

第二章 Windows 用户和组管理

作者: [RSWQRD](#)

原文链接: <https://ld246.com/article/1677714628177>

来源网站: [链滴](#)

许可协议: [署名-相同方式共享 4.0 国际 \(CC BY-SA 4.0\)](#)

仅供交流学习使用，请多支持正版资源。

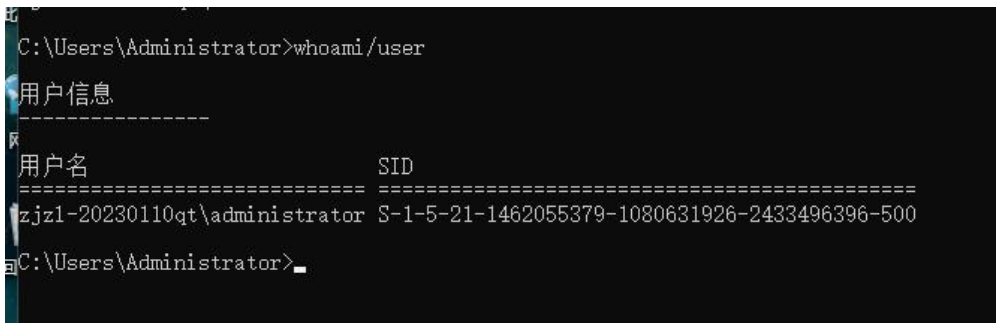
声明：本资源由微信公众号【遨游互联网】搜集整理，仅供大家学习交流，不可作任何商用！

说明：要获得更多的资源的话请随时关注微信公众号【遨游互联网】。=====

第二章

本章所需理解如下

前置知识· 在Windows中，每个用户账户有一个唯一的安全标识符（Security Identifiers，简称SI），用户权限是通过用户的SID记录的，通过“运行 whoami /user” 来查看当前用户的SID。



```
C:\Users\Administrator>whoami /user
用户信息
-----
用户名                               SID
-----
zjz1-20230110qt\administrator S-1-5-21-1462055379-1080631926-2433496396-500
C:\Users\Administrator>
```

lusrmgr.msc 本地用户和组

gpedit.msc 本地组策略编辑器

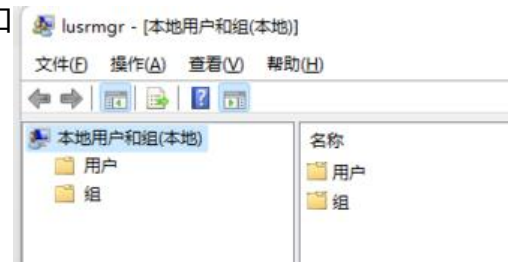
一. 理解用户账户概念

Windows 安全性的主要方法有以下4点：

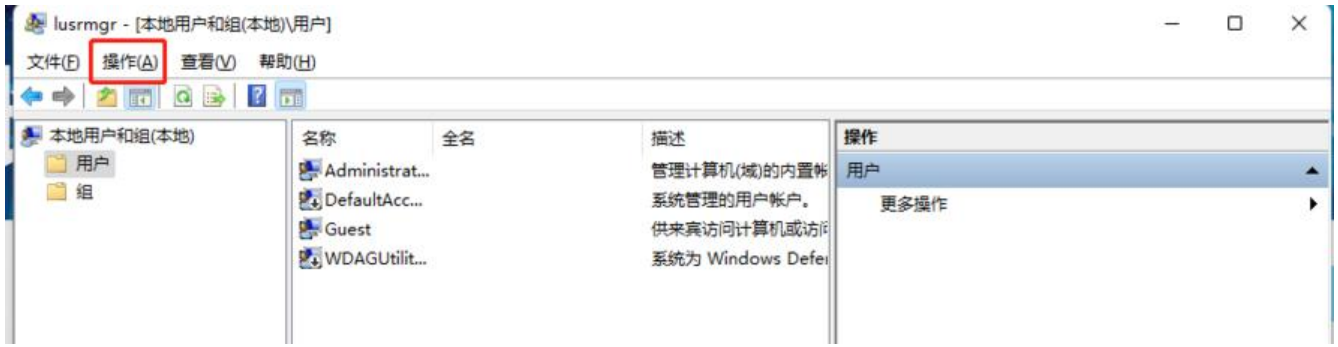
- 1.严格定义各种账户权限
- 2.使用组规划用户权限，简化账户权限的管理
- 3.禁止非法计算机连入网络
- 4.应用本地安全策略和组策略

二. 掌握创建、管理用户账户的方法

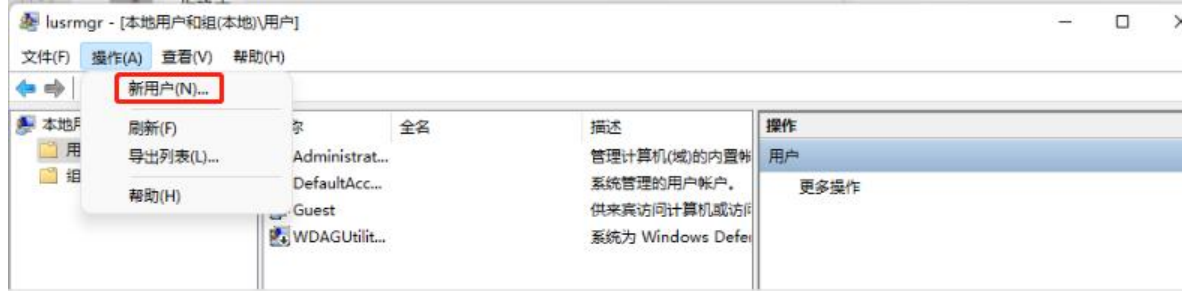
window+r 调出来运行窗口 在里面输入 “lusrmgr.msc” 会打开如下窗口



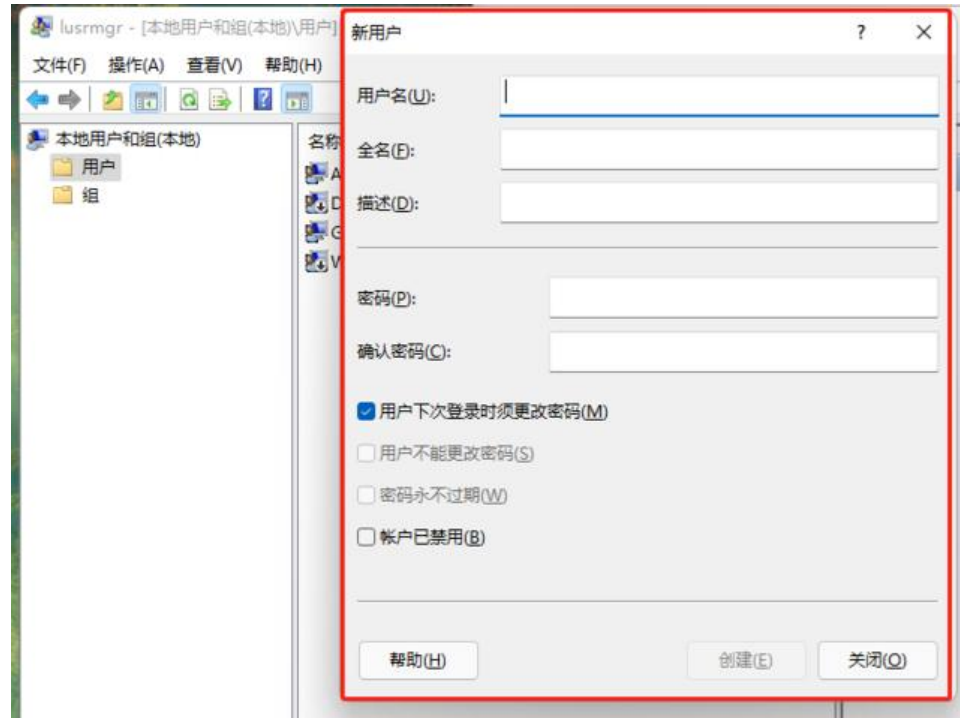
• 首先是创建用户（如下）



- 点击新用户 (如下)



- 点击后会蹦出来一个页面 (如下)



- 用户账户

(1) 账户命名约定:

- ① 账户名必须唯一: 本地账户必须在本地计算机上唯一
- ② 账户名不能包含以下字符: * / \ [] : : | = , + / < > “
- ③ 账户名最长不能超过20个字符

(2) 密码原则:

- ① 一定要给Administrator账户指定一个复杂密码, 以防止他人随便使用该账户
- ② 确定是管理员还是用户拥有密码的控制权。用户可以给每个用户账户指定一个唯一的密码, 并防止他用户对其进行更改, 也可以允许用户在第一次登录时输入自己的密码。一般情况下, 用户应该可以控制自己的密码
- ③ 密码不能太简单, 应该不容易让他人猜出
- ④ 密码最多可由128个字符组成, 推荐最小长度为8个字符
- ⑤ 密码应由大小写字母、数字以及合法的非字母数字的字符混合组成, 如 “Pa\$\$wOrd”

• 用户选项

- **全名和描述:** 记录用户的信息, 如tang kai, 描述为Operation Supervisor。
- **密码和确认密码:** 用户的创建者为该用户指定的初始密码。在Windows Server 2012 R2 中, 默认启用了“密码必须符合复杂性要求”的策略, 所以为用户设置密码必须符合复杂性要求。
- **用户下次登录时须更改密码:** 为防止使用者使用初始密码而不更改(一般情况下, 初始密码比较简单, 且有可能与其他用户初始密码一致), 选中此复选框, 可以强迫使用者在下次登录时必须更改密码。
- **用户不能更改密码:** 在多个使用者使用同一个用户账户时(如果其中一人更改了密码就会造成其他使用者无法登录), 或其他任何不希望使用者更改密码的情况, 可以选中此复选框禁止用户更改密码。此项在取消选中“用户下次登录时须更改密码”复选框时有效。
- **密码永不过期:** 当用户密码使用时间超过了密码策略中设置的最长使用期限, 用户登录时会提示密码过期, 必须更改。如果希望某个用户的密码不受此策略的限制, 可以选中此复选框。此项在取消选中“用户下次登录时必须更改密码”复选框时有效。
- **账户已禁用:** 创建用户后, 通常需要为用户设置权限, 为防止在权限设置完成前, 该用户已被使用者使用。可以创建一个禁用的用户账户, 待权限设置完成后, 再启用该用户。

• 新建组教程 (如下1.2.3.)

**1. 点击到组

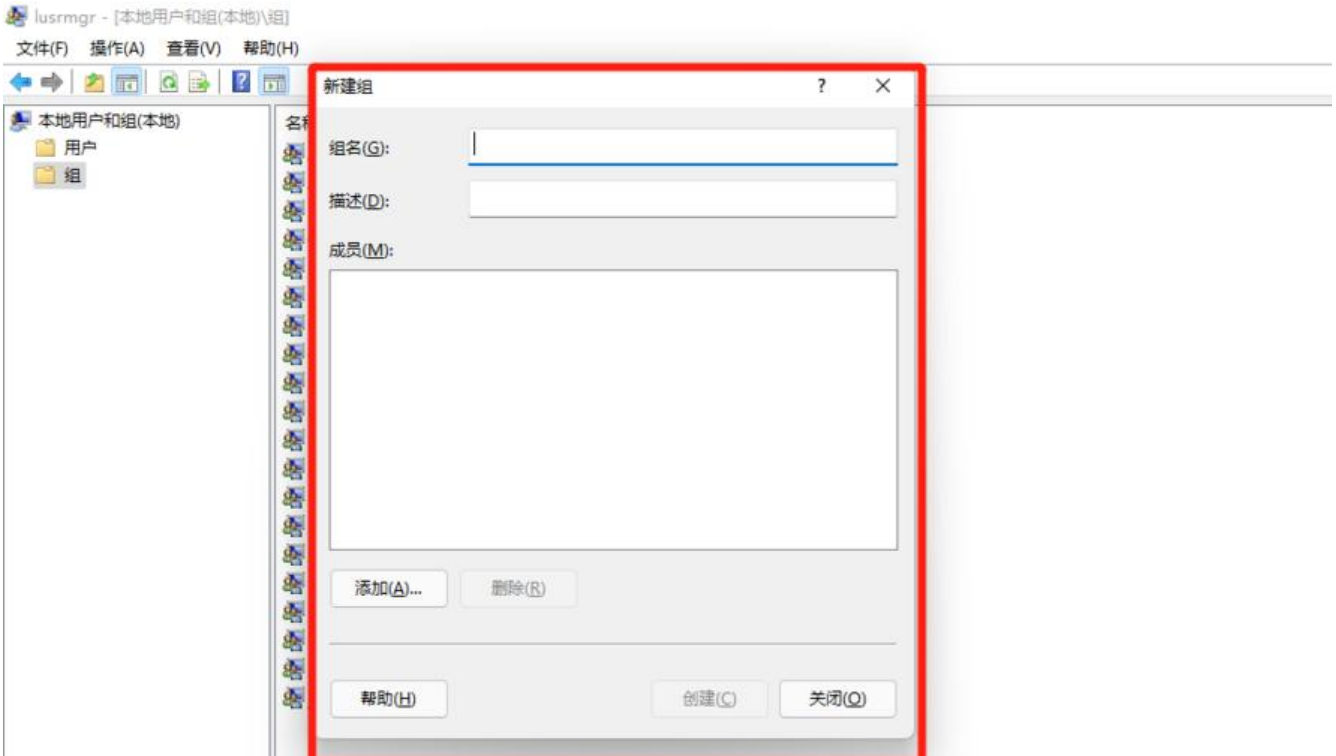
**



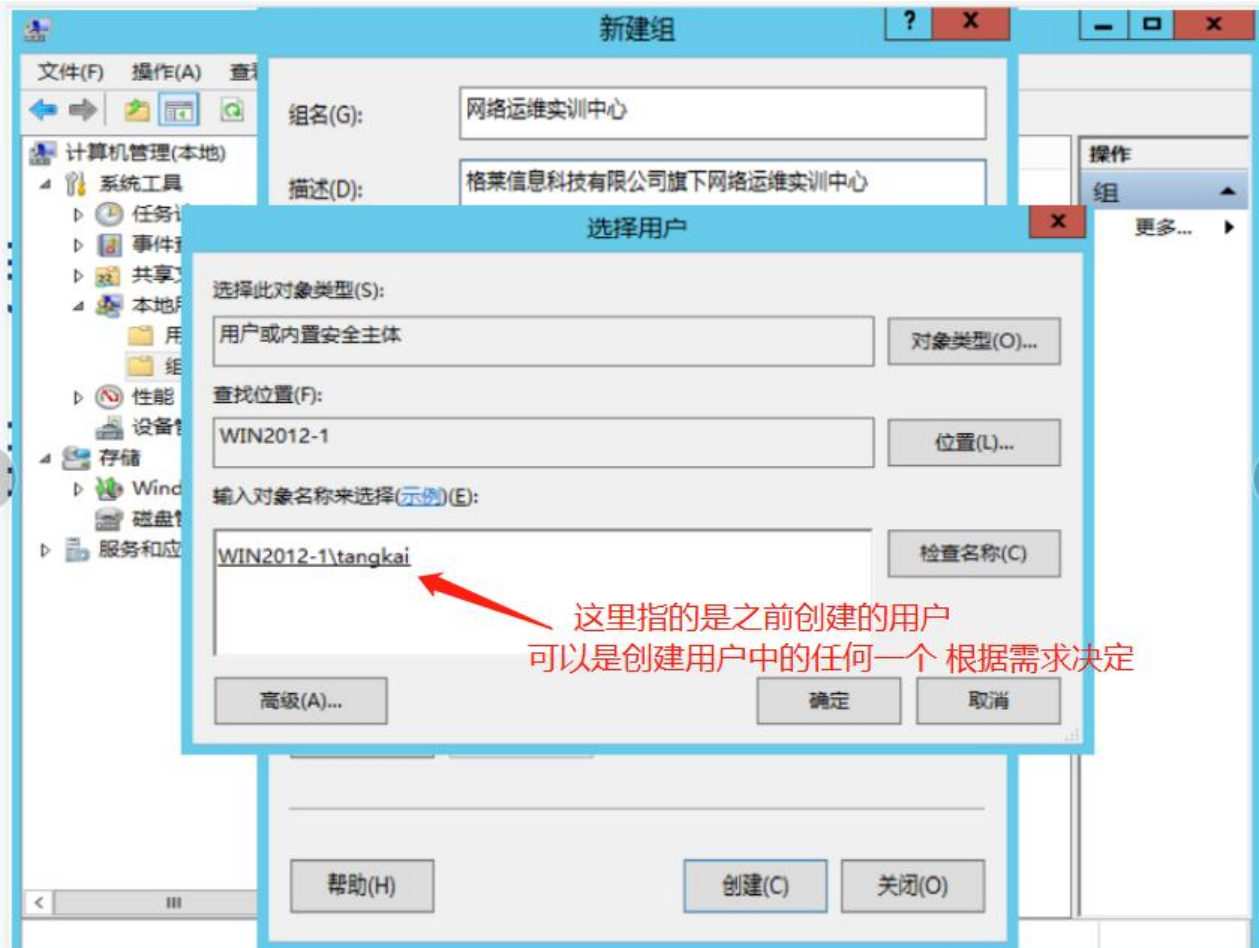
2. 右键创建组 或者是 (如下图)



3.出现以下页面



4.向组内添加成员



•重命名和删除组（例：如下）

命令创建用户：net user wangwu qwe123.. /add

命令修改用户密码：net user wangwu Abc123

命令删除用户账户：net user wangwu /del

命令创建组：net localgroup 市场部/add

命令将用户加入到组：net localgroup 市场部zhangsan /add

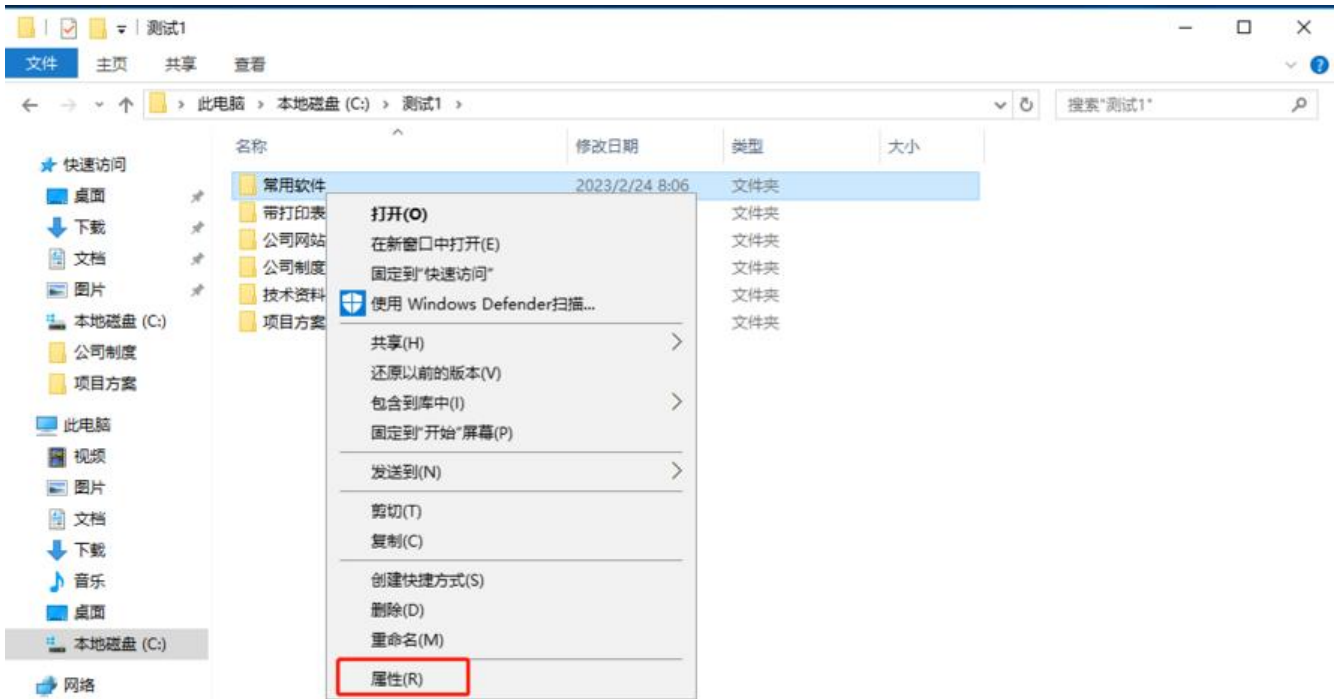
命令将用户从组中移除：net local group 市场部zhangsan /del

命令删除组：net localgroup 市场部/del

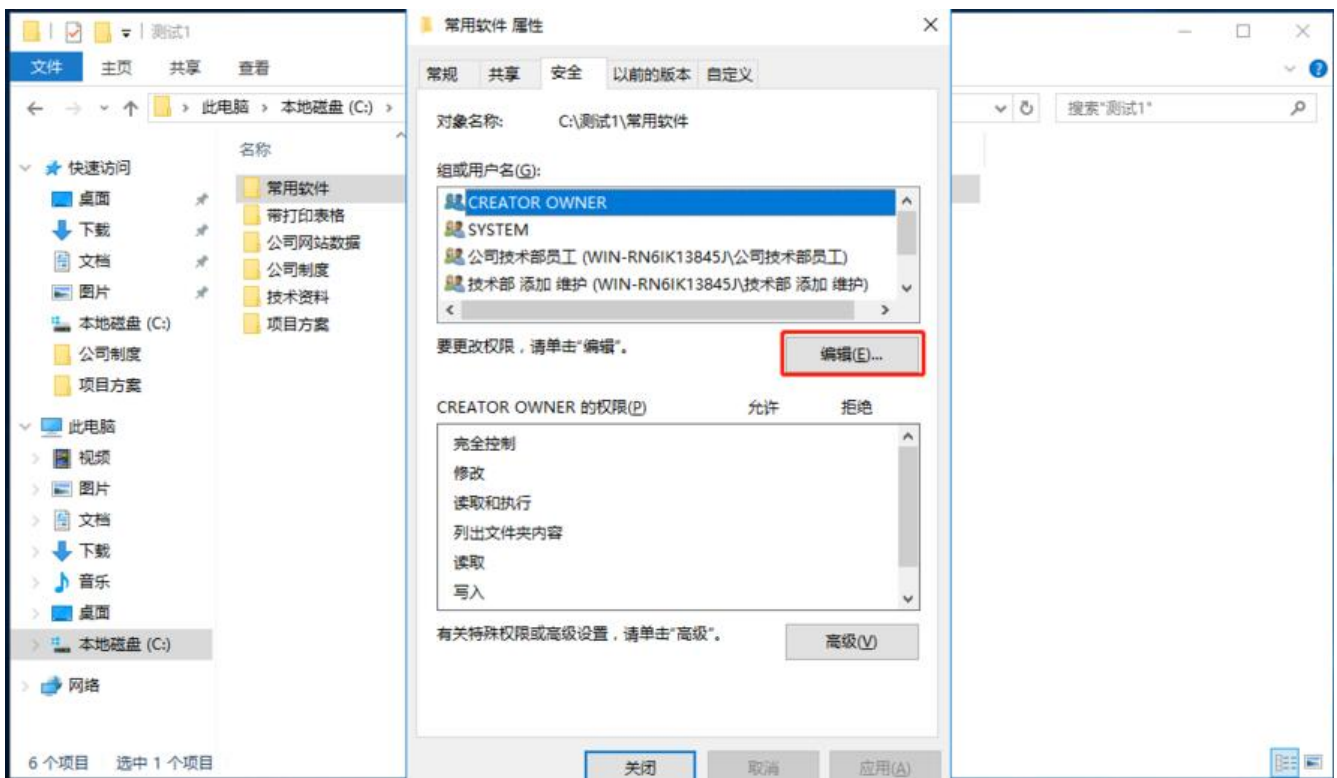
•为组设置权限

在虚拟机里随意找一个文件夹 右键 属性（如下界面）

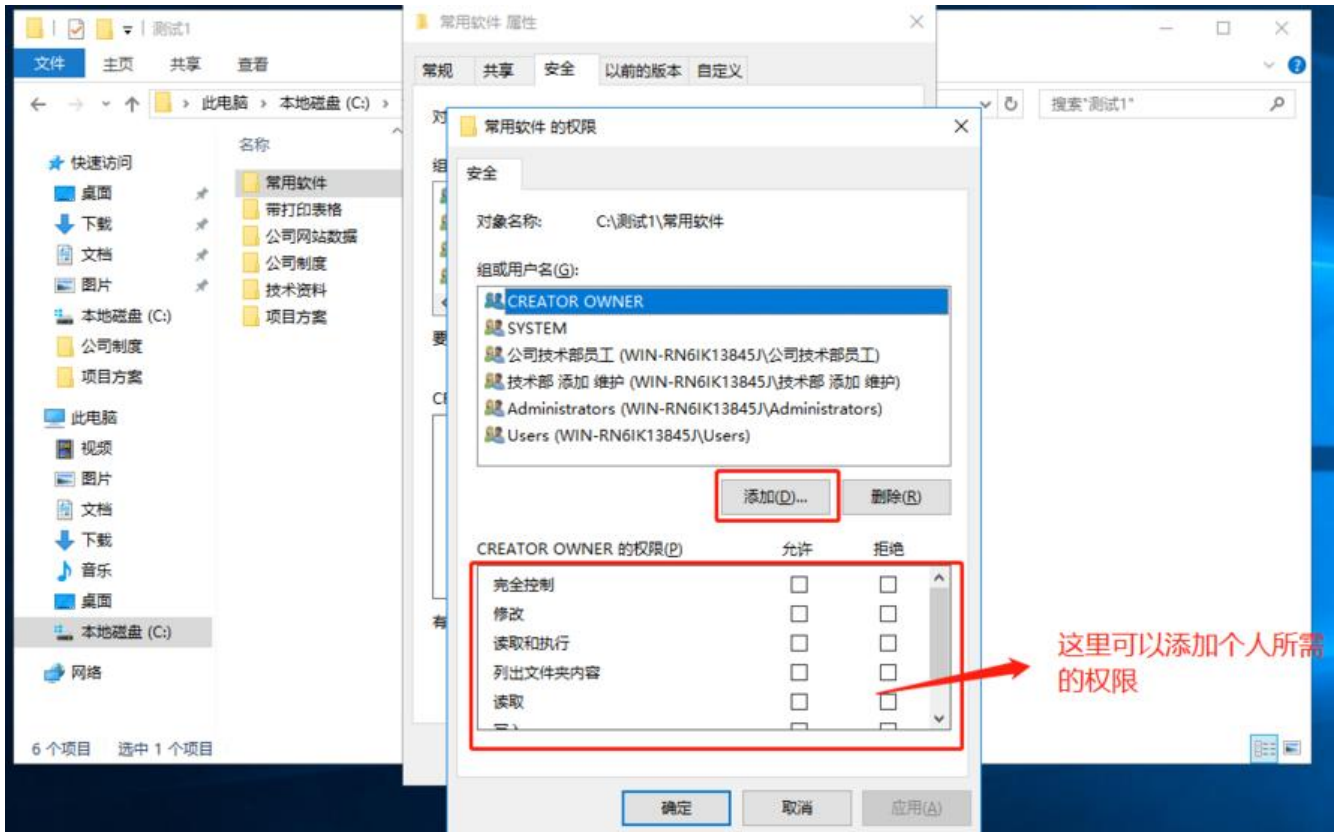




点击“安全”“编辑”



接着 下一步 点击“添加”



• 内置账户分类

- Administrator

Administrator是默认的管理员用户，在所有与使用者关联的账户中，其权限最高，在没有其他管理员账户的情况下，建议不要将该账户禁用。为了保证计算机系统的安全，也不建议将Administrator的密码告诉其他使用者。此账户无法删除，建议将其改名以提高安全性。

- Guest

Guest是提供给没有用户账户的访客使用的。该账户默认是禁用的，它拥有的权限非常有限。此账户也无法删除，但是允许改名。

• 内置组账户

组名	描述信息
Administrators	该组的成员具有对服务器的完全控制权限，并且可以下其他用户分配用户权利和访问控制权限。管理员账户Administrator就是这个组的默认成员。
Backup Operators	加入该组的成员可以备份和还原服务器上的所有文件，而不管这些文件的是否设有权限。
Guests	该组的成员拥有一个在登录时创建的临时配置文件，在注销时，该配置文件将被删除。来宾账户（默认情况下已禁用）也是该组的默认成员。
Network Configuration Operators	该组的成员可以更改 TCP/IP 设置并更新和发布 TCP/IP 地址。
Power Users	该组具有创建用户账户和组账户的权利，可以在 Power Users 组、Users 组和 Guests 组中添加或删除用户，但是不能管理Administrators组成员。可以创建和管理共享资源。
Print Operators	该组的成员可以管理打印机。
Users	该组的成员可以执行一些常见任务，例如运行应用程序、使用本地和网络打印机以及锁定服务器。用户不能共享目录或创建本地打印机。

三. 理解用户组概念

• 用户组概念

- “组”是为了方便管理大量用户的权限而设计的，是用户的集合
- 当我们要给一批用户分配同一个权限时，就可以将这些用户都归到一个组中，只要给这个组分配此权限，组内的用户就都会拥有此权限
- Windows Server 2012也使用唯一安全标识符SID来分辨不同的组。权限的设置都是通过SID设置的，不是利用组名



四. 命令管理用户和组

组名	描述信息
Administrators	该组的成员具有对服务器的完全控制权限，并且可以下其他用户分配用户权利和访问控制权限。管理员账户Administrator就是这个组的默认成员。
Backup Operators	加入该组的成员可以备份和还原服务器上的所有文件，而不管这些文件的是否设有权限。
Guests	该组的成员拥有一个在登录时创建的临时配置文件，在注销时，该配置文件将被删除。来宾账户（默认情况下已禁用）也是该组的默认成员。
Network Configuration Operators	该组的成员可以更改 TCP/IP 设置并更新和发布 TCP/IP 地址。
Power Users	该组具有创建用户账户和组账户的权利，可以在 Power Users 组、Users 组和 Guests 组中添加或删除用户，但是不能管理Administrators组成员。可以创建和管理共享资源。
Print Operators	该组的成员可以管理打印机。
Users	该组的成员可以执行一些常见任务，例如运行应用程序、使用本地和网络打印机以及锁定服务器。用户不能共享目录或创建本地打印机。

• 用户组概念

- “组”是为了方便管理大量用户的权限而设计的，是用户的集合
- 当我们要给一批用户分配同一个权限时，就可以将这些用户都归到一个组中，只要给这个组分配此权限，组内的用户就都会拥有此权限
- Windows Server 2012也使用唯一安全标识符SID来分辨不同的组。权限的设置都是通过SID设置的，不是利用组名



• 总结

- 用户是使用者在计算机系统身份映射，在Windows Server 2012 R2中管理用户需要管理员身份。
- 组是一些用户的集合，组内的用户自动具备为组分配的权限。
- 内置用户和组账户具有特殊的权限，用于特定的用途。

本章实验：配置服务器的用户及组账户

姓名	职位	需加入组	用户名	备注
人力资源部				
白凌	HR主管		Bai.ling	允许管理打印机
技术部				
杨树	技术部经理		Yang.shu	允许关机
唐凯	工程师	云计算项目部	Tang.kai	
张辅政	工程师	网络安全项目部	Zhang.fuzheng	
销售部				
智月楼	销售部经理		Zhi.yuelou	允许关机
陈欢	销售代表	云计算项目部	Chen.huan	
成艳丽	销售代表	网络安全项目部	Cheng.yanli	出差禁用账号
公司办公室				
小马	系统管理员		Xiao.ma	所有权限开放

本章实验：配置服务器的用户及组账户

- 需求描述
 - 为每个员工创建用户账户
 - 根据权限需求创建组账户，并添加成员
 - 为组账户分配策略
 - 测试策略是否生效
- 实现思路
 - 搭建远程访问服务器
 - 创建组账户，并添加对应的成员。
 - 为组分配权限
- 学员练习
 - 30分钟内完成

=====

更多精彩干货内容很快就来，还请持续关注本号哦！

如有找不到的资源，或安装过程出现问题的，请加微信 RSWQRD 告知即可。

(微信如右)



更多精彩干货内容很快就来，还请持续关注本号哦！

如有找不到的资源，或安装过程出现问题的，请关注公众号告知。

(微信公众号如右)

