# AD FSMO 五种角色主机的作用

[AD FSMO 五种角色主机的作用 1](#_Toc12802)

[森林级别 1](#_Toc3838)

[１、架构主机（Schema Master） 1](#_Toc30178)

[２、 域命名主机（Domain Naming Master） 2](#_Toc26205)

[域级别 2](#_Toc2403)

[３、 RID主机（RID Master） 3](#_Toc22300)

[４、 PDC模拟主机（PDC Emulator） 3](#_Toc19714)

[５、 基础结构主机（Infrastructure Master） 4](#_Toc972)

[性能优化考虑 5](#_Toc13548)

Active Directory 定义了五种操作主机角色（又称ＦＳＭＯ）：

1.架构主机 schema master

2.域命名主机domain naming master

3.相对标识号 (RID) 主机 RID master

4.主域控制器模拟器 (PDCE)

5.基础结构主机 infrastructure master

## 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

### 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

### 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

### 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

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恢复后可以抓取回去

### 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恢复后可以抓取回去

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

## 性能优化考虑

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

操作主机的转移

１、转移（Transfer）

把OM角色平滑地传递给另一台DC

操作可逆

２、抓取（Seize）

把OM角色强制地赋予另一台DC

操作不可逆

抓取命令会自动先尝试转移

一．目的：

在安装DC的过程中，系统会默认将域中第一台DC做为五种角色的操作主机，但是有时候我们需要手工指定更可靠更安全的DC来做操作主机，因为操作主机一旦损坏，那么整个域就会产生非常严重的后果，比如：无法新建（大量）用户帐户，用户无法访问AD和更改密码等。

二．目标：

将域中五种操作主机角色进行迁移

三．实现：

迁移之前先查看当前的FSMO操作主机：命令行执行netdom query fsmo

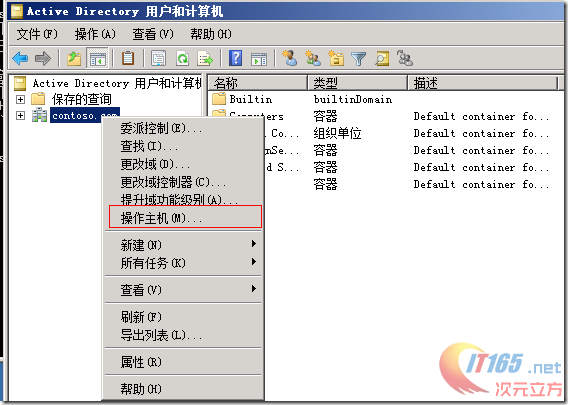
[](http://www.it165.net/uploadfile/2013/0614/20130614101114251.png)

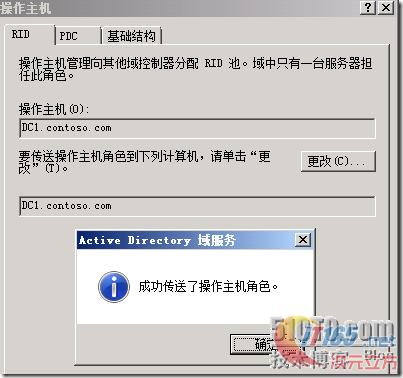
以上图可知，现在的操作主机角色全在DC2上，接下来我们将五种操作主机角色迁移到DC1

1. RID角色转移：

RIP主机主要是管理域中对象相对标识符（RID）池，对象安全标识符SID＝域安全标识符+相对标识符（RID），一旦损坏，域中对象将无法获得新的RID池分配，现象为：无法新建（大量）用户。

转移方法：在“管理工具”－“AD用户和组”管理单元，右键－操作主机中更改。

[](http://www.it165.net/uploadfile/2013/0614/20130614101114481.png)

[](http://www.it165.net/uploadfile/2013/0614/20130614101116408.png)

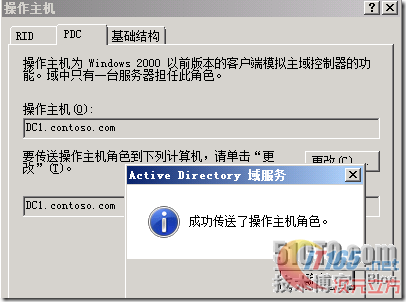
2. PDC角色转移

模拟Windows NT PDC，默认的域主浏览器，默认的域内权威时间服务源，统一管理域帐号密码更新、验证及锁定。一旦损坏，底端客户将不能访问AD，不能更改用户密码，时间也不能同步。

转移：

转移方法：在“管理工具”－“AD用户和组”管理单元，右键－操作主机中更改。

[](http://www.it165.net/uploadfile/2013/0614/20130614101116657.png)

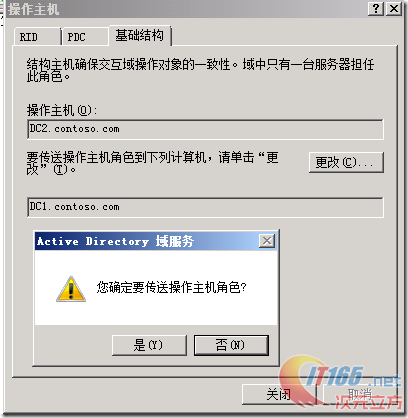
[](http://www.it165.net/uploadfile/2013/0614/20130614101117717.png)

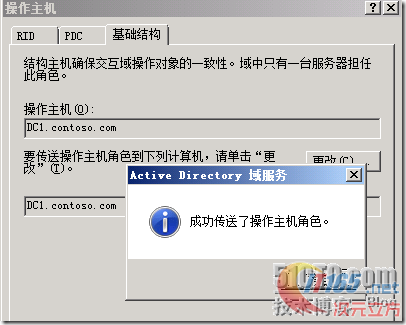
3. 结构主机转移

结构主机主要是负责对跨域对象的引用更新，单域情况下一般不工作，一般产生故障后影响不太明显，故障现象为不能识别外域帐号。

转移：

转移方法：在“管理工具”－“AD用户和组”管理单元，右键－操作主机中更改。

[](http://www.it165.net/uploadfile/2013/0614/20130614101121491.png)

[](http://www.it165.net/uploadfile/2013/0614/20130614101122239.png)

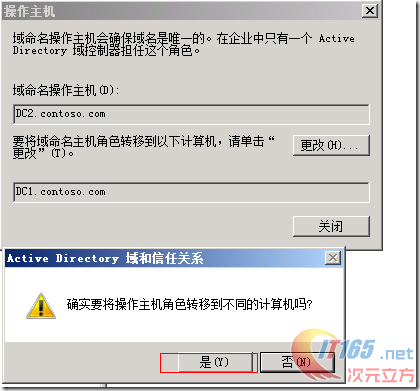
4. 域命名主机转移

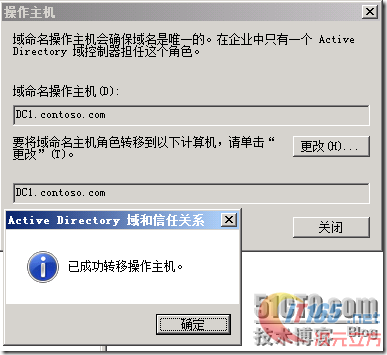
主要功能是负责控制域林内域的添加和删除，损坏后不能添加、删除域。

转移：

转移方法：在“管理工具”－“AD域和信任关系”管理单元，右键－操作主机中更改。

[](http://www.it165.net/uploadfile/2013/0614/20130614101123956.png)

[](http://www.it165.net/uploadfile/2013/0614/20130614101123647.png)

[](http://www.it165.net/uploadfile/2013/0614/20130614101124981.png)

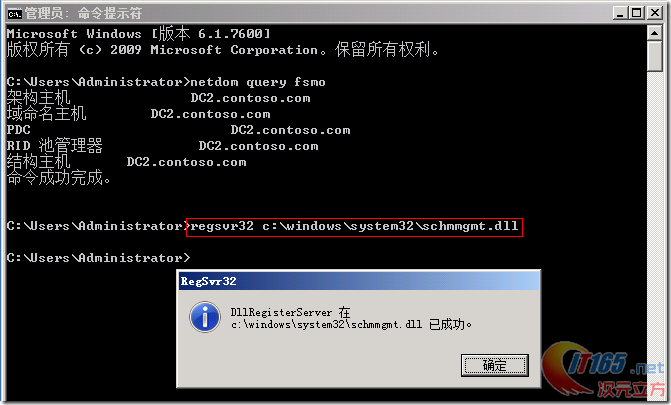
5. 架构主机转移

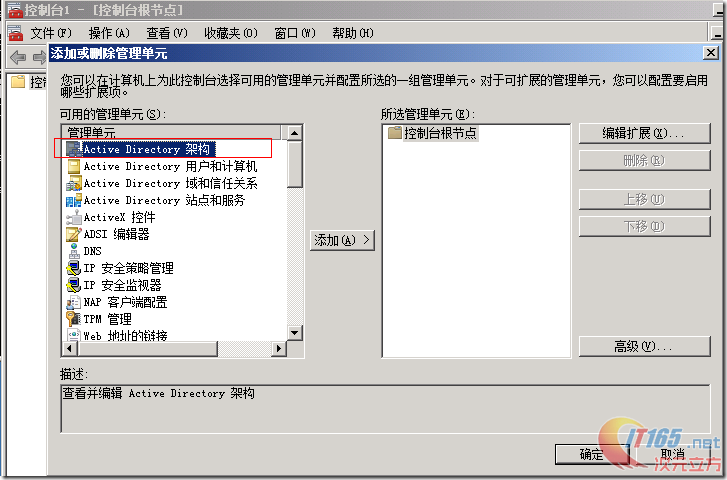
架构主机主要是控制AD内所有对象/属性的定义，损坏后短期内看不到影响，只是在安装布署高级的服务器产品时将会出现问题。比如：安装Exchange时，如果联系不上架构主机，将无法安装成功。

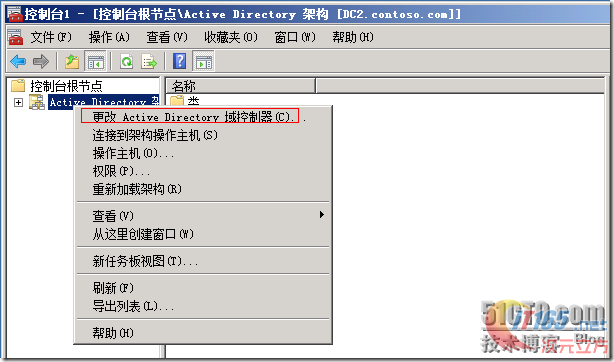
? 转移方法：

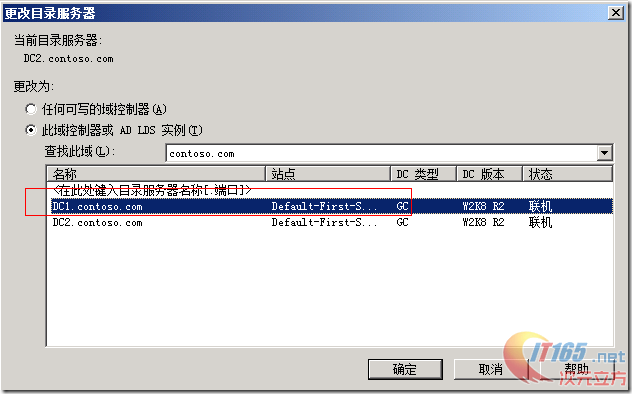
先注册架构域控：regsvr32 C:\WINDOWS\system32\schmmgmt.dll

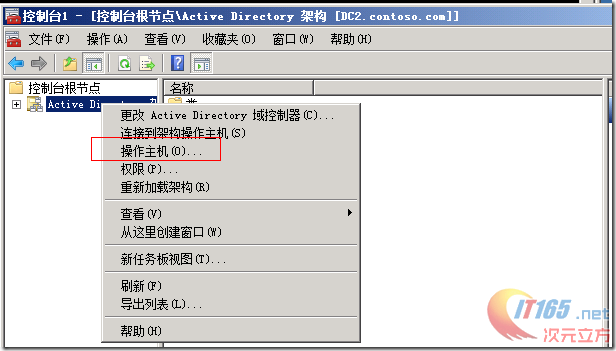
然后在MMC控制台上添加其管理单元，进行角色转换：

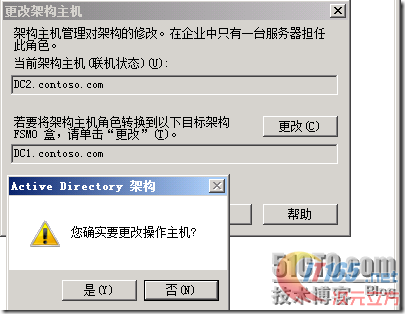
[](http://www.it165.net/uploadfile/2013/0614/20130614101125293.png)

[](http://www.it165.net/uploadfile/2013/0614/20130614101127128.png)

[](http://www.it165.net/uploadfile/2013/0614/20130614101129554.png)

[](http://www.it165.net/uploadfile/2013/0614/20130614101130117.png)

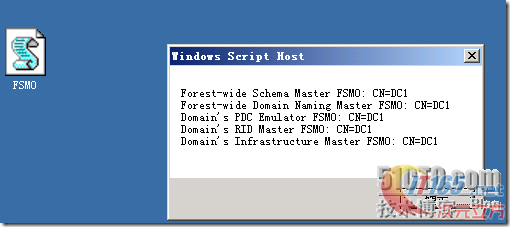
[](http://www.it165.net/uploadfile/2013/0614/20130614101130853.png)

[](http://www.it165.net/uploadfile/2013/0614/20130614101132712.png)

[](http://www.it165.net/uploadfile/2013/0614/20130614101133601.png)

四．测试：

至此五种操作主机在各主机角色都正常的情况下，完成了角色的转移，用VBS脚本查看：

[](http://www.it165.net/uploadfile/2013/0614/20130614101134368.png)

命令行查看：

[](http://www.it165.net/uploadfile/2013/0614/20130614101134677.png)

至此，FSMO五种操作主机角色就完成了正常的迁移了。