



51CTO 博客技术专家 ——活动目录配置指南系列



高金良的技术课堂

简介：国内知名培训机构讲师，从事培训行业10年以上，积累了丰富的教学经验和项目实施经验，桃李满天下。微软认证讲师（MCT）、MCSE、MCITP、MCTS，精通微软服务器的产品规划及部署。



目录

- [活动目录配置指南系列一] 基本概念
- [活动目录配置指南系列二] 单域环境的实现（单站点）
- [活动目录配置指南系列三] 多域环境的实现（单站点）
- [活动目录配置指南系列四] 单域环境的实现（多站点）--基本配置
- [活动目录配置指南系列五] 单域环境的实现（多站点）下一优化
- [活动目录配置指南系列六] 多域环境的实现（多站点）
- [活动目录配置指南系列七] 信任（上）
- [活动目录配置指南系列八] 信任（下）
- [活动目录配置指南系列九] 操作主机
- [活动目录配置指南系列十] 活动目录数据库的维护
- [活动目录配置指南系列十一] 活动目录的修复（上）
- [活动目录配置指南系列十二] 活动目录系列之十二：活动目录的修复（下）
- [活动目录配置指南系列十三] AD 的复制
- [活动目录配置指南系列十四] 实战 SYSVOL 文件夹共享丢失后的修复

基本概念

目录服务可以集中实现组织、管理、控制各种用户、组、计算机、共享文件夹、打印机各种资源等。使用 LDAP（端口 389）轻量级目录访问协议工作，在域环境下所有用户及计算机等帐户信息均保存在一个数据库中，这个数据库位置 %systemroot%\ntds\ntds.dit。

AD（活动目录）的逻辑结构包含如下组件：域/子域/树/森林/OU 等。主要侧重于对网络资源的组织。

AD 的物理结构包含如下组件：DC（域控制器）/site（站点）/OM（操作主机）。主要侧重于对网络资源的配置和优化。

下面介绍有关几个重要的概念：

1. **DN: (可辨别名称)** --用来表示一个对象在 AD 中具体存储位置，类似于文件的绝对路径。

如：cn=user1,ou=sails,dc=blog,dc=com 该用户存在 blog.com 域的 sails OU 下，用户名为 user1。

cn=users（默认的容器 users 也以 cn 表示）

dsadd user cn=test,ou=sails,dc=blog,dc=com 利用 DN 来创建用户的例子。

2. **UPN (用户主名)** 用户名@域名，即用户登录时可以采用，如 jack@net.com，也可以更改此后缀。

修改：domain.msc 后，在根右击--属性--更改 UPN 后缀，然后在用户属性-帐号中选择其后缀。用户登录可以使用此 UPN.但必须在用户属性里进行相应的更改（即启用此 Upn 后缀）

3. **SID (安全标识符)** 用户/组都有唯一

whoami /user 当前用户的 SID

whoami /all 当前用户的详细信息（包含所属组的 SID）

getsid \\dc1 test \\dc1 test (安装 suptools)

psgetsid \\dc1 test 下载工具包。

4. **AD 数据库的目录分区**：（AD 数据库虽然是一个文件，但却是以目录分区的形式组成的）

schema 架构分区 ---森林的对象类和属性，在森林级别复制。

configuration 配置分区--所有 DC 的位置、site，在森林级别复制。

domain 域分区--每个域的各种对象等信息，在域级别复制。

application 应用程序分区—DNS，可以自定义。

通过 adsiedit.msc 来查看前三个目录（事先装支持工具）

5. **site**:在物理位置上区分，一组高速可靠的一个子网或多个子网。（管理 AD 复制）

优点：

a. 优化登录

b. 优化复制

6. **域**：安全的边界，复制的单元。

7. **操作主机**：（OM）--FSMO

森林范围内唯一的有两种：

架构主机：负责森林内架构的统一 regsvr32 schmmgmt.dll

域命名主机：负责森林范围内域的添加和删除。

域范围内唯一的有三种：

RID 主机：建用户时用于分发 ID 号。

PDC 主机：时间同步，密码最小化周期、密码锁定、组策略维护等。

基础结构主机：负责跨域对象的引用和更新。

森林范围内唯一两种 OM 默认由林根域的第一台 DC 承担。



域范围内唯一的三种 OM 默认由域内的第一台 DC 承担。

以上只是一些基本概念的介绍，后期还会以专题的形式和大家一起来学习活动目录！~

单域环境的实现（单站点）

一、安装前提条件：

- *安装者必须具有本地管理员权限
- *操作系统版本必须满足条件
- *本地磁盘至少有一个分区是 NTFS 文件系统
- *有 TCP/IP 设置（IP 地址、子网掩码等、DNS 指向）
- *有相应的 DNS 服务器支持（SRV 记录）
- *有足够的可用空间 250M

二、安装：dcpromo 直接运行完成安装

*注意：一般在一个域内最好要放置多台 DC，做到冗余备份，故下面我们来看一看如何安装第二台 DC。

1. 先设置欲做为附加 DC 的计算机的 DNS 的 IP 地址指向第一台 DC 的 DNS。
2. 运行 Dcpromo 安装结束。
为了实现 DNS 的冗余，还要进行如下设置：
3. 在第二台 DC 上安装 DNS 组件。稍等一会就会自动的把第一台 DNS 的相关区域和记录复制过来。（要求第一台 DNS 必须和第一台 DC 集成在一起，必须是 AD 集成的 DNS 并允许安全的动态更新）
4. 设置两台 DC 和所有的客户机的 DNS 分别指向两个 DNS，即首选 DNS 和备用 DNS。
此时实现了 DNS 的冗余和备份功能。

案例：如果主 DC 在北京，而附加 DC 在上海，如果安装？

不可能在上海直接安装，因为这样复制流量会很大，WAN 线路不可能这么做吧，那怎么办呢？首先在北京的父域上做 AD 的备份（利用 ntbackup 来备份系统状态），把备份还原到上海一台服务器上（位置选择备用位置），再在这台服务器上搭建第二台 DC。

如：北京的 DC：ntbackup———备份“system State” 文件名：bakup.bkf，到上海的一台服务器：恢复备份到一个文件夹，然后开始运行 dcpromo /adv 找恢复目录，即可安装成功。

具体的操作，我想各位应该没有太大问题吧，自己多试几次也就 OK 了。

多域环境的实现（单站点）

在这里我只讨论单站点的情况，有关多站点下次专题再讨论。所谓单站点，只的整个森林结构在一个地理位置，如在北京。内部相连都是高速线路如 100M 等。默认的站点名字是 default-first-site-name. 可以通过“AD 站点和服务”组件来查看。

一、在一个林中创建多个域的原因？

1. 部门（或分公司）之间有不同的密码要求，可以针对部门（或分公司）创建域。
2. 有大量的活动目录对象，可以分解成多个域，使每个域活动目录对象较少。
3. 分散的网络管理，而不是由一个域管理员管理，多个域意味着有多个域管理员。
4. 对复制进行更多的控制。

二、创建子域

先完成公司的第一个域，利用 dcpromo 完成搭建工作。具体搭建情况请参考[活动目录](#)

系列之二：单域环境的实现（单站点）。下面我来谈子域的搭建：这里是实现步骤。

1. 先设置欲做为子域 DC 的计算机的 DNS 的 IP 地址指向林根 DNS。
 2. 运行 Dcpromo 安装完毕。
- **如果想让做为子域的 DC 自己来做 DNS，完成本域内计算机的解析工作，需要在父域的 DNS 上进行子域委派。具体操作如下：**

打开根 DC 的 DNS 组件，删除子域，然后新建“子域委派”，并指定委派的 FQDN 和相应的 IP 地址。

在子域的 DC 上安装 DNS 服务，并新建相应的 DNS 区域，然后将本机的 DNS 指向自己。重启 netlogon 服务。

设置子域 DNS 作条件转发指向林根 DNS。

注：子域的客户机 DNS 指向子域自己的 DNS。

****如果让父域 DNS 兼作子域的名字解析工作，可以不用作上面的操作。**

在子域内也最好安排多台 DC 作冗余。

总结：在林根 DNS 上作子域委派，在子域 DNS 上条件转发指向林根 DNS。

三、创建树

1. 先设置欲做为树的计算机的 DNS 的 IP 地址指向林根 DNS。

下面分两种情况：

如果树下面的客户机的解析由林根 DNS 负责，由事先在林根 DNS 上新建树区域。

如果想让树自己解析本域的客户机，则不必要事先建此区域。

注：如果是第一种情况，运行 dcpromo 安装完毕就结束了。

如果是第二种情况如下再继续：

2. 运行 dcpromo 安装结束。
3. 修改本机的 DNS 指向自己，重新生成 SRV 记录。
4. 运行 dnsmgmt.msc，设置 DNS 转发（条件转发 IP 地址是林根 DNS 的 IP），然后再设置“区域复制”
5. 打开林根的 DNS 服务器，新建“辅助区域”。并执行“从主服务器复制”。

注：树的客户机的 DNS 指向树的 DNS。

总结：在林根 DNS 作树区域的辅助区域，在树 DNS 上允许“区域复制”，并作条件转发到林根 DNS。

四、完成森林的逻辑结构后的优点？

- 1.可以实现整个森林范围内资源的访问，无需要输入密码。
- 2.任一域用户（不管是哪个域的）都可以在任意域的客户机上登录到自己的域。

单域环境的实现（多站点）--基本配置

在上期我们学习了[活动目录系列之二：单域环境的实现（单站点）](#)，当时我们实现的是在一个站点的情况下。下面我们来看这样一个场景：

****一个企业总部在北京，在上海和广东各有其办公区域，要求实现活动目录域环境。****

一、分析：

对于此企业的现状，在逻辑结构上可以采用多域和单域，比如我们先采用单域（这要取决于你是准备集中管理还是分散管理，在这里我采用集中管理，[下个专题我来讲多域多站点的情况](#)）。

如果不采用站点，上海和广东的域用户在客户端登录到域的过程会比较慢（不管你在上海和广东是否放置了 DC，都一样），原因是客户端会通过 DNS 查询本域内的 DC，而查到的 DC 也可能就是北京的（如果是多 DC 会动态定位），这样就通过 WAN 连到北京的 DC 上进行身份验证。此外如果你在每个地区都有 DC 的话，DC 之间的复制也是不可控的，会产生很大流量（[关于复制问题，我会在后面的专题来讲解](#)）。兼于此，我们必须划分站点。

划分站点的好处：

1. 优化客户端的登录。当域用户在上海或广东的客户端上登录时，DNS 会替客户端找本站点内的 DC，这样就加快了身份验证过程。

2. 优化 AD 的复制。每个 DC 之间要同步 AD 数据库，如果不划分站点，这个同步无时无刻都在进行，而且数据是不压缩的。如果划分了站点这个过程变的可控，特别是在多站点的情况下，优越性更加突出，我会在后面的专题中详细讨论。

附：关于何为站点，实际上就是从物理位置上来区分的，[一组高速可靠的一个子网或多个子网](#)。即两点：首先物理位置不同（在一个区域内且高速相连），其次不同站点必须采用相对应的不同子网，即北京是一个子网，上海是另一个子网，广东是第三个子网，当然也可以在北京有多个子网。具体 AD 的概念请阅读[活动目录系列之一：基本概念](#)。

二、搭建过程：

事先规划好各个子网，比如北京子网 10.1.1.0/24，上海子网 172.16.1.0/24，广东子网：192.168.1.0/24。

（一）首先在北京把单域创建好，这个过程请参考[活动目录系列之二：单域环境的实现（单站点）](#)。

（二）在上海和广东利用 dcpromo /adv 完成第二/三台 DC 的搭建，（关于此参数的使用，请参考[活动目录系列之二：单域环境的实现（单站点）](#)）。注意此时在默认站点下完成安装。

（三）完成站点的划分和设置：

打开“AD 站点和服务”管理工具（或利用命令 dssite.msc），如下图所示展开：在 default-first-site-name（默认站点）下有三台服务器，当前都在同一个站点。（N1--北京，N2--上海，N3--广东）



利用如下四个操作完成配置过程:

1. 新建站点:

新建两个站点 shanghai 和 guangzhou (北京站点用那个默认的, 过后改一下名字就可以了), 注意在新建站点时必须选中一个叫“站点连接”的东西, 先选择, 后面再说其作用。

如下图所示, 在 sites 上右击选“新站点”, 输入名字, 并选择 defaultipsitelink, 单击确定。
如下面两图:





建完上海和广东两个站点后，把 default-first-site-name 改名为 beijing。

2. 新建子网:

新建对应的子网，注意选择相对应的站点。一定不要搞错！！！！

具体操作需要在 subnets 上右击先“新建子网”，如下图所示：





最后完成如下图所示：有三个子网，分别对应相应的站点。



3.移动 DC:

把相应的 DC 移动到相应的站点。一定不要搞错！！！！

这个操作就不用做了吧，直接拖动对应的服务器（DC），拽到相应的站点下的 servers 下就可以了。最后如图所示：



说明：在上图的最右侧，大家看见了标注为<自动生成的>两个“连接对象”，这个东西就实现了 DC 之间的相互复制，它是由每个 DC 上叫 KCC 的进程自动产生的。

4. 作相应的其它配置或检查。

新建“站点连接”，即根据你的区域之间的实际物理链路来完成，默认有一个 defaultipsitelink（好像记得是这个名字）。目前这个站点链接包含了三个站点，你可以自定义。

下面说一下有关站点连接的含义。

站点链接：启用站点之间的复制传输，反映了站点之间的物理连接。

如果没有站点链接，则两个站点之间不会复制，故两边里面的所有 DC 只会在站点内相互复制。

******一个站点链接是两个站点或多个站点之间的一种物理连接。有了站点连接，在站点内才会由 KCC 自动生成“连接对象”，完成站点内 DC 之间的复制。

如下图所示：



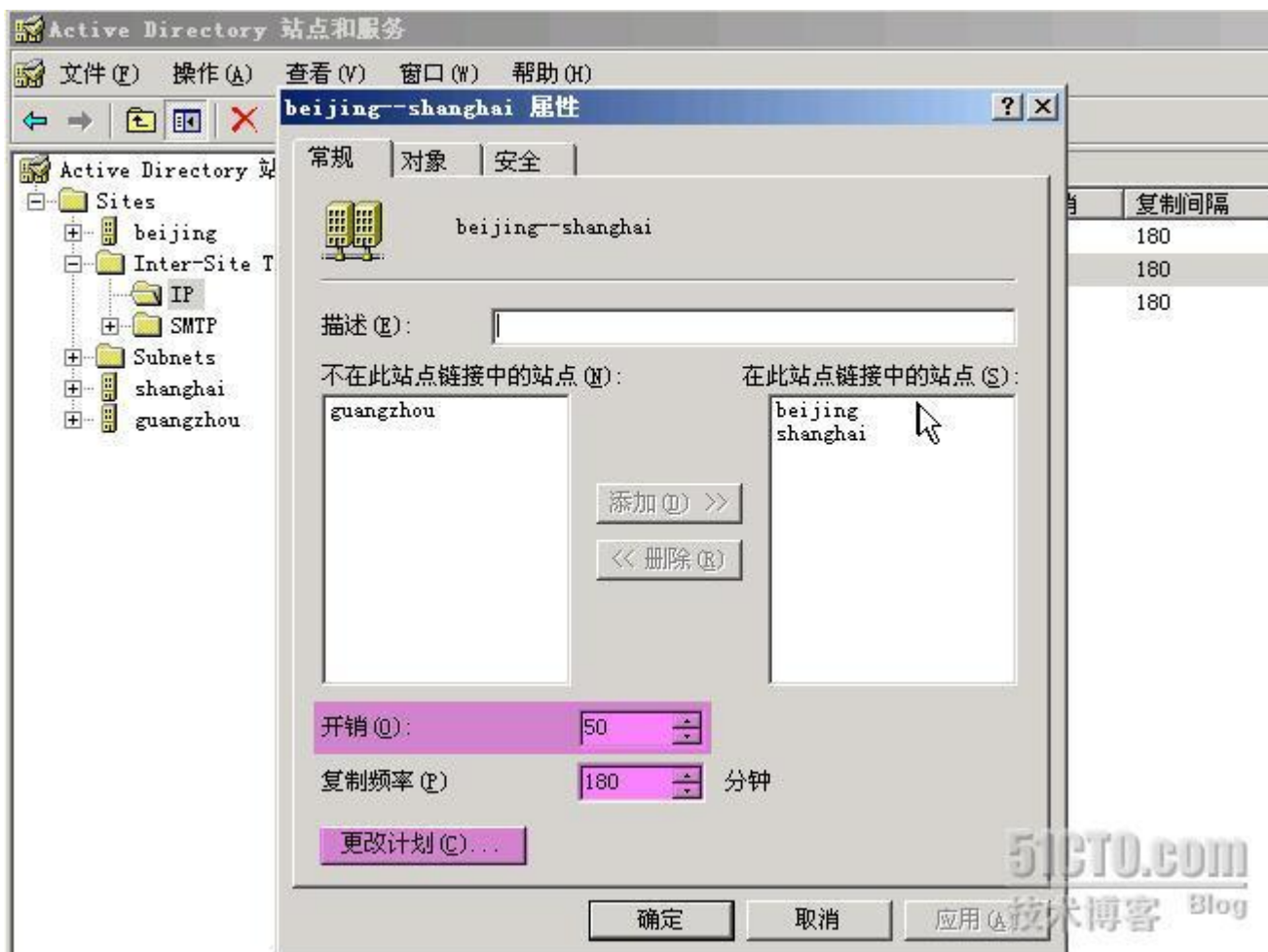
然后在下图输入相应的名字，这是北京和上海之间的站点连接。选择对并单击“添加”，这样就建好一个站点连接。如下所示：





用类似的方法完成北京和广东/广东和上海之间的站点连接,这假设你在物理上真实存在相应的链路,如果没有就不要创建了。

在下图我们编辑任一个站点连接的属性,可以设置开销值(实际物理链路带宽越高其值越小,代表线路越优先)和复制频率。这里的复制计划说明你可以让你的站点在不同的时间进行复制,如在夜间等,此处就不多说了。



最终站点的结构如下图所示：



这样部署下来，我们就实现了上述所说的各项优点！！

不知各位学的如何，看明白了吗？好累，连写代搭环境，近两个小时！希望大家顶一下！！有问题可直接留言！！

<版权所有，转载请注明出处！千山岛主>

注：如何各位想做实验，可以利用 VPC 或 VMware 自己搭建环境，不过需要用 2003 做路由器，如果要完整做下来，也包括客户端的话，需要 6 台虚拟机。哈哈，够强吧，其实各位做时可以搭建两个站点就可以了，需要 4 台虚机即可。

单域环境的实现（多站点）下--优化

通过上次[活动目录系列之四：单域环境的实现（多站点）--基..](#)的学习，我们已经完成了跨地区活动目录环境的实现，基本上也可以充分利用站点的优点，对用户登录和AD数据库的复制进行很好的管理，下面我描述一个场景，大家看如何解决？

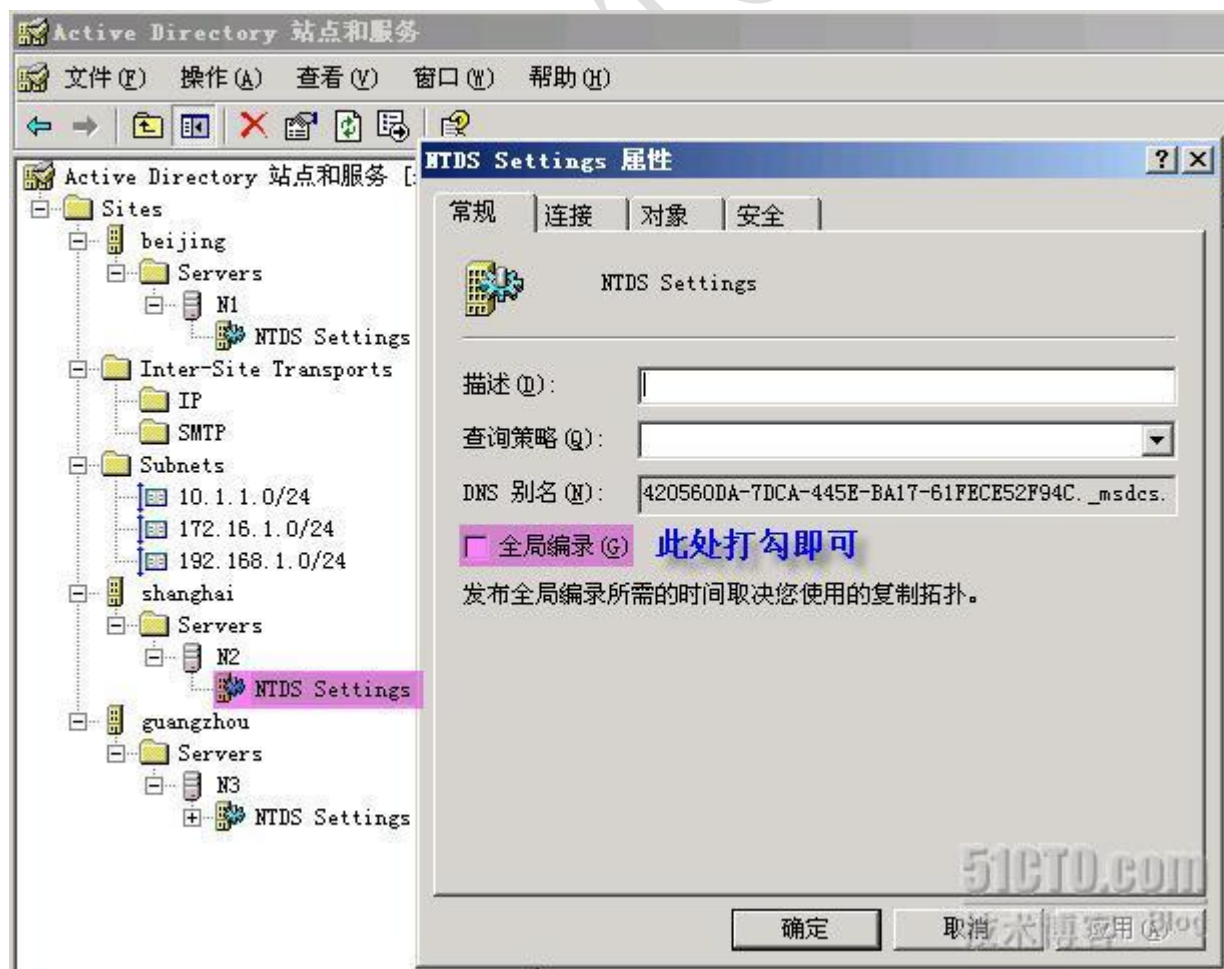
场景：根据上次我们已经完成不同地区单域环境的搭建，在北京/上海/广东分别创建了三个站点，并在每个站点布置了一台 DC（根据公司实际情况也可以放置多台 DC）。试问，如果上海和广东站点无法联系北京站点，此时用户登录是否会出问题？

分两种情况分析：

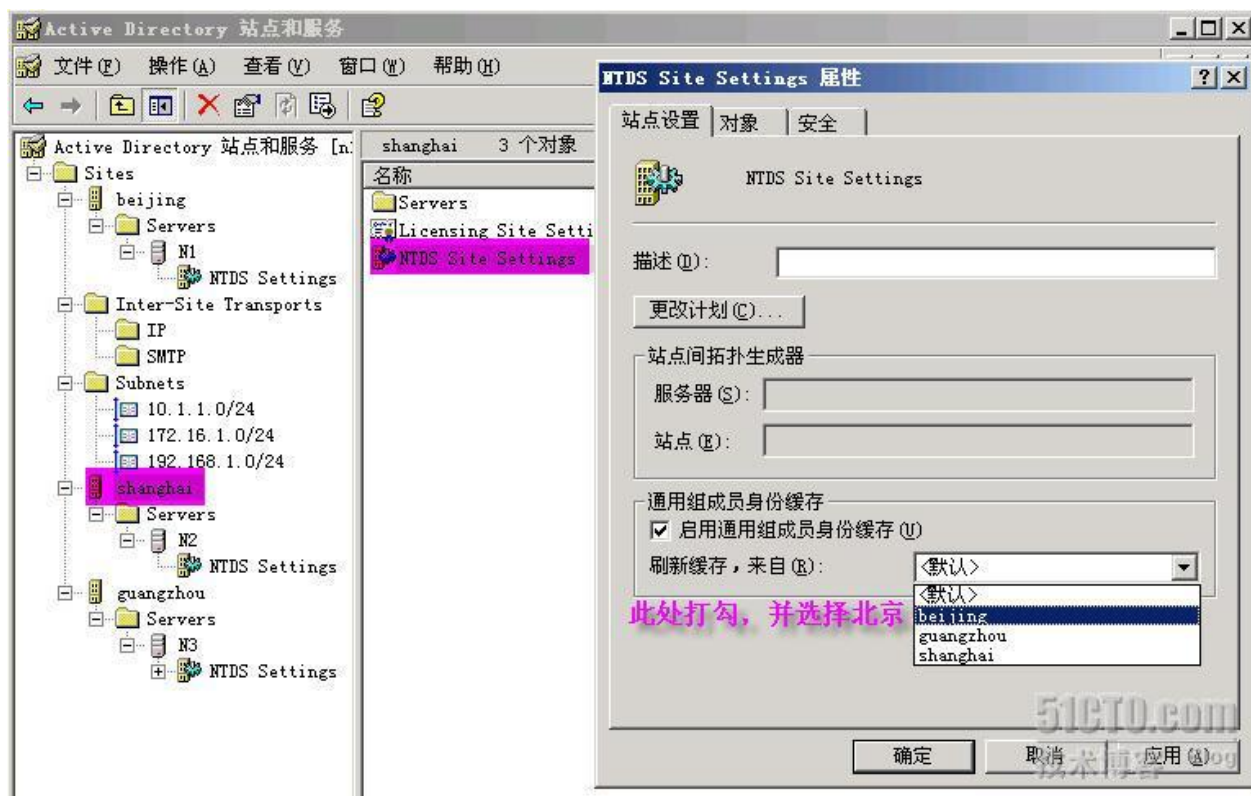
情况一：如果域的功能级别是 windows2000 mixed 模式，上述案例不用再做任何优化，不会出任何问题。

情况二：如果域的功能级别是 windows 2000 native 模式下，上述案例用户登录会出问题，甚至会出现登录不了的情况。如何操作，可参考 [《再谈域环境下用户不能登录问题!!（缓存故障）》](#) 有详细的解决方式。即如下有两种方法。

法一，分别在上海和广东的站点找一台 DC 作为 GC，默认下北京站点的 DC 已经是 GC 了。设置方法如下图所示：



法二，分别为上海和广东的站点启用“通用组成员关系缓存（来自北京站点），如下图所示：



这样，优化工作就完成了。至于为什么，我会在下篇为大家讲一下有关域用户登录过程！大家就明白。这里的两篇文章我会在后面陆续推出！！

多域环境的实现（多站点）

通过前面几期的学习，我们学习了单域单站点和多站点的设计，也学习了多域单站点的设计，今天我们来学习一下多域多站点的设计。

场景：总部在北京，上海和广东各有一个分公司，要求进行活动目录设计。林功能级别是 windows2003 模式。

一、分析：

根据公司的实际情况，我们设计三个域，北京是根域，上海和广东分别是两个子域，这是逻辑结构，在物理结构上我们设计三个站点。有关站点的具体含义，大家可参考前面的教程。

子网设计：由于每个站点必须采用不同的子网，故对于北京站点我们使用 10.1.1.0/24 和 10.2.1.0/24 两个子网，上海站点使用 172.16.1.0/24 子网，广东站点使用 192.168.1.0/24 子网。

GC 的设计：解决用户的登录问题，我们无非有两种办法，一种是在每个站点都设计 GC，第二种办法可以在本站点内不安排 GC，但要为该站点启用“通用组成员关系缓存”功能。我们可以根据实际情况来实施，至于如何实施，请大家参考前面的教程。

二、设计过程：

1. 根域的设计：在北京的 DC 上运行 dcpromo，完成 AD 的安装。如果有必要可以安装第二台或第三台 DC。并设计好 DNS，如果多台 DC，建议都设计为同时做 DNS 服务器。

2. 站点的创建：在北京的 DC 上打开 dssite.msc，创建另外两个站点，并创建相应的子网，并把相应的子网和站点结合，一定不要搞错哟！把 Default-first-site-name 改名为 beijing。

3. 两个子域的设计：在北京 DC 上做 AD 数据库的备份，并把其备份还原到上海和广东的一台服务器的一个特定目录下，在相应的服务器运行 dcpromo /adv 完成两个子域 DC 的搭建。（当然相应的子网等一定要设计正确）。这样做完后，打开 dssite.msc 后你就发现相应的站点内就有对应的 DC。

4. GC 的规则：根据情况，你可以在每个站点设计 GC，或启用“通用组成员关系缓存”。我想具体实现我就不用说了吧，参考前面的教程即可。

5. 子域委派：最后进行 DNS 的子域委派工作。这个过程请参考“[活动目录系列之三：多域环境的实现（单站点）](#)”。

三、小结：

在这个方案的设计过程中，最容易忽视的就是 GC 的设计。如果这里想着的话也就没有太多的问题的。

整个设计过程很简单，就不再一步步的图示解决了。有什么问题大家可以留言。

信任（上）

在一个森林环境中，大家想没想过一个问题，一个域用户不管来自于哪个域，它都可以做两件事：
一是可以不用输密码就可访问森林内任意域的计算机上的共享资源（当然最终能不能访问，要看权限的设置，但至少可以直接打开其计算机）。**二是**可以在任意的计算机上登录到自己的域。为什么会这样呢？这其实就是“信任关系”所最终决定的。

那么到底什么是信任呢？信任有哪些好处？

我们可以这样来理解：我信任你，那意味着什么呢？其 1 我的物品（软件资源）你可以随便使用，其 2 我的车（硬件资源）你随便开。而反之，我能用你的物品吗？不能，因为我信任你，但你并不信任我，所以我们所说的信任是有方向的。回到我们的森林环境中，如下图所示：

A 域信任 B 域，A 域就叫作“信任域”，B 域就叫作“被信任域”，这个方向就相当于从 A 作一条向 B 的箭头。那么可以实现什么呢？



1. 被信任域帐号(B 域用户) 可以具有访问信任域 (A 域) 中资源的能力。
2. 被信任域(B 域用户) 中的用户可以在信任域 (A 域) 中的计算机上登录到被信任域。

(一) 信任方向：有单向和双向两种

a. 单向分为内传和外传两种

i. 内传指指定域信任本地域:在上图中如果在 B 域上实现，就得做单向内传（中箭了~~）

ii. 外传指本地域信任指定域:在上图中如果在 A 域上实现，就得做单向外传（箭头朝外）

b. 双向：指两个域相互信任，就像两个好朋友。

(二) 2003 信任的种类：

父子信任：可传递、双向。自动建立，不可删除。

树根信任：可传递、双向。自动建立，不可删除。

快捷信任：可传递，单向或双向

林信任：可传递，单向或双向

外部信任：不可传递，单向或双向（一般在 2003 域和 NT4 域之间或两个林的任两个域之间）

领域信任：不可或可传递，单向或双向（一般在 windows 域或 Kerberos V5 系统如 Unix 之间）

(三) 查看信任关系：

打开 DC 上的 domain.msc (AD 域和信任关系)，在相应的域上右击--属性，在信任里就能看到具体的该域信任的域以及被信任的域是什么。图示就免了吧~~

(四) 林中的默认信任关系种类及特点

父子信任：在同一个域树中父域和子域之间

树根信任：在同一个林中的两个域树之间

特点：

a. 默认建立，不可删除，可传递。

b. 自动建立



林中的域之间的信任关系是在创建子域或者域树时自动创建的

c.传递信任

林中的域的信任关系是可传递的

如域 A 直接信任域 B，域 B 直接信任域 C，则域 A 信任域 C

d.双向信任

在两个域之间有两个方向上的两条信任路径

例如，域 A 信任域 B，域 B 信任域 A

（五）林间的信任关系：

林之间的信任分为外部信任和林信任

外部信任是指在不同林的域之间创建的不可传递的信任

林信任是 Windows 2003 林根域之间建立的信任

为任一林内的各个域之间提供一种单向或双向的可传递信任关系

（六）林信任的应用场合：

如果两个森林要实现信任的话，只是依靠外部信任则需要多个域之间创建，如果在两个林根之间创建林信任就 OK 了，非常适合于两个企业合并。

（七）林信任的特点及创建注意事项：

- a. 要在两个林上分别作 DNS 转发。
- b. 林功能级别为 Windows Server 2003 才能创建
- c. 只有在林根域之间才能创建
- d. 在建立林信任的两个林中的每个域之间的信任关系是可传递的
- e. 信任方向有单向和双向两种

好了，先写这些吧，下篇我分给大家讲解如何在森林之间实现林信任，而其它信任关系实现类似。

信任（下）

各位好！今天我们来学习一下如何在森林之间实现信任。通过[活动目录系列之七](#)：

信任（上）的学习，我们知道了信任的含义，也知道在森林内部存在两种不可删除的信任：父子信任、树根信任。这就是之所以我们可以在森林范围内可以无障碍的访问资源和使用资源的原因。但两个不同的森林之间如何能实现上述的这种情况呢？这就是我们今天的话题。

场景：两个森林，一个是 net.com 域，有子域 sub.net.com 是父子域，一个是 blogcn.com 域。我们要实现 blogcn.com 域信任 net.com 域，这样 net.com 域内的用户可以无需输密码即可访问 blogcn.com 域的资源，也可以在 blogcn.com 域内客户机上登录到自己的域。这种情况常出现在两个公司有合作的时候。上述可以分成两种情况：

1. blogcn.com 域和子域 sub.net.com 域存在某种信任关系。-->外部信任
2. blogcn.com 森林和 net.com 森林存在某种信任关系。----->林信任

一、blogcn.com 域和子域 sub.net.com 域存在某种信任关系。-->外部信任

这种信任关系只在指定的这两个域之间存在这种信任关系，不会传递到其它域。我们可以直接在二者之间做“外部信任”。

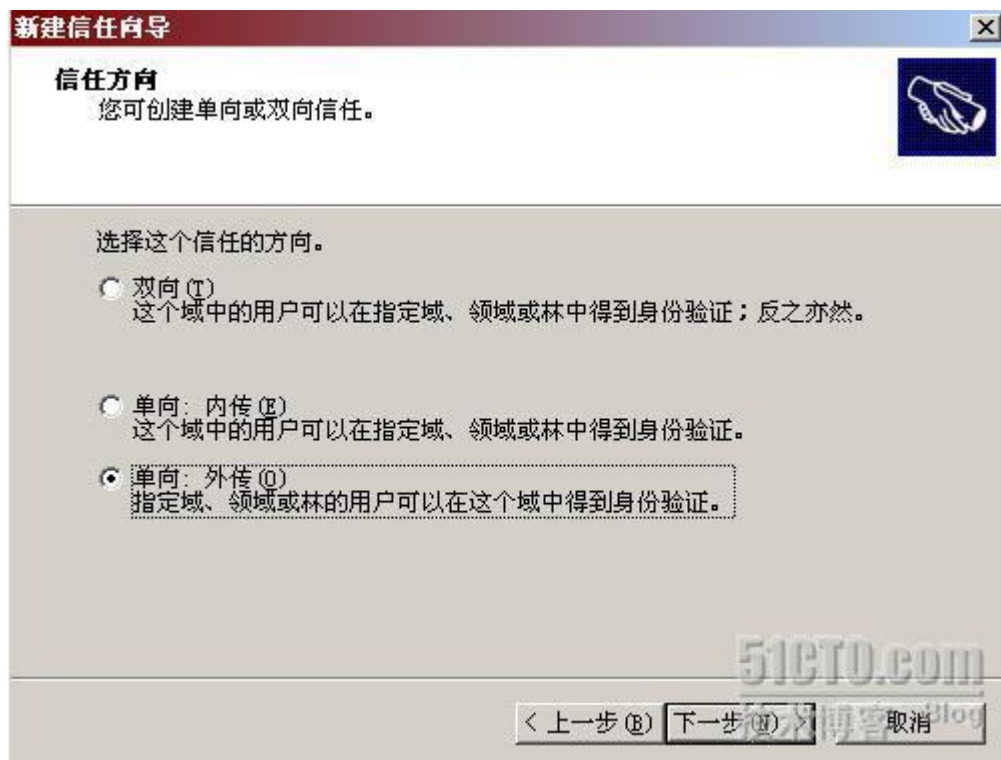
假设 blogcn.com----->sub.net.com （即前者信任后者）

完成这种信任后：sub.net.com 域内的用户可以在 blogcn.com 域上登录到自己的域，同时 sub.net.com 域内的用户可以无需输密码即可访问 blogcn.com 域的资源。

操作：

我们直接在 blogcn.com 做单向外传(箭头向外)，也可以在 sub.net.com 上做单向内传(箭头向内)。

1. 在两个域的 DNS 上作 DNS 转发，相互指向对应的 DNSIP 即可。此处就不用再赘述了吧。自己做就可以了。
2. 打开 blogcn.com 域的“AD 域和信任关系”，在 blogcn.com 域上右击选属性，单击“信任”--新建信任--在信任名称处填写“sub.net.com”，单击下一步，如图所示：



选“单向:外传”,在下一步图中选“这个域和指定的域”,继续,输入 sub.net.com 域的管理员及密码,再次单击,如下所示汇总信息:

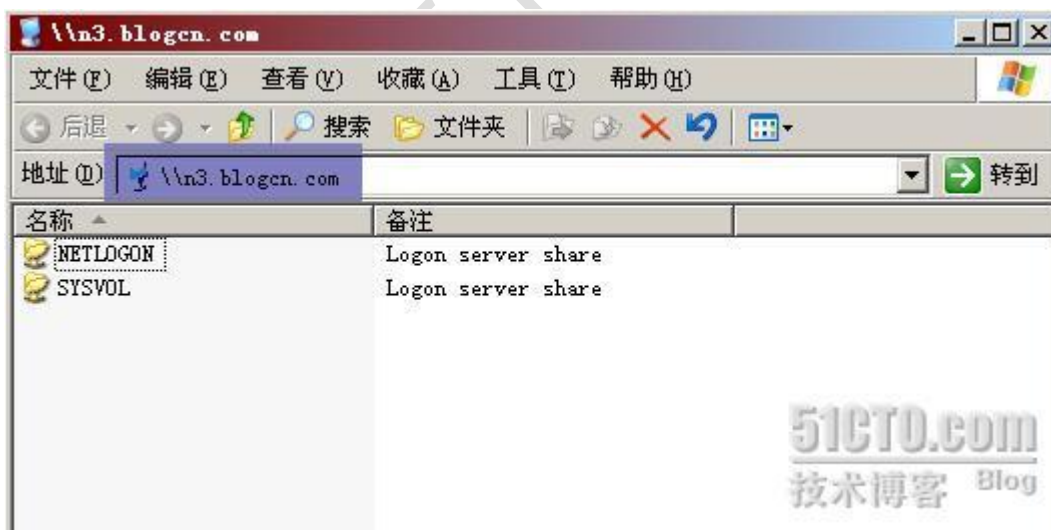


这次做的是外部信任,单击下一步,并选择“是,确认传出信任”,创建成功后,如下图所示:



做好后，我们来验证一下，访问资源和登录问题。

我们在 sub.net.com 的 DC 上利用 UNC 形式访问\\n3.blogcn.com，如下图所示：没有输密码就打开了。



登录验证：把 blogcn.com 域的 DC 注销重新登录，会发现 sub 这个域，选择 sub,并输入相应的该域的用户名和密码就可以登录进去了。当然你如果在 blogcn.com 域的 DC 上去验证还要修改相应的策略，总之这个实验我们已经成功了。



(二) blogcn.com 森林和 net.com 森林存在某种信任关系。----->林信任

我们这次实现两个森林相互信任，我们希望任意域的用户都可随意访问任意林任意域的资源等，怎么做呢？下面我们开始。

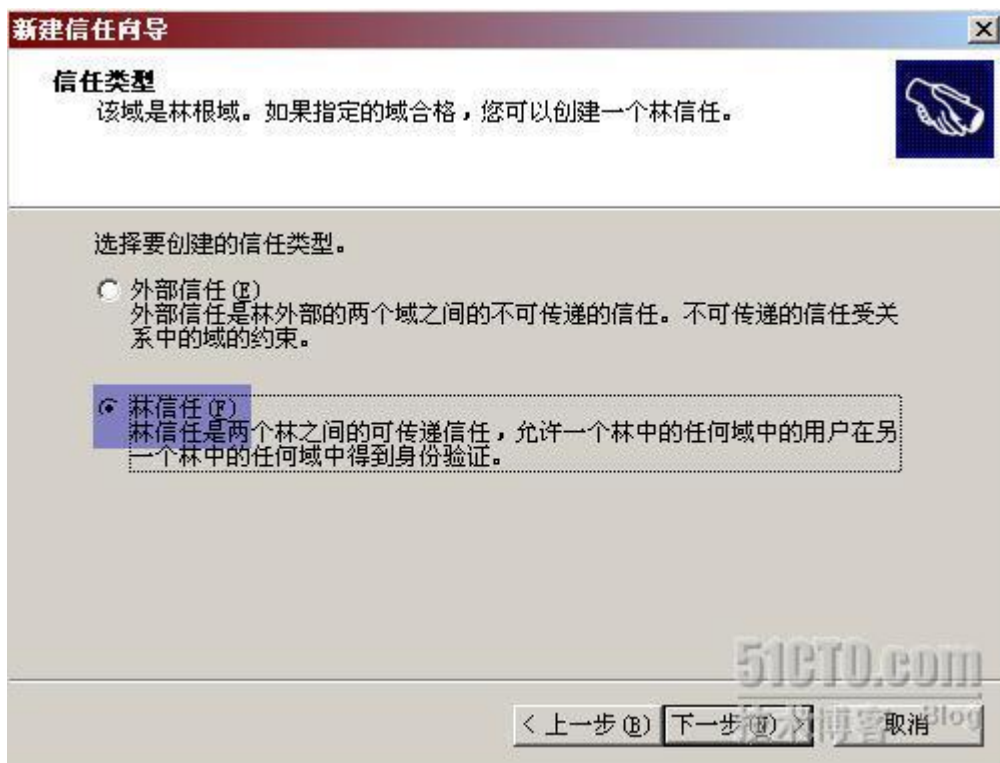
操作：

1. 首先在两个林的根 DNS 上做相互的 DNS 条件转发。此处自己解决吧。
2. 提升两个森林的功能级别全部是 2003 林功能级别。如下所示：对于 net.com 林，可以先提升 sub.net.com 子域和 net.com 域的域功能级别到 windows 2003 模式，再提升林功能级别是 windows 2003。至于如何提升，不用讲了吧，不会的话请留言。懒得写了。
3. 这次我们在 net.com 林根上来做。打开 domain.msc 后，在 net.com 上右击--属性如下图所示：



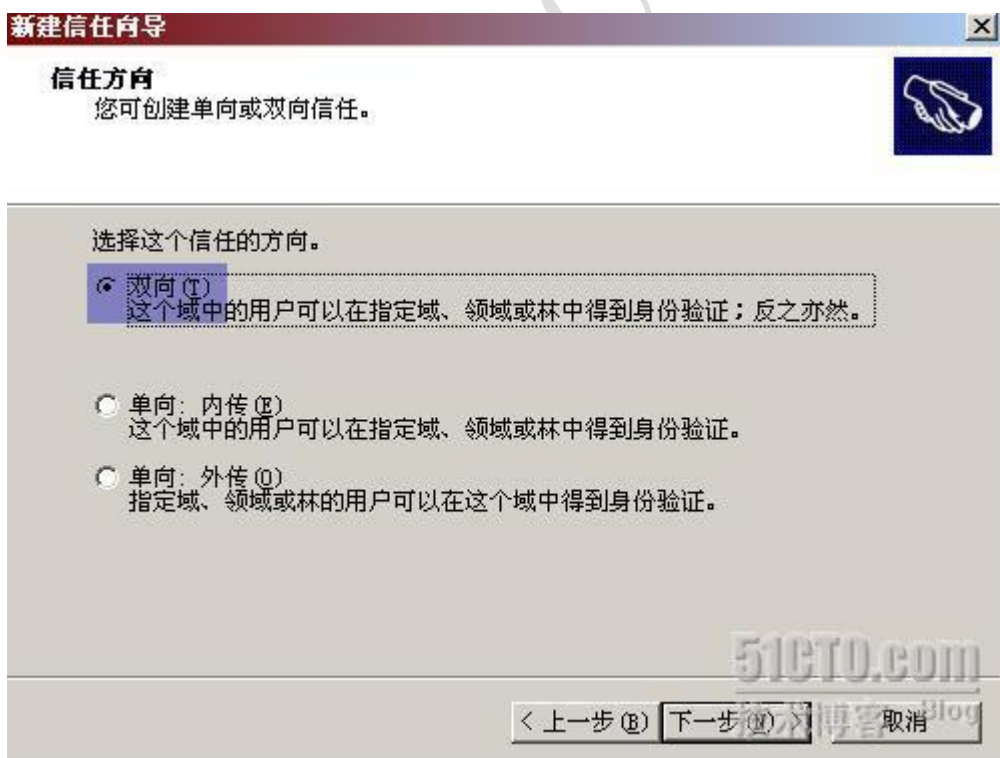
单击信任，你会发现默认的存在“父子信任”，而且不可删除，可传递的。

“新建信任”--输入 blogcn.com 这个域，再次单击下一步，出现如下图所示：

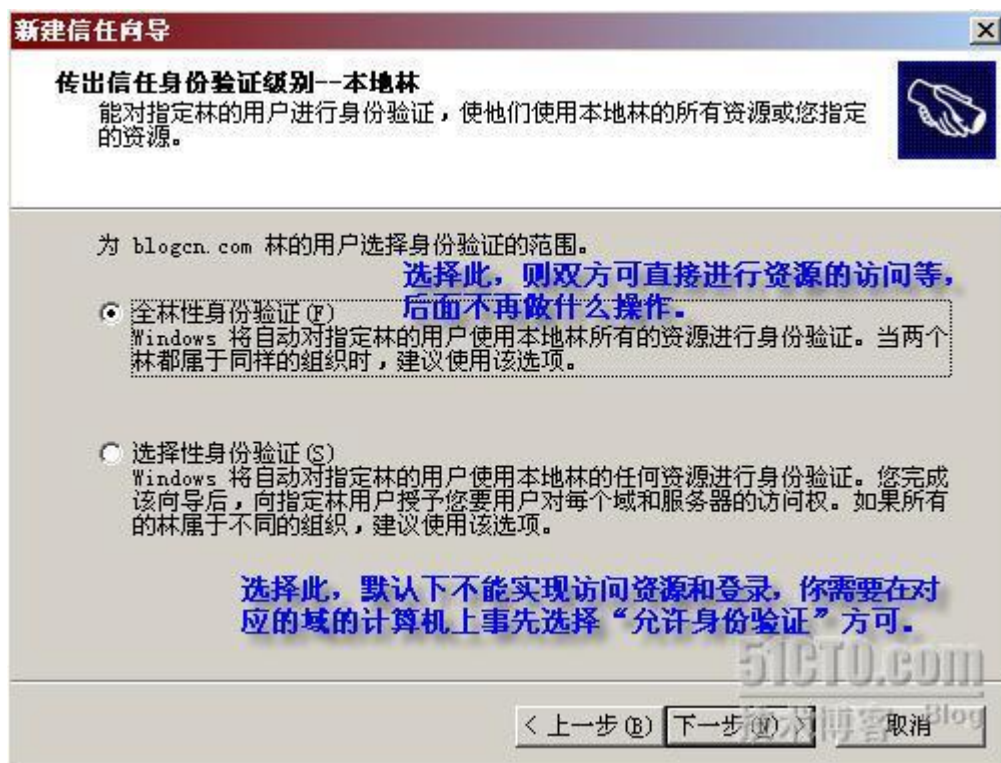


注：如果不提升林功能级别是不会出现这个提示的。

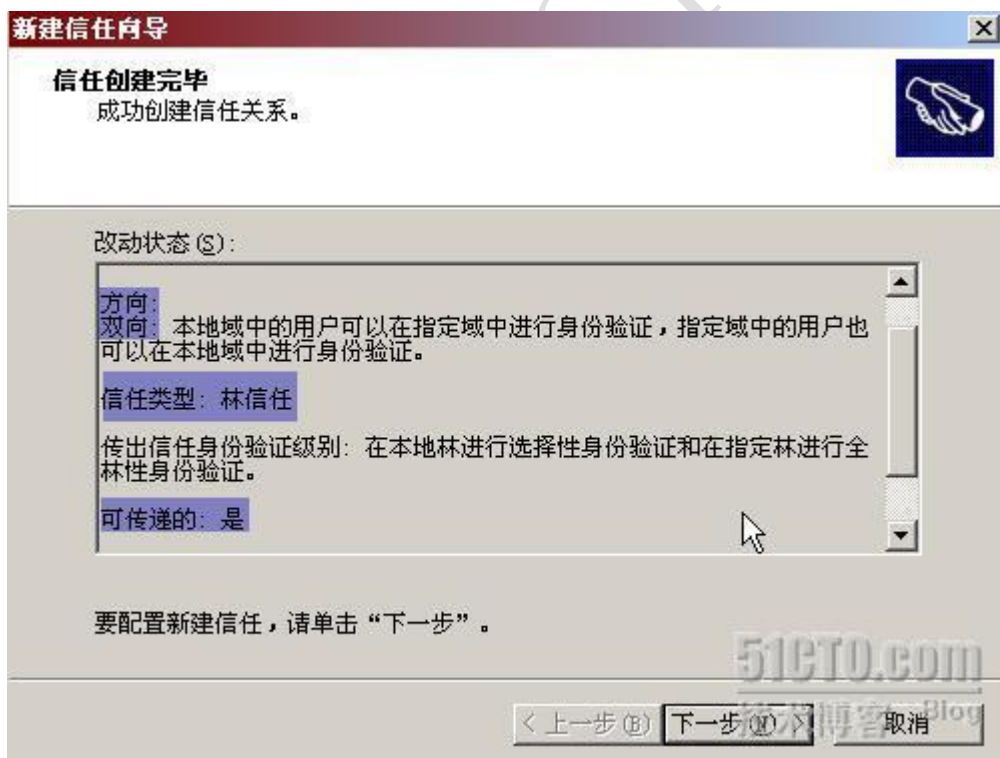
选择“林信任”，下一步，出现如下图所示：



选择“双向”，下一步，选择“这个域和指定的域”，下一步，输入 blogcn.com 域的管理员和密码，下一步，如下图所示：



为了简单，我们选择“全林性身份验证”，最后结果总述如下：



后面一定选择“是，传出信任”，最后完成后如下图所示：



其实在 blogcn.com 的 DC 上的 domain.msc 上也可以看到。至于验证就不用了。这样两个森林做到了相互信任，资源访问没有任何问题了，如果想删除信任关系，直接在上图中选中后，单击“删除”就可以了。

终于写完了，一边写一边做实验带截图，真有些麻烦。好了，下次再见了。

操作主机

今天我们讨论一下有关操作主机的问题。在域环境里，我们不得不考虑活动目录的复制问题，我们知道大多数 DC 之间的复制是一种多主复制的机制。而有一些特定的操作必须采用单主机复制，而复制的源就是操作主机。当然操作主机也是 DC，无非有着特殊的功能而矣。

（一）操作主机的角色：

Forest-wide roles: 存在于根域 DC 中

1.Schema master 架构主机

2.Domain naming master 域命名主机

Domain-wide roles: 每个域中 DC 会拥有这三种角色

3.PDC emulator PDC 仿真主机

4.RID master RID 主机

5.Infrastructure master 基础结构主机

（二）操作主机的查看：

架构主机的查看：先运行 `regsrv32 schmmgmt.dll` 后，利用 MMC 添加“AD 架构”后在根上右击选“操作主机”即可看到。

域命名主机的查看：打开 `domain.msc` 后，在根上右击选“操作主机”即可看到。

域唯一的三种操作主机的查看：右击“AD 用户和计算机”，右击域——操作主机，可以看到有三个操作主机。

或用命令查看：`netdom query fsmo`（事先安装支持工具）

（三）操作主机的作用：

1.架构主机：负责森林架构的删除和修改，如何定义 AD 数据库。比如部署 Exchange 时需要进行森林扩展，其实就是对森林的架构进行修改，这个操作必须要能联系上架构主机。

操作权限的用户必须是 `schema admins` 组的成员。

2.域命名主机：如果要新建一个域，由它来检测是否重名。

功能：控制森林内域的添加和删除；添加和删除对外部目录的交叉引用对象。

建议和 GC 配置在一台主机上。

操作权限：Enterprise Admins 组

3.PDC Emulator:

默认情况下森林中的 GC 和每个子域的第一台 DC 都是 PDC Emulator。

功能：

a.模拟 Windows NT PDC

b.默认的域主浏览器，如网上邻居的列表。

c.默认的域内权威的时间服务源

d.统一管理域帐号密码更新、验证及锁定

e.组策略存放地（默认）

4.RID master:

功能：管理域中对象相对标识符（RID）池。

一般 RID 主机会一次分给域内不同的 DC 各 500 个 RID 号，当每个 DC 用到 80%时会向 RID 主机提出申请。

5. Infrastructure master:

功能：负责对跨域对象引用进行更新。

比如本地域组中有一个其它域的用户，当这个用户被删除后，由基础结构主机负责更新这个组的

内容,并将其复制到同一个域内的其他 DC。这个更新操作由基础结构主机通过查询 GC 来完成。故在多域情况下不能把二者放在一台机器上。否则 Infrastructure master 不起作用。单域情况下不需要工作,而在多域情况下不能和 GC 在一起。

(四) 操作主机的布局原则:

考虑和 GC 的冲突、性能-----所以要更改主机。

a. 基础结构主机与 GC 不放在一起 (多域下)

b. 域命名主机与 GC 放在一起: 如果林功能级别是 win2000 模式, 二者必须在一起, 如果是 2003 模式, 可以分开。

c. 架构主机与域命名主机可放在一起

e. PDC 模拟主机建议单独放置

注意:

**一般建议: 架构主机、域命名主机、GC 可以考虑放在一起。

**PDC 单独存放。

(五) 操作主机角色的转移和占用 (图形方式和命令方式)

根据上述的分析, 我们有两种情况需要对操作主机的角色进行更改, 一种情况就是为了性能或与 GC 的冲突考虑, 在这种情况下我们要对操作主机进行转移。第二种情况就是原来操作主机的角色的 DC 发生的故障, 此时我们考虑进行强夺。下面是当操作主机出现问题时的行为考虑:

a. 当网络中的 schema master/domain naming master/RID 三种角色如果存在有故障, 则由其它 DC 来强夺, 但如果前者再恢复好, 也不要再联机, 最好格式化硬盘。

b. 当网络中的 PDC、基础结构主机这两种角色出现故障, 可以由其它 DC 强夺, 不过当前者恢复好后, 发现角色已被占用, 会自动失效, 不过可以再转移过来。

具体的操作:

1. 转移: 前提是相应的操作主机的角色在线。

比如转移 PDC 主机

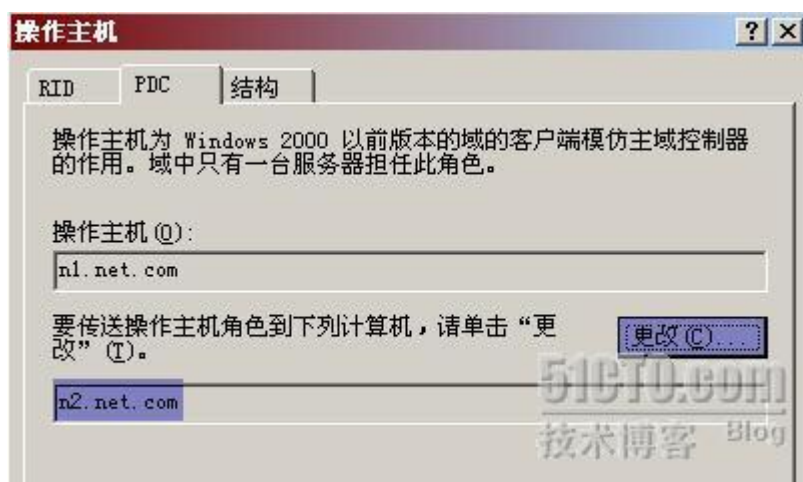
a. 利用图形方式:

打开 PDC 这台 DC 的 dsa.msc, 在域上右击--连接到域控制器 (选择欲成为 PDC 角色的 DC)

如图所示:



再次右击该域--选择操作主机--找到 PDC, 如下图所示:



单击更改，即完成的操作主机的转移工作。至于其它操作主机的转移工作类似操作。不再赘述。

b. 利用命令方式：我们把操作主机再从 n2 转到 n1，如下操作：



单击“是”，即完成的操作主机的转移工作。如上图中如果选择 **seize...** 即是强夺操作。其它操作主机的角色的更改，就不用说了吧。

2. 占用：联系不上相应的操作主机时。（尽可能用命令方式，具体要求操作如上图所示，无非选择 **seize** 行即可。此处略了吧~~~）

（六）建议：

上面五种操作操作，如果 PDC 操作主机出问题，要马上解决或进行强夺，架构主机和域命名主机出问题，可以暂不解决，先进行原有主机的修复，实在修复不了，再考虑强夺。RID 主机出现问题，在域环境相对稳定的情况下也没有大的影响，也可以先对原有主机进行修复，实现修复不了，再考虑强夺。在单域情况下，不用考虑基础结构主机。多域下如果坏了，强夺吧。

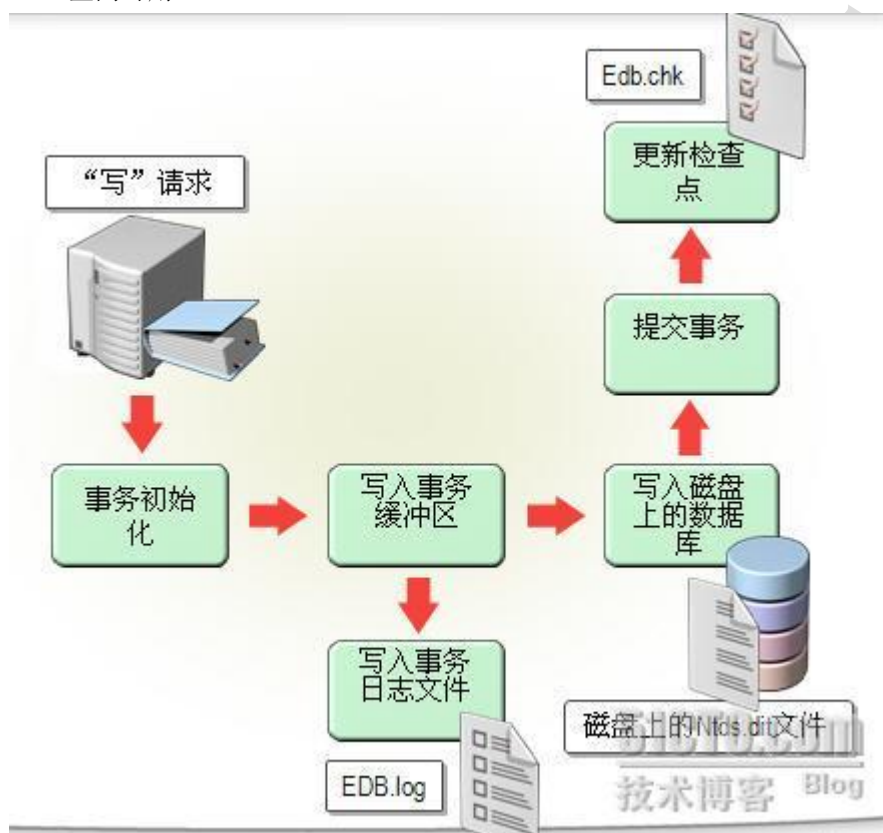
终于写完了，希望这篇文档能对各位有所帮助。

活动目录数据库的维护

今天我们来学习活动目录数据库的维护，各位都知道，在%systemroot%\ntds\下面有一个ntds.dit的文件，这个文件就是我们的AD数据库，但在这个目录下，还存在一些其它文件，试问这些是做什么的呢？再者，如果我的AD数据库出问题了，怎么来修复呢？还有，能不能把AD数据库移动位置呢？怎么对AD数据库进行优化呢？带着这些问题，我们来看今天的课程！

（一）活动目录数据的修改过程：（具体修改过程如下图所示）

在C:\windows\ntds\（如果系统装在C盘）目录下有几个文件，数据库ntds.dit，日志文件edb.log，这个文件最大是10M，当不够时会生成edb00001.log等文件，当创建或删除用户时会写入此文件，（其实首先写出缓存）然后再写入edb.log和ntds.dit，并把该操作记入edb.chk文件。当C盘空间不够时，系统会删除res1.log和res2.log两个文件，这样又有了20M空间可用。



（二）AD数据库的优化：

1. **移动AD数据库**（进入AD的恢复模式，开机F8，选目录还原模式）

应用场合：当C盘空间不够了，可以实现。

ntdsutil

files

info 查看当前数据库等信息存放的情况。

move db to d:\ 该操作适宜场合：原来C盘的空间不够了，或为了提高性能，把数据库和日志文件分开存放。

只移动的是:ntds.dit 和 edb.chk

move log to d:\ 这是移动日志文件，一般情况下可把日志文件和DB分开存放。

51CTO 博客之星-----高金良

<http://jary3000.blog.51cto.com/>

2. 压缩 AD 数据库

有两种压缩方式：一种是在线整理（由 DC 自动完成），一种是离线整理（手动进行）

a. 在线整理：DC 会每隔 12 小时自动运行所谓的“垃圾收集程序”来整理 AD 库，它只是将资料有效率的重新整理、排列。不会减小空间。此时 AD 在线。

b. 离线整理：在目录还原模式内手动进行，会压缩空间，AD 离线。

操作方式：进入目录还原模式后，

运行 ntdsutil

file

compact to d:\temp 压缩后的文件一般会变小，文件名还是 ntds.dit

然后手动复制到原来的位置，你会发现数据库变小了，而且 AD 的性能会变好。

Integrity 检查 AD 数据库文件是否有损坏。

（三）AD 数据库备份和还原：

1. 备份：对于 AD 的备份，不能单独备份，可以通过备份“系统状态”来实现。

操作：运行 ntbackup，高级模式，备份，系统状态，然后选择备份位置和文件名即可，大约需要 10 几分钟左右时间，要看你 AD 的大小了。

2. 还原：（只能还原 60 内的备份数据）分主还原、正常还原、授权还原。

a. 主还原：AD 和操作系统都坏掉了。

操作：当域内所有的 DC 都坏掉了，可以在第一台 DC 上进行主还原，然后再在其它 DC 上依次进行标准还原（正常还原），这样其它 DC 会从第一台 DC 上的数据来同步。

**主还原和正常还原一样，只不过在进行还原时，单击高级后，选择“当还原复制的数据集时，将还原的数据作为所有副本的主要数据”一项，即可结束。

b. 正常还原：AD 坏但操作系统好（F8 进入目录恢复还原模式，运行 ntbackup，还原，选择备份文件还原即可）不用演示了吧~~~~

c. 授权还原：一般对某个用户的删除进行恢复。

如果有多个 DC，之间进行多主控复制，但当你删除了一个对象，想还原之，其它 DC 的 AD 中还会有这个用户。但如果你使用正常还原，即原来备份的 AD 数据库来还原的话，由于原备份的对象的 ID 号肯定会比现存的小，所以即使你还原了，过一段时间又会消失了，怎么办呢？最好采用这里的授权还原。它可以把还原的对象的 ID 号每隔一天增加 10 万次。

具体操作如下：（还原 AD 后，不要重启，运行 ntdsutil，进行相应的操作，如下所示：）

ntdsutil

authoritative restore

restore object cn=bob,cn=users,dc=nwtraders,dc=com 如果删除的是 bob 这个用户。

Restore subtree ou=sails,dc=hp,dc=com 针对 hp.com 内的 sails 的 OU 实施强制性还原。

Restore database 授权还原整个数据库

注：你要注意，你所删除的用户或 OU 必须在备份文件中!!!

授权还原后，进入正常模式，运行

Repadmin /showmeta cn=test,cn=users,dc=hp,dc=com 可以查看版本号的变化情

况。

结束语：有关 AD 的维护就讲完了，各位还有什么问题吗？在企业环境里，记得要经常做 AD 备份，最后做备份计划！别到时你的 DC 崩了，想哭都没地方哭去~~~~

活动目录的修复（上）

在企业里，如果你的域环境出了问题，应该如何去修复呢？今天我们就来解决这个问题。

（一）修复方法

1.重建

Winnt32.exe+dcpromo.exe

2.还原

Ntbackup 还原到个好的状态（60 天）

主还原（非授权还原）

正常还原（非授权还原）

授权还原（权威还原）

3.修复

Ntdsutil 工具

（二）修复的角色

1.OM（操作主机）

架构主机

域命名主机

PDC 主机

RID 主机

基础结构主机

2.GC（全局编目）

3.DNS（域名系统服务器）

（三）案例分析：

a.案例一：

场景：单域环境，一台 DC，配置比较低。

目的：新购买一台服务器，替换掉那台老 DC。

解决办法：

- 1) 将这台新服务器提升为第二台 DC
- 2) 配置 DNS
- 3) 转移五种 OM 和 GC
- 4) 把第一台 DC 降级。

b.案例二：

场景：某单域环境中有两台 DC（DC1 和 DC2），DNS 服务在 DC1 上。某天 DC1 被强行移走不再使用。

目的：恢复 AD 环境的一致性。要求 DC2 能正常维护好 AD 环境。

解决办法：

- 1)重建 DNS（在 DC2 上）。
- 2)修复五种 OM 和 GC。
- 3)在 DC2 上清除有关 DC1 的残留信息。

附：在 DC 前上清除 DC1 的残留信息，需要使用 ntdsutil 工具，有关这个工具的使用，我附一个实例，在这里我要在 n1 上清除 n2 的信息，如下图所示：（我这里是双站点，n2 在 shanghai 站点里）

```

C:\WINDOWS\system32\cmd.exe - ntdsutil

C:\>ntdsutil
ntdsutil: meta clea
metadata cleanup: conn
server connections: con to server n1
绑定到 n1 ...
用本登录的用户的凭证连接 n1。
server connections: quit
metadata cleanup: sel op ta
select operation target: list site
找到 2 站点
0 - CN=beijing,CN=Sites,CN=Configuration,DC=net,DC=com
1 - CN=shanghai,CN=Sites,CN=Configuration,DC=net,DC=com
select operation target: sel site 1
站点 - CN=shanghai,CN=Sites,CN=Configuration,DC=net,DC=com
没有当前域
没有当前服务器
当前的命名上下文
select operation target: list domain in site
找到 1 域
0 - DC=net,DC=com
select operation target: sele domain 0
站点 - CN=shanghai,CN=Sites,CN=Configuration,DC=net,DC=com
域 - DC=net,DC=com
没有当前服务器
当前的命名上下文
select operation target: _

```

```

没有当前服务器
当前的命名上下文
select operation target: list server in site
找到 1 服务器
0 - CN=N2,CN=Servers,CN=shanghai,CN=Sites,CN=Configuration,DC=net,DC=com
select operation target: select server 0
站点 - CN=shanghai,CN=Sites,CN=Configuration,DC=net,DC=com
域 - DC=net,DC=com
服务器 - CN=N2,CN=Servers,CN=shanghai,CN=Sites,CN=Configuration,DC=net,DC=com
DSA 对象 - CN=NTDS Settings,CN=N2,CN=Servers,CN=shanghai,CN=Sites,CN=Con
figuration,DC=net,DC=com
DNS 主机名称 - n2.net.com
计算机对象 - CN=N2,OU=Domain Controllers,DC=net,DC=com
当前的命名上下文
select operation target: quit
metadata cleanup: remove sele server

```

服务器删除确认对话框



确实要删除服务器对象“

CN=N2,CN=Servers,CN=shanghai,CN=Sites,CN=Configuration,DC=net,DC=com”？这不是域“DC=net,DC=com”的最后一个服务器。

注意：此服务器应该已经永久脱机且不再返回服务。如果返回联机，该服务器对象将被恢复。

是(Y)

否(N)

单击“是”即可删除服务器 n2 了，然后再打开 dssite.msc 后，把 shanghai 站点删除，一切就 OK 了。

今天的课程就到这里了，在下篇我们再来看两个案例!!

这里的案例操作不是很详细，有关具体操作，各位可以在本站的其他文档是寻找，不再赘述！



活动目录的修复（下）

各位好，今天我们再继续两个案例。

c. 案例三:

场景：单域环境，所有 DC 全部崩溃，有备份。

目的：重新恢复域环境。

解决办法：

- 1)在第一台服务器，重装 windows2003。(在这里要求硬件配置尽可能和原来的一致，如果差别较大，大家可以参考微软的一篇文档，KB 号记不清了~~~，找到再告诉大家吧。)
- 2)重新搭建活动目录，要求域名一致。
- 3)进入目录恢复还原模式，用备份还原，进行主还原。有关主还原各位可以参考前面一篇文档：活动目录系列之十：活动目录数据库的维护。
- 4)其它服务器，用 dcpromo 提升即可。

具体工作过程就不用说了，应该比较简单，自己做做实验吧，有问题可以留言。

d. 案例四:

场景：活动目录环境，如单域有多台 DC，某天误删除了一个帐户。以前做过备份。

目的：要求恢复此用户

解决办法：（进行 AD 的授权还原）

假设所有 DC 已经同步，即该用户在所有 DC 上均已被删除。

- 1)重启其中的一台 DC，按 F8 进入目录恢复还原模式。注意输入“目录还原模式密码”，就是在安装 AD 时的那个密码。
- 2)进入 AD 的还原，做正常还原即可，还原结束后不要重启计算机。
- 3)进入 CMD 下，输入 ntdsutil 进入授权还原。具体如何进行及原因，各位可参考活动目录系列之十：活动目录数据库的维护

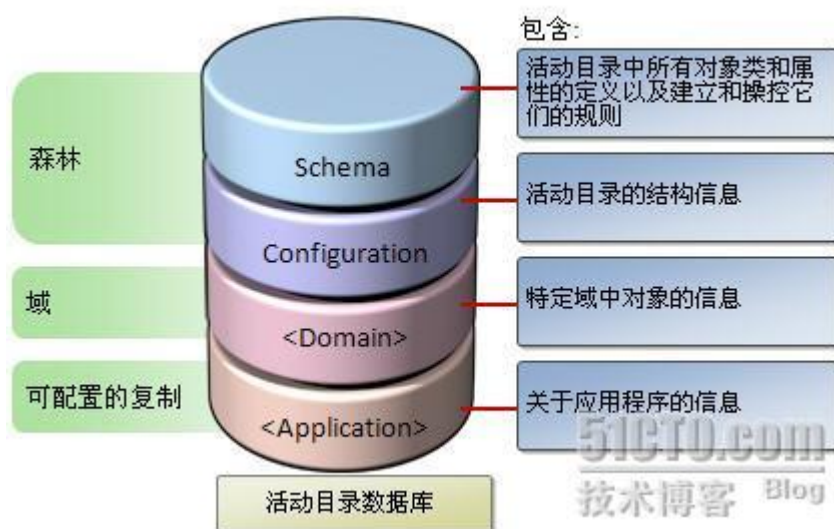
在这里我就不同赘述。

好了，有关活动目录的修复，就讲这四个案例吧，各位如有什么其他解决不了的类似案例，也可以留言，我们讨论！

AD 的复制

通过前面十二次的讲座，其实我们一直在探讨活动目录的逻辑结构较多，今天我们来谈一谈有关 AD 的复制问题。其实对于每一个 DC，都会有一个数据库文件，它就是 AD 数据库，详见活动目录系列之一：基本概念

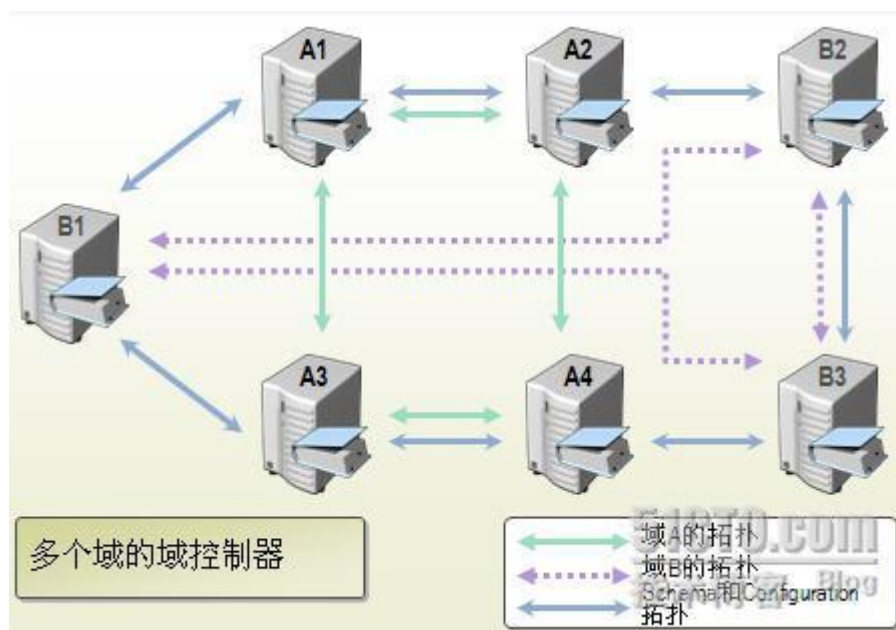
AD 数据库分四个目录分区，如下图所示：



其中在森林级别复制的是前两个分区，即架构分区和配置分区。而在域级别复制的是域分区。应用程序分区是一个可选复制，可以自己配置，在这里不讨论。

(一) 站点内部的复制

如果单域环境，同时存在多台 DC，此时每台 DC 都会同步森林及域级别的三个分区。如果多域环境，同时存在多台 DC，此时便会存在多路复制拓扑。如下图所示：

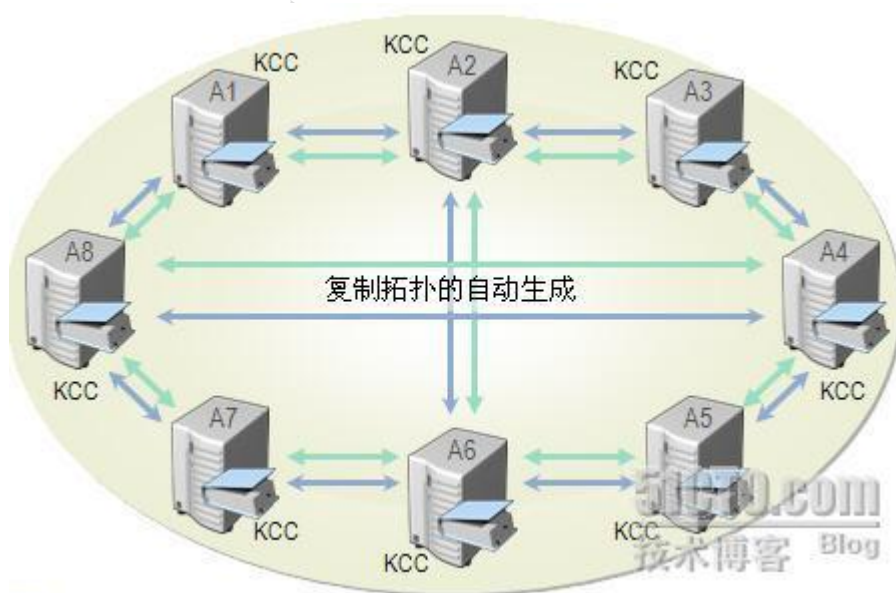


上图有三种复制拓扑，第一路是森林级别的复制，在所有的 DC 之间复制；第二路是域 A 的域分区的复制拓扑，在所有域 A 的 DC 之间复制；第三路是域 B 的域分区的复制拓扑，在所有域 B 的 DC 之间复制。如果在上图的 DC 之中还存在 GC，则上面的复制拓扑还会改变，因为 GC 是一个特殊的角色，它将拥有所有域的域分区对象及对象属性的子集。

其实大家也都看到了，我们的复制拓扑是一个双向环（保证容错），而这个环是由每台 DC 上的 KCC 进程自动生成的。

附：KCC：是一个进程，或翻译成“知识一致性校验”，它用来检查当前的 AD 环境，用于生成环形的复制拓扑。

如果在上图中再加入新的 DC，KCC 会再次计算，生成新的环。当然我们自己也可以自定义，各位可以参考下面第二个图可完成。如下图所示：



如：通过 KCC，在 A1 和 A2 之间创建一个连接对象，A2 就叫做 A1 的直接复制伙伴。如下图所示：



注意：这个连接对象是自己产生的。若自定义，可以在此完成。

AD 的复制有三种复制方式：

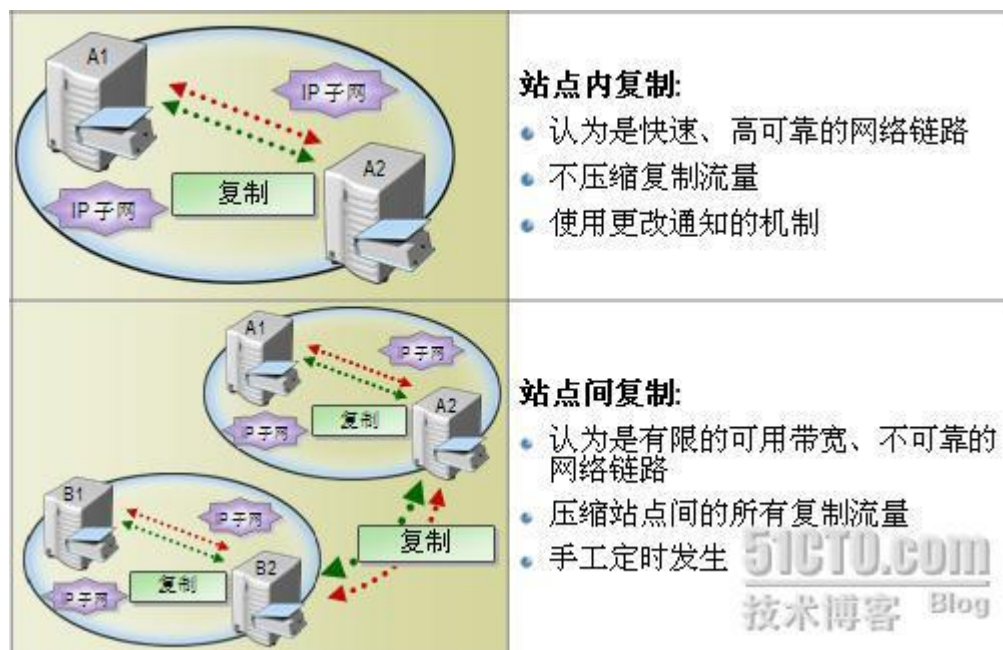
- a. **更改通知的方式**：如果 A1 上创建了一个帐号 test，则它会 15 秒后通知 A2，然后 3 秒后通知 A3、再 3 秒后通知 A4。如果 A2 收到通知后就会从 A1 把数据要过来写到自己的数据库中。这是拉复制。
- b. **紧急复制**：如密码修改、帐户锁定策略等。修改后就马上联系复制伙伴。没有时间延迟。
- c. **每隔 1 小时复制**：检查是否有数据复制遗漏。

其实在上述环中复制允许的路数不能超过 3，即 A1 把数据复制给 A2，A2 再复制给 A3，A3 再复制给 A4，就再不能间接复制给 A5 了，也就是说中间只能跳 3 跳。这个目的其实是不让复制的时间过长。大家可以仔细观察上面复制拓扑就满足这个条件。

（二）站点间的复制

如果你的企业位于两地或多地，试想根据上面的复制情况，不言而喻，DC 之间的复制流量很大，这个流量要跨越 WAN，我们不希望这样。怎么办呢，我们要控制复制。因此我们只能建站点，当然建站点的好处我们也可以**控制用户的登录流量**。详见<活动目录系列之四：单域环境的实现（多站点）--基本配置>。这样我们便可以按计划进行 AD 的复制，同时这里复制还是压缩的，基本上是原来流量的 15%左右吧。

下面我们来比较一下站点内和站点间复制的特点：



(三) 同域内复制冲突问题

有三种冲突：**属性冲突、删除的容器冲突和 RDN 冲突**

属性冲突：是指同一个对象的相同属性在两台 DC 上改的不同。

删除的容器冲突：在某个容器内添加对象或将对象转移到此容器内，但这个容器已经在另一个 DC 上被删除了。（在第一台 DC 上删除的容器还没有复制到这个 DC 之前）：此时该对象会被移动一个叫 lostandfound 的夹中，这个夹你需要打开“高级”来查看到，你可以再把这个对象移到其它容器。

RDN 冲突：是指你在两台 DC 上建两个同名用户。此时时间上后建的那个用户名会被改名。其实两个都存在。

属性值冲突的解决办法：会以戳值最高为优先。

AD 会根据对象的属性戳（stamp）来解决冲突的问题，它包括三个数据：

版本号码：初始为 1，为最先比较者。

修改时间：若版本号相同，此修改时间较后的优先。

DC 的 GUID：若上修改时间相同，会比较 GUID。高的优先。

Repadmin /showmeta DN 可以查看用户或 OU 的版本号

最后问各位一个问题，AD 在复制的时候，究竟复制那些东西呢？其实有两个：数据库本身的复制和 SYSVOL 之间的复制，而 SYSVOL 如果复制不成功，会造成组策略不生效。**有关组策略问题**，各位可以参考本站的《组策略系列》

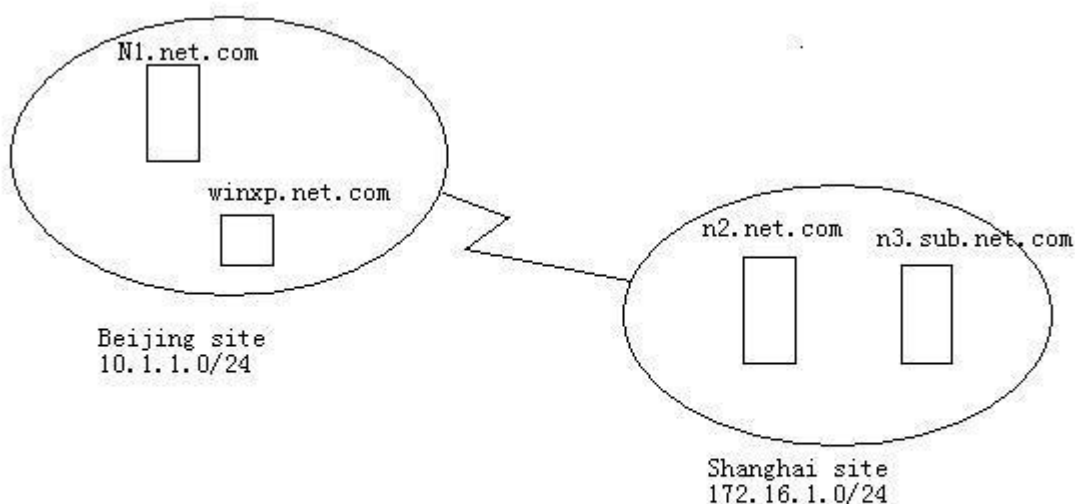
AD 的复制是一个很重要的话题，在你的企业里，如果控制不好，会造成域用户登录有问题或很慢。希望今天的内容能为各位的企业环境的管理带来一些帮助！

实战 SYSVOL 文件夹共享丢失后的修复

活动目录系列其实已经结束，但最近我在一次偶然的实验环境下，发现 SYSVOL 和 NETLOGON 两个共享文件夹突然丢失，想到这是在做了某些误操作所致，于是在这里把该系列再补上一篇，算是收尾吧。

描述一下事情发生的全过程：

我搭建了一个双站点的父子域环境，其中北京站点是有一台根 DC，n1.net.com，上海站点有第二台根 DC，n2.net.com，同时还有一个子域 DC，n3.net.com。如下图所示：

51CTO.com
技术博客 Blog

我在做完站点的相关实验后，故意将上海站点的两台 DC 全部离线，然后把北京站点 DC 的一个用户 jack 和一个 OU 名为 HR（里面有几个用户）删除，当然之前已经把 AD 做了备份，而且备份中包含用户 jack，我用了命令 `repadmin /showmeta cn=jack,ou=sails,dc=net,dc=com >c:\jack.txt` 和 `repadmin /showmeta ou=HR,dc=net,dc=com >c:\HR.txt`，把 jack 用户相关属性的版本信息及 OU 的相应版本信息保存来了，然后我把 DC 重启，按 F8 进入目录还原模式，要验证“授权还原”对用户及 OU 的版本的变化情况。

进行“目录恢复模式”后，先进行正常还原，再进行授权还原，然后重启 DC，成功登录后（发现有些慢，并没在意），然后我进入 CMD，先把 DC 上有关上海站点的信息删除，输入 `ntdsutil`，大致如下操作：

```
ntdsutil:
:meta clea
:conn
:con to server n1.net.com
:quit
:sele oper target
```

:....后面省略，各位可以参见我以前的活动目录系列有此命令的详细说明。

清理干净后，退到 C 盘根目录，我输入：

```
c:\> repadmin /showmeta cn=jack,ou=sails,dc=net,dc=com >c:\jack1.txt
```

```
c:\> repadmin /showmeta ou=HR,dc=net,dc=com >c:\HR1.txt
```

```
c:\> repadmin /showmeta cn=alice,ou=HR,dc=net,dc=com>c:\alice.txt
```

经过验证用户 jack 属性的版本值全部增加 100000 次，如下图是前后的比较：

jack.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

Originating DC	Org.USN	Org.Time/Date	Ver	Attribute
=====	=====	=====	===	=====
beijing\N1	21357	2009-03-25 10:11:15	1	objectClass
beijing\N1	21357	2009-03-25 10:11:15	1	cn
beijing\N1	21358	2009-03-25 10:11:15	1	description
beijing\N1	21357	2009-03-25 10:11:15	1	instanceType
beijing\N1	21357	2009-03-25 10:11:15	1	whenCreated
beijing\N1	21359	2009-03-25 10:11:16	2	displayName
beijing\N1	21357	2009-03-25 10:11:15	1	ntSecurityDesc
beijing\N1	21357	2009-03-25 10:11:15	1	name
beijing\N1	21359	2009-03-25 10:11:16	3	userAccountCon
beijing\N1	21358	2009-03-25 10:11:15	1	codePage
beijing\N1	21358	2009-03-25 10:11:15	1	countryCode
beijing\N1	21358	2009-03-25 10:11:15	1	homeDirectory
beijing\N1	21358	2009-03-25 10:11:15	1	homeDrive
beijing\N1	21359	2009-03-25 10:11:16	2	dBSPwd
beijing\N1	21358	2009-03-25 10:11:15	1	scriptPath
beijing\N1	21358	2009-03-25 10:11:15	1	logonHours
beijing\N1	21358	2009-03-25 10:11:15	1	userWorkstatio
beijing\N1	21359	2009-03-25 10:11:16	2	unicodePwd

jackl.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

Originating DC	Org.USN	Org.Time/Date	Ver	Attribute
=====	=====	=====	===	=====
beijing\N1	24577	2009-03-25 13:48:54	100001	objectClass
beijing\N1	24577	2009-03-25 13:48:54	100001	cn
beijing\N1	24577	2009-03-25 13:48:54	100001	description
beijing\N1	24577	2009-03-25 13:48:54	100001	instanceType
71f3-153b-4163-958d-c557a4dd9567	21357	2009-03-25 10:11:15	1	whenCreated
beijing\N1	24577	2009-03-25 13:48:54	100002	displayName
beijing\N1	24577	2009-03-25 13:48:54	100000	isDeleted
beijing\N1	24577	2009-03-25 13:48:54	100001	nTSecurityDesc
beijing\N1	24577	2009-03-25 13:48:54	100001	name
beijing\N1	24577	2009-03-25 13:48:54	100003	userAccountCon
beijing\N1	24577	2009-03-25 13:48:54	100001	codePage
beijing\N1	24577	2009-03-25 13:48:54	100001	countryCode
beijing\N1	24577	2009-03-25 13:48:54	100001	homeDirectory
beijing\N1	24577	2009-03-25 13:48:54	100001	homeDrive
beijing\N1	24577	2009-03-25 13:48:54	100002	dBSPwd
beijing\N1	24577	2009-03-25 13:48:54	100001	scriptPath
beijing\N1	24577	2009-03-25 13:48:54	100001	logonHours
beijing\N1	24577	2009-03-25 13:48:54	100001	userWorkstatio
beijing\N1	24577	2009-03-25 13:48:54	100002	unicodePwd
beijing\N1	24577	2009-03-25 13:48:54	100002	ntPwdHistory

而对于 OU 也是增加了十万次，OU 里的所有用户也都恢复了，ver 值也增加了十万次。不再图示，实验验证完毕。

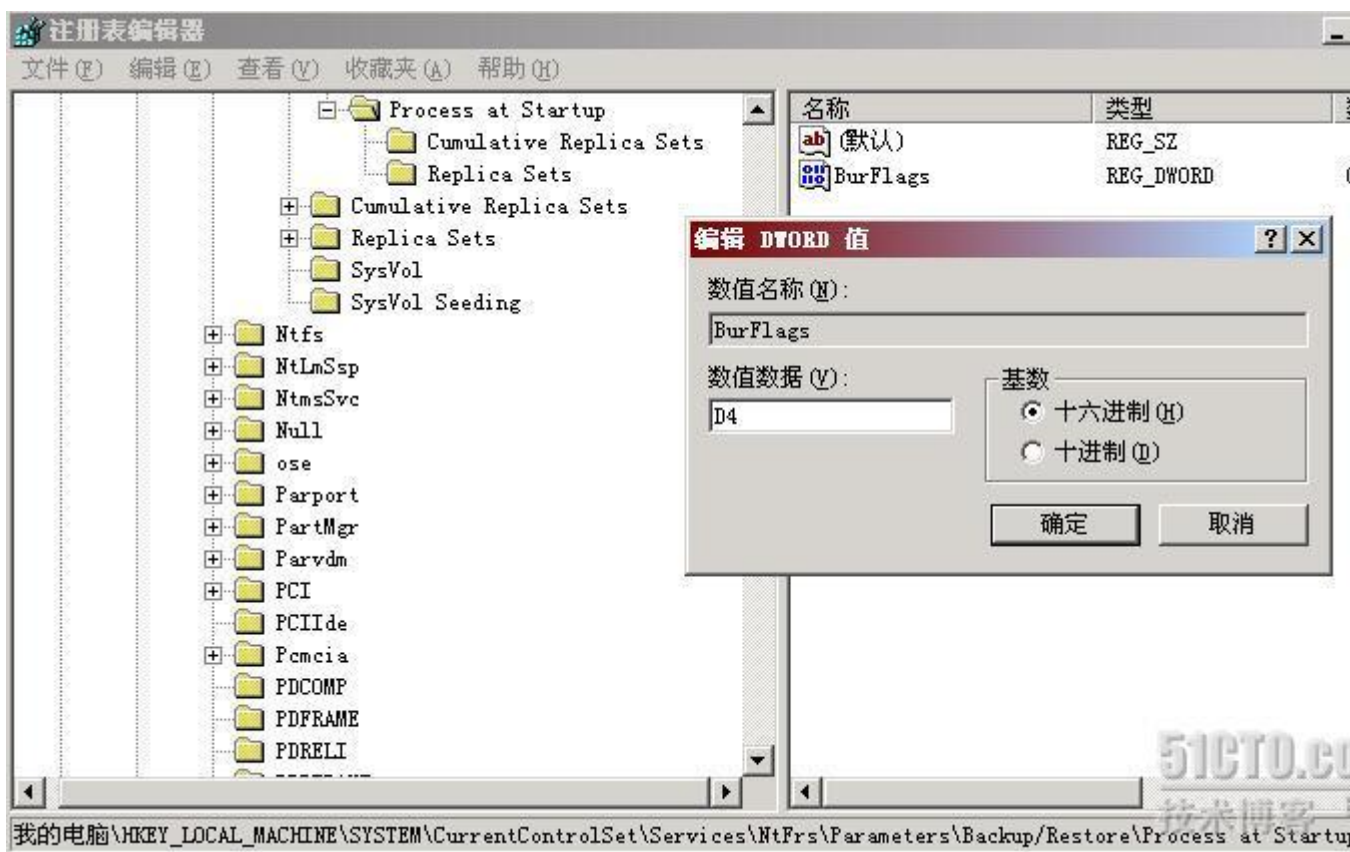
打开 dsa.msc 想看一下用户是否恢复，发现联系不上域，手动联系，成功，于时重启 DC，再次登录，这次这台 DC 应该是独立干净的 DC，想必应该登录较快，而且不会有问题。但情况并不见好转，登录比较慢，登录成功后，运行 dsa.msc，还是联系不上域，只能手动联系。打开 eventvwr.msc 查看日志发现可能 SYSVOL 共享文件夹丢失，于是查看本机，确实 SYSVOL 和 NETLOGON 全部丢失，怪不得，必须进行修复。

用过 AD 的朋友都知道，我们在安装 AD 时有一个文件夹就是 SYSVOL，而这个文件夹必须共享，这里面放的就是组策略模板，即组策略的具体设置，如果这个文件夹没有共享或丢失，那我们的域就不健康了，换句话说，组策略就加载不了了，在这种情况下，客户端登录域会很慢甚至登录不了。而 DC 当然也是一样的。

NETLOGON 里面放的是脚本，这个文件夹也必须共享。没有办法，我们只能进行修复。

为什么会丢失？怀疑是进行授权还原造成的，或进行 ntdsutil 修复 DC 造成，总之我是进行这两项操作所为，查看文件夹还存在，万幸，手动共享重启，发现不成功，只能通过修改注册表实现，如下所示操作步骤：

一、打开 DC 的注册表编辑器（regedit），修改键值如下：



修改后，关闭注册表。

二、重启相关服务：如下图

```

C:\WINDOWS\system32\cmd.exe

C:\>net stop netlogon
Net Logon 服务正在停止。
Net Logon 服务已成功停止。

C:\>net start netlogon
Net Logon 服务正在启动 .....
Net Logon 服务已经启动成功。

C:\>net stop ntfrs
File Replication Service 服务正在停止.....
File Replication Service 服务已成功停止。

C:\>net start ntfrs
服务名无效。

请键入 NET HELPMSG 2185 以获得更多的帮助。

C:\>net start ntfrs
File Replication Service 服务正在启动 .
File Replication Service 服务已经启动成功。

C:\>

```

三、查看共享，发现已经成功

```

C:\>net share

共享名      资源      注释
-----
IPC$         远程 IPC
ADMIN$       C:\WINDOWS 远程管理
D$          D:\       默认共享
E$          E:\       默认共享
C$          C:\       默认共享
NETLOGON     C:\WINDOWS\SYSTEM32\sysvol\net.com\SCRIPTS
             Logon server share
SYSVOL       C:\WINDOWS\SYSTEM32\sysvol
             Logon server share
命令成功完成。

C:\>

```

四、重启 DC。

查看事件查看器，正常。

再利用 `dcdiag /a /v` 来查看有无大的错误，无碍，问题解决。

当然如果你的 `SYSVOL` 文件夹被人为删除，这个修复工作是比较麻烦的，各位如果要实践可以参见 **Bnsen** 的《[解决灾难恢复后域共享目录 `SYSVOL` 与 `NELOGON` 共享丢失](#)》。

后记：其实今天我写这篇文档，也是想写一下解决问题的思路，各位如果没有真实的生产环境，完全可以自己模拟环境，搞坏实验环境，然后再修复，直至域环境健康。

51CTO 下载中心 业界领先的 web2.0 IT 技术资料专门下载站，拥有海量的白皮书、电子书、方案、源码等高价值技术资料，它干净整洁的界面、人性化的设计受到了广大 Down 友的广泛好评，被誉为 IT 人的“开心农场”！

51CTO 博客 面向 IT 技术人的国内主流技术博客，在这里我们关注业界动态，讨论最新技术和产品，是原创氛围最热烈的技术人网上家园。