

# 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。

文件(F) 操作(A) 查看(V) 帮助 ◆ ◆ │ ② □ ↓ □ │ × □	i(H) ] ] ] ] ] [] [] [] [] [] [] [] [] [] []	17 2 %		
Active Directory 用户和计算机	名称	类型	描述	^
> 🛄 保存的查询	🕹 Administrator	用户	管理计算机(域)的内置账户	
✓ m abc.com	Allowed RODC Password	安全组 - 本地域	允许将此组中成员的密码复制到域	
> 🛗 Builtin	Cert Publishers	安全组 - 本地域	此组的成员被允许发布证书到目录	
> Computers	Cloneable Domain Contr	可以克隆此组中作为域控制器的成		
> Domain Controllers	Benied RODC Password	安全组 - 本地域	不允许将此组中成员的密码复制到	
> ForeignSecurityPrincip:	A DnsAdmins	安全组 - 本地域	DNS Administrators 组	
> Managed Service Accc	A DnsUpdateProxy	安全组 - 全局	允许替其他客户端(如 DHCP 服务器	
Users	🗟 Domain Admins	安全组 - 全局	指定的域管理员	
	Bomain Computers	安全组 - 全局	加入到域中的所有工作站和服务器	
	ADomain Controllers	安全组 - 全局	域中所有域控制器	
	👪 Domain Guests	安全组 - 全局	域的所有来宾	
< >	B Domain Users	安全组 - 全局	所有域用户	~

图 3.1 "Active Directory 用户和计算机"窗口

🗲 🗧 🕶 Activ	ve D	irectory 管理中/	۲۰۰	abc (本地)・Users	• ②   管理 帮助
Active Director	< U	sers (23)			任务
		本之生而著	Q		Administrator
■ 积还 〒 abc (本地)	3	名称	类型	描述	重置密码
Users 動 动志访问控制 動 身份验证 の 全局捜索		Administrator Allowed RODC Passwor Cert Publishers Cloneable Domain Cont Denied RODC Password DnsAdmins	用户 组 组 组 组	管理計算机(域)的內容條戶 允许将此組中成员的密码 此組的成员被允许发布证 可以克隆此組中作为域控 不允许将此組中成员的密 DNS Administrators 组	▲ 添加到道… 参用 一 一 一 一 一 一 一 一 一 一 一 一 一
	用电修描	中登录时间: Administrator 宁登录时间: 2022/7/23 9:37 波时间: 2022/7/23 9:37 述: 管理计算机(域)的内置账户		过期时间: 《永不》 上次登录时间: 2022/7/23 9:37	新建 删除 在读节点下搜索 屬性

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。

远 选择管理员: C:\Windows\system32\cmd.exe			- □ >	<
C:\>whoami /all				í
用户信息				
用户名    SID				
abc\administrator S-1-5-21-1579156064-3593	====== 690468-	========== 2403083977-500		
组信息		•		
组名	类型	SID	属性	
	=====			
Everyone 白田工師社) 白田台4日	已知组	S-1-1-0	必需的组,	
后用了款队,后用的组 BUILTIN\Users 白田台49	别名	S-1-5-32-545	必需的组,	
后用丁款队,后用的组 BUILTINAdministrators	别名	S-1-5-32-544	必需的组,	
后用丁默认,后用的组,组的所有者 BUILTIN\Pre-Vindows 2000 Compatible Access	别名	S-1-5-32-554	必需的组,	
后用丁默认,后用的组 NT_AUTHORITY\INTERACTIVE	已知组	S-1-5-4	必需的组,	
启用于默认,启用的组 CONSOLE LOGON 启用于默认、启用的组	已知组	S-1-2-1	必需的组,	,

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。

◆ →   2 🗊   Q 🕞   🛛					
團 计算机管理(本地)	名称	描述	^	操作	
◇ ☆ 系统工具	Access Control Assistance Operators	此组的成员可以远程查询此计算		组	+
<ul> <li>▷ 任务计划程序</li> <li>&gt; 圖 事件查看器</li> <li>&gt; 國 共享文件夹</li> <li>&gt; 國 共享文件夹</li> <li>&gt; 圖 用户</li> <li>□ 用户</li> <li>□ 須</li> <li>&gt; ⑩ 性能</li> <li>▲ 设督管理器</li> <li>&gt; 遵 矽indows Server 留份</li> <li>클 磁盘管理</li> <li>&gt; 副 服务和应用程序</li> </ul>	響 Administrators 響 Backup Operators 響 Certificate Service DCOM Access 響 Cryptographic Operators 響 Device Owners 響 Distributed COM Users 響 Event Log Readers 響 Guests 響 Hyper-V Administrators 響 IIS_IUSRS 響 Network Configuration Operators 響 Performance Log Users	管理员对计算机/域有不受限制的 备份操作员为了备份或还原文件 允许该组的成员连接到企业中的 援权成员执行加密操作。 此组的成员可以更改系统范围内 成员允许启动、激活和使用此计 此组的成员可以从本地计算机中 按默认值,来宾跟用户组的成员 此组的成员拥有对 Hyper-V 所有 Internet 信息服务使用的内置组。 此组中的成员有部分管理权限来 该组中的成员可以计划进行性能	~	更多.	

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。

文件(F) 操作(A)	查看(V) 帮助	)(H) С С С	00820	T 2 %		
<ul> <li>Active Directory</li> <li>※ 保存的查询</li> <li>※ 静 abc.com</li> <li>Builtin</li> <li>※ Comp</li> <li>※ Doma</li> <li>※ Doma</li> <li>※ Foreig</li> <li>※ Manaç</li> <li>※ Users</li> </ul>	(用户和计算机) 查找(I) 新建(N) 所有任务(K) 查看(V)	名称 建 Acces 建 Accou	送型     ss Con 安全组 - 本地域     int O 安全组 - 本地域     istrat 安全组 - 本地域         かの 奈全组 - 本地域         计算机         損         InetOrgPerson         用户	描述 此组的成员可以远程查 成员可以管理域用户和 管理员对计算机/域有不 每份操作员为了备份或 该组的成员连接到 成员执行加密操作。 允许启动、激活和 的成员可以从本地		Î
	刷新(F) 导出列表(L) 雇性(R) 帮助(H)	A Perfo	安全组 - 本地域 -V A 安全组 - 本地域 -RS 安全组 - 本地域 ng F 安全组 - 本地域 rrk C 安全组 - 本地域 rmanc 安全组 - 本地域 rmanc 安全组 - 本地域	<ul> <li>按默认值,未真跟用户</li> <li>此组的成员拥有对 Hyp</li> <li>Internet 信息服务使用</li> <li>此组的成员可以创建到</li> <li>此组中的成员有部分答</li> <li>该组中的成员可以计划</li> <li>此组中的成员可以计划</li> </ul>		
<	>	Pre-W	Vindo 安全组 - 本地域	允许访问在城中所有用		

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。

	X 🛛 🗙 🖸	0	801881	17 <u>2</u> 2			
<ul> <li>Active Directory 用户和计算机</li> <li>○ 保存的查询</li> <li>◇ 論 abc.com</li> <li>○ Builtin</li> <li>&gt; ○ Computers</li> <li>&gt; ○ Domain Controllers</li> <li>&gt; ○ ForeignSecurityPrincip:</li> <li>&gt; ○ Managed Service Accco</li> </ul>		名称 各Admi 融Allow	nistrator ed RODC Password.	类型 用户 安全组 - 本地域	描述 管理计算机(域)的内置账户 允许将此组中成员的密码复制到域…		
		思 Cert I 思 Clone 思 Denie 思 DnsA 思 DnsU	Publishers eable Domain Contr ed RODC Password dmins pdateProxy	安全组 - 本地域 · 安全组 - 全局 · 安全组 - 本地域 安全组 - 本地域 安全组 - 本地域 安全组 - 全局	此組的成员被允许发布证书到目录 可以克隆此组中作为域控制器的成… 不允许将此组中成员的密码复制到… DNS Administrators 组 允许替其他客户端(如 DHCP 服务器…		
Users 委派控制(E 查找(I)	委派控制(E) 查找(I)		in Admins in Computers	安全组 - 全局 安全组 - 全局 安全组 - 全局	指定的城管理员 加入到城中的所有工作站和服务器		
	新建(N) 所有任务(K) 查看(V)	> > >	计算机 联系人 组	lential ePropertyList	5777月3-362143月8日 的所有来宾 与城用户 业的指定系统管理员		
刷新(F) 导出列表(L)	刷新(F) 导出列表(L)		InetOrgPerson msDS-KeyCred msDS-Resourc		目的成员可以对林中的密钥对象… 目的成员是企业中的只读域控制器 个组中的成员可以修改域的组策略		
厪性(R) 帮助(H)			msDS-Shadowi msImaging-PSI	PrincipalContainer Ps z	来宾访问计算机或访问域的内置 目的成员可以对域中的密钥对象		
		RAS Read Sche	打印机 用户 共享文件夹	-	个组中的服务器可以访问用户的 自中的成员是域中只读域控制器 勾的指定系统管理员		

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。



Active Directory 用户和计算机	名称	类型	描述
<ul> <li>→ Every Substrate Device Accom</li> <li>→ Builtin</li> <li>→ ○ Computers</li> <li>→ ○ Domain Controllers</li> <li>&gt; ○ ForeignSecurityPrincip.</li> <li>&gt; ○ Managed Service Acco</li> <li>○ Users</li> </ul>	Administrator Allowed RODC Pass Cert Publishers Cloneable Domain ( Denied RODC Passv DinsAdmins DinsUpdateProxy Domain Admins	11日 「添加型组(G) 禁用帐户(S) 重置密码(E) 移动(V) 打开主页(C) 发送邮件(A)	管理计算机视频的改直称户 允许将此组中成员的密码复制到域… 此组的成员被允许发布证书到目录 可以克整此组中作为域控制器的成… 不允许将此组中成员的密码复制到… DNS Administrators 组 允许替其他客户端(如 DHCP 服务器… 指定的域管理员
	Domain Computers     Domain Controllers     Domain Guests     Domain Users     Domain Users     Enterprise Admins	所有任务(K) >	复制(C)
		剪切(T) 删除(D) 重命名(M)	添加到組(G) 禁用账户(S) 重置密码(E)
	Enterprise Key Adm	履性(R)	参切(V) 打开主页(O)
	Enterprise Read-onl	帮助(H)	发送邮件(A)
	Suguest Key Admins Protected Users RAS and IAS Servers Read-only Domain Con Schema Admins	用户 安全组 - 全局 安全组 - 全局 安全组 - 全局 安全组 - 本地域 tr 安全组 - 全局 安全组 - 通用	策略的结果集(正在计划)(P) 策略的结果集(正在记录)(L) 此组的成员将受到针对身份验证安 这个组中的服务器可以访问用户的 此组中的成员是城中只读城控制器 架构的指定系统管理员

图 3.8 指定用户相关操作

环境	<u></u>	e l	远程控制	沅程卓	面服务配置	文件	COM+	环境	会活		沅程控制	沅程卓丽	前服务配置	文件	COM
常规	地址	账户	配置文件	电话	组织	隶属于	拨入	常规	地址	账户	配置文件	电话	组织	隶属于	援)
								用白斑	3-0/IN.						
8	Adm	inistrate	or						米白(0):						~
							_		Bergar 1-	200					
姓(L):									来者(Windo	ws 200	10以削成本)(1	v): Administr	ator		_
								, and the second				Administr			
名(F):					英文缩与(	l):		登	景时间(L)		登录到(T)	£ 1			
显示名称	称(S):														
描述(D)	):	营	理计算机(域)的	内置账户				□解	劃账户(N)						
anna an							=								
办公室(	(C):							账户选	项(0):						
									用户下次登录	时须更	政密码				î
电话号	码(T):	[     ]     [     ]     ]     ]     ]     ]     [     ]     ]     ]     ]     ]     ]     [     ]     ]     ]     ]     [     ]     ]     ]     [     ]     ]     [     ]     ]     [     ]     ]     [     ]     ]     [     ]				其他((	D)		制户不能更改 を空きてけ期	密码					
由子郎	et/Mi-								更用可逆加速	, 存储密	码				
-6.1 MPI	14(11)-						_								~
网页(W	Ŋ:					其他(	R)	• 账户	过期						
								۲	永不过期(V)						
								0	至这之后(E):	2	022年 8月22	E		1	<b>*</b>

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。

► =>   @ 📰   X 🗉   X 🗉	0 3 2 5 8	* 11 7 2 %			
<ul> <li>Active Directory 用户和计算机</li> <li>● 保存的查询</li> <li>● 課題 abc.com</li> <li>● Builtin</li> <li>&gt; ● Computers</li> <li>&gt; ● Domain Controllers</li> <li>&gt; ● ForeignSecurityPrincips</li> <li>&gt; ● Managed Service Accc</li> <li>■ Users</li> </ul>	名称 Administrator 楽 Allowed RODC Passw 楽 Cert Publishers 楽 Coneable Domain C 楽 Denied RODC Passw 楽 DnsAdmins 楽 DnsUpdateProxy 楽 Davus Patrice	类型 用户 vord 安全组 - 本地域 安全组 - 本地域 安全组 - 全局 ord 安全组 - 全局 ord 安全组 - 本地域 安全组 - 本地域 安全组 - 本地域 安全组 - 全局	描述 管理计算机(域)的内置账户 允许将此组中成员的密码复制到域 此组的成员被允许发布证书到目录 可以克隆此组中作为域控制器的成 不允许将此组中成员的密码复制到 DNS Administrators 组 允许替具他态户演(如 DHCP 服务器		
	Domain Admins Domain Compute Domain Controlle	<u>女主祖 - 主向</u> 添加到组(G) 移动(V) 发送邮件(A)	有短时或后进员 加入到域中的所有工作站和服务器 域中所有域控制器 域的所有来真		
	Domain Users     Enterprise Admin     Enterprise Key Ac     Enterprise Read-	所有任务(K) > 剪切(T) 删除(D)	添加到組(G) 移动(V) 密钥对象 发送邮件(A) 读域控制器		
	Croup Policy Crea Guest Key Admins	重命名(M) <b>属性(R)</b>	这个组中的成员可以修改域的组策略 供来宾访问计算机或访问域的内置 此组的成员可以对域中的密钥对象		
	Arotected Users RAS and IAS Servers Read-only Domain C Schema Admins	帮助(H) 安全组 - 本地域 ontr安全组 - 全局 安全组 - 通用	此组的成员将受到针对身份验证安 这个组中的服务器可以访问用户的 此组中的成员是域中只该域控制器 架构的指定系统管理员		

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。



翻 管理员: C:\Windows\system32\cmd.exe				-		×
C:\>whoami /groups						^
组信息						
组名	类型	SID	属性			
					12000	
Everyone	已知组	S-1-1-0	必需的组,	启用-	于默认,	启
用的组 BUILTIN\Users ■約組	别名	S-1-5-32-545	必需的组,	启用	于默认,	启
BUILTIN\Administrators 用約組 组的所有者	别名	S-1-5-32-544	必需的组,	启用	于默认,	启
BUILTIN\Pre-¥indows 2000 Compatible Access 開始組	别名	S-1-5-32-554	必需的组,	启用	于默认,	启
NT AUTHORITY\INTERACTIVE 用的组	已知组	S-1-5-4	必需的组,	启用	于默认,	启
CONSOLE LOGON 用的组	已知组	S-1-2-1	必需的组,	启用	于默认,	启
NT_AUTHORITY\Authenticated Users	已知组	S-1-5-11	必需的组,	启用	于默认,	启
NT AUTHORITY\This Organization	已知组	S-1-5-15	必需的组,	启用	于默认,	启
LOCAL B 654B	已知组	S-1-2-0	必需的组,	启用	于默认,	启
ABC\Domain Admins	组	S-1-5-21-1579156064-3593690468-2403083977-512	必需的组,	启用	于默认,	启、

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。



#### 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。

安全设置         策戶策略           ● 数户策略         > 圖 密码集略           > 圖 账户锁定策略         圖 密码是短使用期限           > 圖 Kerberos 策略         圖 密码最短使用期限           ■ 本地策略         圖 密码最短使用期限           ■ 本地策略         圖 密码最近使用期限           ■ 本地策略         圖 密码最长使用期限           ■ 成功安全 Windows Defender 防火t         圖 强制密码历史           ■ 网络列汞管理器策略         公捐策略           ○ 公捐策略         应用程序控制策略           ◎ 应用程序控制策略         [] 原安全策略, 在本地计算机	安全设置 已启用 7 个字符 1 天 42 天 24 个记住的密码 已禁用

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。

文件(F) 操作(A) 查看(V) 帮助(H)		
■ 本地計算机 策略         ▲           > ● 計算机配置         ●           > ● 数件设置         ●           ● ● 日都署的打印机         ●           > ● ● 日都署的打印机         ●           > ● ● 医学会设置         ●           > ● ● 素安全设置         ●           ● ● 医素の素略         ●           ● ● 素安全设置         ●           ● ● 素安全设置         ●           ● ● 素の安全公園業略         ●           ● ● 素の安全全 Windows Defeneeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee	第略 二章 密码必须符合复杂性要求 二章 密码长度最小值 二章 密码最近使用期限 二章 密码最长使用期限 二章 密码最长使用期限 二章 强制密码历史 二章 用可还原的加密未储存密码	安全设置 已启用 7 个字符 1 天 42 天 24 个记住的密码 已禁用
< >	<	>

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。

本地安全策略 文件(F) 操作(A) 查看(V) 帮助(H)		-	×
◆ → ≥ ः × = ≥ ≥			
■ 安全设置 ^ > □ 账户策略 > □ 密闭策略 ○ 账户的中等略	策略 ^	安全设置 30 分钟 3 次无效登录	
▲ 和// 和// 和// 和// 和// 和// 和// 和// 和// 和/	123 重置账户锁定计数器	30 分钟之后	
< >	<u> </u>		

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。

唐》计算机管理 文件(F)操作(A)查看(V) ◆ ●   ▲   面   ★ 🗐 🔒	8助(H)		-		×
小算机管理(本地)	名称	全名	描述	操作	_
> ○ 系統工具 > ○ 任务计划程序 > ○ 年务计划程序	Administrator	设置密码(S)	管理计算机(域)的内置制 系统管理的用户账户。	用户 更多	•
> 國 共享文件夹	Guest	所有任务(K)	〉供来宾访问计算机或访 系统力 Windows Data	Administr.	
✓ 基本地用户和组 ○ 用户	EL WDAGUBIRYACCOURT	删除(D) 重命名(M)	35072/3 Windows Dere	更多	•
2 组		<b>属性(R)</b>			
> (2) 住能 書 设备管理器		帮助(H)			
> 曾存储 、	<		>		

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。

№ 任务管理器				
文件(F) 选项(O) 查看(V)				
进程 性能 应用历史记录 启动	用户 详细	暗息 服务		
名称	PID	状态	用户名	^
III dwm.exe	78392	正在运行	DWM-7	
S EasyConnect.exe	68380	正在运行	Administrator-001	
ECAgent.exe	95776	正在运行	Administrator-001	
explorer.exe	28792	正在运行	Administrator-001	
explorer.exe	74592	正在运行	Administrator-001	
III FlashHelperService.exe	3684	正在运行	SYSTEM	
III fontdrvhost.exe	676	正在运行	UMFD-0	
HZ_CommSrv.exe	3756	正在运行	SYSTEM	
W knbcenter.exe	10792	正在运行	SYSTEM	
E kxescore.exe	2600	正在运行	SYSTEM	
III Isass.exe	932	正在运行	SYSTEM	
(iii) mspaint.exe	78224	正在运行	Administrator-001	
Smstsc.exe	80832	正在运行	Administrator-001	
M multitin ava	70512	正在法行	Administrator-001	~
<				>

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。

<b>* *</b>   <b>E</b>							
0. 服务(本地)	○ 服务(本地)						
	Certificate Propagation	名称 ^	描述	状态	启动类型	登录为	^
		ActiveX Installer (AxInstSV)	为从		禁用	本地系统	
	启动此服务	AllJoyn Router Service	路由		手动(触发	本地服务	
		App Readiness	当用		手动	本地系统	
	100×-	Application Identity	确定		手动(触发	本地服务	
	将用户证书和根证书从智能卡复制到	Application Information	使用		手动(触发	本地系统	
	当前用户的证书存储,检测智能卡何	Application Layer Gatewa	为 In		手动	本地服务	
	时插入到智能卡读卡器中,并在需要	Application Management	为通		手动	本地系统	
	时安装智能卡即插即用微型影动器。	AppX Deployment Servic	为部		手动	本地系统	
		AVCTP 服务	这是		手动(触发	本地服务	
		Background Intelligent T	使用		手动	本地系统	
		Background Tasks Infras	控制	正在	自动	本地系统	
		Base Filtering Engine	基本	正在	自动	本地服务	
		CaptureService 41d4d	One		手动	本地系统	
		Certificate Propagation	将用		手动(触发	本地系统	
		Client License Service (Cli	提供		手动(触发	本地系统	
		CNG Key Isolation	CNG	正在	手动(触发	本地系统	
		COM+ Event System	支持	正在	自动	本地服务	
		COM+ System Application	管理	正在	手动	本地系统	
		Connected User Experien	Con	正在	自动	本地系统	
		Concontilly Atdad	44.24		≠⇒h	★+#h苯/在	*

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 计算机管理(本地)	<ol> <li> </li></ol>				-		操作	
<ul> <li>※ 計: 3:50.1.2</li> <li>○ 任务计划程序</li> <li>○ 任务计划程序</li> <li>&gt; 圖 非住查看器</li> <li>&gt; 副 共享文件共</li> <li>&gt; 圖 共享文件共</li> <li>&gt; 圖 本地用户印組</li> <li>&gt; ⑥ 性能</li> <li>畫 设备管理器</li> <li>* 督 存結</li> <li>&gt; ⑧ Windows Server 留份</li> <li>一 確 磁管理</li> <li>* 圖 服务和应用程序</li> <li>&gt; ⑤ 路由和远程访问</li> <li>■ 服务</li> <li>■ 副 WMI 控件</li> </ul>	Certificate Propagation 启动此服务 描述: 将用户证书和根证书从智能卡契制到 当前用户的证书存储。检测智能卡何 时插入到智能卡读卡器中,并在需要 时安装智能卡即插即用微型驱动器。	ActiveX Installer (AxInstSV)     ALIJoyn Router Service     App Readiness     Application Identity     Application Information     Application Information     Application Management     ApX Deployment Servic     ApX Deployment Servic     Background Intelligent T     Background Itasks Infras     Background Tasks Infras     Base Filtering Engine     CaptureService_41d4d	<ul> <li>描述 秋志</li> <li>为从</li> <li>路由</li> <li>当用</li> <li>当用</li> <li>清健定</li> <li>传用</li> <li>方通</li> <li>方通</li> <li>方通</li> <li>支通</li> <li>使用</li> <li>使用</li> <li>正在</li> <li>One</li> </ul>	<ul> <li>自动美型</li> <li>禁却(触发</li> <li>手动(触发</li> <li>手动(触发</li> <li>手动(触发</li> <li>手动</li> <li>手动</li> <li>手动</li> <li>手动</li> <li>手动</li> <li>手动</li> <li>自动</li> <li>手动</li> <li>手动</li> </ul>	登本本本本本本本本本本本本本本本本本本本本本本本本本本本本本本本本本本本本本本	*	服务 更多操作 Certificate Prop. 更多操作	
		Certificate Propagation	将用	手动(触发	本地系统			

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。



				3.5	on 管理员: C:\Windows\system32\cmd.exe -		X
常规	登录	恢复	依存关系				
			21 B		C:\>sc /?		
服务律	名称:	Cer	tPropSvc		错误: 未知命令		
显示	名称:	Cer	tificate Propagation		描述・		
描述:		将服務	用户证书和根证书从智能卡复制到当 检测智能卡何时插入到智能卡读十 户装智能卡明新即用微刑吸动路	前用户的证书存	SC 是用来与服务控制管理器和服务进行通信 的命令行程序。 用法: sc <server> [command] [service name] <option1> <option2< td=""><td>&gt;</td><td></td></option2<></option1></server>	>	
可执行	行文件的新	<b>路径:</b>					
C:\W	findows\	system3	2\svchost.exe -k netsvcs		<pre><server> 洗项的格式为 "\\ServerName"</server></pre>		
ch abà		36	<b>a</b>		可通过键入以下命令获取有关命令的更多帮助: ″sc [command]		
10415	天王(E):	手	9) 动(征识启动)		<sub>대</sub> 구: query查询服务的状态,		
		自治	b		或枚举服务类型的状态。		
_		日本	动 田		或枚举服务类型的状态。		
服务机	状态:	ER	РЩ.		start启动服务。 nause		
	启动(5)		· (6)上(1) - 新高(2)	佐賀(R)	interrogate向服务发送 INTERROGATE 控制请求。		
	M-140(0)	_		TODALINI	continue		
当从山	比处启动	<b>段务时</b> ,(	尔可指定所适用的启动参数。		config更改服务的配置(永久)。		
					failure更改失败时服务执行的操作。		
启动	參数(M):				failureflag更改服务的失败操作标志。 sidtyma		
					privs更改服务的所需特权。		
					managedaccount史改服务以将服务账户密码 标记为中 LSA 管理		
			确定 取	5 应用(A)	qc查询服务的配置信息。		
					qdescription查询服务的描述。		

图 3.20 服务的属性对话框

图 3.21 sc 命令的语法格式

技能实践 3.3

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

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。



V3-1



書 计算机管理 文件(F) 操作(A) 查	看(V) 報	助(H)				- 0	×
<ul> <li>審 计算机管理(本地)</li> <li>◇ ╬ 系统工具</li> </ul>		名称 例 Adminis	trator	全名	描述 管理计算机(域)的内置账户	操作用户	•
<ul> <li>② 任务计划程序</li> <li>&gt; 圖 事件查看器</li> <li>&gt; 國 共享文件夹</li> <li>&gt; 墨 本地用户和組</li> </ul>		Default/	trator Account tilityAccount		系统管理的用户账户。 供来宾访问计算机或访问域的内置账户 系统为 Windows Defender 应用程序防护…	更多	·
11 用户	新用户(N	)					
> ⑧ 性能	查看(V)	>	>				
<ul> <li>□ (2) (2) (2) (2) (2) (2) (2) (2) (2) (2)</li></ul>		(L)					
显示当前所选内容的	帮助(H)						

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。

xx\_student01 属性

					远程控制		远程桌面服务配置了	文件	拨入
					常规	隶属于	配置文件	环境	会语
					xx_stu	dent01			
5			?	×	全名(F):	xx_stud	lent01		
名(U):	xx_stu	ident01			描述(D):	xx_stud	dent01		
F):	xx_stu	ident01				+05.00 3/107.00	MD .		
(D):	xx_stu	ident01				5900年100年1月(1 8 <b>码(C)</b>	(4)		
					☑ 密码永不过期(1	P)			
(P):		•••••			□账户已禁用(B)				
密码(C):	[	•••••			□账户已锁定(0)				
户下次登录	时须更改	密码(M)							
户不能更改	(密码(S)								
码永不过期	(W)								
;户已禁用(B	3)								
taBb/i n			A(39(E) #	(FICO)	ſ			-	

图 3.23 "新用户"对话框

图 3.24 "xx_student01	属性"对话框
----------------------	--------

? X

(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。

student01 属性				? ×		
远程控制		远程桌面服务配置文	件	援入		
常规	隶属于	配置文件	环境	会话		
t)尾于(M):						
總 Users					选择组 选择此对 <b>象</b> 关型(S):	_
					f£	对象类型(O)
					查找位置(F):	().
					DC2	位置(L)
		WINT LLT	TE B at a diff.		输入对象名称来选择(示例)(E):	
溙加(D)	删除(R)	系的更改才生效	**************************************	SHAKOX +		检查名称(C)
	确定	取満	成用(A)	帮助	高级(A) 确定	取消

图 3.25 "隶属于"选项卡

(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 3.26 "选择组"对话框

选择组			×
选择此对象类型	<u>뮏(</u> S):		
组			对象类型(O)
查找位置(F):			
DC2			位置(L)
一般性查询			
名称(A):	起始为 ~		歹](C)
描述(D):	起始为 🗸		立即查找(N)
□ 禁用的则	长户(B)		停止(T)
一不过期整	昭(X)		
自上次登录	后的天数(1):		P
搜索结果(U):			确定取消
名称		所在文件夹	^
Access Con	ntrol Assistance Operators	DC2	
Administrat	tors	DC2	
Backup Op	erators	DC2	
Certificate	Service DCOM Access	DC2	~

图 3.27 "一般性查询"对话框

选择组		>
选择此对象类型(S):		
组		对象类型(O)
查找位置(F):		
DC2		位置(L)
输入对象名称来选择(示例)(E):		
DC2\Administrators	[	检查名称(C)
		Benk
高级(A)	開定	取消

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。

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。

(6)"远程控制"选项卡。



近程控制 常规 隶属于		285 A	Contraction of the second seco
TEAN STATE J	近程果闻服労能宜义件 配置文件 II	10 AVE	辺程控制 近程桌面服务配置文件 拨入 愛柳 静厚子 和端立件 环境
	PRAERIC IT SP	98 Z.HA	4676 30.66 HUHLX1+ A176 2010
用户配置文件			使用这一选项卡配置远程桌面服务启动环境。这些设置会替代客户请所指定的
配置文件路径(P):			
登录開木(I)·			
32.868e-+-(c).			□ 登录时启动下列程序(S):
			程序文件名(P):
E文件夹			
④本地路径(O):			开始位置():
○连接(C): Z:	─ 到(T):		
			- 客白读设备
			▼ 豆束可注接音广频起动器(C)
			▼ 並来引起來者/ 第5100(C)
			· TANANGALILAI BUINNANDI
<b>施定</b> 图 3.29	<b>戰 國</b> "配置文件"选	用(A) 帮助 项卡	· · · · · · · · · · · · · · · · · · ·
确定 图 3.29 udent01 属性	<b>戰 应</b> "配置文件"选	用(A) 帮助 项卡 ? ×	施定 取满 应用(A) 報 图 3.30 "环境"选项卡 xx_student01 Late ?
确定       图 3.29       udent01 厘性       远程控制       常規	取消         应           "配置文件"选。           远程桌面服务配置文件           配置文件	用(A) 帮助 项卡 ? × 扱入 逸 会話	施定         取満         应用(A)         報告           图 3.30         "环境"选项卡           xx_student01 屬性         ?           常规         表属于         配置文件         环境         会话           远程控制         远程桌面服务配置文件         援入
确定           图 3.29           udent01 屬性           远程控制           常規         隶屬于           用此选项卡设置远程桌面服务;	取満         应           "配置文件"选:            远程桌面服务配置文件            配置文件         环           超时和重新连接设置	用(A) 帮助 项卡 ? × 拨入 境 会话	施定         取満         应用(A)         報道           图 3.30         "环境"选项卡           Xx_student01 屬性         ?           第總         東展子         配置文件         环境         会話           远程控制         远程控制         远程空間         资格           更完成的中国政策和自动会話         法国际场和运行的会話         正常可知道家用的公式         正常可知道家用的公式
機定       图 3.29       udent01 屬性       近程控制       第規       東屬子       用此选项卡设置近程桌面服务;	取消         应           "配置文件"选。           远程桌面服务配置文件           配置文件           取消	用(A) 帮助 项卡 ? × 扱入 逸 会話	确定         取満         应用(A)         報酬           图 3.30         "环境"选项卡           图 3.30         "环境"选项卡           家x_student01 屬性         ?           常规         東屋子         配置文件         环境         会活           近程控制         近程点面服务近程注制设置。         要近程控制或观察用户的会话。选择下列复选框:
确定           图 3.29           udent01 厘性           远程控制           第現<東陽子	取消         应           "配置文件"选:            远程桌面服务配置文件         正置文件           配置文件         环           超时和重新连接设置	用(A) 帮助 项卡 ? × 授入 境 会话	确定         取滿         应用(A)         種目           图 3.30         "环境"选项卡           图 3.30         "环境"选项卡           xx_student01 屬性         ?           常规         隶属于         配置文件         环境         会話           近程控制         近程直面服务配置文件         援入         使用这一透项卡配置远程桌面服务远程控制设置。           要远程控制或观察用户的会话。选择下列复选框:         了         自用远程控制(E)
确定           图 3.29           udent01 屬性           远程控制           第現<東陽子	取満         应           **配置文件"选。           远程桌面服务配置文件           配置文件           部時和重新连接设置	用(A) 帮助 项卡 ? × 授入 違 会话	确定         取滿         应用(A)         種目           图 3.30         "环境"选项卡           图 3.30         "环境"选项卡           家x_student01 屬性         ?           常規         東居于         配置文件         环境         会话           近程控制         近程盒面服务配置文件         援入         使用這一透環卡配置远程盒面服务远程控制设置。           要远程控制或现象用户的会话。选择下列复选框:         厂         启用远程控制(E)           若要申请用户的权限以控制或观察会话。请选择下列复选框:
确定           图 3.29           odent01 屬性           远程控制           常規         隶屬于           田此选项卡设置远程桌面服务;           東已漸开的会话(E):           协会法限制(T):	取消         应           "配置文件"选。           远程桌面服务配置文件           配置文件           部时和重新连接设置           从不	用(A) 帮助 项卡 ? × 授入 違 会话	施定         取満         应用(A)         種目           图 3.30         "环境"选项卡           图 3.30         "环境"选项卡           家x_student01 屬性         ?           常規         東居于         配置文件         环境         会話           近程控制         近程盧面服务配置文件         現入         使用这一选项卡配置远程桌面服务远程注制设置。           要远程控制或观察用户的会话,选择下列复选框:         厂         启用远程控制(E)           若要申请用户的权限以控制或观察会话,请选择下列复选框:         C. 需要用会比可(P)
确定           图 3.29           udent01 届性           远程控制           第規         隶属于           用此选项卡设置远程桌面服务;           東已断开的会话(t):           动会话限制(T):           利会话限制(0):	取消     应       **配置文件"选。       远程桌面服务配置文件       配置文件       环       超时和重新连接设置       从不       从不       从不	用(A) 帮助 项卡 ? × 機入 違 会活	施定         取満         应用(A)         報           图 3.30         "环境"选项卡           图 3.30         "环境"选项卡           家x_student01 屬性         ?           常規         東屋子         配置文件         环境         会話           近程控制         近程桌面服务范程控制设置。         要远程控制或观察用户的会话。选择下列算选框:         ?           「 启用远程控制(E)         若要申请用户的权限以控制或观察会话。请选择下列算选框:         「 需要用户许可(R)           计如时用目         ************************************
機定           (至] 3.29           udent01 屬性           远程控制           這程控制           第規         隶屬于           用此选项卡设置远程桌面服务;           東已劃所的会话(E):           动会话限制(T):	取満         应           "配置文件"选:            远程桌面服务配置文件            版置文件         环           超时和重新连接设置            从不            从不	用(A)	施定         取満         应用(A)         報           图 3.30         "环境"选项卡           图 3.30         "环境"选项卡           家student01 屬性         ?           常規         東羅子         配置文件         环境         会話           近程空地         近程空間服务运程注制设置         ?
機定           图 3.29           udent01 屬性           远程控制           這程控制           第級           東圖子           用此选项卡设置远程桌面服务;           東已斷开的会话(E):           动会话限制(1):           制会话限制,或者连接被中断;	取満         应           ** 配置文件**选:            远程桌面服务配置文件            配置文件            超时和重新连接设置            从不            从不            成年	用(A)	施定         取満         应用(A)         種類           图 3.30         "环境"选项卡           图 3.30         "环境"选项卡           家_student01 屬性         ?           常规         東羅子         配置文件         环境         会話           近程控制         远程桌面服务运程控制设置。         要运程控制或观察用户的会话。选择下列复选框:         ?           使用这一选项卡配置远程桌面服务运程控制设置。         要运程控制或观察会话。请选择下列复选框:         ?           定 雇用远程控制(E)         若要申请用户的权限以控制或观察会话。请选择下列复选框:         ?           定 需要用户许可(R)         控制级别         通信思想使用的控制用户会话的级别         ()         查看用户会话(M)
确定           图 3.29           udent01 屬性           近程控制           第規         隶屬于           用此选项卡设置远程桌面服务;           東已斷开的会话(E):           动会话限制(T):           現会话限制,或書连接被中朝           「           人会话斷开(D)           会话限制(D)	取満     应       ** 配置文件**选:       远程桌面服务配置文件       配置文件       振置文件       原       人不       人不       人不       小不       時:	用(A)	施定         取満         应用(A)         種類           图 3.30         "环境"选项卡           图 3.30         "环境"选项卡           家_student01 屬性         ?           常规         東属子         配置文件         环境         会話           近程控制         远程桌面服务近程控制设置。         要远程控制或观察用户的会话。选择下列复选框:         ?           使用这一述项卡配置远程桌面服务远程控制设置。         要远程控制或观察会话。 遗选择下列复选框:         ?           「 雇用远程控制(E)         若要申请用户的权限以控制或观察会话。 遴选择下列复选框:         ?           「 定 需要用户许可(R)         控制级别         近程要要使用的控制用户会流的级别         ?           「 空 需要用户会运(V)         ①         会流的政治         ?
機定           [图] 3.29           udent01 屬性           远程控制           這程控制           第7組           東居于           申此选项卡设置远程桌面服务;           東已斷开的会话(E):           助会话限制(1):           約会话限制,或者连接被中断 (○ 从会话斷开(D)           ○ 始束会话(S)	取満     应       **配置文件"选:       法程桌面服务配置文件       配置文件       振置文件       小不       以不       以不       以不       時:	用(A)	施定         取満         应用(A)         構成           図 3.30         "环境"选项卡           図 3.30         "环境"选项卡           図 3.30         "环境"选项、           家         家場         家場           家場         家屋子         配置文件         环境           遊程空刻         近程桌面服务批型注制设置。         委託         委託           受活程控制或观察用户的会活、选择下列复选框:         「         自用远程控制(E)            若要申请用户的权限以控制或观察会话、请选择下列复选框:         「         業要用户许可(R)           控制级制         」             「 定想要使用的控制用户会法的级别         (* 告書用户会话(V)             (* 与会运互动()
确定           图 3.29           udent01 屬性           远程控制           第規           東居丁           用此选项卡设置远程桌面服务;           東巳新开的会话(E):           动会话限制(T):           現会话限制(I):           到会话限制,或者连接被中新           ○ 从会话斯开(D)           ○ 结束会话(S)	取満     应       **配置文件**选:       法程桌面服务配置文件       配置文件       水石       以不       以不       以不       以不	理(A)	施定         取満         应用(A)         構成           図 3.30         "环境"选项卡           図 3.30         "环境"选项卡           図 3.30         "环境"选项卡           家         東属           家         東属           配置文件         环境           空程空刻         近程桌面服务近程注制设置。           要远程控制或观察用户的云流、选择下列复选框:            「 启用远程控制(C)         若要申请用户的衣服以控制或观察会话、请选择下列复选框:           「 需要用户许可(R)            推定想要使用的控制用户会法的级别         (* 与会适互动(*)
機定           限 3.29           udent01 庫性           远程控制           第規           東田开           用此透明卡设置远程桌面服务;           東日斯开的会话(E):           动会话限制(T):           湖会话限制(T):           到会话限制(T):           到会话限制(T):           到会话限制(T):           第二、公式電気制(D):           計畫新主接後中朝新           (* 从会话期开(D)           「 结束会话(S)           許重新主接。	取消     应       **配置文件"选:       法程桌面服务配置文件       配置文件       环       週初和重新连接设置       以不       以不       以不       時:	)用(A)	施定         取満         应用(A)         和           图 3.30         "环境"选项卡           图 3.30         "环境"选项           家_student01 屬性         ?           常規         東屋子         配置文件         环境         公括           近程控制         近程直期服务配置文件         現入             使用这一透现卡配置远程桌面服务远程控制设置。         要远程控制或观察用户的会话。选择下列复选框:              戶 启用远程控制(F)         若要申请用户的反限以控制或观察会话。请选择下列复选框:               近程度制用户的公式的成别
機定           (茶) 3.29           tudent01 屬性           近程控制           第規<東属子	取消     应       **配置文件"选:       法程桌面服务配置文件       配置文件       死置文件       原       以不       以不       以不       以不	用(A) 帮助 项卡 ? × · · · · · · · · · · · · · · · · · · ·	施定         取満         应用(A)         構成           図 3.30         "环境"选项卡           図 3.30         "环境"选项卡           図 3.30         "环境"选项下表           第         ?           第         2           第         2           第         2           第         2           第         2           第         2           第         2           2         2           2         2           2         2           2         2           2         2           2         2           2         2           2         2           2         2           2         2           2         2           2         2           2         2           2         2           2         2           2         2           3         3           3         3           3         3           3         3           3         3           3         3           3

图 3.31 "会话"选项卡

图 3.32 "远程控制"选项卡

(99)

(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。

				? ×	xx_student01 届性				?
常規	隶属于	配置文件	环境	会话	常规	隶属于	配置文件	环境	会活
远程控制		远程桌面服务配置文件	+	援入	远程控制		远程桌面服务配置文	4	援入
明这一选项卡 程桌面服务。 远程桌面服务/ 配置文件路径	配置远程桌面 用户配置文件 5(P):	服务用户配置文件。此质	遭文件中的说	<b>畫适用于</b>	<ul> <li>网络访问权限</li> <li></li></ul>	の ) 网络策略控制议	5间(P)		
					F 验证呼叫方 回拨选项	ID(V):			
远程桌面服务	主文件夹				( 不回拨(C)				
<ul> <li>本地路径(</li> </ul>	u)				<ul> <li>○ 由呼叫方设</li> <li>○ 总是回拨到</li> </ul>	置(仅路由和远 (Y):	裡访问服务)(S)		
○ 连接(C): 拒绝该用户	· 一	✓ 到(T): 面会话主机服务器的权限	(D)		「 分配静态 IF 定义要为此拨	,地址(I) 入连接启用的	, IP 地址。	静态 IP 地址	(1)
					「「 应用静态路 为此拨入连接	由(R)	進由	能士服	1

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。



(+(r) g(r(A))		(H)					_
書 计算机管理(本地)		名称		描述	^	操作	_
◇ 沿系统工具		Acces	s Control Assi	此组的成员可以远程查询此计算		组	
<ul> <li>         · · · · · · · · · · · · · · ·</li></ul>	ビナ・ 第 モ D組	Admin Backu Certifi Crypto Device	istrators p Operators cate Service D ographic Oper Owners	管理员对计算机/域有不受限制的 备份操作员为了备份或还原文件 允许该组的成员连接到企业中的 授权成员执行加密操作。 此组的成员可以更改系统范围内	1	更多	. )
の性能	新建组(N)		uted COM Us	成员允许启动、激活和使用此计			
🛓 设备管	查看(V)	>	og Readers	此组的成员可以从本地计算机中			
> 習存儲 > 晶服务和应	刷新(F) 导出列表(L)		V Administra RS	此组的成员拥有对 Hyper-V 所有 Internet 信息服务使用的内置组。			
	ありまたり (山)		rk Configurat	此组中的成员有部分管理权限来	~		

图 3.35 选择"新建组"命令

			xx_group01 属性		?	>
			常规			
冠组		? ×	xx_g	proup01		
且名(G):	xx_group01					_
載述(D):	xx_group01		描述(E):	xx_group01		
戊员(M):			成员(M):			
添加(A)	<b>删除(R)</b>		添加(D)	直到下一次用户登录 删除(R) 系的更改才生效。	时对用户的组成员	Ð
帮助(H)	Arthuro		1			
	的雄(C)	关闭(O)		<b>确定 取消</b> 应用	(A) <b>報</b> 員	b

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。



选择用户					3
选择此对象类型	뮡(S):				
用户或内置安	全主体			对象的	<u> 進型(O)</u>
查找位置(F):					
DC2				位	置(L)
一般性查询					
名称(A):	起始为	<b>U</b>			列(C)
描述(D):	起始为	¥			立即查找(N)
□ 禁用的财	(户(B)				停止(T)
一不过期这	彁(X)				
自上次登录	后的天数(1):		2		<del>?</del> //
搜索结果(U):				确定	取消
称			所在文件夹		
This Organ	ization Certifica	ate			
WDAGUtilit	yAccount		DC2		
xx_student(	01		DC2		
四个现然户 2 大地账户和1	<b>新理员约成员</b>				
	SAT NOT DECK				

图 3.38 选择用户账户 xx\_student01

选择用户		3
选择此对象类型(S):		
用户或内置安全主体	সা	象类型(0)
查找位置(F):		
DC2		位置(L)
輸入对象名称来选择(示例)(E):		
DC2\xx_student01	松	查名称(C)
高级(A)	确定	取消

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。



回 运行		×
0	Windows 将根据你所输入的名称,为你打开相应的程序、 文件夹、文档或 Internet 资源。	
打开(0)	: cmd 🗸	
	♥ 使用管理权限创建此任务。	
	确定 取消 浏览( <u>B</u> )	

图 3.40 "运行"对话框

om 管理员: C:\Windows\system32\cmd.exe	-		×
C:\>net /? 此命令的语法是:			î
NET [ ACCOUNTS   COMPUTER   CONFIG   CONTINUE   FILE   HELPMSG   LOCALGROUP   PAUSE   SESSION   SHARE   STATISTICS   STOP   TIME   USE   USER   VIEW ]	GROUP START	HELF	
C:\>net_user /? 此命令的语法是:			
NET USER [username [password   *] [options]] [/DOMAIN] username [password   *} /ADD [options] [/DOMAI username [/DELETE] [/DOMAIN] username [/TIMES: {times   ALL}] username [/ACTIVE: {YES   NO}]	IN]		
c:\>			Ļ

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。

	C:\>net user \\DC2 的用户账户		
	 Administrator	DefaultAccount	Guest
Lncc@123 /add	user01 命令成功完成。	WDAGUtilityAccount	xx_student01
	C:\>_		

user0

user 戓功完成。

C:\>

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。

C:\>net user 命令成功完成。	user01	Lncc@456
C:\>_		

图 3.44 修改用户账户 user01 的密码

(5) 查看当前本地组列表,执行命令如下。

net localgroup

C:\>net localgroup	ł
\\DC2 的别名	(
	命令女
*Access Control Assistance Operators	
*Administrators	n
*Dackup Operators	
*Certificate Service DCOM Access	
*Cryptographic Operators	書
*Device owners *Distributed COW Hears	
*Front Log Readers	(
*Guests	
*Hyper-V Administrators	命令女
*IIS IUSRS	
*Network Configuration Operators	
*Performance Log Users	n
*Performance Monitor Users	
*Power Users	
*Print Operators	書
*RDS Endpoint Servers	
*RDS Management Servers	(
*RDS Remote Access Servers	
*Remote Desktop Users	令如
*Remote Management Users	
*Replicator	
*Storage Replica Administrators	n
*Jystem manageu Accounts Group	
*vy groun01	
*xx localgroun01	Ð
命令成功完成。	
	(
C:\>	
	n

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。

localgroup xx\_localgroup01 /add

图 3.45 创建本地组 xx\_localgroup01

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 →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 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 命令成功完成。	xx_loca1group01	user01 /add	
	C:\>			
	图 3.47 用户账户	user01 添加到组 xx	x_localgroup01	
C:\>net localgroup 别名 xx_localgrou 注释	xx_loca1group01 p01			
成员				
user01 命令成功完成。		C:\>net local; 命令成功完成。	group xx_localgroup	01 user01 /del
C:\>		C:\>		
3.48 组 xx_localgrou	p01 内用户账户信息	图 3.49 删除约	狙 xx_localgroup01 片	中用户账户 user01



图 3.50 删除用户账户 user01

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

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 v3-2 资源。

### 1. 项目规划

图

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。

	Q 🗟 🛛	88			
<ul> <li>Active Directory用</li> <li>○ 保存的查询</li> <li>○ Grand Comparison</li> <li>○ Builtin</li> <li>○ Compute</li> <li>○ Domain (</li> <li>○ ForeignSi</li> <li>○ Managec</li> <li>&gt; ○ Users</li> </ul>	户和计算机 [DC1.Int 委派控制(E) 查找(I) 更改域(D) 更改域控制器(C) 提升域功能级别(A) 提作主机(M)	名称 I Builtin II -	ers Controllers SecurityPrincipals xd Service Accounts	类型 builtinDomain 容器 组织单位 容器 容器 容器	描述 Default container for upgraded computer accounts Default container for domain controllers Default container for security identifiers (SIDs) associa Default container for managed service accounts Default container for upgraded user accounts
	新建(N)	>	计算机		
	所有任务(K) 查看(V)	,	紙系入		
	刷新(F) 导出列表(L)		InetOrgPerson msDS-ShadowPr msImaging-PSP	incipalContainer	
	属性(R)		MSMQ 队列别名		
	帮助(H)		组织单位 打印机 用户		

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



创建于:	Incc.abc.con	n/	
名称(A):			 
OU_project_B01			
一防止容器被意外删	除(P)		
一防止容器被意外删	除(P)		
☑ 防止容器被意外删	除(P)		
☑ 防止容器被意外删	除(P)		
☑ 防止容器被意外删	(P)		
☑ 防止容器被意外删	滕仲(P)		
☑ 防止容器被意外删	滕(P)		
☑ 防止容器被意外删	<b>滕</b> (P)		

图 3.54 "新建对象-组织单位"对话框

Active Directory 用户和i	+算机		_		×
文件(F) 操作(A) 查看(V)	帮助(H)				
** 2 1 4 1	X 🖬 Q 🖻 🛛 🖬		8 2 6 7 0 2		
<ul> <li>Active Directory 用户和:</li> <li>○ 保存的查询</li> <li>○ 除存的查询</li> <li>○ Builtin</li> <li>&gt; ○ Domain Controlle</li> <li>&gt; ○ Domain Controlle</li> <li>&gt; ○ Managed Service</li> <li>&gt; ○ Users</li> </ul>	增机 [DC1.Int 名称 ers incipals Accounts		类型 这里没有任何项目。	描述	
OU_project_801	委派控制(E) 移动(V) 查找(I)				
	新建(N)	>	计算机		
	所有任务(K)	>	联系人		
	查看(V)	>	组 InstOrePerson		
	劈切(T) 删除(D) 重命名(M) 刷新(F) 导出列表(L) 屋性(R)		mstorgrenson msDS-ShadowPrincipalContainer msImaging-PSPs MSMQ 队列别名 组织单位 打印机		
	in Photo	-	共享文件夹		
	#PED(H)		117 MILES		

图 3.55 选择新建用户



冠建对象 - 用户			X 新建对象 - 用户	×
8 19587	F: Incc.abc.c	com/OU_project_B01	8 113	建于: Incc.abc.com/OU_project_B01
姓(L):			密码(P):	•••••
名(F):	I	英文缩写(I):	确认密码(C):	•••••
姓名(A):	project_use	er801		录时须更改密码(M)
用户登录名(U):				改密码(S)
project_userB01	1	@Incc.abc.com	~ ☑密码永不过	期(W)
用户登录名(Wind	lows 2000 以前版	本)(W):	□账户已禁用(	(O)
LNCC\		project_userB01		
		<上一步(B) 下一步(N) >	取消	< 上一步(B) 下一步(N) > 取消

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。

-
^



(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



建对象 - 组		
畿 创建于: Incc.abc	com/OU_project_B01	
组名(A):		
project_groupB01		
/////////////////////////////////////	000-	
project_groupB01		
组作用域	组类型	_
〇本地域(O)	● 安全组(S)	
◉ 全局(G)	○通讯组(D)	
○通用(U)		

#### 图 3.59 "新建对象-组"对话框

Active Directory 用户和计算机 文件(F) 操作(A) 查看(V) 帮助(H)			-		×
<ul> <li>❑ Active Directory 用户和计算机 [DC1.lne</li> <li>&gt; ❑ 保存的查询</li> <li>&gt; ❑ Builtin</li> <li>&gt; ❑ Computers</li> <li>&gt; ❑ Domain Controllers</li> <li>&gt; ❑ ForeignSecurityPrincipals</li> <li>&gt; ❑ Managed Service Accounts</li> <li>❑ Users</li> <li>⊇ OU_project_B01</li> </ul>	名称 Project_groupB01 Project_userB01 Project_userB02	类型 安全组 用户	- 全局	描述	3
< >	<				>

图 3.60 "Active Directory 用户和计算机"窗口



					•	
常规	成员	隶属于	管理者			
成员	(M):					
名和 & 1	弥 project_u project_u	userB01 userB02	Active Directory 域服务文件 Incc.abc.com/OU_project_E Incc.abc.com/OU_project_E	夹 301 301		
						I
<					_	>
<	轰力ቢ(D)		部除(R)		_	>
<u>د</u>	轰力D(D)	1	割除(R)		_	>

图 3.61 "project\_groupB01 属性"对话框

aminar c minator sc prismir la labora sco anas	<b>a</b>	
轻华此对象类型(S):		
用户、服务账户、组或其他对象		对象类型(O)
的拉位置(F):		
ncc.abc.com		位置(L)
认对象名称来选择( <u>示例</u> )(E):		
		检查名称(C)

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"→

(110)

选择用户、联系人、计具作。服务账户或组 选择此对象类型(S):			×
用户、服务账户、组或其他对象		对象类型(O)	
查找位置(F):			_
Incc.abc.com		位置(L)	
一般性查询			
名称(A): 起始为 ~		歹](	C)
描述(D): 起始为 ~		立即重	查找(N)
□ 禁用的账户(B)		停止	E(T)
□ 不过期密码(X)		÷	Z
□ 不过期密码(X) 自上次登录后的天数(I):		÷	<i>a</i>
□ 不过期密码(X) 自上次登录后的天数(I):		ý Mie B	5 M
□ 不过期密码(X) 自上次登录后的天数(I): 搜索结果(U): 名称 电子邮 Domain Controllers Domain Guests Domain Users	件地址 描述 域中所有域控… 域的所有来宾 所有域用户	确定 耶 所在文件夹 Incc.abc.com/ Incc.abc.com/ Incc.abc.com/	5% ^
□ 不过期密码(X) 自上次登录后的天数(I): 搜索结果(U): 名称 电子邮 Domain Controllers Domain Guests Domain Users Group Policy Creator Owners	件地址 描述 域中所有域控 域的所有来宾 所有域用户 这个组中的成	确定 取 所在文件夹 Incc.abc.com/ Incc.abc.com/ Incc.abc.com/ Incc.abc.com/	5% 
□ 不过期密码(X) 自上次登录后的天数(I): 搜索结果(U): 名称 电子邮 Domain Controllers Domain Guests Domain Users Group Policy Creator Owners Guest	(+地址 描述 域中所有域控 域的所有来宾 所有域用户 这个组中的成 供知知时宫一	确定 単定 所在文件夹 Incc.abc.com/ Incc.abc.com/ Incc.abc.com/ Incc.abc.com/	S#
□ 不过期密码(X) 自上次登录后的天数(I): 建憲结果(U): 名称 电子邮 Domain Controllers Domain Guests Domain Users Group Policy Creator Owners Guest Key Admins A project groupP01	件地址 描述 域中所有域控 域的所有来宾 所有域用户 这个组中的成 供来宾访问计 此组的成员可	确定 所在文件夫 Incc.abc.com/ Incc.abc.com/ Incc.abc.com/ Incc.abc.com/ Incc.abc.com/ Incc.abc.com/ Incc.abc.com/	5% ^
□ 不过期密码(X) 自上次登录后的天数(I): 建憲结果(U): 名称 电子邮 Domain Controllers Domain Guests Domain Users Group Policy Creator Owners Group Policy Creator Owners Guest Key Admins project_groupB01 project_userB01	件地址 描述 域中所有域 <u>控</u> 域的所有来真 所有域用户 这个组中的成 供来宾访问计 此组的成员可	确定 即 所在文件夹 Incc.abc.com/ Incc.abc.com/ Incc.abc.com/ Incc.abc.com/ Incc.abc.com/ Incc.abc.com/ Incc.abc.com/ Incc.abc.com/	5% 
□ 不过期密码(X) 自上次登录后的天数(I): 搜查结果(U): 名称 电子邮 Domain Controllers Domain Guests Domain Users Group Policy Creator Owners Guest Key Admins project_groupB01 project_userB01 project_userB01 project_userB02	件地址 描述 域中所有域控… 域的所有来宾 所有域用户 这个组中的成… 供来宾访问计… 此组的成员可…	确定 即 所在文件夹 Incc.abc.com/ Incc.abc.com/ Incc.abc.com/ Incc.abc.com/ Incc.abc.com/ Incc.abc.com/ Incc.abc.com/ Incc.abc.com/ Incc.abc.com/ Incc.abc.com/	5% () () () () () () () () () () () () ()
□ 不过期密码(X) 自上次登录后的天数(I):	件地址 描述 域中所有域控… 域的所有来宾 所有域用户 这个组中的成… 供来宾访问计… 此组的成员可…	際定 原在文件夹 Incc.abc.com/ Incc.abc.com/ Incc.abc.com/ Incc.abc.com/ Incc.abc.com/ Incc.abc.com/ Incc.abc.com/ Incc.abc.com/ Incc.abc.com/ Incc.abc.com/ Incc.abc.com/	SH A

图 3.63 "一般性查询"选项卡

选择用户、联系人、计算机、服务账户或组	×
选择此对象类型(S):	
用户、服务账户、组或其他对象	对象类型(O)
查找位置(F):	
Incc.abc.com	位置(L)
输入对象名称来选择(示例)(E):	
project_userB01 (project_userB01@lncc.abc.com); project_userB02 (project_userB02@lncc.abc.com)	检查名称(C)
高级(A)	确定取消

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。

彩 创建于: Incc.a	abc.com/OU_project_B01	
组名(A):		
project_localgroupB01		
组名(Windows 2000 以前版)	本)(W):	
project_localgroupB01	TANK .	
组作用域	组类型	
●本地域(O)	● 安全组(S)	
〇全局(G)	○通讯组(D)	
○通用(U)		

图 3.65 "新建对象-组"对话框

Active Directory 用户和计算机     文件(F) 操作(A) 查看(V) 穆助(H)     本市 Active Directory 用户和計算机 [DC1.Ind     《    《    《    和市政 和 和 和 和 和 和 和 和 和 和 和 和 和 和 和 和	至而 名 和 可 名称 是 project_group801 是 project_localgroup801 多 project_user801	医择用户、联系人、计算机、服务账户或组 选择此对象类型(5): 用户、服务账户、组或其他对象 查找位置(F): Incc.abc.com	× 对象类型(O) 位置(L)
	<ul> <li>G. project userB02</li> <li>西塚田中、京玄人、计算机、最</li> <li>透探此対象关型(S):</li> <li>用中、服务账户、组或其他对象</li> <li>着线位置(F):</li> <li>Incc.abc.com</li> <li>输入对象名称未选择(示型)(E):</li> </ul>	- 版在重加 名称(A): 脳協力 ✓ 当該(D): 影協力 ✓ 一 新用的影件(B) □ 不过期密码(X) 自上次登录后的天致(I): ✓	<b>利(C)…</b> 立即査找(N) 等止(T)
<	Project_grouppul 泡吸(A)	複数結果(U): 在称 电子邮件地址 描述 Key Admins 此相的成员可 project_oroupB01 project_userB01 project_userB02 Project_userB02	満定 取消 所在文件夹 Incc.abc.com/ Incc.abc.com/ Incc.abc.com/ Incc.abc.com/ Incc.abc.com/

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。

选择用户、联系人、计算机、服务账户或组	
选择此对象类型(S):	
用户、服务账户、组或其他对象	对象类型(O)
查找位置(F):	
Incc.abc.com	位置(L)
輸入对象名称来选择(示例)(E):	
project groupB01	检查名称(C)
高级(A)	确定取消

图 3.67 添加组

19750	成员	隶属于	管理者		
成员(	M):				
名称	s project_g	roupB01	Active Directory 域服务文 Incc.abc.com/OU_project	件夹 _B01	
<				_	>

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



<ul> <li>☐ Active Directory 用户和计算机</li> <li>文件(F) 操作(A) 查看(V) 帮助(H)</li> </ul>		- 0	×
Active Directory 用户和计算机 [DC1.Incc.abc.com]  ④ 保存的查询   ※ 論 Incc.abc.com   ※ 論 Incc.abc.com   ※ 節 Domain Controllers   ※ 節 ForeignSecurityPrincipals   ※ Managed Service Accounts   ③ Users   ③ OU_project_B01	<ul> <li>         ・</li> <li></li></ul>	类型 安全组 - 全局 安全组 - 本地域 用户 用户	描述
	<		>

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。

🗏 pro	ject_sha	re01 属性	ŧ		×
常规	共享	安全	以前的版本	自定义	
「「「「」」の説	留文件和DS	文件 <del>夹共</del> 勇 · · · · · · · · · · · · · · · · · · ·	are01		
	♥高	<b>汉限,创</b> 3 级共享([	建多个共享,并 ))	设置其他高级共	宴选项。
			确定	取消	应用(A)

图 3.70 "project\_share01 属性"对话框



🛎 网络访问	
选择要与其共享的网络上的用户	
键入名称,然后单击"添加",或者单击箭头查	找用户。
	~ 添加(A)
Everyone	
●找个人	法取得入事
Administrator	医叭/与∧ ▼
Administrators	
共享时有问题	

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。

≒.
✔ 添加(A)
权限级别
读取/写入 ▼ 所有者
读取/写入 ▼ 读取 ✓ 读取/写/
删除

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



MH2010	
你的文件夹已共享。	
可通过用子邮件向某个人发送到这些共享项的链接,或将链接复制	并粘贴到其他应用中。
各个项目	
project_share01	

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。

ternet muchg 4 (TCP/IPV4) 應1	tt .	•
開		
如果网络支持此功能,则可以获用 络系统管理员处获得适当的 IP 设	取自动指派的 IP 设置。否则,你需要从网 置。	
○自动获得 IP 地址(O)		
●使用下面的 IP 地址(S):		
IP 地址(I):	192 . 168 . 100 . 10	
子网掩码(U):	255 . 255 . 255 . 0	
默认网关(D):	192.168.100.2	
	D	
● 白动武寺 DNS 服务器地址(	at(E):	個 运行
) 首选 DNS 服务器(P):	192.168.100.100	
备用 DNS 服务器(A):	192.168.100.101	Windows 将根据你所输入的名称,为你引升相应的程序、 文件夹、文档或 Internet 资源。
		打开(O): \\DC1.lncc.abc.com\project_share01
□ 退出时验证设置(L)	高级(V)	
		· · · · · · · · · · · · · · · · · · ·

图 3.74 DNS 服务器地址设置

图 3.75 "运行"对话框



Windows 安全中心 输入网络凭据		×
输入你的凭据以连接到:DC1.Inco	.abc.com	
project_userB01@Incc.abc.com	n	
••••••	୕	
域: Incc.abc.com		
✓ 记住我的凭据		
		ł

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。

↓  ⑦   =   文件 主页	project_s 共享	hare01 查看					-		× ~ 🕐
← → · ↑	🖳 « D0	C1.Incc.abc.com	> project_share01	~	ō	Q	搜索"project	_share01"	
<ul> <li>→ 快速访问</li> <li>→ OneDrive</li> <li>→ 世由脑</li> <li>→ 例络</li> <li>1 个项目</li> </ul>		名称 个	修改日期 2022/7/23 20:14	<u>美型</u> 文本文	档		大小 7 KB	ſ	

图 3.77 访问共享目录

\\DC1.	Incc.abc.com\project_share01	×
$\otimes$	\\DC1.lncc.abc.com\project_share01	
	我们无法使用此凭握登录,因为你的域不可用。请确保你的设备已连接到你组织的网络, 重试。如果你以前使用其他凭握登录到了此设备,则可以使用该凭握登录。	然后
	通知	

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 S	erver 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。

