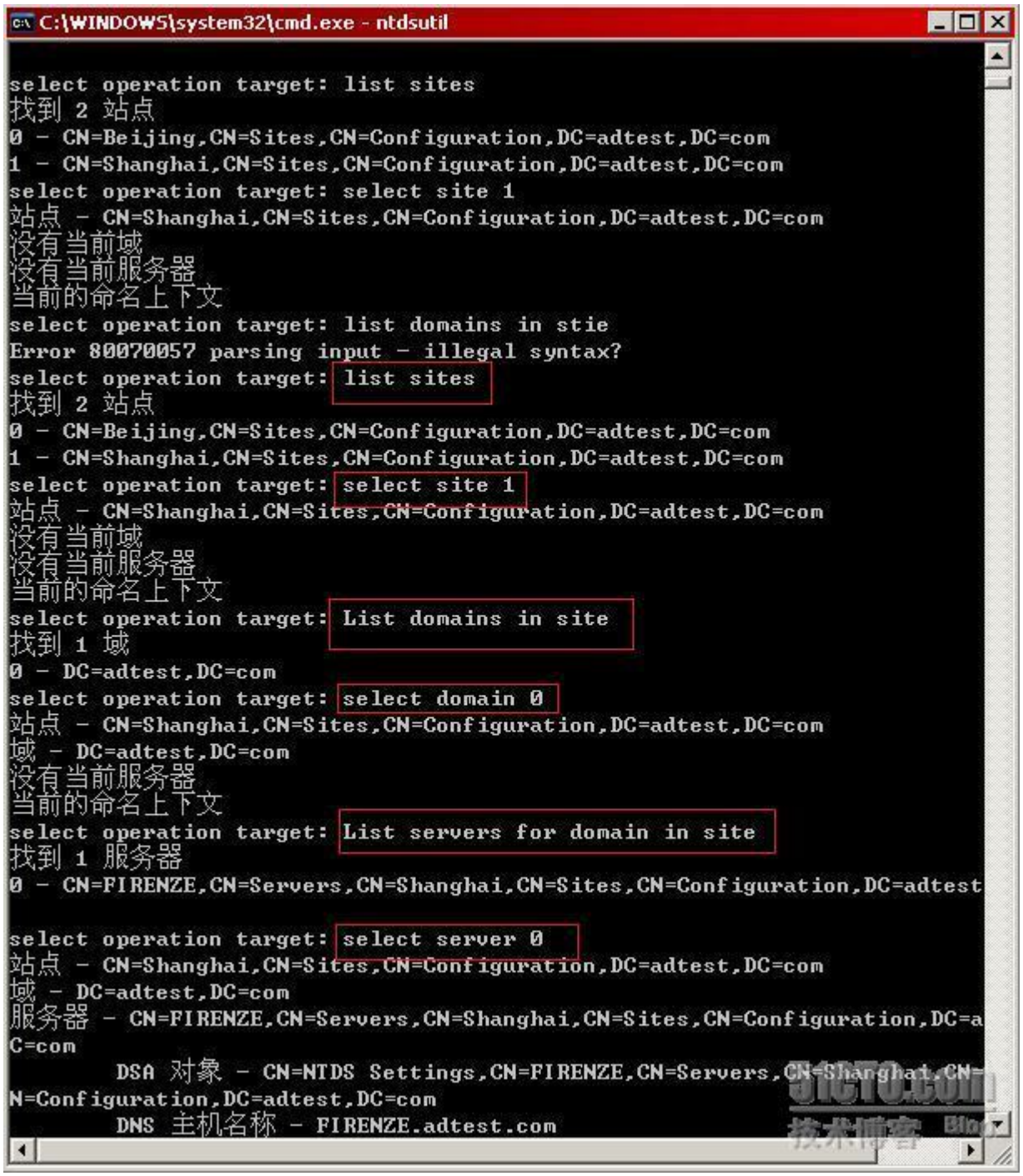
在 Berlin 上运行 NTDSUTIL，如下图所示，选择“Metadata Cleanup”，准备清除不使用的服务器对象。

然后使用“connections”准备连接到指定的域控制器执行删除操作，输入“connect to server berlin”连接到 Berlin，然后输入“quit”返回上级菜单。

接下来我们需要使用“Select operation target”来选择被删除的服务器对象，选择服务器时，我们需要指定服务器所在的域和站点。我们可以先用 list 指令列出站点和域，然后再进行选择。Firenze 隶属于 shanghai 站点，Firenze 所在的域是 adtest.com。



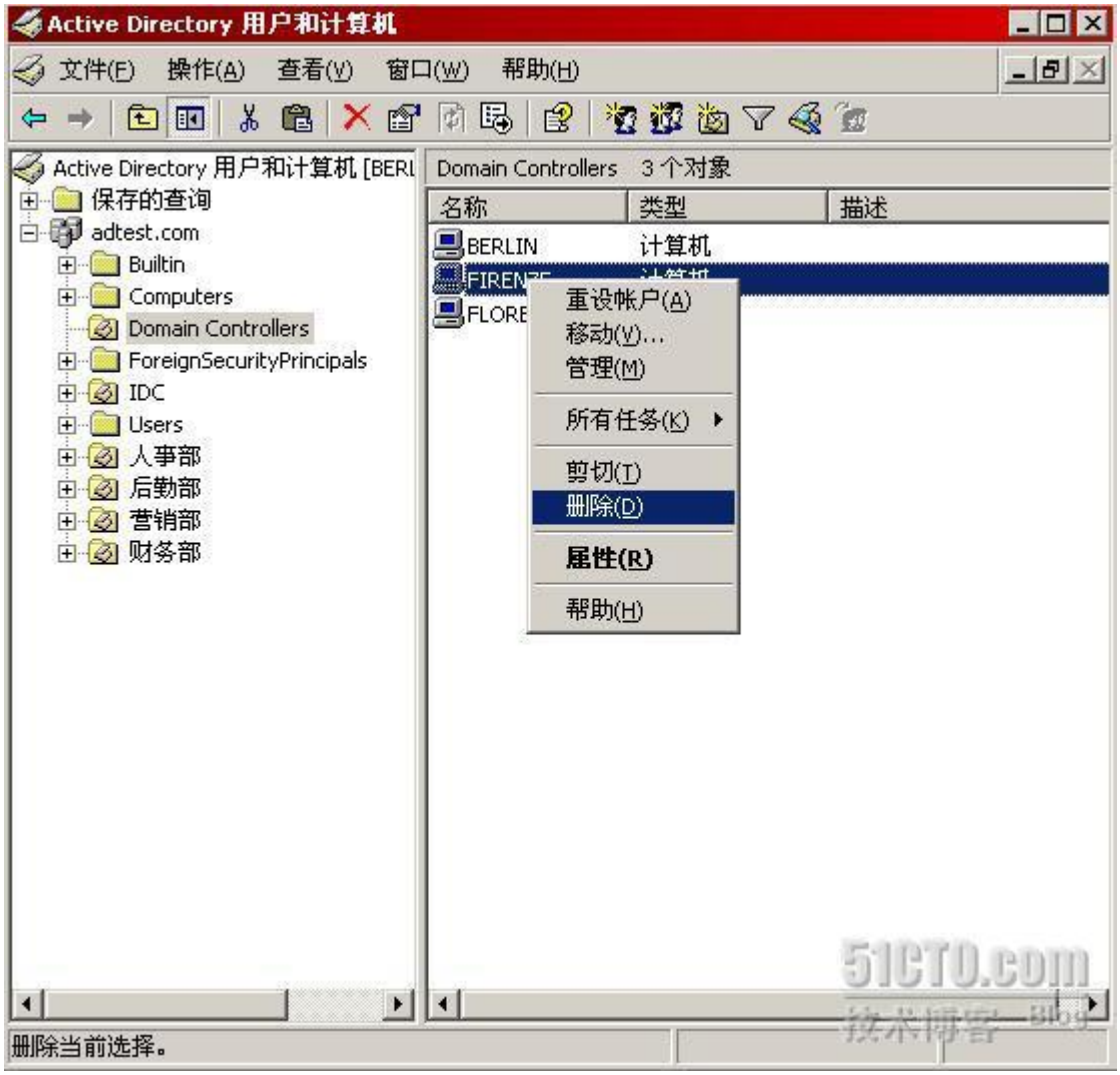
如下图所示，我们首先用“list sites”列出了当前站点，然后用“select site 1”选定了 shanghai 站点，我们可以看到对站点的描述用的是数字而不是字符。选择了站点之后，我们接下来使用“list domains in site”列出了站点中的域，当前只有一个域 adtest.com，编号是 0，因此我们接下来使用“select domain 0”就可以把域也选定了。域和站点都选定了，我们就可以进行服务器的选择了，使用“list servers for domain in site”可以列出所有的服务器，当前 shanghai 站点只有 Firenze 一个域控制器，因此我们使用“select server 0”选定服务器 Firenze。至此，被手工清理的目标已被我们锁定了。



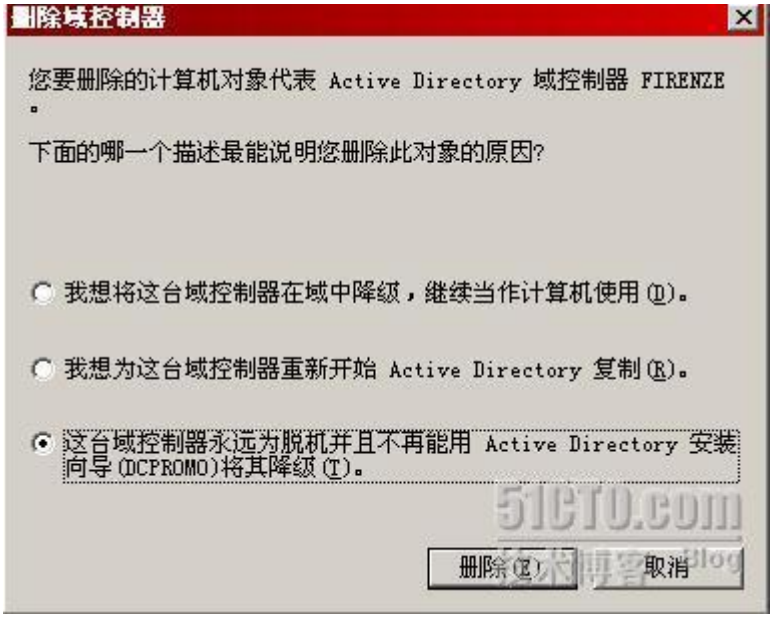
用“quit”命令退出选择操作对象的环境，返回到上级菜单，然后我们使用“Remove selected Server”删除被选定的服务器对象 Firenze。

NTDSUTIL 提示我们对删除 Firenze 服务器的行为进行确认，我们选择“Y”确定操作。

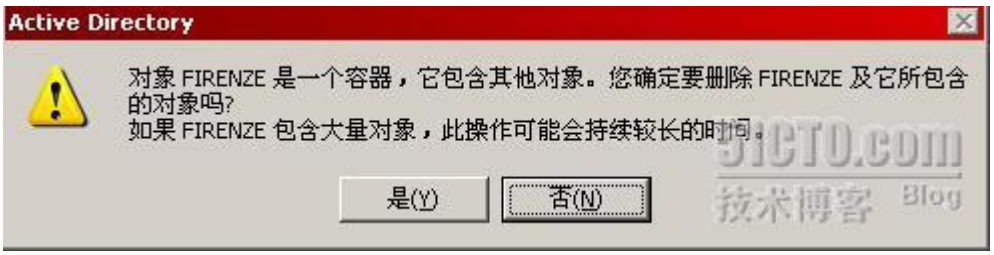
这样 Firenze 被我们从 Berlin 的 Active Directory 中清除了，然后我们在 Berlin 上打开 Active Directory 用户和计算机，如下图所示，删除域控制器 Firenze。



我们需要对删除 Firenze 的原因进行描述，如下图所示，它是被我们强制卸载的。



确定要进行删除 Firenze 的操作，选择“Y“。



至此，我们在 Berlin 上基本完成了对 Firenze 的手工清除，完成操作后还需要注意以下几点：

1. **手工清除 DNS 中 Firenze 的 SRV 记录**
2. **如果 Firenze 承担了操作主机角色，把操作主机角色转移到其他域控制器**
3. **如果 Firenze 是全局编录服务器，选择其他的域控制器负责全局编录**
4. **把 Berlin 的 Active Directory 复制到其他域控制器上**

综上所述，我们发现其实对域控制器进行强制卸载是很麻烦的事，我们不应该把它当成一种常态行为，只有当域控制器确实没有希望进行常规卸载时，我们才考虑使用强制卸载，而且使用强制卸载后一定要注意后续对 Active Directory 的手工清理！

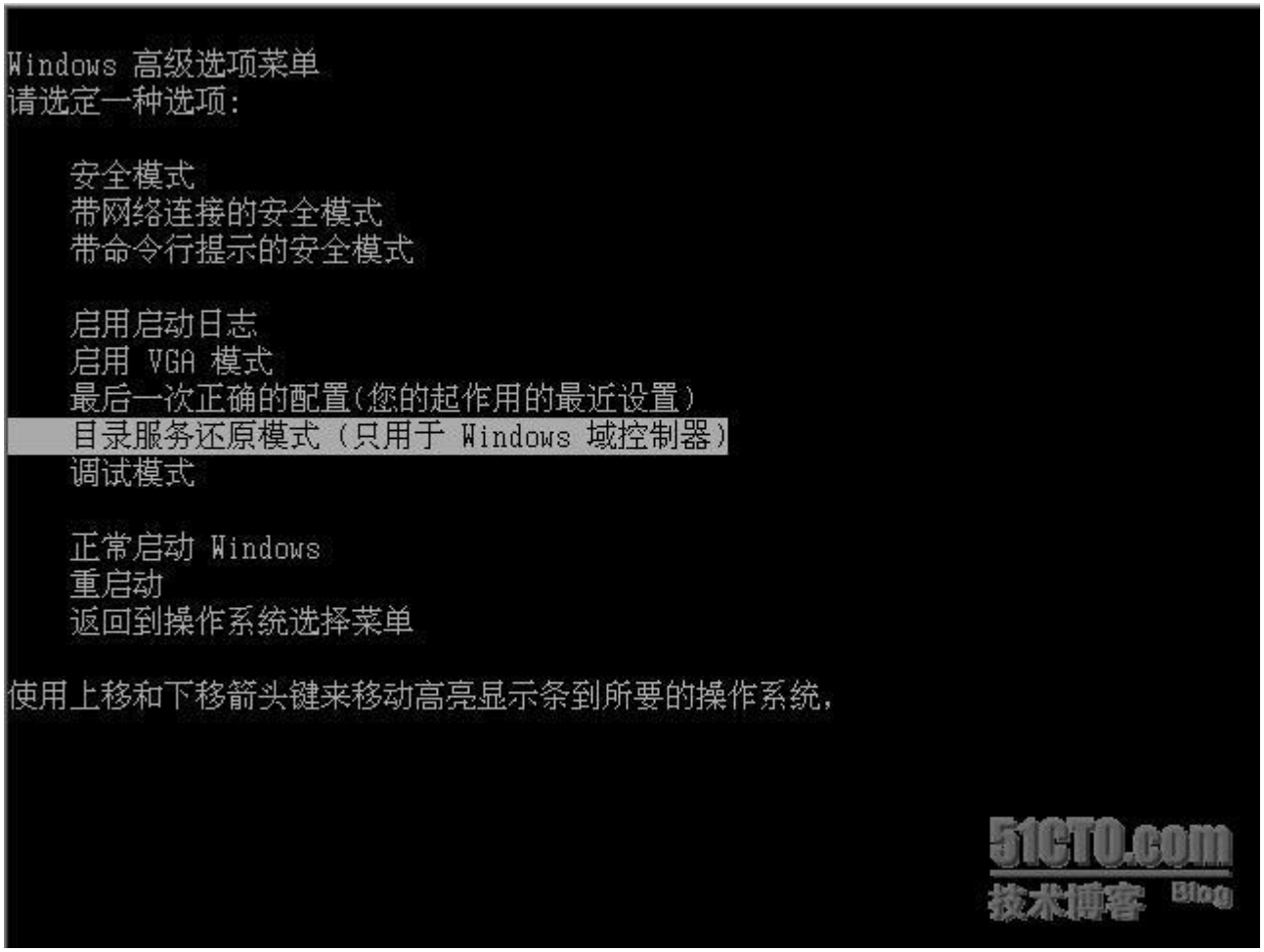
域控制器的终极卸载

在上篇博文中，我们介绍了用 Dcpromo/Forceremoval 对域控制器进行强行卸载。一般情况下，用这种强制卸载方法基本可以解决问题。但如果有些域控制器的 Active Directory 损坏严重，严重到了无法对 Active Directory 进行初始化，以致于无法登录操作系统。这种情况下我们就要犯愁了，Dcpromo/forceremoval 需要登录系统后才能执行，现在系统无法正常登录，那该如何是好呢？别着急，本文将为大家介绍另外一种卸载 Active Directory 的方法，这种方法将更加麻烦，更加血腥，更加暴力，更加强大.....

这种强制卸载方法的思路是先进入目录服务还原模式，这样就可以避开损坏的 Active Directory，以安全模式进入系统。然后通过修改注册表强行将域控制器

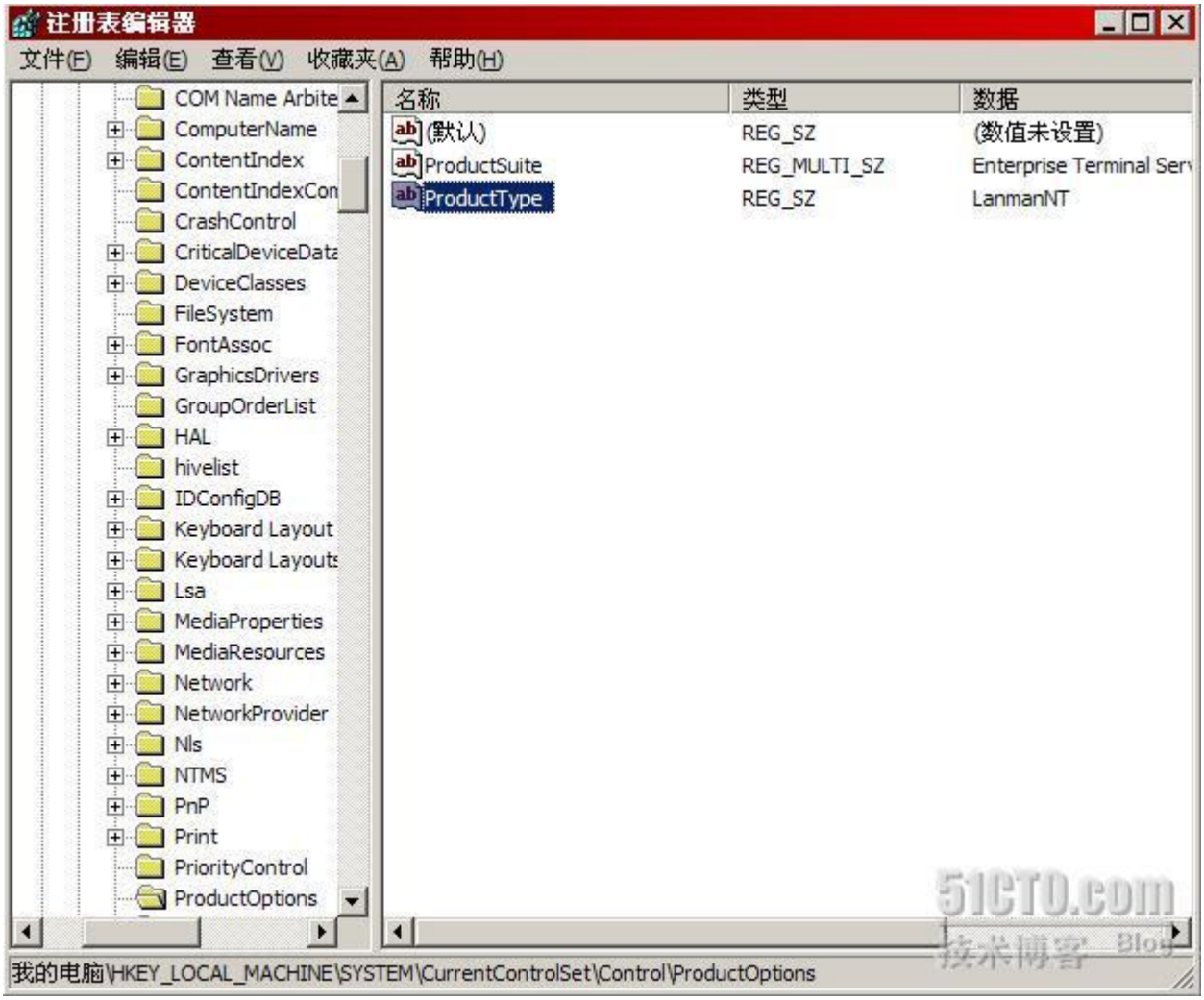
改为独立服务器，最后再手工删除 Active Directory 数据库。这样做完后从形式上看域控制器就变成一个成员服务器了，只是系统中还保留了一些域控制器使用的服务和注册表键值。如果希望做得更完善一些，可以临时把这台计算机升级为一个域的域控制器，升级完成后立即进行域控制器的卸载，这样一番复杂操作后基本上可以保证卸载效果和运行 Dcpromo/forceremoval 大致相当。

我们以 Florence 为例为大家演示操作过程。Florence 是 ITET.COM 的域控制器，由于 Active Directory 损坏无法进入系统，我们首先要使用目录服务还原模式进入系统，在系统启动时我们按下 F8，如下图所示，选择进入“目录服务还原模式”。

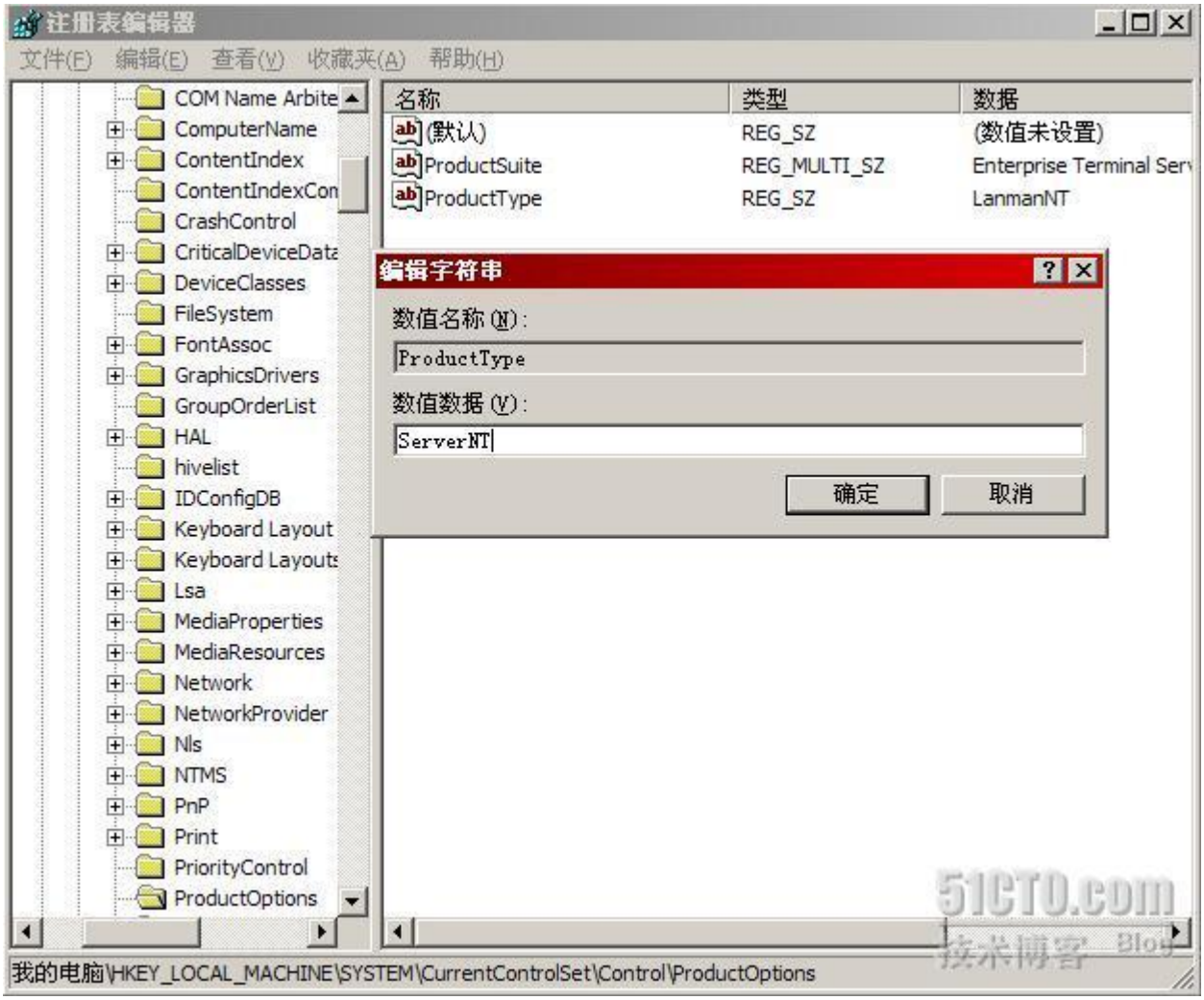


目录服务还原模式不加载 Active Directory，因此可以避开损坏的 Active Directory 所带来的问题，如下图所示，我们通过目录服务还原模式可以顺利进入系统。

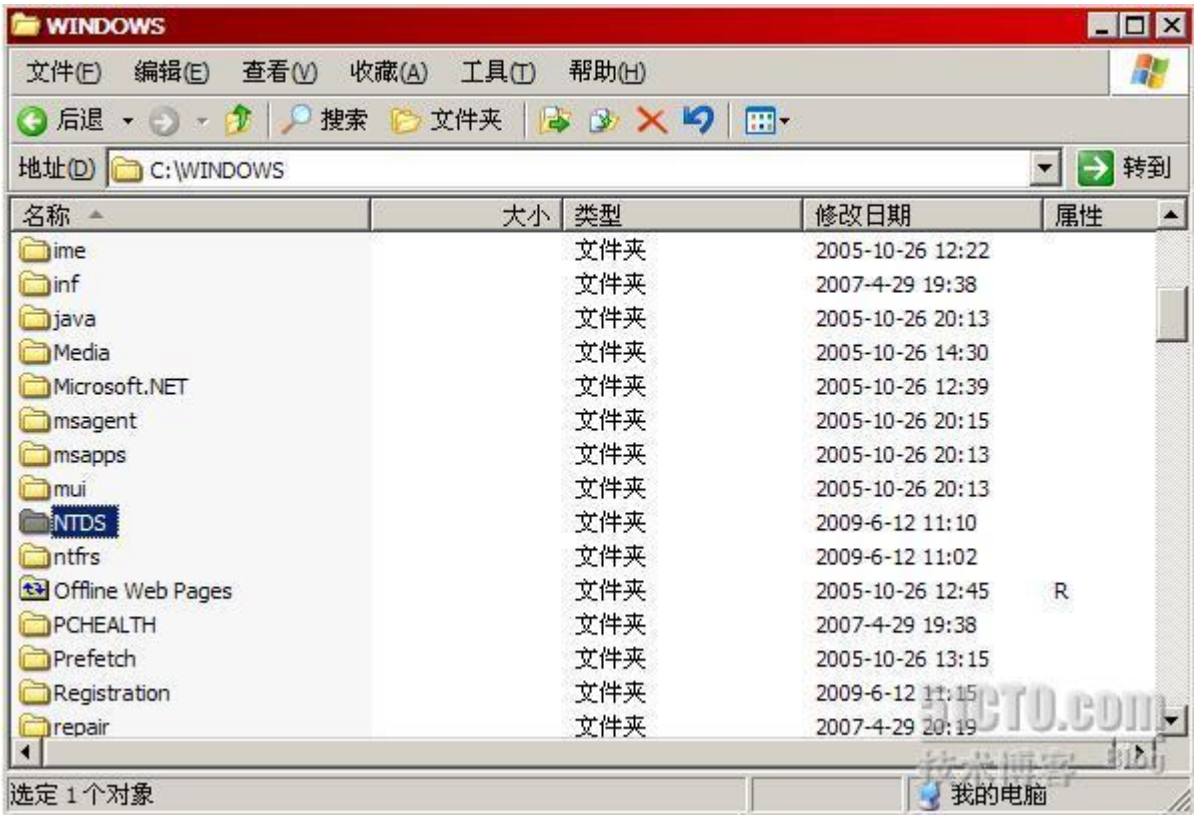
登录进入系统后，我们要通过修改注册表键值把域控制器强行变为独立服务器，运行 Regedit，如下图所示，定位到 HKEY_Local_Machine\System\CurrentControlSet\Control\Productoptions\ProductType，这个键值决定了服务器的身份。



如下图所示，我们把 ProductType 的键值从 LanmanNT 改为 ServerNT，这样我们就强行把 Florence 设置为一个和 Active Directory 无关的独立服务器了。



改完键值后，我们需要手工删除 Active Directory 数据，Active Directory 数据的默认路径是 C:\Windows\NTDS。如下图所示，我们在目录服务还原模式下直接删除 NTDS 目录即可。



修改完注册表键值，然后删除 NTDS 目录后重启 Florence。如下图所示，我们发现 Florence 已经认为自己不是一个域控制器了！我们可以轻松进入变形后的系统。

如果强行卸载到此为止，那 Florence 还是有很多隐患的，因为 Florence 上还有不少服务以及注册表键值和 Active Directory 有关。怎么才能消除这些隐患呢？

我们的方法是把 Florence 临时升级为一个域的域控制器，然后再降下来，这样就可以把相关的注册表及服务清理干净。如下图所示，我们把 Florence 升级为 test.com 的域控制器。

升域完成后，我们立即把 Florence 降下来，如下图所示，我们通过 Dcpromo 对 Florence 进行正常卸载，卸载完成后 Florence 就可以恢复正常了。

以上做了那么多操作，其实效果相当于执行了 Dcpromo/Forceremoval。虽然过程很麻烦，但我们从中又多掌握了一种应急修复方法，下次遇到 Active Directory 损坏无法启动，我们就不用担心了。

理解域信任关系

在同一个域内，成员服务器根据 Active Directory 中的用户账号，可以很容易地把资源分配给域内的用户。但一个域的作用范围毕竟有限，有些企业会用到多个域，那么在多域环境下，我们该如何进行资源的跨域分配呢？也就是说，我们该如何把 A 域的资源分配给 B 域的用户呢？一般来说，我们有两种选择，一种是使用镜像账户。也就是说，我们可以在 A 域和 B 域内各自创建一个用户名和口令都完全相同的用户账户，然后在 B 域把资源分配给这个账户后，A 域内的镜像账户就可以访问 B 域内的资源了。

镜像账户的方法显然不是一个好的选择，至少账户的重复建设就很让管理员头疼。资源跨域分配的主流方法还是创建域信任关系，在两个域之间创建了信任关系后，资源的跨域分配就非常容易了。域信任关系是有方向性的，如果 A 域信任 B 域，那么 A 域的资源可以分配给 B 域的用户；但 B 域的资源并不能分配给 A 域的用户，如果想达到这个目的，需要让 B 域信任 A 域才可以。

如果 A 域信任了 B 域，那么 A 域的域控制器将把 B 域的用户账号复制到自己的 Active Directory 中，这样 A 域内的资源就可以分配给 B 域的用户了。从这个过程来看，A 域信任 B 域首先需要征得 B 域的同意，因为 A 域信任 B 域需要先从 B 域索取资源。这点和我们习惯性的理解不同，信任关系的主动权掌握在被信任域手中而不是信任域。

A 域信任 B 域，意味着 A 域的资源有分配给 B 域用户的可能性，但并非必然性！如果不进行资源分配，B 域的用户无法获得任何资源！有些朋友误以为只要两个域之间存在信任关系，被信任域的用户就一定可以无条件地获得信任域内的所有资源，这个理解是错误的。我刚工作时在一家港资企业担任网络管理工作，企业的香港公司是一个域，深圳公司也是一个域。有一次我们需要把两家公司的 Exchange 服务器进行站点连接，这个操作需要两个域建立信任关系，但

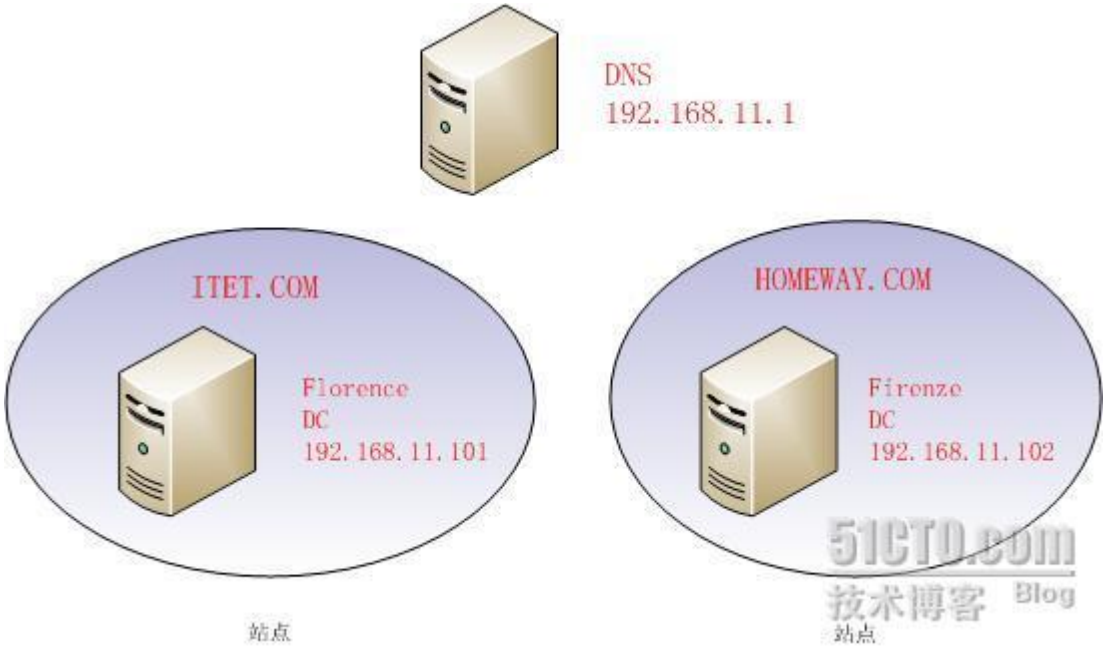
当时一位老工程师坚决不同意建立信任关系。他的理由是只要建立信任关系，香港公司的资料就全被深圳公司的员工看到了。这个理由很山寨，很明显对域信任关系的理解有些是是而非。我通过一个实验纠正了他的错误概念，事实证明，深圳公司和香港公司建立了域信任关系后，安全性并没有因此降低。

在 NT4 的域时代，信任关系是不具有传递性的。也就是说如果 A 域信任 B 域，B 域信任 C 域，那么 A 域和 C 域没有任何关系。如果信任关系有传递性，那么我们就可以推导出 A 域是信任 C 域的。信任关系没有传递性极大地降低了灵活性，你可以想象一下如果 70 个域都要建立完全信任关系，那么需要多么大的工作量。而且这种牺牲灵活性的做法也没有获得安全上的补偿，因此微软在 Win 2000 发布时，允许在域树和域林内进行信任关系的传递，在 Win2003 中更是允许在域林之间进行信任关系的传递。

下篇博文中我们将通过一个实例为大家介绍如何进行信任关系的创建，敬请期待。

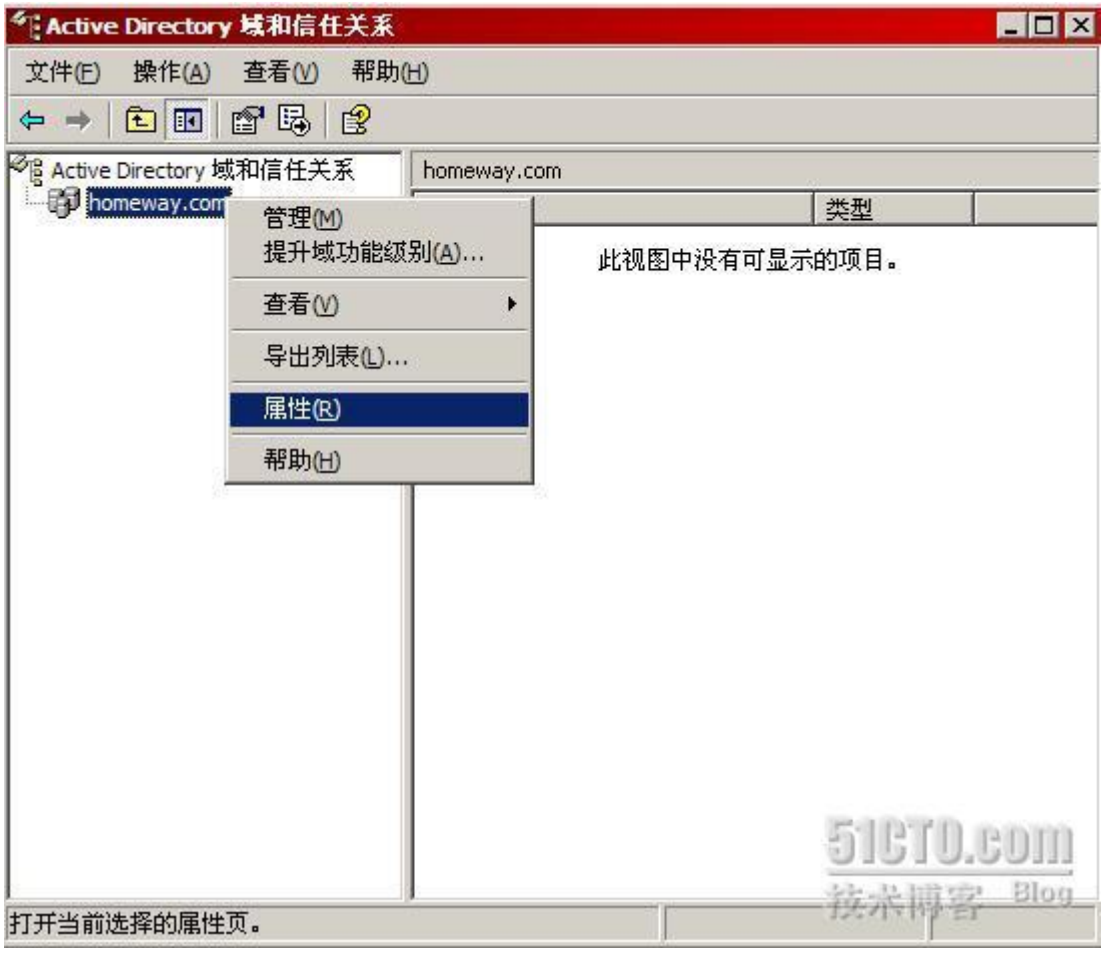
实战详解域信任关系

上篇博文中我们对域信任关系作了一下概述，本文中我们将通过一个实例为大家介绍如何创建域信任关系。拓扑如下图所示，当前网络中有两个域，一个域是 ITET.COM，另一个域是 HOMEWAY.COM。两个域内各有一个域控制器，分别是 Florence 和 Firenze，我们让两个域使用了同一个 DNS 服务器。

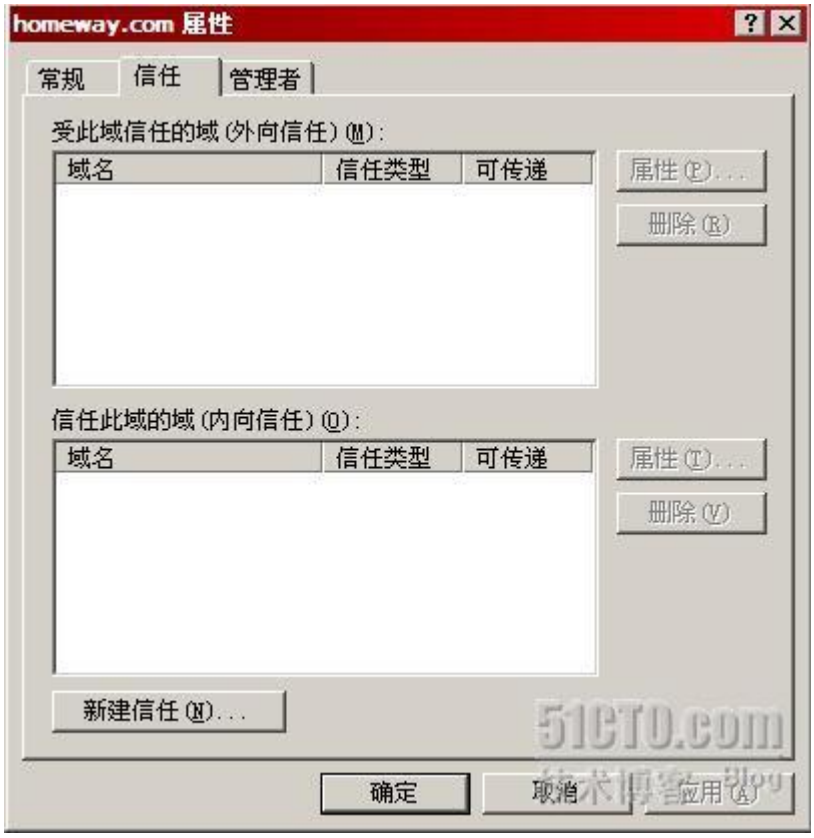


创建域信任关系要注意 DNS 服务器的设置，因为 DNS 服务器要负责定位域控制器，关键之处在于域控制器使用的 DNS 服务器要能够把两个域的域控制器都定位出来。我们在实验中规划让两个域使用同一个 DNS 服务器，显然是出于这个考虑。如果两个域都使用域控制器作 DNS，那么要使用辅助区域，转发器等技术才能保证 DNS 服务器可以把两个域的域控制器都解析出来。如下图所示，我们可以看到两个域的区域数据都在同一个 DNS 服务器上。

我们准备构建一个单向信任关系，让 ITET.COM 域信任 HOMEWAY.COM 域，根据之前的分析，ITET 想信任 HOMEWAY，必须征得被信任域的同意，因此我们先在 HOMEWAY.COM 域上进行操作。在 HOMEWAY.COM 的域控制器 Firenze 上打开管理工作中的域和信任关系，如下图所示，右键点击 HOMEWAY.COM 域，选择“属性”。



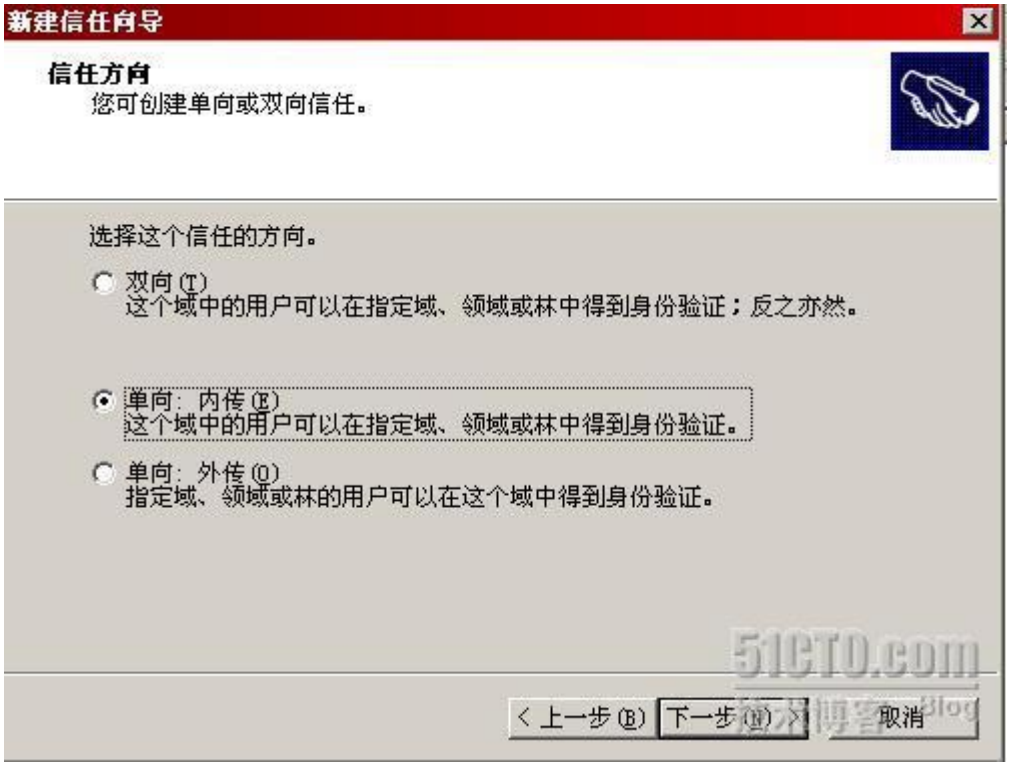
在域的属性中切换到信任标签，如下图所示，点击“新建信任”。



如下图所示，出现信任信任向导，点击“下一步”继续。

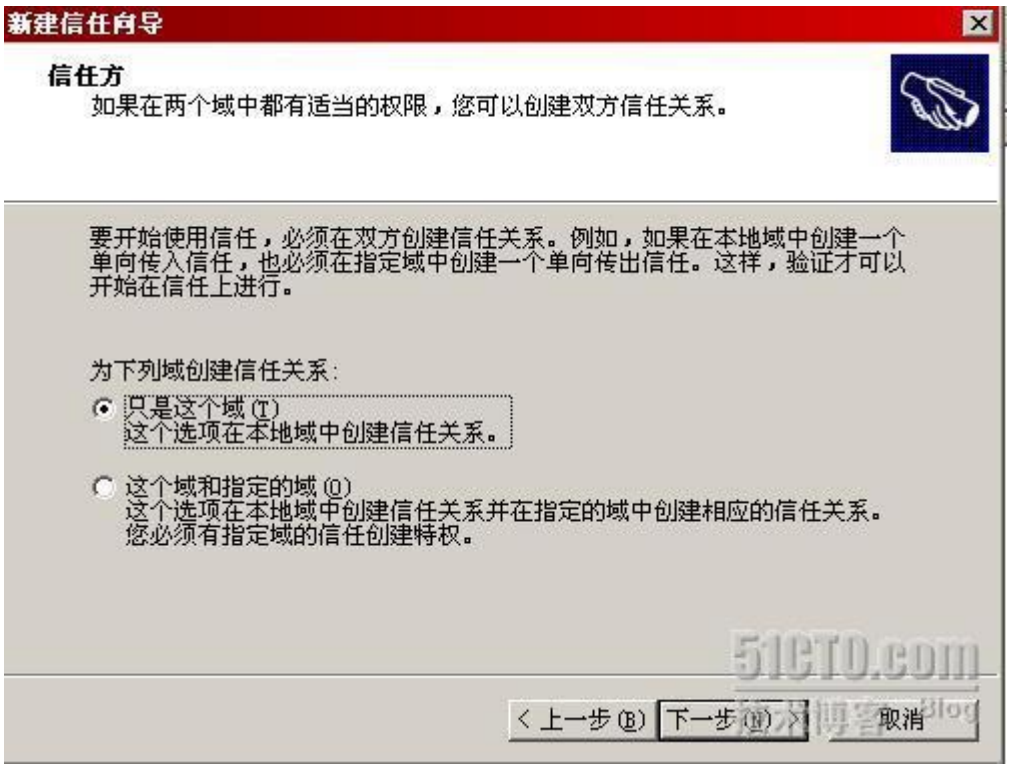
输入有信任关系域的名称，如下图所示，我们输入域名为 ITET.COM。

选择信任方向，内传指的是被其他域信任，外传则是信任其他域。由于 ITET.COM 信任 HOMEWAY.COM，因此 Firenze 的信任方向应该选择单向内传。



接下来我们要选择是在两个域控制器上分别设置信任关系还是同时设置信任关

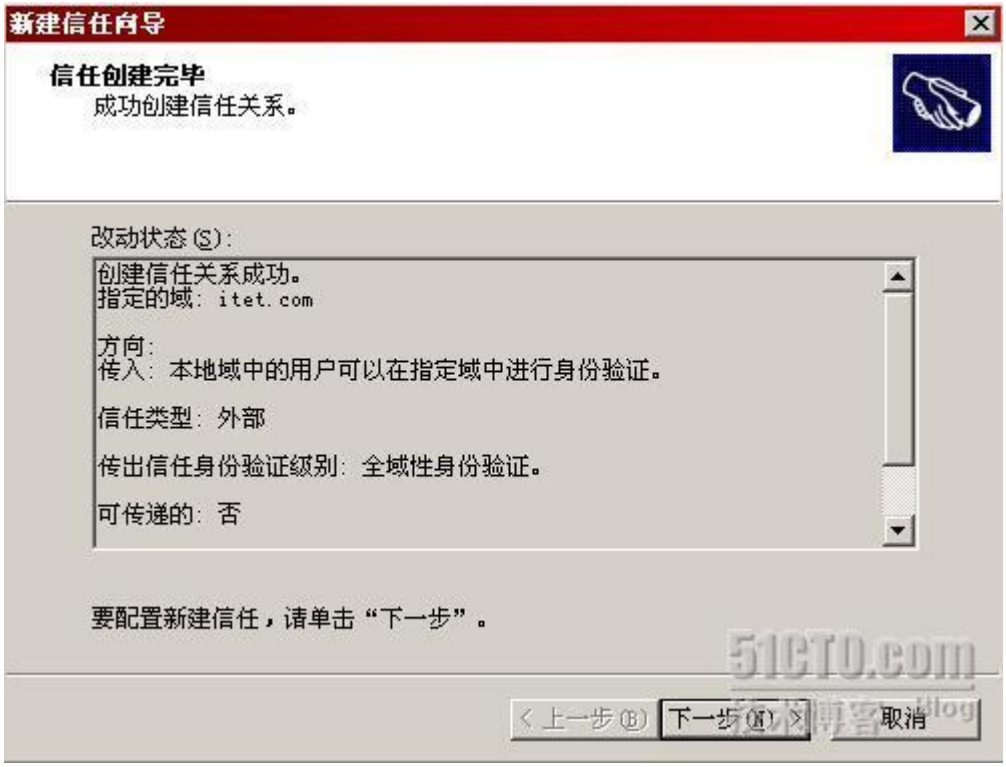
系，为了更清晰地展示这个过程，我们选择在两个域控制器上分别进行信任关系的设置。如果对域信任关系已经熟练掌握，完全可以选择在两个域控制器上同时进行操作。



如下图所示，为了保证不被其他域恶意信任，HOMEWAY.COM 设置了一个信任口令，只有信任域能回答出这个口令，信任关系才可以建立。

如下图所示，信任向导已经做好准备，点击下一步继续。

信任关系已经创建成功，HOMEWAY.COM 已经允许 ITET.COM 信任自己了。



接下来要选择是否确认传入信任关系，由于我们还没有在 ITET.COM 域中进行设置，因此我们先选择“否，不确认传入信任”。

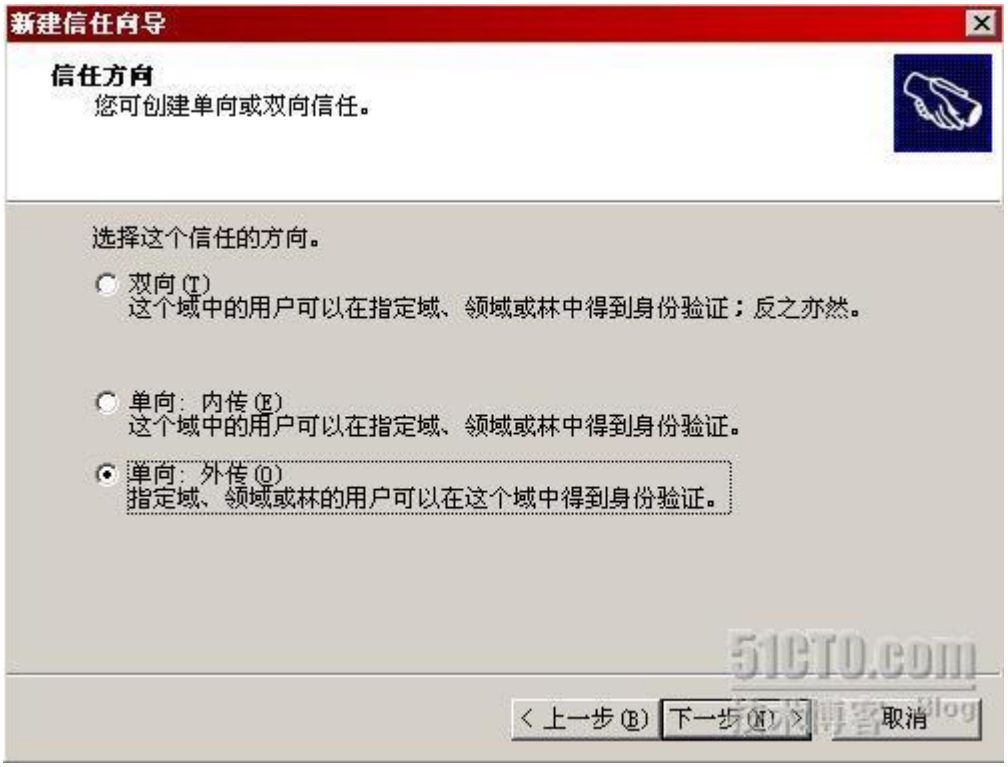
如下图所示，信任关系创建成功，点击完成结束 HOMEWAY.COM 域的设置工作。

HOMEWAY.COM 允许被 ITET.COM 信任后，我们接下来就可以在 ITET.COM 的域控制器 Florence 上设置信任关系，让 ITET.COM 主动信任 HOMEWAY.COM。我们在 Florence 的管理工具中打开域和信任关系，在域的属性中切换到信任标签，如下图所示，点击“新建信任”。

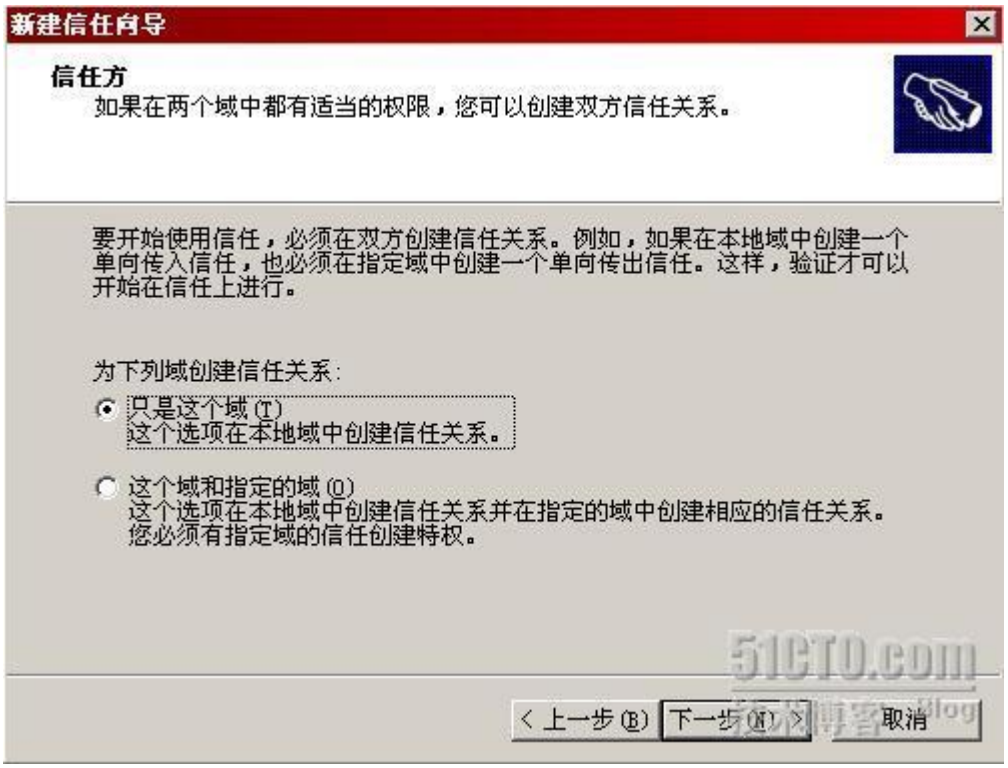
出现新建信任向导，点击“下一步”继续。

信任域的名称为 HOMEWAY.COM。

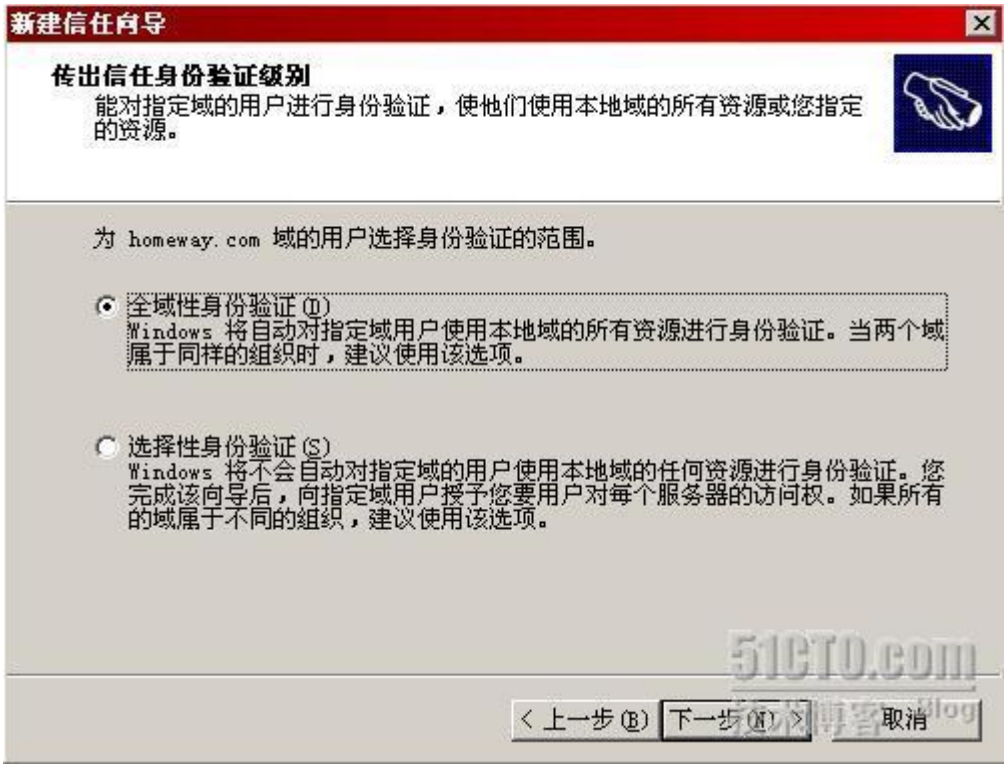
对 ITET.COM 来说，信任方向应该是单向外传。



我们选择只是在 ITET.COM 域进行信任关系的设置，并不涉及 HOMEWAY.COM 域。



接下来我们要选择用户身份验证的范围，我们选择全域性身份验证，这样分配资源时会更加灵活。



接下来要输入域信任口令，我们输入 homeway.com 设置的信任口令。

如下图所示，域信任向导已经做好了准备，点击下一步继续。

如下图所示，域信任关系设置成功！

由于 homeway.com 已经允许被 itet.com 信任，因此我们现在可以在 itet.com 上确认传出信任了。

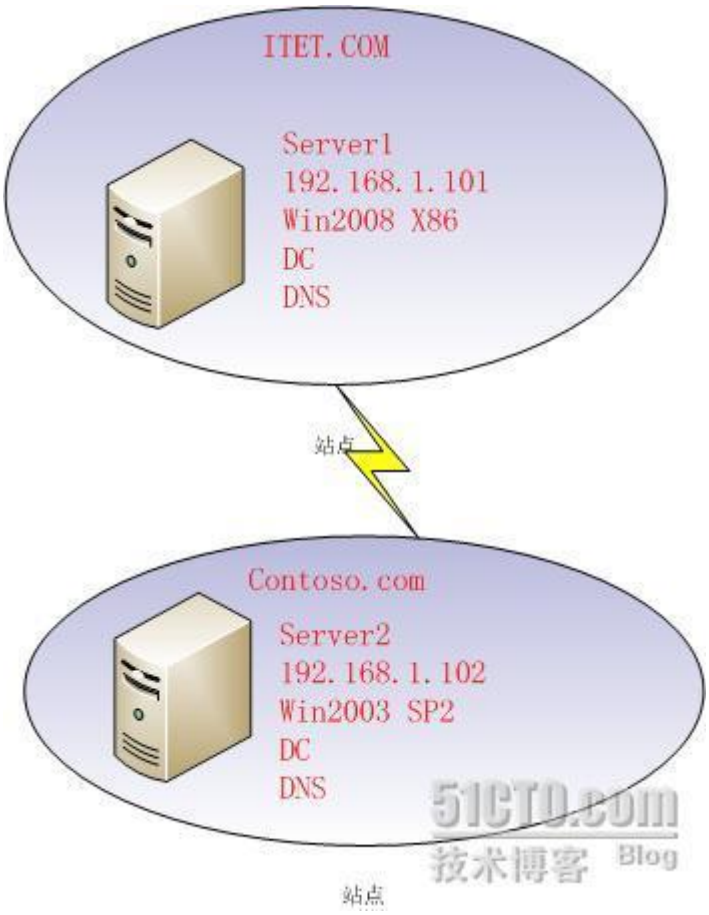
如下图所示，信任关系创建完成。

我们来看看设置信任后的效果，我们在 itet.com 的域控制器 Flroence 上找到一个文件夹，看看能否把文件夹的访问权限分配给 homeway.com 的用户。我们在文件夹属性中找到安全标签，点击添加按钮，如下图所示，点击“位置”。

如下图所示，我们发现位置列表中已经有 homeway.com 域了，我们现在已经可以把资源分配给 homeway.com 域的用户了，单向域信任关系创建成功了。

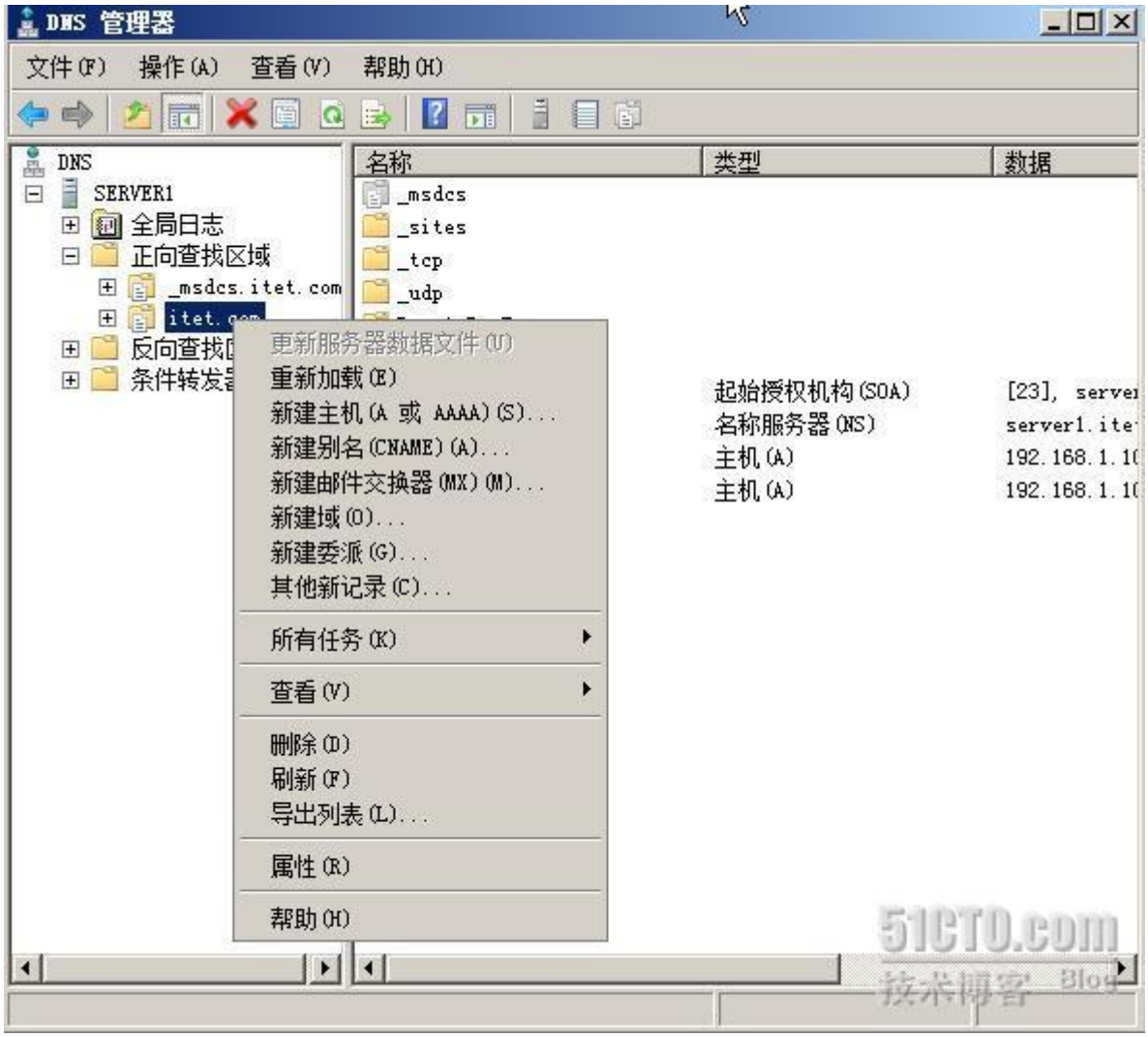
创建 Win2003 域和 Win2008 域之间的信任关系

我们在上一篇文章中创建了域信任关系，这个信任关系发生在两个 Win2003 域之间，而且两个域使用了同一个 DNS 服务器。今天我们更换一个实验场景，拓扑如下图所示。一个是 Win2003 域，另一个是 Win2008 域。两个域都使用各自的域控制器提供 DNS 解析，而且 Win2008 域的功能级别是 Win2003，我们将为大家演示如何在这两个域之间创建信任关系。

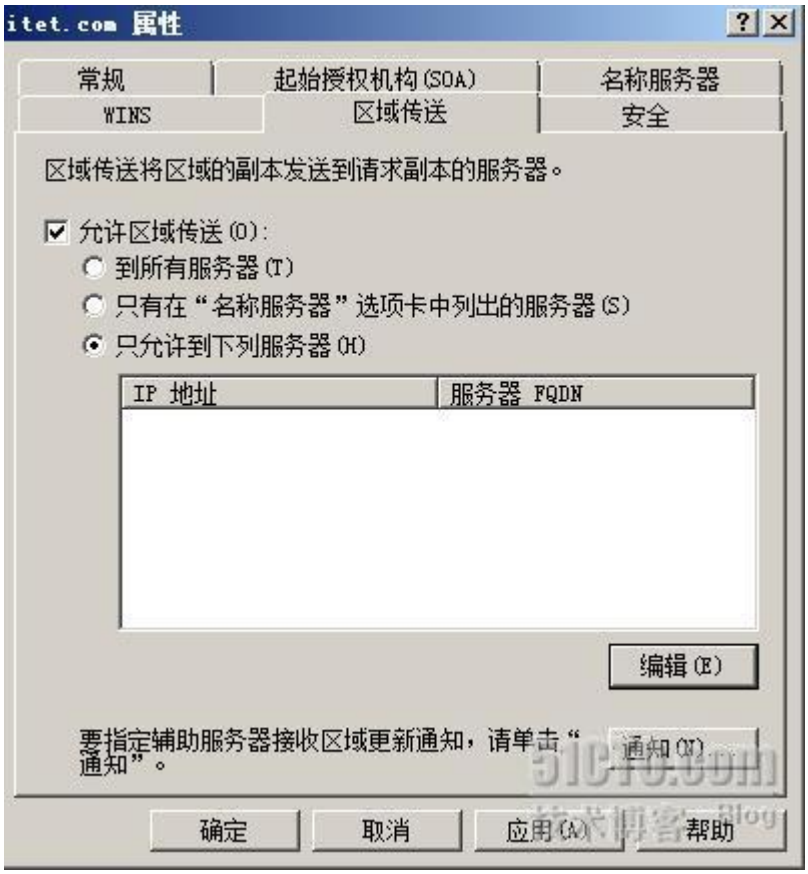


这个实验的关键是 DNS！操作系统的差异并不重要，Win2008 域可以和 Win2003 域，甚至可以和 Win2000 域创建信任关系。我们要注意的是 DNS 的设置，每个域控制器要确保自己使用的 DNS 服务器不但可以解析本域的 SRV 记录，还可以解析与自己有信任关系域的 SRV 记录，也就是说 DNS 服务器要对信任域和被信任域的 SRV 记录都能进行解析。如何让每个 DNS 服务器都能解析两个域的 SRV 记录呢？我们有多种技术可以选择，例如辅助区域，存根区域，私有根或者转发器。在本次实验中我们使用辅助区域来解决这个问题，在每个 DNS 服务器上创建一个对方域的辅助区域，这样 DNS 服务器就可以对两个域进行解析了。

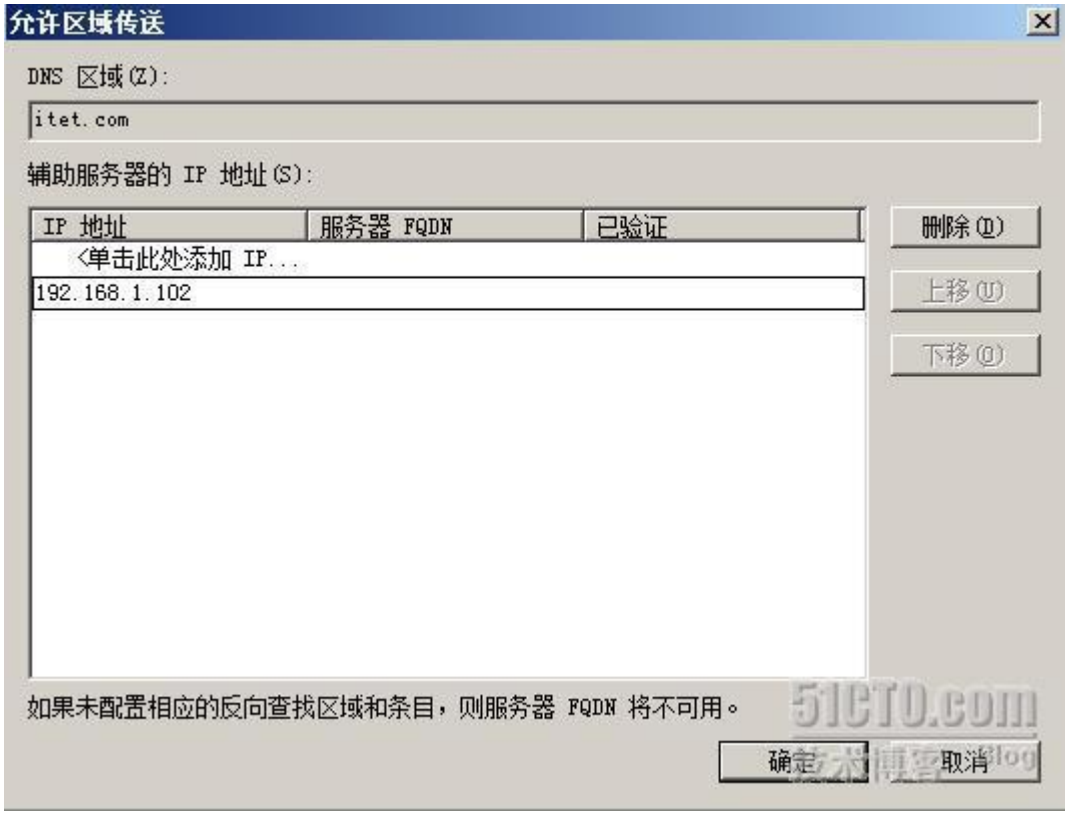
我们为大家演示如何创建 itet.com 的辅助区域。首先我们要在 Server1 负责的 itet.com 区域中进行设置，允许 Server2 创建 itet.com 的辅助区域。在 Server1 上打开 DNS 管理器，如下图所示，右键点击 itet.com 区域，选择“属性”。



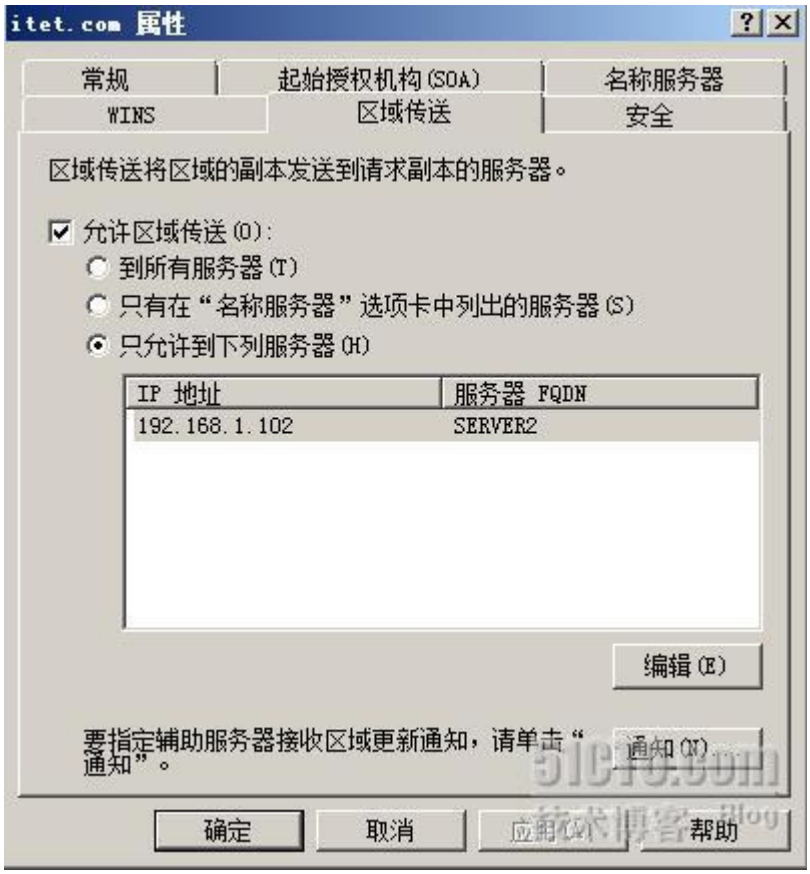
在区域属性中切换到“区域传送”标签，如下图所示，勾选“允许区域传送”，选择“只允许到下列服务器”，点击“编辑”按钮。



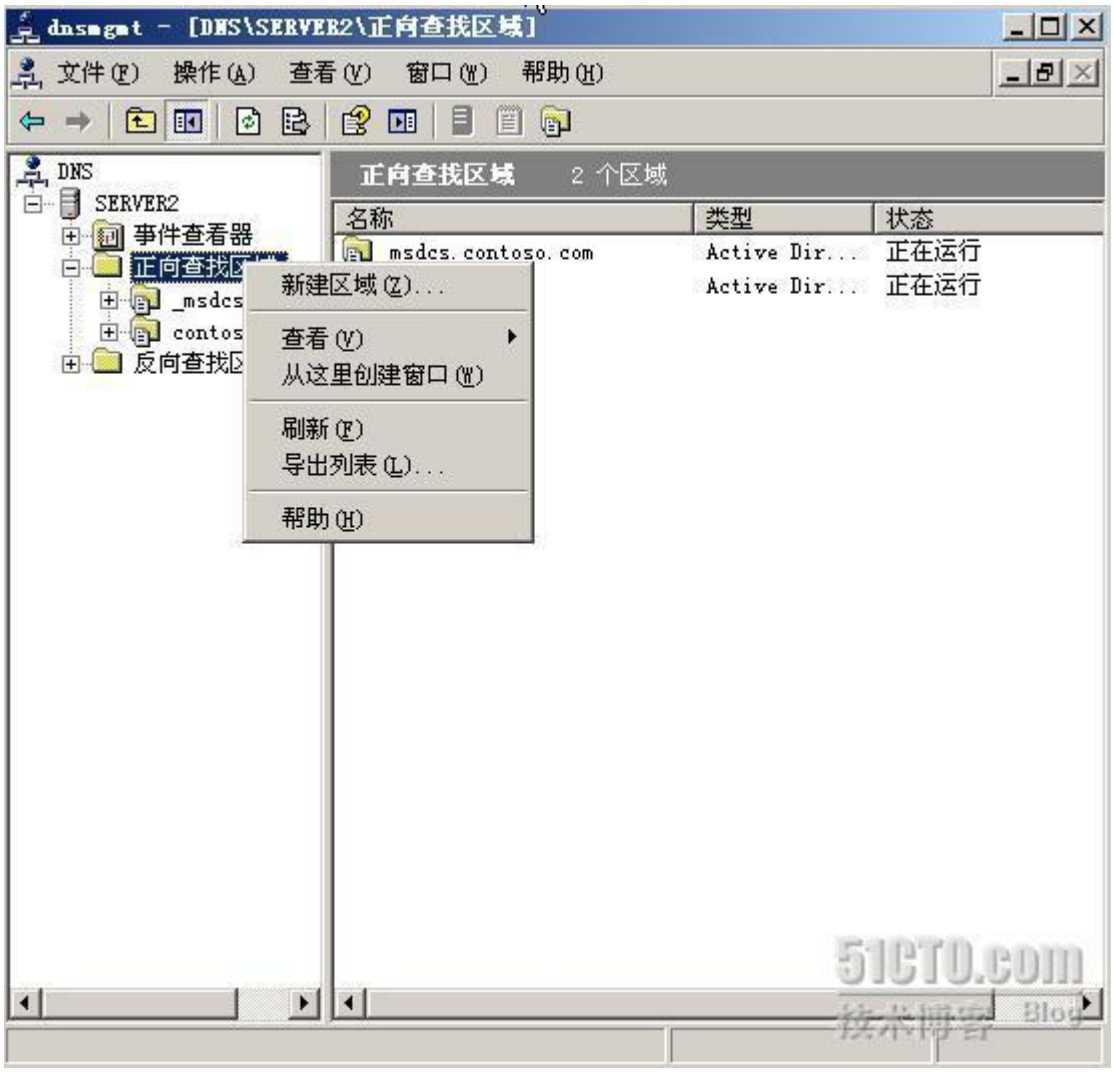
点击编辑按钮后，如下图所示，我们添加了 Server2 的地址 192.168.1.102，点击确定。



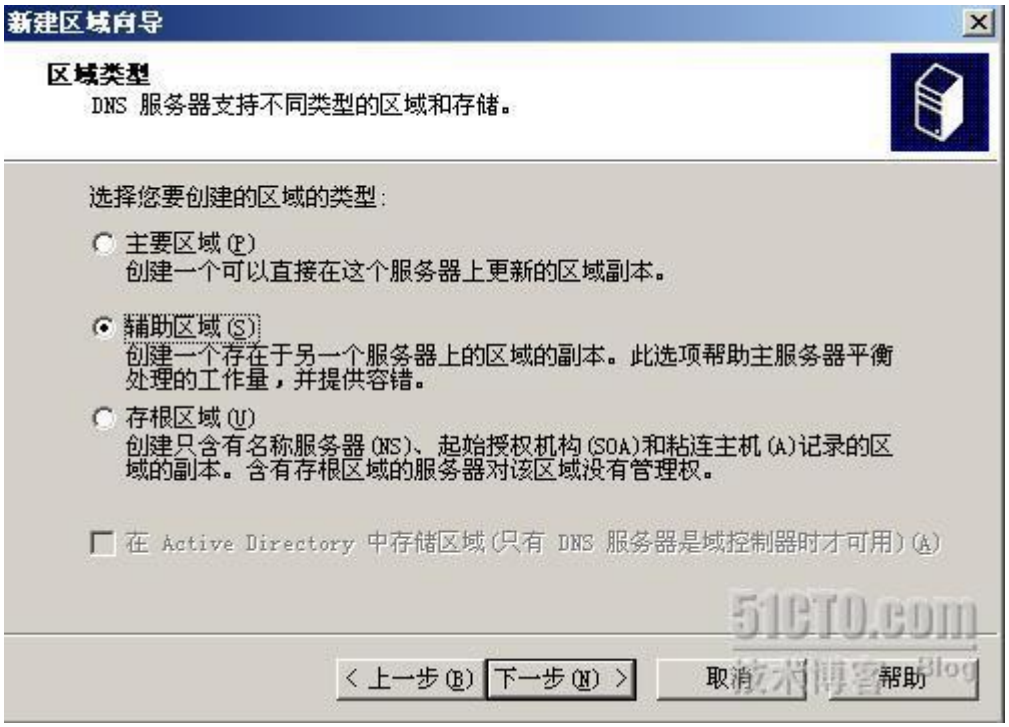
如下图所示，我们已经设定了允许 192.168.1.102 复制 itet.com 的区域数据，其实就是允许 192.168.1.102 成为 itet.com 的辅助 DNS 服务器。



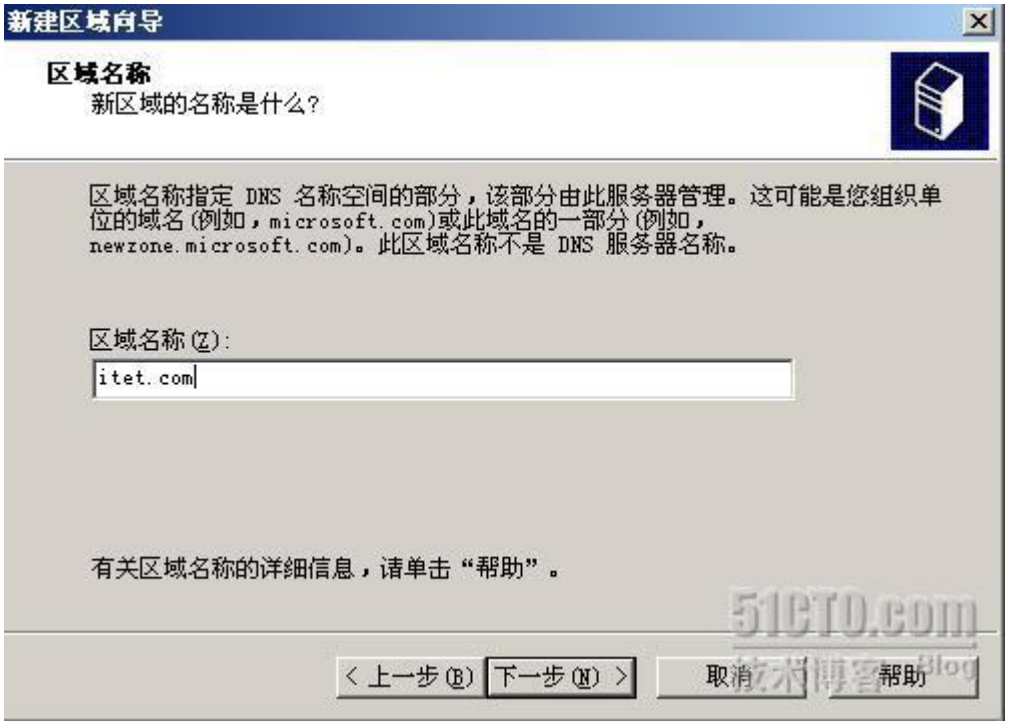
Itet.com 区域既然已经允许 Server2 成为辅助服务器了，那我们接下来就开始在 Server2 上创建辅助区域了。在 Server2 上打开 DNS 管理器，如下图所示，选择“新建区域”。



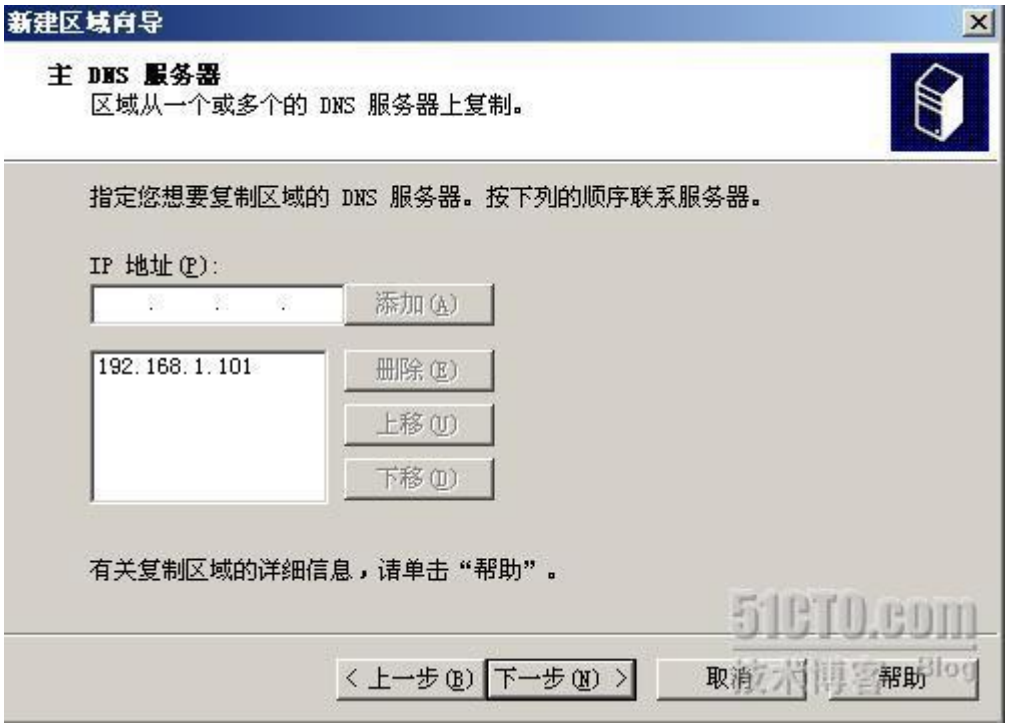
区域类型设置为辅助区域。



区域的名称设置为 itet.com。

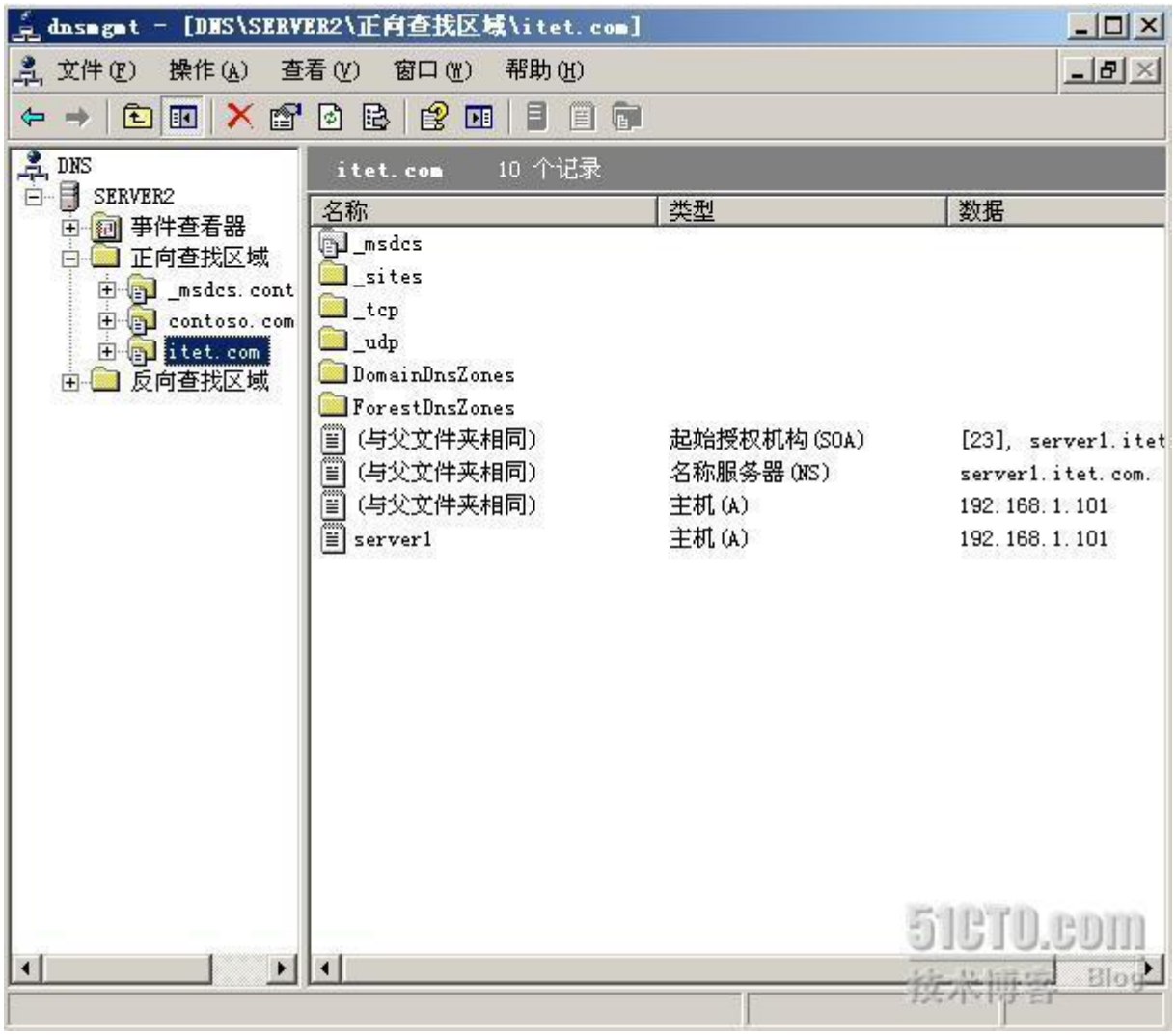


接下来需要设置 itet.com 的主服务器，显然，itet.com 的主服务器是 server1，也就是 192.168.1.101。

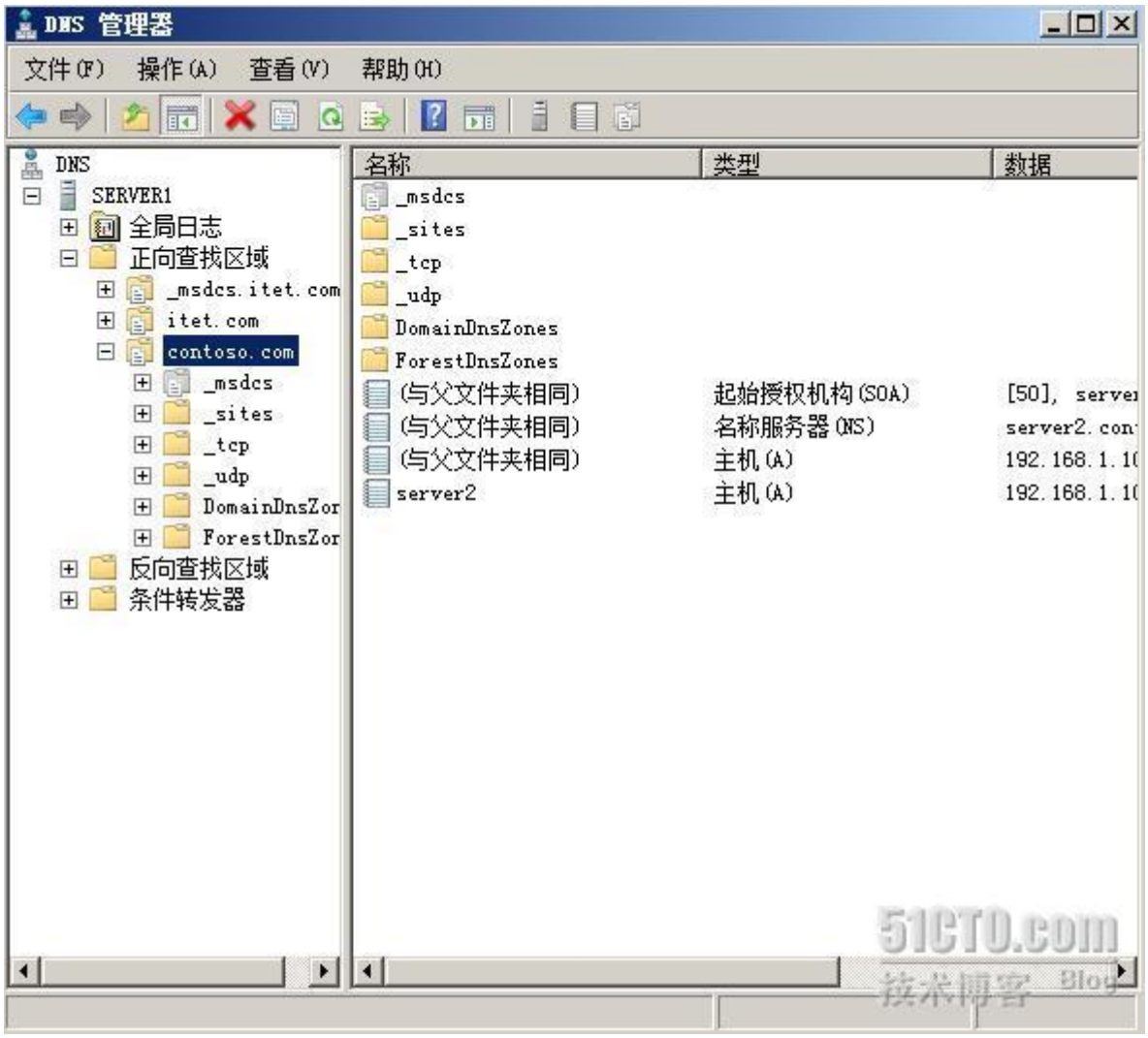


如下图所示，点击“完成”按钮完成 itet.com 区域的创建。

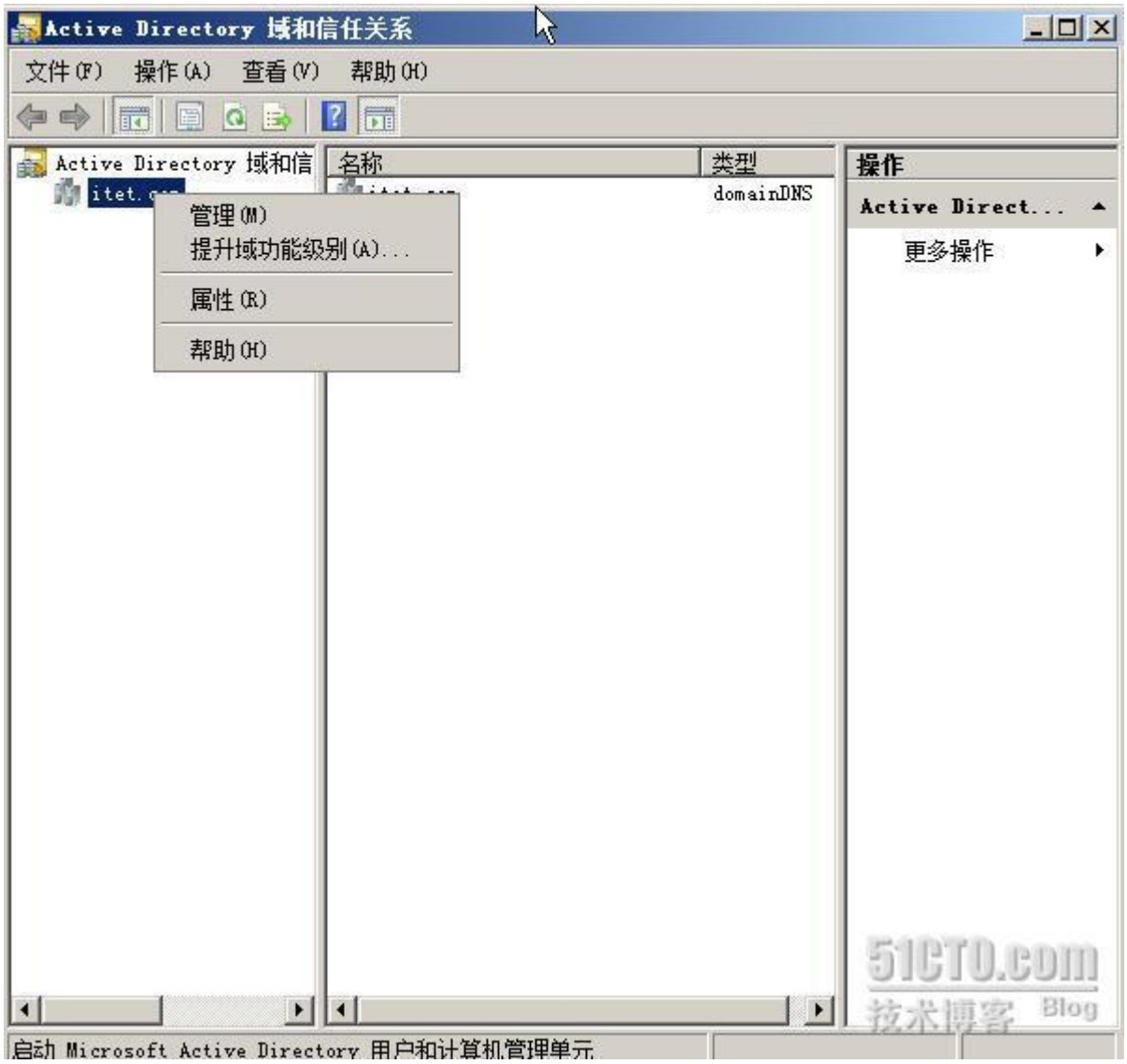
我们在 Server2 的 DNS 管理器中可以看到，itet.com 的区域记录已经被复制到 Server2 上，Server2 已经成功地成为了 Server2 的辅助服务器。



接下来我们要如法炮制，在 Server2 上允许 Server1 成为 contoso.com 的辅助服务器，然后在 Server1 上创建 contoso.com 辅助区域，把 contoso.com 的区域数据复制到 Server1 上。如下图所示，我们看到 Server1 上也已经成功地把 contoso.com 的区域数据复制过来了。

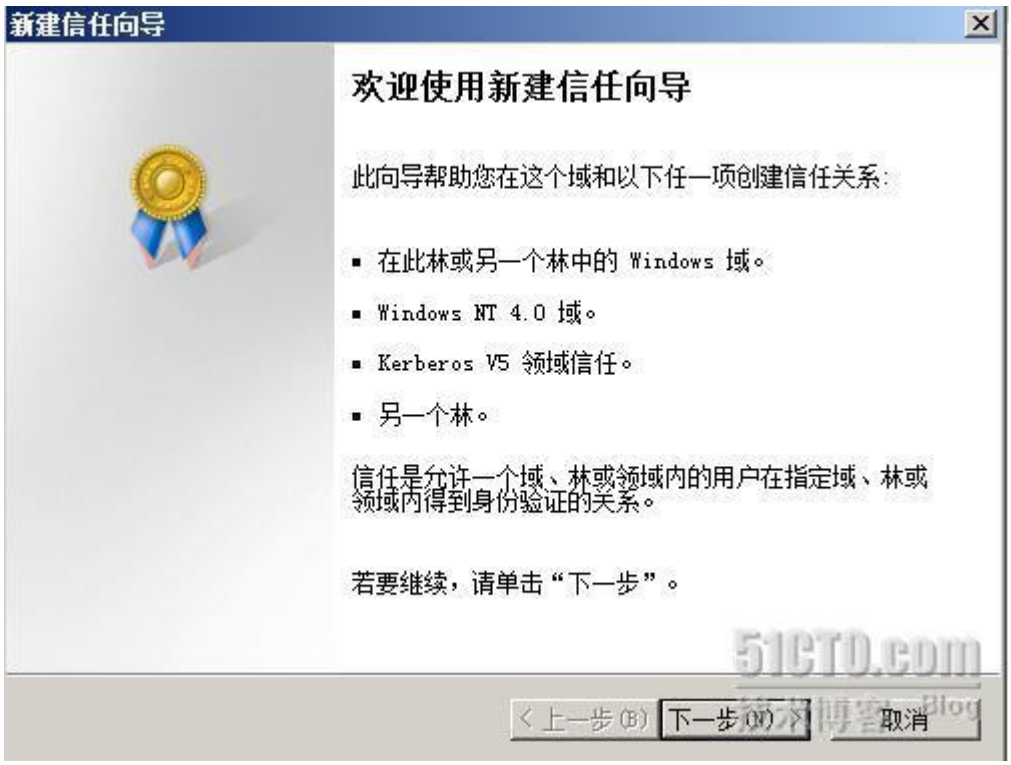


DNS 进行了充分的准备后，我们就可以进行域信任关系的设置了。我们准备在 itet.com 和 contoso.com 之间设置双向信任关系，如下图所示，我们在 Server1 上打开“Active Directory 域和信任关系”，右键点击 itet.com，选择“属性”。



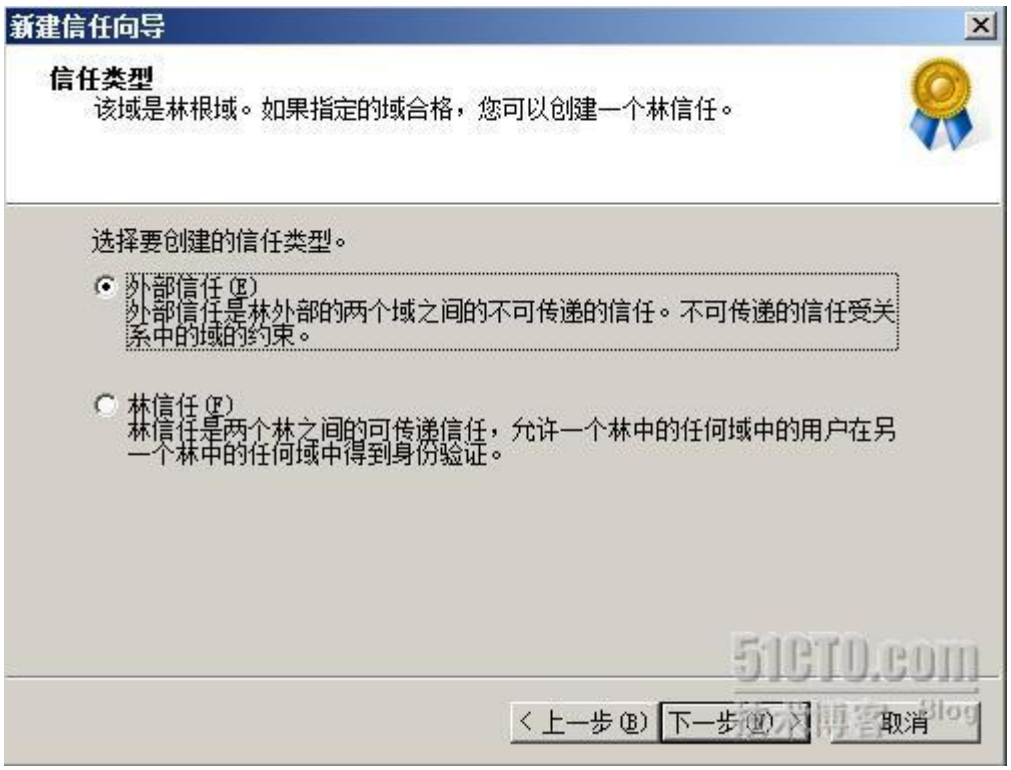
在 itet.com 的域属性中切换到“信任”标签，点击“新建信任”。

出现新建信任关系向导，点击“下一步”继续。

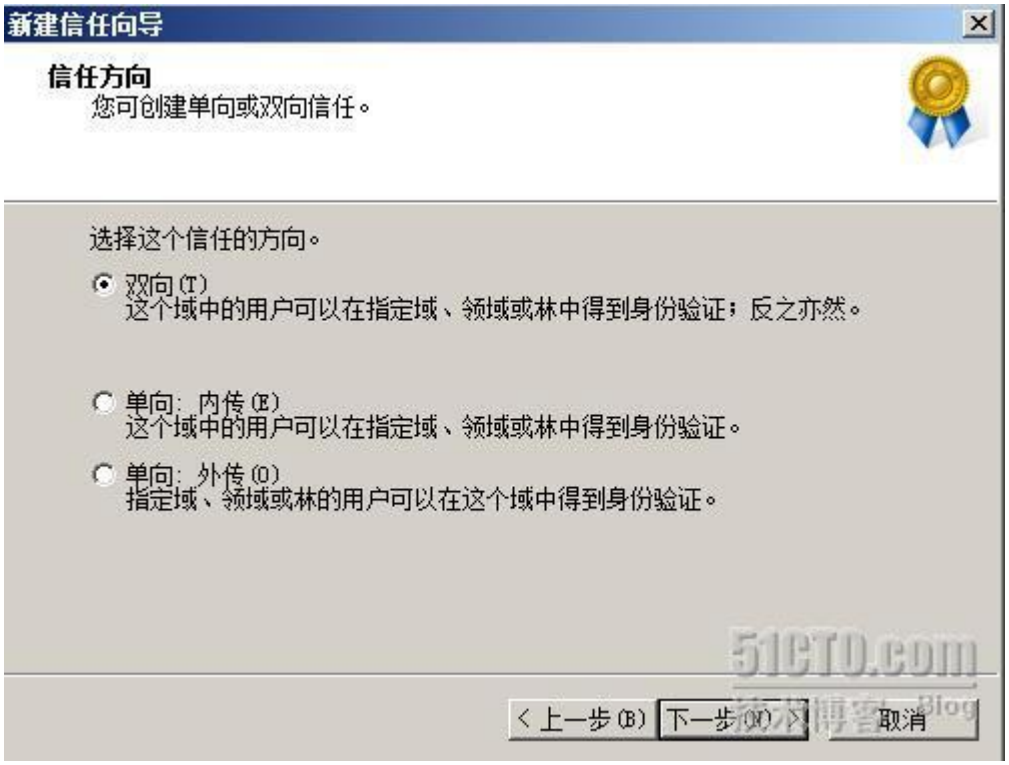


向导询问 server1 准备和哪个域建立信任关系，我们输入 contoso.com 的域名。

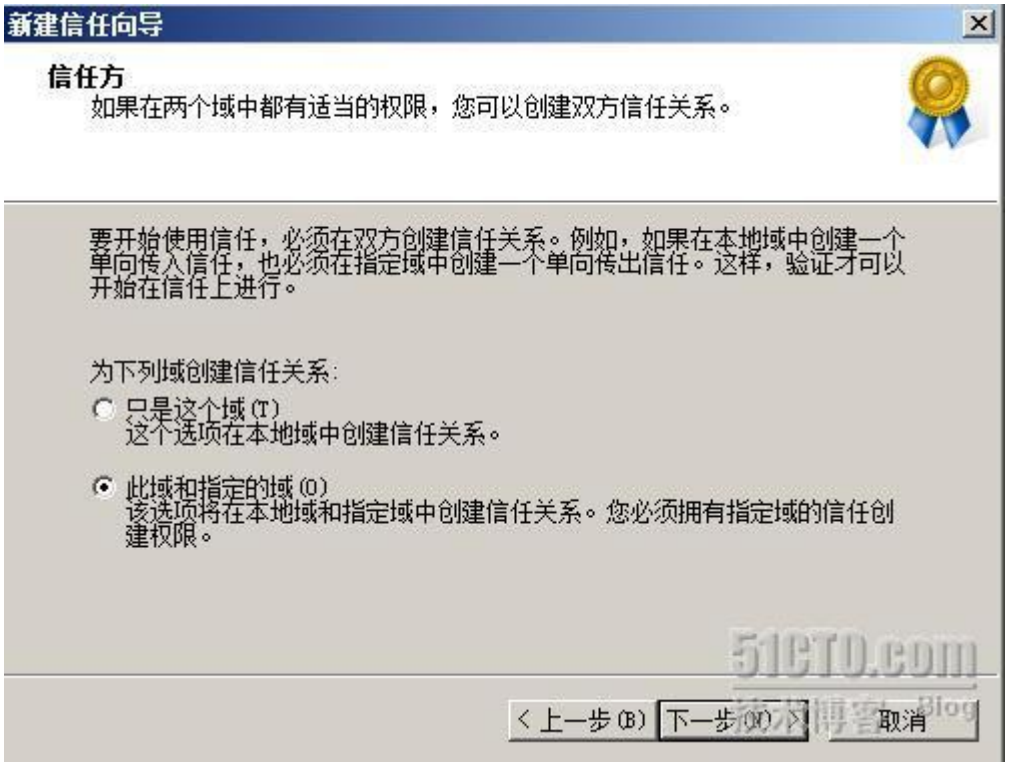
接下来我们要选择是在两个域之间建立不可传递的外部信任，还是可传递的林信任，我们选择建立外部信任。



如下图所示，我们选择建立双向信任关系。



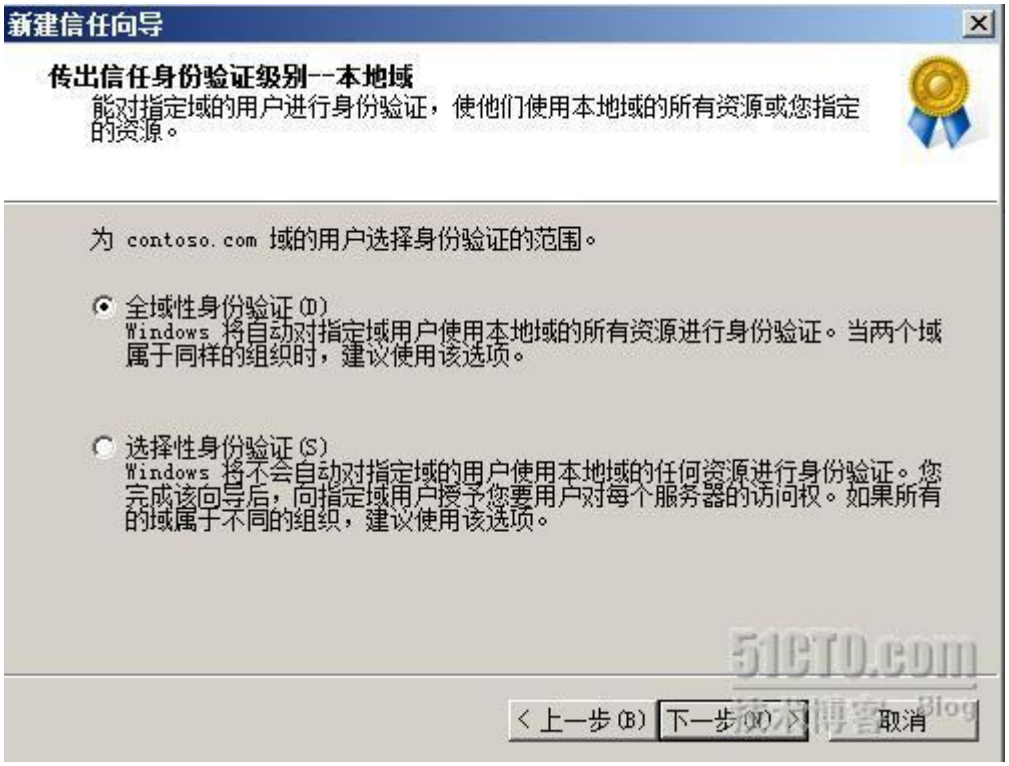
接下来向导询问是在两个域的域控制器上分开设置，还是同时进行设置，我们选择“此域和指定的域”，准备在两个域的域控制器上同时进行信任关系的设定。



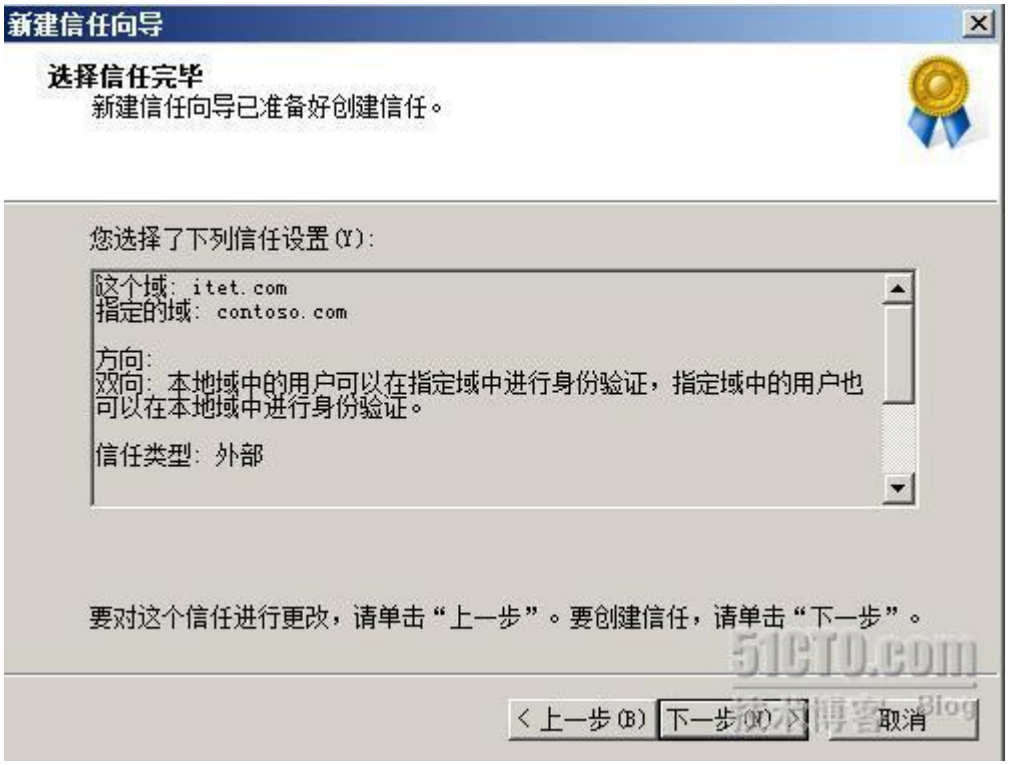
接下来向导要求输入 contoso.com 的域管理员口令，这样才可以在 contoso.com

的域控制器上设置信任关系。

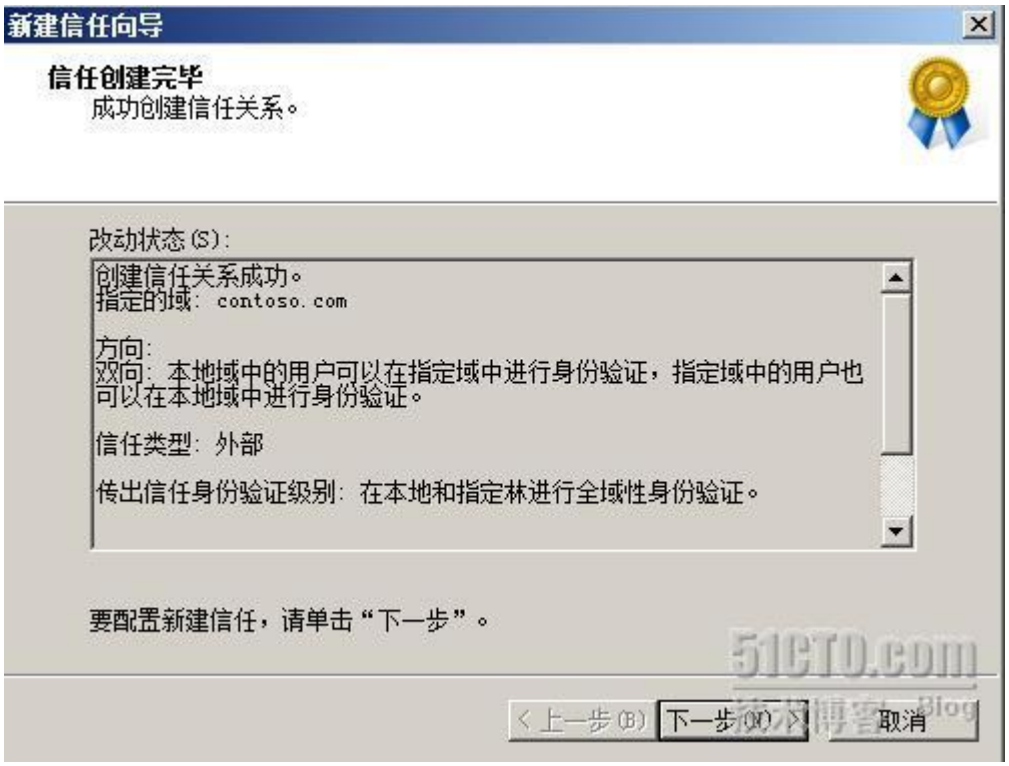
我们选择“全域性身份验证”，允许信任域用户使用被信任域的所有资源。



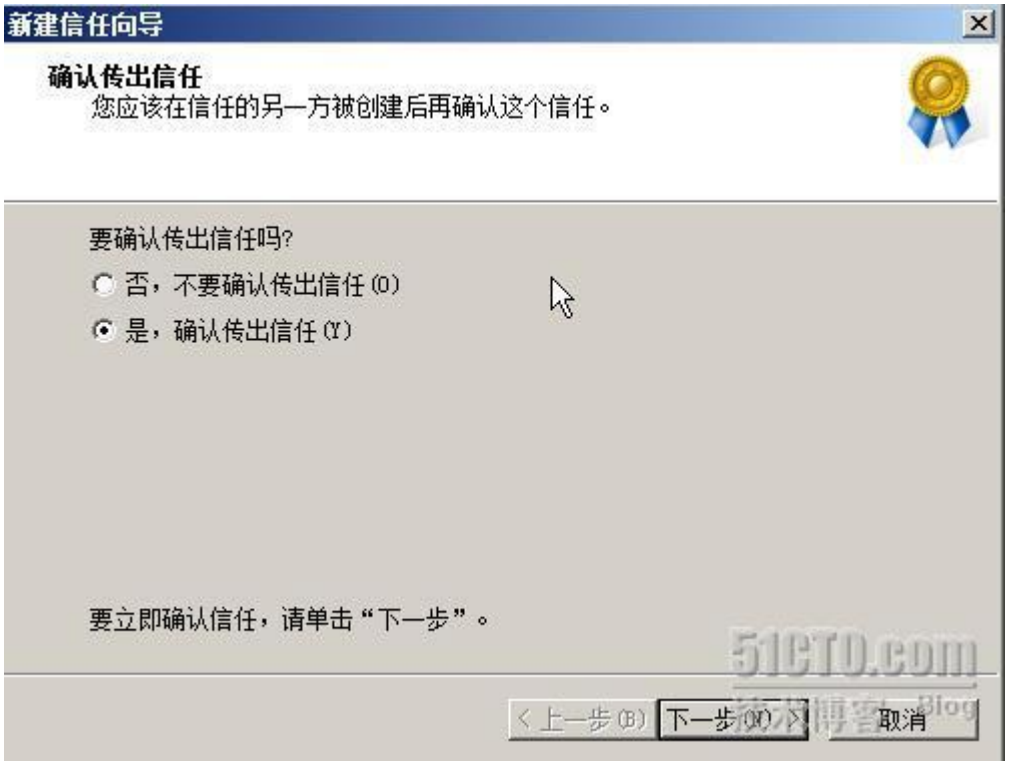
如下图所示，信任关系的创建已经准备完毕，点击下一步继续。



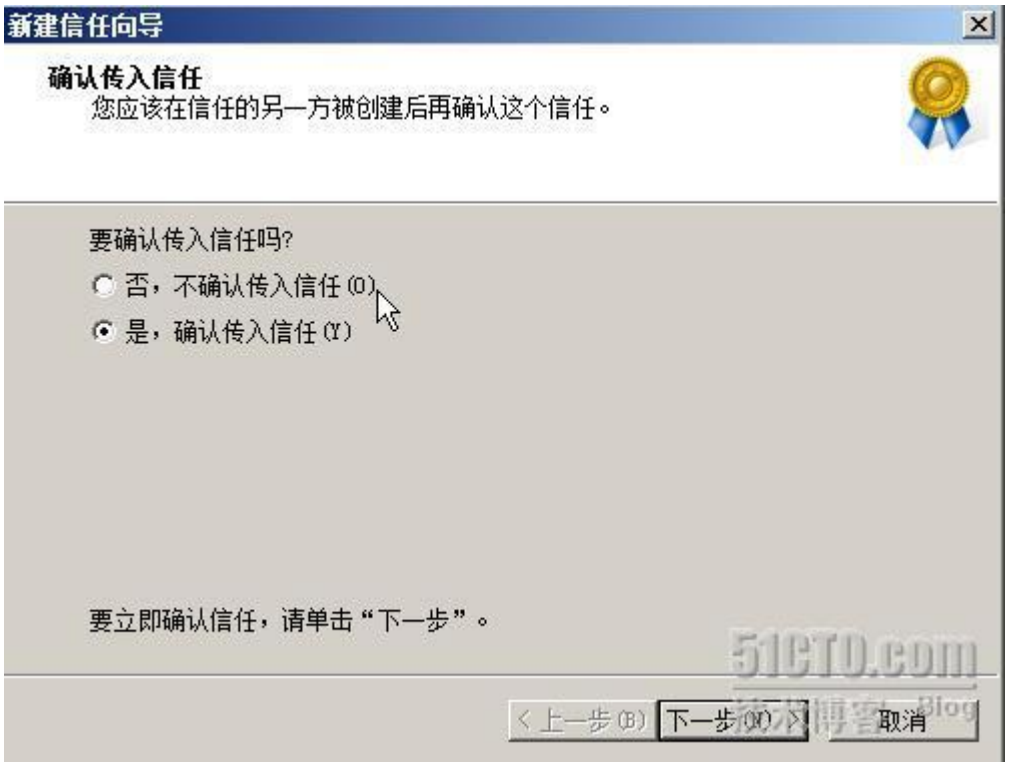
如下图所示，两个域之间的信任关系已经成功创建。



确定在 itet.com 域上传出信任关系。

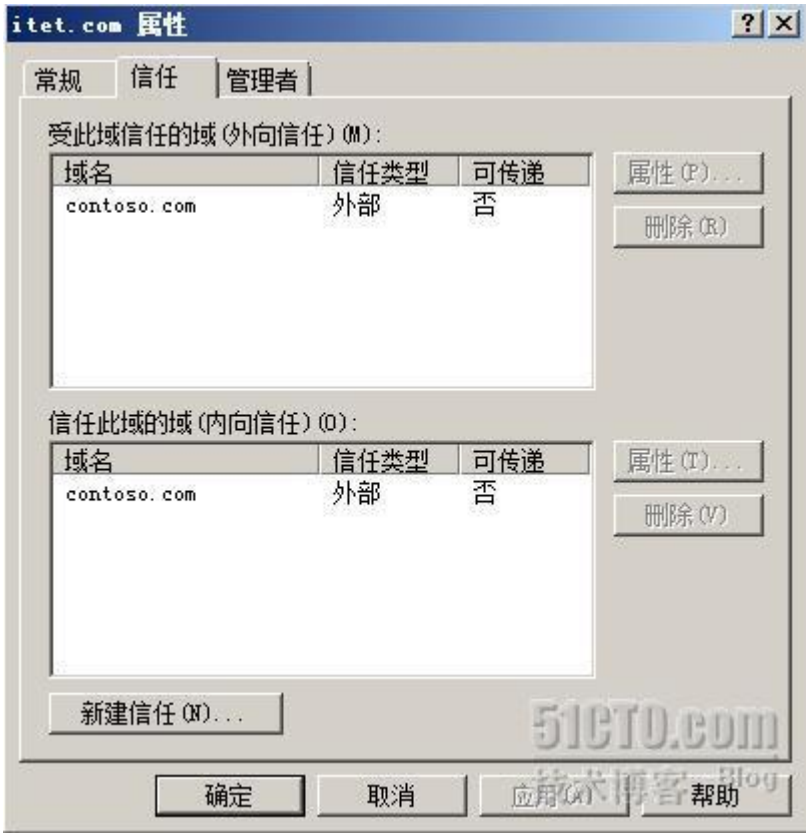


接下来在 itet.com 域上确定传入信任关系。



如下图所示，所有的工作都已完成，点击“完成”结束域信任关系的创建爱你。

从下图中可以看到，两个域之间确实创建了不可传递的双向域信任关系，我们的实验目标已经实现。这个实验其实有更广泛的适应性，同时可以用于 Win2000 与 Win2003，Win2000 与 Win2008 等信任关系的创建。大家可以举一反三，慢慢体会。

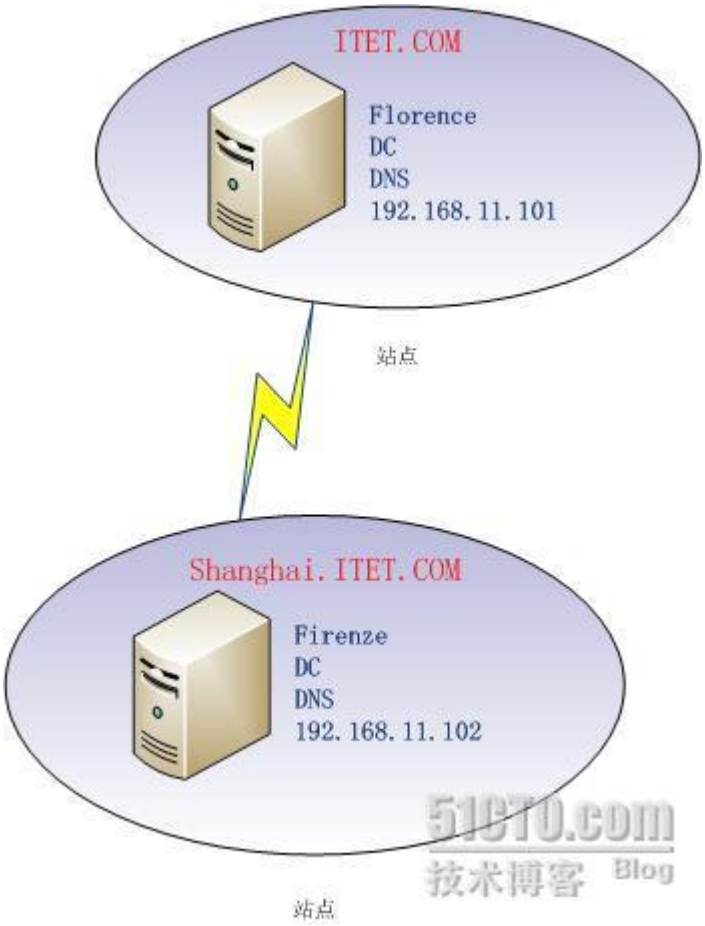


实战子域部署

域树是 Active Directory 针对 NT4 的传统域模型所进行的重要改进。在 NT 4 时代的域模型中，每个域都要使用没有层次结构的 NETBIOS 名称，而且域和域之间缺少关联，只能创建不能传递的域信任关系。这会在企业管理方面造成诸多不利因素，首先域和域之间很难根据域名判断彼此间的隶属关系，例如 beijing 域和 shanghai 域；其次由于域之间的信任关系不可传递，在域数量较多时光是创建域之间的完全信任就要耗费大量时间。假定有 10 个域，那我们在 10 个域之间要建立 45 次信任关系才能让这些域相互之间都完全信任。

域树针对以上问题进行了很好的解决，域树的父域和子域之间由于使用了层次分明的 DNS 域名，只要根据域名我们就可以判断出两个域的隶属关系，例如有两个域 abc.com 和 test.abc.com，我们可以很轻易地判断出后者是前者的子域。域树在信任关系上也有很好的改进，域树内的各个域之间会自动建立起双向可传递的信任关系，显然这是一个效率上的重大改进。

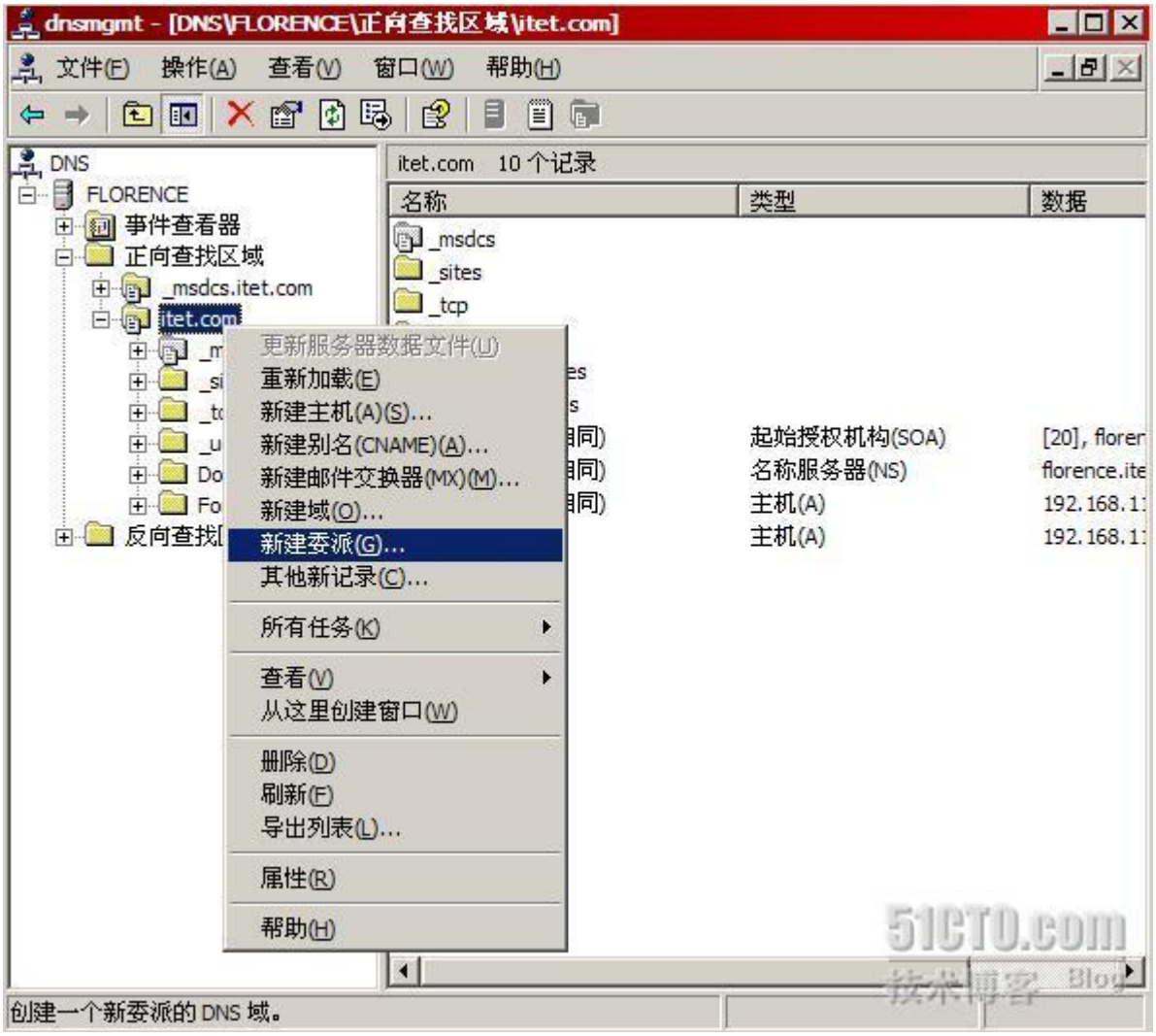
既然域树如此重要，那我们将通过一个实例为大家介绍如何部署一个包括父域和子域的两层域树。拓扑如下图所示，父域为 itet.com，域控制器和 DNS 都是 Florence。子域是 shanghai.itet.com，域控制器和 DNS 都是 Firenze。父域已经创建完毕，我们将为大家介绍如何部署子域。如果父域和子域都使用同一个 DNS 服务器，部署起来会更容易。但我们考虑到有可能子域希望能拥有独立的域名解析权，这样很多工作会更容易开展，因此我们决定在子域也设置一个独立的 DNS 服务器。



一 DNS 委派

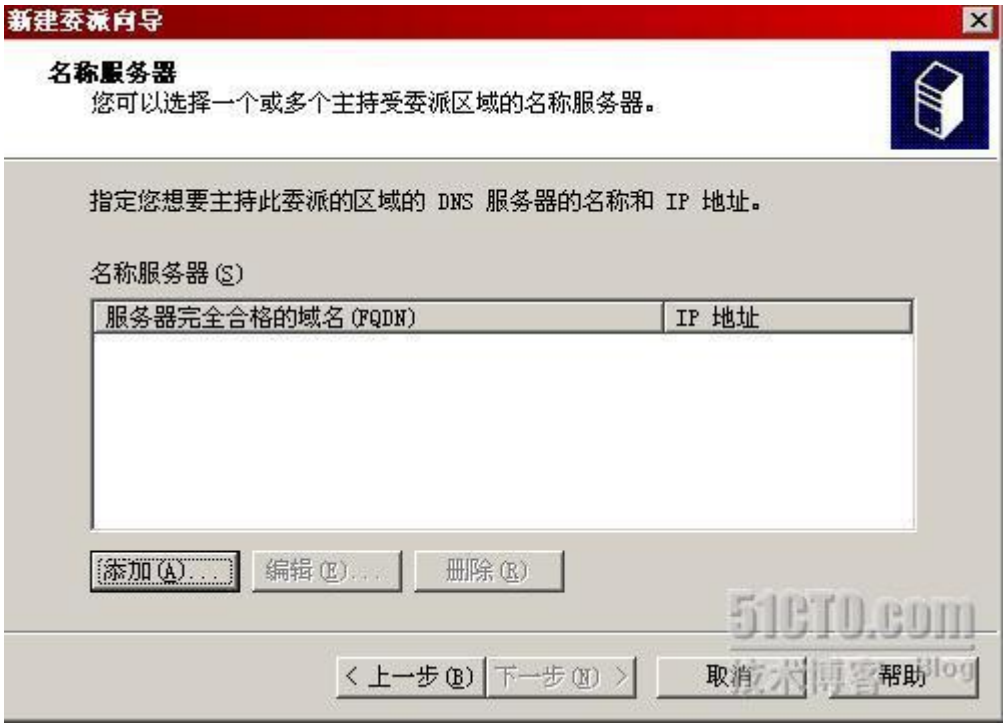
首先我们要考虑 DNS 的委派问题。目前，itet.com 的解析权归 Florence，也就是说 Florence 可以解析所有以 itet.com 结尾的域名。如果我们希望 Firenze 能够解析 shanghai.itet.com，那么我们必须在 Florence 上对 Firenze 进行委派，授权 Firenze 可以解析 shanghai.itet.com。我们在 Florence 上打开 DN

S 管理器，如下图所示，右键点击 itet.com，选择“新建委派”。

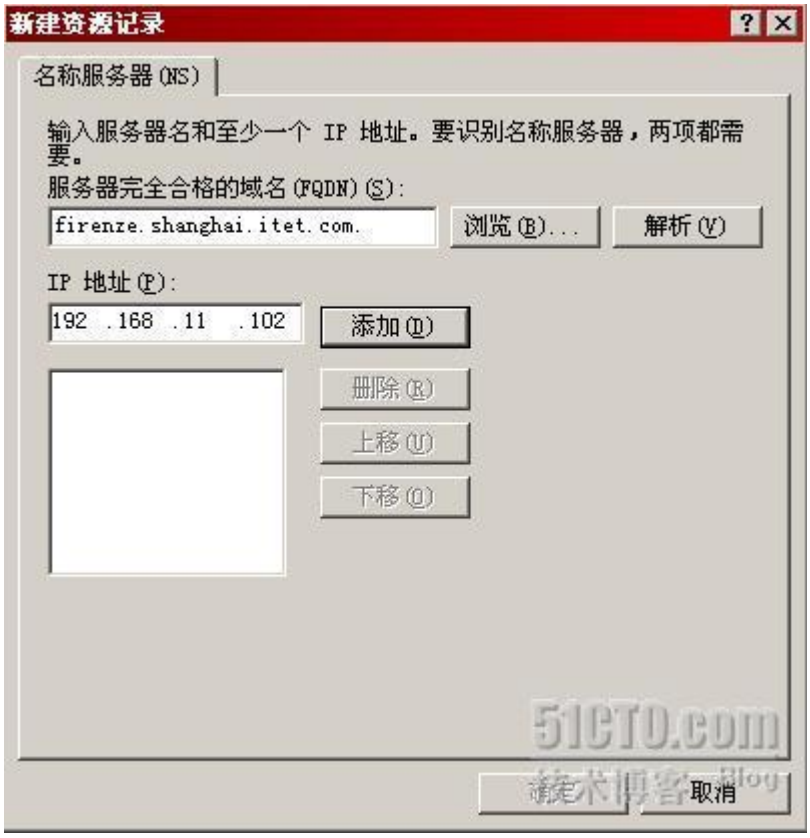


如下图所示，我们准备对 shanghai.itet.com 区域进行委派。

接下来要设置委派对象，如下图所示，点击“添加”按钮来设置被委派的 DNS 服务器。

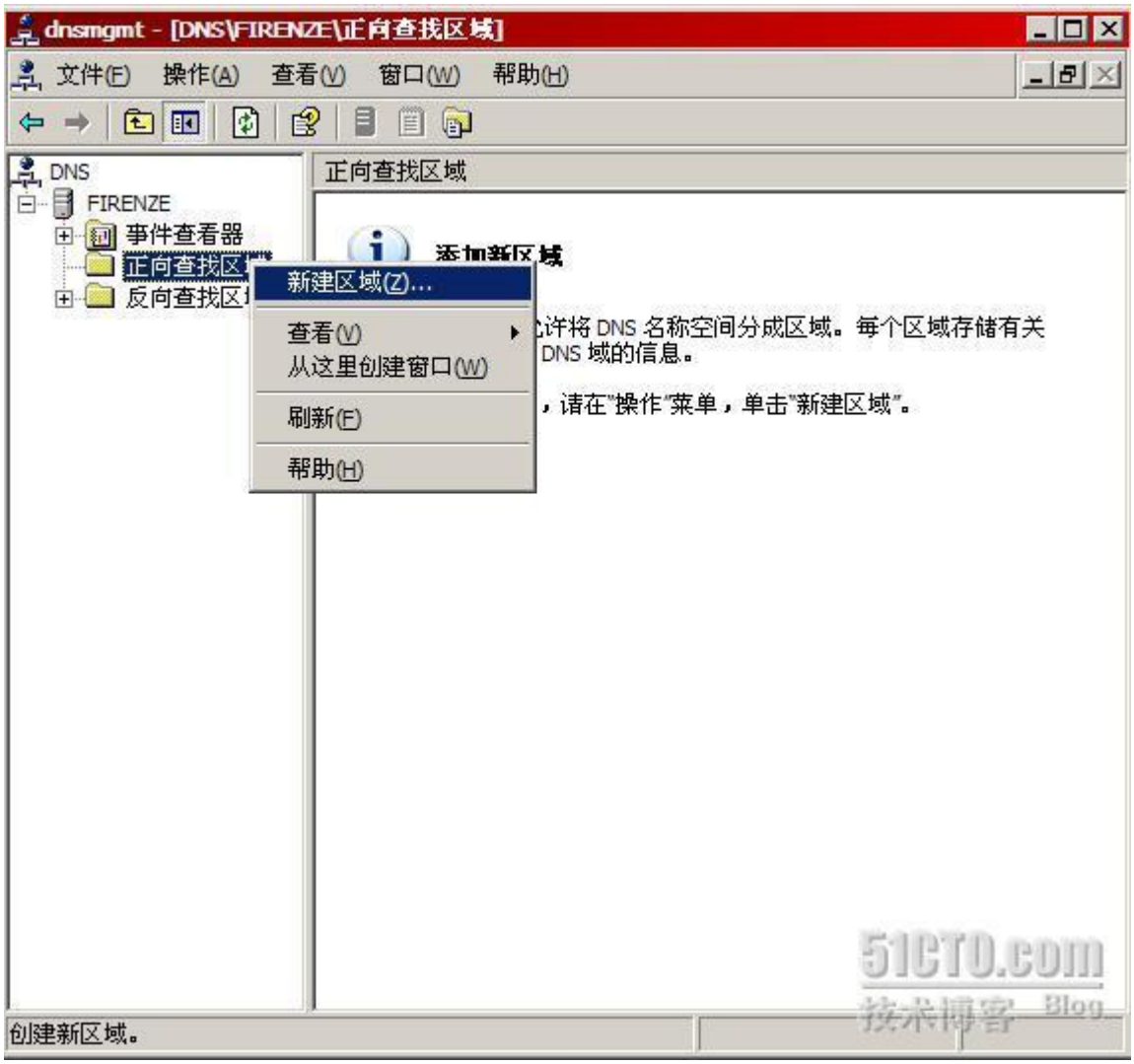


如下图所示，我们输入被委派 DNS 服务器的完全合格域名：firenze.shanghai.itet.com，同时输入这个完全合格域名对应的 IP 地址，点击“添加”按钮就可以结束委派了。

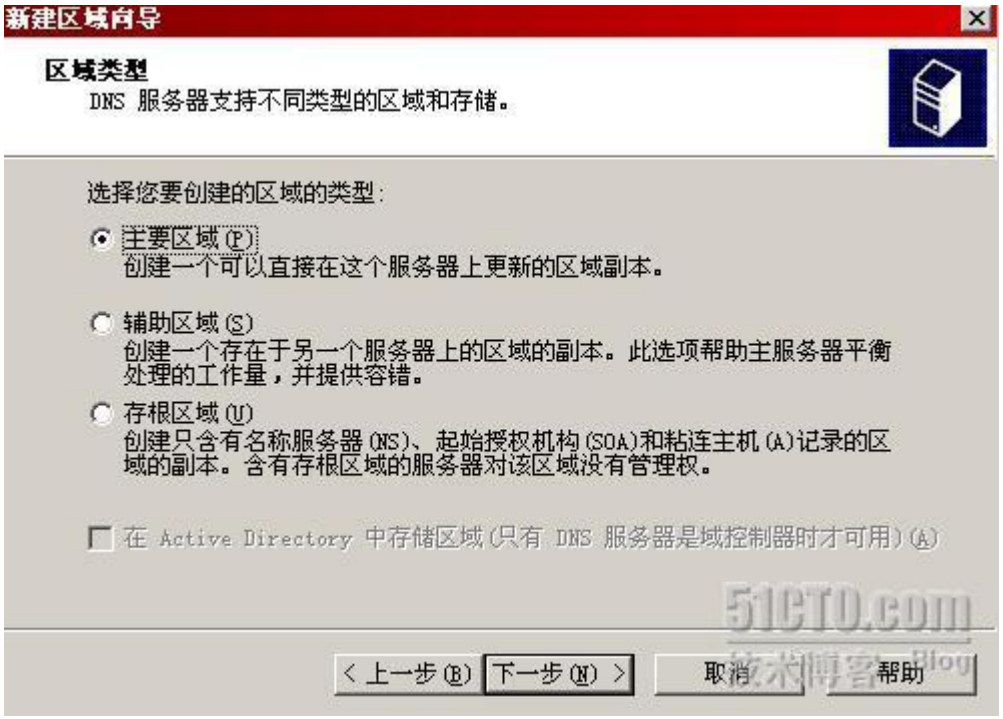


二　创建 DNS 区域

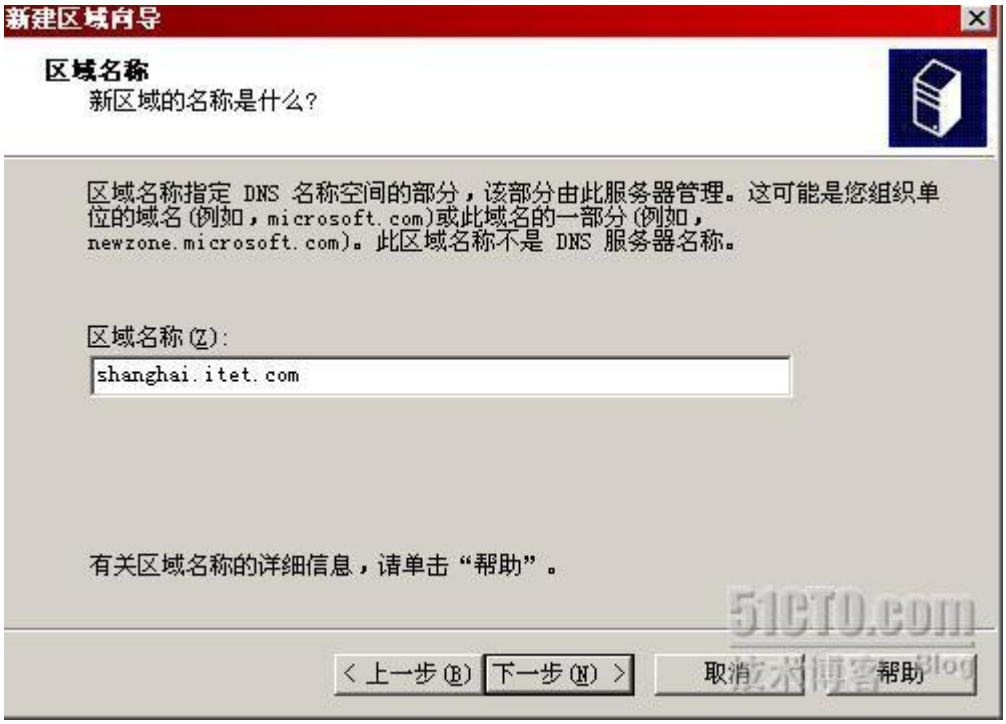
Florence 对 Fienze 进行了解析委派之后，Firenze 就可以解析以 shanghai.itet.com 结尾的域名了。接下来我们可以在 Firenze 上创建一个 DNS 区域：shanghai.itet.com，如下图所示，在 Firenze 上打开 DNS 管理器，选择“新建区域”。


dnsmgmt - [DNS\FIRENZE\正向查找区域]
文件(F) 操作(A) 查看(V) 窗口(W) 帮助(H)
DNS
FIRENZE
事件查看器
正向查找区域
反向查找区域
新建区域(Z)...
查看(V)
从这里创建窗口(W)
刷新(F)
帮助(H)
正向查找区域
许将 DNS 名称空间分成区域。每个区域存储有关
DNS 域的信息。
，请在"操作"菜单，单击"新建区域"。
创建新区域。

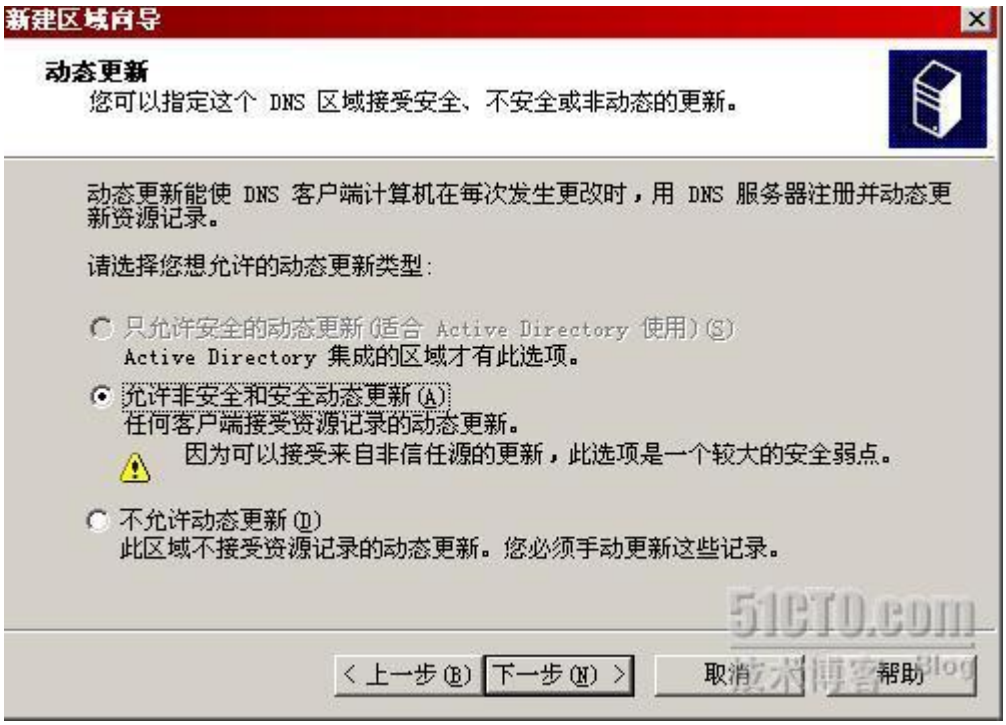
区域类型为主要区域。



区域名称和 Firenze 获得委派解析的域名一致，是 shanghai.itet.com。

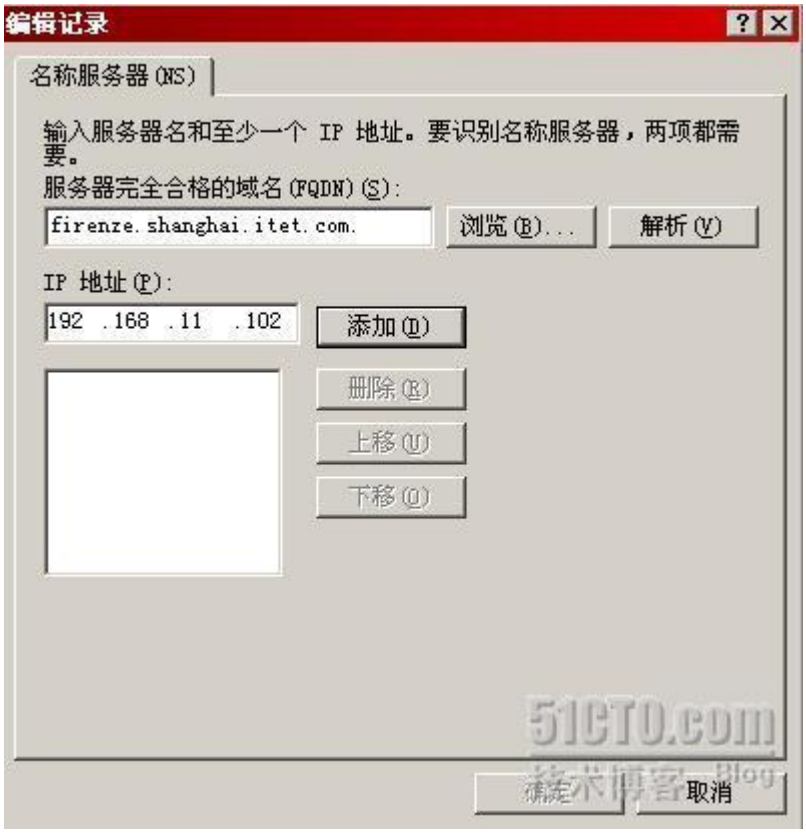


由于 Firenze 要为子域提供 DNS 解析服务，因此这个区域一定要允许动态更新，我们知道，在创建子域的 AD 时需要在 DNS 区域中主动注册 A 记录，Cname 记录和 SRV 记录。

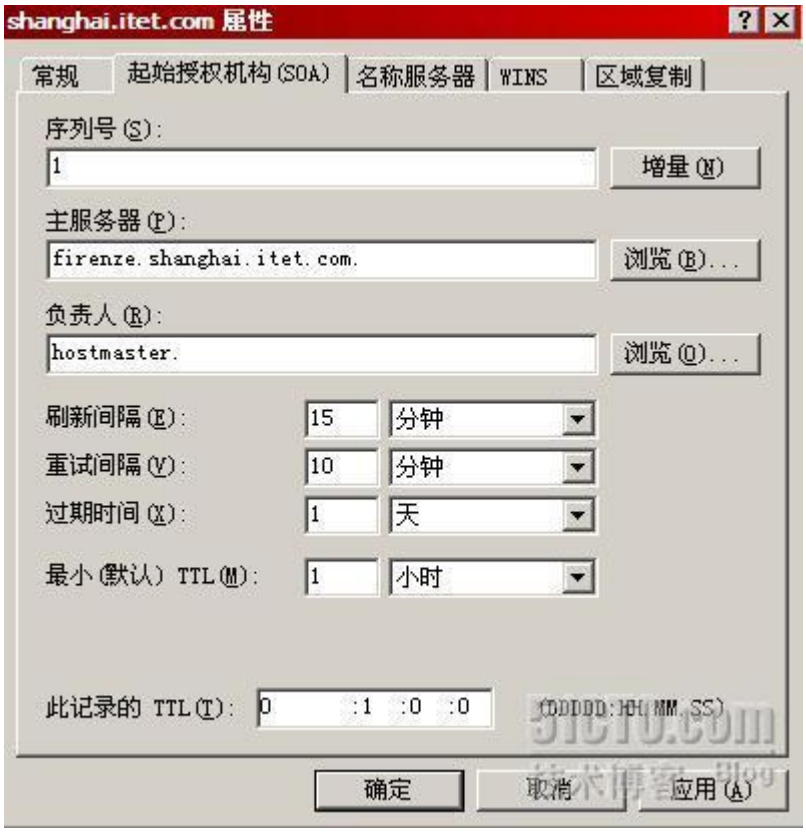


如下图所示，创建完区域后，我们发现 DNS 区域中的 NS 记录和 SOA 记录都有问题。问题在于这些记录都不是用完全合格域名描述的，我们需要对这些记录进行修改。

首先我们修改 NS 记录，我们用 firenze.shanghai.itet.com 来描述 NS 记录，同时用 IP 地址 192.168.11.102 对这个记录进行解析。



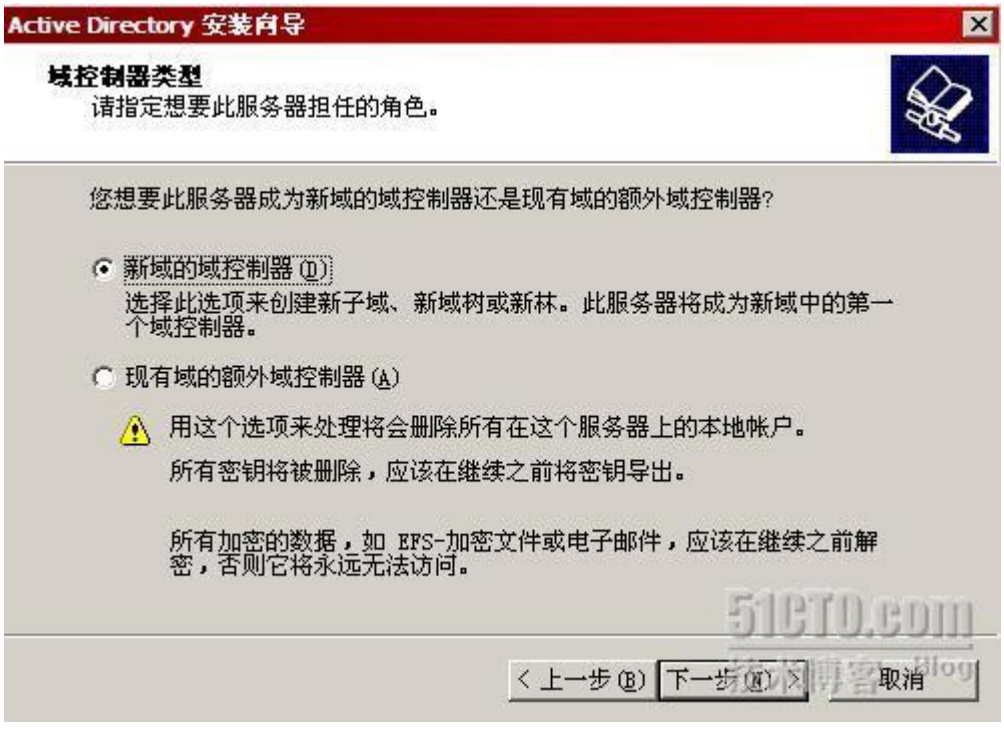
修改完 NS 记录后，我们再来修改 SOA 记录，如下图所示，我们在 SOA 记录中也用 firenze.shanghai.itet.com 来描述主服务器。NS 和 SOA 记录描述完后，DNS 方面的准备工作就算是完成了。



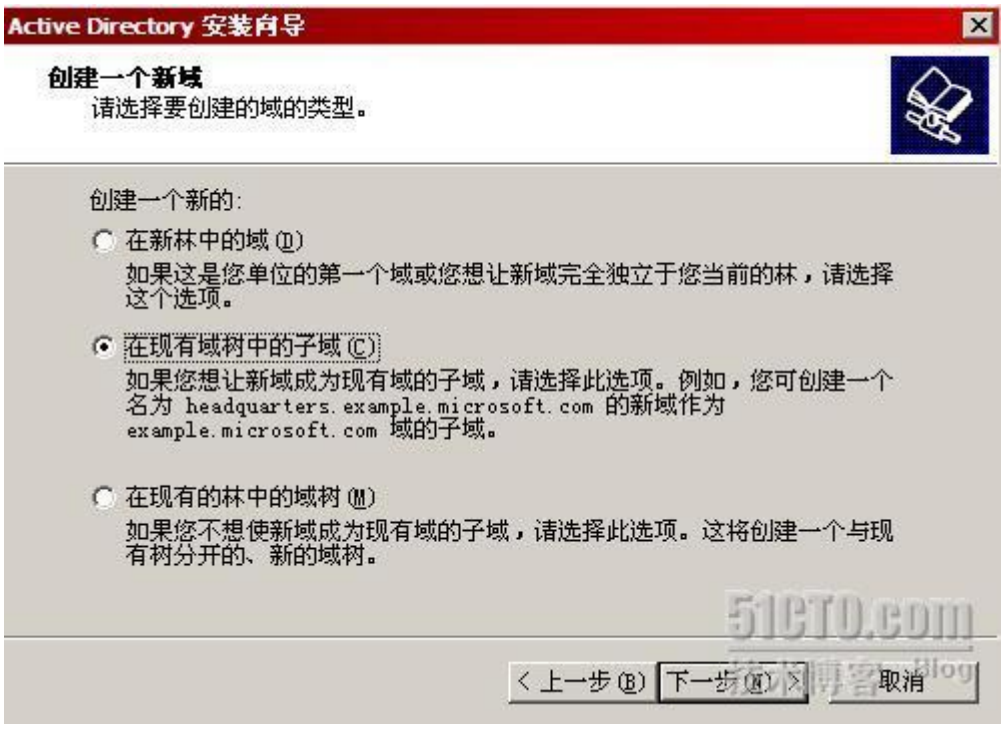
三　部署子域

DNS 的准备工作就绪后，接下来我们就可以在 Firenze 上进行子域的部署了。我们在 Firenze 上运行 Dcpromo，如下图所示，准备开始 Active Directory 的部署。

我们选择部署一个新域的域控制器。



接下来在域的类型中选择部署一个现有域树中的子域。



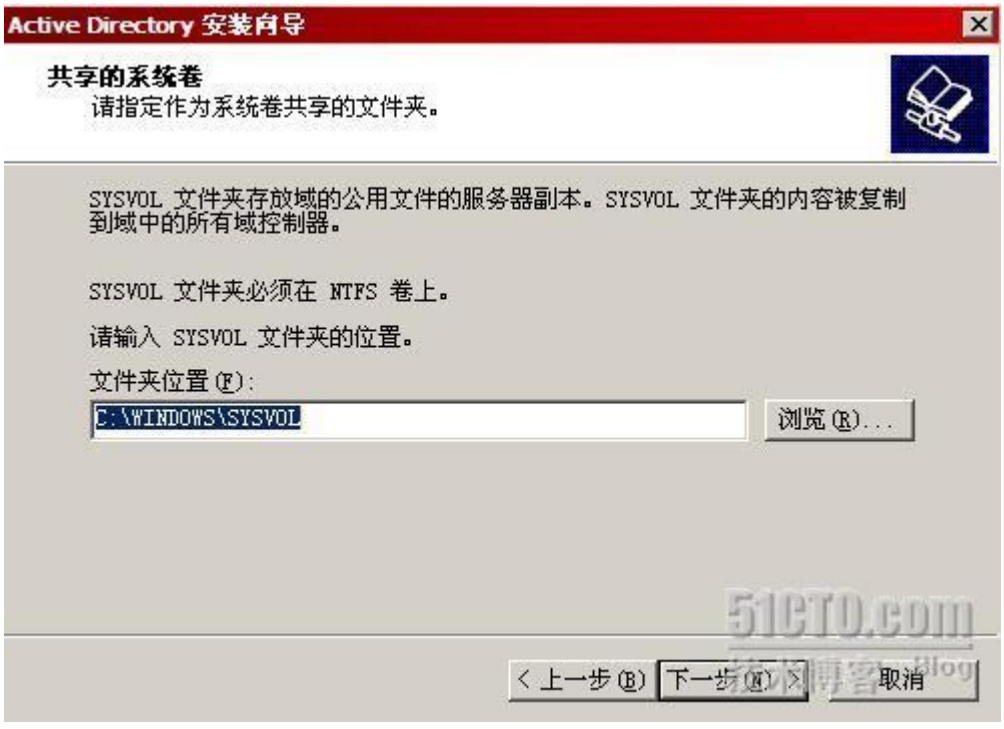
部署子域，需要得到域林管理员的授权。tet.com 是域林内的第一个域，因此 itet.com 的域管理员拥有整个域树的管理权限。如下图所示，我们用 itet.com 的域管理员完成身份验证。

父域是 itet.com，子域的名称设置为 shanghai.itet.com。

子域的 NETBIOS 名称为 shanghai。

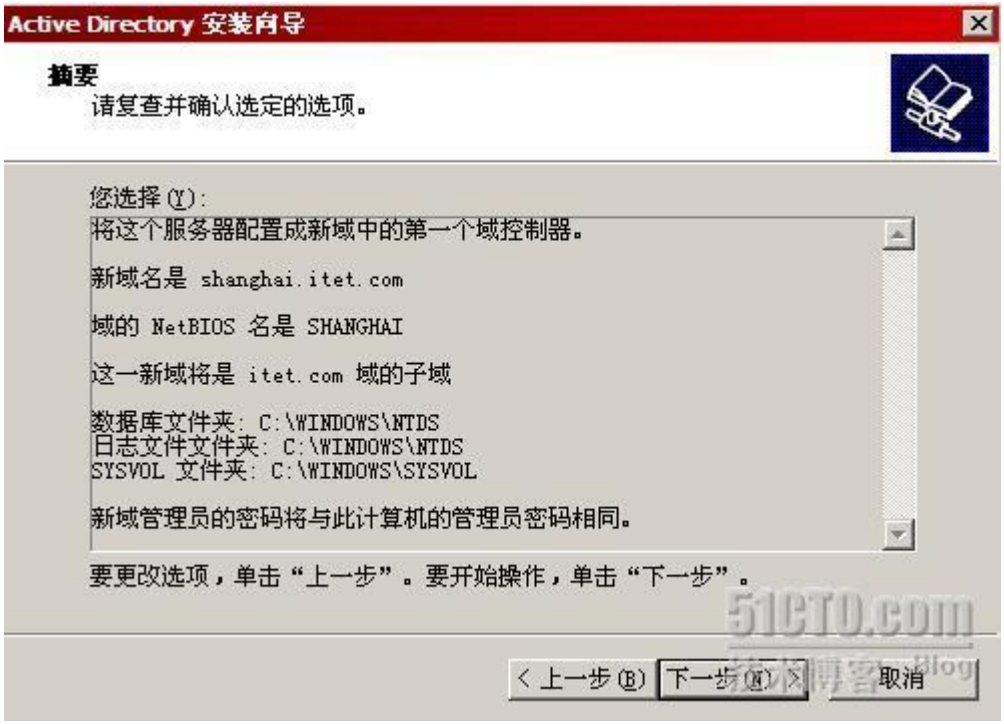
由于是在测试环境下，因此 Active Directory 数据库和日志的存储路径我们使用默认路径就可以了。

Sysvol 文件夹的路径也可以使用默认值。

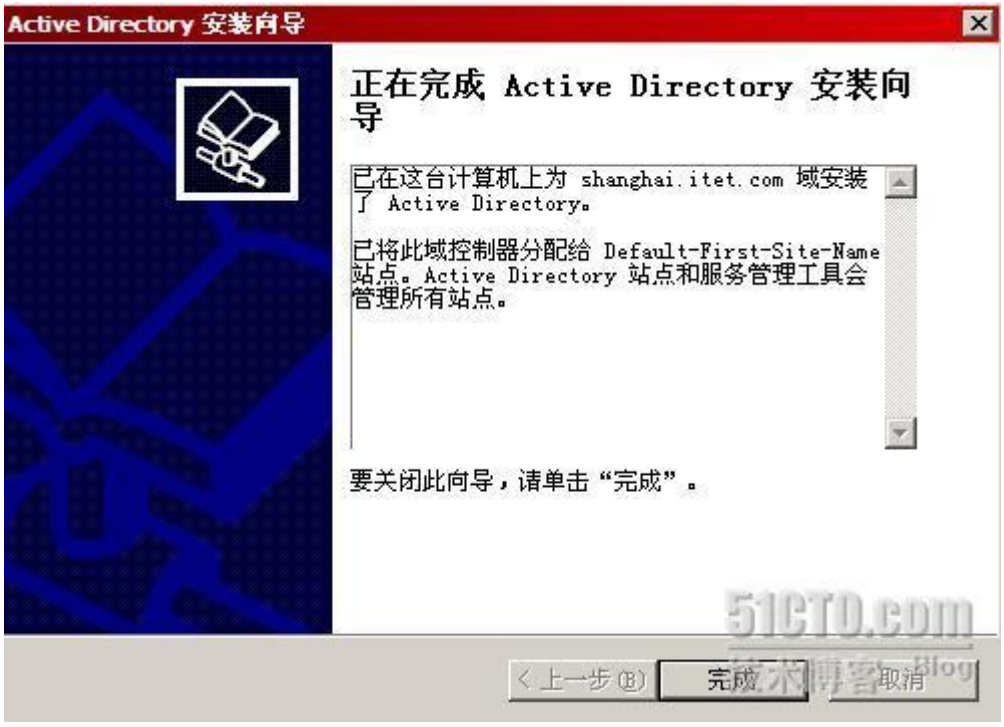


注意，下图中的DNS诊断结果已经显示出了Firenze已经为子域做好了解析准备，这说明我们之前进行的DNS准备工作是行之有效的。

摘要中显示了我们准备部署一个子域，如果摘要中的结论正确，点击下一步就可以开始子域的部署了。



经过了一段时间的部署后，子域被创建出来，如下图所示，点击“完成”就可以结束子域的部署了。



创建完子域后，我们在 Florence 上打开 Active Directory 域和信任关系，如下图所示，我们可以很清楚地看到父域和子域之间的层次关系。

利用 Active Directory 域和信任关系这个管理工具，在 itet.com 域的属性中查看域信任关系，我们看到 itet.com 和 shanghai.itet.com 之间已经自动创建出了双向可传递的信任关系。

至此，我们完成了一棵两层域树的搭建。对一般规模的企业来说，域树已经足以支持企业的管理规模了，只有对特大型企业，才有可能会使用到多棵域树。在后续的内容中我们会介绍如何在域林中加入第二棵域树。

创建可传递的林信任

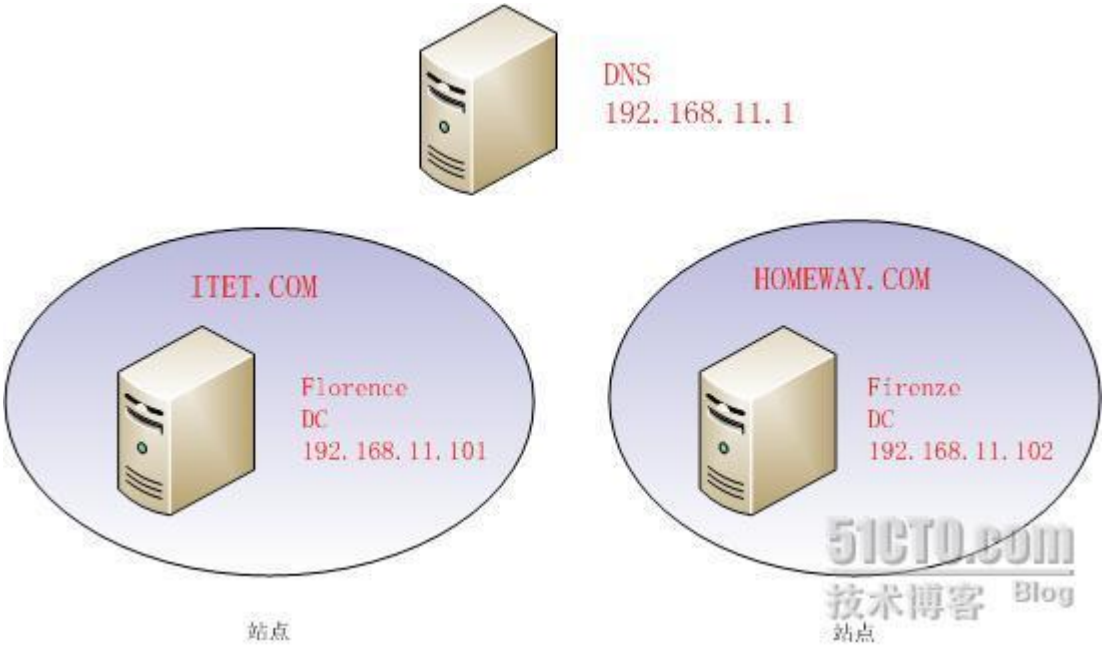
在实战详解域信任关系中，我们介绍了如何创在两个域之间创建域信任关系。实战的结果是我们在 itet.com 和 homeway.com 之间成功创建了信任关系，达到了预期目的。但我们打开域控制器上的 Active Directory 域和信任工具，可以从下图中发现，itet.com 和 homeway.com 之间的信任关系是不可传递的！这个要引起我们的关注。

如果域之间的信任关系是可以传递的，那我们就可以推论只要 A 信任 B，B 信任 C，那么 A 必然信任 C。但是域信任关系如果是不可传递的，那就会导致 A 和 C 之间没有任何信任关系，必须手工创建 A 和 C 之间的信任关系。显然，在多域的条件下，如果域的数量较多，信任关系的不可传递会给我们带来很多效率上的麻烦。例如我们可以计算一下，如果有 20 个域，每两个域之间都要创建双向信任关系，那我们就至少要创建 20*19/2=190 次信任关系，这显然也太啰嗦了！

微软对域信任关系的不可传递也给出了相应的解决方法，从 Win2000 开始，微软推出了域树和域林的概念。凡是在同一域树内的域，都会自动创建出双向可传递的信任关系。同一个域林内的域，也会自动创建双向可传递的信任关系。当微软发布 Win2003 时，微软又推出了林信任的概念，也就是说可以在两个林之间创建可传递的信任关系，把可传递的信任关系从一个林推广到了多个林。

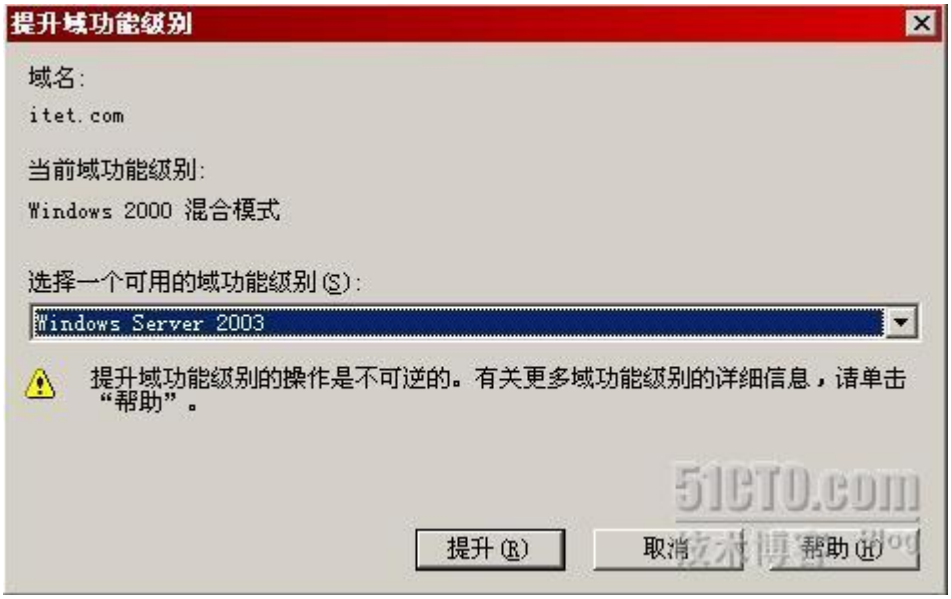
我们看到这儿时，要回忆一下实战详解域信任关系**这篇文章中的拓扑图。**拓扑如下图所示，我们会忽然意识到 itet.com 和 homeway.com 就是分别在一个单独的域林内，他们之间是域林间的关系，那我们为什么不能在这两个域之间创建可传递的林信任呢？回忆一下创建信任关系的过程，没有发现可以创建可传递的

林信任啊，为什么呢？



其实问题很简单，由于可传递的林信任只有 Win2003 才可以支持，因此我们必须把林功能级别和域功能级别都提升到 Win2003，这样才可以使用可传递的林信任这个高级特性。我们在 Florence 上为大家介绍如何提升域功能级别和林功能级别，在 Florence 上打开 Active Directory 域和信任关系，如下图所示，右键点击 itet.com，选择“提升域功能级别”。

当前的域功能级别是 Win2000，我们选择把域功能级别提升到最高的 Win2003。



然后右键点击“Active Directory 域和信任关系”，选择“提升林功能级别”。

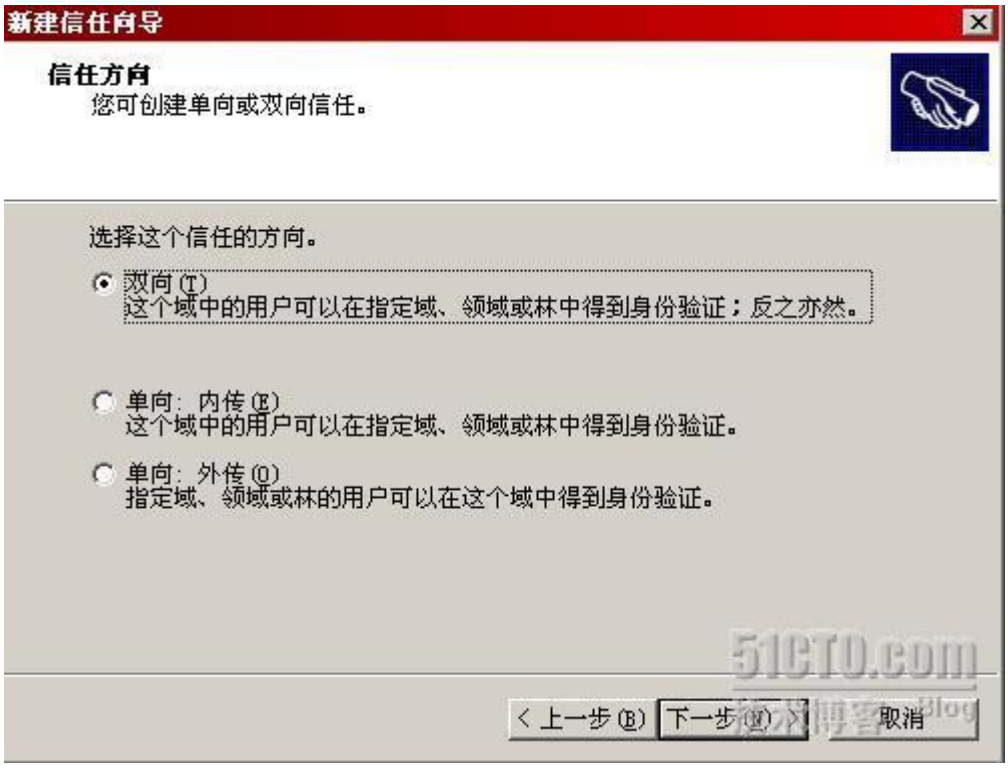
如下图所示，我们选择把林功能级别从 Win2000 提升到 Win2003，这样我们在 itet.com 上就完成了域功能级别和林功能级别的提升，然后我们在 firenze 上也对 homeway.com 进行同样的操作就可以了。

域功能级别和林功能级别提升完毕后，我们在 Florence 上打开 Active Directory 域和信任关系，如下图所示，点击“新建信任”。

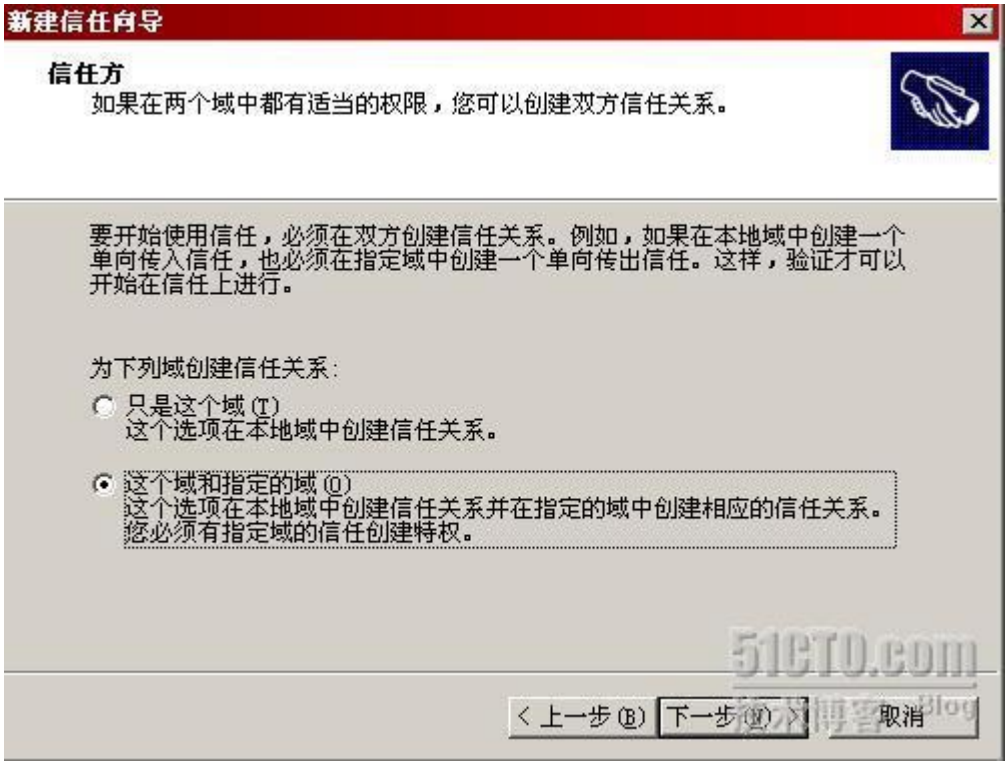
输入信任域的名称 homeway.com。

如下图所示，我们看到向导提示是创建外部信任还是林信任，外部信任是不可传递的信任关系，我们要选择创建林信任。看到这个提示，说明我们之前提升域功能级别和林功能级别成功了。

选择创建双向信任关系。

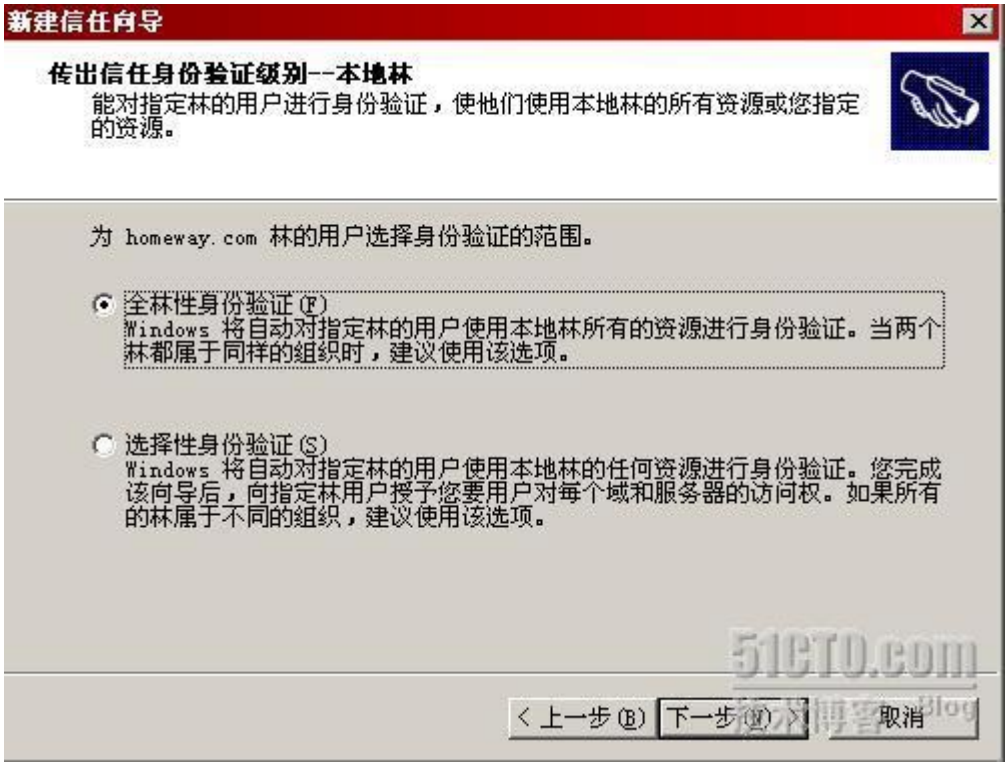


我们选择同时在两个域控制器上进行信任关系的创建，这样效率更高一些，当然，你必须知道另一个域的管理员口令。



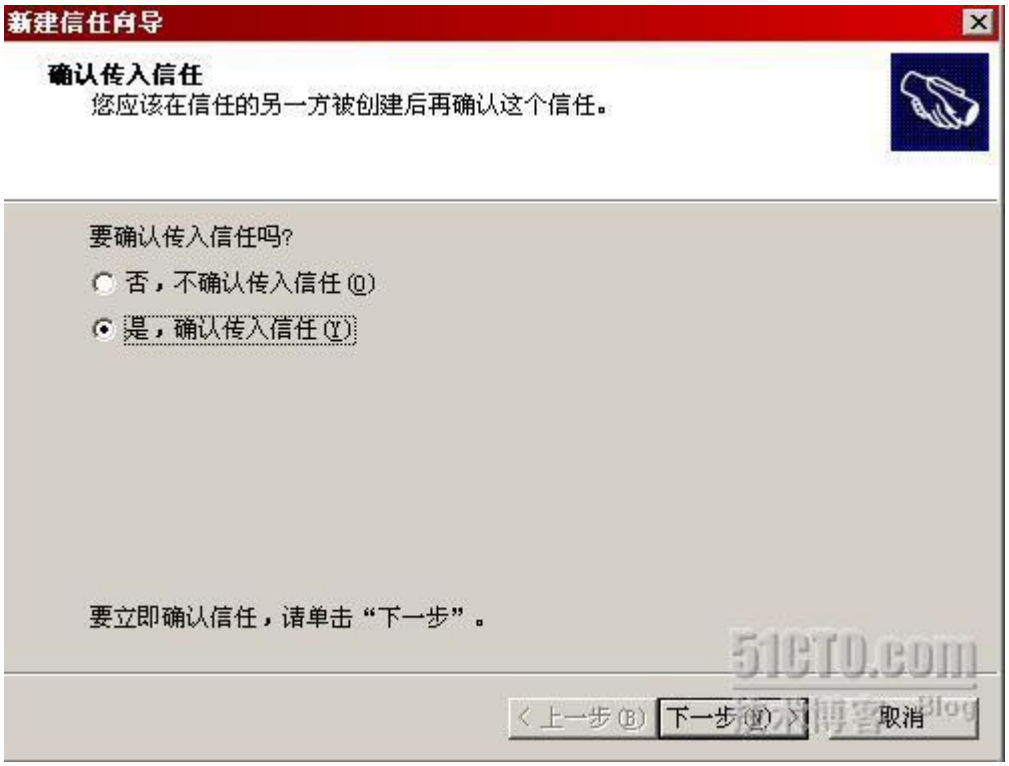
如下图所示，我们输入了 homeway.com 的域管理员口令进行身份验证。

我们选择身份验证的范围是“全林性身份验证”。



确认从 itet.com 传出信任关系。

然后从 itet.com 再传入信任关系。



如下图所示，林信任信任关系创建完毕，创建的过程其实并不复杂。

再次打开 Active Directory 域和信任关系，我们可以发现两个域林之间已经有了双向可创建的信任关系，实验成功！

初步理解组策略

组策略是 Active Directory 中非常重要的一项技术，很多朋友都听说过组策略对于管理的重要意义，也明白有些疑难问题可以用传说中的"策略"来解决。但并不清楚组策略该如何理解，如何部署，如何管理。今天起我们将组织一系列的博文为大家介绍组策略的来龙去脉，力争让大家可以更好地利用组策略来完善管理工作。

我们首先从组策略的概念谈起，什么是组策略呢？组策略是一个允许执行针对用户或计算机进行配置的基础架构。这个概念听起来有些晦涩，不太容易理解。其实通俗地说，组策略和注册表类似，是一项可以修改用户或计算机设置的技术。那组策略和注册表的区别在哪儿呢？注册表只能针对一个用户或一台计算机进行设置，但组策略却可以针对多个用户和多台计算机进行设置。这个你明白组策略的优点了吧，在一个拥有 1000 用户的企业中，如果我们用注册表来进行配置，我们可能需要在 1000 台计算机上分别修改注册表。但如果改用组策略，那只要创建好组策略，然后通过一个合适的级别部署到 1000 台计算机上就可以了。

组策略和 Active Directory 结合使用，可以部署在 OU，站点和域的级别上，当然也可以部署在本地计算机上，但部署在本地计算机并不能使用组策略中的全部功能，只有和 Active Directory 配合，组策略才可以发挥出全部潜力。组策略部署在不同级别的优先级是不同的，本地计算机<站点<域<OU。我们可以根据管理任务，为组策略选择合适的部署级别。

组策略对象存储在两个位置，链接 GPO 的 Active Directory 容器和域控制器上的 Sysvol 文件夹。GPO 是组策略对象的缩写，GPO 是组策略设置的集合，是 存储在 Active Directory 中的一个虚拟对象。GPO 由组策略容器(GPC) 和组策略模板(GPT)组成，GPC 包含 GPO 的属性信息，存储在域中每台域控制器活动目录中；GPT 包含 GPO 的数据，存储在 Sysvol 的 /Policies 子目录下。

组策略管理可以通过组策略编辑器和组策略管理控制台（GPMC），组策略编辑器是 Windows 操作系统中自带的组策略管理工具，可以修改 GPO 中的设置。GPMC 则是功能更强大的组策略编辑工具，GPMC 可以创建，管理，部署 GPO，最新的 GPMC 可以从微软网站下载。

至此，我们对组策略的功能，结构和管理工具都有了一定的了解，下篇博文中我们将通过实例为大家介绍如何对组策略进行部署及管理。