

51CTO 博客技术专家

——为企业维护 windows server 2008 系列



宋杨的技术课堂 51CTO 博客之星 微软 MVP

简介：微软最有价值专家，资深IT 讲师。长期致力于微软产品的信息化解决方案，并成功为

一汽大众、上汽奇瑞、郑州日产等多家国内外知名企业成功整合信息化系统。

推荐阅读： [为企业部署 Windows Server 2008 系列](#)



目录

- [为企业维护 windows server 2008 系列一] 离线还原活动目录数据库
- [为企业维护 windows server 2008 系列二] 歌唱 online 活动目录数据库还原
- [为企业维护 windows server 2008 系列三] 还原意外删除的用户账户
- [为企业维护 windows server 2008 系列四] 减肥计划之 AD 数据库压缩重整
- [为企业维护 windows server 2008 系列五] 通用类别目录 Global Catalog
- [为企业维护 windows server 2008 系列六] 操作主机 PDC Emulator
- [为企业维护 windows server 2008 系列七] 操作主机 RID master
- [为企业维护 windows server 2008 系列八] 操作主机 Infrastructure Master
- [为企业维护 windows server 2008 系列九] 操作主机 Schema Master
- [为企业维护 windows server 2008 系列十] 操作主机 Domain Naming Master
- [为企业维护 windows server 2008 系列十一] 域控制器位置的选择
- [为企业维护 windows server 2008 系列十二] 组织单位的管理权委派
- [为企业维护 windows server 2008 系列十三] 为企业用户配置专有 UPN 后缀
- [为企业维护 windows server 2008 系列十四] ADMT3.1 快速迁移域用户账户和组

离线还原活动目录数据库

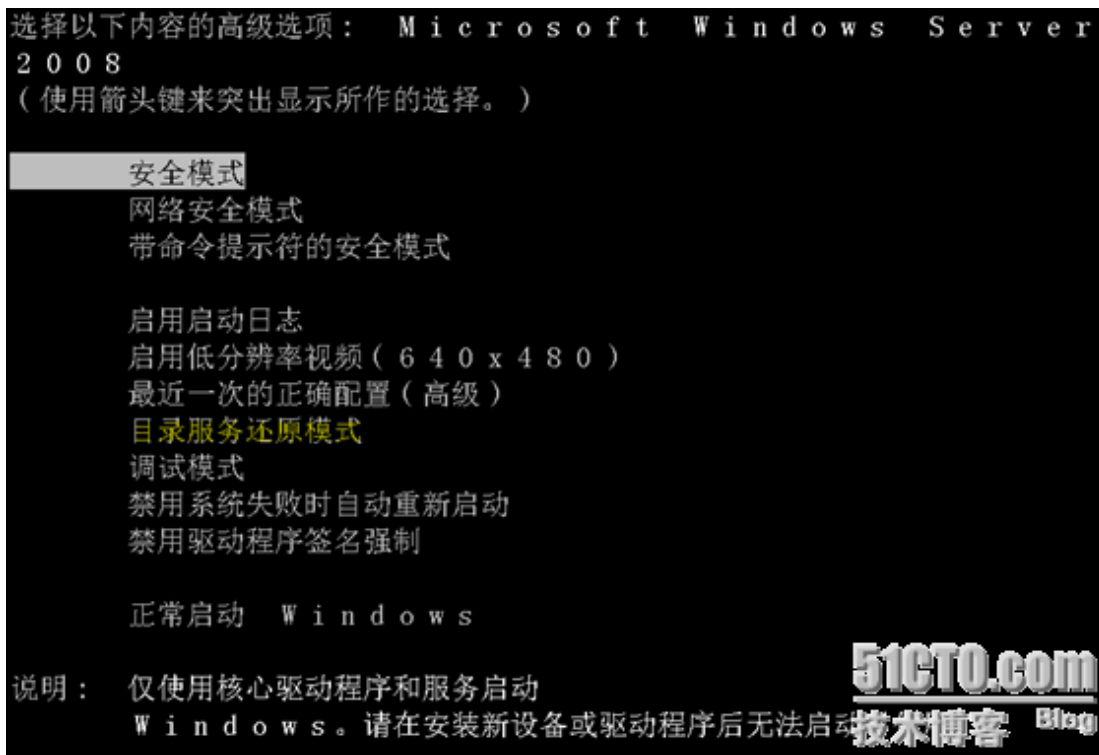
在企业基础架构环境的日常维护中，存储在域控制器上的活动目录（AD）数据是非常重要的。万一域控制器的 AD 数据库有损毁，如何进入目录服务还原模式来进行离线式的数据库还原。下面为大家做详细介绍：

假设，您已经做过备份了，具体备份步骤请看 ['AD 数据库备份\[为企业部署 Windows Server 2008 系列十五\]'](#)

首先，在正常模式下，选择开始-管理工具 打开 windows server backup 工具，可以看到我前面已经做过备份。（如果没备份那就惨了，自己写一个可以查询删除标记的工具估计能找回来，这里不详说了，有兴趣的朋友留言交流。）



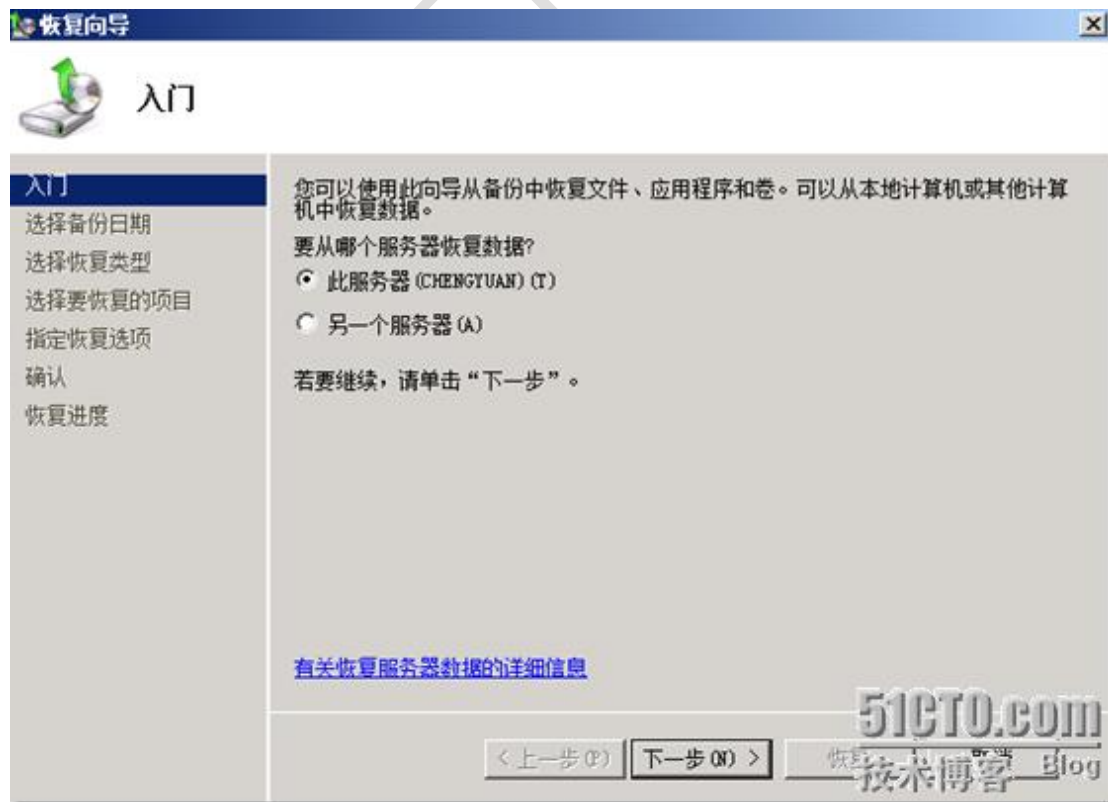
有了上面的备份，我们就可以进入目录服务还原模式来对活动目录进行还原了（因为正常模式时，活动目录服务处于运行状态，所以数据库正在被调用，所以无法在这时对活动目录数据库进行还原。进入目录服务还原模式，此时目录服务处于离线状态，也可以理解为活动目录数据库处于冻结状态，那么我们就可以对活动目录数据库进行还原了。）于是我重新启动域控制器，在 bios 画面时按 F8，出现如下画面，



选择目录服务还原模式，按 enter。

在登陆画面输入目录还原模式的管理人员密码（当初在 DCpromo 的时候设置的，不同于域管理员）。

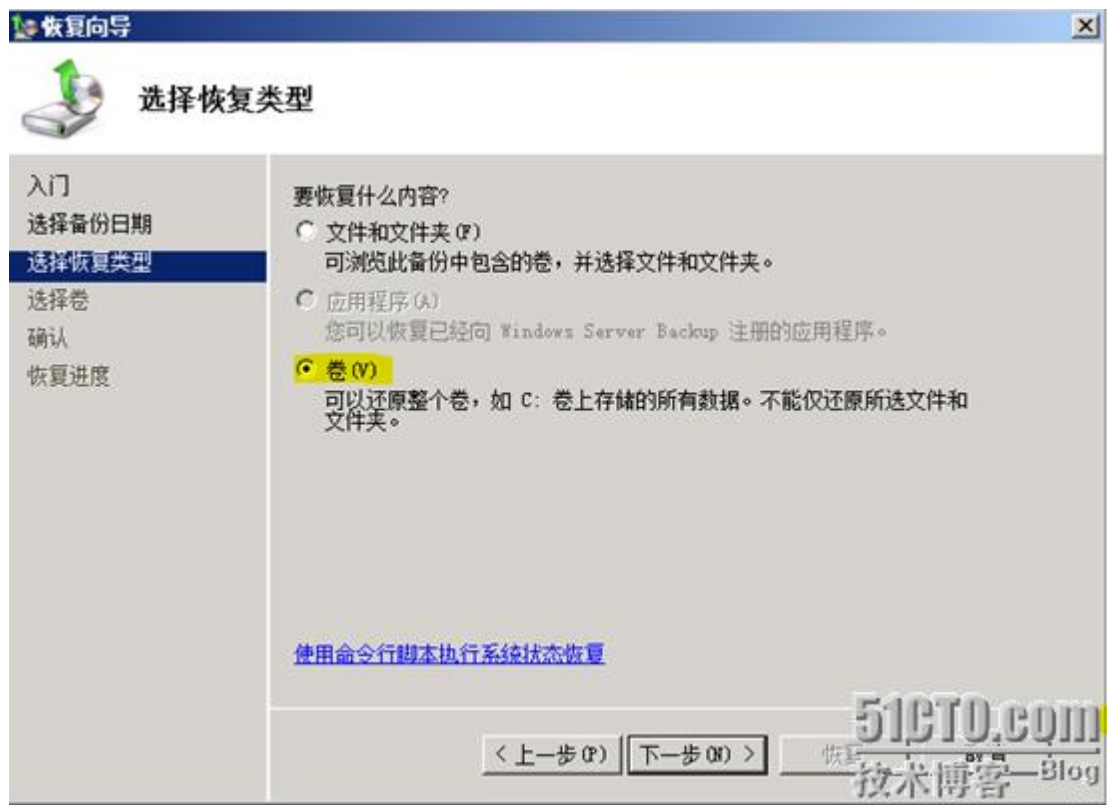
登陆后打开 windows server backup 工具，选择右边'操作窗口'中的'恢复'，弹出'恢复向导'。



选择此服务器，下一步，



可以看到以前做过的可用备份，这里我做过三次，一次是 2009 年 9 月 10 日 11: 00，一次是 2009 年 9 月 18 日 23: 00，一次是 2009 年 9 月 18 日 23: 20。我选择最近的一次。



选择恢复内容是整个 C 盘，下一步后提示无法执行，因为 C 盘现在正在使用，这里提示如果要还原系统状态（域控制器的系统状态中包含活动目录数据库），只能使用命令行工具 'WBADMIN' 来实现。



下面我们打开命令提示符，输入 `wbadmin` 后按 `enter` 可以看到提示 `start systemstaterecovery` 运行系统状态恢复，

```
管理员：命令提示符
C:\Users\administrator.WGS>wbadmin
wbadmin 1.0 - 备份命令行工具
(C) 版权所有 2004 Microsoft Corp.

错误 - 命令不完整。请参阅以下列表。
要获得其他帮助信息，请键入 wbadmin <command> -help

---- 支持的命令 ----

ENABLE BACKUP          -- 启用或修改每日计划备份
DISABLE BACKUP          -- 禁止运行每日计划备份
START BACKUP            -- 运行备份
STOP JOB                -- 停止当前正在运行的备份或恢复
GET VERSIONS            -- 列出可从特定位置恢复的
                        -- 备份详细信息
GET ITEMS                -- 列出备份中包含的项目。
START RECOVERY           -- 运行恢复
GET STATUS              -- 报告当前正在运行的作业状态
GET DISKS                -- 列出当前联机的磁盘
START SYSTEMSTATERECOVERY -- 运行系统状态备份
START SYSTEMSTATEBACKUP  -- 运行系统状态备份
DELETE SYSTEMSTATEBACKUP -- 删除系统状态备份
```

在上图中，还有一个很关键的提示：get versions 列出备份详细信息

```
C:\Users\administrator.WGS>wbadmin GET VERSIONS
wbadmin 1.0 - 备份命令行工具
(C) 版权所有 2004 Microsoft Corp.

备份时间：2009/9/10 11:00
备份目标：网络共享，标记为 \\172.16.0.1\share
版本标识符：09/10/2009-03:00
可以恢复：卷， 文件， 应用程序， 裸机恢复， 系统状态

备份时间：2009/9/18 23:00
备份目标：1394/USB 磁盘，标记为 新加卷(E:)
版本标识符：09/18/2009-15:00
可以恢复：卷， 文件， 应用程序， 裸机恢复， 系统状态

备份时间：2009/9/18 23:20
备份目标：1394/USB 磁盘，标记为 新加卷(E:)
版本标识符：09/18/2009-15:20
可以恢复：卷， 文件， 应用程序， 裸机恢复， 系统状态
```

从上图中可以看到我备份三次的状态，这里重点需要复制版本标识符，因为恢复的时候需要靠这个标识符来定位备份文件。

拿到了标识符，我们开始使用 'wbadmin start systemstaterecovery -version: 版本标识符' 的方式来还原系统状态。

```
C:\Users\administrator.WGS>WBADMIN START SYSTEMSTATERECOVERY -version:09/18/2009-15:20
wbadmin 1.0 - 备份命令行工具
(C) 版权所有 2004 Microsoft Corp.

是否要启动系统状态恢复操作?
[Y] 是 [N] 否 Y
```

键入 Y，再按 enter 后开始还原系统状态：

```
启动系统状态还原 [2009/9/19 0:13]
正在处理要还原的文件<这可能需要几分钟时间>...
已处理<126>文件
已处理<539>文件
```

等待还原完成后，就可以重新开机了。

以上我们介绍了 AD 数据库的离线式还原，在下次我会跟大家介绍另一种还原方式。

歌唱 online 活动目录数据库还原

我宁愿你冷库到底...让我死心塌地忘记...我宁愿...（半夜三更，灯火通明的机房里，一个正在做活动目录数据库还原的新人歇斯底里...）

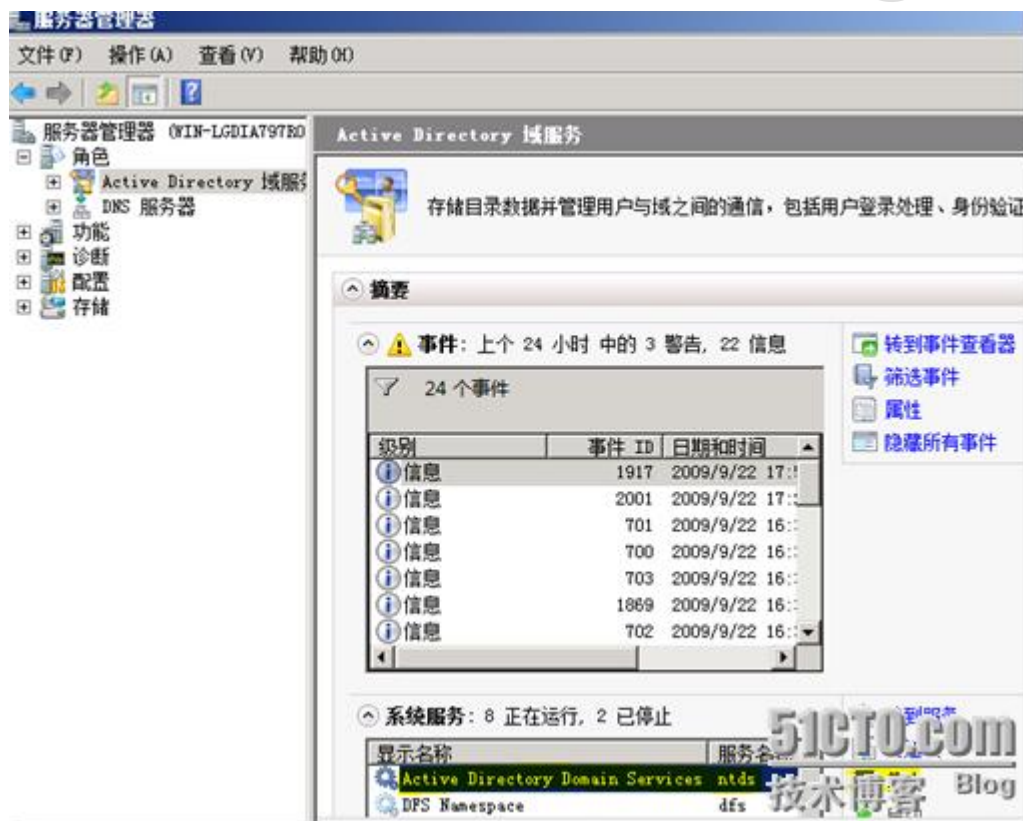
only you~ 能帮我...哦 only you~...（又回想起老板对自己的重托，说不定会有加薪的机会，老老实实的继续干了...）

哦...原来...是这样...如梦一场...（连接加班做完数据还原，第二天，老板说这个月的奖金评分你最低，但是你很有潜力，好好干...明天会更好）

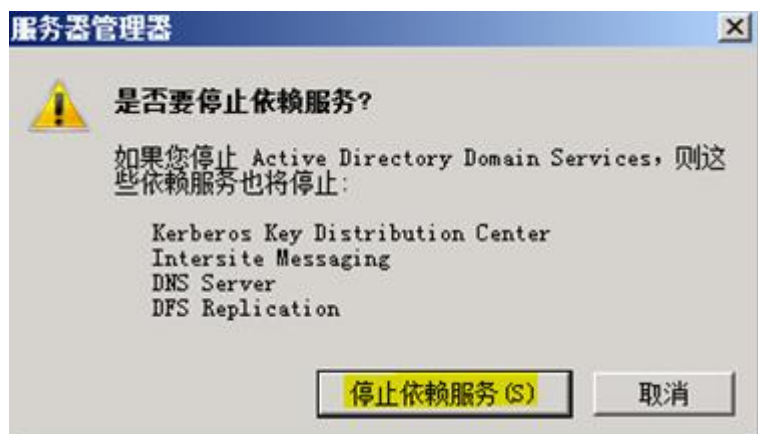
上一集中我们实现了离线（offline）的方式还原活动目录数据，但是这样的方式需要重新启动域控制器，对于企业生产环境来说可能会耽误很多业务，那么这一集咱们就来加快活动目录数据的还原，不重启 DC，照样还原活动目录数据库（windows server 2008 特性之一）。因为 windows server 2008 的活动目录服务是独立于系统之上的。

下面我们来看一下线上还原活动目录如何实现：

首先，停止活动目录服务，取消对活动目录数据库的锁定状态：打开‘服务器管理器’展开‘角色’点击‘Active Directory 域服务’找到‘系统服务’中的‘Active Directory Domain Services’选中这个服务，



点击停止，



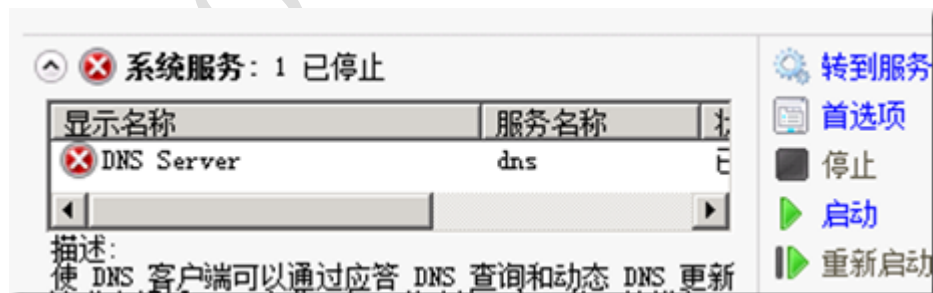
再选择停止依赖服务，停止后如下图所示



此时，咱们的活动目录数据库文件就处于一个可写的状态了，咱们就可以不进入目录还原模式来做 AD 数据库还原了。当然，此时的状态就是我们所说的 online 状态了。

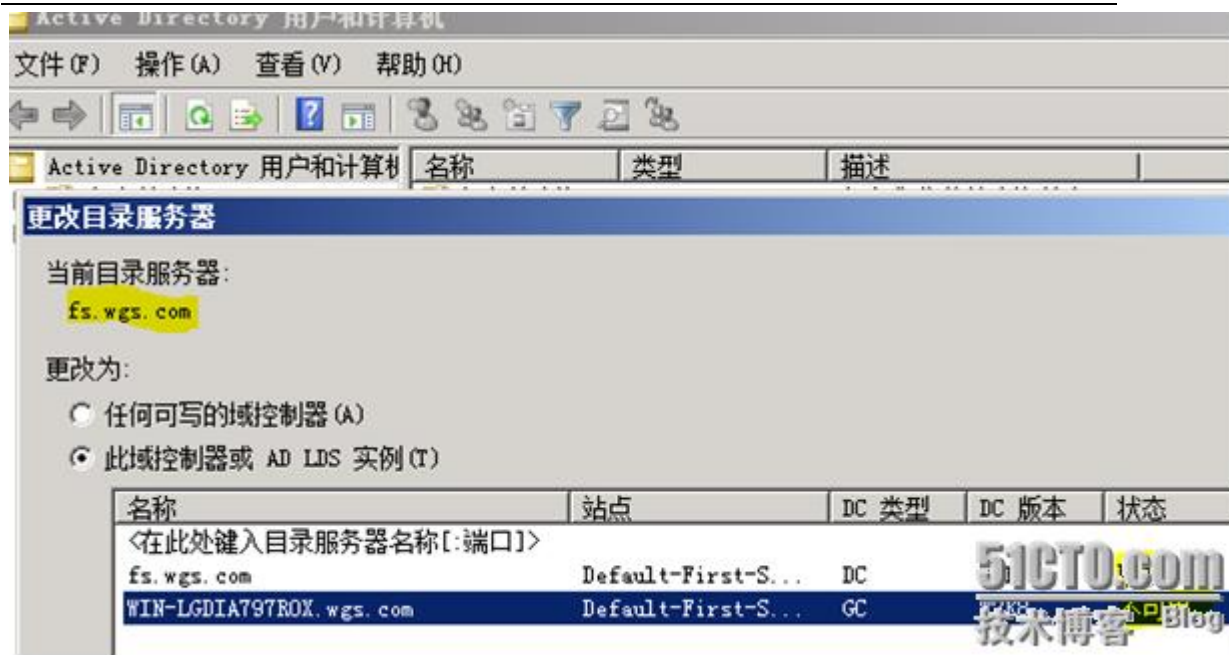
啦...啦...啦...我的心里只有你没有她~~~! (2008 的活动目录数据库还原就可以做到这么让人心动!!!)

随着这台 DC 活动目录主服务 down 掉，这台 dc 的 dns 也会一起 down 掉。



down 掉...down 掉...down 掉，一起 down 掉! *掉...*掉...*掉...***掉 (貌似是限制级..... -_-!!!!)

因为我有两台 DC 所以我此时打开 'Active Directory 用户和计算机' 工具选择更改域控制器，填写另一台域控制器计算机名后可以变更域控制器，并看到两台域控制器服务的状态：



如上图所示，我的已经将 DC 变更为另一台叫做 fs 的域控制器，而当前的这台由于 AD 服务停止所以不可用成为了一台只有活动目录数据库记录的服务器。

其实此时我们还是可以使用 fs 这台 DC 的活动目录服务。说重点，现在咱们关心的事 online 活动目录数据库还原的问题。

豆腐...豆腐...功夫...功夫...（下面的又是命令提示符的工作了）

此时，我们打开命令提示符进行活动目录数据库的数据还原，在命令提示符中键入：

wbadmin（我已经事先使用 windows server backup 工具[还附带安装了命令行备份工具#注释这个必须安装的]据库，如果您不清楚如何备份请看这篇文章：[AD 数据库备份\[为企业部署 Windows Server 2008 系列十五\]](#)）



上图中：GET VERSIONS 表示列出备份文件的版本

START SYSTEMSTATE RECOVERY 表示还原系统状态（包括活动目录数据库在内）

键入：wbadmin get versions

```
C:\Users\Administrator>wbadmin GET VERSIONS
wbadmin 1.0 - 备份命令行工具
(C) 版权所有 2004 Microsoft Corp.

备份时间: 2009/9/22 17:21
备份目标: 1394/USB 磁盘, 标记为 新加卷(E:)
版本标识符: 09/22/2009-09:21
可以恢复: 卷, 文件, 应用程序, 裸机恢复, 系统状态
```

从上图中可以看到我有做过一次备份, 并且备份版本是 09/22/2009-09:21 #注释: 通过这个版本号我可以实现活动目录数据库的还原。

键入: wbadmin START SYSTEMSTATERECOVERY -version:09/22/2009-09:21 还原活动目录数据库

```
C:\Users\Administrator>wbadmin START SYSTEMSTATERECOVERY -version:09/23/2009-11
19
wbadmin 1.0 - 备份命令行工具
(C) 版权所有 2004 Microsoft Corp.
```

通过上面的步骤咱们就实现了, 在线还原活动目录。

哦...我的心里只有你没有她...我的情谊对你并不假...让甲流来吧...让扎针去吧...金融危机我也不怕他~! (禁不住把歌词唱错了~ @_@!!)

还原意外删除的用户账户

通过前面两回，我们了解到在 windows server 2008 中还原活动目录数据库的方法。那么在活动目录数据的日常维护中，难免出现意外删除用户账户的情况。

面对这样的场景，您可能会惊慌失措，今天咱们就来传授不用惊慌失措的绝招：还原意外删除的用户账户

虽然是绝招，但是少不了基本功（活动目录数据库的备份，我这里已经是提前备份好的，所以我就可以直接还原了）。

下面大家来看一下这个意外删除到还原的全过程：

在我的 Active Directory 用户的计算机中有 demo 这个 OU，在此 OU 下有 user1 和 user2 两个用户



由于误操作，管理员意外删除了 user1



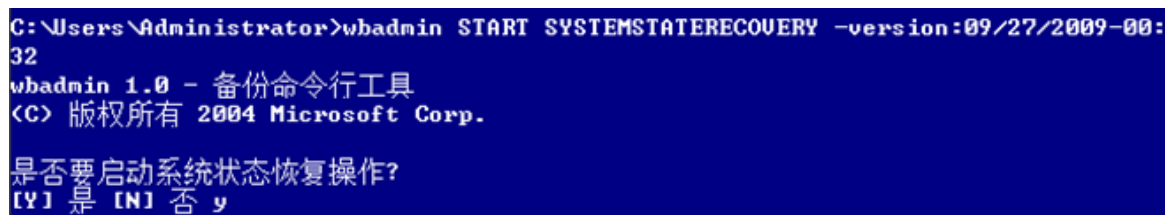
现在咱们把 user1 还原回来！首先，重新启动计算机按 F8 进入目录服务还原模式（再次提醒和生命我在删除 user1 之前已经做过活动目录的备份了哦）



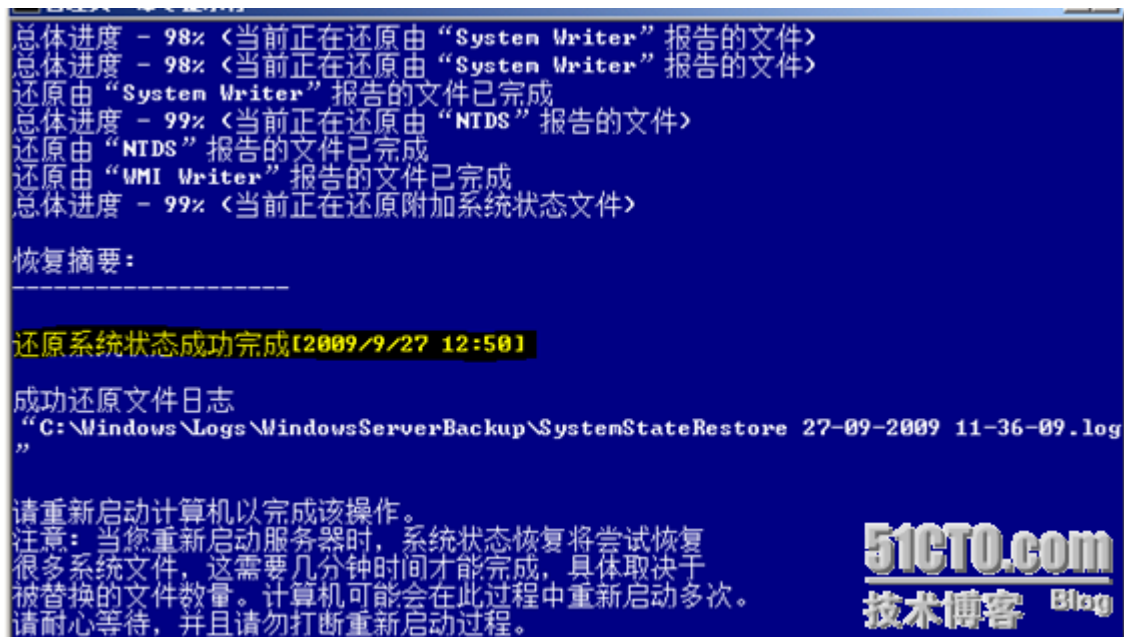
进入系统后，使用 wbadmin 命令来实现系统状态还原，



获得版本后，执行下面命令（wbadmin start systemstaterecovery -version:版本 id）来还原系统状态到我最后一次备份的状态，



还原完毕之后，先不要着急重新开机，因为还原完成后的 AD 数据库版本比较低，所以其他的域控制器会因为复制的原因把刚刚还原的数据覆盖掉。



所以我们需要把当前域控制器上已经还原回来的 AD 数据库版本刷新，来防止被其他域控制器覆盖数据。

下面我们就用 ntdsutil 工具来实现：

打开命令提示符界面，键入 ntdsutil 并设置当前连接的 AD 数据库实例为 ntds（这里指的是当前正在使用的数据库文件%systemroot%\ntds\ntds.dit）



接着我进入一个目录叫做 authoritative restore（授权还原）



选择我要还原一个对象，使用 'Restore object ldap 路径'（这里解释下什么叫 ldap 路径：我所要还原的对象的名称：'CN=user1' 表示，对象所属的 OU：'OU=demo' 表示，对象和 OU 所属的域：'DC=wgs,DC=com' 表示）的命令如下，

```
authoritative restore: Restore object CN=user1,OU=demo,DC=wgs,DC=com
```

按下 enter 后，系统提示是否要执行此授权还原：



选择是，还原完成后大家可以看到我所选择要还原的对象 user1 的版本号被增加了十万，如下图：

```
authoritative restore: Restore object CN=user1,OU=demo,DC=wgs,DC=com
正在打开 DIT 数据库... 完成现在时间是 09-27-09 13:34.52。
最近的数据库更新发生在 09-27-09 08:32.05。
增加属性版本号 100000。
计算需要更新的记录...
找到的记录: 0000000001
完成
找到 1 要更新的记录。
更新记录...
所剩记录: 0000000000
完成
成功的更新了 1 个记录。
已在当前工作目录中创建带有授权还原对象列表的下列文本文件:
ar_20090927-133452_objects.txt
指定的对象均不具有此域中的返回链接。未创建任何链接还原文件。
Authoritative Restore 成功完成。
```

此时，再重新启动计算机，我们意外删除的用户数据就被找回来了，而且不会被其他 DC 覆盖数据。大家可以从下图中看到被意外删除的 user1 回来了！！！（路人甲曰：兴奋 ing、激动 ing、跃跃欲试 ing.....）



最后总结并解释下今天这篇文章涉及到的概念和名词：

DC：域控制器

OU：组织单位

具体解释，请参考：<http://angerfire.blog.51cto.com/198455/43217>

AD 还原方式分两种：

- 1 非授权还原：恢复活动目录到备份它时的状态
- 2 授权还原：恢复活动目录的特定对象

减肥计划之 AD 数据库压缩重整

在生产环境中，AD 数据库随着公司的运作时间会变的比较肥硕，导致活动目录数据的读写效率降低。作为企业 IT 环境的管理员，我们应该有计划的整理活动目录数据库，从而实现提升 DC 的运行效率，同时保证 IT 基础架构环境持续高效运行。

要做 AD 数据库压缩重整，首先要在 DC 上按 F8 进入目录服务还原模式。在目录服务还原模式下打开命令提示符，键入 ntdsutil

```
管理员: 命令提示符 - ntdsutil
C:\Users\Administrator.WIN-LGDIA797R0X>ntdsutil
ntdsutil: ?

? - 显示这个帮助信息
Activate Instance %s - 设置“NTDS”或特定的 AD LDS 实例
                        作为活动实例。
Authoritative restore - 授权还原 DIT 数据库
Change Service Account %s1 %s2 - 将 AD DS/LDS 服务帐户更改为
                                用户名为 %s1，密码为 %s2。
                                使用“NULL”表示空密码，* 表示
                                从控制台输入密码。
Configurable Settings - 管理可配置的设置
DS Behavior - 查看和修改 AD DS/LDS 行为
Files - 管理 AD DS/LDS 数据库文件
Group Membership Evaluation - 评估给定用户或
                              组的令牌中的 SID。
Help - 显示这个帮助信息
IFM - IFM 媒体创建
LDAP policies - 管理 LDAP 协议策略
LDAP Port %d - 为 AD LDS 实例配置 LDAP 端口。
List Instances - 列出该计算机上安装的所有 AD LDS 实例
Local Roles - 本地 RODC 角色
Metadata cleanup - 清理不使用的服务
Partition management - 管理目录分区
```

再键入 Activate Instance NTDS 将当前的活动目录数据库 NTDS 设置为活动实例（这样就可以对活动目录相关文件进行操作了）

```
ntdsutil: Activate Instance NTDS
活动实例设置为“NTDS”。
ntdsutil: _
```

键入 Files 进入活动目录数据实例的管理界面，可以在这个界面下对 AD 数据库文件和日志文件执行压缩、查询、移动、路径设定等操作，如下图所示：

```
ntdsutil: Files
file maintenance: ?

? - 显示这个帮助信息
Checkpoint - 转储 Jet 检查点文件
Checksum - 执行 Jet 物理完整性检查
Compact to %s - 将 DB 压缩到指定的目录
Dump page %d - 转储 Jet 数据库 %d 页码
Header - 转储 Jet 数据库头
Help - 显示这个帮助信息
Info - 返回有关 DS 文件的信息
Integrity - 执行 Jet 逻辑完整性检查
Logfile %s - 转储 Jet 日志文件 %s。%s 可以是日志目录中的日志文件，也可以是日志目录中的日志文件。
```

首先，咱们来查看下 ntds 的信息：键入 Info 后按 enter

```
file maintenance: info

驱动器信息:

C:\ NTFS <硬盘> 空白<21.8 Gb> 总共<29.2 Gb>
D:\ NTFS <硬盘> 空白<30.6 Gb> 总共<30.7 Gb>

DS 路径信息:

数据库       : C:\Windows\NTDS\ntds.dit - 16.1 Mb
备份目录     : C:\Windows\NTDS\dsadata.bak
工作目录     : C:\Windows\NTDS
Log dir      : C:\Windows\NTDS - 40.0 Mb total
               edbres00002.jrs - 10.0 Mb
               edbres00001.jrs - 10.0 Mb
               edb00001.log - 10.0 Mb
               edb.log - 10.0 Mb
```

接下来，我们键入 Compact to c: 命令将当前 C:\WINDOWS\NTDS\ntds.dit 文件压缩到 C:\ntds.dit

```
file maintenance: Compact to C:
正在启动碎片整理模式...
源数据库: C:\Windows\NTDS\ntds.dit
目标数据库: C:\ntds.dit

Defragmentation Status (% complete)

0    10   20   30   40   50   60   70   80   90  100
|----|----|----|----|----|----|----|----|----|
.....

建议您立即执行该数据库的完整
备份。如果您先恢复备份，然后
才进行碎片整理，则会将数据库
回滚到备份时其所处的状态。

压缩成功。您需要执行下列操作：
复制 "C:\ntds.dit" "C:\Windows\NTDS\ntds.dit"
并删除旧的日志文件：
del C:\Windows\NTDS\*.log
```

此时，咱们再打开一个命令提示符并在 C 盘下查看刚刚压缩过来的 AD 数据库文件

```
C:\>dir
驱动器 C 中的卷没有标签。
卷的序列号是 8879-9EDE

C:\ 的目录

2009/09/27  17:15                14,696,448 ntds.dit
2008/01/19  18:11                <DIR>          PerfLogs
2009/09/27  08:45                <DIR>          Program Files
2009/09/27  08:44                <DIR>          Program Files (x86)
2009/09/27  16:04                <DIR>          Users
2009/09/27  13:40                <DIR>          Windows
                    1 个文件          14,696,448 字节
                    5 个目录      20,950,761,472 字节
```

可以看到压缩过的数据库文件 ntds.dit 比原始的 C:\WINDOWS\NTDS\ntds.dit 文件要小很多。

现在只要当前的 AD 数据库实例使用这个数据库文件就可以了，我们可以通过以下方式实现：将 AD 数据库实例的路径设置为 C:\ntds.dit。命令参考：set path DB C:\ntds.dit

```
file maintenance: Set path DB C:\ntds.dit
正在从 c:\windows\ntds 拷贝 NTFS 安全性到 C:...
已成功更新备份排除项。
file maintenance: info

驱动器信息:

C:\ NTFS (硬盘) 空白(19.5 Gb) 总共(29.9 Gb)
E:\ NTFS (硬盘) 空白(2.6 Gb) 总共(29.9 Gb)

DS 路径信息:

数据库       : C:\ntds.dit - 14.1 Mb
备份目录     : C:\Windows\NTDS\dsadata.bak
工作目录     : C:\Windows\NTDS
Log dir      : C:\Windows\NTDS - 30.0 Mb total
               edbres00002.jr
               edbres00001.jr
               edb.log - 10.0 Mb
```

我们还可以直接把 AD 数据库路径移动到指定地点，比如把刚刚设定到 C:\ntds.dit 的 AD 数据库文件移动到原始位置 C:\WINDOWS\NTDS\ntds.dit

先要把原始位置 C:\WINDOWS\NTDS\ntds.dit（大小为 16.1M）的数据库文件删除或者移动到其他位置，

```

C:\Windows\NTDS>del ntds.dit

C:\Windows\NTDS>dir
驱动器 C 中的卷没有标签。
卷的序列号是 8879-9EDE

C:\Windows\NTDS 的目录

2009/09/27  17:50    <DIR>          .
2009/09/27  17:50    <DIR>          ..
2009/09/27  17:13                8,192 edb.chk
2009/09/27  17:13            10,485,760 edb.log
2009/09/22  16:13            10,485,760 edbres00001.jrs
2009/09/22  16:13            10,485,760
4 个文件          31,465,4
2 个目录    20,963,868,6

```

接着使用 Move DB to C:\WINDOWS\NTDS\ 指定 AD 数据库实例移动的位置目录

```

file maintenance: Move DB to C:\WINDOWS\NTDS

已成功更新备份排除项。
正在从 C: 拷贝 NTFS 安全性到 C:\WINDOWS\NTDS...

驱动器信息:

C:\ NTFS <硬盘> 空白<19.5 Gb> 总共<29.9 Gb>
E:\ NTFS <硬盘> 空白<2.6 Gb> 总共<29.9 Gb>

DS 路径信息:

数据库       : C:\WINDOWS\NTDS\ntds.dit - 14.1 Mb
备份目录     : C:\WINDOWS\NTDS\DSADATA.BAK
工作目录     : C:\WINDOWS\NTDS
Log dir      : C:\Windows\NTDS - 30.0 Mb total
               edbres00002.jrs - 10.0 Mb
               edbres00001.jrs - 10.0 Mb
               edb.log - 10.0 Mb

移动数据库成功。
请立即进行备份，否则将无法
还原新文件位置。

```

大家可以看到位置已经移动到了 C:\WINDOWS\NTDS\ 目录下，并且大小为 14.1M

此时因为活动目录数据已经是压缩更新的了所以建议大家及时做好新的 AD 备份。

此时您的 IT 基础架构环境就可以飞奔如初了，DC 也会感觉到自己走路轻了一些。（DC 同志兴奋的说：哈哈！减肥大成功！！！ @_@!!）

减肥是需要的，但平时锻炼身体是必须的，基于 AD 的基础架构环境需要长期锻炼才能强健如牛！您的收益也会走出一条如牛市股票般的曲线！

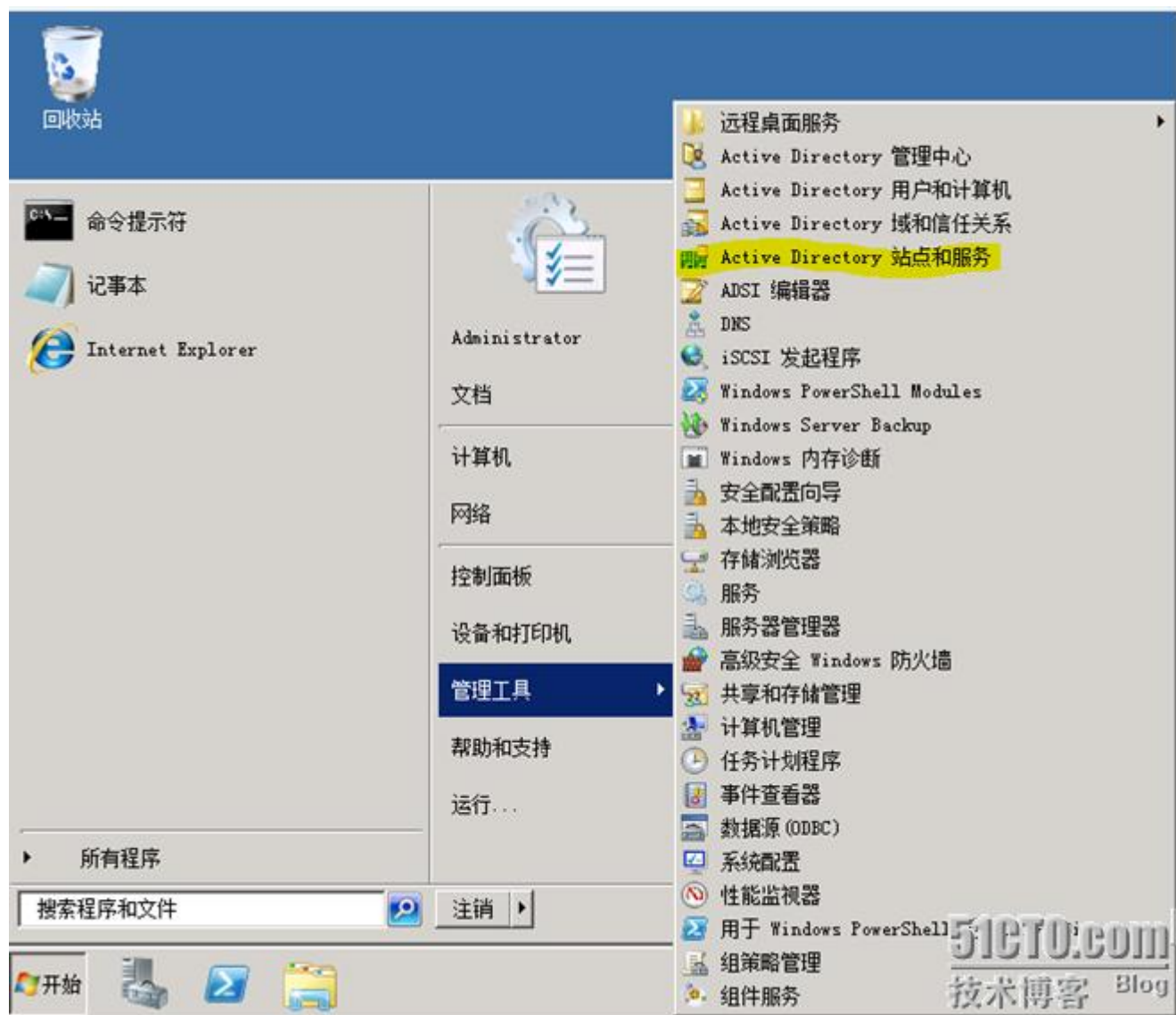
通用类别目录 Global Catalog

Global Catalog，简称为“GC”，有的地方叫“全局编录”，这里我把它叫做“通用类别目录”。

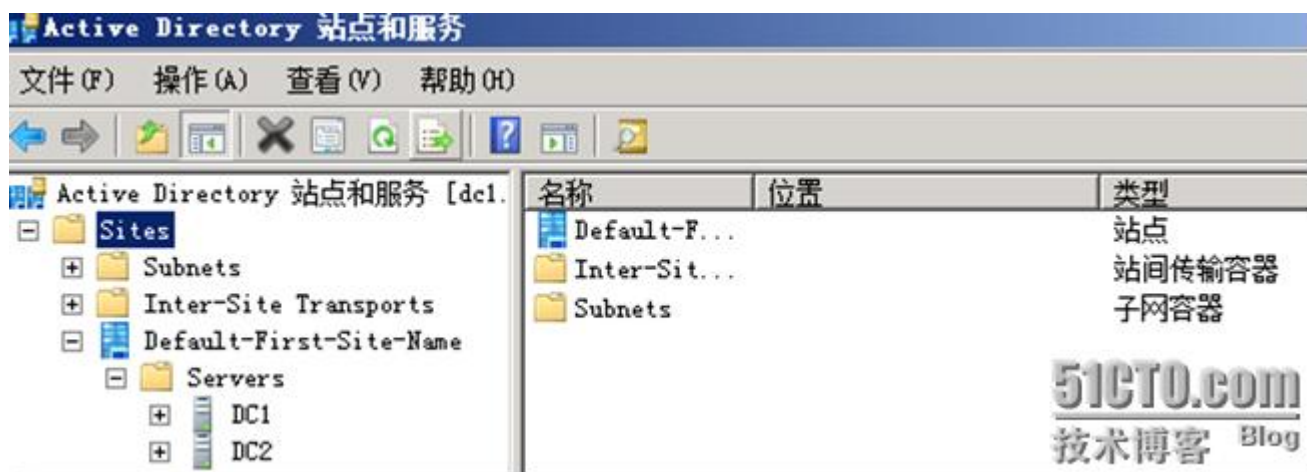
主要功能是：帮助域控制器把其他域包含本域的资料收集起来，便于客户端查询。

下面我们就边走边瞧，看看传说中的 GC。

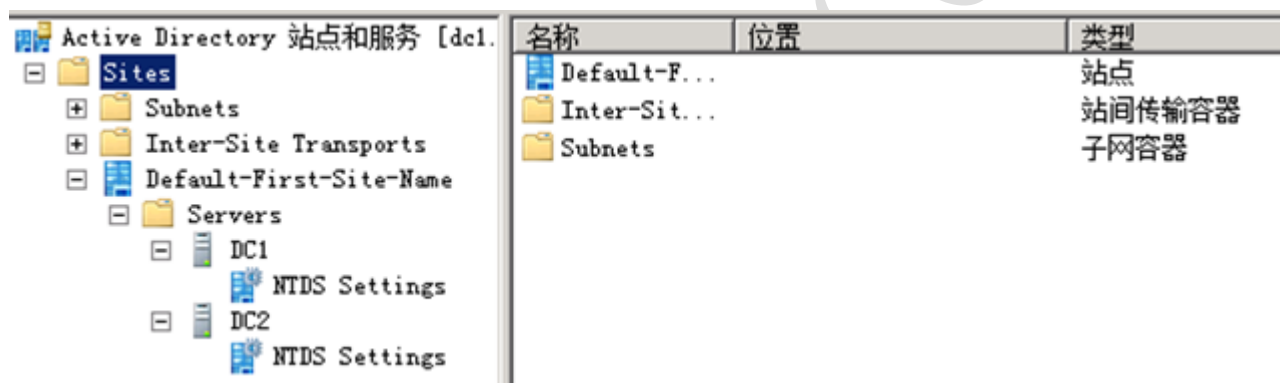
首先登陆 DC，选择开始-程序-管理工具-Active Directory 站点和服务，通过这个工具我们就可以找到在当前域哪些 DC 是担任全局编录[通用类别目录 GC]的角色。



打开站点和服务管理工具，依次展开 Default-First-Site-Name 下的 Servers，可以看到域控制器。



可以看到 DC1 和 DC2 这两台域控制器（DC1 和 DC2 是我的两台 DC 的名字），将其展开，可以看到 NTDS Settings 节点



我们先来看叫做 DC1 的这台：

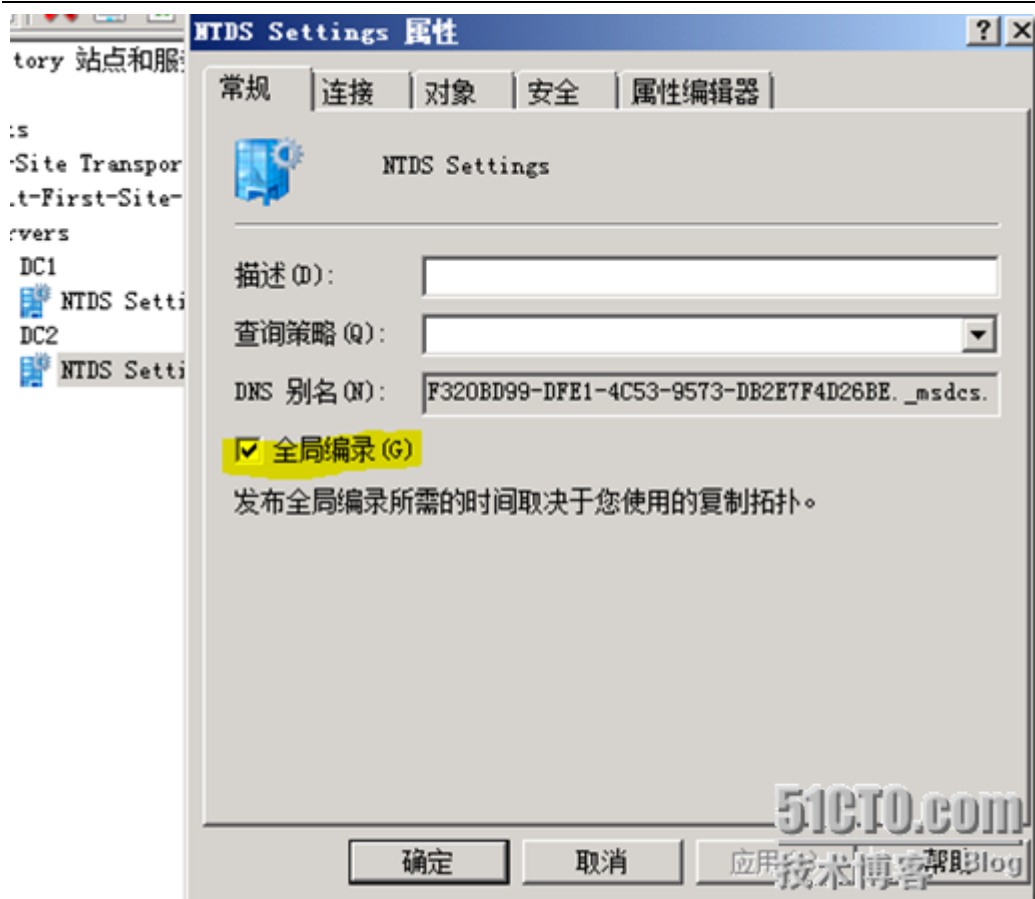
鼠标右击 DC1 下 NTDS Settings 节点，选择属性。可以在属性的常规选项中看到“全局编录”这个选项，并且是被勾选状态。



从上图中可以看出我的 DC1 是 GC（全局编录）。

我们再来看一下另外一台叫做 DC2 的域控制器：

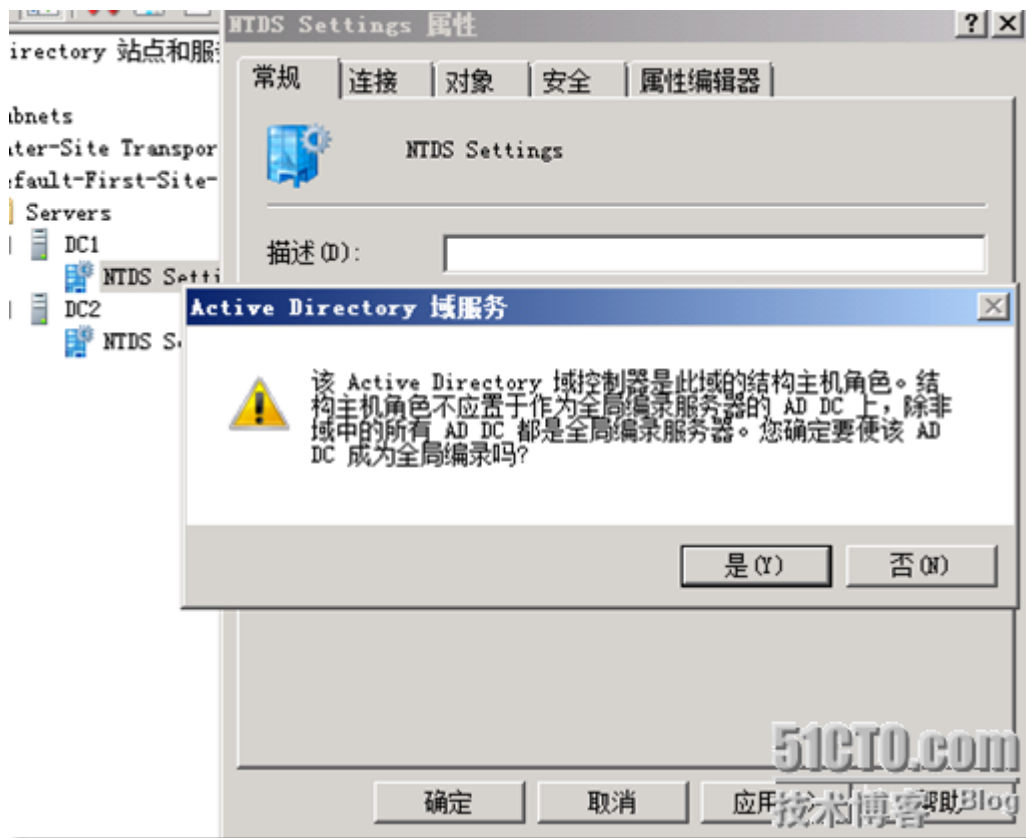
鼠标右击 DC2 下 NTDS Settings 节点，选择属性。



可以看到 DC2 也是 GC（全局编录）。

那么 GC 什么情况下会被使用呢？

假设，在我当前域有很多客户端需要查询域环境中的资料，而且很多都是其他域的资料，那么这个时候我当前域就需要至少有一台 GC 给客户端提供查询。



大家可以看到我在 DC1 下的 NTDS Settings 节点属性的常规选项卡中把“全局编录”的钩去掉后再打钩就会出现上图中的警告信息。

那么什么时候能够将当前 DC 设置为 GC 什么时候不能设置为 GC 呢？这里有两种情况：

情况一：如果说当下您的只有一个域，也就是“单域环境”，那么我建议您把所有的 DC 都设置成 GC。因为在单域环境下“结构主机”是不发挥作用的（没有被使用），所以不存在上图中警告信息所担心的情况，所以可以忽略这个警告信息。

情况二：如果当下您有多个域，也就是“多域环境”，你的 GC 的角色的服务器，他绝对不能担任“结构主机”的操作主机角色（现在咱们还没讲过操作主机，咱们会在后续的文章中和大家介绍）。为什么不能担任呢？因为在多域环境下，如果你的一台域控制器即担任“GC”又担任“结构主机”（Infrastructure Master）的话，会造成“结构主机”失效。

所以我当下的域环境就是单域环境，所以我把两台 DC 都设置成了 GC，而我在选择 DC1 下的 NTDS Settings 节点 属性的 GC 选项时，之所以会出现上图中的警告信息，就是因为我所选择的这台 DC 他就担任着“结构主机”的角色。

那我当前的单域环境中我设定了两台 GC 所以他们之间会彼此复制相互的资料，如果您的多域环境，那么您所设定的 GC 之间也会彼此复制相互的资料，来方便用户查询。

这就是咱们今天和大家分享的关于“通用类别目录” Global Catalog 的课程，希望能对您有所帮助。

操作主机 PDC Emulator

一个以活动目录为核心的基础架构管理环境运行效率的高低取决于操作主机和 DC 的位置的设计，在后期域环境的维护工作中也起着非常重要的作用。

今天跟大家介绍的是域环境中五大操作主机之一 "PDC Emulator" 全称 "Primary domain controller (PDC) emulator operations master" 中文:PDC 仿真主机。

我习惯把它称为"PDC Emulator"。

现在咱们就来一步步认识 "PDC Emulator"。

如果我们要设置当前域的 "PDC Emulator" 角色，必须选择开始 - 管理工具 - Active Directory 用户和计算机，可以看到当前域的名称为 "wgs.com"。



鼠标右击当前域，选择“操作主机”，



打开操作主机选项卡后选择 PDC,就可以查看到当前域的 PDC Emulator 是 dc1.wgs.com 这台主机。



PDC Emulator 总共有五项功能：

第一个功能：模拟 NT 的 PDC：所有当您的域环境中 NT 的 BDC 的话，请务必准备一台 PDC，他才可以把资料复制给 NT 的 BDC。

第二个功能：时间同步或者叫对时：当前域中的所有的主机会跟 PDC Emulator 对时，当前域的 PDC Emulator 会跟整个树的树根中的 PDC Emulator 对时，当前树根中的 PDC Emulator 会跟整个林的根域的 PDC Emulator 对时，所以可以让整个森林的时间保持一致。

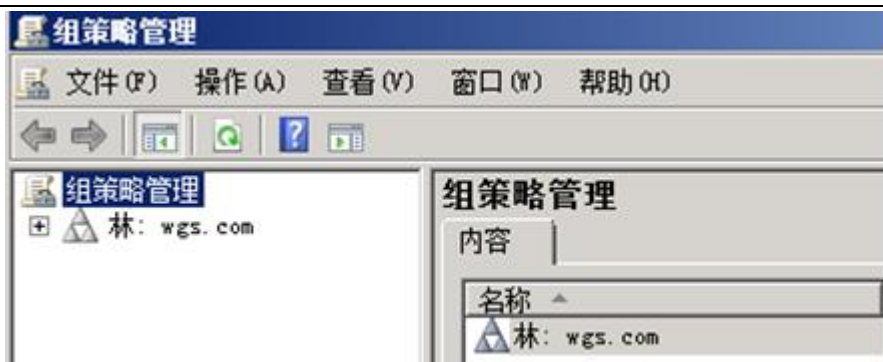
第三个功能：给 NT 以前的客户端改密码：因为 NT 以前的客户端改密码必须要连到以前 NT 域的 PDC 上才可以改，PDC 是只读的。

第四个功能：密码仲裁：2000 以后的客户端改密码，会用到 PDC 来避免密码修改的延迟。比如说我把密码修改完以后我把它修改到 a 这台 DC，下次我登陆的时候我登陆到 B，B 还没有来得及把 AD 数据复制过来，就会有旧密码存在，这样就会有问题，所以客户端就会找 PDC Emulator 做仲裁，从而得到最新的密码。

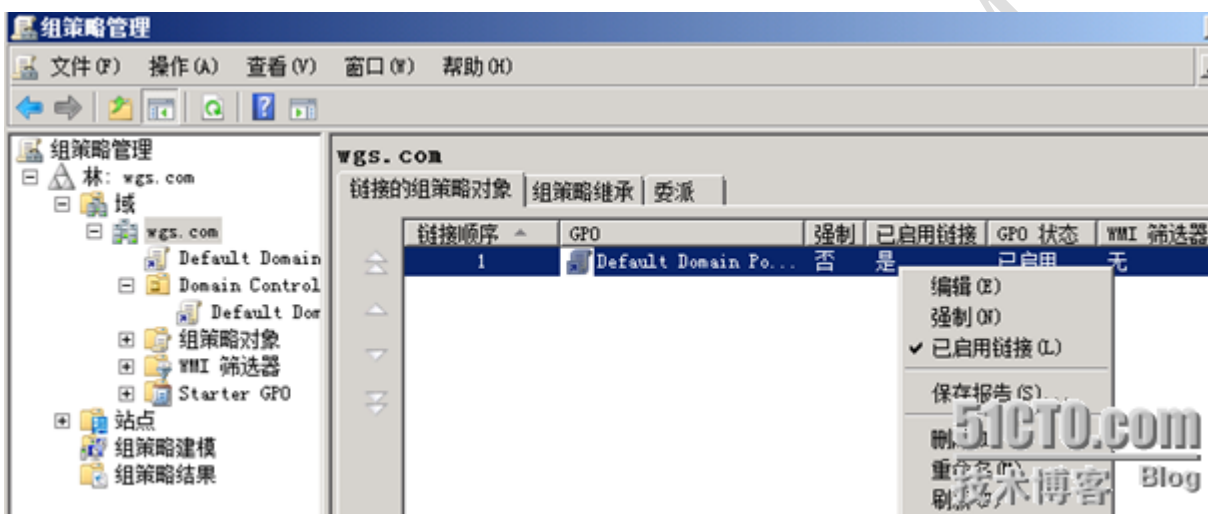
第五个功能：防止重复套用组策略：当我们使用组策略时，我们的组策略编辑器会连到 PDC Emulator 去做修改，来防止组策略套用出错。

这个功能我们可以看图来说明下：

我们先打开“组策略管理”



假设我要编辑某一个 GPO，比如默认域策略



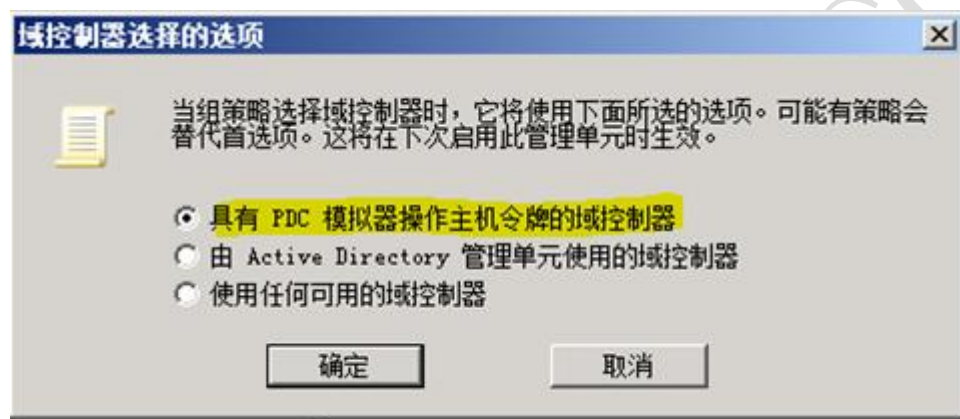
大家可以看到 组策略管理编辑器 会默认连接到一台主机名字叫“dc1.wgs.com”而这台 DC 正是我当前域的 PDC Emulator，这样的设定就会防止，在复制组策略对象（GPO）的时候出现重复。



我们可以在组策略管理编辑器的 查看 下拉菜单中找到 DC 选项 单击，



可以看到如下提示



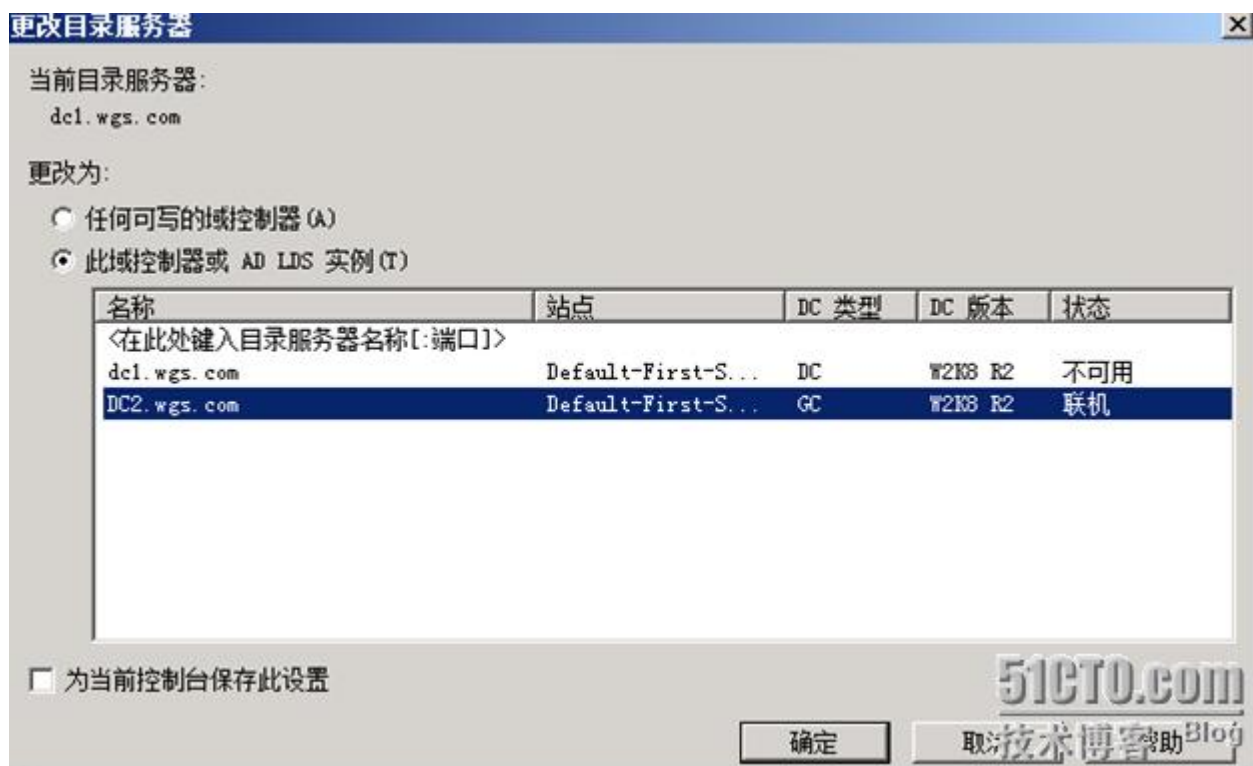
从上图中我们可以看出，默认情况下在套用 GPO 的时候就会去找 PDC Emulator 去做复制，这样就可以避免 GPO 设置在复制的时候重复。

下面再来看一下如何去实现 PDC Emulator 的转移：

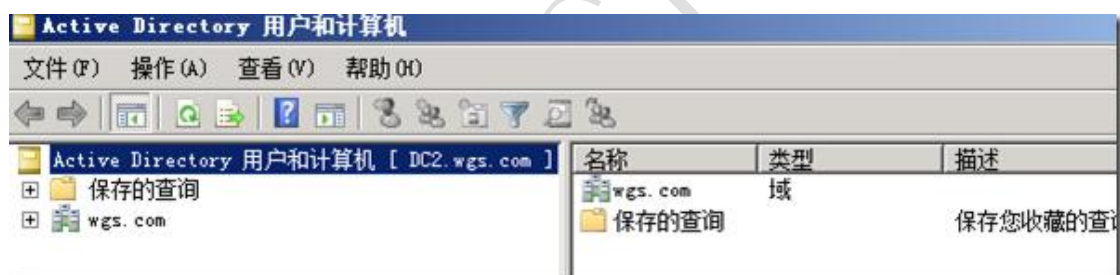
打开 Active Directory 用户和计算机 鼠标右击 Active Directory 用户和计算机 选择更改域控制器。



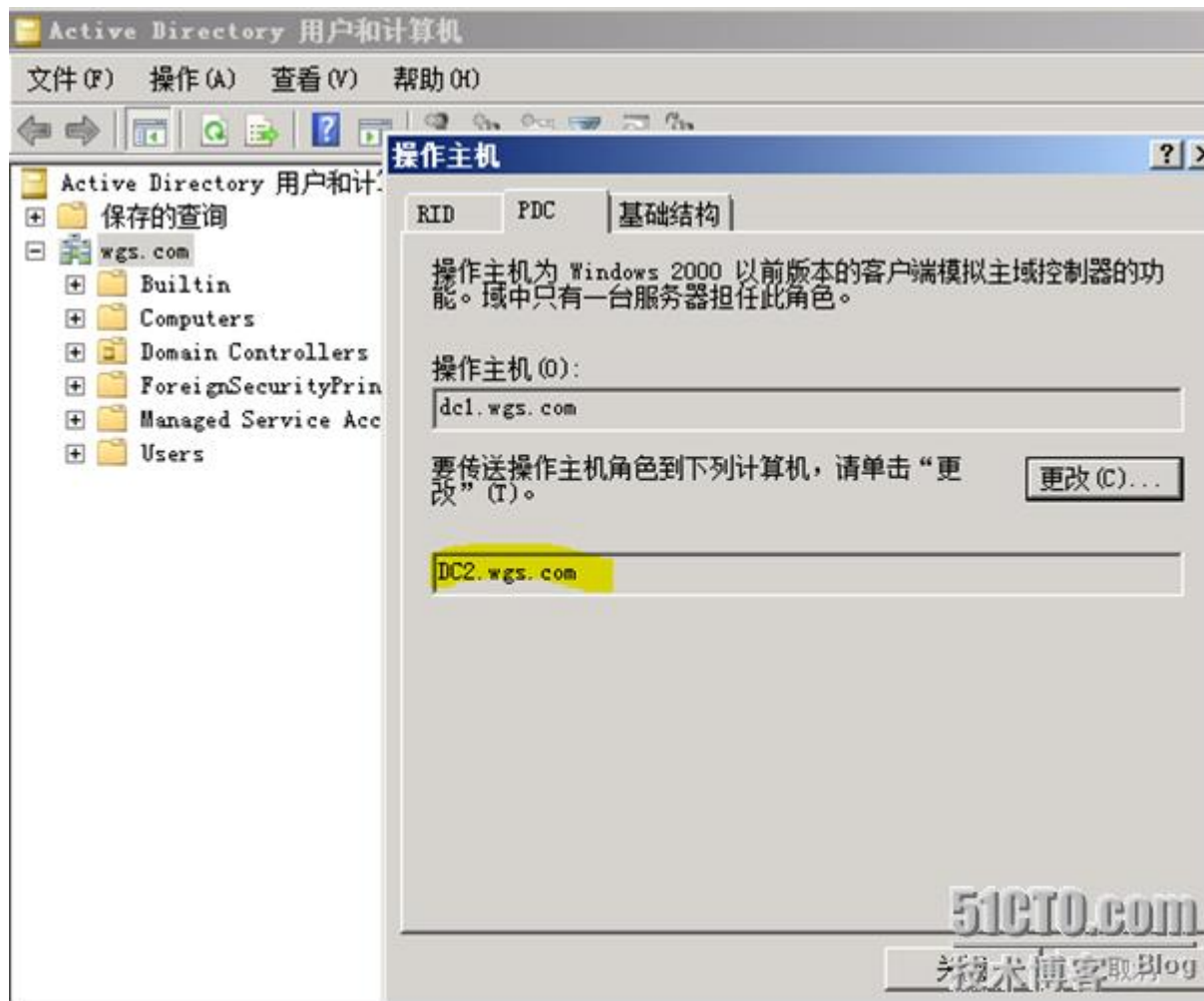
出现如下图所示窗口，大家可以看到我当前域有两台 DC：DC1 和 DC2，我选择更改目录服务器为 DC2.wgs.com



下图为更改后的状态，



然后鼠标右击当前域 **wgs.com** 选择操作主机，可以看到目前的操作主机是 **DC1.wgs.com**。



再选择更改，
结果如下：

选择传送操作主机，



此时操作主机 PDC Emulator 就已经成功变更为 DC2.wgs.com

通过今天这篇文章您了解到了 五大操作主机之一 PDC Emulator 的功能 和 转移方法。其他的操作主机会在后续文章中为您放出。

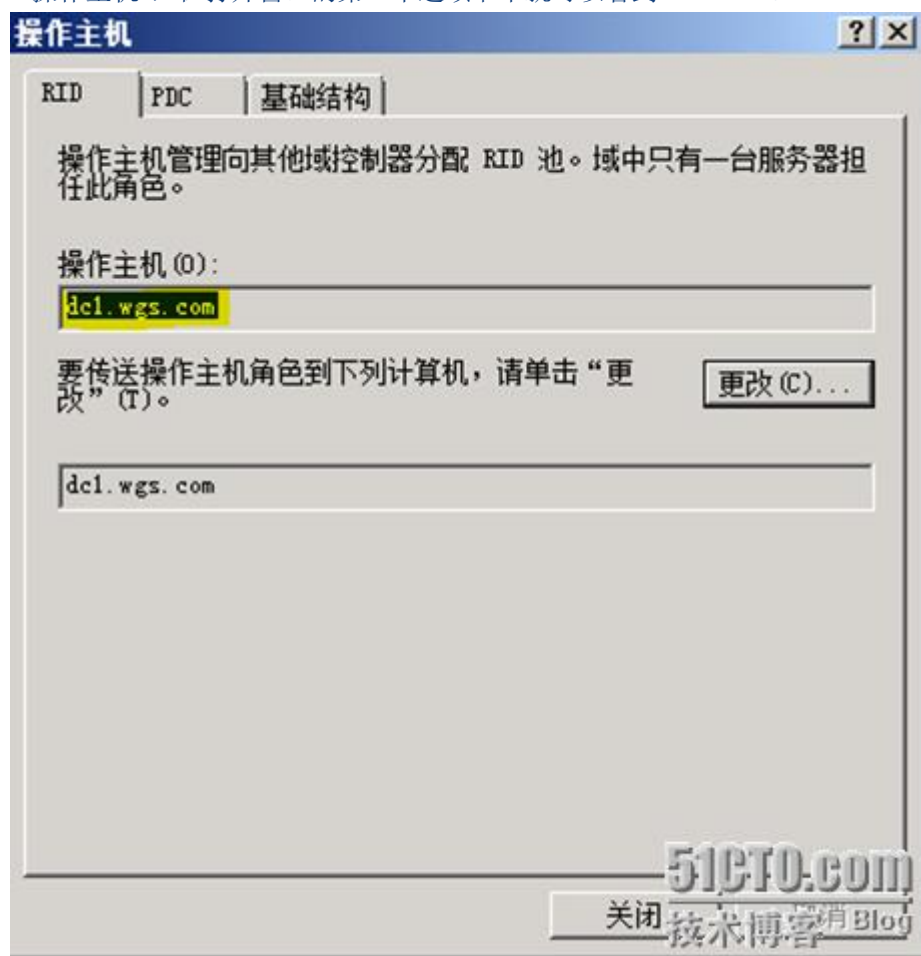
操作主机 RID master

一个以活动目录为核心的基础架构管理环境运行效率的高低取决于操作主机和 DC 的位置的设计，在后期域环境的维护工作中也起着非常重要的作用。

今天跟大家介绍在 Active Directory 中，RID Master（RID 主机）的相关设定和所负责的功能。

咱们来一步步认识 RID Master：

RID Master 和 PDC Emulator 一样，也是域中必须唯一的操作主机之一，所以同样打开“开始”--“管理工具”--“Active Directory 用户和计算机”鼠标右击 当前域“wgs.com”选择“操作主机”，在打开窗口的第一个选项卡中就可以看到“RID”。



从上图中可以看到当前域的 RID Master 是 dc1.wgs.com 这台 DC。

RID 的功能是这样，当我们要在 AD 中建立对象（如：用户，组，计算机等等），每一个对象都要有一个独一无二的 SID，一个 SID 是由两个号码所组成：DomainID（当前域的 ID）+ Relative ID（相对 ID 或者简称 RID）。所以为了避免两个对象的 SID 一样，所以必须要把 RID 做独一无二的编码。所以 RID Master 就负责把这些 RID 的码编出来。那默认状态下呢，DC 会向 RID Master 去要一堆的 RID 号码，等到将来咱们在创建帐户的时候就从这些号码拿出来用。等用完后再去跟 RID Master 去要。所以 RID Master 他很重要。如果说他坏掉的话，当前你可能可以建立一些帐号没有问题，因为域控制器这边会有些预留的，但一旦用光了之后，你就再也无法新增新的帐号了（包含：用户、计算机、组）。

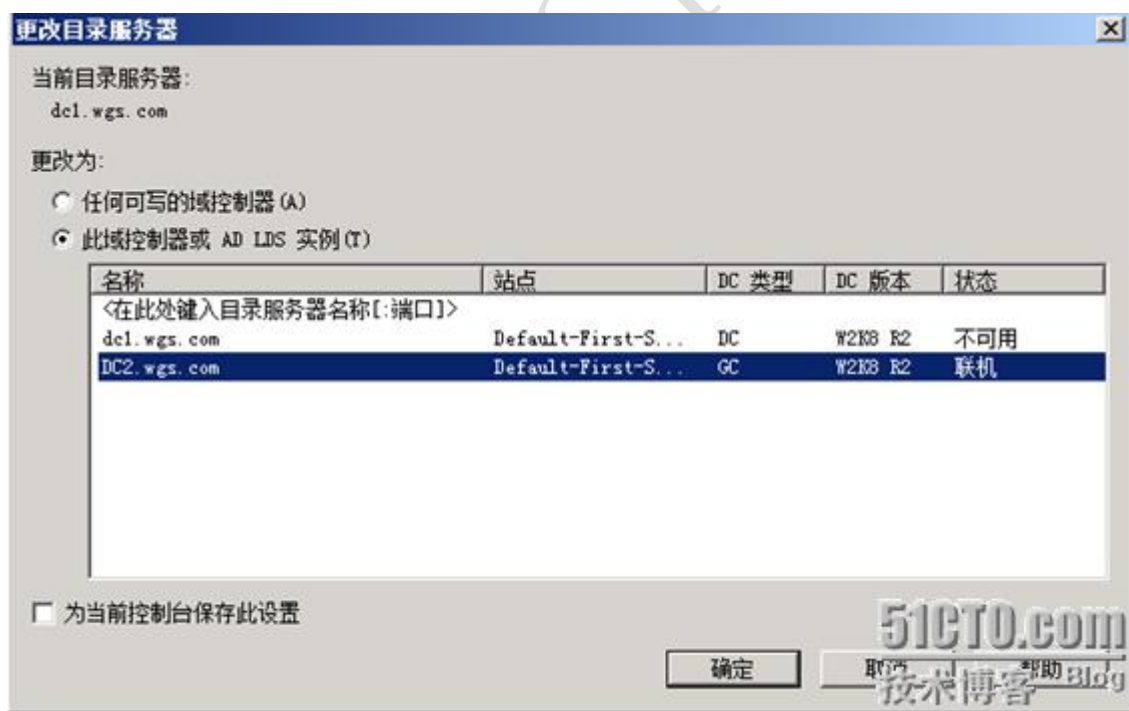
RID master 还有一个功能就是当你跨域去转移帐号的时候也可以透过 RID Master 去比对是不是有相同号码的帐号存在，以免造成重复的操作。

现在如果您要去转移 RID Master，做法是这样的：

首先 鼠标右击 “Active Directory 用户和计算机”工具中的 Active Directory 用户和计算机 选择 “更改域控制器”



打开如下图所示窗口后，选择需要切换到另一台 DC，比如我所选择的 dc2.wgs.com 这一台。



确定后可以看到目前我是连接到 DC2 这台 DC 上了。

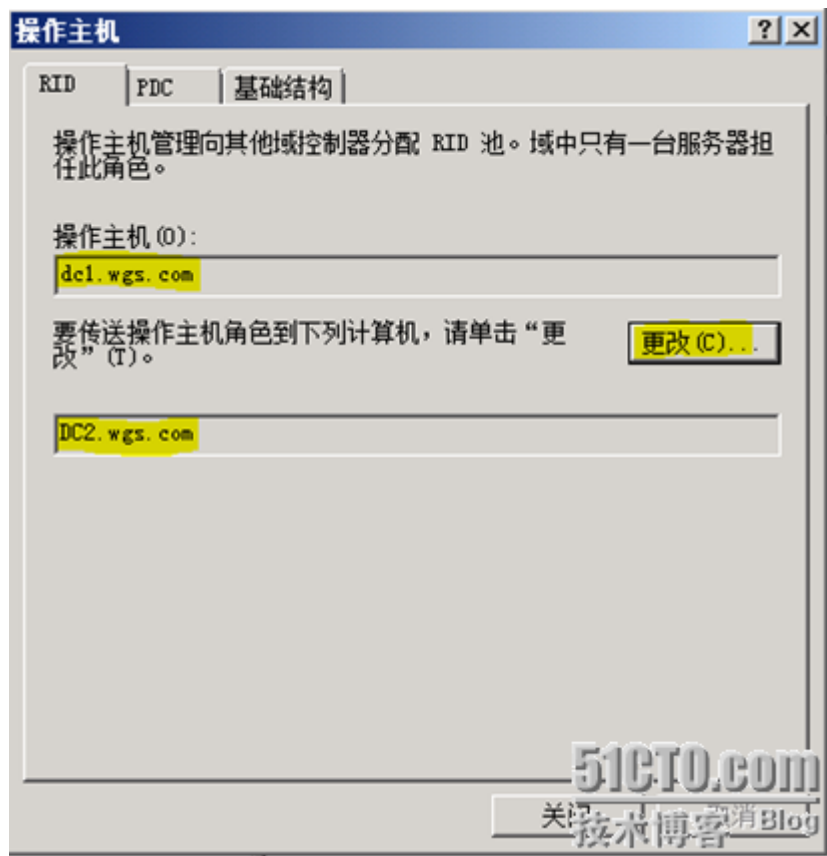


准备好上面的步骤，现在咱们就可以来实现 操作主机 RID Master 的转移操作了，如下图所示：

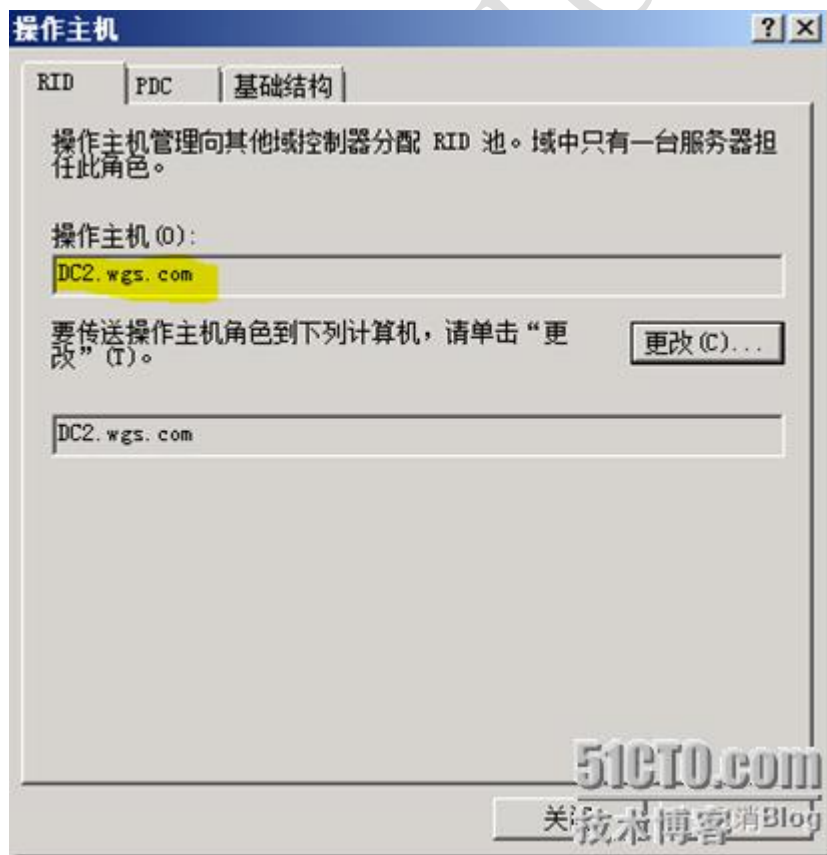
右击当前域 “wgs.com” 选择 “操作主机”



打开如图所示窗口：



选择更改，是，确定。可以看到当前的操作主机 RID Master 已经变成 dc2.wgs.com,



这样就顺利把操作主机 RID Master 转到 dc2 那一台去了。

其实，我们也可以使用命令提示符去做：

点击 开始--程序--命令提示符，键入“ntdsutil”后 在 ntdsutil 界面中键入“?”回车。



找到 Roles 如下图所示：



键入 Roles，按 enter，进入角色管理界面；

```
ntdsutil: Roles
fsmo maintenance: _
```

再键入 Connections，按 enter，进入连接界面；

```
fsmo maintenance: Connections
```

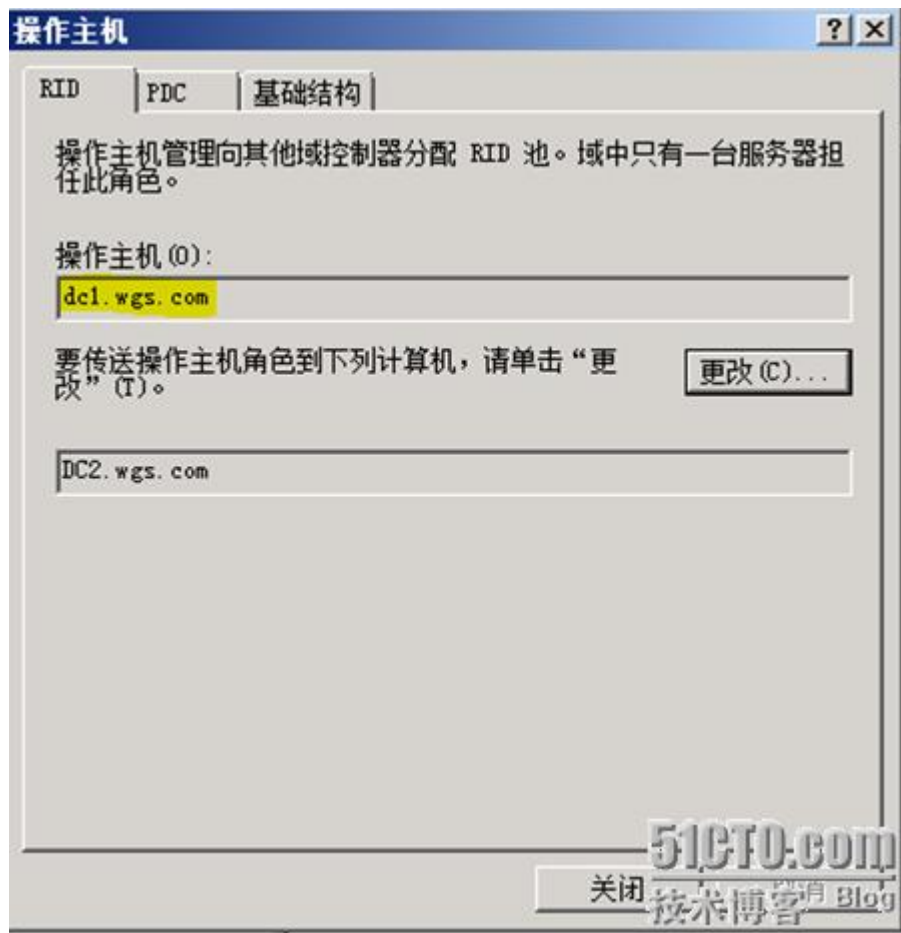
键入 connect to server dc1 按 enter 连接到 dc1 上；

```
server connections: Connect to server dc1
绑定到 dc1 ...
用本登录的用户的凭证连接 dc1。
server connections:
```

接着键入 quit 退出连接界面，在角色管理界面中键入“Transfer RID master”，弹出提示 “是否转移操作主机”，选择“是”。

```
fsmo maintenance: Transfer RID master
服务器 "dc1" 知道有关 5 作用
架构 - CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=
=Configuration,DC=wgs,DC=com
命名主机 - CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-First-Site-Name,CN=Site
s,CN=Configuration,DC=wgs,DC=com
PDC - CN=NTDS Settings,CN=DC2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=
Configuration,DC=wgs,DC=com
RID - CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=
Configuration,DC=wgs,DC=com
结构 - CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=
=Configuration,DC=wgs,DC=com
```

再回到图形界面中查看，可以看到操作主机又被转移到了 dc1.wgs.com 这台 DC 上，如下图：



这样就把 RID master 又转移到了 dc1.wgs.com 这台 DC 上，当然其他的五个操作主机都可以象这样的做法传送。

通过这一篇文章，您了解到域内必须唯一的操作主机 RID master 的相关功能和转移的操作方法。



BLOG.51CTO.COM

操作主机 Infrastructure Master

今天跟大家介绍的是域环境下第三个操作主机:Infrastructure Master(基础结构主机)

Infrastructure Master 的作用是:当你的域环境中的组内成员如果来自其他域的话(比如你把其他域的用户加入到当前域的组中),在 DC 间在进行 AD 数据复制的时候就必须维护当前域的成员(比如想要知道组内成员是否有变更了,就必须到 Infrastructure Master 上去做查询).也就是用来确定当前域和其他域之间对象的引用关系的,并且在一个域内必须是唯一的.

也正因为这样 Infrastructure Master 只在多域环境下起作用,在单域环境下是不会用到 Infrastructure Master 的。

要查看 Infrastructure Master ,只需在 DC 上打开"Active Directory 用户和计算机",



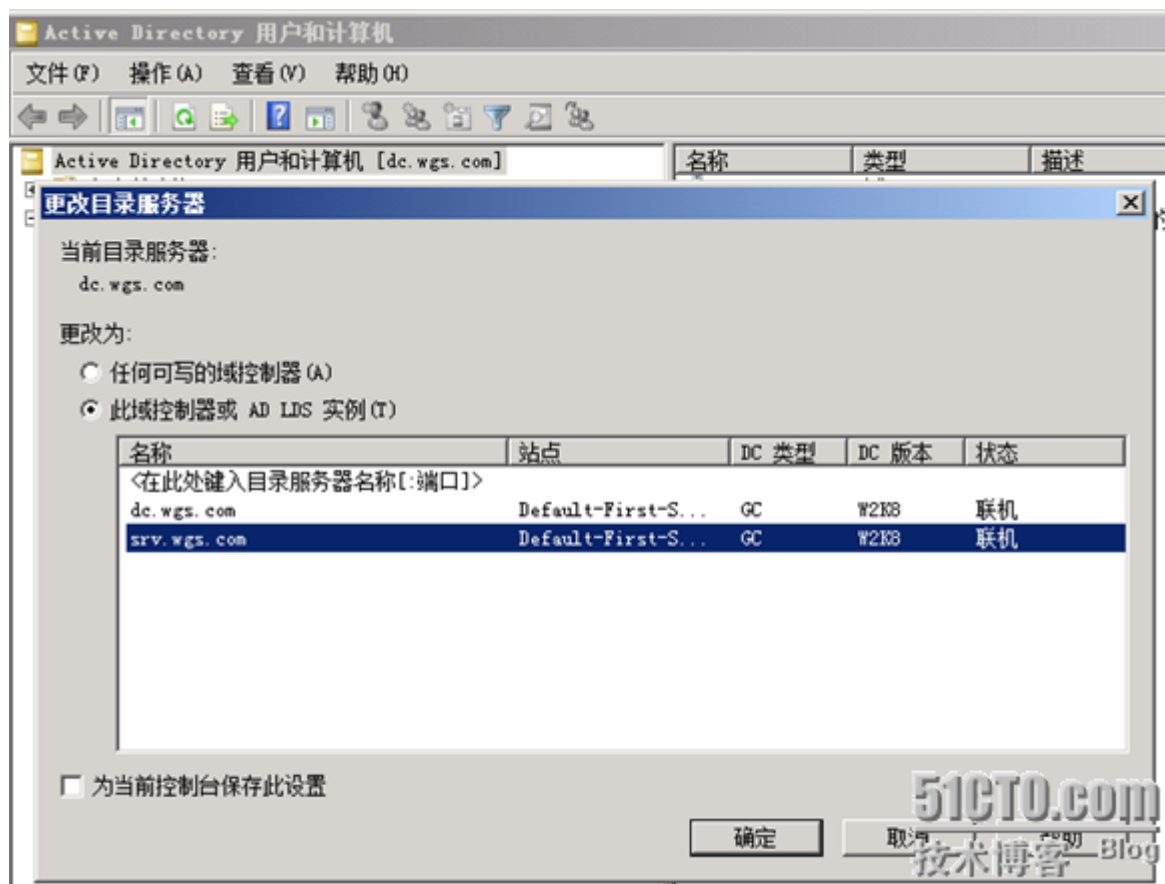
然后鼠标右击当前域"wgs.com",选择"操作主机",



就会打开操作主机的管理界面,然后选择"基础结构"选项卡,就可以看到当前的 Infrastructure Master 是 "dc .wgs.com"这台服务器.



如果要作转移，就和本系列七讲过的 RID Master 一样，首先如下图所示，连接到另外一台服务器“SRV.wgs.com”



再打开操作主机的操作界面，选择“基础结构”选项卡，再选择更改，这样就可以完成操作主机的转移了。



今天，咱们再说一个在转移操作主机时采取的非常规转移方法（应用场景：原来放置 Infrastructure Master 的那台 DC 已经坏掉了，没办法适用的情况下）：

打开在需要放置操作主机的 DC 上，打开命令提示符，输入 ntdsutil

```
CA 管理员: C:\Windows\system32\cmd.exe - ntdsutil
Microsoft Windows [版本 6.0.6001]
版权所有 (C) 2006 Microsoft Corporation. 保留所有权利。

C:\Users\Administrator>ntdsutil
ntdsutil: _
```

在 ntdsutil 管理界面中键入 Roles

```
ntdsutil: Roles
fsmo maintenance: _
```

再键入 connections，进入 connections 界面

```
fsmo maintenance: Connections
server connections: _
```

连接到服务器“DC”

```
server connections: Connect to server dc
绑定到 dc ...
用本登录的用户的凭证连接 dc。
```

然后键入 quit 命令退回到 FSMO 管理界面，使用 seize Infrastructure Master 强行覆盖操作主机就可以了（其他的操作主机也可以用同样的方法强行覆盖转移）。

Seize infrastructure master	- 在已连接的服务器上覆盖结构角色
Seize naming master	- 覆盖已连接的服务器上的命名主机角色
Seize PDC	- 在已连接的服务器上覆盖 PDC 角色
Seize RID master	- 在已连接的服务器上覆盖 RID 角色
Seize schema master	- 在已连接的服务器上覆盖架构角色

注意：如果我们在域环境中，使用了以上覆盖的方式转移了操作主机，那么一定要确保原来放置操作主机 Infrastructure Master 的那台 DC 不能上线，就算把他修好了也要把它摧毁，否则就会在当前域出现两台操作主机 Infrastructure Master，这样就会出问题。

通过今天，大家就可以了解到操作主机 Infrastructure Master 的作用以及如何转移和强占（覆盖）操作主机。

操作主机 Schema Master

今天要跟大家介绍的是AD中的操作主机 Schema Master(架构主机) 他的功能以及如何实现转移。

要管理 Schema 必须用到一个 mmc 的管理组件中的名为“Active Directory 架构”这么一个工具，但是这个工具默认并没有注册。

所以我们要必须先注册：

1、打开命令提示符：

2、键入：regsvr32 schmmgmt.dll(嵌入式管理组件“Active Directory 架构”的动态连接库文件是 schmmgmt.dll，可以用 regsvr32 把它注册到 mmc 里面去。)



3、注册成功后，我们就可以打开 mmc 的工具了，



4、在 mmc 中加入一个管理单元，点击文件--添加/删除管理单元，在窗口左边就可以看到一个名为“Active Directory 架构”的管理组件，选中并添加；

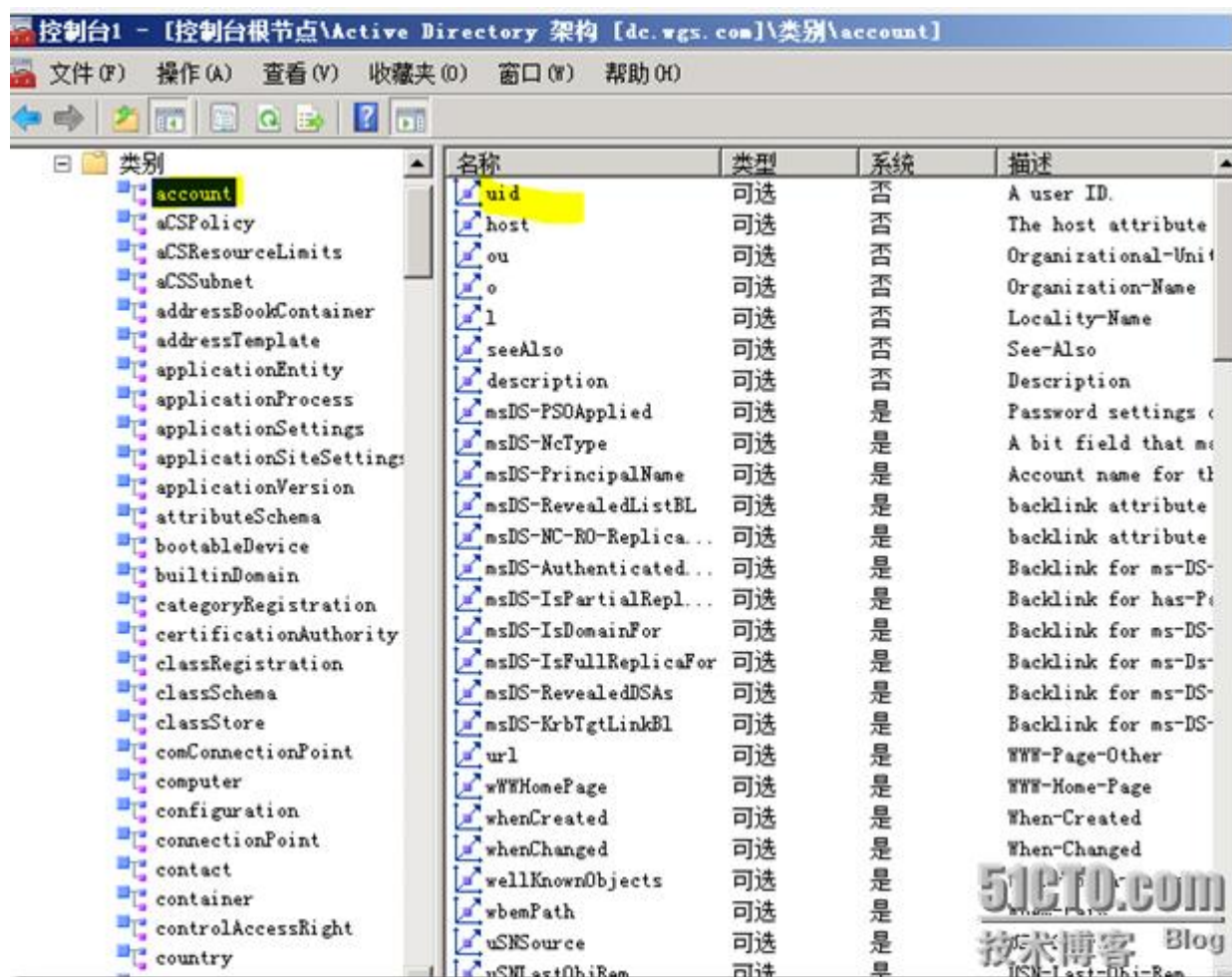


5、确定后如下图，就打开了这个管理组件，展开“Active Dircetory 架构”节点后，可以看到两个东西，一个是类别、一个是属性。

那么这里先来介绍下什么叫 Schema, Schema 在 AD 里所扮演的角色就是用来定义 AD 里面的结构的（举个例子说：AD 的对象中会有用户，那么用户会有多少个属性？比如：密码、显示名、登录名、部门、电话等等的栏目。那么，就必须定义这些东西。用来定义对象的东西我们叫“类别”，那对象里面的属性比如刚刚所说的用户这个对象的属性有密码、部门、电话就由下图中大家看到的“属性”来定义。）



举个例子：account 类别 会有很多属性，比如 uid 等等，如下图所示：



所以在这个工具中你可以进行 Schema 的管理，比如建立帐户的属性啊、建立新的类别以及他们的关系等。

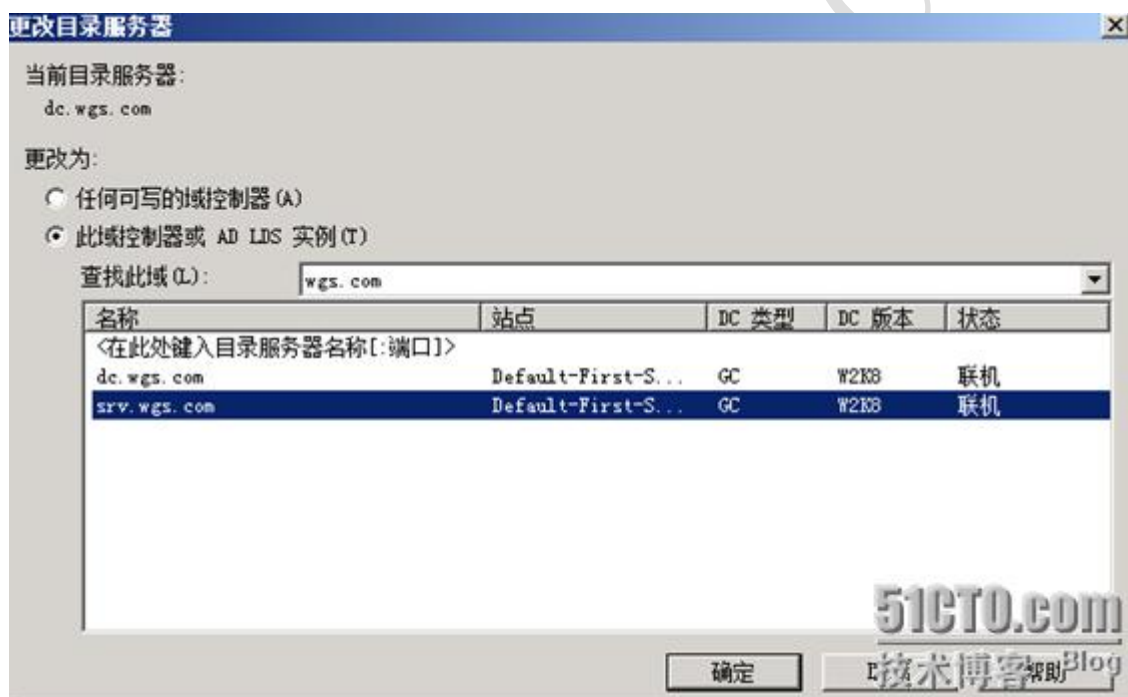
6、那么接下来我们要谈的是 Schema Master：在 AD 的五大操作主机角色里面，Schema Master 就是负责修改 Schema 的。也就是说在整个森林里面，假设我所用的这台机器是我的 Schema Master 的话，那么只有这台机器里面的那一份 Schema 是可以被修改的，那么其他 DC 上的那一份 Schema 则是只读的。这就是 Schema Master 他的功能。

7、查看 Schema Master:

在“Active Directory 架构”上按鼠标右键，可以看到一个“操作主机”，然后选择它，就可以看到当前的操作主机 Schema Master（架构主机）就是我所使用的这台机器“DC”



如果说要做转移到另外一台的话，就需要先连到另外一台 DC，比如我就连到 SRV 这台了



就会有一个提示说他是只读的，不能修改 Schema 的，因为当前的 Schema Master 是 DC 那一台，并不是 SRV 这台。



接着我选择操作主机，目前我是连接到 SRV，可是我的 Schema Master 却还是原来的 DC 那一台。所以我按更改，再点是，如下图所示：



这样操作主机 Schema Master 就转移到了 SRV 这一台。

当然，你也可以使用 `ntdsutil` 的这个命令在命令提示符中去作操作主机的转移。

通过今天的讲解大家可以了解到操作主机之一 Schema Master（架构主机）他的功能和转移的方法。

补充一句，在整个林下它必须是唯一的,而且只有你在修改它(比如安装 Exchange 的时候)才会用到他,所以平常并不会使用到 Schema Master。

操作主机 Domain Naming Master

本次为大家介绍 AD 的五大操作主机中的最后一位:Domain Naming Master (域命名主机).

在域环境中必须有一个机构来储存整个 AD 的架构(比如说整个域环境中哪一个域在哪一个域的下面,这样的树状结构必须有一个地方去记录).

那我们现在来稍微看一下,在系统管理工具里可以找到 Active Directory 域和信任关系这一项.我们打开他就可以看到整个 AD 的树状结构.那么必须有一台机器可以去维护这个树状结构,当 AD 的树状结构变动的时候,就需要找这台机器去做修改.

我们可以在 "Active Directory 域和信任关系" 上按右键,选择"操作主机".大家可以看到域命名主机,就是 Domain Naming Master.同时也可以在这里做这个操作主机的更改,也就是操作主机的转移的动作.

我们可以再次 右键 "Active Directory 域和信任关系" 选择连接到另一台服务器,再选择另一台 DC 后,确定连接到另一台 DC.

接着在 "Active Directory 域和信任关系" 上按右键,选择"操作主机",此时选择更改.那么咱们的 Domain Naming Master 就转移到另一台 DC 上了.

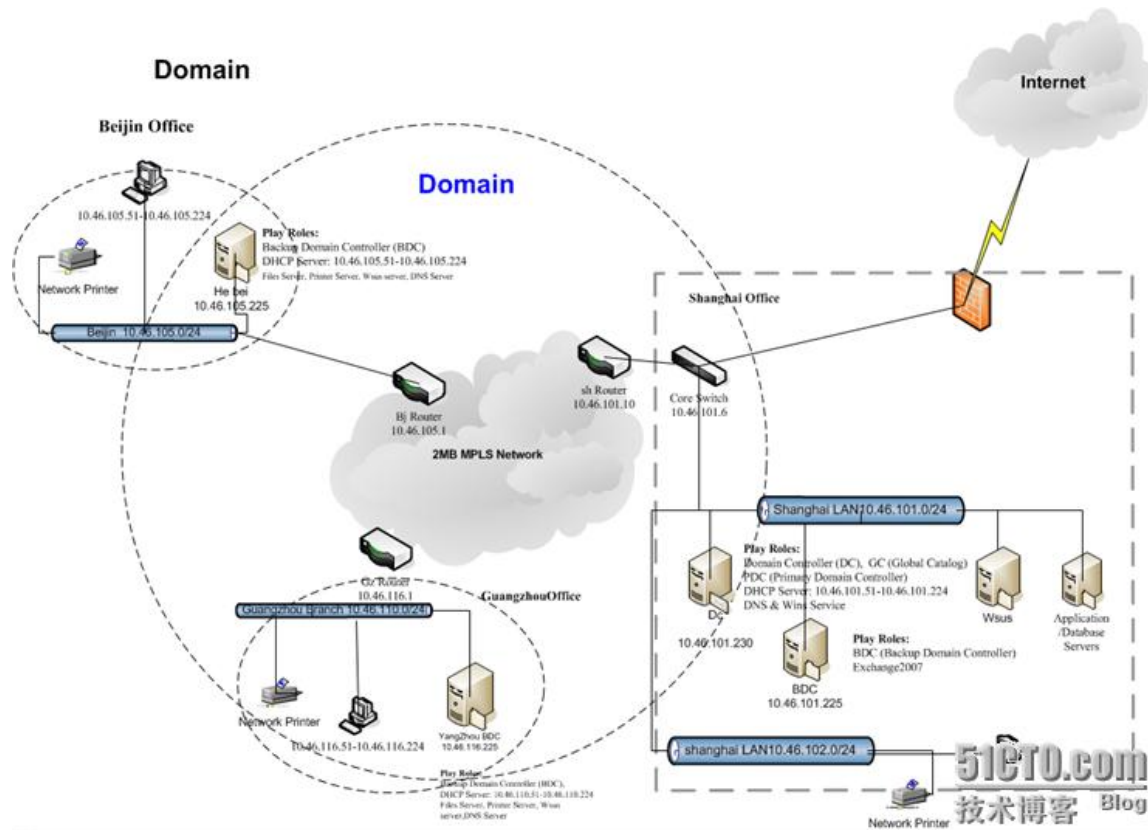
当然你也可以使用命令行的方式用 Ntdsutil 工具进行操作主机 Domain Naming Master 的转移工作.具体做法请参考:

<http://angerfire.blog.51cto.com/198455/212380>

域控制器位置的选择

五个操作主机的作用通过前面几篇文章的介绍大家都已经了解了,那么如何选择操作主机在企业网络中的位置来让五大操作主机发挥他们的最佳功效来实现活动目录服务的最佳运作呢?

今天我们来举例说明下, 请看下面这幅网络拓扑图:



在网络中 DC 要放置在哪一个网段呢? 因为 DC 在网络中的作用就是让用户能够在做 AD 查询时很方便的找到他, 来做查询、登陆的动作。

所以假设我有多个站点的话, 比方上图中我有北京、上海、广州 3 个站点, 那么就必须要保证每个站点中都有一个 DC, 来避免跨站点做查询。比如我们在北京登陆, 如果在北京没有 DC 的话那么我们需要去上海或者广州做查询登陆, 那么效率肯定会很低。

于是我们总结出第一个规则: 每一个站点中必须有至少一个 DC。

而 DC 上有很多角色, 比如有一个角色叫做 GC, 那么哪些域控制器上应该有 GC 呢?

建议每一个站点中至少有一个 GC (通用类别目录), 可以让当前站点中的用户可以到这个 GC 做查询、登陆的动作。

另外, 我们今天所说的重点五个操作主机应该如何选择位置呢? 那么现在咱们分别来看。

首先是 RID master, 它是负责去生成 RID 号, 并分给其他的 DC。而在 IT 环境管理过程中只有网络管理员才做 AD 对象的创建工作 (比如创建用户、组、计算机帐户时), 所以建议 RID master 就放置在靠近网管人员的地方 (因为只有网管人员去建帐号时, 才会使用 RID master);

PDC Emulator 的 5 个作用 (1、时间同步或者叫对时 2、模拟 NT 的 PDC 3、给 NT 以前的客户端改密码 4、密码仲裁 5、防止重复套用户策略) 都是面向客户端的, 所以建议这个操作主机放置的距离用户近些;

基础结构主机呢，主要是负责多域环境中组跟用户、组跟组之间的对象引用关系维护的。所以只有在网络管理员进行更改组之间的关系组和用户之间的关系（比方把 A 域的全局组加入 B 域的本地域组的时候，也就是使用 AGDLP 规则的时候。）建议放置到离 IT 管理人员近的地方。

域命名主机和架构主机也分别是在网络管理员创建子域（此时使用域命名主机）和部署 exchange（此时需要更改 AD 架构，会使用到架构主机）时，所以建议也放在靠近 IT 人员的地方。

总结一下，当您要决定域控制器应该放在哪里的时候，请考虑下面三条规则：

一、每一个站点中必须有至少一个 DC；

二、每一个站点中至少有一个 GC；

三、五个操作主机的位置：

a、RID master、基础结构主机、域命名主机、架构主机这四个

主机靠近网管人员；

b、PDC Emulator 靠近用户。

注：关于站点的概念在后续文章中跟大家做详细介绍。

组织单位的管理权委派

本次跟大家介绍如何通过 AD 组织单位(下文中简称 OU)委派,从而让公司的每个部门都可以自行管理自己部门中的用户账户。

首先介绍下应用案例,被国际偷菜组织授予 09 年度最有价值偷菜专家称号的某电力公司业务主管 A 某。在做年终总结时,除了总结了全年的业务数据之外,还总结了在 09 年使用高度集中管理的信息化方案后对业务管理带来的利弊(在请 IT 部门主管 S 某一顿牛魔王烤鸡翅之后)。同时重点提出了一些需要改进的问题:主要就是 IT 权限过于集中,各个部门不能自主管理员工账户(尤其是业务部经常需要根据市场的变动及时的做人员功能及结构的调整)。最后提出了对于 2010 年 IT 环境的希望:希望每个部门可以自行管理自己部门中的用户账户。

针对 A 某的需求,IT 主管 S 某迅速定制了实现其需求的评估方案,并组织部门内的技术骨干--老 T 和技术尖兵--小 P 在 3 天内搭建起了评估环境。

评估环境简介:

域控制器:1 台

系统版本:windows server 2008 企业版

ip:192.168.99.1/24

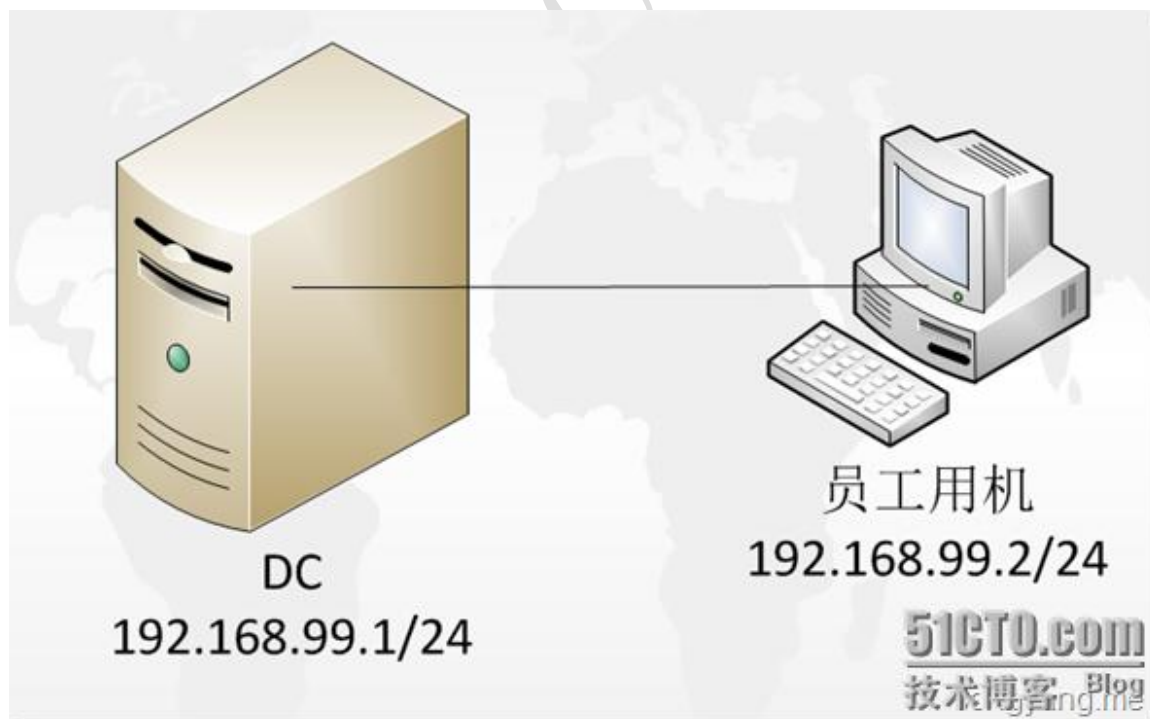
DNS:127.0.0.1

员工用机:1 台

系统版本:windows7 旗舰版

IP:192.168.99.2/24

DNS:192.168.99.1



操作步骤:

1 创建 OU 和用户账户;

使用管理员账户登录 DC, 打开"Active Directory 用户和计算机"在域下创建一个名为"_DEMO"的 OU, 并在此 OU 中创建名为"manager"的用户;

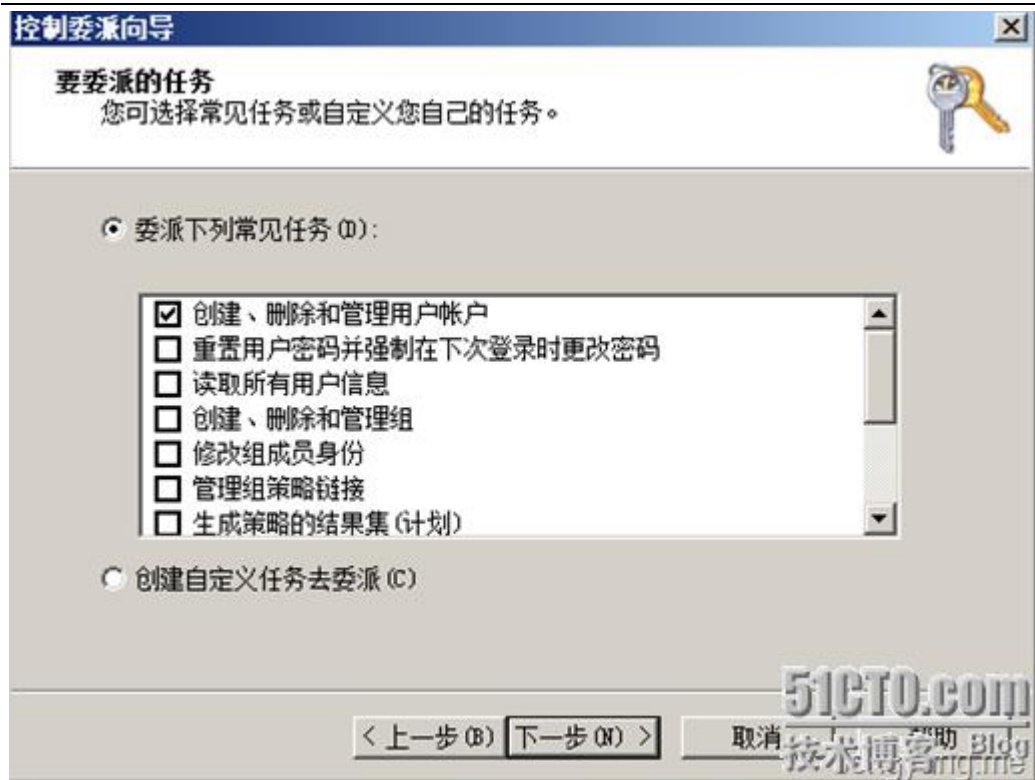


2 为部门经理账户委派管理用户账户的权限；

右击 “_DEMO” OU 选择“委派控制” 打开委派控制向导，下一步后添加要被委派权限的用户账户“manager”



下一步，再勾选需要委派给“manager”用户的具体权限



然后下一步，确认配置后完成，这样就为“manager”用户委派了管理创建和删除“_DEMO” O U 中用户账户的权限。

3 为部门经理的 PC 安装管理工具。

首先，去微软官网下载管理工具包：

<http://www.microsoft.com/downloads/details.aspx?displaylang=zh-cn&FamilyID=7d2f6ad7-656b-4313-a005-4e344e43997d>

然后以域管理员身份登录为用户安装(后续文章中为大家介绍使用组策略分发的方式)

4 分析委派的权限

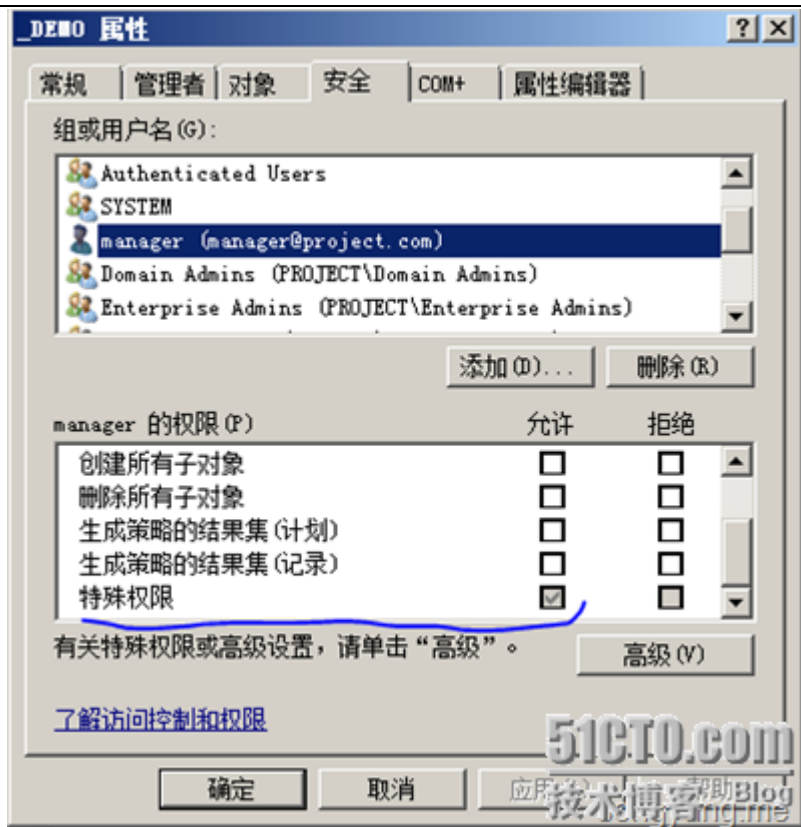
a 显示高级功能

打开 “Active Directory 用户和计算机” 中的高级功能(勾选下图所示部分)

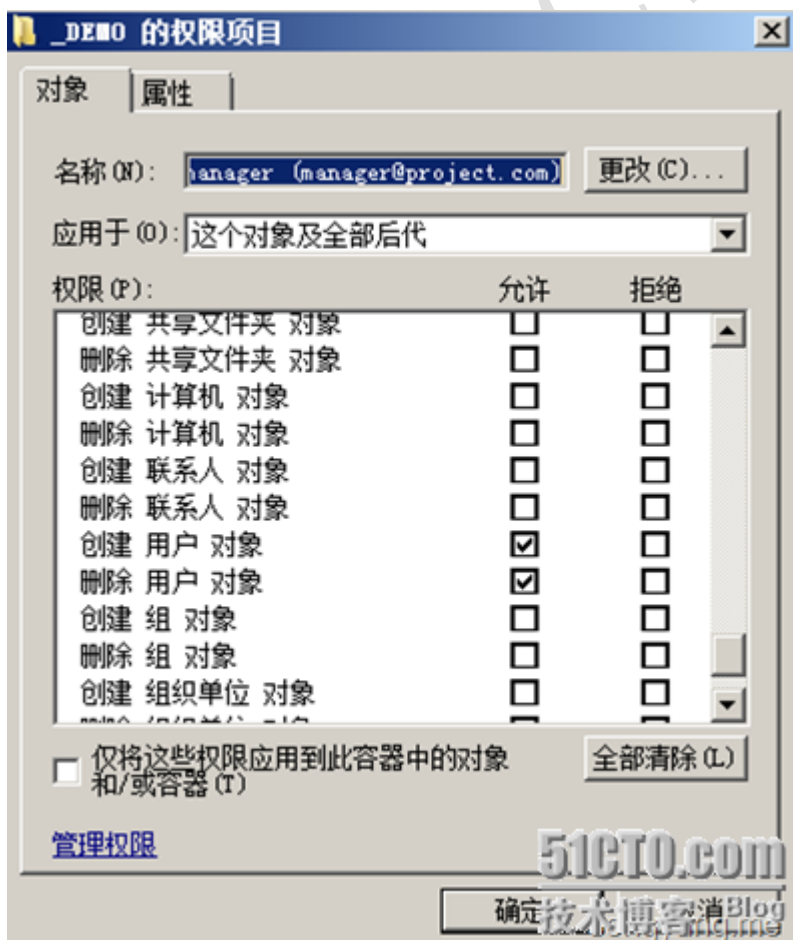


b 查看被委派的权限：

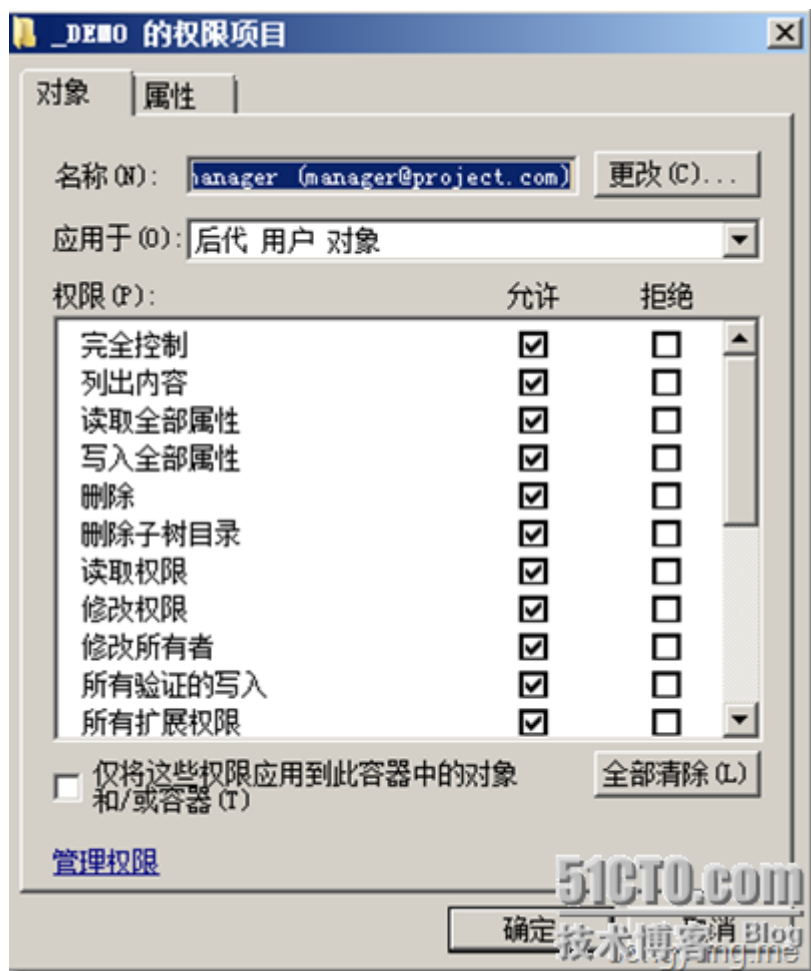
右击“_DEMO”选择属性 中的安全选项卡，可以看到 manager 有特殊权限。



可以通过下图可以看出部门经理具有创建删除用户的权限



可以通过下图可以看出部门经理具有对此 OU 中所有用户对象的完全控制的权限



总结:通过今天的学习大家可以认识到通过 OU 委派可以为企业定制更加灵活的管理方案,同时也为企业及时调整人员职能提供了充分的 IT 支持。

为企业用户配置专有 UPN 后缀

本次课程咱们介绍一下传说中的 UPN 后缀的设置及其应用场景。

应用案例介绍：

张飞同志在改革开放的浪潮中把祖传绝学老张家臭豆腐的招牌越做越响，响彻国内外。成为全球最为畅销产品，并申请了国际专利。为了加速老张家臭豆腐市场的盈利，张飞张老板引进了加盟连锁的营销模式。张老板在读完 MBA 后，决定用网络推广+网络营销这样现代化的营销手段再创新高。张老板的生意可以说是如火如荼了，但是张老板还有一件十分棘手的事情急需解决，那就是在采用了微软的 AD 环境进行全球营销网络建立之后，有很多加盟店的用户，总是记不住加盟账户，经常来电或者邮件反复所要登录账户密码（这里存在严重的安全隐患，而且还延误商机）。在一次全球视频会议上，一位拉斯维加斯的加盟商提出：如果能够使用自己平时跟用户联络时用的 E-Mail 账户登录，那就不会忘记了。于是老张家臭豆腐集团全球荣誉总裁兼董事长张总找到我，商量了对策之后决定采用 UPN 后缀来解决这个问题。

评估环境介绍：

DC1 台

IP: 192.168.99.1/24

DNS:127.0.0.1

客户机 1 台

IP:192.168.99.2/24

DNS:192.168.99.1

操作步骤：

1、设置 UPN 后缀：

使用管理员账户在 DC 上登录打开“Active Directory 域和信任关系”

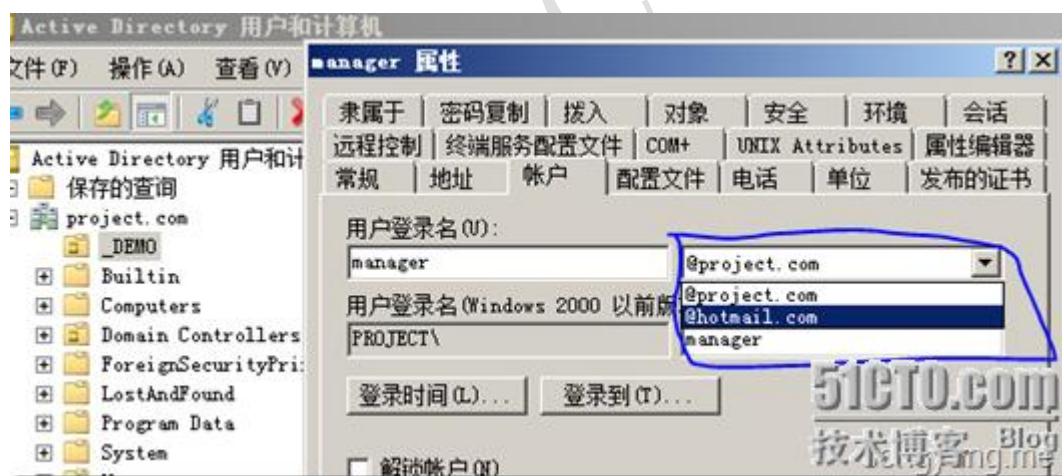


右击“Active Directory 域和信任关系”选择属性，并添加 UPN 后缀（比如拉斯维加斯的那位老板用的是 Hotmail 的邮箱）那么只需要为用户创建一个和他 hotmail 账户相同的用户名就 OK 了。



2、为用户指定 UPN 后缀;

打开“Active Directory 用户和计算机”右击需要更改 UPN 后缀的用户账户，选择属性中的账户选项，并为其选择新的 UPN 后缀



3、在客户机上使用新 UPN 后缀的用户账户登录验证。

在客户机上选择切换用户并键入新的登录名 manager@hotmail.com 和用户密码 登录成功。



总结：通过本次课程的学习，大家可以认识到如何使用 UPN 后缀的设置来满足企业中对登录名后缀有特殊需求的用户。

ADMT3.1 快速迁移域用户账户和组

在 windows server 2008 的 AD 维护工作中，我们可能需要将当前域的用户账户和组转移到另外一个域中（这个动作我们称之为迁移）。

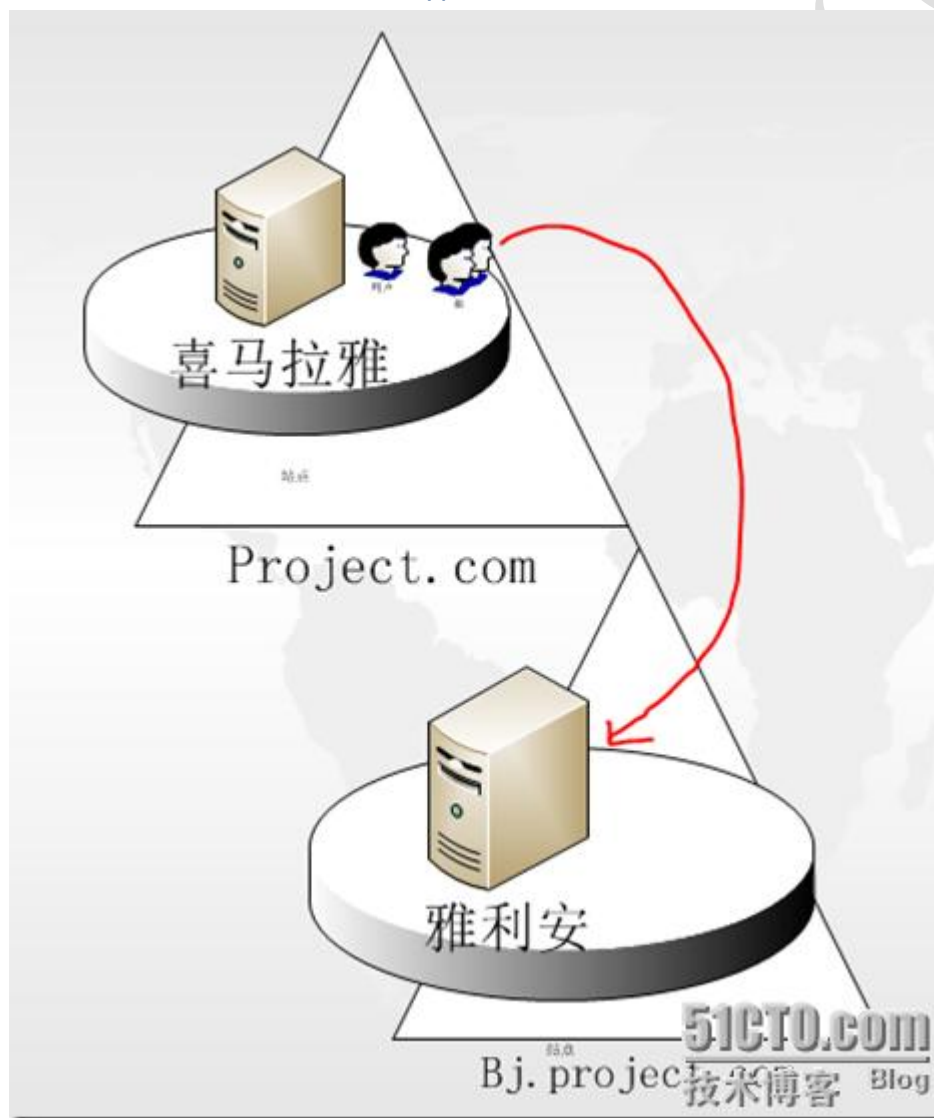
在雅利安星际疫苗接种公司工作的 windows 网络管理员号称不重疫苗也能顶的灵灵狗同志，正在为一件棘手的工作事件发愁。

雅利安公司因为研制出可以成功抵御十全星际流感的疫苗，在整个银河系名声大震，巴斯股（3009 年最火爆的星际股市）也一路狂涨。同时，兼并了太阳系的喜马拉雅驴友公司。

喜马拉雅公司的精英研发部门“珠穆朗玛二部”也被收编进了雅利安公司的研发部。因为所有的资源管理都是基于活动目录的，所以灵灵狗同志需要将“珠穆朗玛二部”的所有员工账户和组迁移转移到雅利安公司的域下。

在查询了无所不知的位于雅利安星球的知识古树后，灵灵狗拨通了远在银河系另一端的地球村的 AD 客户支持部的售后电话。

按照客服妹妹的指导，灵灵狗使用 Hyper-V3009 快速的搭建起了虚拟的评估环境。具体如下：



灵灵狗同志看完客服妹妹同步过来的指导文档后很顺利的使用域管理员在喜马拉雅公司的 project.com 域上登录了。

打开“Active Directory 域和信任关系”，可以看到两个域，现在要把属于 project.com 的域用户账户和组（原喜马拉雅公司）移动到 bj.project.com(雅利安公司)



具体的账户可以通过下图看到，在 “_Demo”OU 中有 user1 、 manager 两个用户和 group 组，其中 user1 属于 group 组。



在确认了上面三点要素后，客服妹妹发来了专门的迁移工具 ADMT3.1 （2008 的活动目录迁移，必须使用 ADMT3.1 版本的工具 3.0 是不行的。客服妹妹很细心的边指导边解释着。）

在妹妹的指导下，灵灵狗打开了嵌套在管理工具中的 “Active Directory 迁移工具”，并右键点击。



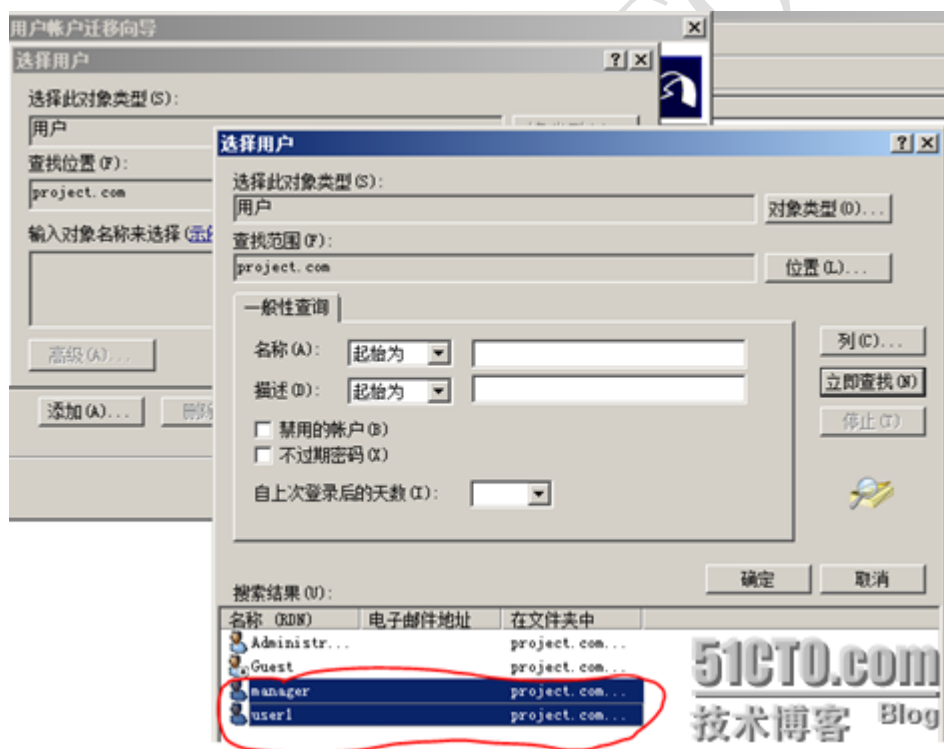
在出现的如上图的选项中，选择了用户账户迁移向导。



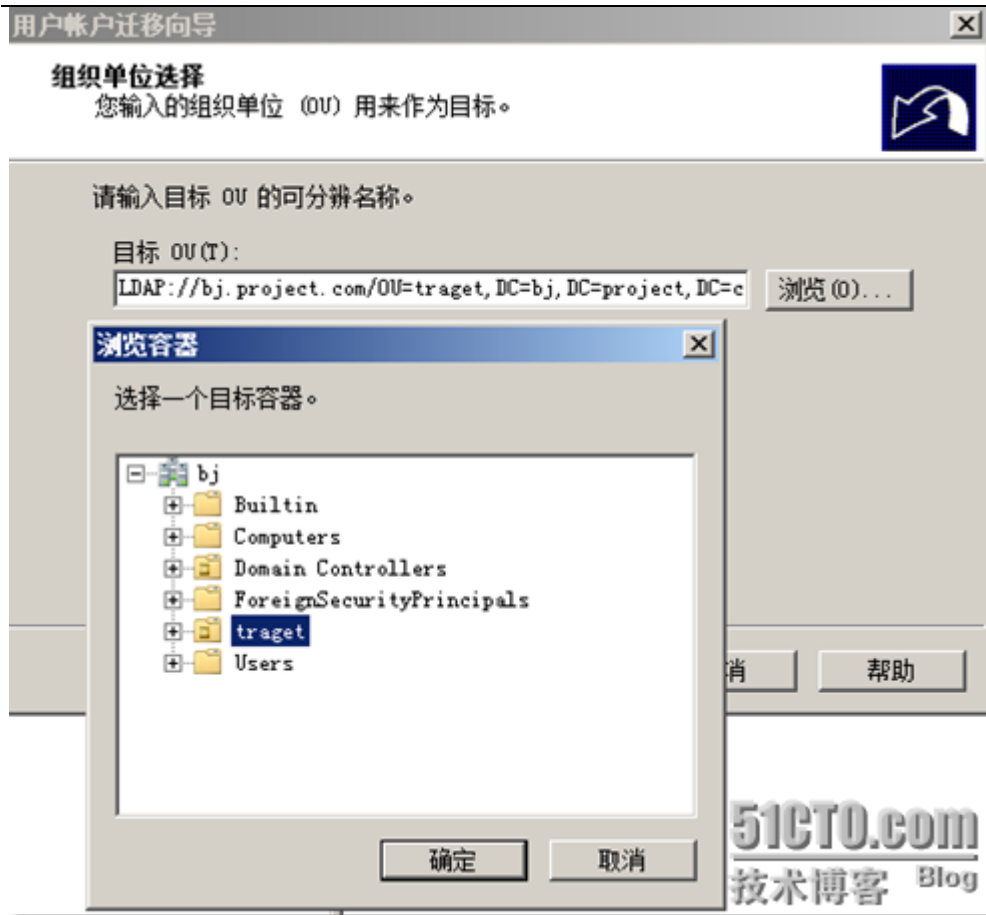
第一步需要设置用户账户迁移的源（project.com）和目标(bj.project.com)。



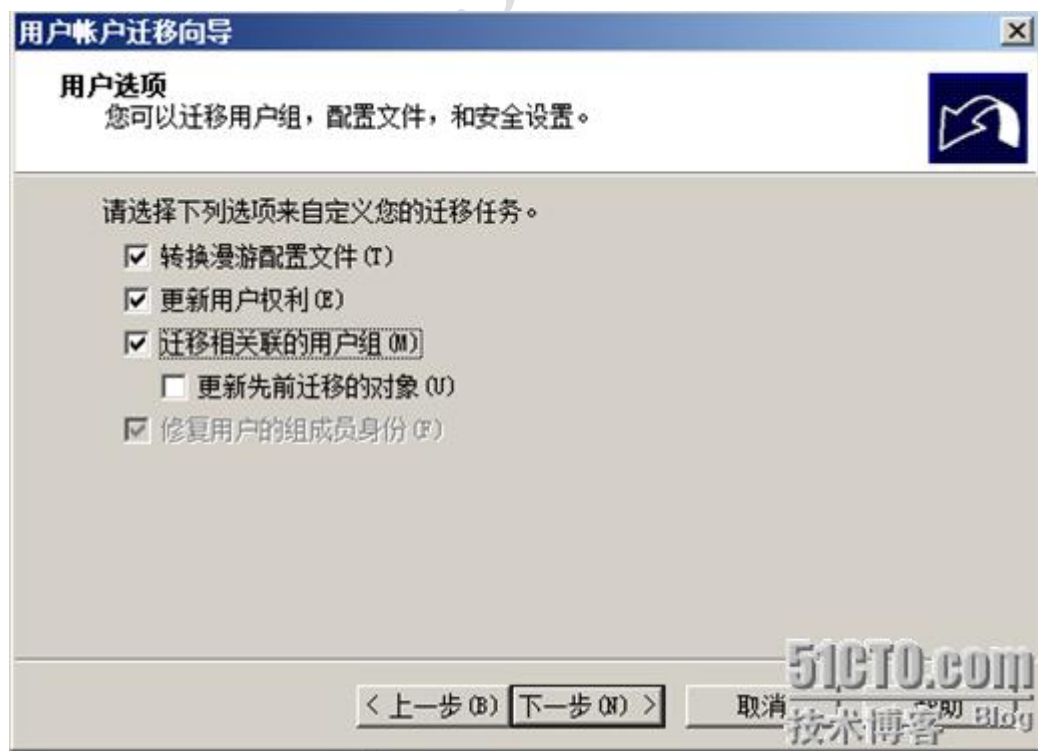
第二步从源域（project.com）中选择需要迁移的用户账户



第三步：选择要转移到的目标域中的目标 OU（灵灵狗够灵的，已经在妹妹的提示下提前在目标域创建了用于存放转移过来的用户账户的专用 OU“target”）

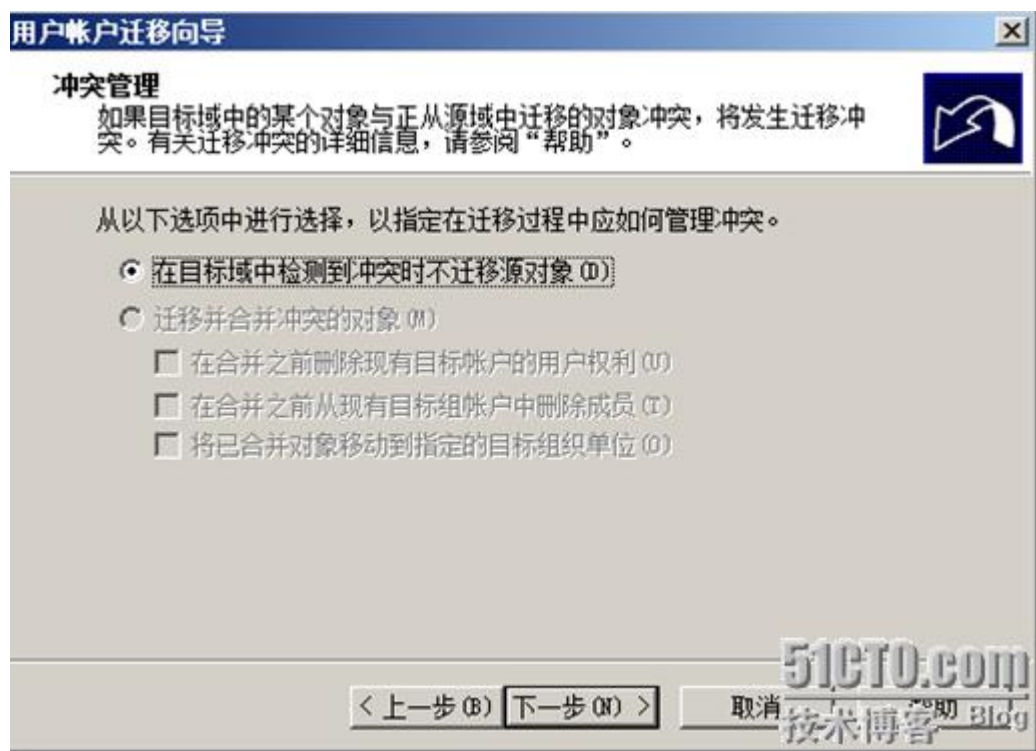


第四步：此时灵灵狗同志看不明白了，不敢轻易选择。（客户妹妹及时的做了提点：此时您需要选择转移动作时的用户选项，比如用户的配置文件、权限以及相关的组是否要一起迁移到目标域去，如果要一起迁移这些属性的话，请您勾选。）灵灵狗毫不犹豫的勾选了。



第五步：冲突设置：本项默认就帮您选择了，也就是说当做用户账户转移动作时如果检测到目标OU中有相同的用户账户那么就不会做转移的动作。

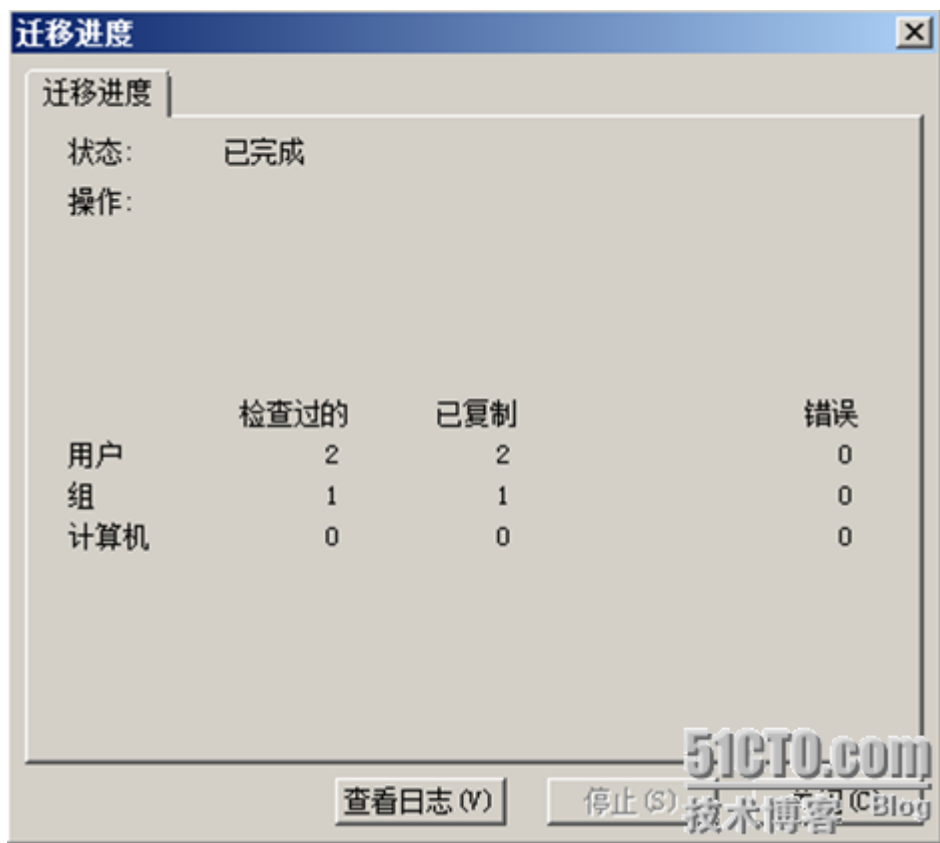
来保证目标域原有的用户账户不会被替换而导致数据丢失。（客服妹妹继续耐心的解释着.....）



第六步：点击完成后开始转移账户



完成后会出现一个完成报告，通过下面的报告，您可以看到已经成功转移了刚刚的两个用户账户和一个组。



通过查看日志可以看到更加详细的转移信息如下:

[设置节]

任务: 用户迁移(1)

ADMT 控制台

用户: PROJECT\Administrator

计算机: shanghai.project.com (SHANGHAI)

域: project.com (PROJECT)

OS: Windows Server (R) 2008 Enterprise 6.0 (6001) Service Pack 1

源域

名称: project.com (PROJECT)

DC: shanghai.project.com (SHANGHAI)

OS: Windows Server? 2008 Enterprise 6.0 (6001) Service Pack 1

OU:

目标域

名称: bj.project.com (BJ0)

DC: bj.bj.project.com (BJ)

OS: Windows Server? 2008 Enterprise 6.0 (6001) Service Pack 1

OU: LDAP://bj.project.com/OU=traget,DC=bj,DC=project,DC=com

林内: 是

更新权利: 是

转换漫游配置文件: 是

固定组成员身份: 是

51CTO 专家博客-----宋杨

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



冲突选项: 忽略

迁移组: 是

更新已迁移的对象: 否

迁移服务帐户: 是

[对象迁移节]

2009-11-21 17:02:23 启用帐户复制程序。

2009-11-21 17:02:26 从属于成员的全局组删除 CN=manager (LDAP://shanghai.project.com/CN=manager,OU=_DEMO,DC=project,DC=com):

2009-11-21 17:02:26 将 LDAP://shanghai.project.com/CN=manager,OU=_DEMO,DC=project,DC=com 移到 LDAP://bj.bj.project.com/CN=manager,ou=traget,dc=bj,dc=project,dc=com

2009-11-21 17:02:27 已更新 CN=manager 的用户权利

2009-11-21 17:02:27 从属于成员的全局组删除 CN=user1 (LDAP://shanghai.project.com/CN=user1,OU=_DEMO,DC=project,DC=com):

2009-11-21 17:02:27 从 LDAP://shanghai.project.com/CN=group,OU=_DEMO,DC=project,DC=com 上删除 LDAP://shanghai.project.com/CN=user1,OU=_DEMO,DC=project,DC=com

2009-11-21 17:02:27 将 LDAP://shanghai.project.com/CN=user1,OU=_DEMO,DC=project,DC=com 移到 LDAP://bj.bj.project.com/CN=user1,ou=traget,dc=bj,dc=project,dc=com

2009-11-21 17:02:27 已更新 CN=user1 的用户权利

2009-11-21 17:02:27 从属于成员的全局组删除 CN=group (LDAP://shanghai.project.com/CN=group,OU=_DEMO,DC=project,DC=com):

2009-11-21 17:02:27 将 LDAP://project.com/CN=group,OU=_DEMO,DC=project,DC=com 移到 LDAP://bj.bj.project.com/CN=group,ou=traget,dc=bj,dc=project,dc=com

2009-11-21 17:02:27 已更新 CN=group 的用户权利

2009-11-21 17:02:28 正在将成员更新到组 CN=group (LDAP://bj.bj.project.com/CN=group,ou=traget,dc=bj,dc=project,dc=com)。

2009-11-21 17:02:28 为 CN=user1 (LDAP://bj.bj.project.com/CN=user1,ou=traget,dc=bj,dc=project,dc=com) 重新建立组成员身份。

2009-11-21 17:02:28 将 LDAP://bj.bj.project.com/CN=user1,ou=traget,dc=bj,dc=project,dc=com 重新添加到 LDAP://bj.bj.project.com/CN=group,ou=traget,dc=bj,dc=project,dc=com 中

2009-11-21 17:02:29 完成操作。

最终打开目标域(bj.project.com)雅利安公司的“Active dircetory 用户和计算机”可以看到被成功转移过来的用户账户和组。



通过这次事件，灵灵狗同志除了掌握了用户账户的迁移方法外，又有了一个新的思路：以后域控制器物理升级的时候，也可以用 ADMT（活动目录迁移工具）来将旧 DC 上的数据迁移到新的 DC 上来实现 DC 的升级。

宋 杨

2009 年 11 月 21 日于西安