第3章

用户账户和组管理

学习目标

- 了解用户账户和组基础知识。
- 掌握安全策略服务管理。
- 掌握配置用户账户与组方法。

3.1 用户账户和组基础知识

在一个网络中，用户账户和计算机都是网络的主体，两者缺一不可。拥有用户账户是用户登录网络并使用网络资源的基础，因此用户账户和计算机管理是 Windows 网络管理中最必要且最经常的工作。

域系统管理员需要为每一个域用户分别建立一个用户账户，让他们可以利用这个账户登录域、访问网络上的资源。域系统管理员同时需要了解如何有效利用组，以便高效地管理资源的访问。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，访问有权访问的资源。换句话说，域用户在一台域成员计算机上成功登录后，要连接域内的其他成员计算机时，并不需要再登录被访问的计算机，这个功能称为单点登录。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，连接其他计算机时，需要再次登录被访问的计算机。

在服务器升级为域控制器之前，位于其本地安全数据库内的本地账户，会在服务器升级为域控制器之后被转移到 AD DS 数据库内，并且被放置到 Users 容器内。可以通过“Active Directory 用户和计算机”窗口查看本地账户的变化情况，如图 3.1 所示；也可以通过“Active Directory 管理中心”窗口查看本地账户的变化情况，如图 3.2 所示。

图 3.1 “Active Directory 用户和计算机”窗口

图 3.2 “Active Directory 管理中心”窗口

只有在建立域内的第一台域控制器时，该服务器原来的本地账户才会被转移到 AD DS 数据库内，其他域控制器内的本地账户并不会被转移到 AD DS 数据库内，而是被删除。

3.1.1 本地用户账户管理

Windows Server 2019 支持两种用户账户：本地账户和域账户。本地账户只能登录一台特定的计算机，并访问其资源；域账户可以登录域，并获得访问该网络的权限资源。

本地用户账户仅允许用户登录并访问创建该账户的计算机。当创建本地用户账户时，Windows Server 2019 仅在%systemroot%\system32\config 文件夹下的安全账户管理器(Security

Account Manager,SAM)数据库中创建该账户,如 C:\Windows\System32\config\SAM。

Windows Server 2019 默认有 Administrator 和 Guest 两个账户。Administrator 账户可以执行计算机管理的所有操作；Guest 账户是为临时访问用户设置的,默认是禁用的。

用户账户用来记录用户的用户名和口令、隶属的组、可以访问的网络资源,以及用户的个人文件和设置等相关信息。Windows Server 2019 为每个账户提供了名称,如 Administrator、Guest 等,这些名称是为了方便用户记忆、输入和使用的。本地计算机中的用户账户是不允许相同的,系统内部则使用安全标识符(Security Identifiers,SID)识别用户身份,每个用户账户对应一个唯一的安全标识符,这个安全标识符在用户创建时由系统自动产生。系统指派权利、授予资源访问权限等都需要使用安全标识符。

Windows NT 是微软发布的桌面端操作系统,于 1993 年 7 月 27 日发布,Windows NT 支持多处理器系统。在 Windows NT 的安全子系统中,安全标识符起什么作用呢？假设某公司有一个用户 admin 离开了公司,注销了该用户,又来了一个同名的员工,他的用户名、密码与离开公司的那名员工相同,操作系统能把二者区分开吗？二者的权限是否一样？

每当创建一个账户或一个组时,系统会分配给该账户或组一个唯一的 SID,Windows NT 中的内部进程将引用账户的 SID。换句话说,Windows NT 对登录的用户指派权限时,表面上是看用户名,实际上是根据 SID 进行的。如果创建账户后,再删除该账户,然后使用相同的用户名创建另一个账户,则新账户将不具有授权前账户的权利或权限,原因是即使账户被删除,它的 SID 仍然被保留；如果在计算机中再次添加一个相同名称的账户,它将被分配一个新的 SID,该账户具有不同的 SID,在域中利用账户的 SID 来决定用户的权限。

一个完整的 SID 包括用户和组的安全描述、48bit 的 ID authority、修订版本、可变的验证值(Variable Sub-Authority Values)。可以使用 Windows 内置的命令：whoami 查看账户的 SID 等相关信息,如图 3.3 所示。

图 3.3　账户的 SID 号

在SID列的属性值中，第1项S表示该字符串是SID；第2项是SID的版本号，对于Windows NT来说，版本号是1；第3项是标识符的颁发机构(Identifier Authority)，对于Windows NT内的账户来说，颁发机构就是NT，值是5；第4项表示一系列的子颁发机构代码，这里的值为21；前4项是标志域的，中间的30位数据，由计算机名、当前时间、当前用户线程的CPU耗费时间的总和这3个参数决定，以保证SID的唯一性；最后一个标志着域内的账户和组，称为相对标识符(Relative Identifiers，RID)，RID为500的SID是系统内置Administrator账户，即使重命名，其RID保持为500不变，许多黑客也是通过RID找到真正的系统内置Administrator账户。RID为501的SID是Guest账户。在域中从1000开始的RID代表用户账户，例如，RID为1010是该域创建的第10个用户。

在Windows Server 2019操作系统桌面，选择“此电脑”图标，右击，在弹出的快捷菜单中选择“管理”选项，弹出“服务器管理器”窗口，选择“工具”→“计算机管理”→“本地用户和组”→“用户”选项，查看默认用户账户情况，如图3.4所示。

图3.4　本地默认用户

(1) Administrator。管理计算机(域)的内置账户。

(2) DefaultAccount。系统管理的用户账户。

(3) Guest。供来宾访问计算机或访问域的内置账户。

(4) WDAGUtilityAccount。系统为Windows Defender应用程序防护方案管理和使用的用户账户。

3.1.2　本地组管理

对用户账户进行分组管理可以更加有效并且灵活地分配设置权限，以方便管理员对Windows Server 2019进行具体的管理。如果Windows Server 2019计算机被安装为成员服务器(而不是域控制器)，将自动创建一些本地组。如果将特定角色添加到计算机中，还将创建额外的组，用户可以执行与该组角色相对应的任务。例如，如果计算机被配置成为FTP服务器，将创建管理和使用FTP服务的本地组。

在 Windows Server 2019 操作系统桌面，选择“此电脑”图标，右击，在弹出的快捷菜单中选择“管理”选项，弹出“服务器管理器”窗口，选择“工具”→“计算机管理”→“本地用户和组”→“组”查看默认组情况，如图 3.5 所示。

图 3.5　本地默认组

3.1.3　域用户账户管理

在 Windows Server 2019 操作系统中，选择“开始”菜单→“Windows 管理工具”→“Active Directory 用户和计算机”选项，可以进行相关的域用户账户管理操作。

Builtin 容器里面包含的是工作组模式下的所有本地组，给文件赋予权限时可能会用到，如图 3.6 所示。

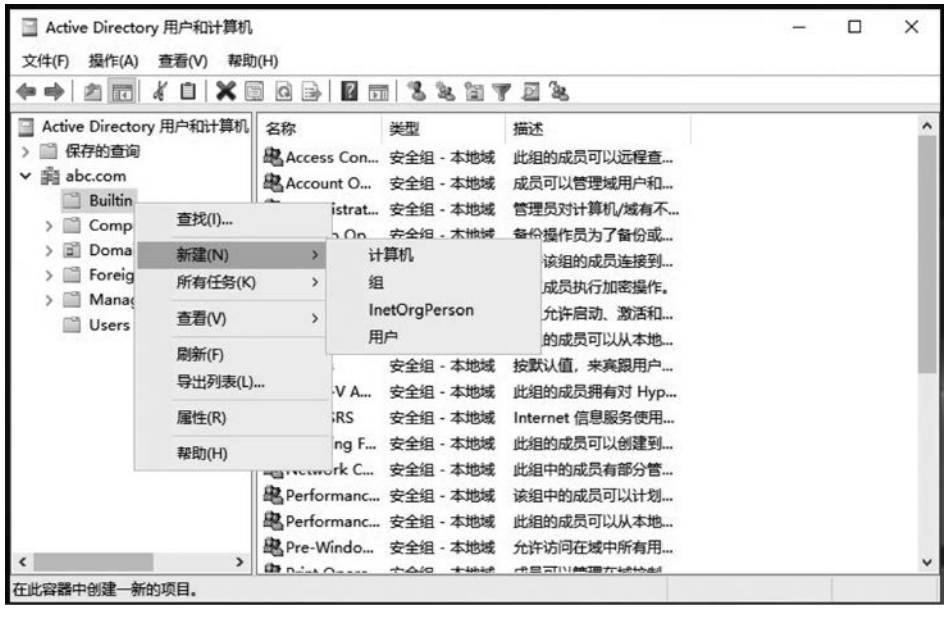

图 3.6　Builtin 容器相关操作

Users是默认的可以放置活动目录对象的容器。除了自建的组织单位(Organization Unit，OU)之外，这个容器中的用户和组都是用得最广泛的，包括域管理员账户、域管理员组、企业管理员组等，如图3.7所示。

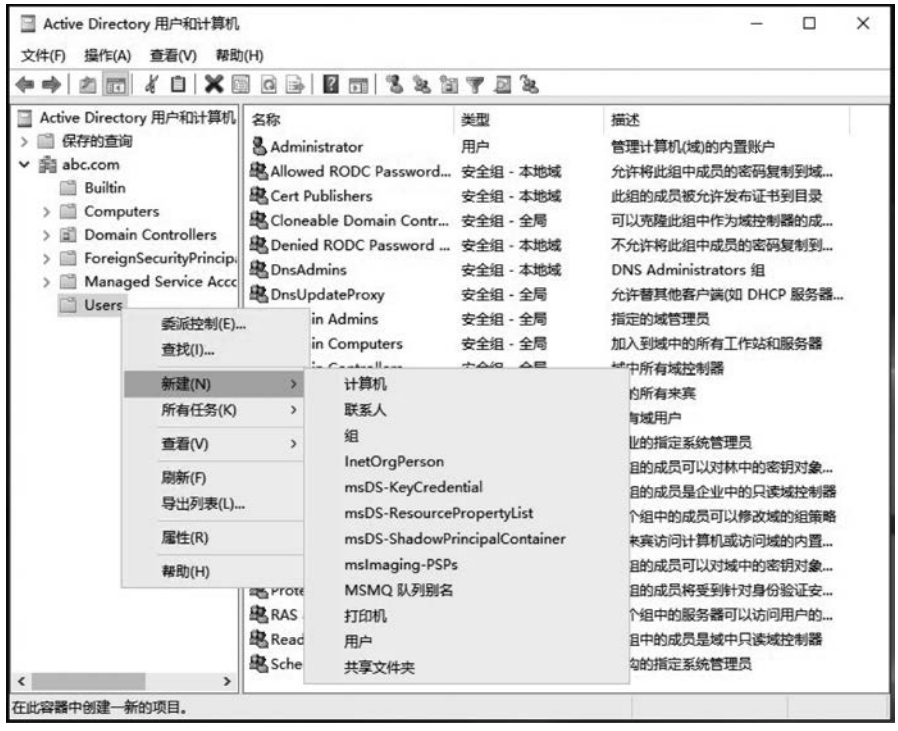

图3.7　Users容器相关操作

1. 域用户账户的一般管理

域用户账户的一般管理是指复制、添加到组、禁止账户、重置密码、移动、剪切、删除、重命名等相关操作。在左侧窗口中选择Users选项，在右侧区域窗口中选择想要管理的用户账户(如Administrator)，如图3.8所示。

2. 设置域用户账户的属性

每一个域用户账户内都有一些相关的属性信息，如电话号码、电子邮件、网页等，域用户可以通过这些属性来查找AD DS数据库内的用户。例如，通过电话号码来查找用户。因此，为了更容易地找到所需要的用户账户，这些属性信息应该越完整越好。下面通过“Active Directory用户和计算机”来介绍用户账户的部分属性，双击要设置的用户账户Administrator，弹出“Administrator属性”对话框，如图3.9所示。

用户账户属性窗口中，包含常规、地址、账户、配置文件、电话、组织、隶属于、拨入、环境、会话、远程控制、远程桌面服务配置文件、COM+等选项卡，可以对用户账户属性进行相关设置。例如，选择“账户”选项卡，勾选“解锁账户”复选框，可以对账户进行解锁；可以对“账户选项”区域进行设置，如勾选“密码永不过期”复选框；在“账户过期”区域，可以选择“永不过期”或“在这之后”单选按钮等，如图3.10所示。

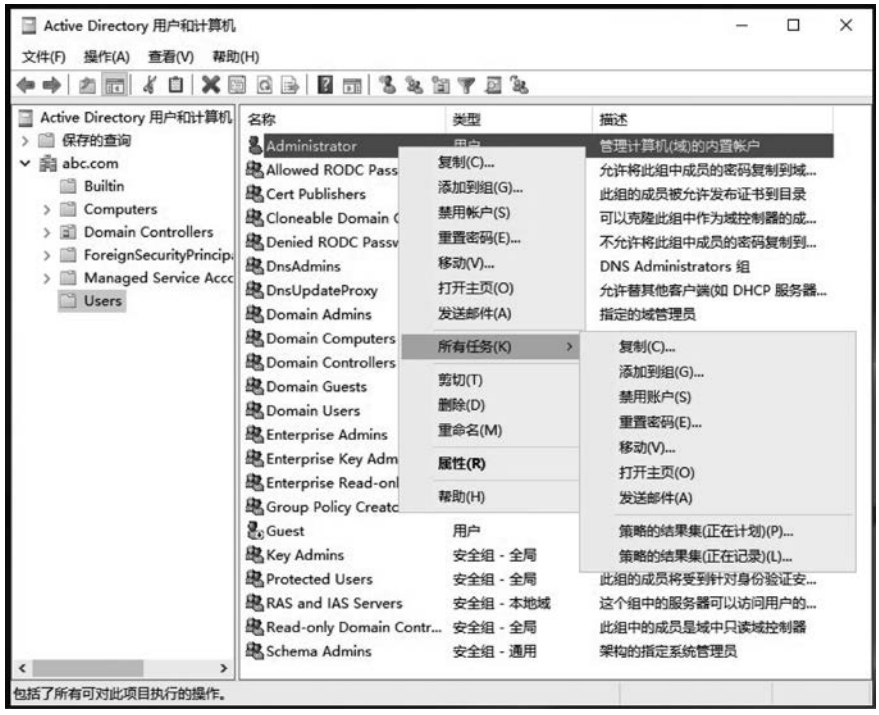

图 3.8　指定用户相关操作

图 3.9　“Administrator 属性”对话框

图 3.10　“账户”选项卡

3.1.4 域组管理

在 Windows Server 2019 操作系统中，选择“开始”菜单→“Windows 管理工具”→“Active Directory 用户和计算机”选项，打开“Active Directory 用户和计算机”窗口，在左侧窗口中选择 Users 选项，在右侧区域窗口中选择想要管理的组（如 Domain Admins），可以进行相关的域组管理操作，如图 3.11 所示。

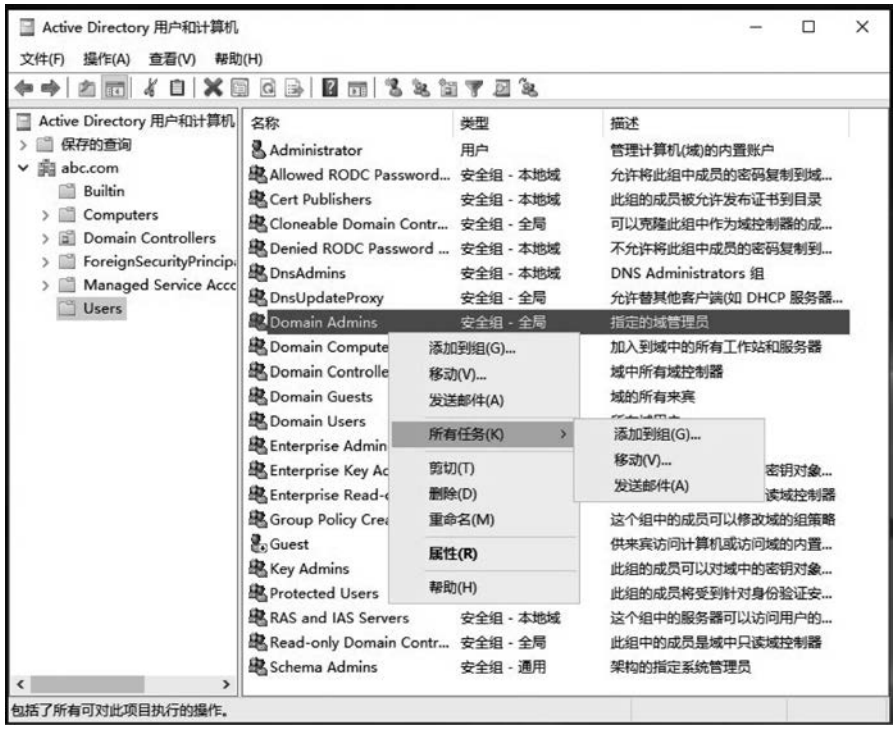

图 3.11 域组管理相关操作

1. 域内的组类型

使用组（Group）来管理用户账户，能够减轻许多网络管理的负担。针对组设置权限后，组内的所有用户账户都会自动拥有此权限，因此不需要对每一个用户进行设置。域组账户也都有唯一的安全标识符 SID，命令“whoami /users”显示当前用户的信息和安全标识符；命令“whoami /groups”显示当前用户的组成员信息、账户类型、安全标识符和属性，如图 3.12 所示；命令“whoami /?”显示该命令的常见用法。

AD DS 的域组分为安全组（Security Group）和通信组（Distribution Group）两种类型，且它们之间可以相互转换。

（1）安全组。安全组可以被用来分配权限与权利，可以指定安全组对文件具备读取的权限；也可以用在与安全无关的工作，可以给安全组发送电子邮件。

（2）通信组。通信组被用在与安全（权限与权利设置等）无关的工作上，可以给通信组发送电子邮件，但是无法为通信组分配权限与权力。

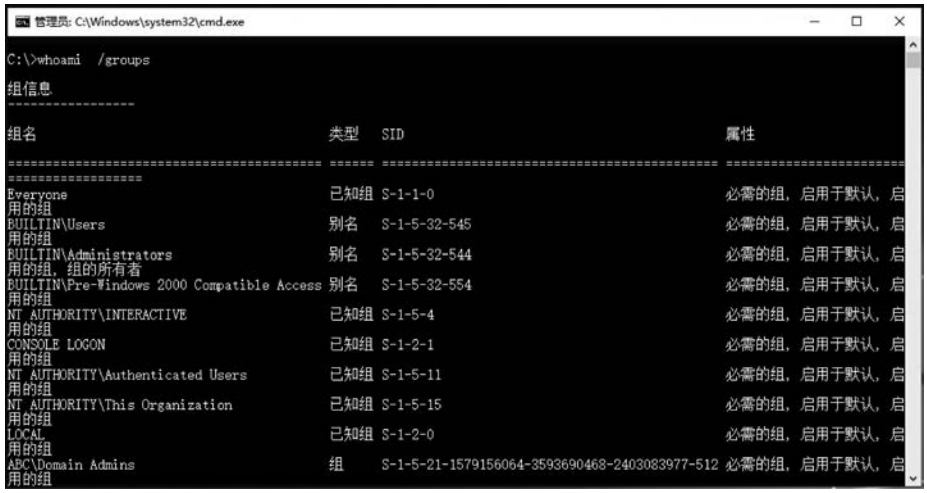

图 3.12　显示当前用户的组成员相关信息

2. 组作用域

从组的使用范围来看，域内的组分为本地域组(Domain Local Group)、全局组(Global Group)和通用组(Universal Group)。

(1) 本地域组。

本地域组主要被用来分配其所属域内的访问权限，以便访问该域内的资源。本地域组的成员可以包含任何一个域的用户、全局组、通用组；也可以包含相同域的本地域组；但无法包含其他域的本地域组。本地域组只能访问该域的资源，无法访问其他不同域的资源；换句话说，在设置权限时，只可以设置相同域的本地域组的权限，无法设置其他不同域的本地域组的权限。

内置的本地域组本身已经被赋予了一些权利与权限，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这些组内，这些账户就会自动具备相同的权利与权限。

下面是 Users 容器内常用的本地域组。

- Allowed RODC Password Replication Group。允许将此组中成员的密码复制到域中的所有只读域控制器。
- Cert Publishers。此组的成员被允许发布证书到目录。
- Denied RODC Password Replication Group。不允许将此组中成员的密码复制到域中的所有只读域控制器。
- DnsAdmins。DNS Administrators 组。
- RAS and IAS Servers。这个组中的服务器可以访问用户的远程访问属性。

下面是 Builtin 容器内常用的本地域组。

- Account Operators。成员可以管理域用户和组账户。
- Administrators。管理员对计算机/域有不受限制的完全访问权。
- Backup Operators。备份操作员为了备份或还原文件可以替代安全限制。
- Guests。按默认值，来宾跟用户组的成员有同等访问权，但来宾账户的限制更多。
- IIS_IUSRS。Internet 信息服务使用的内置组。
- Remote Desktop Users。此组中的成员被授予远程登录的权限。

- Event Log Readers。此组的成员可以从本地计算机中读取事件日志。
- Server Operators。成员可以管理域服务器。
- Users。防止用户进行有意或无意的系统范围的更改，但是可以运行大部分应用程序。
- Print Operators。成员可以管理在域控制器上安装的打印机。

（2）全局组。

全局组主要用来组织用户，也就是说，可以将多个即将被赋予相同权限的用户账户加入同一个全局组。全局组的成员只可以包含相同域的用户与全局组。全局组可以访问任何一个域的资源，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，以便让此全局组具备权限来访问该域的资源。

AD DS 内置的全局组本身没有任何的权利与权限，但是可以将其加入具备权利或权限的本地域组，或另外直接分配权利或权限给此全局组，这些内置全局组位于 Users 容器。

（3）通用组。

通用组可以在所有域内为通用组分配访问权限，以便访问所有域的资源。通用组具备万用领域的特性，其成员可以包含林中任何一个域的用户、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，以便让此通用组具备权限来访问该域的资源，这些内置通用组位于 Users 容器。

3.2 安全策略服务管理

作为网络操作系统或服务器操作系统，高性能、高可靠性和高安全性是其必备要素，随着日趋复杂的企业应用和 Internet 应用，对操作系统提出了更高的要求，因此安全的操作系统需要对用户账户与系统安全策略服务进行必要的管理。

3.2.1 用户账户安全策略管理

随着密码破解工具不断进步，而用于破解密码的计算机也比以往更为强大，弱密码很容易被破解，强密码则难以破解。系统用户账户密码口令的暴力破解主要是基于密码匹配的破解方法，最基本的方法有两个：穷举法和字典法。穷举法是效率最低的办法，将字符或数字按照穷举的规则生成口令字符串，进行遍历尝试。在口令稍微复杂的情况下，穷举法的破解速度很低。字典法相对来说破解速度较高，用口令字典中事先定义的常用字符去尝试匹配口令。口令字典是一个很大的文本文件，可以通过自己编辑或者由字典工具生成，里面包含单词或者数字的组合。如果密码是一个单词或者是简单的数字组合，那么就可以很轻易地破解密码。理论上讲，只要有足够多的时间，就可以破解任何密码。即便如此，破解强密码也远比破解弱密码困难得多。因此，安全的计算机需要对所有账户都使用强密码。

1. 用户账户命名规则

（1）账户名必须唯一。本地账户在本地计算机上必须是唯一的。

（2）账户名最长不能超过 20 个字符。

(3) 账户名不能包含 * 、?、|、:、=、+、<、>、\、/、[、]等特殊符号。

2. 强密码原则

操作系统一定要给 Administrator 账户指定一个强密码,以防止他人随意使用该账户。Windows Server 2019 允许最多由 128 个字符组成的口令,其中包括 3 类字符。

(1) 英文大、小写字母。

(2) 阿拉伯数字: 0、1、2、3、4、5、6、7、8、9。

(3) 键盘上的符号。键盘上所有未定义为字母和数字的字符,应为半角状态。

强密码应该遵循以下原则。

(1) 口令应该不少于 6 个字符。

(2) 同时包含上述 3 种类型的字符。

(3) 不包含完整的字典词汇。

(4) 不包含用户名、真实姓名、生日、公司名称等。

3. 账户策略

增强操作系统的安全,除了启用强壮的密码外,操作系统本身有账户的安全策略。账户策略包含密码策略和账户锁定策略。在密码策略中,可以设置增加密码复杂度,提高暴力破解的难度,增强安全性。在账户锁定策略中,可以设置账户锁定时间、账户锁阈值以及重置账户锁定计数器等相关操作。

可以使用以下 4 种方法打开“密码策略”设置窗口。

方法 1: 在 Windows Server 2019 操作系统中,选择“开始”菜单→“Windows 管理工具”→“本地安全策略”→“安全设置”→“账户策略” →“密码策略”选项。

方法 2: 在 Windows Server 2019 操作系统桌面,选择“此电脑”图标,右击,在弹出的快捷菜单中选择“管理”选项,弹出“服务器管理器”窗口,选择“工具”→“本地安全策略”→“安全设置”→“账户策略”→“密码策略”选项。

方法 3: 在 Windows Server 2019 操作系统桌面,使用 Win+R 组合键,打开“运行”窗口,输入 secpol.msc 命令,弹出“本地安全策略”窗口,如图 3.13 所示,选择“安全设置”→“账户策略”→“密码策略”选项。

图 3.13　“本地安全策略”窗口

方法 4：在 Windows Server 2019 操作系统桌面，使用 Win＋R 组合键，打开“运行”窗口，输入 gpedit. msc 命令，弹出“本地组策略编辑器”窗口，如图 3.14 所示，选择“计算机配置”→“Windows 设置”→“安全设置”→“账户策略”→“密码策略”选项。

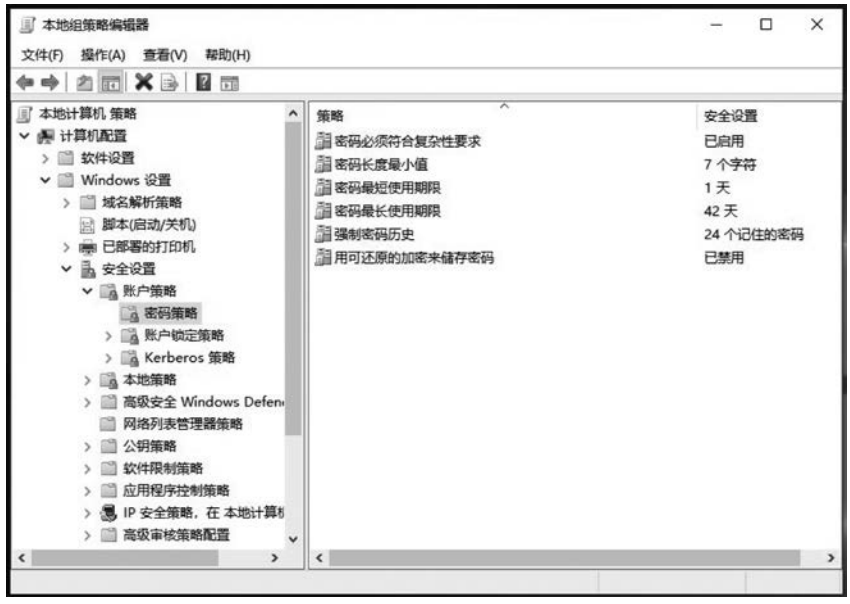

图 3.14 “本地组策略编辑器”窗口

针对不同的企业安全需求，Microsoft 公司给出了建议值，如表 3.1 所示。

表 3.1 密码策略设置建议值

策　略	本 地 设 置
密码必须符合复杂性要求	已启用
最短密码长度最小值	7 个字符
密码最短使用期限	1 天
密码最长使用期限	42 天
强制密码历史	24 个记住的密码
用可还原的加密来存储密码	已禁用

(1) 密码必须符合复杂性要求。

此安全设置确定密码是否必须符合复杂性要求。如果启用此策略，密码必须符合下列最低要求。

① 不能包含用户的账户名，不能包含用户姓名中超过两个连续字符的部分。

② 至少有 6 个字符长。

③ 包含以下 4 类字符中的 3 类。

英文大写字母(A～Z)；英文小写字母(a～z)；10 个基本数字(0～9)；非字母字符(例如 !、$、#、%)。

在更改或创建密码时执行复杂性要求。默认值：在域控制器上启用，在独立服务器上禁用。

注意：

在默认情况下，成员计算机沿用各自域控制器的配置。

(2) 最短密码长度最小值。

此安全设置确定了用户账户密码包含的最少字符数,可以将值设置为介于 1 和 20 之间;或者将字符数设置为 0,从而确定不需要密码。默认值在域控制器上为 7,在独立服务器上为 0。

注意:

在默认情况下,成员计算机沿用各自域控制器的配置。

(3) 密码最短使用期限。

此安全设置确定在用户更改某个密码之前,必须使用该密码一段时间(以天为单位)。可以设置一个介于 1 和 998 之间的值;或者将天数设置为 0,允许立即更改密码。

密码最短使用期限必须小于密码最长使用期限,除非将密码最长使用期限设置为 0,指明密码永不过期。如果将密码最长使用期限设置为 0,则可以将密码最短使用期限设置为介于 0 和 998 之间的任何值。

如果希望"强制密码历史"有效,则需要将密码最短使用期限设置为大于 0 的值。如果没有设置密码最短使用期限,用户则可以循环选择密码,直到获得期望的旧密码。默认设置没有遵从此建议,以便管理员能够为用户指定密码,然后要求用户在登录时更改管理员定义的密码。如果将密码历史设置为 0,用户将不必选择新密码。因此,默认情况下将"强制密码历史"设置为 1。默认值在域控制器上为 1,在独立服务器上设置为 0。

注意:

在默认情况下,成员计算机沿用各自域控制器的配置。

(4) 密码最长使用期限。

此安全设置确定在系统要求用户更改某个密码之前可以使用该密码的期间(以天为单位)。可以将密码设置为在某些天数(介于 1 到 999 之间)后到期,或者将天数设置为 0,指定密码永不过期。如果密码最长使用期限介于 1 天和 999 天之间,密码最短使用期限必须小于密码最长使用期限。如果将密码最长使用期限设置为 0,则可以将密码最短使用期限设置为介于 0 和 998 之间的任何值。

注意:

安全最佳操作是将密码设置为 30～90 天后过期,具体取决于用户的环境。这样,攻击者用来破解用户密码以及访问网络资源的时间将受到限制。默认值为 42。

(5) 强制密码历史。

此安全设置确定再次使用某个旧密码之前必须与某个用户账户关联的唯一新密码数。该值必须介于 0 和 24 之间。

此策略使管理员能够通过确保旧密码不被连续重新使用来增强安全性。默认值在域控制器上为 24,在独立服务器上为 0。

注意:

在默认情况下,成员计算机沿用各自域控制器的配置。若要维护密码历史的有效性,还要同时启用密码最短使用期限安全策略设置,不允许在密码更改之后立即再次更改密码。

(6) 用可还原的加密来存储密码。

此安全设置确定操作系统是否使用可还原的加密来存储密码。此策略为某些应用程序提供支持,这些应用程序使用的协议需要用户密码来进行身份验证。使用可还原的加密存储密码与存储纯文本密码在本质上是相同的。因此,除非应用程序需求比保护密码信息更重要,否则绝不要启用此策略。通过远程访问或 Internet 身份验证服务(IAS)使用三次握手身份验证协议(CHAP)验证时需要设置此策略。在 Internet 信息服务(IIS)中使用摘要式身份验证时也需要设置此策略。

默认值：禁用。

在以上的密码策略中加强了密码的复杂度，以及强迫密码的位数，但是并不能够完全抵抗使用字典文件的暴力破解法，还需要制定账户锁定策略，如图 3.15 所示。例如，3 次无效登录后就锁定账户，使字典文件的穷举法执行不了。

图 3.15　账户锁定策略

4. 重新命名 Administrator 账户

由于 Windows Server 2019 的默认管理员账户 Administrator 已众所周知，所以该账号通常称为攻击者猜测口令攻击的对象。为了降低这种威胁，可以将账户 Administrator 重新命名，打开“服务器管理器”窗口，选择“工具”→“计算机管理”选项，如图 3.16 所示。

图 3.16　账户 Administrator 重新命名

5. 创建一个陷阱账户

在设置完账户策略后，再创建一个名为 Administrator 的本地账户，将其权限设置成为最低，并且设置一个 10 位以上的超级复杂密码，这样就可以提高系统的安全性。

6. 禁用或删除不必要的账户

应该在计算机管理单元中查看系统的活动账号列表，并且禁止所有非活动账户，特别是 Guest 账户，删除或者禁用不再需要的账户。

3.2.2　常用的系统进程与服务

进程与服务是 Windows NT 操作系统性能管理中常用的内容，科学地管理进程与服务能提升系统的性能。Windows NT 常用系统进程与服务的管理、系统日志的管理，以保护操作系统的安全。

1. 进程的概念

进程是操作系统中最基本、最重要的概念。进程为应用程序的运行实例，是应用程序的一次动态执行，可以将进程理解为操作系统当前运行的执行程序。程序是指令的有序集合，本身没有任何运行的含义，是一个静态的概念。进程是程序在处理器中的一次执行过程，是一个动态的概念。例如，当运行记事本程序(Notepad)时，就创建了一个用来容纳组成 Notepad.exe 的代码及其所需调用动态链接库的进程。每个进程均运行在其专用且受保护的地址空间。因此，如果同时运行记事本的两个副本，该程序正在使用的数据在各自实例中是彼此独立的。在记事本的一个副本中将无法看到该程序的第二个实例打开的数据。进程可以分为系统进程和用户进程，凡是用于完成操作系统的各种功能的进程就是系统进程，它们就是处于运行状态下的操作系统本身；用户进程就是所有由用户启动的进程。进程是操作系统进行资源分配的单位，在 Windows 下进程又被细化为线程，也就是一个进程下有多个能独立运行的更小的单位。

对应用程序来说，进程像一个大容器。在应用程序启动后，就相当于将应用程序装入容器，可以往容器中添加其他东西，如应用程序在运行时所需的变量数据等。一个进程可以包含若干线程，线程可以帮助应用程序同时做几件事，如一个线程向磁盘写入文件，另一个线程接收用户的按键操作，并及时做出反应，互相不干扰。在程序被运行后，系统第一时间为该程序进程建立一个默认的线程，此后，程序可以根据需要自行添加或删除相关的线程。

进程可以简单地理解为运行中的程序，需要占用内存、CPU 时间等系统资源。Windows NT 支持多用户多任务，即支持并行运行多个程序。为此，内核不仅要有专门代码负责为进程或线程分配 CPU 时间，还要开辟一段内存区域，用来存放记录这些进程详细情况的数据结构。内核就是通过这些数据结构知道系统中有多少进程及各进程的状态等信息的。换句话说，这些数据结构就是内核感知进程存在的依据。因此，只要修改这些数据结构，就能达到隐藏进程的目的。

2. 系统的关键进程

可通过 Windows NT 操作系统的任务管理器(Ctrl＋Alt＋Delete 组合键)可查看系统进程。任务管理器能够提供很多信息，如现在系统中运行的进程、进程 PID、内存情况等，如图 3.17 所示。

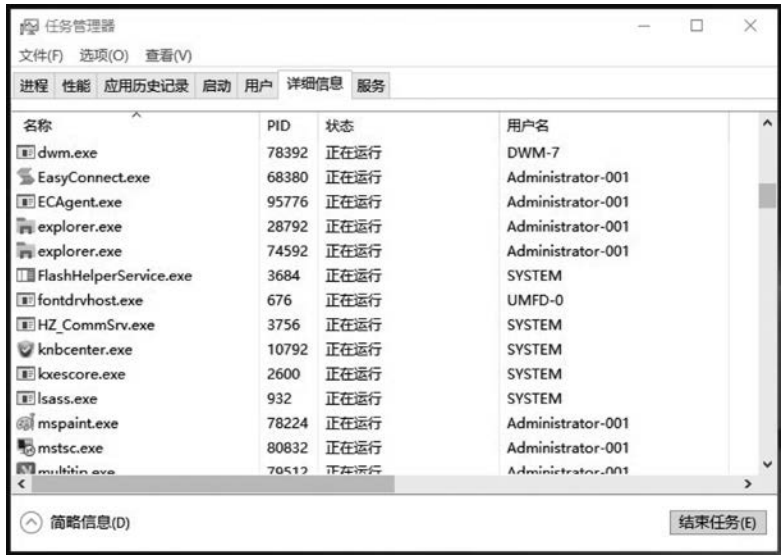

图 3.17　任务管理器

进程是操作系统进行资源分配的单位，用于完成操作系统各种功能的进程就是系统进程。系统进程又可以分为系统的关键进程和一般进程。

Windows NT 系统的关键进程是系统运行的基本条件。有了这些进程，系统就能正常运行。系统的关键进程列举如下。

（1）smss.exe。Session Manager 会话管理，负责启动用户会话。这个进程用于初始化系统变量，并且对许多活动的进程和设定的系统变量做出反应。

（2）csrss.exe。子系统服务器进程用于管理 Windows 图形的相关任务，用于维持 Windows 的控制。该进程崩溃时系统会蓝屏。

（3）winlogon.exe。此进程用于管理用户登录，且 Winlogon 在用户按 Ctrl＋Alt＋Delete 组合键时被激活，弹出安全对话框。

（4）services.exe。此进程包含很多系统服务，包括用于管理启动和停止服务。其对系统的正常运行是非常重要的。

（5）lsass.exe。本地的安全授权服务，管理 IP 安全策略以及启动 IP 安全驱动程序。产生会话密钥以及授予用于交互式客户/服务器验证的服务凭据。

（6）svchost.exe。此进程包含很多系统服务，在启动时会检查注册表中的位置以构建需要加载的服务列表。多个 svchost.exe 可以在同一时刻运行；每个 svchost.exe 在会话期间包含一组服务，单独的服务必须依靠 svchost.exe 获知“怎样启动”“在哪里启动”。

（7）spoolsv.exe。将文件加载到内存中以便滞后打印，管理缓冲池中的打印和传真作业。

（8）explorer.exe。Windows 资源管理器，管理桌面进程。

（9）wininit.exe 是 Windows NT 6.x 系统的一个核心进程。该进程不能强制结束，否则会蓝屏。wininit.exe 的工作是开启一些主要的 Windows NT 后台服务，如中央服务管理器、本地安全验证子系统和本地会话管理器。

（10）system。system 是 Windows 系统进程（其 PID 最小），是不能被关闭的，控制着系统核心模块（Kernel Module）的操作。如果 system 占用了 100％的 CPU，则表示系统的核心模块一直运行系统进程。没有 system 进程，系统就无法启动。

（11）System Idle。系统空闲进程，这个进程作为单纯程序运行在每个处理器中，其会在 CPU 空闲的时候发出一个 Idle 命令，使 CPU 挂起（暂时停止工作），可有效地降低 CPU 内核的温度，在操作系统服务中没有禁止该进程的选项；其默认占用除了当前应用程序所分配的 CPU 之外的所有占用率；一旦应用程序发出请求，处理器就会立刻响应。这个进程中出现的 CPU 占用数值并不是真正的占用，而是体现 CPU 的空闲率。也就是说，这个数值越大，CPU 的空闲率就越高；反之，CPU 的占用率就越高。

（12）System interrupt。系统中断进程是 Windows 的官方组成部分。尽管它在任务管理器中显示为一个进程，但它不是传统意义上的进程；相反，它是一个聚合占位符，用于显示计算机上发生的所有硬件中断使用的系统资源。

3. 系统的一般进程

系统的一般进程不是系统必需的，可以根据需要通过服务管理器来增加或减少。一般进程列举如下。

（1）internat.exe。Windows 多语言输入程序。

(2) mstask.exe。允许程序在指定时间运行。

(3) winmgmt.exe。提供系统管理信息。

(4) lserver.exe。注册客户端许可证。

(5) ups.exe。管理连接到计算机的不间断电源。

(6) dns.exe。应答对域名系统(DNS)名称的查询和更新请求。

(7) ntfrs.exe。在多个服务器间维护文件目录内容的文件同步。

(8) dmadmin.exe。磁盘管理请求的系统管理服务。

(9) smlogsvc.exe。配置性能日志和警报。

(10) mnmsrvc.exe。允许有权限的用户使用 NetMeeting 远程访问 Windows 桌面。

4. Windows 系统服务

在 Windows 操作系统中,服务是指执行指定系统功能的程序、进程等,以便支持其他程序,尤其是底层程序。服务是一种应用程序类型,在后台长时间运行,不显示窗口。服务应用程序通常可以在本地或通过网络为用户提供一些功能,如客户端/服务器端应用程序、Web 服务器、数据库服务器及其他基于服务器的应用程序。

对系统服务的操作可以通过服务管理器来实现。以管理员或组成员身份登录。可以使用以下 4 种方式打开服务管理器。

(1) 在 Windows Server 2019 操作系统中,选择“开始”菜单→“Windows 管理工具”→“服务”选项,弹出“服务”窗口,如图 3.18 所示。

图 3.18　“服务”窗口

（2）在 Windows Server 2019 操作系统桌面，选择“此电脑”图标，右击，在弹出的快捷菜单中选择“管理”选项，弹出“服务器管理器”窗口，选择“工具”→“服务”选项，弹出“服务”窗口，如图 3.18 所示。

（3）在 Windows Server 2019 操作系统桌面，使用 Win＋R 组合键，打开“运行”窗口，输入 services.msc 命令，弹出“服务”窗口，如图 3.18 所示。

（4）在 Windows Server 2019 操作系统桌面，选择“此电脑”图标，右击，在弹出的快捷菜单中选择“管理”选项，弹出“服务器管理器”窗口，选择“工具”→“计算机管理”→“服务和应用程序”→“服务”选项，如图 3.19 所示。

图 3.19　选择“服务”选项

在服务管理器中，双击任意一个服务，如 Certificate Propagation 服务，即可打开该服务的属性对话框，如图 3.20 所示。

在服务的属性对话框中，可以选择启动类型。对于任意一个服务，通常都有 3 种启动类型，即“自动”“手动”“禁用”。只要从“启动类型”下拉列表中选择，就可以更改服务的启动类型。

“服务状态”是指服务现在的状态是启动还是停止。通常可以利用“启动”“停止”“暂停”“恢复”按钮来改变服务的状态。

Windows 操作系统中有强大的 DOS 命令，sc 命令用于与服务管理器和服务进行通信。可以使用 sc.exe 来测试和调试服务程序，其语法格式如图 3.21 所示。

常用命令格式及命令的相关注释如下。

（1）sc query 服务名。查看服务的运行状态（如果服务名中间有空格，则需要加引号）。

（2）sc start 服务名。启动服务。

（3）sc stop 服务名。停止服务。

（4）sc qc 服务名。查询服务的配置信息。

（5）sc pause 服务名。向服务发送 PAUSE 控制请求。

（6）sc config start＝disabled 服务名。禁用服务。

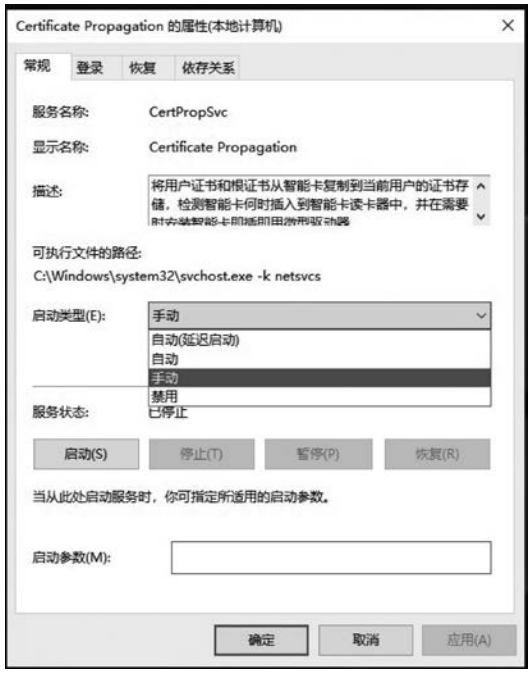

图 3.20　服务的属性对话框

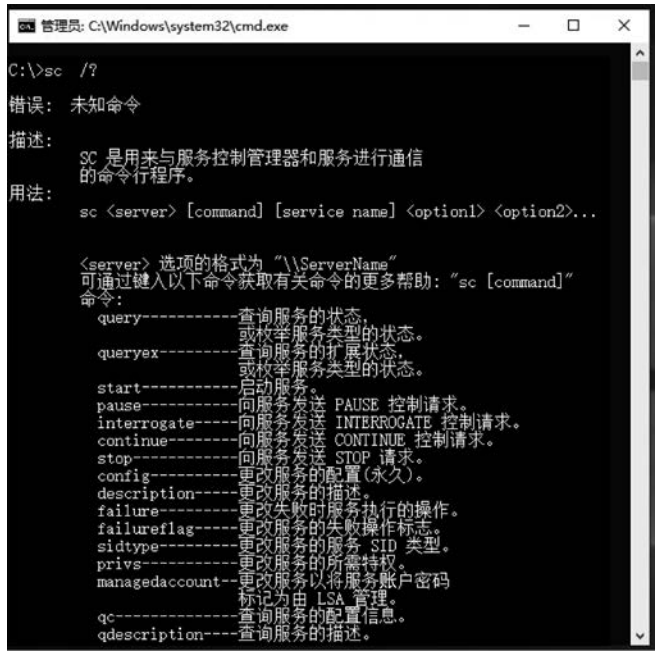

图 3.21　sc 命令的语法格式

3.3　技能实践

为了让网络管理更为方便容易，也为了减轻以后维护的负担，需要使用成员服务器上本地用户账户和组，或域控制器上用户账户和组来管理网络资源。

3.3.1　成员服务器上本地用户账户和组管理


V3-1

在成员服务器上使用本地用户账户和组来管理网络资源，用户可以在成员服务器上以本地管理员账户登录计算机，使用“计算机管理”中的“本地用户和组”管理单元来创建本地用户账户，而且用户必须拥有管理员权限。

1. 创建新用户账户

(1) 打开“服务器管理器”窗口，选择“工具”→“计算机管理”选项，弹出“计算机管理”窗口，在“计算机管理”窗口中，展开“本地用户和组”选项，在“用户”目录上右击，在弹出的快捷菜单中选择“新用户”命令，如图 3.22 所示。

(2) 打开“新用户”对话框，输入用户名、全名、描述和密码，如图 3.23 所示。设置密码时，密码要满足密码策略的要求，否则会提示“密码不满足密码策略的要求。检查最小密码长度、密码复杂性和密码历史的要求。”窗口。可以设置密码选项，包括“用户下次登录时须更改密码”“用户不能更改密码”“密码永不过期”“账户已禁用”。设置完成后，单击“创建”按钮，新增用户账户 xx_student01。创建完成后，单击“关闭”按钮，返回“计算机管理”窗口。

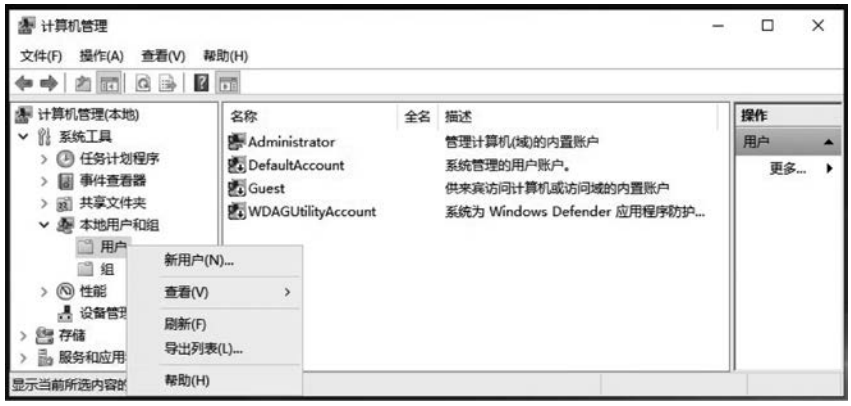

图 3.22　选择“新用户”命令

2. 设置本地用户账户的属性

用户账户不只包括用户名和密码等信息。为了管理和使用方便，一个用户账户还包括其他属性，如用户隶属于的用户组、用户配置文件、远程控制、远程桌面服务配置文件等。

在“本地用户和组”的右侧窗格中，双击刚刚建立的用户账户 xx_student01，打开“xx_student01 属性”对话框，如图 3.24 所示。

图 3.23　“新用户”对话框

图 3.24　“xx_student01 属性”对话框

(1)“常规”选项卡。

在“常规”选项卡中，可以设置与用户账户有关的描述信息，如全名、描述、密码选项等。

（2）“隶属于”选项卡。

在“隶属于”选项卡中，可以设置将用户账户加入其他本地组。为了管理方便，通常需要为用户组分配与设置权限。用户属于哪个组，就具有该用户组的权限。新增的用户账户默认加入Users组，如图3.25所示。Users组的用户一般不具备一些特殊权限，如安装应用程序、修改系统设置等。所以，当要分配给这个用户账户一些权限时，可以将用户账户加入其他组，也可以单击“删除”按钮，将用户账户从用户组中删除。

将用户账户xx_student01添加到管理员组，具体操作如下。

在“隶属于”选项卡中，单击“添加”按钮，弹出“选择组”对话框，如图3.26所示；在“选择组”对话框中，单击“高级”按钮，弹出“一般性查询”选项卡，在“一般性查询”选项卡中，选择“立即查找”按钮，选择要查询的组，如图3.27所示；单击“确定”按钮，返回“选择组”对话框，如图3.28所示；在“选择组”对话框中，单击“确定”按钮，返回“隶属于”选项卡。

图3.25　“隶属于”选项卡

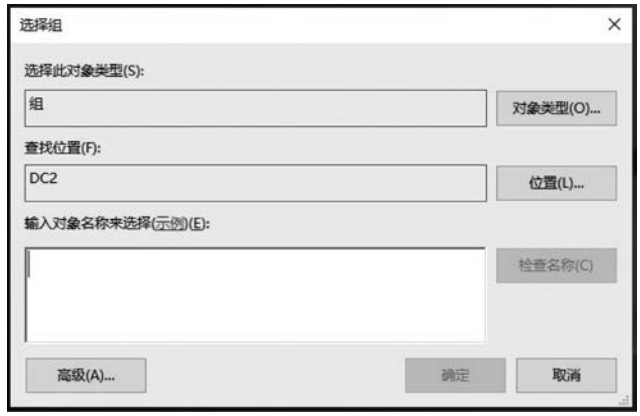

图3.26　“选择组”对话框

（3）“配置文件”选项卡。

在“配置文件”选项卡中，可以设置用户账户的配置文件路径、登录脚本和主文件夹路径，如图3.29所示。当用户账户第一次登录某台计算机时，Windows Server 2019根据默认用户配置文件自动创建一个用户配置文件，并将其保存在该计算机上。默认用户账户配置文件位于“C:\用户\default”文件夹下，该文件夹是隐藏文件夹（单击“查看”菜单，可选择是否显示隐藏项目），用户账户xx_student01的配置文件位于“C:\用户\ xx_student01”文件夹下。

（4）“环境”选项卡。

在“环境”选项卡中，可以配置远程桌面服务启动环境，这些设置会替代客户端所指定的设置，如图3.30所示。

图 3.27 “一般性查询”对话框

图 3.28 添加可用的组

(5)“会话”选项卡。

在“会话”选项卡中,可以配置远程桌面服务超时和重新连接设置,如图 3.31 所示。

(6)“远程控制”选项卡。

在“远程控制”选项卡中,可以配置远程桌面服务远程控制设置,如图 3.32 所示。

图 3.29　“配置文件”选项卡

图 3.30　“环境”选项卡

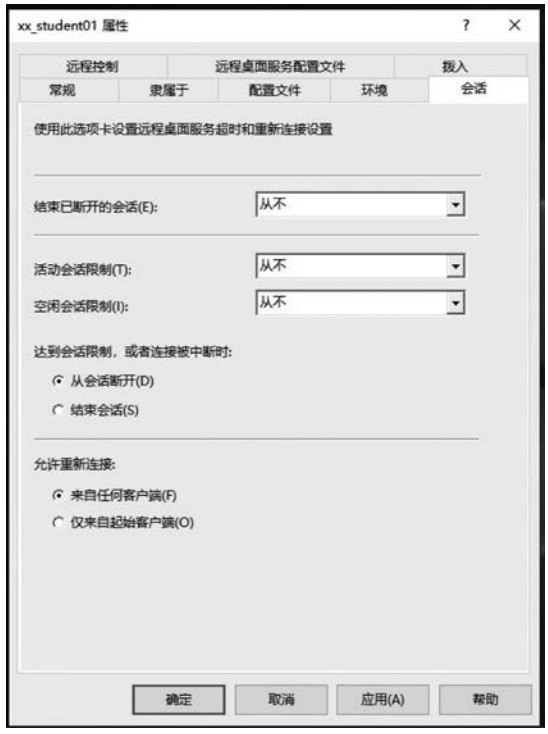

图 3.31　“会话”选项卡

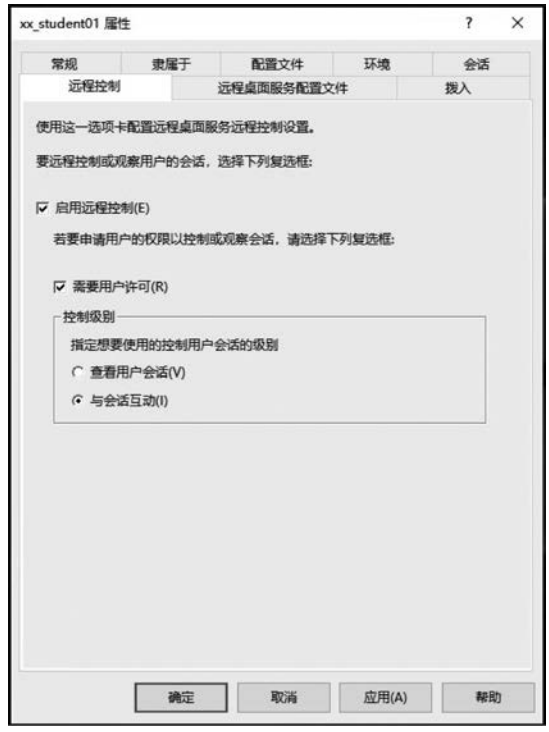

图 3.32　“远程控制”选项卡

（7）“远程桌面服务配置文件”选项卡。

在“远程桌面服务配置文件”选项卡中，可以配置远程桌面服务用户配置文件，此配置文件中的设置适用于远程桌面服务，如图 3.33 所示。

（8）“拨入”选项卡。

在“拨入”选项卡中，可以配置网络访问权限、回拨选项、分配静态 IP 地址、应用静态路由等相关设置，如图 3.34 所示。

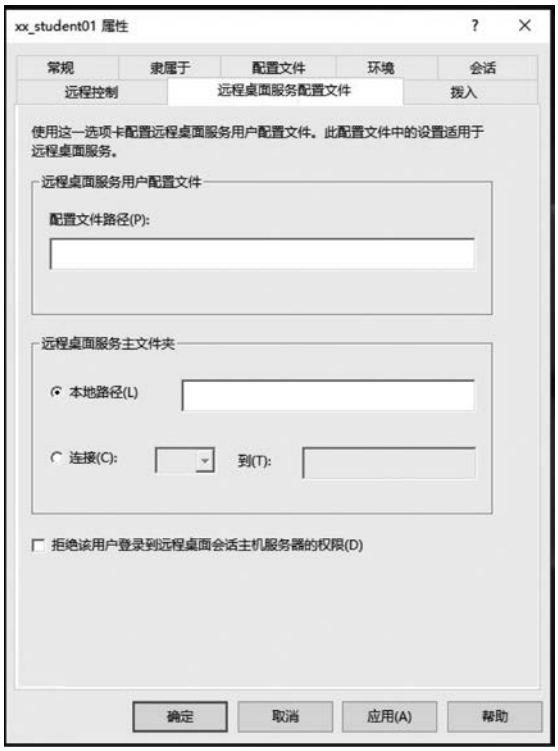

图 3.33 “远程桌面服务配置文件”选项卡

图 3.34 “拨入”选项卡

3. 创建本地组

（1）打开“服务器管理器”窗口，选择“工具”→“计算机管理”选项，弹出“计算机管理”窗口，在“计算机管理”窗口中，展开“本地用户和组”选项，在“组”目录上右击，在弹出的快捷菜单中选择“新建组”命令，如图 3.35 所示。

（2）打开“新建组”对话框，输入组名、描述，如图 3.36 所示；单击“创建”按钮，完成新建组 xx_group01 工作，单击“关闭”按钮，返回“计算机管理”窗口。

（3）向组中添加用户。双击组 xx_group01，打开组“xx_group01 属性”对话框，如图 3.37 所示；单击“添加”按钮，弹出“选择用户”对话框，在“选择用户”对话框中，单击“高级”按钮，弹出“一般性查询”对话框，单击“立即查找”按钮，选择要添加的用户账户 xx_student01，如图 3.38 所示；单击“确定”按钮，返回“选择用户”窗口，可看到，添加了用户账号 xx_student01，如图 3.39 所示；单击“确定”按钮，返回“计算机管理”窗口。

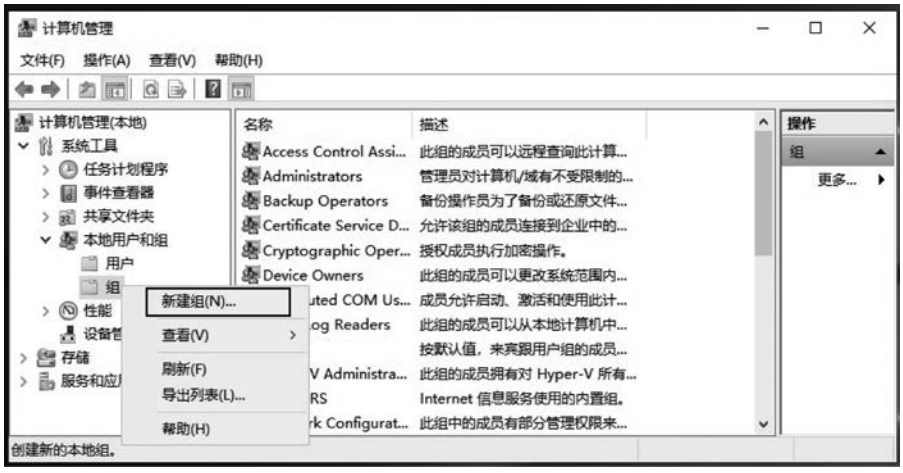

图 3.35　选择“新建组”命令

图 3.36　“新建组”对话框

图 3.37　组“xx_group01 属性”对话框

4. 删除本地用户账户和组

当用户和组不再需要使用时，可以将其删除。删除用户账户和组会导致与该用户账户和组有关的所有信息遗失。因此，在删除用户账号和组之前，最好确认其必要性或者考虑用其他方法，如禁用账户。许多企业给临时员工设置了 Windows 账户，当临时员工离开企业时将其账户禁用，新来的临时员工需要用该账户时只需要改名即可。在“计算机管理”控制台中，右击要删除的用户账户或组，就可以执行删除操作，但是系统内置用户账户是不能删除的，如 Administrator。

图 3.38　选择用户账户 xx_student01

图 3.39　添加用户账户 xx_student01

5. 使用命令管理本地用户账户和组

以管理员身份登录到成员服务器上，使用 Win＋R 组合键，打开“运行”对话框，输入 cmd 命令，如图 3.40 所示；单击“确定”按钮，弹出“命令行管理器”窗口，在“命令行管理器”窗口中，可以使用 net 命令管理本地用户账户和组，可以 net　/? 命令查看 net 命令的语法格式，如图 3.41 所示。

（1）创建用户账户 user01，密码为 Lncc@123（注意必须符合密码复杂度要求），执行命令如下。

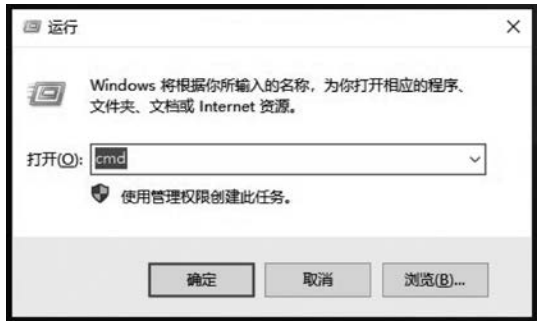

图 3.40　“运行”对话框

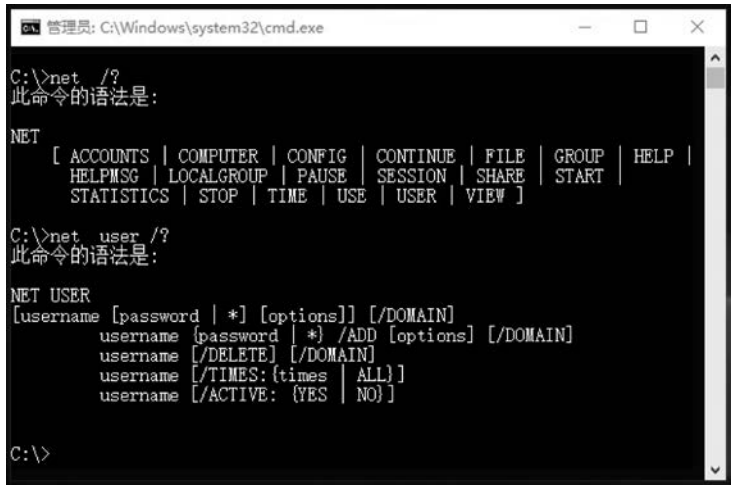

图 3.41　net 命令的语法格式

```
net user  user01  Lncc@123  /add
```

执行命令结果如图 3.42 所示。

(2) 查看当前用户账户列表,执行命令如下。

```
net  user
```

执行命令结果如图 3.43 所示。

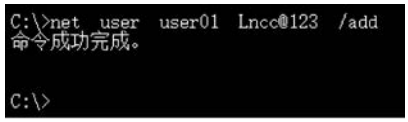

图 3.42　创建用户账户 user01

图 3.43　查看当前用户账户列表

(3) 修改用户账户 user01 的密码,密码修改为 Lncc@456(注意必须符合密码复杂度要求),执

行命令如下。

```
net user  user01  Lncc@456
```

执行命令结果如图 3.44 所示。

(4) 创建本地组 xx_localgroup01,执行命令如下。

```
net  localgroup  xx_localgroup01  /add
```

执行命令结果如图 3.45 所示。

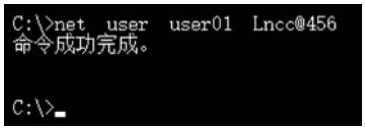

图 3.44　修改用户账户 user01 的密码

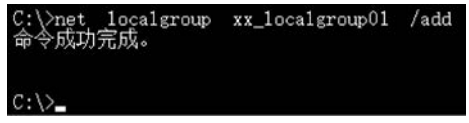

图 3.45　创建本地组 xx_localgroup01

(5) 查看当前本地组列表,执行命令如下。

```
net  localgroup
```

图 3.46　当前本地组列表

执行命令结果如图 3.46 所示。

(6) 将用户账户 user01 添加到组 xx_localgroup01,执行命令如下。

```
net localgroup  xx_localgroup01  user01  /add
```

执行命令结果如图 3.47 所示。

(7) 查看当前组 xx_localgroup01 内用户账户信息,执行命令如下。

```
net localgroup  xx_localgroup01
```

执行命令结果如图 3.48 所示。

(8) 删除组 xx_localgroup01 中用户账户 user01,执行命令如下。

```
net localgroup  xx_localgroup01  user01  /del
```

执行命令结果如图 3.49 所示。

(9) 删除用户账户 user01,执行命令如下。

```
net user  user01  /del
```

执行命令结果如图 3.50 所示。

(10) 删除组 xx_localgroup01,执行命令如下。

```
net localgroup  xx_localgroup01  /del
```

```
C:\>net  localgroup  xx_localgroup01  user01  /add
命令成功完成。


C:\>
```

图 3.47　用户账户 user01 添加到组 xx_localgroup01

```
C:\>net  localgroup  xx_localgroup01
别名        xx_localgroup01
注释

成员

-------------------------------------
---------
user01
命令成功完成。


C:\>
```

图 3.48　组 xx_localgroup01 内用户账户信息

```
C:\>net  localgroup  xx_localgroup01  user01  /del
命令成功完成。


C:\>
```

图 3.49　删除组 xx_localgroup01 中用户账户 user01

执行命令结果如图 3.51 所示。

```
C:\>net  user  user01  /del
命令成功完成。


C:\>
```

图 3.50　删除用户账户 user01

```
C:\>net  localgroup  xx_localgroup01  /del
命令成功完成。


C:\>
```

图 3.51　删除组 xx_localgroup01

3.3.2　域控制器上用户账户和组管理

V3-2

Windows Server 2019 支持域账户和组管理，域账户可以登录到域上，获得访问该网络的权限资源。

1. 项目规划

某公司目前正在实施项目，该项目分为总公司项目部项目 OU_projectA01 和分公司项目部 OU_projectB01 共同完成，需要创建一个共享目录。总公司项目部和分公司项目部需要对共享目录有写入和删除权限。公司决定在子域控制器 lncc. abc. com 上临时创建共享目录 project_share01，网络拓扑结构图如图 3.52 所示。

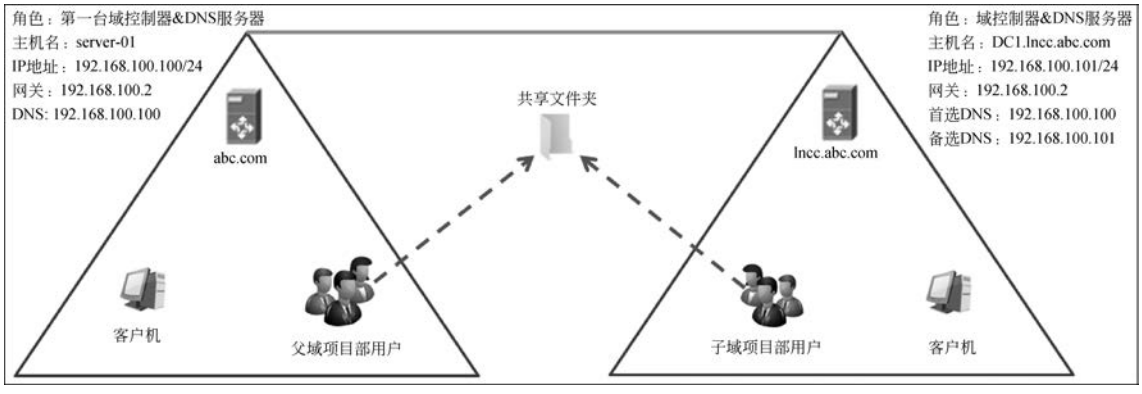

图 3.52　网络拓扑结构图

（1）父域控制器 abc.com，主机名：server-01；IP 地址：192.168.100.100/24；网关：192.168.100.2；DNS：192.168.100.100。

（2）子域控制器 lncc.abc.com，主机名：DC1.lncc.abc.com；IP 地址：192.168.100.101/24；网关：192.168.100.2，首选 DNS：192.168.100.100；备用 DNS：192.168.100.101。

（3）在父域控制器上，创建组织单位 OU_project_A01；创建总公司项目部用户账户 project_userA01、project_userA02；创建全局组 project_groupA01；将总公司项目部用户账户 project_userA01、project_userA02 加入全局组 project_groupA01 中。

（4）在子域控制器上，创建组织单位 OU_project_B01；创建子公司项目部用户账户 project_userB01、project_userB02；创建全局组 project_groupB01；将总公司项目部用户账户 project_userB01、project_userB02 加入全局组 project_groupB01 中；创建本址域组 project_localgroupB01，将全局组 project_groupB01 加入本址域组 project_localgroupB01。

2. 项目实施

（1）在分公司 DC1 上创建组织单位 OU_project_B01。打开“Windows 管理工具”→“Active Directory 用户和计算机”窗口，选中 lncc.abc.com 选项，右击，在弹出的快捷菜单中选择“新建”→“组织单位”选项，如图 3.53 所示，弹出“新建对象-组织单位”对话框，输入组织单位名称 OU_project_B01，勾选“防止容器被意外删除”复选框，如图 3.54 所示。

图 3.53　选择新建组织单位

（2）在“新建对象-组织单位”对话框中，单击“确定”按钮，返回“Active Directory 用户和计算机”窗口，选择刚刚创建的组织单位 OU_project_B01 选项，右击，在弹出的快捷菜单中选择“新建”→“用户”选项，如图 3.55 所示；弹出“新建对象-用户”对话框，如图 3.56 所示。创建用户账户 project_userB01、project_userB02。

（3）在“新建对象-用户”对话框中，输入要创建的用户账户名称，单击“下一步”按钮，弹出密码设置对话框，如图 3.57 所示；输入密码，并再次确认密码，单击“下一步”按钮，弹出用户创建完成

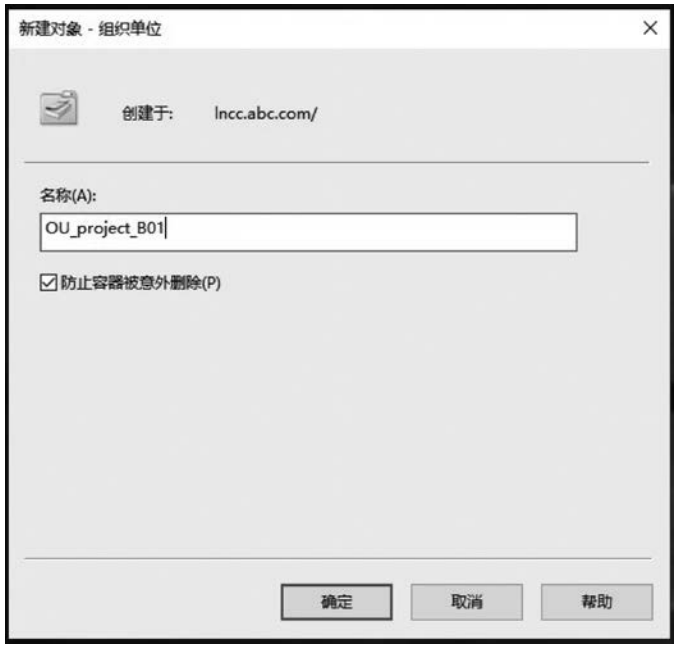

图 3.54　“新建对象-组织单位”对话框

图 3.55　选择新建用户

图 3.56 “新建对象-用户”对话框

图 3.57 密码设置对话框

对话框，如图 3.58 所示；单击“完成”按钮，用户账户 project_userB01 创建完成。

图 3.58 用户创建完成对话框

（4）创建全局组 project_groupB01。选择刚刚创建的组织单位 OU_project_B01 选项，右击，在弹出的快捷菜单中选择“新建”→“组”选项，弹出“新建对象-组”对话框，如图 3.59 所示；输入组名：project_groupB01，在“组作用域”区域，选中“全局”单选按钮，创建全局组 project_groupB01；单击“确定”按钮，返回“Active Directory 用户和计算机”窗口，如图 3.60 所示，双击刚刚创建的全局组 project_groupB01，弹出“project_groupB01 属性”对话框，如图 3.61 所示。

（5）将总公司项目部用户账户 project_userB01、project_userB02 加入全局组 project_groupB01。在“project_groupB01 属性”对话框中，选择“成绩”选项卡，单击“添加”按钮，弹出“选择用户、联系人、计算机、用户账户或组”对话框，如图 3.62 所示；在“选择用户、联系人、计算机、用户

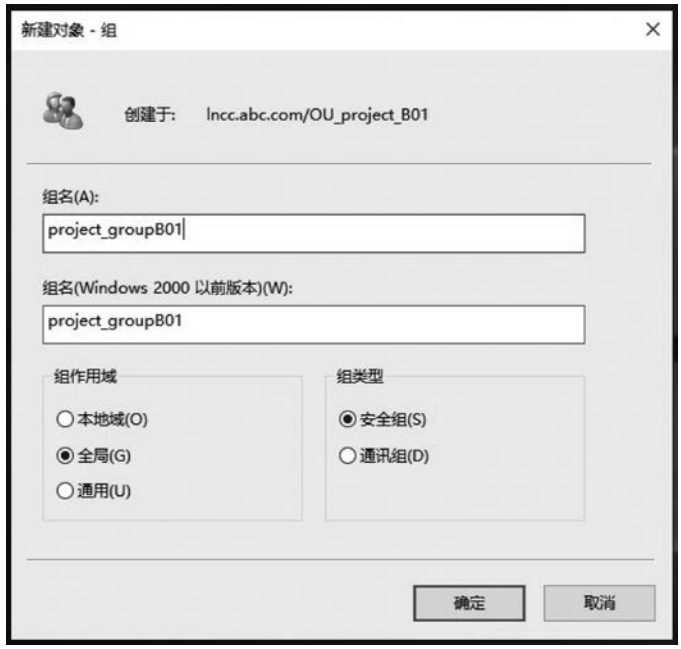

图 3.59　“新建对象-组”对话框

图 3.60　“Active Directory 用户和计算机”窗口

图 3.61 “project_groupB01 属性”对话框

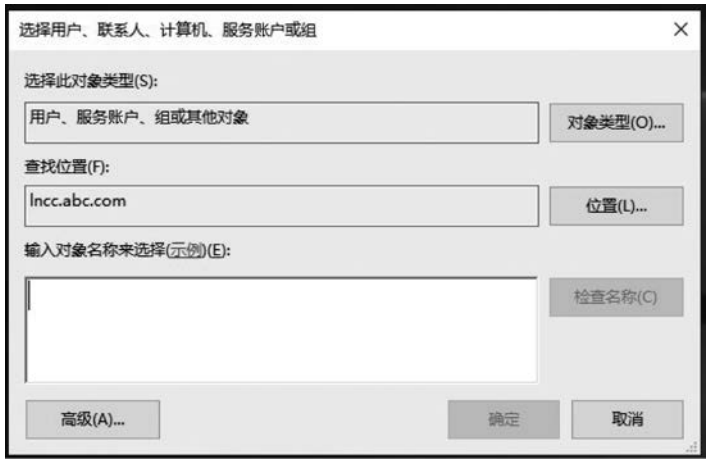

图 3.62 “选择用户、联系人、计算机、服务账户或组”对话框(1)

账户或组”对话框中，单击“高级”按钮，弹出“一般性查询”选项卡，如图 3.63 所示。

(6) 在“一般性查询”选项卡中，单击“确定”按钮，返回“选择用户、联系人、计算机、服务账户或组”对话框，如图 3.64 所示；单击“确定”按钮，返回“project_groupB01 属性”对话框；单击“确定”按钮，返回“Active Directory 用户和计算机”对话框。

(7) 创建本址域组 project_localgroupB01，将全局组 project_groupB01 加入本址域组 project_localgroupB01。选中组织单位 OU_project_B01 选项，右击，在弹出的快捷菜单中选择“新建”→

图 3.63　“一般性查询”选项卡

图 3.64　“选择用户、联系人、计算机、服务账户或组”对话框(2)

“组”选项，弹出“新建对象-组”对话框，输入组名 project_localgroupB01，如图 3.65 所示；在“组作用域”区域中，选中“本地域”单选按钮，单击“确定”按钮，返回“Active Directory 用户和计算机”窗口，双击刚刚创建的本地域组 project_localgroupB01，弹出“选择用户、联系人、计算机、服务账户或组”对话框，如图 3.66 所示。

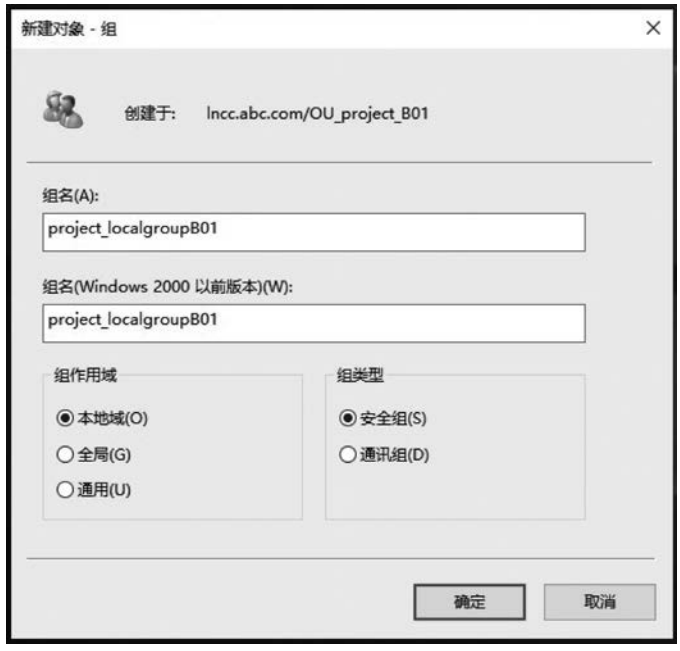

图 3.65 “新建对象-组”对话框

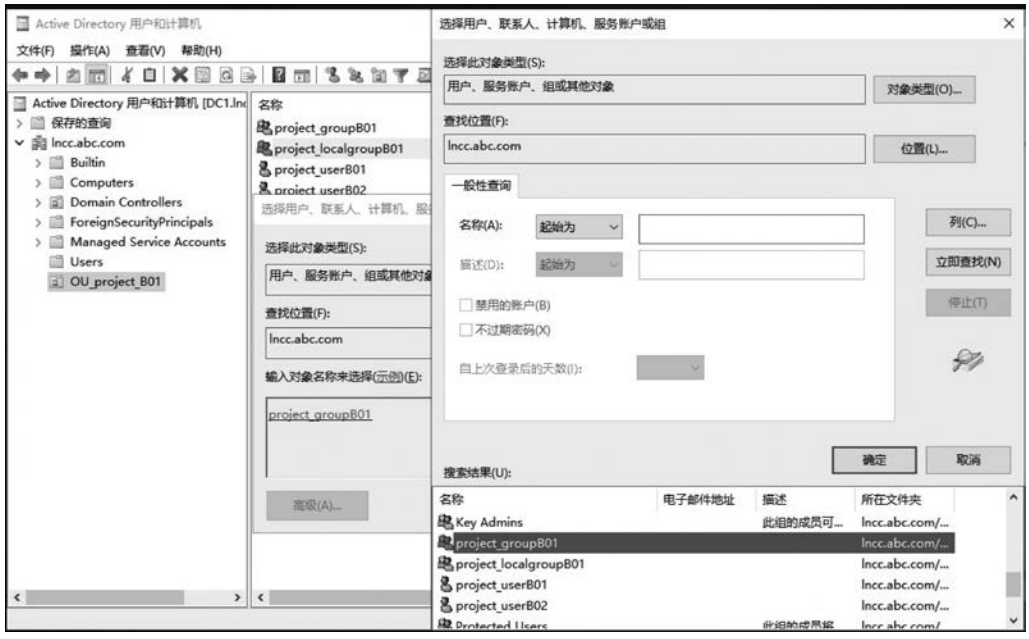

图 3.66 “选择用户、联系人、计算机、服务账户或组”对话框(3)

(8) 在“选择用户、联系人、计算机、服务账户或组”对话框中，单击“立即查找”按钮，选择要加

的全局组域 project_groupB01，单击“确定”按钮，返回“选择用户、联系人、计算机、服务账户或组”，如图 3.67 所示，单击“确定”按钮，返回“project_localgroupB01 属性”对话框，如图 3.68 所示。

图 3.67　添加组

图 3.68　“project_localgroupB01 属性”对话框

(9) 在“project_localgroupB01 属性”对话框中，单击“确定”按钮，返回“Active Directory 用户和计算机”窗口，完成本地域组的添加，如图 3.69 所示。

(10) 在父域控制器 SERVER-01 上，创建组织单位 OU_project_A01；创建总公司项目部用户账户 project_userA01、project_userA02；创建全局组 project_groupA01；将总公司项目部用户账

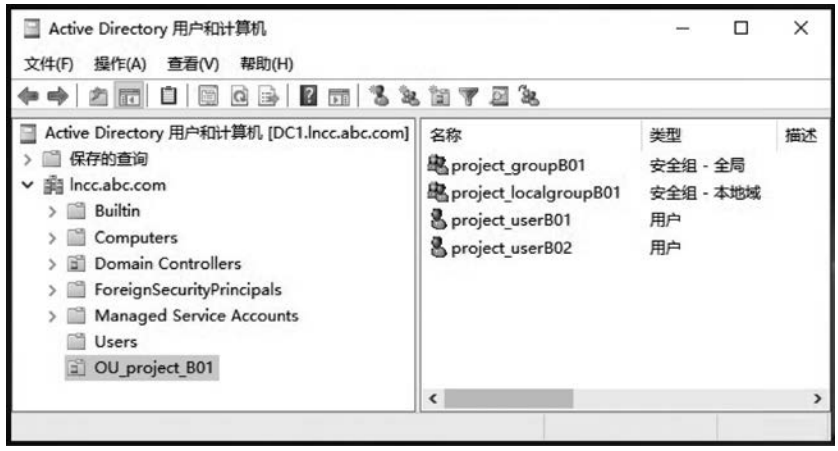

图 3.69　组织单位 OU_projectB01 添加成功

户 project_userA01、project_userA02 加入全局组 project_groupA01 中，其创建过程与子域控制器 DC1 创建过程相似，这里不再赘述。

（11）在子域控制器 DC1 上创建共享目录 project_share01，右击该目录，在弹出的快捷菜单中选择“属性”选项，弹出“project_share01 属性”对话框，如图 3.70 所示，选择“共享”选项卡，在“网络路径”区域，单击“共享”按钮，弹出“网络访问”对话框，如图 3.71 所示。

图 3.70　“project_share01 属性”对话框

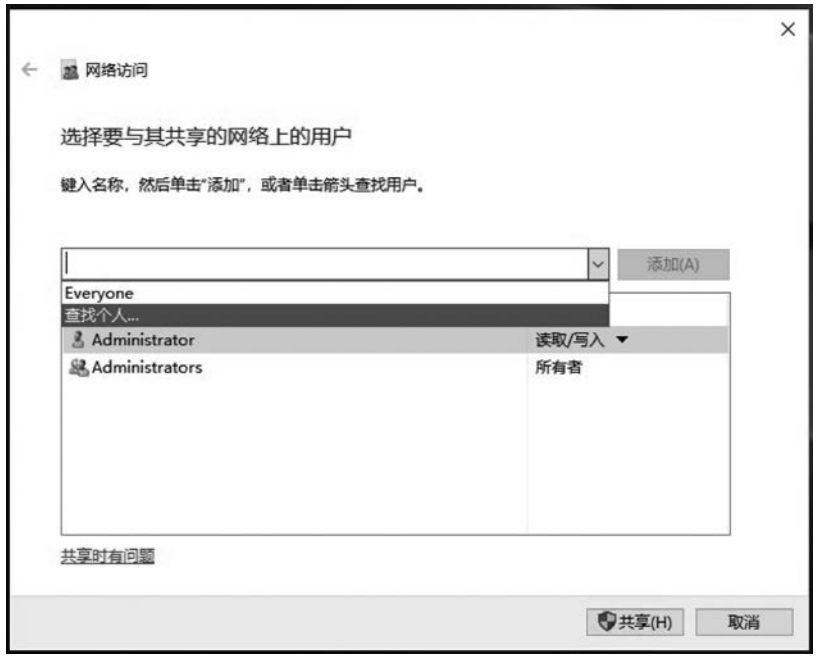

图 3.71　"网络访问"对话框

(12) 在"网络访问"对话框的下拉列表中选择"查找个人…"选项，找到本地域组 project_localgroupB01 并添加，将读写的权限赋予该本地域组，如图 3.72 所示；单击"共享"按钮，弹出"你的文件夹已共享"对话框，单击"完成"按钮，完成共享目录的设置，如图 3.73 所示。

图 3.72　设置共享目录权限

(13) 测试验证结果。在 Win10 客户端上(DNS 服务器地址必须设置为 192.168.100.100 和

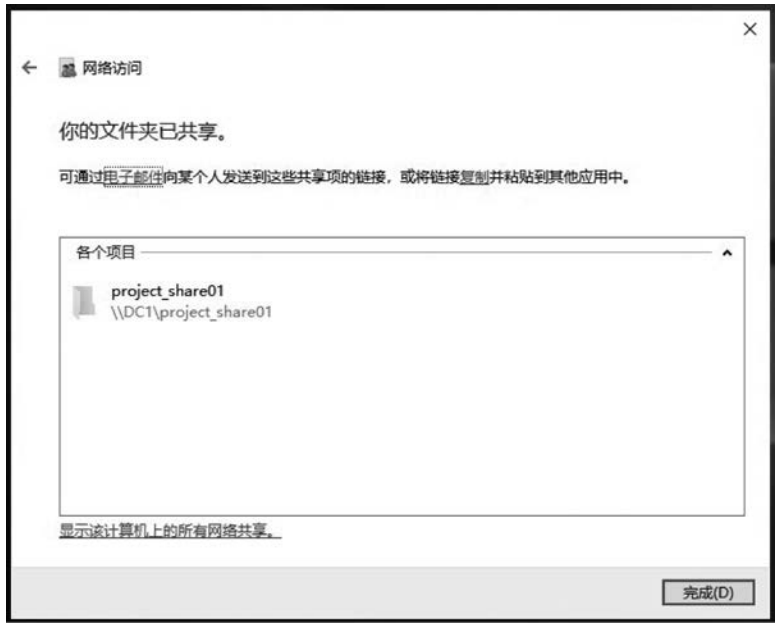

图 3.73　完成共享目录的设置

192.168.100.101)，如图 3.74 所示；使用 Win＋R 组合键，打开“运行”对话框，如图 3.75 所示；输入打开\\DC1.lncc.abc.com\project_share01 路径，弹出“输入网络凭据”对话框，如图 3.76 所示。

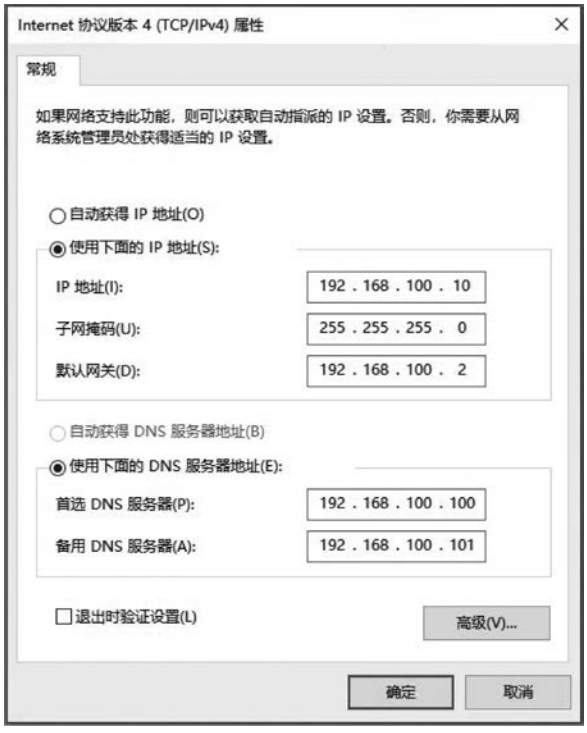

图 3.74　DNS 服务器地址设置

图 3.75　“运行”对话框

图 3.76　“输入网络凭据”对话框

(14) 使用分公司域用户账户 project_userB01@lncc. abc. com\和总公司域用户账户 project_userA01@abc. com\分别访问\\DC1. lncc. abc. com\project_share01 共享目录,如图 3.77 所示。

注意:

测试用户账户需要设置访问权限,否则无法访问。为了测试成功,可以将测试用户账户添加管理员 Administrator 权限进行测试。

(15) 再次注销 Win10 客户端。重新登录后,使用总公司域用户账户 userA03@abc. com 访问\\DC1. lncc. abc. com\project_share01 共享目录,提示没有访问权限,如图 3.78 所示,因为 userA03 用户账户不是项目部用户。

图 3.77　访问共享目录

图 3.78　提示没有访问权限

课后习题

1. 选择题

（1）在 Windows 操作系统中，类似于“S-1-5-21-5789120546-2054893054-5105896483-500”的值代表的是（　　）。

A. UPN　　B. SID　　C. DN　　D. GUID

（2）下面不是 Windows Server 2019 的系统进程的是（　　）。

A. services.exe　　B. svchost.exe　　C. csrss.exe　　D. iexplorer.exe

2. 判断题

（1）Windows Server 2019 支持两种用户账户：本地账户和域账户。（　　）

（2）Windows Server 2019 的 Guest 账户，默认是启用的。（　　）

（3）Windows Server 2019 每个用户账户的安全标识符(SID)是唯一的。（　　）

（4）在“运行”对话框中输入 gpedit.msc 命令，可以打开“本地组策略编辑器”对话框。（　　）

（5）winlogon.exe 进程用于管理用户登录窗口。（　　）

3. 简答题

（1）简述安全标识符(SID)的作用。

（2）简述组作用域。

（3）简述系统的关键进程。