11

第 11 章　AD DS 的维护

为了维持域环境的正常运行，因此应该定期备份AD DS（Active Directory域服务）的相关数据。同时为了保持AD DS的运行性能，因此也应该充分了解AD DS数据库。

- 系统状态概述
- 备份AD DS
- 还原AD DS
- AD DS数据库的移动与整理
- 重置“目录服务修复模式”的管理员密码
- 更改“可重新启动的AD DS”的注册表设置
- Active Directory回收站

11.1 系统状态概述

Windows Server 2016服务器的系统状态（system state）内所包含的数据，因服务器所安装的角色种类而有所不同，例如可能包含着以下的数据：

- 键值
- COM+ 类别注册数据库（Class Registration database）
- 启动文件（boot files）
- Active Directory证书服务（AD CS）数据库
- AD DS数据库（Ntds.dit）
- SYSVOL文件夹
- 群集服务信息
- Microsoft Internet Information Services（IIS） metadirectory
- 受Windows Resource Protection保护的系统文件

11.1.1 AD DS数据库

AD DS内的组件主要分为AD DS数据库文件与SYSVOL文件夹，其中AD DS数据库文件默认是位于%*systemroot*%\NTDS文件夹内，如图11-1-1所示。

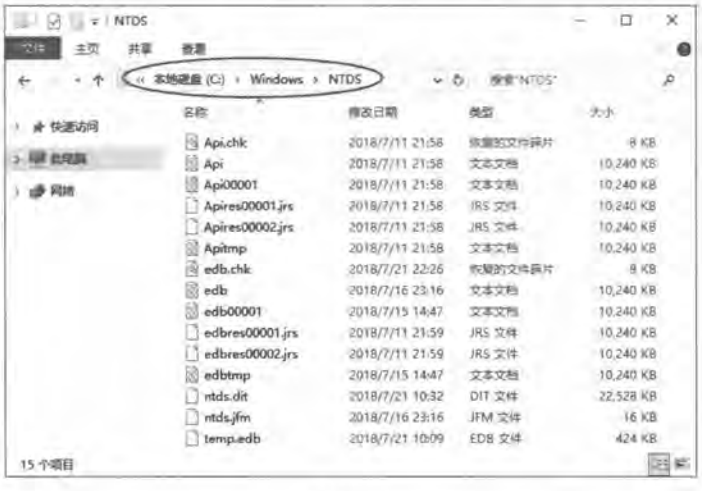

图 11-1-1

- **ntds.dit**：AD DS数据库文件，存储着这台域控制器的AD DS内的对象。
- **edb.log**：它是AD DS事务日志（扩展名.log默认会被隐藏），容量大小为10 MB。当要更改AD DS内的对象时，系统会先将变动数据写入到内存（RAM）中，然后等适当时机（例如系统空闲、关机时等），再根据内存中的记录来将更新数据写入AD DS数

据库（ntds.dit）。这种先在内存中处理的方式，可提高AD DS的工作效率。

系统也会将内存中数据的变动过程写到事务日志内（edb.log），如果系统不正常关机（例如断电），以至于内存中尚未被写入AD DS数据库的更新数据丢失时，系统就可以根据事务日志，来推算出不正常关机前，在内存中的更新记录并将这些记录写入AD DS数据库。如果事务日志填满了数据，则系统会将其改名，例如Edb00001.log、Edb00002.log、……，并重新建立一个事务日志。

- **edb.chk**：它是**检查点**（checkpoint）文件。每一次系统将内存中的更新记录写入AD DS数据库时，都会一并更新edb.chk，它会记载事务日志的检查点。如果系统不正常关机，以至于内存中尚未被写入AD DS数据库的更新记录丢失的话，则下一次开机时，系统便可以根据edb.chk来得知需要从事务日志内的哪一个变动过程开始，来推算出不正常关机前内存中的更新记录，并将它们写入AD DS数据库。
- **edbres00001.jrs**与**edbres00002.jrs**：这两个是预留文件，未来如果硬盘的空间不够时可以使用这两个文件，每一个文件都是10 MB。

11.1.2 SYSVOL文件夹

SYSVOL文件夹是位于*%systemroot%*内，此文件夹内存储着以下的数据：**脚本文件**（scripts）、**NETLOGON共享文件夹**、**SYSVOL共享文件夹**与**组策略相关设置**。

11.2 备份AD DS

应该定期备份域控制器的系统状态，以便当域控制器的AD DS损坏时，可以通过备份数据来还原域控制器。

11.2.1 安装Windows Server Backup功能

首先需要添加Windows Server Backup功能：【打开**服务器管理器**➲单击**仪表板**处的**添加角色和功能**➲持续单击 下一步 按钮，直到出现如图11-2-1所示的界面时勾选**Windows Server Backup**➲单击 下一步 按钮、 安装 按钮】。

图 11-2-1

11.2.2 备份系统状态

我们将通过备份**系统状态**的方式来备份AD DS，系统状态的文件是位于安装Windows系统的磁盘内，一般是C盘，这个磁盘我们将它称为备份的**源磁盘**，然而备份**目的地磁盘**默认是不能包含源磁盘，所以无法将系统状态备份到源磁盘C:，因此需要将其备份到另外一个磁盘、DVD或其他计算机内的共享文件夹。操作用户必须隶属于Administrators或Backup Operators组才有权限执行备份系统状态的工作，而且必须有权限将数据写入目的地磁盘或共享文件夹。

附注

如果要开放可以备份到源磁盘的话，请在以下注册表路径新建一条名称为AllowSSBToAnyVolume的键值，其类型为DWORD：

```
HKLM\SYSTEM\CurrentControlSet\Services\wbengine\SystemStateBackup
```

其值为1表示开放，为0表示禁止。建议不要开放，否则可能会备份失败，而且需要使用比较多的磁盘空间。

以下假设我们要将系统状态数据备份到网络共享文件夹\\dc2\backup内（请先在dc2计算机上建立好此共享文件夹）：

STEP 1 单击左下角**开始**图标⊞➲**Windows 管理工具**➲**Windows Server Backup**➲如图11-2-2所示单击**一次性备份…**。

图 11-2-2

STEP 2 如图11-2-3所示选择**其他选项**后单击下一步按钮。

STEP 3 在图11-2-4中选择**自定义**后单击下一步按钮。

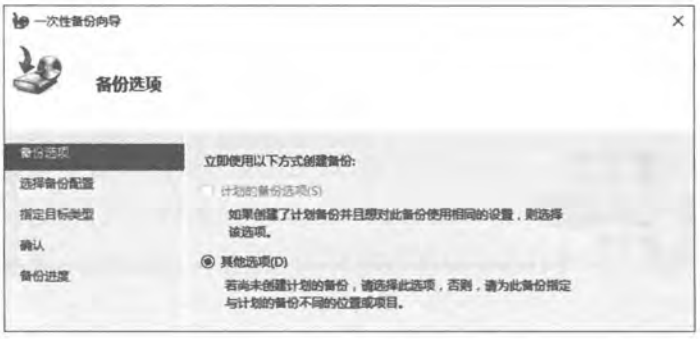

图 11-2-3

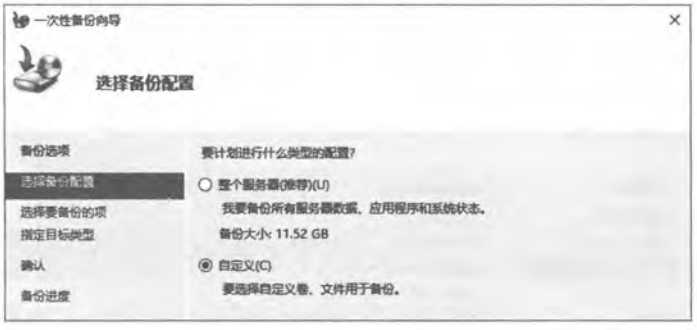

图 11-2-4

附注

也可以通过**整个服务器**来备份整台域控制器内的所有数据，它包含系统状态。

STEP 4 如图11-2-5所示单击添加项目按钮。

图 11-2-5

STEP 5 如图11-2-6所示勾选**系统状态**后单击确定按钮。

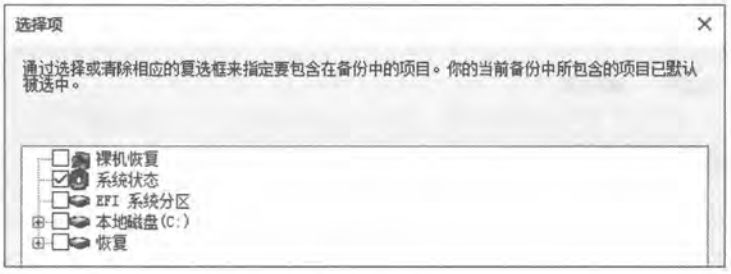

图 11-2-6

STEP 6 回到**选择要备份的项**界面后单击下一步按钮。

STEP 7 如图11-2-7所示选择**远程共享文件夹**后单击下一步按钮。

图 11-2-7

STEP 8 如图11-2-8所示在**位置**处输入\\dc2\backup后单击下一步按钮。

图 11-2-8

STEP 9 在**确认**界面中单击备份按钮。

附注

也可以通过**wbadmin**命令来备份系统状态，例如：

```
wbadmin start systemstatebackup -backuptarget:\\dc2\backup
```

此范例假设是要备份到网络共享文件夹\\dc2\backup。

11.3 还原AD DS

在系统状态备份完成后，若之后AD DS数据损坏的话，就可以通过执行**非授权还原**（nonauthoritative restore）的程序来修复AD DS。必须进入**目录服务修复模式**（Directory Services Restore Mode，DSRM），然后利用之前的备份来执行**非授权还原**的工作。

附注

如果系统无法启动的话，则应该执行完整服务器的还原程序，而不是**非授权还原**程序。

11.3.1 进入目录服务修复模式的方法

打开**命令行**窗口，然后执行以下命令：

```
Bcdedit /set {bootmgr} displaybootmenu Yes
```

重新启动后将出现如图11-3-1的**Windows启动管理器**界面，此时请在30秒内按F8键（如果计算机内安装了多套Windows系统的话，它会自动显示图11-3-1的界面，不需要执行上述命令）。

图 11-3-1

注意

如果使用虚拟机的话，按F8键前先确认焦点是虚拟机上。

之后将出现图11-3-2的**高级启动选项**界面，请选择**目录服务修复模式**后按Enter键，之后

就会出现**目录服务修复模式**的登录界面（后述）。

图 11-3-2

附注

1. 也可以执行**bcdedit /set safeboot dsrepair**命令，不过以后每次启动计算机时，都会进入**目录服务修复模式**的登录界面，因此在完成AD DS还原程序后，请执行**bcdedit /deletevalue safeboot**命令，以便之后启动计算机时，会重新以普通模式来启动系统。
2. 也可以在域控制器上通过重新启动，完成自检后，在系统启动初期立刻按F8键的方式来显示图11-3-2的**高级启动选项**界面，不过却不容易抓准按F8键的时机。

11.3.2 执行AD DS的非授权还原

接下来需要利用**目录服务修复模式**的系统管理员账户与密码登录，并执行AD DS的标准修复程序，也就是**非授权还原**。以下假设之前制作的系统状态备份是位于网络共享文件夹\\dc2\backup内。

STEP 1 在**目录服务修复模式**的登录界面中，如图11-3-3所示输入**目录服务修复模式**的系统管理员的用户名称与密码来登录，其中用户名称可输入.**Administrator**或***计算机名称*****Administrator**。

图 11-3-3

STEP 2 单击左下角**开始**图标⊞➲**Windows 管理工具**➲**Windows Server Backup**➲单击图11-3-4左侧**本地备份**➲单击右侧的**恢复**…。

图 11-3-4

STEP 3 如图11-3-5所示选择**在其他位置存储备份**后单击下一步按钮。

图 11-3-5

STEP 4 如图11-3-6所示选择**远程共享文件夹**后单击下一步按钮。

图 11-3-6

STEP 5 如图11-3-7所示输入共享文件夹路径\\dc2\backup后单击下一步按钮。

图 11-3-7

STEP 6 在图11-3-8中选择备份的日期与时间后单击下一步按钮。

图 11-3-8

STEP 7 如图11-3-9所示选择恢复**系统状态**后单击下一步按钮。

图 11-3-9

STEP 8 如图11-3-10所示选择**原始位置**后单击下一步按钮。

图 11-3-10

STEP 9 在图11-3-11中单击确定按钮。

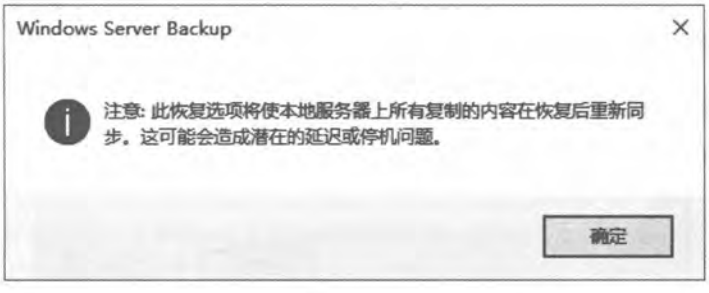

图 11-3-11

STEP 10 参考图11-3-12中的说明后单击确定按钮。

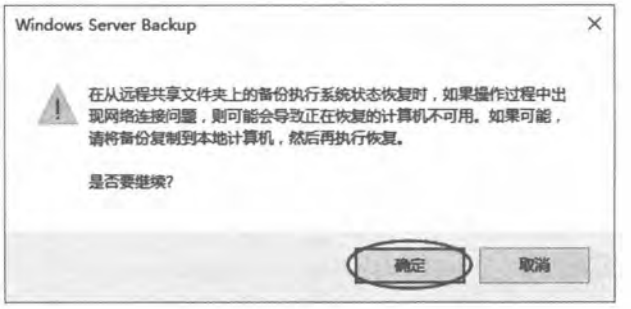

图 11-3-12

STEP 11 如图11-3-13所示单击恢复按钮。

图 11-3-13

STEP 12 在图11-3-14中单击是（Y）按钮。

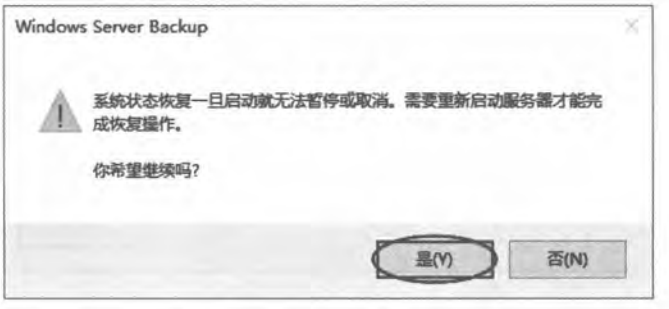

图 11-3-14

STEP 13 完成恢复后，请依照界面提示重新启动计算机。

附注

如果是利用**bcdedit /set safeboot dsrepair**命令进入目录服务修复模式的话，可先执行bcdedit /deletevalue safeboot，以便让系统重新以普通模式启动。

如果要通过wbadmin.exe程序来恢复系统状态的话，请先执行以下命令：

```
wbadmin get versions -backuptarget:\\dc2\backup
```

它用来读取备份的版本号码，其中的**-backuptarget**用来指定存储备份的位置。

附注

如果在存储备份的位置内存储着多台服务器的备份，则可以指定要读取的服务器，例如要读取属于服务器DC1的备份的话，可增加**-machine:dc1** 这个参数。

请记下要用来恢复的备份版本，它是位于**版本标识符**处的字符串（假设是**07/21/2018-23:42**），然后执行以下命令：

```
wbadmin start systemstaterecovery-version:07/21/2018-23:42 -
ackuptarget:\\dc2\backup
```

11.3.3 针对被删除的AD DS对象执行授权还原

如果域内只有一台域控制器，则只需要执行**非授权还原**即可，但是如果域内有多台的域控制器的话，则可能还需配合**授权还原**。

例如域内有两台域控制器DC1与DC2，而且曾经备份域控制器DC2的系统状态，可是今天却不小心利用**Active Directory管理中心**控制台将用户账户**王乔治**删除，之后这个变动数据会通过AD DS复制机制被复制到域控制器DC1，因此在域控制器DC1内的**王乔治**账户也会被删除。

注意

当你将用户账户删除后，此账户并不会立刻从AD DS数据库内删除，而是被移动到AD DS数据库内一个名称为**Deleted Objects**的容区内，同时这个用户账户的版本号码会被加1。系统默认是180天后才会将其从AD DS数据库内删除。

若要恢复被不小心删除的**王乔治**账户，可能会在域控制器DC2上利用标准的**非授权还原**来将之前已经备份的旧**王乔治**账户恢复，可是虽然在域控制器DC2内的**王乔治**账户已被恢复

了，但是在域控制器DC1内的**王乔治**却是被标记为**已删除**的账户，请问下一次DC1与DC2之间执行Active Directory复制过程时，将会有什么样的结果呢？

答案是在DC2内刚被恢复的**王乔治**账户会被删除，因为对系统来说，DC1内被标记为**已删除**的**王乔治**的版本号较高，而DC2内刚恢复的**王乔治**是旧的数据，其版本号较低。在第9章曾经介绍过两个对象发生冲突时，系统会以**标记**（stamp）来作为解决冲突的依据，因此版本号码较高的对象会覆盖掉版本号码较低的对象。

如果要避免上述现象发生的话，需要另外再执行**授权还原**。当在DC2上针对**王乔治**账户另外执行过**授权还原**后，这个被恢复的旧**王乔治**账户的版本号将被增加，而且是从备份当天开始到执行**授权还原**为止，每天增加100,000，因此当DC1与DC2开始执行复制工作时，由于位于DC2的旧**王乔治**账户的版本号会比较高，所以这个旧**王乔治**会被复制到DC1，将DC1内被标记为**已删除**的**王乔治**覆盖掉，也就是说旧**王乔治**被还原了。

以下练习假设上述用户账户**王乔治**是建立在域sayms.local的组织单位**业务部**内，我们需要先执行**非授权还原**，然后再利用**ntdsutil**命令来针对用户账户**王乔治**执行**授权还原**。可以依照以下的顺序来练习：

- 在域控制器DC2建立组织单位**业务部**、在**业务部**内建立用户账户**王乔治**（George）
- 等组织单位**业务部**、用户账户**王乔治**账户被复制到域控制器DC1
- 在域控制器DC2备份**系统状态**
- 在域控制器DC2上将用户账户**王乔治**删除（此账户会被移动到**Deleted Objects**容器内）
- 等这个被删除的**王乔治**账户被复制到域控制器DC1，也就是等DC1内的**王乔治**也被删除（默认是等15秒）
- 在DC2上先执行**非授权还原**，然后再执行**授权还原**，它便会将被删除的**王乔治**账户还原

以下仅说明最后一个步骤，也就是先执行**非授权还原**，然后再执行**授权还原**。

STEP 1 请到DC2执行**非授权还原**步骤，也就是前面11.3.2小节的**执行AD DS的非授权还原** STEP 1到STEP 12，注意不要执行STEP 13，也就是完成恢复后，**不要**重新启动计算机。

STEP 2 继续在**Windows PowerShell**窗口下执行以下命令（完整的操作界面可以如图11-3-16所示）：

```
ntdsutil
```

STEP 3 在**ntdsutil**：提示符下执行以下命令：

```
activate instance ntds
```

表示要将域控制器的AD DS数据库设置为使用中。

STEP 4 在**ntdsutil**：提示符下执行以下命令：

```
authoritative  restore
```

STEP 5 在**authoritative restore**：提示符下，针对域sayms.local的组织单位**业务部**内的用户**王乔治**执行**授权还原**，其命令如下所示：

```
restore  object  CN=王乔治,OU=业务部,DC=sayms,DC=local
```

附注

如果要针对整个AD DS数据库执行**授权还原**的话，请执行**restore database**命令；如果要针对组织单位**业务部**执行**授权还原**的话，请执行以下命令（可输入**?**来查询命令的语法）：

```
restore  subtree  OU=业务部,DC=sayms,DC=local
```

STEP 6 在图11-3-15中单击是（Y）按钮。

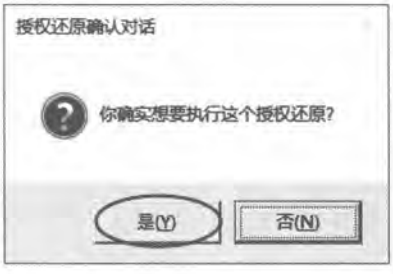

图 11-3-15

STEP 7 图11-3-16为前面几个步骤的完整操作过程。

图 11-3-16

STEP 8 在authoritative restore：提示符下，执行**quit**命令。

STEP 9 在**ntdsutil**：提示符下，执行**quit**命令。

STEP 10 利用普通模式重新启动系统。

STEP 11 等域控制器之间的AD DS自动同步完成，或利用**Active Directory站点和服务**手动同步，或执行以下命令来手动同步：

```
repadmin  /syncall dc2.sayms.local  /e  /d  /A  /P
```

其中/e表示包含所有站点内的域控制器，/d表示信息中以distinguished name（DN）来识别服务器，/A表示同步此域控制器内的所有目录分区，/P表示同步方向是将此域控制器（dc2.sayms.local）的变动数据传送给其他域控制器。

完成同步工作后，可利用**Active Directory管理中心**来验证组织单位**业务部**内的用户账户王乔治已经被恢复，也可以通过以下命令来验证**王乔治**账户的属性版本号码确实被增加了100,000，如图11-3-17中的**版本**字段所示。

```
repadmin /showmeta CN=王乔治,OU=业务部,DC=sayms,DC=local
```

图 11-3-17

附注

如果是使用wbadmin程序，并且要针对SYSVOL文件夹执行**授权还原**的话，请在执行**非授权还原**时，增加**-authsysvol**参数，例如：

```
wbadmin  start  systemstaterecovery  -其他参数  -authsysvol
```

11.4 AD DS数据库的移动与整理

AD DS数据库与事务日志的存储位置默认是在*%systemroot%*\NTDS文件夹内，然而一段时间以后，如果硬盘存储空间不够或为了提高工作效率的话，有可能需要将AD DS数据库移

动到其他位置或重整。

11.4.1 可重新启动的AD DS（Restartable AD DS）

如果要进行AD DS数据库维护工作的话，例如移动AD DS数据库、数据库脱机整理等，可以选择重新启动计算机，然后进入**目录服务修复模式**内来执行这些维护工作。如果这台域控制器也同时提供其他网络服务的话，例如它同时也是DHCP服务器，则重新启动计算机将造成这些服务会暂时停止对客户端服务。

除了进入**目录服务修复模式**之外，Windows Server 2016域控制器还提供**可重新启动的AD DS**功能，此时只需要将AD DS服务停止，就可以执行AD DS数据库的维护工作，不需要重新启动计算机来进入**目录服务修复模式**，如此不但可让AD DS数据库的维护工作更容易、更快完成，并且其他服务也不会被中断。完成维护工作后再重新启动AD DS服务即可。

在AD DS服务停止的情况下，只要还有其他域控制器在线，则仍然可以在这台AD DS服务已经停止的域控制器上利用域用户账户来登录。

11.4.2 移动AD DS数据库文件

在此我们不采用进入**目录服务修复模式**的方式，而是利用将AD DS服务停止的方式来进行AD DS数据库文件的移动工作，此时必须至少是隶属于Administrators组的成员才有权限进行以下的工作。

我们要利用**Ntdsutil.exe**来移动AD DS数据库与事务日志，以下练习假设要将它们都移动到C:\NewNTDS文件夹。

附注

1. 不需要手动建立此文件夹，因为**Ntdsutil.exe**会自动建立。如果要事先建立此文件夹，请确认SYSTEM与Administrators对此文件夹拥有**完全控制**的权限。
2. 如果要更改SYSVOL文件夹的存储位置，建议方法为：删除AD DS、重新安装AD DS、在安装过程中指定新的存储位置。

STEP 1 打开Windows PowerShell窗口。

STEP 2 如图11-4-1所示执行以下命令来停止AD DS服务：

```
net stop ntds
```

接着输入**Y**后按Enter键。它也会将其他相关服务一起停止。

图 11-4-1

STEP 3 在**Windows PowerShell**提示符下执行以下命令（参考图11-4-2）：

```
ntdsutil
```

STEP 4 在**ntdsutil**：提示符下执行以下命令：

```
activate instance ntds
```

表示要将域控制器的AD DS数据库设置为使用中。

STEP 5 在**ntdsutil**：提示符下，执行以下命令：

```
files
```

STEP 6 在file maintenance：提示符下执行以下命令：

```
info
```

它可以查看AD DS数据库与事务日志当前的存储位置，由图11-4-2下方可知道它们目前都是位于C:\Windows\NTDS文件夹内。

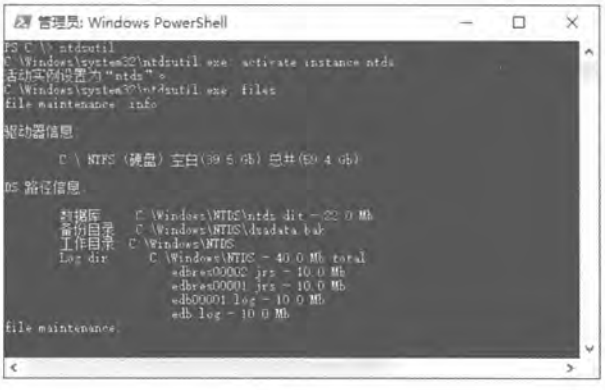

图 11-4-2

STEP 7 在**file maintenance**：提示符下，如图11-4-3所示执行以下命令，以便将数据库文件移动到C:\NewNTDS：

```
move db to C:\NewNTDS
```

图 11-4-3

STEP 8 在**file maintenance**：提示符下，如图11-4-4所示执行以下命令，以便将事务日志文件也移动到C:\NewNTDS：

```
move  logs  to  C:\NewNTDS
```

由图中下半部可知数据库与事务日志都已经正确地被移动到新位置C:\NewNTDS。

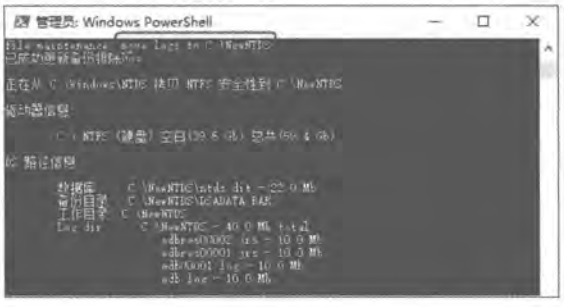

图 11-4-4

STEP 9 在**file maintenance**：提示符下，如图11-4-5所示执行以下命令，以便执行数据库的完整性检查：

```
Integrity
```

由图下方的文字Integrity check successful可知完整性检查成功。

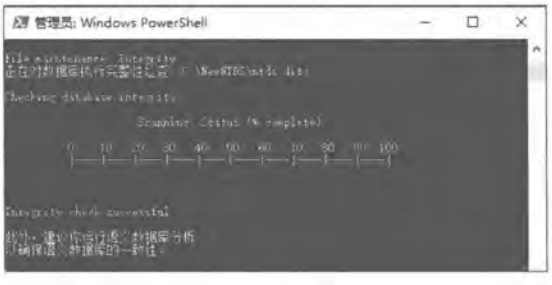

图 11-4-5

STEP 10 在 **file maintenance**：提示符下执行以下命令：

```
quit
```

STEP 11 如果完整性检查成功的话，可跳到STEP 20，否则请继续以下的步骤。

STEP 12 在**ntdsutil**：提示符下执行以下命令（参考图11-4-6）：

```
semantic database analysis
```

STEP 13 在**semantic checker**：提示符下执行以下命令，以便启用详细信息模式：

```
verbose on
```

STEP 14 在**semantic checker**：提示符下执行以下命令，以便执行语义数据库分析工作：

```
go fixup
```

图 11-4-6

STEP 15 在semantic checker：提示符下执行以下命令：

```
quit
```

STEP 16 如果语义数据库分析没有错误的话，可跳到STEP 20，否则继续以下的步骤。

STEP 17 在**ntdsutil**：提示符下执行以下命令（参考图11-4-7）：

```
files
```

STEP 18 在**file maintenance**：提示符下执行以下命令，以便修复数据库：

```
recover
```

图 11-4-7

STEP 19 在file maintenance：提示符下执行以下命令：

```
quit
```

STEP 20 在**ntdsutil**：提示符下执行以下命令：

```
quit
```

STEP 21 回到**Windows PowerShell提示符**下执行以下命令，以便重新启动AD DS服务：

```
net start ntds
```

11.4.3 重整AD DS数据库

AD DS数据库的重整操作（defragmentation），会将数据库内的数据排列整齐，让信息的读取速度更快，可以提升AD DS运行效率。AD DS数据库的重整分为：

- **在线重整**：每一台域控制器会每隔12小时自动执行所谓的**垃圾回收程序**（garbage collection process），它会重整AD DS数据库。**在线重整**并无法减少AD DS数据库文件（ntds.dit）的大小，而只是将数据有效地重新整理、排列。由于此时AD DS还在运行中，因此这个重整操作被称为**在线重整**。
  另外，我们曾经说过一个被删除的对象，并不会立刻被从AD DS数据库内删除，而是被移动到一个名称为**Deleted Objects**的容器内，这个对象在180天以后才会被自动清除，而这个清除操作也是由**垃圾回收程序**所负责。虽然对象已被清除，不过腾出的空间并不会还给操作系统，也就是数据库文件的大小并不会减少。当建立新对象时，该对象就会使用腾出的可用空间。
- **脱机重整**：脱机重整必须在AD DS服务停止或**目录服务修复模式**内手动进行，脱机重整会建立一个全新的、整齐的数据库文件，并会将已删除的对象所占用空间还给操作系统，因此可以腾出可用的硬盘空间给操作系统或其他应用程序来使用。

附注

在一个包含多个域的林中，如果有一台域控制器曾经兼具**全局编录服务器**角色，但现在已经不再是**全局编录服务器**的话，则这台域控制器经过**脱机重整**后，新的AD DS数据库文件会比原来的文件小很多，也就是说可以腾出很多的硬盘空间给操作系统。

以下将介绍如何来执行**脱机重整**的步骤。请确认当前存储AD DS数据库的磁盘内有足够可用空间来存储**脱机重整**所需的缓存文件，至少保留数据库文件大小的15%可用空间。还有重整后的新文件的存储位置，也需要保留至少与原数据库文件大小的可用空间。以下假设原数据库文件是位于C:\Windows\NTDS文件夹，而我们要将重整后的新文件放到C:\NTDSTemp文件夹。

附注

1. 不需要手动建立C:\NTDSTemp文件夹，**Ntdsutil.exe**会自动建立。
2. 如果要将重整后的新文件存储到网络共享文件夹，需要开放Administrators组有权利来访问此共享文件夹，并先利用网络驱动器来连接到此共享文件夹。

STEP 1 开启Windows PowerShell窗口。

STEP 2 执行**net stop ntds**命令、输入**Y**后按Enter键来停止AD DS服务（它也会将其他相关服务停止）。

STEP 3 在**Windows PowerShell提示符**下执行以下命令（参考图11-4-8）：

```
ntdsutil
```

STEP 4 在**ntdsutil**：提示符下执行以下命令：

```
activate instance ntds
```

表示要将域控制器的AD DS数据库设置为使用中。

STEP 5 在**ntdsutil**：提示符下执行以下命令：

```
files
```

STEP 6 在file maintenance：提示符下执行以下命令：

```
info
```

它可以查看AD DS数据库与事务日志当前的存储位置，由图11-4-8下方可知道它们当前都是位于C:\Windows\NTDS文件夹内。

图 11-4-8

STEP 7 在**file maintenance**：提示符下，如图11-4-9所示执行以下命令，以便重整数据库文件，并将所产生的新数据库文件放到E:\NTDSTTemp文件夹内（新文件的名称还是**ntds.dit**）：

```
compact to C:\NTDSTemp
```

附注

1. 如果路径中有空格的话，请在路径前后加上双引号，例如“C:\New Folder”。
2. 如果要将新文件放到网络驱动器的话，例如K:，利用**compact to K:**命令：

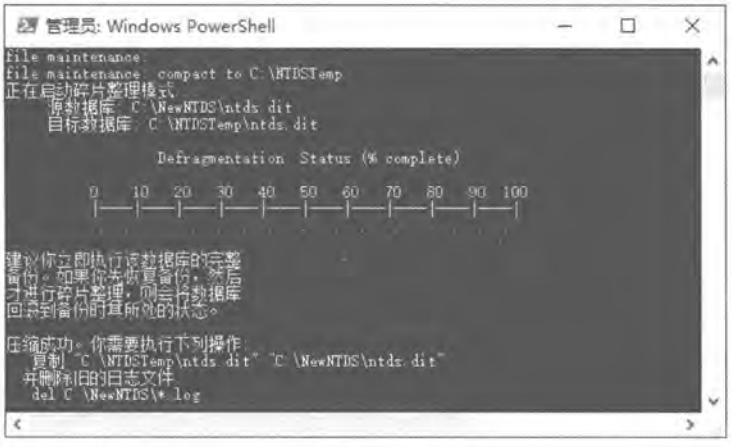

图 11-4-9

STEP 8 暂时不要离开**ntdsutil**程序、打开**文件资源管理器**后执行以下几个步骤：

- 将原数据库文件C:\Windows\NTDS\ntds.dit备份起来，以备不时之需。
- 将重整后的新数据库文件C:\NTDSTemp\ntds.dit复制到C:\Windows\NTDS文件夹，并覆盖原数据库文件。
- 将原事务日志C:\Windows\NTDS*.log删除。

STEP 9 继续在**ntdsutil**程序的**file maintenance**：提示符下，如图11-4-10所示执行以下命令，以便执行数据库的完整性检查：

```
integrity
```

由图下方所显示的Integrity check successful可知完整性检查成功。

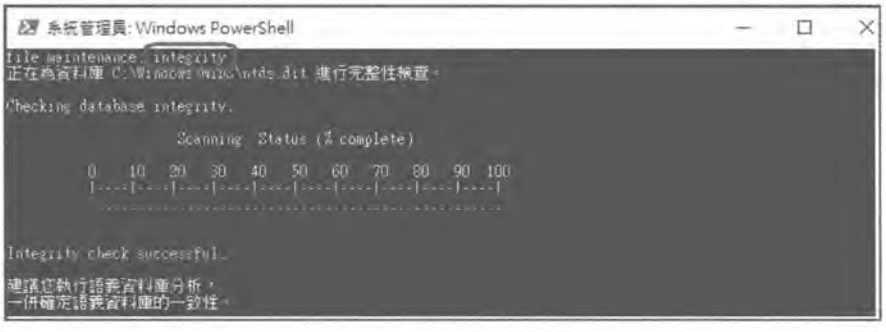

图 11-4-10

STEP 10 在file maintenance: 提示符下执行以下命令：

```
quit
```

STEP 11 在**ntdsutil**: 提示符下执行以下命令：

```
quit
```

STEP 12 回到**Windows PowerShell提示符**下执行以下命令，以便重新启动AD DS服务：

```
net  start  ntds
```

如果无法启动AD DS服务的话，请试着采用以下方法来解决问题：

- 利用**事件查看器**来查看**目录服务**日志文件，如果有事件标识符为1046或1168的事件日志的话，请利用备份来还原AD DS。
- 再执行数据库完整性检查（integrity），如果检查失败的话，请将之前备份的数据库文件ntds.dit复制回原数据库存储位置，然后重复数据库重整操作，如果这个操作中的数据库完整性检查还是失败的话，请执行语义数据库分析操作（semantic database analysis），如果失败的话，请执行修复数据库的操作（recover）。

11.5 重置“目录服务修复模式”的系统管理员密码

如果**目录服务修复模式**的系统管理员密码忘了，以至于无法进入**目录服务修复模式**时该怎么办呢？此时可以在普通模式下，利用**ntdsutil**程序来重置**目录服务修复模式**的系统管理员密码，其步骤如下所示：

STEP 1 请到域内的任何一台成员计算机上利用域系统管理员账户登录。

STEP 2 打开**Windows PowerShell**窗口，执行以下命令（完整的操作界面请见图11-5-1）：

```
ntdsutil
```

STEP 3 在**ntdsutil**: 提示符下执行以下命令：

```
set  DSRM  password
```

STEP 4 在**重置DSRM管理员密码**: 提示符下执行以下命令：

```
reset  password on server  dc2.sayms.local
```

以上命令假设要重置域控制器dc2.sayms.local的**目录服务修复模式**的系统管理员密码。

注意

要被重置密码的域控制器，其AD DS服务必须启动中。

STEP 5 输入与确认新密码。

STEP 6 连续输入**quit**命令以便离开**ntdsutil**程序，图11-5-1为以上几个主要步骤的操作界面。

图11-5-1

11.6 更改可重新启动的AD DS的登录设置

在AD DS服务停止的情况下，只要还有其他域控制器在线，则仍然可以在这台AD DS服务已经停止的域控制器上利用域用户账户来登录。如果没有其他域控制器在在线的话，可能会产生问题，例如：

- 在域控制器上利用域系统管理员的身份登录。
- 将AD DS服务停止。
- 一段时间未操作此计算机，因而屏幕保护程序被启动，并且需输入密码才能解锁。

此时如果要继续使用这台域控制器的话，就需要输入域系统管理员账户来解开屏幕保护的锁定，不过因为AD DS服务已经停止，而且网络上也没有其他域控制器在线，因此无法验证域系统管理员身份，也就无法解开屏幕保护的锁定。如果事先更改默认登录设置的话，就可以在这个时候利用**目录服务修复模式**（DSRM）的系统管理员（**DSRM管理员**）账户来解除锁定。更改登录设置的方法为：执行注册表编辑器REGEDIT.EXE，然后修改或新建以下的键值：

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\DSRMAdminLogonBehavi
or
```

DSRMAdminLogonBehavior的数据类型为REG_DWORD，它用来决定在这台域控制器以正常模式启动、但AD DS服务停止的情况下，能否利用**DSRM管理员**登录：

- **0**：不能登录。DSRM管理员只能登录到目录服务修复模式（默认值）。
- **1**：**DSRM管理员**可以在AD DS服务停止的情况下登录，不过**DSRM管理员**不受密码策略设置的约束。在域中只有一台域控制器的情况之下，或某台域控制器是在一个隔离的网络等状况之下，此时或许希望能够将此参数改为这个设置值。

2：在任何情况之下，也就是不论AD DS服务是否启动、不论是否在**目录服务修复模式**下，都可以使用**DSRM系统管理员**来登录。不建议采用此方式，因为**DSRM管理员**不受密码策略设置的约束。

11.7 Active Directory回收站

在旧版Windows系统中，系统管理员容易不小心将AD DS对象删除，因而造成对象恢复的问题，尤其是误删除组织单位的话，其中所有对象都会丢失。虽然系统管理员可以进入**目录服务修复模式**来恢复被误删的对象，不过很耗费时间，并且在进入**目录服务修复模式**这一段期间内，域控制器会暂时停止对客户端提供服务。

较新版本的Windows Server系统中针对此事进行了改良，例如可以在新建用户与组账户等对象时，勾选**防止意外删除**（如图11-7-1所示）。如果是新增组织单位的话，系统甚至默认就会自动勾选**防止意外删除**。除此之外，Windows Server 2016也支持**Active Directory回收站**（Active Directory Recycle Bin），它支持不需要进入**目录服务修复模式**，就可以快速恢复被删除的对象。

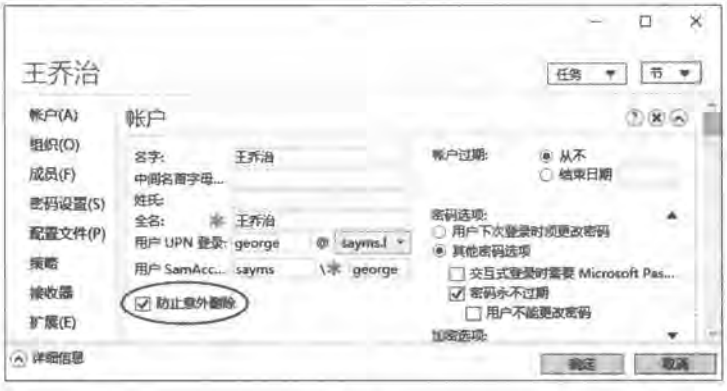

图 11-7-1

附注

一旦启用**Active Directory回收站**后，就无法再禁用。林与域功能级别需要为Windows Server 2008 R2（含）以上的级别，才具备**Active Directory回收站**功能。

启用**Active Directory回收站**与恢复误删对象的演练步骤如下所示。

STEP 1 打开**Active Directory管理中心**➲如图11-7-2所示单击左方域名sayms➲单击右侧的**启用回收站**。

图 11-7-2

STEP 2 如图11-7-3所示单击确定按钮。

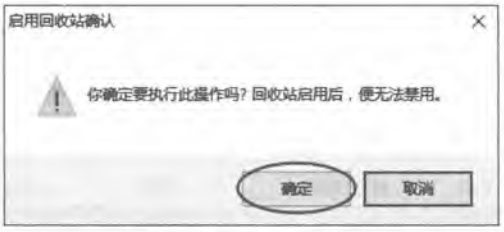

图 11-7-3

STEP 3 在图11-7-4单击确定按钮后按F5键刷新界面。

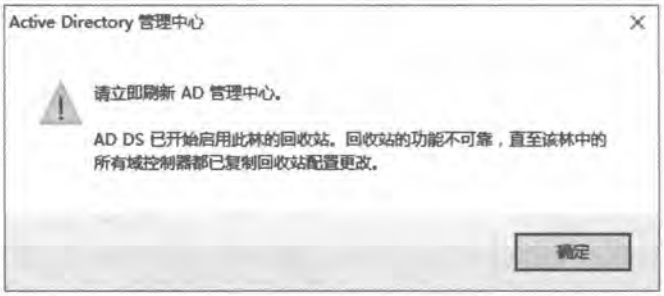

图 11-7-4

附注

如果域内有多台域控制器或有多个域的话，则需要等设置值被复制到所有的域控制器后，**Active Directory回收站**的功能才会完全正常。

STEP 4 试着将某个组织单位（假设是**业务部**）删除，但是要先将防止删除的选项删除：如图11-7-5所示点选**业务部**、单击右侧的**属性**。

图 11-7-5

STEP 5 取消勾选图11-7-6中选项后单击确定按钮➲选中组织单位**业务部**并右击➲**删除**➲单击两次是（Y）按钮。

图 11-7-6

STEP 6 接下来要通过回收站来恢复组织单位**业务部**：双击如图11-7-7所示的**Deleted Objects**容器。

图 11-7-7

STEP 7 在图11-7-8中选择要恢复的组织单位**业务部**后，单击右侧的**还原**来将其还原到原始位置。

附注

如果单击**还原到...**的话，则可以选择将其还原到其他位置。

图 11-7-8

STEP 8 组织单位**业务部**还原完成后，接着继续在图11-7-9中选择原本位于组织单位**业务部**内的用户账户后单击**还原**。

图 11-7-9

STEP 9 利用**Active Directory管理中心**来检查组织单位**业务部**与用户账户**王乔治**等账户是否已被还原，而且这些被还原的账户也会被复制到其他域控制器。