

10

第 10 章 操作主机的管理

在AD DS内有一些数据的维护与管理是由**操作主机**（operations master）来负责的，作为系统管理员必须彻底了解它们，以便能够充分掌控与维持域的正常工

- 操作主机概述
- 操作主机的放置优化
- 找出扮演操作主机角色的域控制器
- 转移操作主机角色
- 夺取操作主机角色



10.1 操作主机概述

AD DS数据库内绝大部分数据的复制是采用**多主机复制模式**（multi-master replication model），也就是可以直接更新任何一台域控制器内绝大部分的AD DS对象，之后这个对象会被自动复制到其他域控制器。

然而有少部分数据的复制是采用**单主机复制模式**（single-master replication model）。在此模式下，当提出变更对象的请求时，只会由其中一台被称为**操作主机**的域控制器负责接收与处理此请求，也就是说该对象是先被更新在这台操作主机内，再由它将其复制到其他域控制器。

Active Directory域服务（AD DS）内总共有5个操作主机角色：

- 架构操作主机（schema operations master）
- 域命名操作主机（domain naming operations master）
- RID操作主机（relative identifier operations master）
- PDC模拟器操作主机（PDC emulator operations master）
- 基础结构操作主机（infrastructure operations master）

一个林中只有一台**架构操作主机**与一台**域命名操作主机**，这两个林级别的角色默认都是由林根域内的第一台域控制器所扮演。而每一个域拥有自己的**RID操作主机**、**PDC模拟器操作主机**与**基础结构操作主机**，这3个域级别的角色默认是由该域内的第一台域控制器所扮演。

附注

1. 操作主机角色（operations master roles）也被称为flexible single master operations（FSMO）roles。
2. 只读域控制器（RODC）无法扮演操作主机的角色。

10.1.1 架构操作主机

扮演**架构操作主机**角色的域控制器，负责更新与修改**架构**（schema）内的对象种类与属性数据。隶属于Schema Admins组内的用户才有权限修改**架构**。一个林中只可以有一台**架构操作主机**。

10.1.2 域命名操作主机

扮演**域命名操作主机**角色的域控制器，负责林内**域目录分区**的新建与删除，也就是负责

林内的域新建与删除工作。它也负责应用程序目录分区的新建与删除。一个林中只能有一台域命名操作主机。

10.1.3 RID操作主机

每一个域内只可以有一台域控制器来扮演**RID操作主机**角色，而其主要的工作是发放RID（relative ID）给其域内的所有域控制器。RID有什么用途呢？当域控制器内新建了一个用户、组或计算机等对象时，域控制器需要分配一个唯一的安全标识符（SID）给这个对象，此对象的SID是由域SID与RID所组成的，也就是说**对象SID = 域SID + RID**，而RID并不是由每一台域控制器自己产生的，它是由**RID操作主机**来统一发放给其域内的所有域控制器。每一台域控制器需要RID时，它会向**RID操作主机**索取一些RID，这些RID用完后再向**RID操作主机**索取。

由于是由**RID操作主机**来统一发放RID，因此不会有RID重复的情况发生，也就是每一台域控制器所获得的RID都是唯一的，因此对象的SID也是唯一的。如果是由每一台域控制器各自产生RID的话，则可能不同的域控制器会产生相同的RID，因而会有对象SID重复的情况发生。

10.1.4 PDC模拟器操作主机

每一个域内只可以有一台域控制器来扮演**PDC模拟器操作主机**角色，而它所负责的工作有：

- ✎ **支持旧客户端计算机**：例如用户在域内的旧客户端计算机（例如Windows NT 4.0）上更改密码时，这个密码信息会被更新在PDC（primary domain controller）上，而AD DS通过**PDC模拟器操作主机**来扮演PDC的角色。
- ✎ **减少因为密码复制延迟所造成的问题**：当用户的密码更改后，需要一点时间这个密码才会被复制到其他所有的域控制器。如果在这个密码还没有被复制到其他所有域控制器之前，用户利用新密码登录，则可能会因为负责检查用户密码的域控制器内还没有用户的新密码数据，因而无法成功登录。
AD DS采用以下方法来减少这个问题发生的概率：当用户的密码更改后，这个密码会优先被复制到**PDC模拟器操作主机**，而其他域控制器仍然是依照常规复制程序，也就是需要等一段时间后会收到这个最新的密码。如果用户登录时，负责验证用户身份的域控制器发现密码不对时，它会将验证身份的工作转发给拥有新密码的**PDC模拟器操作主机**，以便让用户可以成功登录。
- ✎ **负责整个域时间的同步**：域用户登录时，如果其计算机时间与域控制器不一致的话，将无法登录，而**PDC模拟器操作主机**就是负责整个域内所有计算机时间的同步工作。AD DS的时间同步程序请参考图10-1-1：

■ 图中林根域sayms.local的**PDC模拟器操作主机**DC1默认是使用本地计算机时间，



但也可以将其设置为与外部的时间服务器同步。

- 所有其他域的**PDC模拟器操作主机**的计算机时间会自动与林根域sayms.local内的**PDC模拟器操作主机**同步，例如图中的DC2、DC4、DC5、DC6会与DC1同步。
- 各域内的其他域控制器都会自动与该域的**PDC模拟器操作主机**时间同步，例如DC3会与DC2同步。
- 域内的成员计算机会与验证其身份的域控制器同步，例如图中sh.sayms.local内客户端计算机会与DC3同步。

由于林根域sayms.local内**PDC模拟器操作主机**的计算机时间会影响到林内所有计算机的时间，因此请确保此台**PDC模拟器操作主机**的时间正确性。

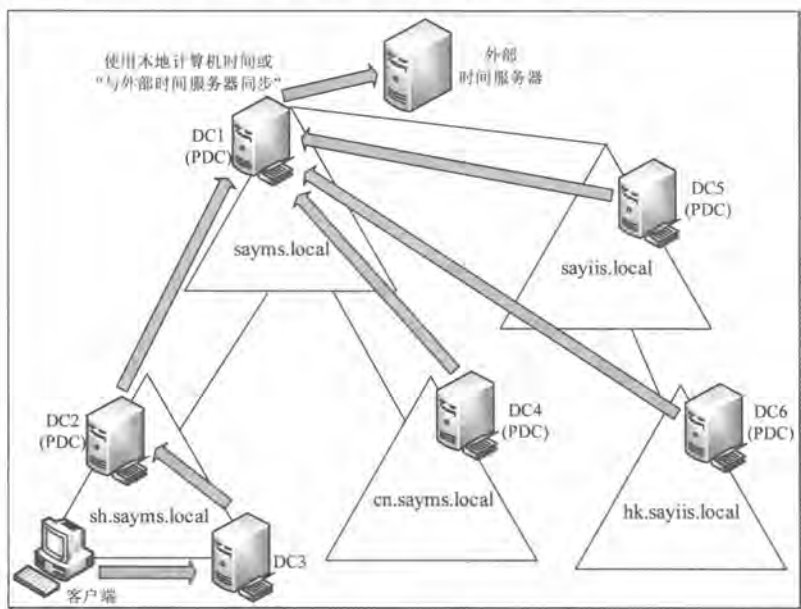


图 10-1-1

我们可以利用 `w32tm /query /Source` 命令来查看时间同步的设置，例如林根域sayms.local的**PDC模拟器操作主机**DC1默认是使用本地计算机时间，如图10-1-2所示的Local CMOS Clock（如果是Hyper-V虚拟机的话，则会显示VM IC Time Synchronization Provider，除非取消虚拟机的集成服务中的时间同步）。



图 10-1-2

如果要将其改为与外部时间服务器同步的话，可执行以下命令（参考图10-1-3）：

```
w32tm /config /manualpeerlist:"time.windows.com time.nist.gov time-nw.nist.gov" /syncfromflags:manual /reliable:yes /update
```

此命令被设置成可与3台时间服务器（time.windows.com、time.nist.gov与time-nw.nist.gov）同步，服务器的DNS主机名之间使用空格来隔开，同时利用""符号将这些服务器框起来。



图 10-1-3

客户端计算机也可以通过w32tm /query /configuration命令来查看时间同步的设置，而我们可以从此命令的结果界面（参考图10-1-4）的Type字段来判断此客户端计算机时间的同步方式：

附注

未加入域的客户端计算机可能需要先启动**Windows Time**服务，再来执行上述程序，而且必须以系统管理员的身份来执行此程序。

- ✎ **NoSync**: 表示客户端不会同步时间。
- ✎ **NTP**: 表示客户端会从外部的时间服务器来同步，而所同步的服务器会显示在图中NtpServer字段，例如图中的time.windows.com。
- ✎ **NT5DS**: 表示客户端是通过前面图10-1-1的域架构方式来同步时间。
- ✎ **AllSync**: 表示客户端会选择所有可用的同步机制，包含外部时间服务器与域架构方式。

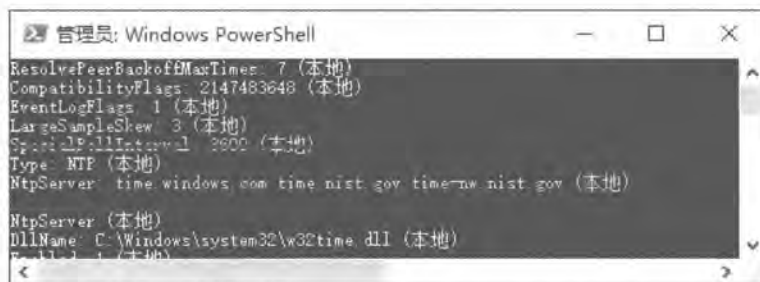


图 10-1-4

附注

上述命令适用于Windows Vista（含）以后的系统，如果是旧版Windows系统的话，可用net time /queryntp命令，不过其所显示的信息有限。



如果客户端计算机是通过图10-1-1域架构方式来同步时间的话,则执行`w32tm /query /configuration`命令后的Type字段为如图10-1-5所示NT5DS。也可以通过如图10-1-6所示的`w32tm /query /source`命令来得知其当前所同步的时间服务器,例如图中的`dc1.sayms.local`,它就是前面图10-1-1中域`sayms.local`的PDC。

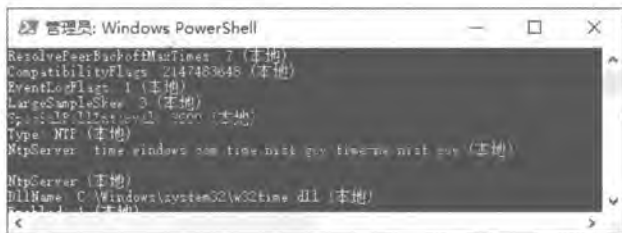


图 10-1-5

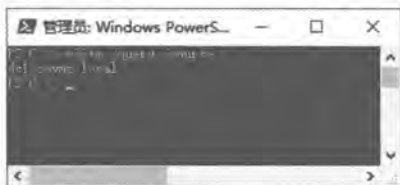


图 10-1-6

附注

时间同步所使用的通信协议为SNTP (Simple Network Time Protocol), 其端口号码为UDP 123。

未加入域的计算机,其时间默认会自动与微软的时间服务器`time.windows.com`同步,如果要更改此设置或执行手动同步的话,以Windows 10计算机来说,可以在此计算机上【按`Win+R`键→输入`control`后按`Enter`键→单击**时钟和区域**→单击**日期和时间**→如图10-1-7所示单击**Internet时间**选项卡→单击**更改设置**按钮→通过前景图来设置】,图中可通过**立即更新**按钮来立即同步时间。域成员计算机或未加入域的计算机都可以利用`w32tm/resync`命令来手动同步。



图 10-1-7

10.1.5 基础结构操作主机

每一个域内只能有一台域控制器来扮演**基础结构操作主机**的角色。如果域内有对象参考到其他域的对象时, **基础结构操作主机**会负责更新这些参考对象的数据,例如本域内有一个



组的成员包含另外一个域的用户账户，当这个用户账户发生变动时，**基础结构操作主机**便会负责更新这个组的成员信息，并将其复制到同一个域内的其他域控制器。

基础结构操作主机是通过**全局编录服务器**来得到这些参考数据的最新版本，因为**全局编录服务器**会收到由每一个域所复制的最新变动信息。

10.2 操作主机的放置优化

为了提高运行效率、减轻系统管理的负担与减少问题发生的概率，因此如何适当地放置操作主机便成为不可忽视的课题。

10.2.1 基础结构操作主机的放置

由于基础结构操作主机与全局编录并不兼容，因此请勿将基础结构操作主机放置到全局编录服务器上，除非是以下的情况：

- ✎ **所有的域控制器都是“全局编录服务器”**：由于全局编录服务器会收到由每一个域所复制来的最新变动信息，故此时由哪一台域控制器来扮演**基础结构操作主机**都无所谓。
- ✎ **只有一个域**：如果整个林中只有一个域，则**基础结构操作主机**就没有作用了，因为没有其他域的对象可供参考，此时不需要理会**基础结构操作主机**是由哪一台域控制器来扮演。

为了便于管理起见，建议将域级别的**RID操作主机**、**PDC模拟器操作主机**与**基础结构操作主机**都放置到同一台域控制器上。

10.2.2 PDC模拟器操作主机的放置

PDC模拟器操作主机经常需要与网络上其他系统通信，它的负担比其他操作主机重，因此这台计算机的设备性能应该要最好、最稳定，以确保能够应付比较繁重的负担与提供比较高的可用性。

如果要降低**PDC模拟器操作主机**负载的话，可以在DNS服务器内调整它的**权重（weight）**。当客户端需要查找域控制器来验证用户身份时，客户端会向DNS服务器查询域控制器，而DNS服务器会将客户端导向（refer to）到指定的域控制器，由这台域控制器来负责验证用户身份，由于所有域控制器默认的**权重值**是相同的（100），因此每一台域控制器被导向的概率是相同的。如果将**PDC模拟器操作主机**的**权重值**降低的话，例如降为一半（50），则客户端被导向到这台**PDC模拟器操作主机**的概率就会降低一半，如此便可以降低



它的负载。

假设PDC模拟器操作主机为dc1.sayms.local，而要降低其权重值的话：【打开DNS管理控制台如图10-2-1所示展开到区域sayms.local之下的_tcp文件夹双击右侧的dc1.sayms.local修改图10-2-2中的权重值】。

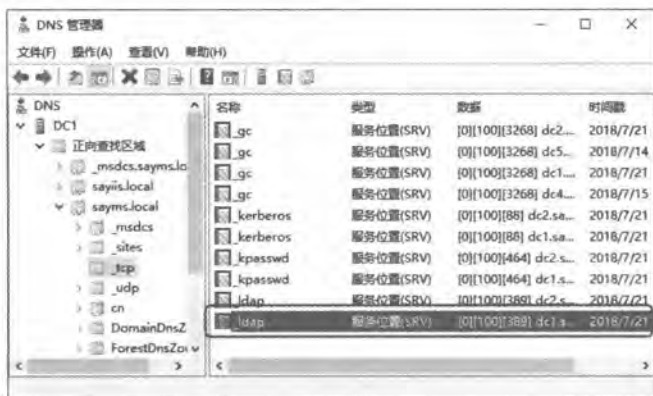


图 10-2-1



图 10-2-2

10.2.3 林级别操作主机的放置

林中第一台域控制器会自动扮演林级别的架构操作主机与域命名操作主机的角色，它同时也是全局编录服务器。这两个角色并不会对域控制器造成太大负担，它们也与全局编录兼容，而且即使将这两个角色移动到其他域控制器也不会改善运行性能，因此为了便于管理与执行备份、还原工作，建议将这两个角色继续保留由这台域控制器来扮演。

10.2.4 域级别操作主机的放置

每一个域内的第一台域控制器会自动扮演域级别的操作主机，而以林根域中的第一台域

控制器来说，它同时也扮演两个林级别与3个域级别的操作主机，同时也是**全局编录服务器**，不过因为其中的**基础结构操作主机**与**全局编录**并不兼容，因此除非所有域控制器都是**全局编录服务器**或林中只有一个域，否则请将**基础结构操作主机**的角色转移到其他域控制器，如前所述，为了便于管理起见，请将**RID操作主机**与**PDC模拟器操作主机**也一并转移到这台域控制器。

除了林根域之外，其他域请将3台域级别操作主机保留由第一台域控制器来扮演，但不要将这台域控制器设置为**全局编录服务器**，除非所有域控制器都是**全局编录服务器**或林中只有一个域。除非工作负担太重，否则请尽量将这3个操作主机交由同一台域控制器来扮演，以减轻管理负载。

10.3 找出扮演操作主机角色的域控制器

在建立AD DS域时，系统会自动选择域控制器来扮演操作主机，我们将在本节介绍如何找出扮演操作主机的域控制器。

10.3.1 利用管理控制台找出扮演操作主机的域控制器

不同的操作主机角色可以利用不同的Active Directory管理控制台来检查，如表10-3-1所示。

表10-3-1

角色	管理控制台
架构操作主机	Active Directory架构
域命名操作主机	Active Directory域和信任关系
RID操作主机	Active Directory用户和计算机
PDC模拟器操作主机	Active Directory用户和计算机
基础结构操作主机	Active Directory用户和计算机

1. 找出架构操作主机

我们可以利用**Active Directory架构**控制台来找出当前扮演**架构操作主机**角色的域控制器。

STEP 1 请到域控制器上登录、注册schmmgmt.dll，才可使用Active Directory架构控制台，如果尚未注册schmmgmt.dll的话，请先执行以下命令：

```
regsvr32 schmmgmt.dll
```

并在出现登录成功界面后，再继续以下的步骤。



STEP 2 按 **Win+R** 键输入 MMC 后单击 **确定** 按钮单击 **文件** 菜单单击 **添加/删除管理单元** 在图 10-3-1 中选择 **Active Directory 架构** 单击 **添加** 按钮单击 **确定** 按钮。

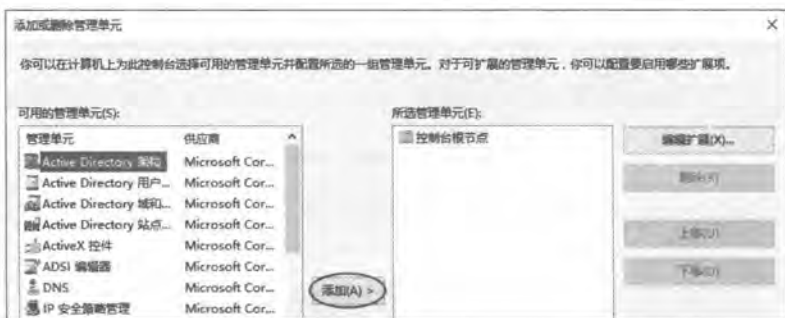


图 10-3-1

STEP 3 如图 10-3-2 所示【选中 **Active Directory 架构** 并右击 **操作主机**】。

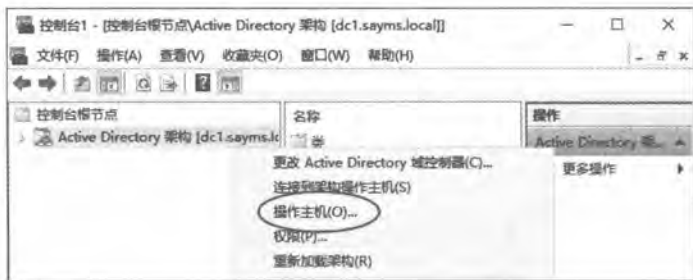


图 10-3-2

STEP 4 从图 10-3-3 可知架构操作主机为 dc1.sayms.local。

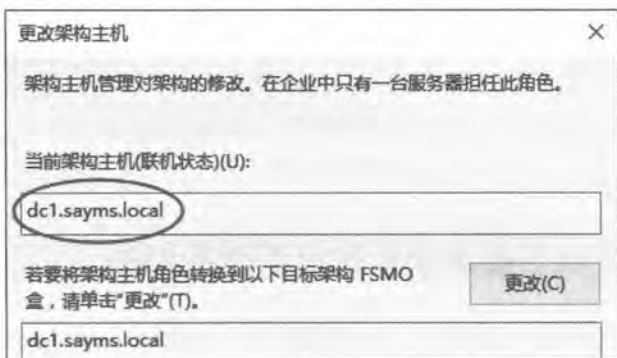


图 10-3-3

2. 找出域命名操作主机

找出当前扮演域命名操作主机角色的域控制器的方法为：【单击左下角开始图标 **Win** Windows 管理工具 **Active Directory 域和信任关系** 如图 10-3-4 所示选中 **Active Directory 域和信任关系** 并右击 **操作主机** 从前景图可知域命名操作主机为 dc1.sayms.local】。

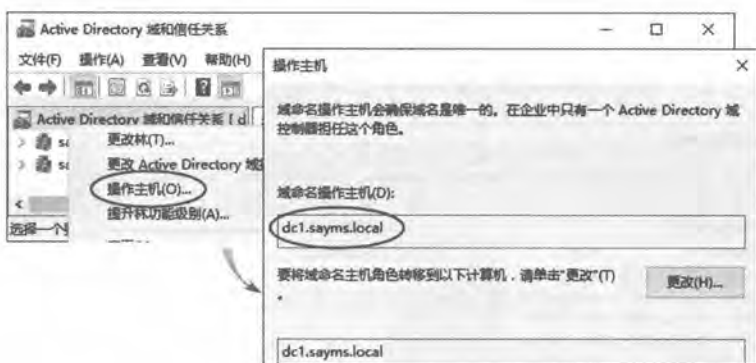


图 10-3-4

3. 找出 RID、PDC 模拟器与基础结构操作主机

找出当前扮演这3个操作主机角色的域控制器的方法为：【单击左下角开始图标田➡Windows 管理工具➡Active Directory用户和计算机➡如图10-3-5所示选中域名（sayms.local）并右击➡操作主机➡从前景图可知RID操作主机为dc1.sayms.local】，还可以从图中的PDC与基础结构选项卡来得知扮演这两个角色的域控制器。



图 10-3-5

10.3.2 利用命令找出扮演操作主机的域控制器

可以打开Windows PowerShell窗口，然后通过执行netdom query fsmo命令来查看扮演操作主机角色的域控制器，如图10-3-6所示。

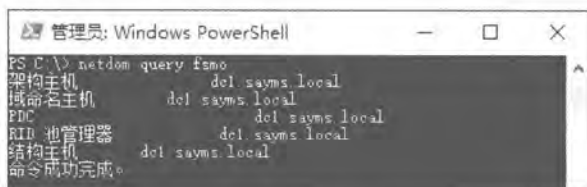


图 10-3-6

也可以在Windows PowerShell窗口内，通过执行以下的Get-ADDomain命令来查看扮演域级别操作主机角色的域控制器（参考图10-3-7）。

```
Get-ADDomain sayms.local | FT PDCEmulator,RIDMaster,InfrastructureMaster
```

或是通过执行以下的Get-ADForest命令来查看扮演林级别操作主机角色的域控制器（参考图10-3-7）。

```
Get-ADForest sayms.local | FT SchemaMaster,DomainNamingMaster
```

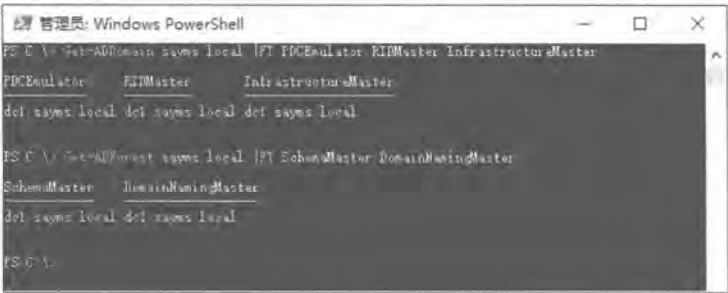


图 10-3-7

10.4 转移操作主机角色

在建立AD DS域时，系统会自动选择域控制器来扮演操作主机，而在要将扮演操作主机角色的域控制器降级为成员服务器时，系统也会自动将其操作主机角色转移到另外一台适当的域控制器，因此在大部分的情况下，并不需要自行转移操作主机角色。

不过有时可能需要自行转移操作主机角色，例如域架构更改或原来扮演操作主机角色的域控制器负载太重，而想要将其转移到另外一台域控制器，以便降低原操作主机的负载。

请在将操作主机角色安全转移到另外一台域控制器之前，先确定两台域控制器都已经连上网络、可以相互通信，同时操作用户必须是隶属于表10-4-1中的组或被委派权限，才有权执行转移的工作。

表10-4-1



角色	有权限的组
架构操作主机	Schema Admins
域命名操作主机	Enterprise Admins
RID操作主机	Domain Admins
PDC模拟器操作主机	Domain Admins
基础结构操作主机	Domain Admins

在执行安全转移操作之前，请注意以下事项：

- ✎ 转移角色的过程中并不会会有数据丢失；
- ✎ 可以将林级别的架构操作主机与域命名操作主机转移到同一个林中的任何一台域控制器；
- ✎ 可以将域级别的RID操作主机与PDC模拟器操作主机转移到同一个域中的任何一台域控制器；
- ✎ 不要将基础结构操作主机转移到兼具全局编录服务器的域控制器，除非所有域控制器都是全局编录服务器或林中只有一个域。

10.4.1 利用管理控制台

转移任何一种操作主机的步骤都类似，因此以下利用转移PDC模拟器操作主机为例来说明，并且假设要将PDC模拟器操作主机由dc1.sayms.local转移到dc2.sayms.local。

STEP 1 单击左下角开始图标 Windows 管理工具  Active Directory 用户和计算机。

附注

转移PDC模拟器操作主机、RID操作主机与基础结构操作主机都是使用Active Directory 用户和计算机控制台，而转移架构操作主机是使用Active Directory架构控制台、转移域命名操作主机是使用Active Directory域及信任控制台。

STEP 2 如果当前所连接的域控制器就是即将扮演操作主机的dc2.sayms.local（如图10-4-1所示），则请跳到 **STEP 5**，否则请继续以下的步骤。



图 10-4-1


STEP 3 如图10-4-2所示【选中Active Directory用户和计算机并右击 更改域控制器】（目前所连接到域控制器为dc1.sayms.local）。



图 10-4-2

STEP 4 在图10-4-3中选择即将扮演操作主机角色的域控制器dc2.sayms.local后单击 **确定** 按钮。



图 10-4-3

STEP 5 如图10-4-4所示【选中域名sayms.local并右击 **操作主机**】。



图 10-4-4

STEP 6 如图10-4-5所示【单击PDC选项卡 **确认** 当前所连接的域控制器是dc2.sayms.local **单击** **更改** 按钮 **单击** **是 (Y)** 按钮 **单击** **确定** 按钮】。



图 10-4-5

STEP 7 从图10-4-6中可以确定已成功将操作主机转移到dc2.sayms.local。

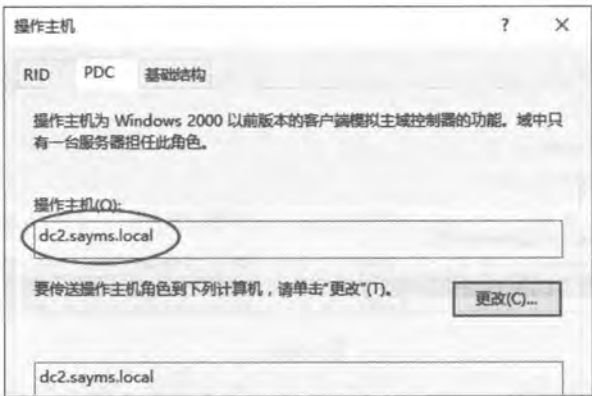


图 10-4-6

10.4.2 利用Windows PowerShell命令

单击左下角开始图标 Windows PowerShell，然后通过执行命令 `Move-ADDirectoryServerOperationMasterRole` 来转移操作主机角色。例如要将PDC模拟器操作主机转移到dc2.sayms.local的话，请执行以下命令后按Y键或A键（参考图10-4-7）：

```
Move-ADDirectoryServerOperationMasterRole -Identity "DC2" -  
OperationMasterRole PDCEmulator
```

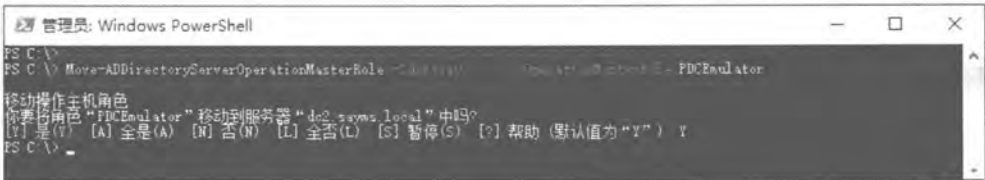


图 10-4-7



如果要转移其他角色的话，只要将 PDCEmulator 字样换成 RIDMaster、InfrastructureMaster、SchemaMaster或DomainNamingMaster即可。

如果要一次同时转移多个角色的话，例如同时将**PDC模拟器操作主机**与**基础结构操作主机**转移到dc2.sayms.local的话，请输入以下命令（角色名称之间以逗号隔开）后按**A**键：

```
Move-ADDirectoryServerOperationMasterRole -Identity "DC2" -
OperationMasterRole PDCEmulator, InfrastructureMaster
```

这些角色也可以利用数字来代表，如表10-4-2所示。

表10-4-2

操作主机	代表号码
PDC模拟器操作主机	0
RID操作主机	1
基础结构操作主机	2
架构操作主机	3
域命名操作主机	4

因此，如果要将所有操作主机都转移到dc2.sayms.local的话，可执行以下指令后按**A**键：

```
Move-ADDirectoryServerOperationMasterRole -Identity "DC2" -
OperationMasterRole 0,1,2,3,4
```

10.5 夺取操作主机角色

若扮演操作主机角色的域控制器发生故障或网络有问题时，则可能需要采用**夺取**（seize，拿取）方式来将操作主机角色强迫转移到另外一台域控制器。

注意

只有在无法安全转移的情况下，才使用夺取的方法。由于夺取是非常的手段，因此请确认有其必要性后，再执行夺取的步骤。

10.5.1 操作主机停摆所造成的影响

有的操作主机发生故障时，短时间内就会对网络造成明显的影响，然而有的却不会，因此请参考以下说明来决定是否要尽快夺取操作主机角色。

由于新操作主机是根据其中的AD DS数据库来运作，因此为了减少数据丢失，请在执行夺取步骤之前等一段足够的时间（至少等所有域控制器之间完成一次AD DS复制所需的时间）。



间)，让这台即将成为新操作主机的域控制器完整接收到从其他域控制器复制的异动数据。

由于夺取操作主机时并未与原操作主机沟通协调，因此一旦夺取操作主机角色后，请不要再启动原扮演操作主机角色的域控制器，否则会出现两台域控制器都各自认为是操作主机，因而会影响到AD DS的运作。

注意

一旦架构操作主机、域命名操作主机或RID操作主机的角色被夺取后，请永远不要将原来扮演这些操作主机角色的域控制器再连接到网络上，否则严重的话，整个AD DS数据库可能会损毁。建议将这台域控制器的硬盘格式化。

1. 架构操作主机停止服务时

由于用户并不会直接与架构操作主机沟通，因此若架构操作主机暂时无法提供服务的话，对用户并没有影响；而对系统管理员来说，除非他们需要存取架构内的数据，例如安装会修改架构的应用程序（例如Microsoft Exchange Server），否则也暂时不需要使用到架构操作主机，所以请等架构操作主机修复后重新上线即可，不需要执行夺取的步骤。

如果架构操作主机停摆的时间太久，以至于影响到系统运作时，则您应该夺取操作主机角色，以便改由另外一台域控制器来扮演。

2. 域命名操作主机停止服务时

域命名操作主机暂时无法提供服务的话，对网络用户并没有影响，而对系统管理员来说，除非他们要添加或删除域，否则也暂时不需要使用到域命名操作主机，所以请等域命名操作主机修复重新上线即可，不需要执行夺取的步骤。

如果域命名操作主机停止服务的时间太久，以至于影响到系统运作时，则应该夺取操作主机角色，改由另外一台域控制器来扮演。

3. RID 操作主机停止服务时

RID操作主机暂时无法提供服务，对网络用户并没有影响，而对系统管理员来说，除非他们要在域内新增对象，同时他们所连接的域控制器之前所索取的RID已经用完，否则也暂时不需要使用到RID操作主机，故可以不需要执行夺取的步骤。

如果RID操作主机停止服务的时间太久，以至于影响到系统运作时，则您应该夺取操作主机角色，改由另外一台域控制器来扮演。

4. PDC 模拟器操作主机停止服务时

由于PDC模拟器操作主机无法提供服务时，网络用户可能会比较快察觉到，例如密码复



制延迟问题，造成客户端无法使用新密码来登入（参考章节10-1关于**PDC模拟器操作主机**的说明），此时应该尽快修复**PDC模拟器操作主机**，若无法在短期内修复的话，则需要尽快执行夺取步骤。

5. 基础结构操作主机停止服务时

基础结构操作主机暂时无法提供服务的话，对网络用户并没有影响，而对系统管理员来说，除非他们最近搬移大量账户或改变大量账户的名称，否则也不会察觉到**基础结构操作主机**已经停止服务，所以暂时可以不需要执行夺取的步骤。

若**基础结构操作主机**停止服务的时间太久，以至于影响到系统运作时，则应该夺取操作主机角色，改由另外一台不是**全局编录服务器**的域控制器来扮演此角色。

10.5.2 夺取操作主机角色实例演练

我们利用以下范例来解说如何夺取操作主机角色，以便让域能够继续正常运作。

注意

只有在无法利用**转移**方法的情况下，才使用**夺取**方法。你必须是隶属于适当的组才可以执行**夺取**的操作（参见表10-4-1）。

假设图10-5-1中只有一个域，其中除了**PDC模拟器操作主机**是由dc2.sayms.local所扮演之外，其他4个操作主机都是由dc1.sayms.local所扮演。现在假设dc2.sayms.local这台域控制器因故永远无法使用了，因此需要夺取**PDC模拟器操作主机**角色，改由另外一台域控制器dc1.sayms.local来扮演。

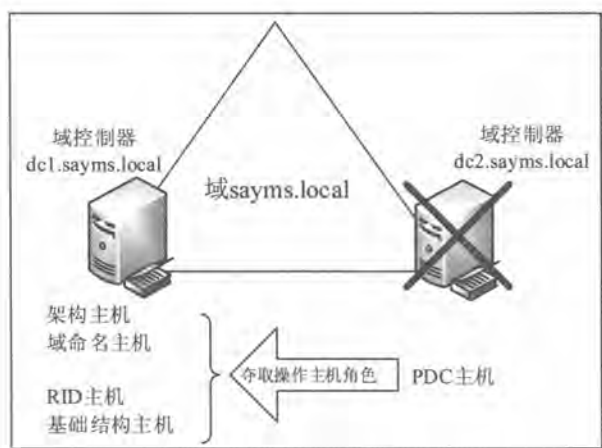



图 10-5-1

单击左下角开始图标  Windows PowerShell，然后跟前面转移角色一样使用命令 **Move-ADDirectoryServerOperationMasterRole**，不过要增加 **-Force** 参数来夺取操作主机角色，例如以下命令会夺取 **PDC模拟器操作主机**，并改由 **dc1.sayms.local** 来扮演：

```
Move-ADDirectoryServerOperationMasterRole -Identity"DC1"-OperationMasterRole  
PDCEmulator -Force
```

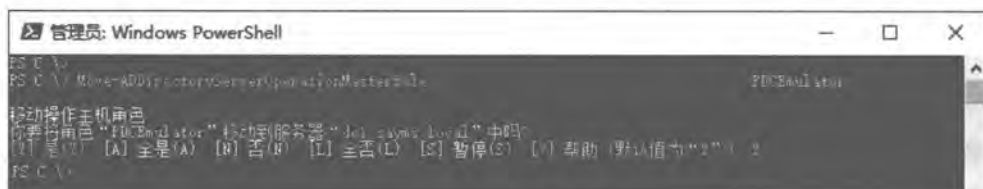


图 10-5-2