

# 3

## 第3章 域用户与组账户的管理

域系统管理员需要为每一个域用户分别创建一个用户账户，让他们可以利用这个账户登录域、访问网络上的资源。域系统管理员同时也需要了解如何有效利用组，以便高效地管理资源的访问。

- 管理域用户账户
- 一次同时新建多个用户账户
- 域组账户
- 组的使用原则



## 3.1 管理域用户账户

域系统管理员可以利用**Active Directory管理中心**或**Active Directory用户和计算机控制台**来建立与管理域用户账户。当用户利用域用户账户登录域后，便可以直接连接域内的所有成员计算机、访问有权限访问的资源。换句话说，域用户在一台域成员计算机上登录成功后，当他要连接域内的其他成员计算机时，并不需要再手动输入用户名与密码进行登录，这个功能被称为**单点登录**。

### 附注

本地用户账户并不具备**单点登录**的功能，也就是说利用本地用户账户登录后，当要再连接其他计算机时，需要再手动输入用户名与密码进行登录。

在服务器还没有升级成为域控制器之前，原本位于其本地安全数据库内的本地用户账户，会在升级成域控制器后被异动到AD DS数据库内，并且是被存储到Users容器内的，可以通过**Active Directory管理中心**来查看，如图3-1-1中所示（可先单击上方的**树视图**图标），同时这台服务器的计算机账户会被存储到图中的组织单位Domain Controllers内。其他加入域的计算机账户默认会被存储到图中的Computers容器内。



图 3-1-1

也可以通过**Active Directory用户和计算机**来查看，如图3-1-2所示。



图 3-1-2

只有在建立域内的第1台域控制器时，该服务器原来的本地账户才会被转移到AD DS数据库，其他域控制器原有的本地账户并不会被转移到AD DS数据库，而是被删除。

### 3.1.1 创建组织单位与域用户账户

可以将用户账户创建到任何一个容器或组织单位内。以下假设要先建立名称为**业务部**的组织单位，然后在其内创建域用户账户mary。

创建组织单位**业务部**的方法为：【单击左下角开始图标→Windows 管理工具→Active Directory管理中心（或Active Directory用户和计算机）→选中域名并右击→新建→组织单位→如图3-1-3所示输入组织单位名称**业务部**→单击**确定**按钮】。

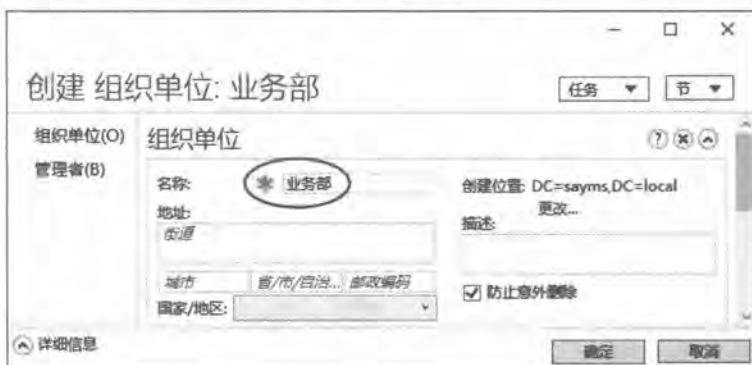


图 3-1-3

#### 注意

图中默认已经勾选**防止意外删除**，因此无法直接将此组织单位删除，除非取消勾选此选项。如果是使用Active Directory用户和计算机的话：【选择查看菜单→高级功能→对着此组织单位并右击→属性→如图3-1-4所示取消勾选对象选项卡之下的**防止对象被意外删除**】。



图 3-1-4

在组织单位**业务部**内建立用户账户mary的方法为：**【选中组织单位业务部并右击新建 ➤ 用户】**。注意域用户的密码默认需至少7个字符，且不能包含用户账户名称（指用户SamAccountName）或全名（后述），还有至少要包含A~Z、a~z、0~9、非字母数字（例如!、\$、#、%）等4组字符中的3组，例如123saymsSAYMS是有效的密码，而1234567是无效的密码。如果要更改此默认值的话，请参考第4章的说明。

### 3.1.2 用户登录账户

域用户可以到域成员计算机上（域控制器除外）利用两种账户名称来登录域，它们分别是图3-1-5中的**用户UPN登录**与**用户SamAccountName登录**。普通的域用户默认是无法在域控制器上登录的（可参考第4章进行设置）。



图 3-1-5

➤ **用户UPN登录**：UPN（User Principal Name）的格式与电子邮件账户相同，如前面图3-1-5中的mary@sayms.local，这个名称只能在隶属于域的计算机上登录域时使用（如图3-1-6所示）。整个林内，这个名称必须是唯一的。



图 3-1-6

UPN并不会随着账户被移动到其他域而改变，举例来说，用户mary的用户账户位于域sayms.local内，其默认的UPN为mary@sayms.local，之后即使此账户被移动到林中的另一个域内，例如域sayiis.local，其UPN仍然是mary@sayms.local，并没有被改变，因此mary仍然可以继续使用原来的UPN登录。

- ✎ **用户 SamAccountName 登录：**如前面图3-1-5中的sayms\mary，这是旧格式的登录账户。Windows 2000之前版本的旧客户端需要使用这种格式的名称来登录域。在隶属于域的Windows 2000（含）之后的计算机上也可以采用这种名称来登录，如图3-1-7所示。同一个域内，这个名称必须是唯一的。



图 3-1-7

附注

在Active Directory用户和计算机控制台内，上述用户UPN登录与用户SamAccountName登录分别被称为用户登录名与用户登录名（Windows 2000以前版本）。

### 3.1.3 创建UPN后缀

用户账户的UPN后缀默认是账户所在域的域名，例如用户账户是被建立在域sayms.local内，



则其UPN后缀为sayms.local。在某些情况之下，用户可能希望能够改用其他替代后缀，例如：

- 因为UPN的格式与电子邮件账户相同，因此用户可能希望其UPN可以与电子邮件账户相同，以便让其不论是登录域或收发电子邮件，都可使用同一个名称。
- 如果域树状目录内有多层的子域，则域名会太长，例如sales.tw.sayms.local，如此UPN后缀也会太长，这将造成用户在登录时的不便。

可以通过添加UPN后缀的方式让用户拥有替代后缀，如下所示：

**STEP 1** 单击左下角开始图标 Windows 管理工具 Active Directory域和信任关系 如图3-1-8所示单击Active Directory域和信任后单击上方的属性图标。



图 3-1-8

**STEP 2** 在图3-1-9中输入替代的UPN后缀后单击添加按钮并单击确定按钮。后缀不一定需要DNS格式，例如可以是sayiis.local，也可以是sayiis。

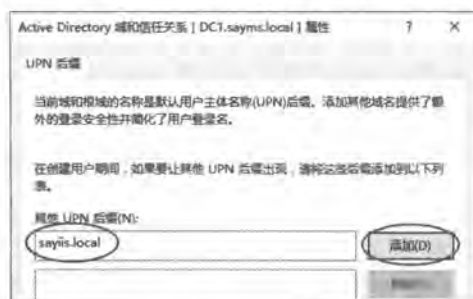


图 3-1-9

完成后，就可以通过Active Directory管理中心（或Active Directory用户和计算机）控制台来更改用户的UPN后缀，如图3-1-10所示。

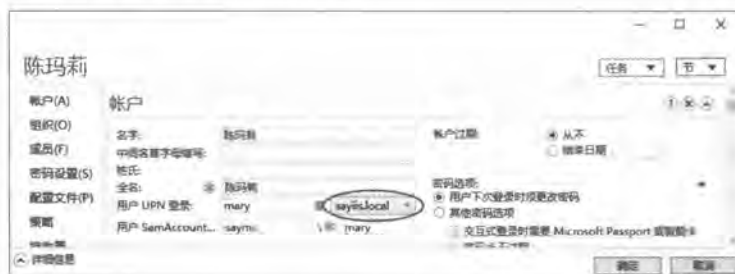


图 3-1-10



### 3.1.4 账户的常规管理工作

本节将介绍用户账户的常规管理工作，例如重置密码、禁用（启用）账户、移动账户、删除账户、更改登录名称与解除锁定等。可以如图3-1-11所示单击待管理的用户账户（例如图中的陈玛莉），然后通过右侧的选项来设置。



图 3-1-11

- **重置密码：**当用户忘记密码或密码使用期限到期时，系统管理员可以利用此处为用户设置一个新的密码。
- **禁用（或启用）：**如果某位员工因故在一段时间内无法来上班的话，可以先将该用户的账户禁用，等该员工回来上班后，再将其重新启用即可。如果用户账户已被禁用，则该用户账户图标上会有一个向下的箭头符号（例如图3-1-11中的用户账号李小洋）。
- **移动：**可以将账户移动到同一个域内的其他组织单位或容器。
- **重命名：**重命名以后（可通过【选中用户账户并右击➤属性】的方法），该用户原来所拥有的权限与组关系都不会受到影响。例如当某员工离职时，可以暂时先将其用户账户禁用，等到新员工来接替他的工作时，再将此账户名称改为新员工的名、重新设置密码、更改账户登录名称、修改其他相关个人信息，然后重新启用此账户。

完成用户账户新建之后，系统会为其建立一个唯一的安全标识符（security identifier, SID），而系统是利用这个SID来代表该用户，同时权限设置等都是通过SID来记录的，并不是通过用户名，例如某个文件的权限列表内，它会记录着哪些SID具备着哪些权限，而不是哪些用户名拥有哪些权限。

由于用户账户名或登录名更改后，其SID并没有被改变，因此用户的权限与组关系都不变。

可以通过双击用户账户或右侧的**属性**来更改用户账户名与登录名等相关设置。

- **删除账户：**如果这个账户以后再也用不到的话，就可以将此账户删除。将账户删除后，即使再新建一个相同名称的用户账户，这个新账户并不会继承原账户的权限与组关系，因为系统会给予这个新账户一个新的SID，而系统是利用SID来记录用户的权限与组关系，不是利用账户名称。因此对系统来说，这是两个不同的账户，当然





就不会继承原账户的权限与组关系。

- **解锁账户**：我们可以通过**账户策略**来设置用户输入密码失败多次后，就将此账户锁定，而系统管理员可以利用以下方法来解锁：**【双击该用户账户 单击图3-1-12中的解锁账户（账户被锁定后才会有此选项）】**。



图 3-1-12

### 3.1.5 域用户账户的属性设置

每一个域用户账户内都有一些相关的属性信息，例如地址、电话与电子邮件地址等，域用户可以通过这些属性信息来查找AD DS数据库内的用户，例如通过电话号码来查找用户，因此为了更容易找到所需要的用户账户，这些属性信息应该越完整越好。我们将通过**Active Directory管理中心**来介绍用户账户的部分属性，请先双击要设置的用户账户。

#### 1. 组织信息的设置

组织信息就是指显示名称、职务、部门、地址、电话、电子邮件、主页等，如图3-1-13中**组织**区域所示，这部分的内容都很简单，请自行浏览这些字段。



图 3-1-13



## 2. 账户过期的设置

我们可以如图3-1-14所示通过**账户**区域内的**账户过期**来设置账户的有效期限，默认为从不过期。如果要设置过期时间的话，选择**结束日期**，然后输入格式为yyyy/m/d的过期日期。



图 3-1-14

## 3. 登录时间的设置

**登录时间**用来指定用户可以登录到域的时段，默认是任何时段都可以登录域。如果要更改设置的话，请单击图3-1-15中的**登录小时...**，然后通过前景图来设置。图中横轴每一方块代表一个小时，纵轴每一方块代表一天，填满方块与空白方块分别代表允许与不允许登录的时段，默认是开放所有的时段。选好时段后选择**允许登录**或**拒绝登录**来允许或拒绝用户在上述时段登录。

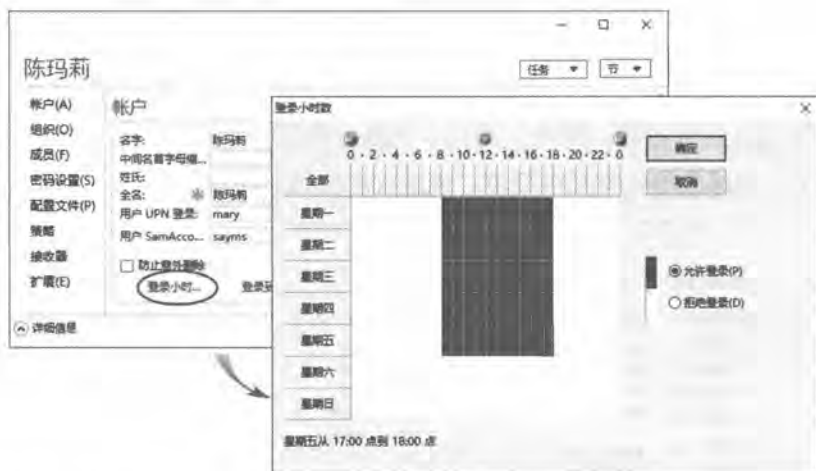


图 3-1-15

## 4. 限制用户只能够通过某些计算机登录

普通的域用户默认可以利用任何一台域成员计算机（域控制器除外）来登录域，不过我们也可以通过以下方法来限制用户只可以利用某些特定计算机来登录域：【单击图3-1-16中



的**登录到...** 在前景图中选择**下列计算机** 输入计算机名称后单击**添加**按钮】，计算机名称可为NetBIOS名称（例如win10pc1）或DNS名称（例如win10pc1.sayms.local）。

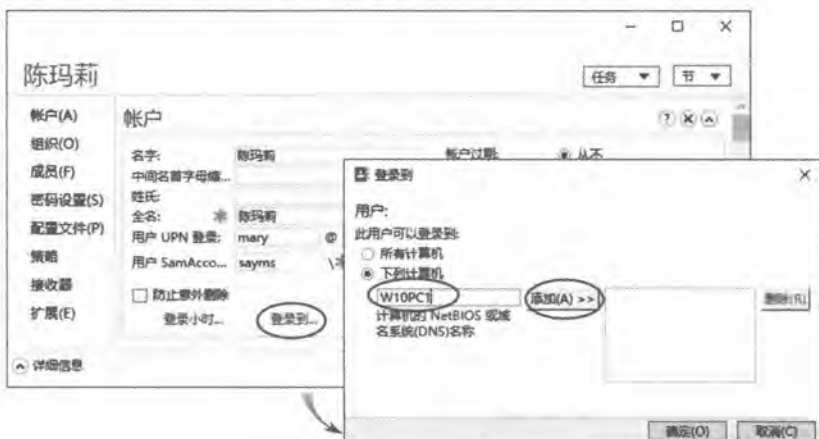


图 3-1-16

### 3.1.6 搜索用户账户

AD DS将用户账户、组账户、计算机账户、打印机、共享文件夹等对象存储在AD DS数据库内，域系统管理员可以方便地在AD DS数据库中搜索与管理所需的用户账户。

如果要在某个组织单位（或容器）内来搜索用户账户的话，只要如图3-1-17所示【单击组织单位 在中间窗口上方输入要搜索的用户账户名称即可】，搜索到的用户账户会被显示在中间窗口的下方。如果要搜索的对象要包含此组织单位之下的组织单位的话，请单击右方任务窗口中的**在该节点下搜索**。



图 3-1-17

若要搜索整个域的话，请如图3-1-18所示【点选左侧的**全局搜索** 在中间窗口上方输入要搜索的用户账户名称 单击**搜索**按钮】。



图 3-1-18

也可以通过全局编录服务器来搜索位于其他域内的对象，不过需先将搜索范围更改为全局编录搜索，如图3-1-19所示。

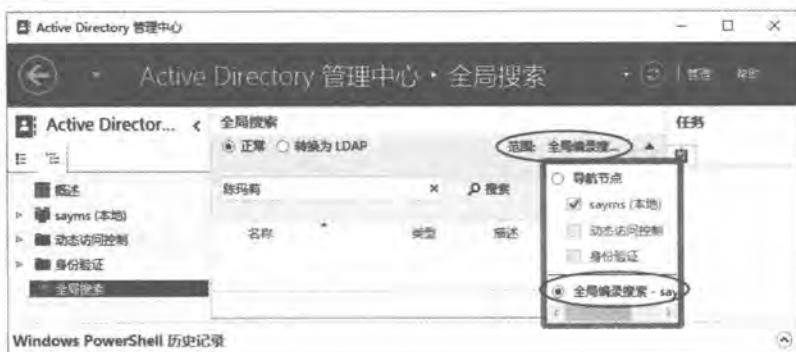


图 3-1-19

也可以通过图3-1-20中的概述界面来执行全局搜索工作。

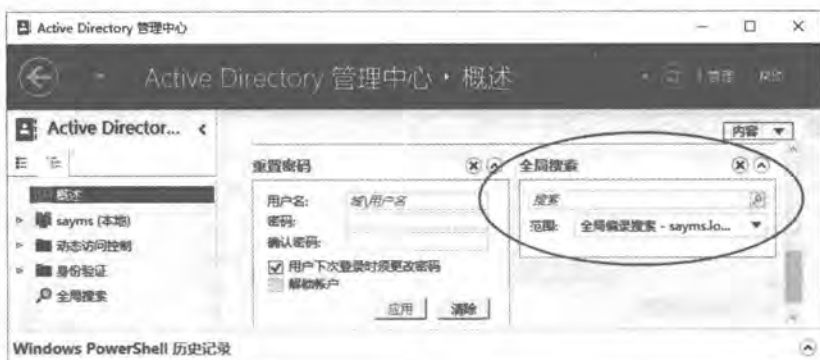


图 3-1-20

还可以进一步通过指定的条件来搜索用户账户，例如要搜索业务部内电话号码是空白的所有用户账户的话，则请如图3-1-21所示【单击组织单位业务部中的添加标准（如果未出现添加标准选项的话，先单击右上方的箭头符号~）勾选类型勾选添加按钮如图3-1-22所示在类型处选择等于，然后输入用户】。



图 3-1-21



图 3-1-22

接着如图3-1-23所示【单击添加标准按钮勾选电话号码单击添加按钮在图3-1-24中的电话号码旁选择为空】，系统便会显示业务部内电话号码属性值是空白的的所有用户账户。



图 3-1-23

可以将所定义的查询（搜索）条件保存起来，也就是单击图3-1-25中的保存图标，然后为此查询命名，之后可以如图3-1-26所示通过此查询内所定义的条件来搜索。



图 3-1-24



图 3-1-25



图 3-1-26

如果要在没有安装Active Directory管理中心的成员服务器或其他成员计算机上查找AD DS对象的话，以Windows 10计算机为例：可以通过【打开文件资源管理器（可按 $\text{Win}+\text{X}$ 键 $\Rightarrow$ 文件资源管理器） $\Rightarrow$ 单击左下方的网络 $\Rightarrow$ 如图3-1-27所示单击上方网络下的搜索Active Directory】的方法（可能需要先启用网络发现）。



图 3-1-27

接着如图3-1-28所示在查找处选择用户、联系人及组、在范围处选择整个目录（也就是全局编录）或域名、在名称处输入要查找的名称后单击开始查找按钮，然后就可以从最下面的搜索结果来查看与管理所查找到的账户。

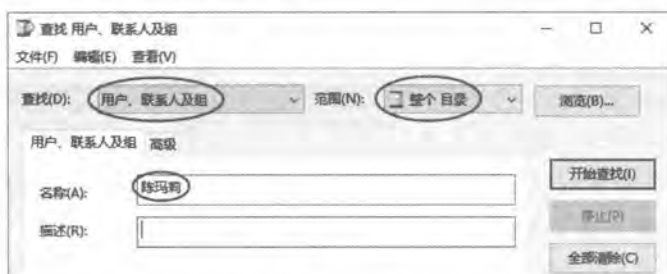


图 3-1-28

若要进一步通过特定条件来查找用户账户的话，例如如果要查找业务部内电话号码为空白的所有用户账户的话：【请如图3-1-29所示单击高级选项卡通过字段来选择用户对象与电话号码属性条件选择不存在单击添加按钮单击开始查找按钮】，可以同时设置多个查找条件。



图 3-1-29



### 3.1.7 域控制器之间数据的复制

如果域内有多台域控制器的话，则当更改AD DS数据库内的数据时，例如利用**Active Directory管理中心**（或**Active Directory用户和计算机**）来添加、删除、修改用户账户或其他对象，则这些变更数据会先被存储到所连接的域控制器，之后再自动被复制到其他域控制器。

可如图3-1-30所示【选中域名并右击**更改域控制器**】查看当前所连接的域控制器，例如图中的DC1.sayms.local，而此域控制器何时会将其最新更新信息复制给其他域控制器呢？可分为以下两种情况：



图 3-1-30

- ✎ **自动复制**：如果是同一个站点内的域控制器，则默认是15秒钟后会自动复制，因此其他域控制器可能等15秒或更久时间就会收到这些最新的信息；如果是位于不同站点的域控制器，则需要根据所设置的复制计划来确定（详见第9章）。
- ✎ **手动复制**：有时候可能需要手动复制，例如网络故障造成复制失败，这时不希望等到下一次的自动复制，而是能够立即复制。以下假设要从域控制器DC1复制到DC2。请到任意一台域控制器上【单击左下角开始图标**Windows 管理工具** **Active Directory站点和服务** **Sites** **Default-First-Site-Name** **Servers** 展开目标域控制器（DC2） **如图3-1-31所示单击NTDS Settings** **选中右侧源域控制器（DC1）并右击立即复制**】。

#### 附注

与**组策略**有关的设置会先被存储到扮演**PDC模拟器操作主机**角色的域控制器内，然后由**PDC模拟器操作主机**复制给其他的域控制器（见第10章）。





图 3-1-31

## 3.2 一次同时新建多个用户账户

如果是利用Active Directory管理中心（或Active Directory用户和计算机）的图形界面来新建大量用户账户的话，将花费很多时间来重复执行相同的创建账户操作。此时可以利用系统内置的工具程序csvde.exe、ldifde.exe或dsadd.exe等，以节省创建用户账户的时间。

- ✎ **csvde.exe**: 可以利用它来新建用户账户（或其他类型的对象），但不能修改或删除用户账户。请事先将用户账户数据输入到纯文本文件（text file），然后利用csvde.exe将文件内的这些用户账户一次同时导入到AD DS数据库。
- ✎ **ldifde.exe**: 可以利用它来新建、删除、修改用户账户（或其他类型的对象）。请事先将用户账户数据输入到纯文本文件内，然后利用ldifde.exe将文件内的这些用户账户一次同时导入到AD DS数据库。
- ✎ **dsadd.exe**、**dsmod.exe**与**dsrm.exe**: dsadd.exe用来新建用户账户（或其他类型的对象），dsmod.exe用来修改用户账户，dsrm.exe用来删除用户账户。这里需要建立批处理文件，然后利用这3个程序将要新建、修改或删除的用户账户输入到此批处理文件。

以csvde.exe与ldifde.exe这两个程序来说，请先利用可以编辑纯文本文件的程序（例如记事本）来将用户账户数据输入到文件内：

- ✎ 需要指明用户账户的存储路径（distinguished name, DN）
- ✎ 需要包含对象的类型，例如user
- ✎ 需要包含“用户SamAccountName登录”账户
- ✎ 应该要包含“用户UPN登录”账户
- ✎ 可以包含用户的其他信息，例如电话号码、地址等
- ✎ 无法设置用户的密码
- ✎ 由于所建立的用户账户都没有密码，因此最好将用户账户禁用

### 3.2.1 利用csvde.exe来新建用户账户

我们将利用**记事本**（notepad）来说明如何建立供csvde.exe使用的文件，此文件的内容如图3-2-1所示。

图中第2行（含）以后都是要建立的每一个用户账户的属性数据，各属性数据之间利用逗号（，）隔开。第1行是用来定义第2行（含）以后相对应的每一个属性。例如第1行的第1个字段为DN（Distinguished Name），表示第2行开始每一行的第1个字段代表新对象的存储路径；又如第1行的第2个字段为objectClass，表示第2行开始每一行的第2个字段代表新对象的对象类型。

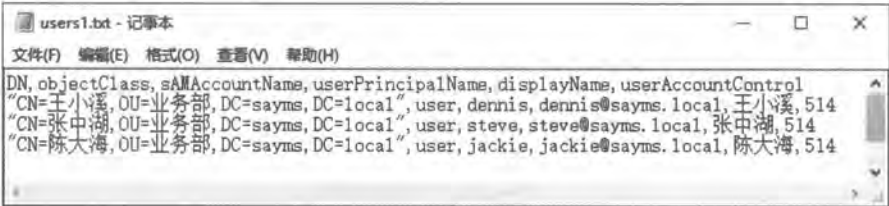


图 3-2-1

下面利用图3-2-1中的第2行数据进行说明，如表3-2-1所示。

表3-2-1

属性	值与说明
DN（distinguished name）	CN=王小溪, OU=业务部, DC=sayms, DC=local: 对象的存储路径
objectClass	user: 对象类型
sAMAccountName	dennis: 用户SamAccountName登录名
userPrincipalName	dennis@sayms.local: 用户UPN登录名
displayName	王小溪: 显示名称
userAccountControl	514: 表示禁用此账户（512表示启用）

文件建好后，打开**Windows PowerShell**，然后执行以下命令（参考图3-2-2），假设文件名为users1.txt，并且文件是位于C:\test文件夹内：

```
csvde -i -f c:\test\users1.txt
```

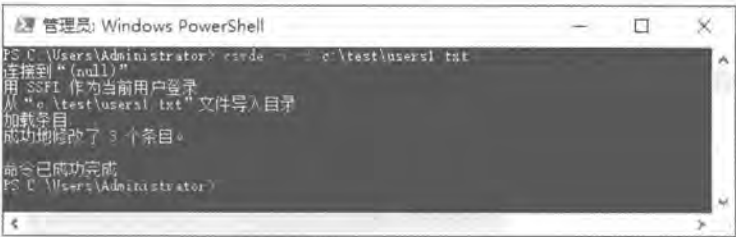


图 3-2-2



图3-2-3为执行后所建立的新账户，图中向下箭头符号表示账户被禁用。



图 3-2-3

### 3.2.2 利用ldifde.exe来新建、修改与删除用户账户

以下利用记事本来说明如何建立供ldifde.exe使用的文件，其内容类似于图3-2-4。



图 3-2-4

请参考图3-2-4来建立文件，如果此文件最后还要增加其他账户的话，请在减号之后至少空一行后再输入数据。注意保存时需如图3-2-5所示在**编码**处选择**Unicode**，否则文件内的中文字符在导入到AD DS数据库时会有问题。

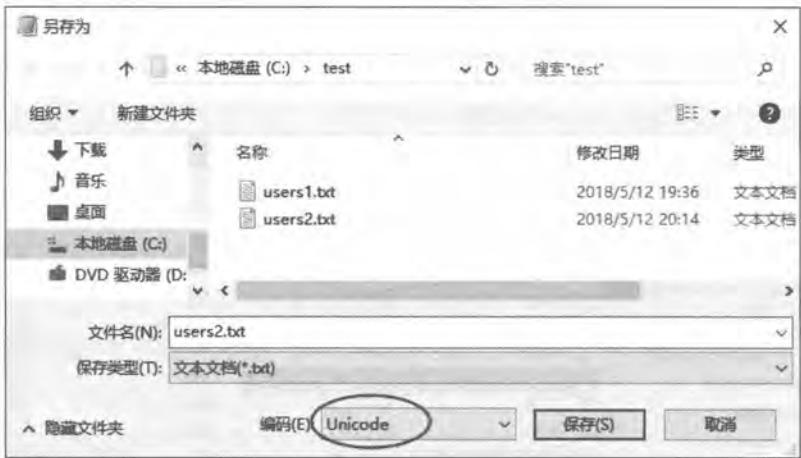


图 3-2-5

完成后请打开Windows PowerShell，然后执行以下命令（参考图3-2-6），假设文件名为users2.txt，并且文件是位于C:\test文件夹内：

```
ldifde -i-f c:\test\users2.txt
```



图 3-2-6

如果要将数据导入到指定的域控制器的话，请加入-s参数，例如（此范例假设是要导入到域控制器dc1.sayms.local）：

```
ldifde -s dc1.sayms.local -i-f c:\test\users2.txt
```

附注

csvde与ldifde命令的详细语法可利用csvde /?与ldifde /?来查看。

### 3.2.3 利用dsadd.exe等程序添加、修改与删除用户账户

以下利用记事本来说明如何建立批处理文件（batch file），然后将dsadd、dsmod与dsrm命令输入到此文件内，并利用它们来添加、修改与删除用户账户。此文件内容类似图3-2-7，图中针对这3个命令各给出一个示例。

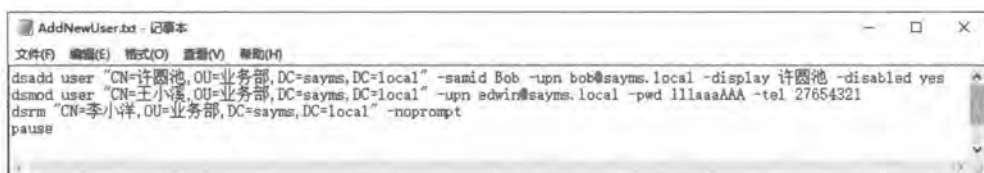


图 3-2-7

- 第1行dsadd命令：它用来新建一个位于CN=许圆池,OU=业务部,DC=sayms,DC=local的用户账户，其中的-samid Bob用来将其用户SamAccountName登录名设置为Bob、-upnbob@sayms.local用来将其用户UPN登录名设置为bob@sayms.local、-display 许圆池用来将其显示名设置为许圆池、-disabled yes表示禁用此账户。
- 第2行dsmod命令：用来修改位于CN=王小溪,OU=业务部,DC=sayms,DC=local的用户账户，其中-upnedwin@sayms.local用来将其用户UPN登录名更改为edwin@sayms.local、-pwd 111aaaAA用来将其密码更改为111aaaAA、-tel 27654321用来将其电话号码更改为27654321。
- 第3行dsrm命令：用来删除位于CN=李小平,OU=业务部,DC=sayms,DC=local的用户账户，其中的-noprompt表示不显示删除确认的界面。
- 最后一行的pause命令是为了让界面暂停，以便于查看命令执行的结果。

请参考图3-2-7来建立文件，注意保存时因为记事本默认会自动附加.txt的扩展名（系统默认会隐藏扩展名），然而我们必须将其存储成扩展名是.bat或.cmd的文件，因此保存时请如图3-2-8所示在文件名前后附加双引号，例如“AddNewUser.bat”，否则其扩展名将是.txt。



图 3-2-8

完成后可通过直接在文件资源管理器内双击此批处理文件的方式来执行它，此时系统会依序执行此文件内的命令，如图3-2-9所示。

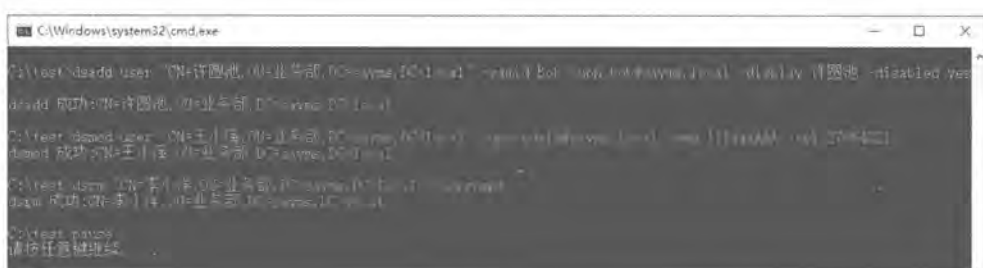


图 3-2-9

### 附注

Dsadd.exe、dsmod.exe与dsrm.exe等3个程序还有许多参数可以使用，其详细语法请利用 dsadd /?、dsmod /?与dsrm /?来查看。

## 3.3 域组账户

如果能善于利用组（group）来管理用户账户，则必定能够减轻许多网络管理负担。例如当针对业务部组设置权限后，此组内的所有用户都会自动拥有此权限，因此就不需要单独针对每一个用户进行配置了。

### 附注

组账户也都有唯一的安全标识符（security identifier，SID）。

### 3.3.1 域内的组类型

AD DS的域组分为以下两种类型，并且它们之间可以相互转换：

- **安全组（security group）**：它可以被用来分配权限，例如可以指定安全组对文件具备读取的权限。它也可以用在与安全无关的工作上，例如可以给安全组发送电子邮件。
- **发布组（distribution group）**：它被用在与安全（权限设置等）无关的工作上，例如可以给发布组发送电子邮件，但是无法为发布组分配权限。

### 3.3.2 组的作用域

从组的使用范围（作用域）角度出发，域内的组分为以下三种（见表3-3-1）：本地域组（domain local group）、全局组（global group）、通用组（universal group）。



## 1. 本地域组

它主要是被用来分配对其所属域内资源的访问权限，以便可以访问该域内的资源。

- 其成员可以包含任何一个域内的用户、全局组、通用组；也可以包含相同域内的本地域组；但无法包含其他域内的本地域组。
- 本地域组只能够访问该域内的资源，无法访问其他不同域内的资源；换句话说在设置权限时，只能设置相同域内的本地域组的权限，无法设置其他不同域内的本地域组的权限。

表3-3-1

特性组	本地域组	全局组	通用组
可包含的成员	所有域内的用户、全局组、通用组；相同域内的本地域组	相同域内的用户与全局组	所有域内的用户、全局组、通用组
可以在哪一个域内被设置权限	同一个域	所有域	所有域
组转换	可以被转换成通用组（只要原组内的成员不包含本地域组即可）	可以被转换成通用组（只要原组不隶属于任何一个全局组即可）	可以被转换成域本地组；可以被换成全局组（只要原组内的成员不包含通用组即可）

## 2. 全局组

它主要是用来组织用户，也就是可以将多个即将被赋予相同权限的用户账户，加入到一个全局群组内。

- 全局组内的成员，只能够包含相同域内的用户与全局组。
- 全局组可以访问任何一个域内的资源，也就是说可以在任何一个域内设置全局组的权限（这个全局组可以位于任何一个域内），以便让此全局组具备权限来访问该域内的资源。

## 3. 通用组

它可以在所有域内被设置访问权限，以便访问所有域内的资源。

- 通用组具备“通用范围”特性，其成员可以包含林中任何一个域内的用户、全局组、通用组。但是它无法包含任何一个域内的本地域组。
- 通用组可以访问任何一个域内的资源，也就是说可以在任何一个域内设置通用组的权限（这个通用组可以位于任何一个域内），以便让此通用组具备权限来访问该域内的资源。





### 3.3.3 域组的创建与管理

#### 1. 组的新建、删除与重命名

















如果新建域组时，可通过【单击左下角开始图标  Windows 管理工具  Active Directory管理中心  展开域名  单击容器或组织单位  单击右侧任务窗格的新建  组】的方法，然后在图3-3-1中输入组名、输入供旧版操作系统来访问的组名、选择组类型与组作范围等。若要删除组的话：【选中组账户并右击  删除】。



图 3-3-1

#### 2. 添加组的成员

如果要用户、组等加入到组内的话：【如图3-3-2所示单击成员区域右侧的添加  按钮  单击高级  按钮  单击立即查找  按钮  选择要被加入的成员（按 **Shift** 或 **Ctrl** 键可同时选择多个账户）  单击确定  按钮  ……】。

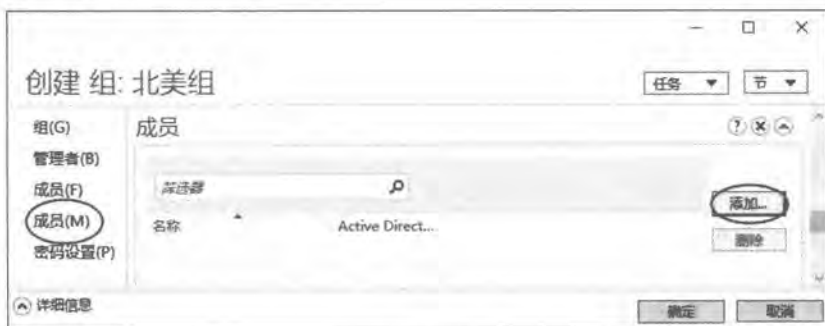


图 3-3-2

### 3.3.4 AD DS内置的组

AD DS有许多内置组，它们分别隶属于本地域组、全局组、通用组与特殊组。



## 1. 内置的本地域组

这些本地域组本身已被赋予一些权限，以便让其具备管理AD DS域的能力。只要将用户或组账户加入到这些组内，这些账户也会自动具备相同的权限。以下是Builtin容器内常用的本地域组。

- **Account Operators:** 其成员默认可以在容器与组织单位内新建/删除/修改用户、组与计算机账户，不过部分内置的容器例外，例如Builtin容器与Domain Controllers 组织单位，同时也不允许在部分内置的容器内新建计算机账户，例如Users。他们也无法更改大部分组的成员，例如Administrators等。
- **Administrators:** 其成员具备系统管理员权限，他们对所有域控制器拥有最大的控制权限，可以执行AD DS管理工作。内置系统管理员Administrator就是此组的成员，而且无法将其从此组内删除。  
此组默认的成员包含了Administrator、全局组Domain Admins、通用组Enterprise Admins等。
- **Backup Operators:** 其成员可以通过Windows Server Backup工具来备份与还原域控制器内的文件，不论他们是否有权限访问这些文件。其成员也可以将域控制器关机。
- **Guests:** 其成员无法永久改变其桌面环境，当他们登录时，系统会为他们建立一个临时的用户配置文件，而注销时此配置文件就会被删除。此组默认的成员为用户账户Guest与全局组Domain Guests。
- **Network Configuration Operators:** 其成员可在域控制器上执行常规的网络配置工作，例如更改IP地址，但不可以安装、删除驱动程序与服务，也不能执行与网络服务器设置有关的工作，例如DNS与DHCP服务器的配置。
- **Performance Monitor Users:** 其成员可监视域控制器的工作性能。
- **Pre-Windows 2000 Compatible Access:** 此组主要是为了与Windows NT 4.0（或更旧的系统）兼容。其成员可以读取AD DS域内的所有用户与组账户。其默认的成员为特殊组Authenticated Users。请仅在用户的计算机是Windows NT 4.0或更旧的系统时，才将用户加入到此组内。
- **Print Operators:** 其成员可以管理域控制器上的打印机，也可以将域控制器关机。
- **Remote Desktop Users:** 其成员可从远程计算机通过远程桌面来登录。
- **Server Operators:** 其成员可以备份与还原域控制器内的文件；锁定与解锁域控制器；将域控制器上的硬盘格式化；更改域控制器的系统时间；将域控制器关机等。
- **Users:** 其成员仅拥有一些基本权限，例如执行应用程序，但是他们不能修改操作系统的设置、不能更改其他用户的数据、不能将服务器关机。此组默认的成员为全局组Domain Users。

## 2. 内置的全局组

AD DS内置的全局组本身并没有任何的权限，但是可以将其加入到具备权限的本地域



组，或另外直接给此全局组分配权限。这些内置全局组是位于Users容器内。以下列出常用的全局组。

- **Domain Admins:** 域成员计算机会自动将此组加入到其本地组Administrators内，因此Domain Admins组内的每一个成员，在域内的每一台计算机上都具备系统管理员权限。此组默认的成员为域用户Administrator。
- **Domain Computers:** 所有的域成员计算机（域控制器除外）都会被自动加入到此组内。
- **Domain Controllers:** 域内的所有域控制器都会被自动加入到此组内。
- **Domain Users:** 域成员计算机会自动将此组加入到其本地组Users内，因此Domain Users内的用户将享有本地组Users所拥有的权限，例如拥有**允许本地登录**的权限。此组默认的成员为域用户Administrator，而以后新建的域用户账户都自动会隶属于此组。
- **Domain Guests:** 域成员计算机会自动将此组加入到本地组Guests内。此组默认的成员为域用户账户Guest。

### 3. 内置的通用组

- **Enterprise Admins:** 此组只存在于林根域，其成员有权管理林内的所有域。此组默认的成员为林根域内的用户Administrator。
- **Schema Admins:** 此组只存在于林根域，其成员具备管理架构（schema）的权限。此组默认的成员为林根域内的用户Administrator。

## 3.3.5 特殊组账户

除了前面所介绍的组之外，还有一些特殊组，而用户无法更改这些特殊组的成员。以下列出几个常用的特殊组。

- **Everyone:** 任何一个用户都属于这个组。如果Guest账户被启用的话，则在为Everyone分配权限时需要小心，因为如果一位在计算机内没有账户的用户，通过网络登录你的计算机时，他会被自动允许利用Guest账户来连接，此时因为Guest也是隶属于Everyone组，所以他将具备Everyone所拥有的权限。
- **Authenticated Users:** 任何利用有效用户账户来登录此计算机的用户，都隶属于此组。
- **Interactive:** 任何在本地登录（例如按`Ctrl` + `Alt` + `Del`登录）的用户，都隶属于此组。
- **Network:** 任何通过网络登录此计算机的用户，都隶属于此组。
- **Anonymous Logon:** 任何未利用有效的普通用户账户登录的用户，都隶属于此组。Anonymous Logon默认并不隶属于Everyone组。
- **Dialup:** 任何利用拨接方式来连接的用户，都隶属于此组。



## 3.4 组的使用原则

为了让网络管理更加容易，同时也为了减少以后维护的负担，因此在利用组来管理网络资源时，建议尽量采用以下的原则，尤其是大型网络。

- A、G、DL、P原则
- A、G、G、DL、P原则
- A、G、U、DL、P原则
- A、G、G、U、DL、P原则

A代表用户账户（user Account）、G代表全局组（Global group）、DL代表本地域组（Domain Local group）、U代表通用组（Universal group）、P代表权限（Permission）。

### 3.4.1 A、G、DL、P原则

A、G、DL、P原则就是先将用户账户（A）加入到全局组（G）、再将全局组加入到本地域组（DL）内、然后设置本地域组的权限（P），如图3-4-1所示。以此图为例来说，只要针对图中的本地域组来设置权限，则隶属于该本地域组的全局组内的所有用户，都自动会具备该权限。

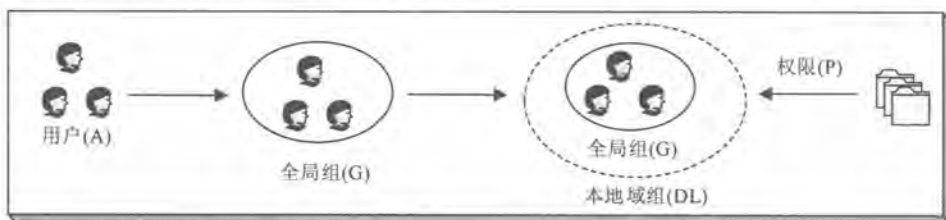


图 3-4-1

举例来说，如果甲域内的用户需要访问乙域内资源的话，则由甲域的系统管理员负责在甲域建立全局组、将甲域用户账户加入到此组内；而乙域的系统管理员则负责在乙域建立本地域组、设置此组的权限、然后将甲域的全局群组加入到此组内。之后由甲域的系统管理员负责维护全局组内的成员，而乙域的系统管理员则负责维护权限的设置，如此便可以分散管理工作的负担。

### 3.4.2 A、G、G、DL、P原则

A、G、G、DL、P原则就是先将用户账户（A）加入到全局组（G）、将此全局群加入到另一个全局组（G）内、再将此全局组加入到本地域组（DL）内、然后设置本地域组的权限（P），如图3-4-2所示。图中的全局组（G3）内包含了2个全局组（G1与G2），它们必须是



同一个域内的全局组，因为全局组内只能够包含位于同一个域内的用户账户与全局组。

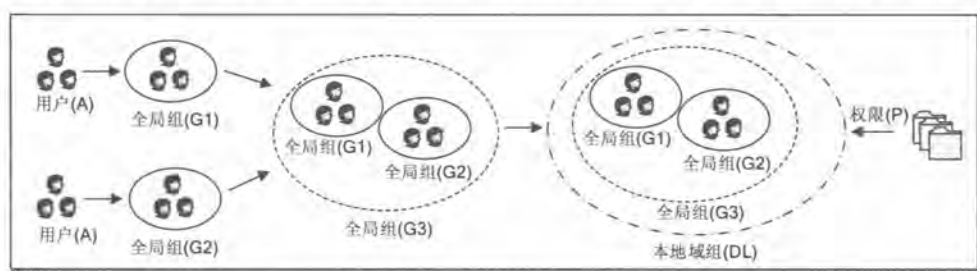


图 3-4-2

### 3.4.3 A、G、U、DL、P原则

图3-4-2中的全局组G1与G2若不是与G3在同一个域内，则无法采用A、G、G、DL、P原则，因为全局组（G3）内无法包含位于另外一个域内的全局组，此时需将全局组G3改为通用组，也就是需改用A、G、U、DL、P原则（如图3-4-3所示），此原则是先将用户账户（A）加入到全局组（G）、将此全局组加入到通用组（U）内、再将此通用组加入到域本地组（DL）内、然后设置本地域组的权限（P）。

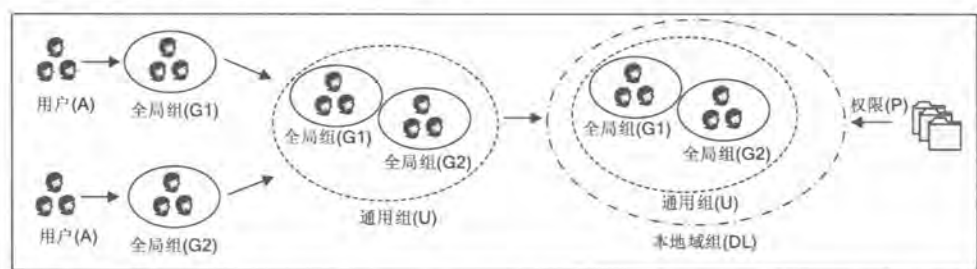


图 3-4-3

### 3.4.4 A、G、G、U、DL、P原则

A、G、G、U、DL、P原则与前面两种类似，在此不再重复说明。

也可以不遵循以上的原则来使用组，不过会有一些缺点存在，例如可以：

- ❖ 直接将用户账户加入到本地域组内，然后设置此组的权限。它的缺点是无法在其他域内设置此本地域组的权限，因为本地域组只能访问所属域内的资源。
- ❖ 直接将用户账户加入到全局组内，然后设置此组的权限。它的缺点是如果网络内包含多个域，而每个域内都有一些全局组需要对此资源具备相同的权限的话，则需要分别为每一个全局组设置权限，这种方法比较浪费时间，会增加网络管理的负担。