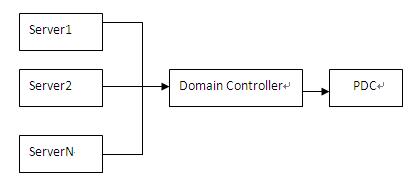
域控设定外GPS时钟源

前言：

 域控环境下的时钟同步原则

1).客户端与DC做时钟同步；2).DC与本域PDC做时钟同步；3).PDC与林根域PDC同步时钟；4).域 或 林的PDC与外部时钟源同步时钟；

在域环境中，只需设置根域控制器的外部时间源即可，其它服务器在添加进域中时将自动设置与域控制器时间同步。



组策略和GPO的区别是什么?

说到组策略，就不得不提注册表。注册表是Windows系统中保存系统、应用软件配置的数据库，随着Windows功能的越来越丰富，注册表里的配置项目也越来越多。很多配置都是 可以自定义设置的，但这些配置发布在注册表的各个角落，如果是手工配置，可想是多么困难和烦杂。而组策略则将系统重要的配置功能汇集成各种配置模块，供管理人员直接使用，从而达到方便管理计算机的目的。简单点说，组策略就是修改注册表中的配置。当然，组策略使用自己更完善的管理组织方法，可以对各种对象中的设置进行管理和配置，远比手工修改注册表方便、灵活，功能也更加强大。而GPO是组策略对象，是一种与域或组织单元相联系的物理策略每台计算机都有本地的GPO，可以通过运行gpedit.msc来定制也可以通过AD定义一个集中的策略.

正文：

相关参数的定义和相关指令：

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config下的AnnounceFlags为5．该设定强制主机将它自身宣布为可靠的时间源,但是如果是默认的10，就证明采用外面的时间服务器。

gpupdate /force :域控制器刷新策略

**w32tm.exe /config /update :**更新时间服务配置文件。

**Restart-Service w32time :**重启时间服务

net stop w32time   : 命令执行后，停止时间服务。

w32tm /unregister   : 命令执行后，删除已有w32tm时间服务配置。

w32tm /register  : 命令执行后，导入默认的时间服务配置。

net start w32time   : 命令执行后，启动时间服务。

To configure a client computer or a member server to sync time from the domain, run the following command:

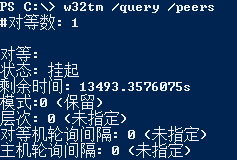
w32tm /config /syncfromflags:domhier /update

net stop w32time && net start w32time

一些默认情况下的时钟源状态  
1）查看DC中的PDC主机



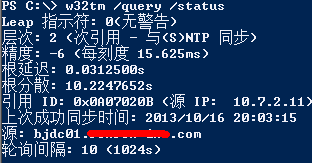
2）查看默认情况下的PDC的时钟同步对等列表、同步源主机地址和上次的同步状态



3） 查看默认情况下的其它DC的时钟同步对等列表、同步源主机地址和上次的同步状态

[](http://img1.51cto.com/attachment/201310/094650134.png)

[094650224.png](http://img1.51cto.com/attachment/201310/094650224.png)

[](http://img1.51cto.com/attachment/201310/094650100.png)

4） 查看默认情况下的域内Client计算机的时钟同步对等列表、同步源主机和上次的同步状态

[](http://img1.51cto.com/attachment/201310/094718702.png)

[094719670.png](http://img1.51cto.com/attachment/201310/094719670.png)

[](http://img1.51cto.com/attachment/201310/094719352.png)

3 在PDC域控制器执行时钟源的更改

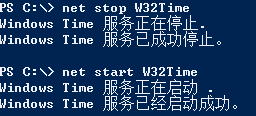
1） 指定同步列表IP

[094741975.png](http://img1.51cto.com/attachment/201310/094741975.png)

2） 指定同步源为上述同步列表

[094049563.png](http://img1.51cto.com/attachment/201310/094049563.png)

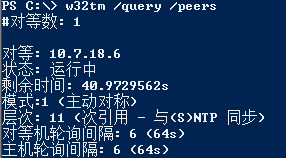
3） 重新启动时钟服务

[](http://img1.51cto.com/attachment/201310/094216830.png)

4） 手动执行时钟同步

[094311854.png](http://img1.51cto.com/attachment/201310/094311854.png)

5）查看同步后的一些时钟状态

[](http://img1.51cto.com/attachment/201310/094405289.png)

[](http://img1.51cto.com/attachment/201310/094405993.png)

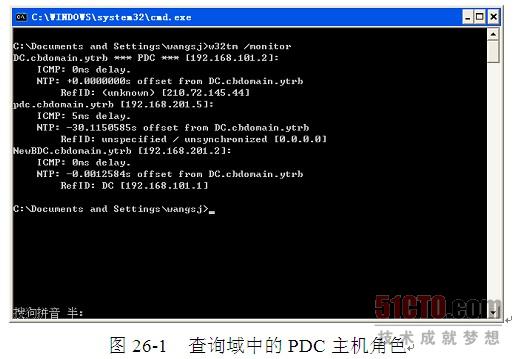
[094405916.png](http://img1.51cto.com/attachment/201310/094405916.png)

3．确认时间源

域用户登录后，使用"w32tm /monitor"命令确认当前计算机使用哪台DC作为时间源。

在命令行提示符下，键入如下命令。

w32tm /monitor



26.1.3  时间同步方式

服务器运行Windows Server 2012/2008/2008R2，客户端计算机运行Windows 7/8操作系统，可以通过"w32tm /query /configuration"查看时间同步设置，通过输出的"Type"字段判断计算机的同步方式。Type输出参数如表26-1所示。

表26-1  TYPE输出参数

|  |  |
| --- | --- |
| 输出参数 | 描    述 |
| Nosync | 客户端计算机不会同步时间，使用硬件时钟 |
| NTP | 客户端计算机从外部时间服务器同步，  时间服务器显示在NtpServer字段 |
| NT5DS | 客户端计算机通过域架构模式同步时间 |
| AllSync | 客户端计算机选择所有的同步机制，  包括外部时间服务器和域架构模式 |

此处开始为 域控 设置

方法1：直接修改注册表

在域控服务器CMD窗口运行 regedit，打开注册表

1、进入HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\W32Time\Parameters，修改NtpServer，由原来的 time.windows.com,0x9 改为 IP（时钟源的）,0x1 或者IP,0x8。IP为目标时钟源的IP，目标时钟源的标准时间可能是世界时（1）或者北京时（8）。

2、进入 HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\W32Time\TimeProviders\NtpServer，修改 Enable 为1。

3、进入HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\W32Time\TimeProviders\NtpClient，修改 Enable为1。

4、打开 cmd，运行以下指令：  
w32tm /config /manualpeerlist:IP（时钟源的）,0x1 /syncfromflags:MANUAL /reliable:YES

5、运行完以上指令后，重启windows Time 服务。在cmd窗口中，运行net stop w32time ，执行完毕之后，运行 net start w32time。

6、最后在cmd运行 w32tm /resync ，如果提示“成功地执行了命令”，则配置成功。

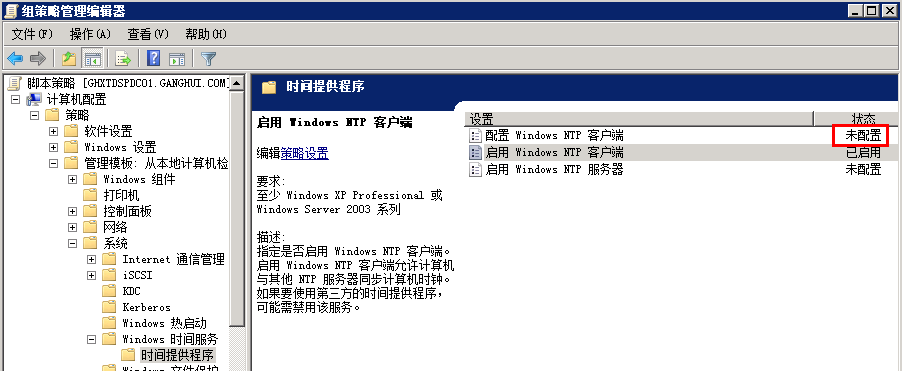
方法2 ：通过修改组策略

域控(PDC)所在OU的GPO，一定不要设定 NtpServer。 保持无设定状态使用系统默认设定即可。

GPO: Policies -> administratortive templates -> system -> windows time setting -> time providers -> Configure windows ntp client -> NtpServer

此处如果设定了时间服务器域名，将导致PDC时间同步错误。 类似如下：

具体原因是，在GPO内的设定，优先级比上述步骤1所做的设定高； 在此情况下，PDC基于此设定的时间同步尝试，将会失败；非PDC不在讨论范围内，所以不做说明。



如果已经配置会出现如下问题：

C:\Users\administrator.GANGHUI>w32tm /resync

将 resync 命令发送到本地计算机

此计算机没有重新同步，因为没有可用的时间数据。

C:\Users\administrator.GANGHUI>w32tm /query /source

Local CMOS Clock

6、设置同步间隔时间（校时周期）

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NtpClient\SpecialPollInterval

修改键SpecialPollInterval的值为十进制的604800（即为604800秒，1天）

7、查看事件日志-系统日志，查找w32time接收时钟同步信息

8、配置组策略，设置域成员的时间同步（**此策略一定不能影响PDC**）

1. 打开"Active Directory 用户和计算机"，在域上点右键，属性。组策略，打开。
2. 在"Default Domain Policy"上右键，编辑。
3. 计算机配置—管理模板—系统—Windows时间服务，双击"全局时间配置"，选择"已启用"。

修改MaxNegPhaseCorrection的值为3600（即为3600秒，1小时）

修改MaxPosPhaseCorrection的值为3600（即为3600秒，1小时）

修改AnnounceFlags的值为5

点"应用"，"确定"。

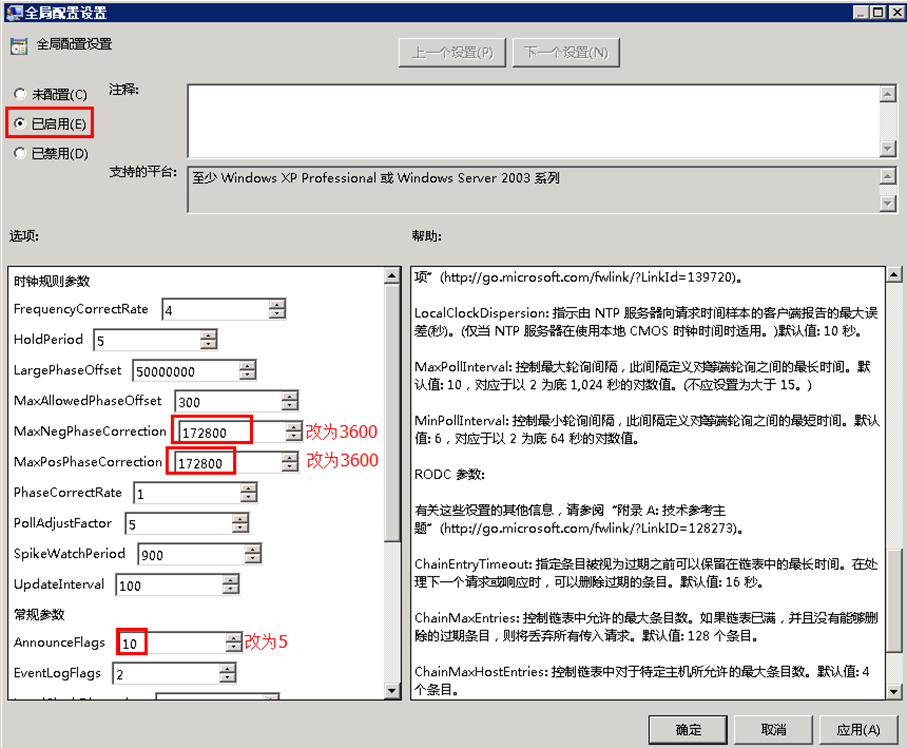
1. 计算机配置—管理模板—系统—Windows时间服务—时间提供程序，"启用Windows NTP客户端"，选择"已启用"。

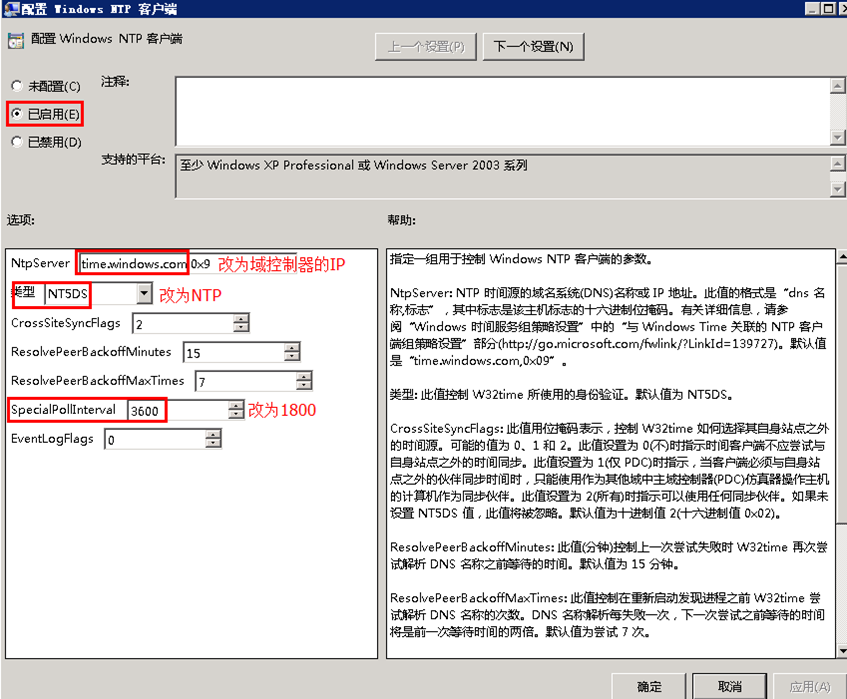
"配置Windows NTP客户端"，选择"已启用"。

修改NtpSever的值为ad-server.rybb.com,0x6

修改Type的值为NTP

修改SpecialPollInterval的值为1800（30分钟）





客户终端同步操作

本例中客户端计算机运行Windows 7操作系统，域用户登录网络后，通过以下命令确认客户端计算机的时间配置。

1．验证PDC角色所在的域控制器

在命令行提示符下，键入如下命令。

Netdom query FSMO

命令执行后，显示5种操作主机角色所在的域控制器，本例中PDC角色位于名称为"dc.book.com"域控制器中，如图26-2所示。

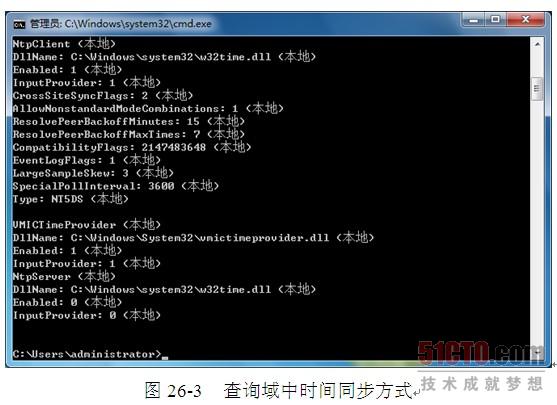
[](http://s5.51cto.com/wyfs02/M00/19/AF/wKiom1MT9qbx67a0AABWPZWsS2w519.jpg)

2．验证时间配置信息

在命令行提示符下，键入如下命令。

w32tm /query /configuration

命令执行后，输出当前计算机的时间配置信息。其中，Type类型显示为"NT5DS"，说明客户端计算机通过域架构模式同步时间，如图26-3所示。

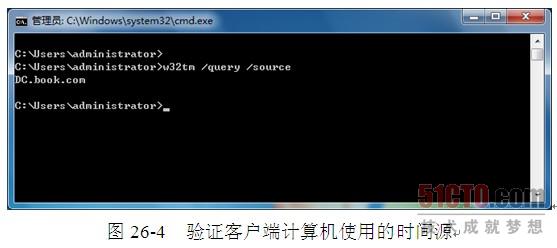
[](http://s1.51cto.com/wyfs02/M00/19/AF/wKiom1MT9rXDHJ8KAACdUIMJd7k726.jpg)

3．验证客户端计算机使用的时间源

在命令行提示符下，键入如下命令。

w32tm /query /source

命令执行后，查询当前客户端计算机使用的时间服务器，如图26-4所示。时间源服务器为"dc.book.com"，该服务器是域控制器，也是PDC所在的服务器。

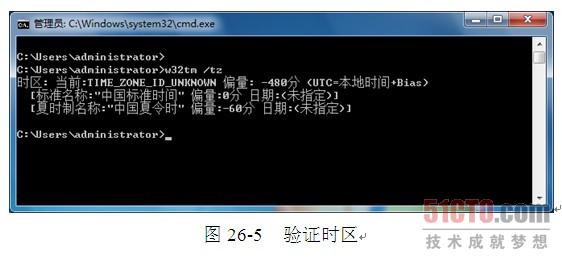
[](http://s3.51cto.com/wyfs02/M02/19/B0/wKioL1MT9rbSXaGDAABI3mbBfk4339.jpg)

4．验证时区

在命令行提示符下，键入如下命令。

w32tm /tz

命令执行后，显示客户端计算机的时区设置，如图26-5所示。

[](http://s8.51cto.com/wyfs02/M00/19/B0/wKioL1MT9wnQ7R4tAABeQiXqtbk243.jpg)

5．验证域中PDC

在命令行提示符下，键入如下命令。

W32tm /monitor /domain:book.com

命令执行后，显示域"book.com"中PDC角色所在的域控制器以及该域控制器的IP地址，如图26-6所示。

[](http://s2.51cto.com/wyfs02/M02/19/B0/wKioL1MT9x_jQedEAACFa2ZDoUs228.jpg)

同步域内时间方法一：net time 比较重要

Net time是Net命令组中的常用命令，Windows XP/7/8以及Windows服务器操作系统都支持该命令，确认域中的PDC主机角色后，可以使用该命令结合组策略，当用户登录域时自动和PDC主机时间同步。

第１步，确定域内的PDC主机所在的域控制器。

在命令行提示符下，运行"Netdom Server FSMO"命令，显示PDC主机角色所在的域控制器，如图26-8所示。PDC主机角色位于名称为"DC.book.com"域控制器中。

[](http://s2.51cto.com/wyfs02/M01/19/B1/wKioL1MT-IejqvNtAABjL7NrnyA305.jpg)

第2步，修改PDC使用的时间源。同步前，PDC主机如果能够接入互联网，通过手动或者自动方式同步时间。如果没有接入到互联网，网络中的计算机将PDC主机服务器的当前时间作为网络基准时间。

第3步，立即手动同步域内其他服务器（域控制器和成员服务器）的时间，使其与PDC保持一致。

在命令行提示符下，运行"net time /set"命令，手动方式和PDC主机同步。本例中PDC主机的IP地址为"192.168.0.1"。

Net time \\192.168.0.1 /set /y

命令执行后，立即同步当前计算机和PDC主机的时间，如图26-9所示。

[](http://s5.51cto.com/wyfs02/M01/19/B2/wKiom1MT-YzBjHzrAABpjw3MAoE421.jpg)

域控制器PDC和BDC （不太重要的东西，已下内容为转移主时间源域控的设置）

　　在域中只有一个主域控制器，它负责维护域中安全数据库，这个安全数据库会自动复制到域的备份域控制器中，备份域控制器可以升级为主域控制器，当服务器升级时，域安全数据库的最新备份会从旧的主域控制器复制一份到新的域控制器上，然后，旧的主域控制器会降为备份域控制器。

要将备份域控制器升为主域控制器，在“服务器管理器”窗口的计算机列表中，选择备份域控制器，从“计算机”菜单中选择“升级至主域控制器”，这个步骤可能会花上数分钟的时间，完成时，旧的主域控制器会自动还原为服务器状态。同样要将先前主域控制器降为服务器，在“服务器管理器”窗口的计算机列表中选择先前的主域控制器，在“计算机”菜单中，“升级至主域控制器”命令会变成“降级为备份域控制”命令，从“计算机”菜单中选择“降级为备份域控制器”，即可将PDC降为BDC。但在实际的操作中我没有这样做，我只是先把PDC正常关机，然后又重新启动，这时PDC则变为BDC了。

经验总结

　　后来，我又经过反复测试，终于掌握了规律：启动机器，必须先启动PDC，然后再启动BDC。关机时如果只关闭PDC，而没有把BDC升为PDC，则会出现上面相关错误信息提示。

　　虽然NT主域、备份域的概念并不复杂，有些细节我还是想在此提醒你：通常，当备份域控制器升级为主域控制器时，不需要采取任何特殊的操作，系统会自动将先前的主域控制器降为备份域控制器；如果原来的主域控制器失效，在将一台备份域服务器升级为主域控制器之后，如果原来的主域控制器又恢复了服务，必须将其降级，在它降级前不会运行NETLOGON服务，亦不会参加用户登录确认，同时，它在“服务器管理器”窗口中的图标会变成灰色。

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。

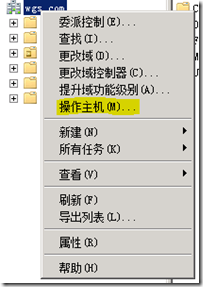
今天跟大家介绍的是域环境中五大操作主机之一 "PDC Emulator" 全称 "Primary domain controller (PDC) emulator operations master" 中文:PDC仿真主机。

我习惯把它称为“PDC Emulator” 。

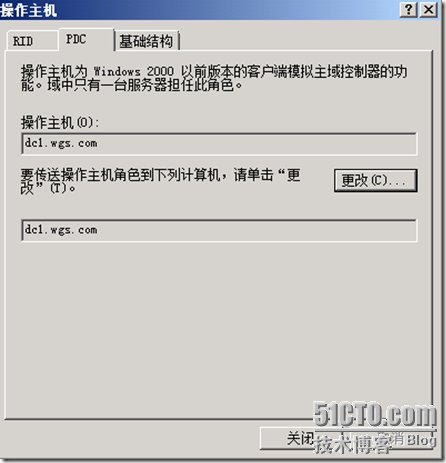
现在咱们就来一步步认识  “PDC Emulator” 。

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” 。

[](http://img1.51cto.com/attachment/200910/13/198455_12554296872Hfz.png)   
鼠标右击当前域，选择“操作主机”，

[](http://img1.51cto.com/attachment/200910/13/198455_1255429690pMLp.png)

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.

[](http://img1.51cto.com/attachment/200910/13/198455_1255429691pPjt.png)

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有NT的BDC的话，请务必要准备一台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。

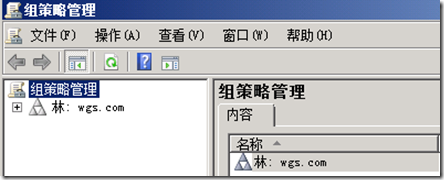
第三个功能：给NT以前的客户端改密码：因为NT以前的客户端改密码必须要连到以前NT域的PDC上才可以改，PDC是只读的。

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。

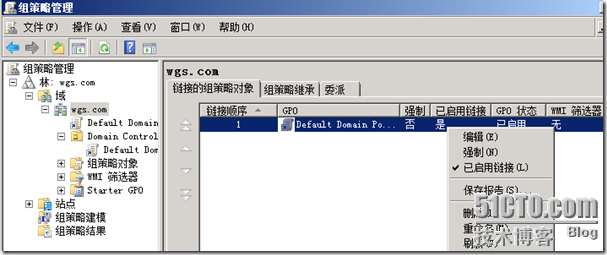
第五个功能：防止重复套用组策略：当我们使用组策略时，我们的组策略编辑器会连到 PDC Emulator 去做修改，来防止组策略套用时出错。

这个功能我们可以看图来说明下：

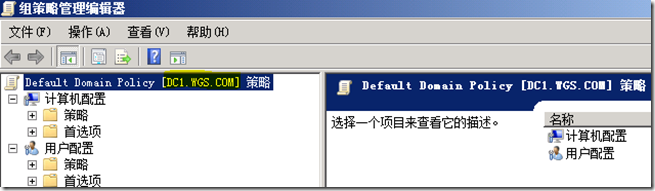
我们先打开 “组策略管理”

[](http://img1.51cto.com/attachment/200910/13/198455_1255429693BWCg.png)

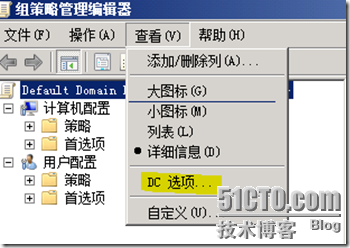
假设我要编辑某一个GPO，比如默认域策略

[](http://img1.51cto.com/attachment/200910/13/198455_1255429693OQPi.png)

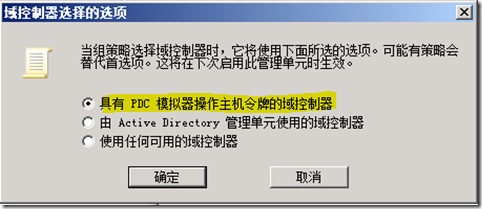
大家可以看到 组策略管理编辑器 会默认连接到一台主机名字叫 “dc1.wgs.com” 而这台DC正是我当前域的 PDC Emulator ，这样的设定就会防止，在复制组策略对象（GPO）的时候出现重复。

[](http://img1.51cto.com/attachment/200910/13/198455_1255429697WeCX.png)

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，

[](http://img1.51cto.com/attachment/200910/13/198455_1255429698dJhR.png)

可以看到如下提示

[](http://img1.51cto.com/attachment/200910/13/198455_12554297004Pb2.png)

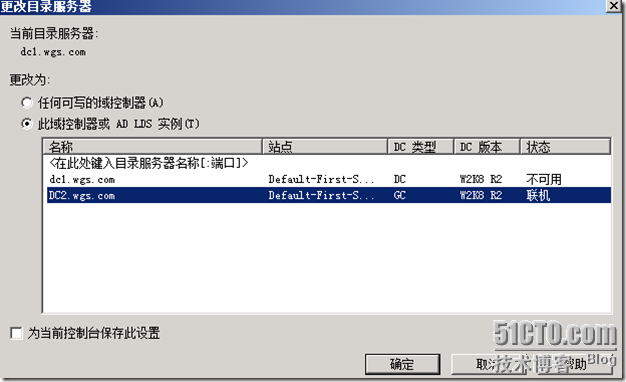
从上图中我们可以看出，默认情况下在套用GPO的时候就会去找 PDC Emulator 去做复制，这样就可以避免GPO设置在复制的时候重复。

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。

[](http://img1.51cto.com/attachment/200910/13/198455_1255429701bTCT.png)

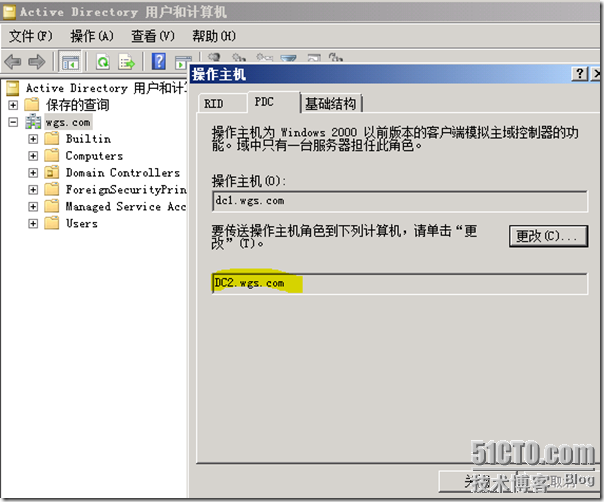
出现如下图所示窗口，大家可以看到我当前域有两台DC ：DC1和DC2 ，我选择更改目录服务器为 DC2.wgs.com

[](http://img1.51cto.com/attachment/200910/13/198455_1255429703LmxH.png)

下图为更改后的状态，

[](http://img1.51cto.com/attachment/200910/13/198455_1255429705R0bk.png)

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。

[](http://img1.51cto.com/attachment/200910/13/198455_12554297065oQr.png)

再选择更改，[](http://img1.51cto.com/attachment/200910/13/198455_1255429710u4Ji.png)  选择传送操作主机，

结果如下：

[](http://img1.51cto.com/attachment/200910/13/198455_1255429710gNqg.png)

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

窗体底端