AD 概念&FSMO 概念&GC 概念

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。

操作主机：（OM）--FSMO

森林级别 ：

1、架构主机（Schema Master）

功能：控制活动目录内所有对象/属性的定义

提示：Regsvr32 schmmgmt.dll

Schema Admins 组

故障影响：更新 Schema 受影响

短期内一般看不到影响

典型问题如：无法安装 Exchange

故障处理：需确定原 OM 为永久性脱机才可抓取

确保目标 DC 为具有最新更新的 DC

2、域命名主机（Domain Naming Master）

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

提示：建议与 GC 配置在一起

Enterprise Admins 组

故障影响：更改域结构/添加删除域受影响

短期内一般看不到影响

典型问题如：添加/删除域

故障处理：需确定原 OM 为永久性脱机才可抓取

确保目标 DC 为具有最新更新的 DC

域级别

1、RID主机（RID Master）

功能：管理域中对象相对标识符（RID）池

提示：对象安全标识符（SID）= 域安全标识符 + 相对标识符（RID）

形如：S-1-5-21-1343024091-879983540-3…

故障影响：无法获得新的 RID 池分配

典型问题如：无法新建（大量）用户帐号

故障处理：需确定原 OM 为永久性脱机才可抓取

确保目标 DC 为具有最新更新的 DC

2、PDC模拟主机（PDC Emulator）

功能：模拟 Windows NT PDC

默认的域主浏览器

默认的域内权威的时间服务源

统一管理域帐号密码更新、验证及锁定

提示：PDC 模拟主机不仅仅是模拟 NT PDC

一般负荷较大

故障影响：底端客户不能访问 AD

不能更改域帐号密码

浏览服务问题

时间同步问题

故障处理：需要比较及时地恢复

可以临时抓取到其他 DC

在原 OM 恢复后可以迁移回去

3、基础结构主机（Infrastructure Master）

功能：负责对跨域对象引用进行更新

提示：单域情况下基础结构主机不需要工作

不能同时和 GC 配置在一起（单域控除外）

故障影响：外域帐号不能识别，标记为 SID

故障处理：需要比较及时地恢复

可以临时抓取到其他 DC

在原 OM 恢复后可以迁移回去

查看操作主机角色

命令行工具：Ntdsutil Netdom Dcdiag

操作主机的放置

默认情况：架构主机在根域的第一台 DC 上

域命名主机在根域的第一台 DC 上

其他三个主机角色在各自域的第一台 DC 上

考虑问题：和 GC 的冲突

性能考虑

手工优化：基础结构主机与 GC 不放在一起

域命名主机与 GC 放在一起

架构主机与域命名主机可放在一起

PDC 模拟主机建议单独放置

（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。比如部属 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。

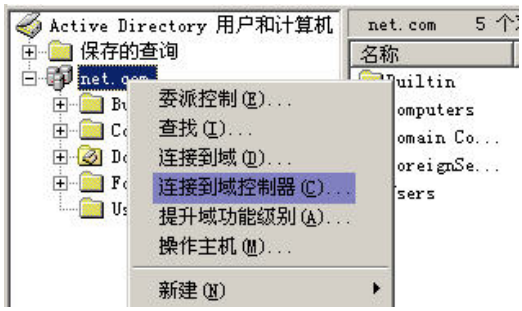
具体的操作：

1. 转移：前提是相应的操作主机的角色在线。

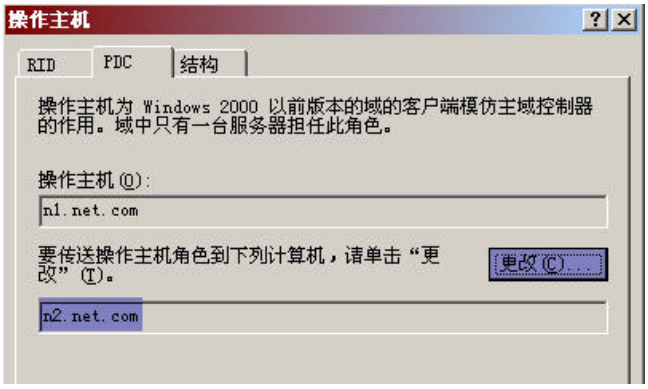
比如转移 PDC 主机

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：

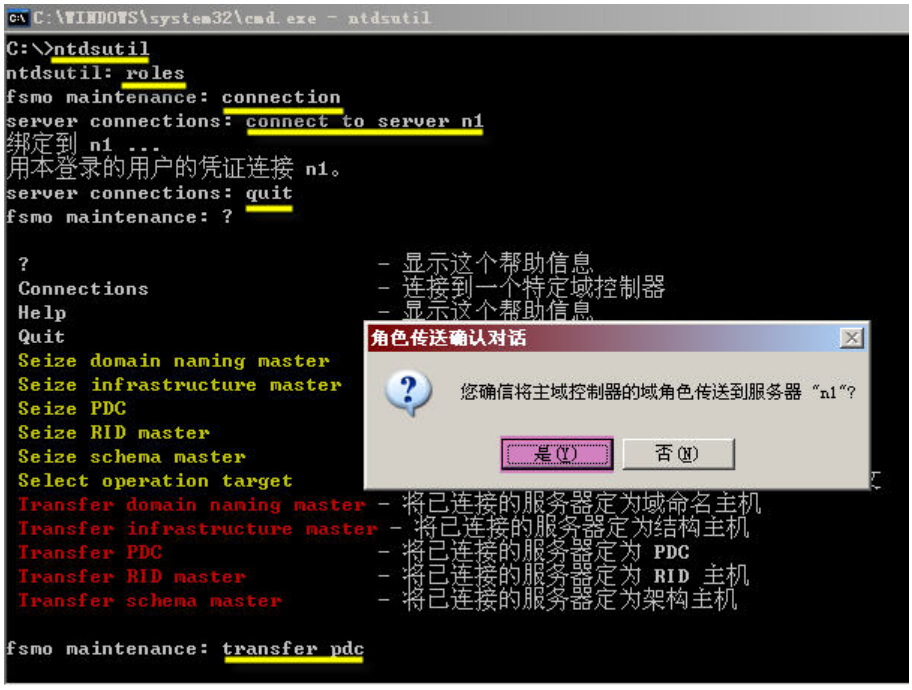


再次右击该域--选择操作主机--找到 PDC，如下图所示：



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。

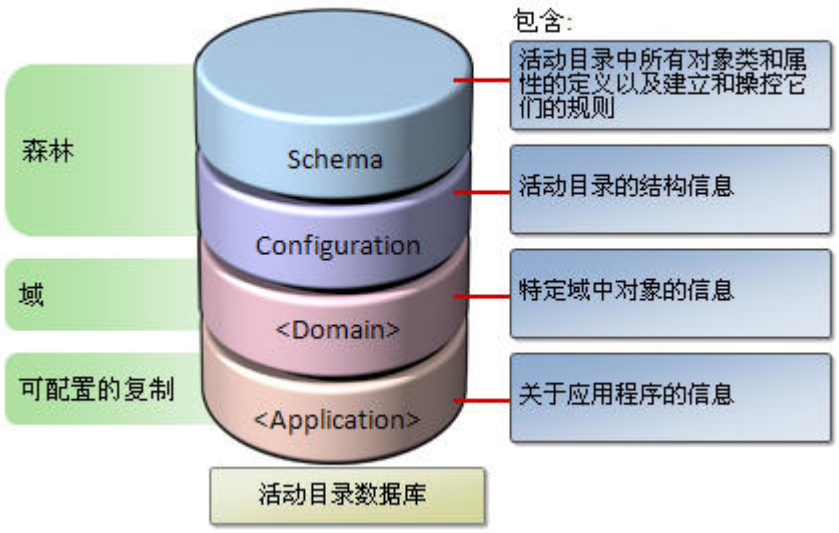
2. 占用：联系不上相应的操作主机时。(尽可能用命令方式，具体要求操作如上图所示，无非选择 seize 行即可。此处略了吧~~~)

（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。

AD 数据库的目录分区介绍

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。

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朴就满足这个条件。

（八）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。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。

（九）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）：此时该对像会被移动一个叫 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。

墓碑生存时间（tombstoneLifetime）

墓碑生存时间（tombstoneLifetime）是指：从在 AD 中删除某对象开始，到该对象真正被删除的时间间隔，默认值为 60 天，这样做是为了保证：这种删除操作被复制到域中其它的 DC。恢复 DC 的“系统状态数据”备份是有时间限制的，不能从比墓碑默认的 60 天生存时间更旧的系统状态数据的备份中，恢复活动目录。

可手动将墓碑生存时间的默认值，由 60 天修改为更大的值，具体操作步骤如下：

1、安装 ADSIedit.msc 工具：运行 03 光盘\SUPPORT\TOOLS\ suptools.msi，所有支持工具将安装在 C:\Program Files\Support Tools 夹下，还有许多别的工具。

2、开始/运行：ADSIedit.msc

3、找到 Configuration\Services\Windows NT\Directory Service,在其上右键/属性。

4、找到 tombstoneLifetime 属性，将其值由（注意：并不显示默认的 60 天）改为 365 天或更大

深入理解全局编录服务器 GC

引用位置: http://alligator.blog.51cto.com/36993/101261

概述：在 Win2003AD 域环境中，除了 FSMO 操作主机角色外，全局编录服务器(GC)也是有着特殊含义的域控制器。通过 GC，可以提高在活动目录中搜索对象的速度，可以加快用户登录验证等。

简单的说，GC 是森林中所有对象的只读调整缓冲存储器(Read Only Cache),目录只用于搜索。GC 服务器存储本域中所有对象的所有属性，同时会存储林中其它域中所有对象的部分属性。一般来说，属性是否存储在 GC 中，取决于该属性在搜索中使用的频率,由系统自动进行决定。但 AD 架构管理员也可以定义对象的哪些属性保存的 GC 中，同时决定该属性是否可以进行索引。

本文拟就与 GC 相关的内容一一阐述，希望能起抛砖引玉作用，与有兴趣的朋友一起更好的了解和熟悉全局编录服务器。

GC 出现的原因

GC 的作用

查看当前环境中 GC 服务器

提升 DC 为全局编录服务器

验证全局编录服务器的提升

验证全局编录服务器是否工作正常

删除全局编录服务器

使用 AdsiEdit 工具查看全局编录服务器中的数据

一：GC 出现的原因

在 Win2003 活动目录中有两种目录服务，分别是 DNS 以及 LDAP，两个目录服务互为补充。DNS 的目的比较简单，用于简单快速的定位域控制器，但定位到具体的域控制器后，对活动目录信息的更细致访问，如活动目录中关于用户，计算机，打印机等对象信息搜索，DNS 就无能为力。此时就需要通过 LDAP 服务来访问。

如果用户知道某个对象处于哪个域，也知道对象的标识名，那么用 LDAP 搜索对象就非常容易。但如果用户只知道某个对象的某个属性，根本不知道对象所处的域，也不知道该对象的标识名，那么使用 LDAP 来搜索对象是一件非常困难的事，AD 不得不对当前环境中每一个域的每个对象都搜索一遍。为了解决这个问题，活动目录提供了全局编录服务器(GC，到 Global Catalog)。GC 中包含了当前林中每个域中所有对象的副本，如果在一次 LDAP 搜索中，涉及到搜索中多个域的名称上下文时，AD 会选择搜索 GC 服务器，从而实现加快搜索速度，减少网络通信量的目的。

二：GC 的作用

1：存储对象信息副本，提高搜索性能

全局编录服务器中除了保存本域中所有对象的所有属性外，还保存林中其它域所有对象的部分属性，这样就允许用户通过全局编录信息搜索林中所有域中对象的信息，而不用考虑数据存储的位置。通过 GC 执行林中搜索时可获得最大的速度并产生最小的网络通信量。

2：存储通用组成员身份信息，帮助用户构建访问令牌

全局组成员身份存储在每个域中，但通用组成员身份只存储在全局编录服务器中。

我们知道，用户在登陆过程中需要由登录的 DC 构建一个安全的访问令牌，而要构建成功一个安全的访问令牌由三方面信息组成：用户 SID，组 SID，权力。其中用户 SID 和用户权力可以由登录 DC 获得，但对于获取组 SID 信息时，需要确定该用户属不属于通用组，而通用组信息只保存在 GC 中。所以当 GC 故障，负责构建安全访问令牌的 DC 就无法联系 GC 来确认该用户组的 SID，也就无法构建一个安全的访问令牌。

注：在 Win2003 中，可以通过通用组缓存功能解决 GC 不在线无法登录情况，具体操作本文略过。

3：提供用户 UPN 名称登录身份验证。

当执行身份验证的域控制器没有用户 UPN 帐号信息时，将由 GC 解析用户主机名称(UPN)进行身份验证，以完成登录过程

4：验证林中其他域对象的参考

当域控制器的某个对象的属性包含有另一个域某个对象的参考时，将由全局编录服务器来完成验证。

三：查看当前环境中 GC 服务器

1：通过“Active Directory 站点和服务”查看

步骤：

点击“开始-设置-控制面板-管理工具-Active Directory 站点和服务”：

选中具体的“NTDS Setting”。

选中"NTDS Setting",右键选择“属性”

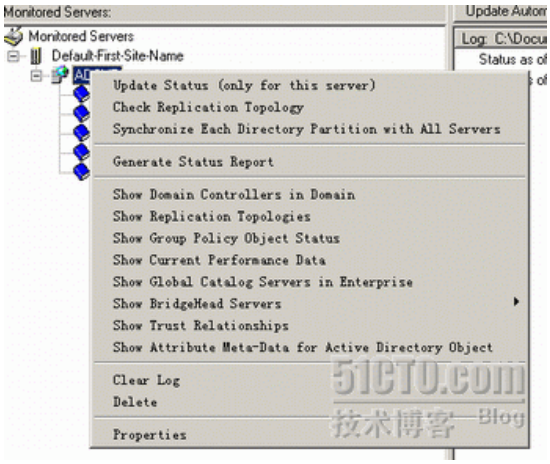
在弹出的“NTDS Setting 属性”对话框中，有“全局编录”复选框,如果选中，表示是一台全局编录服务器， 如果没有选中，则表示当前的服务器不是全局编录服务器。

2：利用复制监视器 Replmon 查看

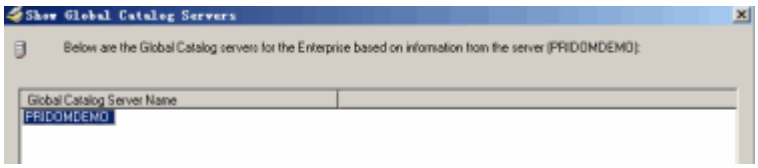
复制监视器 Replication Monitor(ReplMon)是针对 Windows Server 的故障查找工具,不但是定位活动目录复制故障强有利的工具，同时也可以使用该工具查看和检查操作主机角色状态。

详细 Replmon 工具使用方法本文不做过多说明，这里只列出如何使用 Replmon 工具 GC 角色。

步骤：选中当前 DC，右键单击，选择“Show Global Catalog Servers in Enterprise”



在弹出窗口中，清楚列出当前林中所有的全局编录服务器

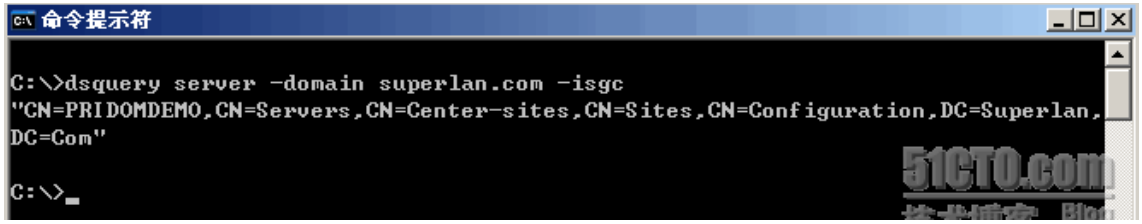


3：通过命令行方式查看全局编录服务器

在 Supprot Tools 和 Resource Tools 工具中，有多个命令行工具可以查看全局编录服务器，这里只列出两个最常见的命令行工具

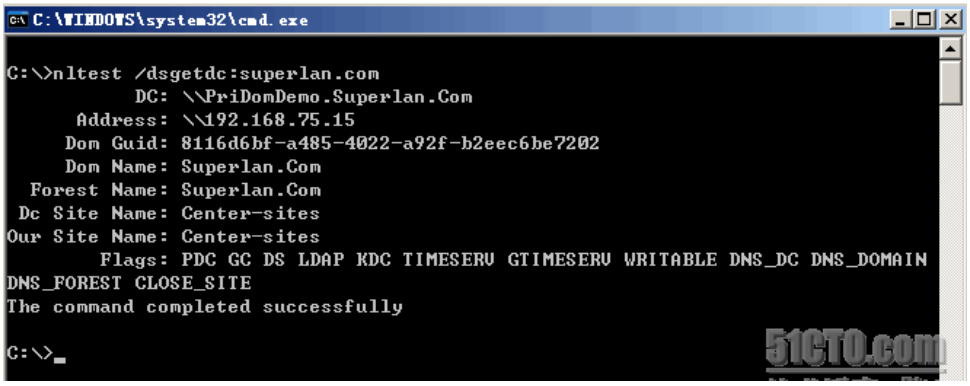
使用 dsquery 命令查看当前域中的 GC

```
dsquery server -domain superlan.com -isgc
```



使用 nltest 命令查看当前域中的 GC

```
nltest /dsgetdc:superlan.com
```

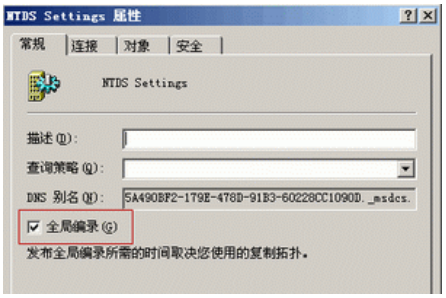


四：提升 DC 为全局编录服务器

将一台域控制器提升为全局编录服务器操作很简单，方法见通过“Active Directory 站点和服务”管理单元查看全局编录服务器，

将“全局编录”复选框选中即可。

注意：设置完成后，并不代表当前的全局编录服务器已经提升完成，因为全局编录服务器中包含有多个域的所有对象，需要时间来进行全局编录数据库同步。



五：验证全局编录服务器的提升

通过提升 DC 为全局编录服务器操作，需要时间同步全局编录服务器，同步完成后，全局编录服务器才开始真正运行。

下面介绍如何查看全局编录服务器是否已经开始工作。

1：使用 LDP 工具查看当前 DC 的 IsGlobalCatalogReady 属性

LDP(LDAP 浏览器工具)是一个轻量目录访问协议 (LDAP) 客户端实用工具,可以用来查询和浏览 LDAP 目录服务，详细用法本文不做具体介绍，

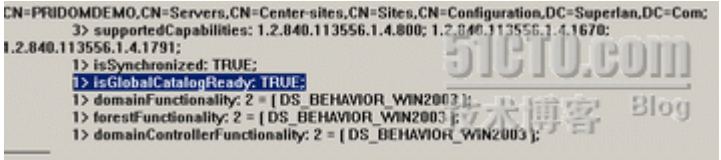
可以搜索相关的说明文档或后期的 Blog 文章介绍。这里只给出简单的使用说明

步骤：

与 LDAP 目录绑定

“运行”，输入“LDP”，打开 LDP 窗口后，选择“Connection|Bind”,打开 Bind 对话框，输入身份凭证。

单击”OK“按钮,LDP 连接到”Superlan.Com"域控制器，显示检测结果，从下图可以看出“IsGlobalCatalogReady"属性为 True



2：查看 DNS 管理工具查看 GC 记录是否已更新到 DNS 中。

从下图可以看出当前哪个域控制器是 GC，且使用的端口是多少，默认的 GC 使用端口是 3268。

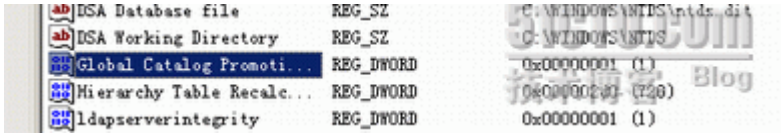
六：验证全局编录服务器是否工作正常

全局编录服务器正确提升后，可以通过查看注册表信息和端口状态来查看

全局编录服务器是否工作正常。

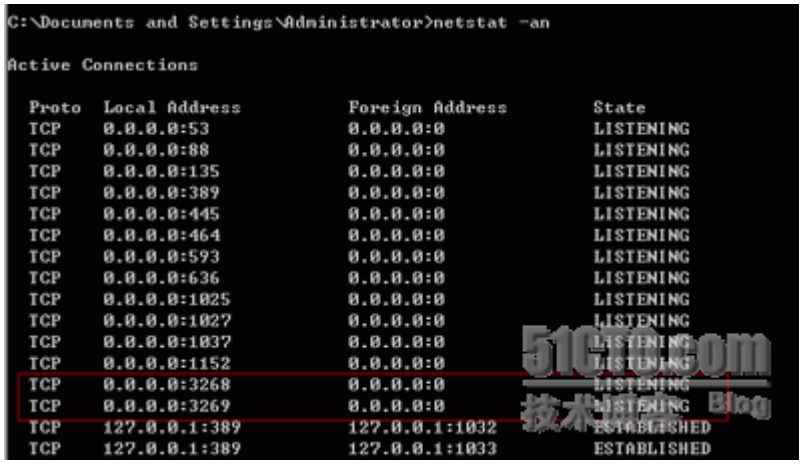
1：查看注册表信息(HKLM\System\CurrentControlSet\Services\NTDS\Parameters)

健值：Global Catalog Promotion Complete，值为 1，表示 GC 工作正常



2：全局服务编录器默认使用 3268/3269 端口，通过查看端口是否处于监听状态可以判断 GC 是否工作正常

使用 netstat -an 命令查看当前正在运行的端口,可以看到 3268/3269 端口已经处于正常监听状态



七：删除全局编录服务器

删除全局编录服务器方法请参见”四：提升全局编录服务器“，将”全局编录“复选框取消即可，此处略过。

八：使用 AdsiEdit 工具查看全局编录服务器中的数据

全局编录服务器并不是一个独立的实体，域控制器也没有单独为 GC 准备一个独立的 DIT 文件，GC 服务器与当前的域公用同一个 NTDS.DIT 文件，两者的区别只是使用的端口号不同，前者使用 3268 端口，后者使用 389 端口。理解了这一点，也就理解了如何来查看 GC 数据。

AdsiEdit 工具是一个超级强大的 AD 查看与编辑工具，我们可以使用这个工具做一些其它工具无法实现的功能。

比如本文准备阐述的查看全局编录服务器中的数据等。

为了更好的说明如何使用 AdsiEdit 工具查看 GC 数据，先介绍一下当前的演示环境：

两个域，父域为 Superlan.Com,子域为 Sub.Superlan.Com,其中 Superlan.Com 域中有一台 DC(PriDomDemo.Superlan.Com),同时担任 GC 角色，子域中有一台 DC(SubDomDemo.Sub.Superlan.Com),非 GC。

域结构如下：

因 PriDomDemo.Superlan.Com 为父域 DC，同时又为 GC，所以在 PriDomDemo AD 数据库中，应该包含有子域 Sub.Superlan.Com 数据。

那么如何在 PriDomDemo 中查看子域数据，同时验证 GC 相关的概念，比如

GC 是森林中所有对象的只读调整缓冲存储器

包含有子域所有对象的部分属性。

自定义对象的哪些属性保存的 GC 中，同时决定该属性是否可以进行索引等等。

本文利用 AdsiEdit 工具，分别连接 GC 以及 Sub.Superlan.Com 域，通过比较标准的 Sub 域数据与保存在 GC 中 Sub 域数据，就上述问题做深入阐述!

具体操作如下

一：使用 AdsiEdit 查看 AD 数据

1：连接到 GC 服务器

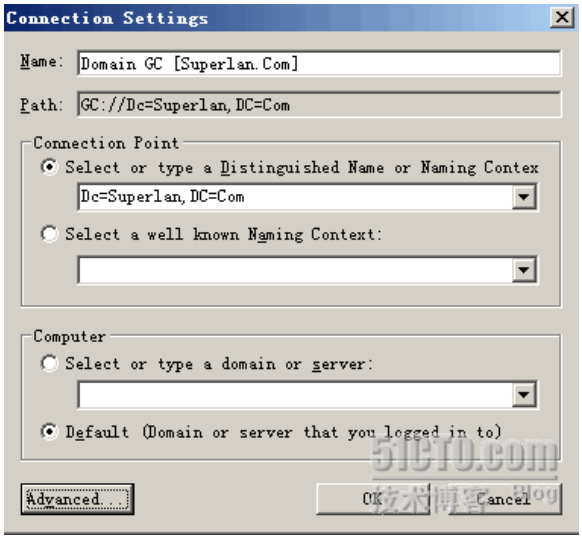
在 AdsiEdit 中,连接到 GC 服务器很简单，唯一需要注意的是，需要在“高级”中指定使用 Global Catalog 协议

具体如下：

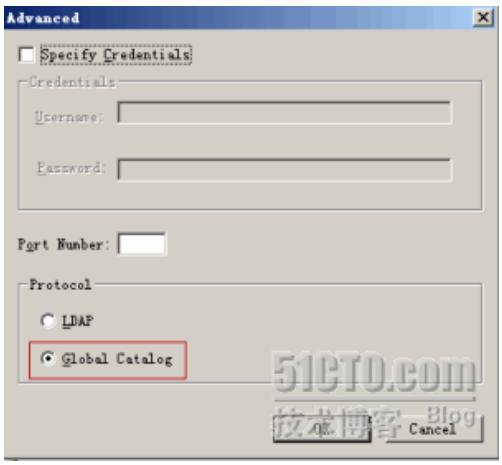
在“运行”窗口输入“AdsiEdit.msc”,打开 AdsiEdit 编辑器。

选中"AdsiEdit",右键选择”Connect to“

在"Connection Setting"弹出框，输入相应的名称上下文

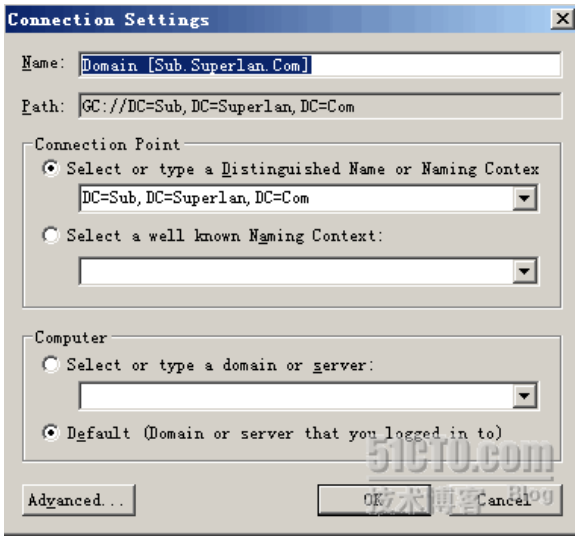


输入名称上下文后，打开"Advanced "按钮，选择”Global Catalog"协议

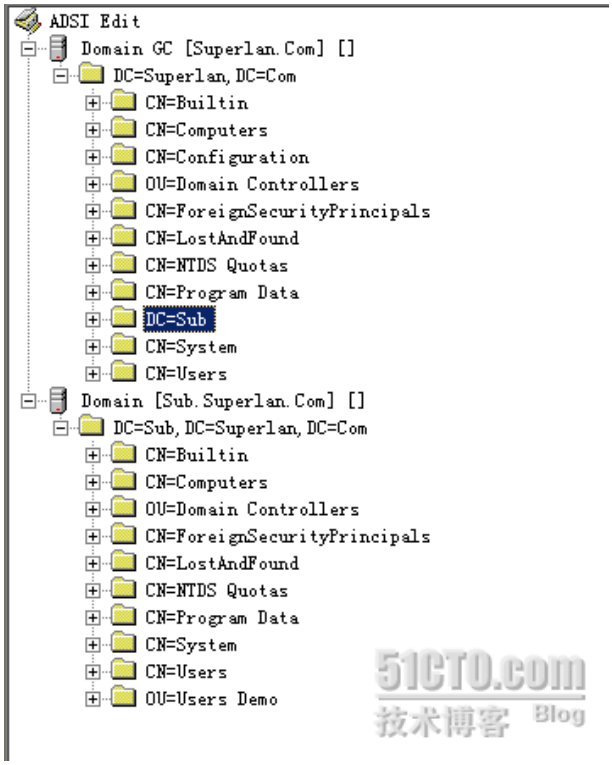


选择两次 OK 按钮，确定输入无误后，就可以正确连接到 GC 服务器。

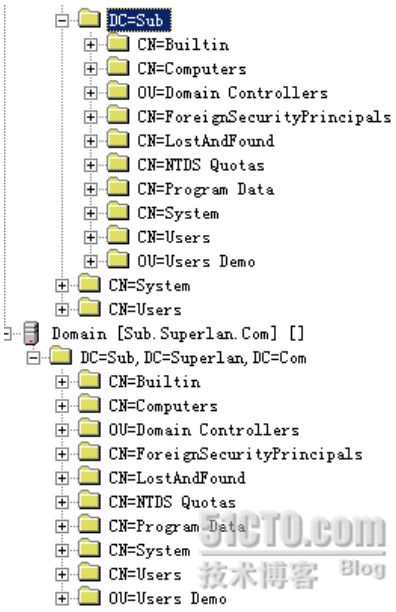
2：新建一个连接到 Sub.Superlan.Com 域：操作与连接到 GC 步骤类似，保留“Advanced”中默认的 LDAP 协议



建立好上述两个连接后，AdsiEdit 工具窗口中存在两个连接，分别是 GC 服务器数据和 Sub 子域数据。

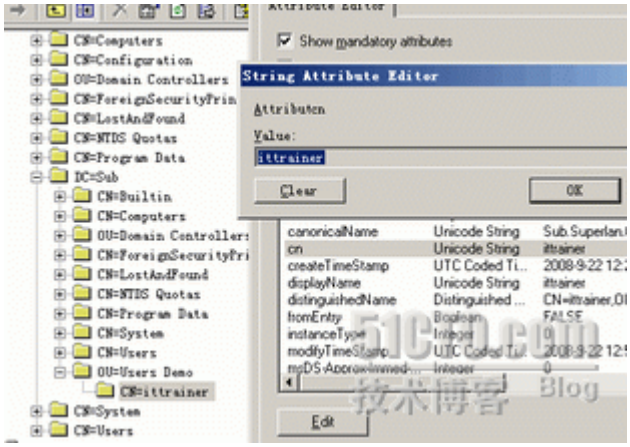


从上图我们可以看出，在 GC 服务器数据中，有一个“DC=Sub”容器。展开该容器后，我们可以看到该容器中所包含的信息与 Sub 子域数据完全相同



从上图我们也可以看出，GC 中确实保存着林中其它域的所有对象

二：验证 GC 是林中所有对象的只读存储器。任意展开 GC 中容器中任意对象的任意属性，点击“Edit”按钮，都可以看到， 所有的属性都是处于 ReadOnly 状态，无法进行修改。



而在非 GC 连接中，可以直接进行修改编辑，从中我们可以看出不论是对于当前域，还是非本地域，GC 中保存的都只是对象的只读副本。

三：验证 GC 中只包含林中其它域所有对象的部分属性

为验证这个结论，在 Sub 子域新建一个 OU：User Demo,其中建立有一个用户：itTrainer.分别在 GC 服务器和 Sub 子域中查看该对象属性，我们可以看出，GC 中该对象有值的属性比 Sub 子域中该对象有值的属性少得多。GC 中只保留有系统属性以及明确指出保存在 GC 中的属性。 而 Sub 子域中会保存该对象的所有属性值。

四：如何自定义哪些属性保存在 GC 中

要自定义哪些属性保存在 GC 中，需要使用 AD 架构管理单元。

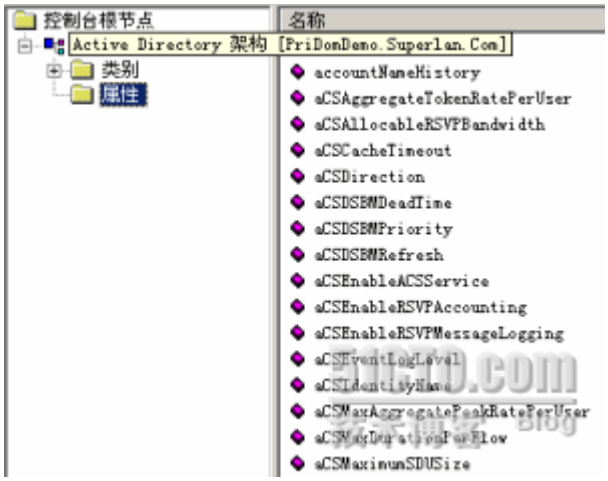
注意，默认情况下，只有父域的 Administrator 属于架构管理组，而子域管理员不属于该管理组。

1：注册 AD 架构管理单元

步骤：注册：regsvr32 schmmgmt

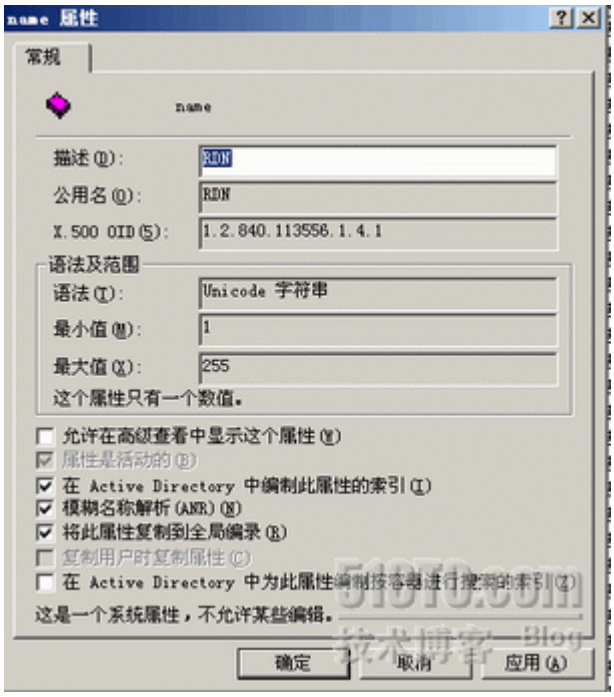
在 MMC 中添加 AD 架构管理单元

打开 MMC 控制台，选中“Active Directory 架构”，点击“属性”,在右侧内容栏列出当前域架构中存在所有属性。



2：自定义属性保存在 GC 中

选择任一个属性，右键选择”属性“，在弹出的”属性编辑器“中，可以自定义该属性是否保存在 GC 中， 同时也可以决定该属性在 GC 中是否编制索引，以提高搜索性能。



因为篇幅关系，本文不再演示如何自定义某个属性是否存在到 GC。

有兴趣的朋友可以试着将某一个属性自定义为保存在 GC 中，同时建立某个对象，在该对象中对这个属性赋值，在 GC 中检查是否存在该属性值。甚至于可以通过架构管理单元取消某个默认保存到 GC 中的某个属性，然后通过 GC 检查该属性是否仍然保存在 GC 中。

相信通过相应的操作，一定会对 GC 相关的概念有更深入的理解!

域用户登录过程和 GC 的关系

1.模拟环境

根域为 contoso.msft，dc 为 dc1.contoso.msft，dc2.contoso.msft 同时也是 GC，所处站点 site 1；子域为 child.contoso.msft，dc 为 child-dc.child.contoso.msft，所处站点 site 2 不是 GC；在域 child.contoso.msft 上有用户 john 用于验证本实验!

2.GC 存储着森林中所有域的域分区的所有对象的部分属性，同时还存储着林中所有通用组的成员列表，在域用户登录的过程中和查询过程中，GC 发挥着重要的作用；或者可以说没有 GC 域用户在一般情况下就不能登录，这里为什么说是在一般情况下，因为有特例（后面再说)!

先说说域用户的登录过程和 GC 的关系：首先域用户要想登录成功，必须从所在域的 dc 那里成功构建“安全访问令牌”，没有这个安全访问令牌域用户是不能登录的；那么这个域用户所在域的 dc 是如何来为用户成功构建安全访问令牌呢？要成功构建安全访问令牌必须满足三个条件：

a．从 dc 那里取得这个域用户的 SID

b．从 DC 那里取得这个域用户所具有的权限

c．取得这个域用户的所属组：包括本地域组、全局组、通用组；本地域组和全局组可以向 dc 查询，但是通用组只有由 DC 向

GC 去查询，因为只有 GC 存储了通用组的成员列表；这里不管这个用户是否属于某个通用组，都要去查询 GC 来确定这个用户是否属于某个通用组。

综合以上三个因素，所以当 GC 不在线的情况下，即使当前域的 dc 是 ok 的，当前域的 dns 是 ok 的，同样用户不能登录域！

结合实例就是：当 contoso.msft 中的 dc2.contoso.msft（同时也是 GC）宕机的情况下，其子域中的用户 john 是不能登录其所在的域 child.contoso.msft 的，即使 child-dc.child.comtoso.msft 是正常的！

例外：

a 域管理员组的成员不受此限制

b 登陆过的客户端可以使用本机的缓存来登录

c 2003 的域模式如果为默认的混合模式，在这种情况下通用组是不可用的，所以这个时候是不用去查询 GC 来确定通用组的情况的！

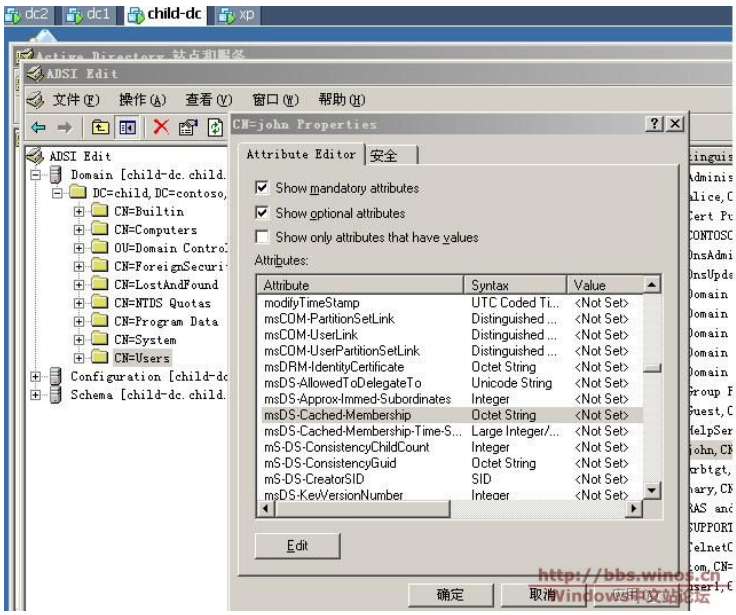
3.通用组成员缓存

那如何在 GC 不在线的情况下，也能让域用户顺利登录呢？

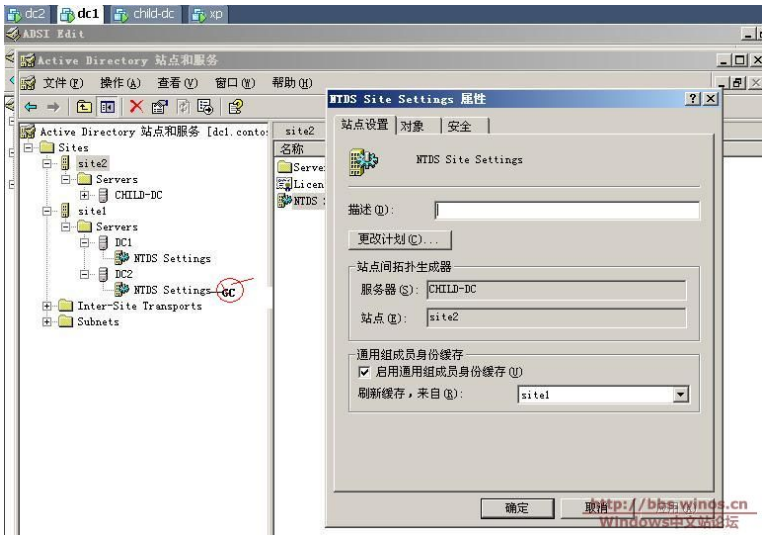
解决问题的方法就是使用通用组成员缓存（当然了，在每个站点都设置 GC 就不提了，这样做就要考虑硬件成本，毕竟 GC 会复制大量信息；单域的情况下除外，单域中建议所有的 dc 都提升为 GC，这个时候是不会增加复制流量的）；要想在 GC 不在线的情况下，域用户也能登录；那就必须使用缓存，使用客户机的缓存(前提是此用户必须在这个客户机上登录)或使用 dc 缓存（这样即使此用户没有在这台客户机上登录，也能登录；当然了要有缓存信息的话，必须要在域中的某个地方登录）；这个缓存在 dc 上信息的可以在 dc 上看的到的。

4．验证

首先在 child-dc.child.contoso.msft 上新建一个用户 john，然后在 dc 上看一下；这个用户的 msds-cached-membership 属性，是空的，是 not set！这个属性就是缓存用户的通用组和全局组的信息的！



a．首先来看一下，在哪里设置通用组成员缓存

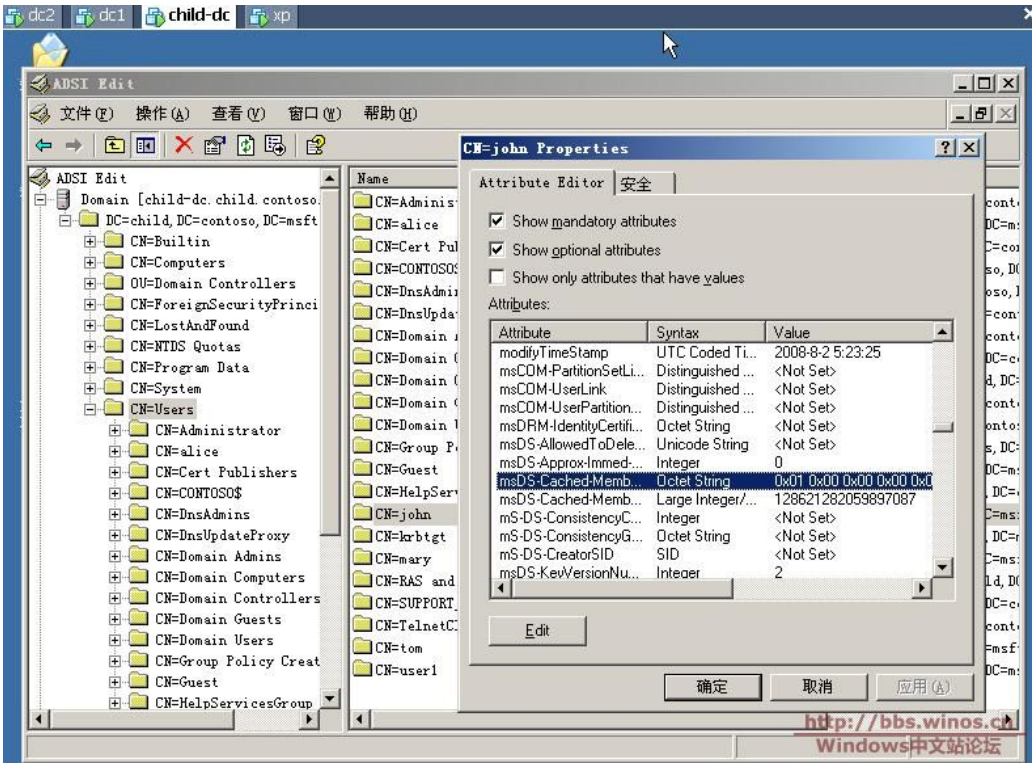


b．禁用 dc2.contoso.msft 的网卡（相当于 GC 不可用），在域 child.contoso.msft 内用用户 john 在 xp 客户端登录，这时会发现登

录不了（即使这个时候 dc 和 dns 都是 ok 的）

c．启用 GC，用 john 在 child-dc.child.contoso.msft 上登录（没有多余的客户端了，前提是修改默认域控制器策略允许 john 在本地登录），以让 child-dc.child.contoso.msft 从 GC 上缓存该用户的通用组和全局组的信息！

这个时候 john 用户在 child-dc.child.contoso.msft 上是可以登录的；注销；用 administrator 登录看看这个用户的缓存的信息：



d．禁用GC，在xp客户端上用john登录！这个时候你会发现即使GC不在线，即使这个用户以前没有在xp这台客户端上登录过（一点要在本域的其他地方登陆过），它照样能登录成功。