

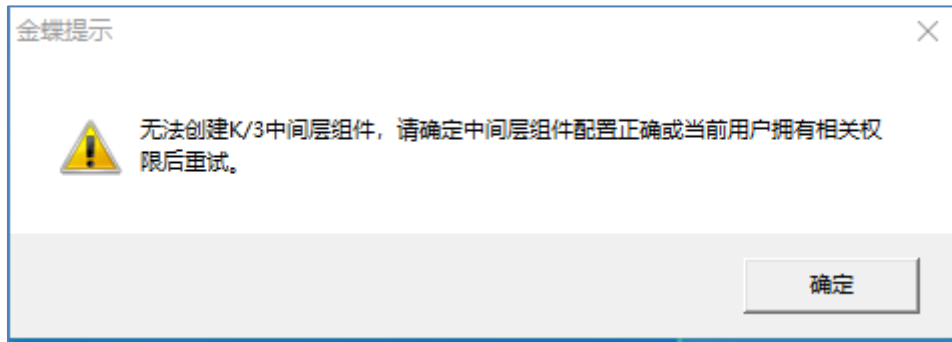
Windows10 系统更新微软补丁后 K/3 WISE 客户端无法使用处理指南

目 录

故障现象:	2
原因分析:	3
解决方案:	4

故障现象：

近来很多客户遇到 win 10 和 win11 电脑，突然无法打开 K/3 WISE，打开之后登录不了界面提示：无法创建中间层，远程组件配置不通过，出现提示如下图所示。



经分析发现，是由于微软发布的最新累积补丁，对 Windows 的安全性进行了调整，调整了 NTLM 非交互式认证过程，以致 K/3 客户不能正常运行远程组件(COM+)服务所致。

受影响的系统及微软补丁例如下表：

windows 版本	小版本	补丁	
win10	21H2	KB5018410 KB5016616	KB5017262
win10	LTSC	KB5018419	
win11		KB5018418	

详细的漏洞补丁列表请见以下链接：

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-37988>

受影响的用户：所有使用 Win10\Win11 的 K/3 客户端用户。

原因分析：

K/3 WISE 客户端调用服务器（中间层）组件时，是采用的 windows 的 RPC（远程过程调用）机制，在调用时，需要进行身份认证，微软累积补丁修订了此认证过程，服务器端不允许其他电脑通过仅来宾身份和匿名身份进行 DCOM 身份验证，若服务器使用仅来宾模式，客户端通过 Guest 帐户提交访问申请，在发起远程调用时，服务器审核会失败，从而导致无法通过 DCOM 通讯。

系统日志分析发现，在更新微软补丁前，远程调用的登录信息如下：



在更新微软补丁后，远程调用的登录信息如下：



由此而引发了 K/3 WISE 的 Win10、Win11 客户端不能正常应用的问题。

解决方案:

经多次尝试,总结出此问题解决方案可以有以下三个,推荐使用“方案一”或“方案二”。

方案一:采用域控模式,确保使用 K/3 的用户具有网络访问权限

域控模式下,域用户是具备域内网络访问权限的,默认会以域用户进行网络验权,不存在此影响。如何启用域控管理,请参考 Windows 域控服务器管理相关说明。

方案二:增加 Com+专用用户,并在客户端添加凭据,客户端将以此用户进行网络认证

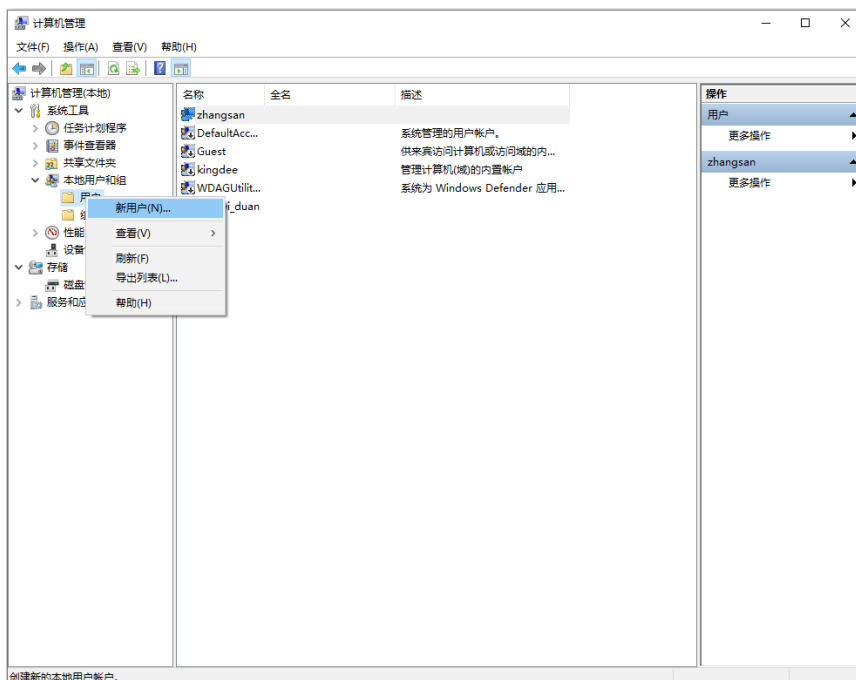
有以下两种方式可以进行配置,根据需要自行选择哪种方式都可。

一、手动配置

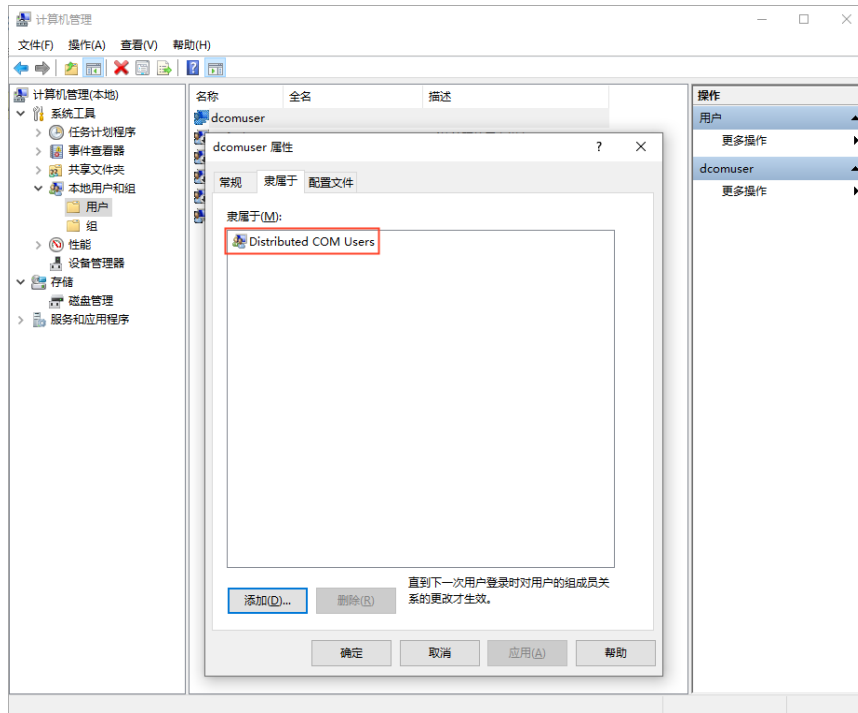
1、在服务器端建立一个用户

(1) 打开【控制面板】->【管理工具】->【计算机管理】,切换到本地用户与组分支,

如下图所示,建立一个新用户,专用于 Com+网络认证;

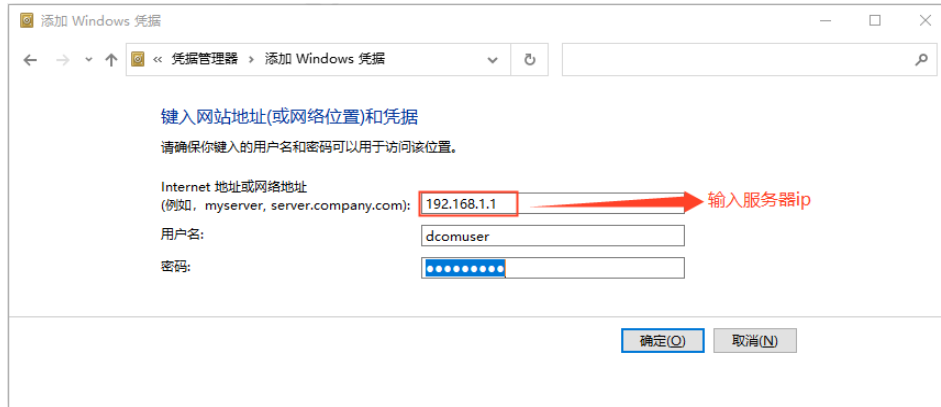


- (2) 新增用户时，勾选【用户不能更改密码】和【密码永不过期】选项后，并采用高强度密码；
- (3) 修改用户的“隶属于”属性，让其隶属于 Distributed COM Users 组，删除其它用户组，如下图所示。



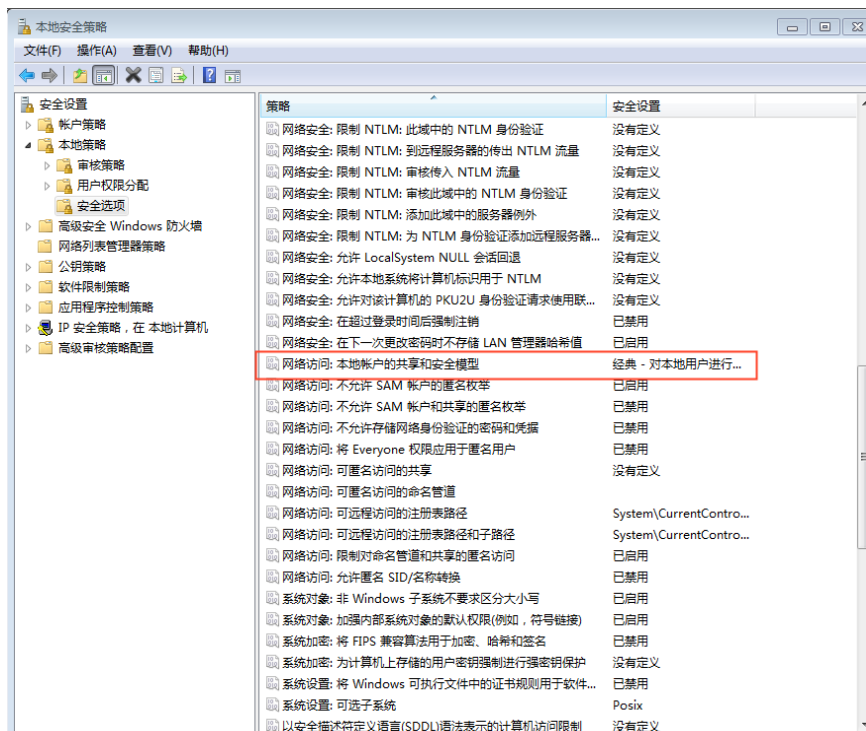
2、客户端添加服务器的 Windows 认证凭据

- (1) 打开“控制面板” ->查看方式设置“大图标”，找到“凭据管理器”（或者运行中输入：control keymgr.dll，直接打开凭据管理界面）；
- (2) 打开凭据管理器，切换到“windows 凭据”，点击“添加 windows 凭据”；
- (3) 在添加 windows 凭据界面，分别输入正确的服务器 IP 地址或计算机名、用户名（如服务器刚建立的用户 dcomuser），再输入正确的密码，点击“确定”完成；
- (4) 部分系统添加凭据后需要重启才能生效，建议添加凭据后重启电脑，如下图所示。

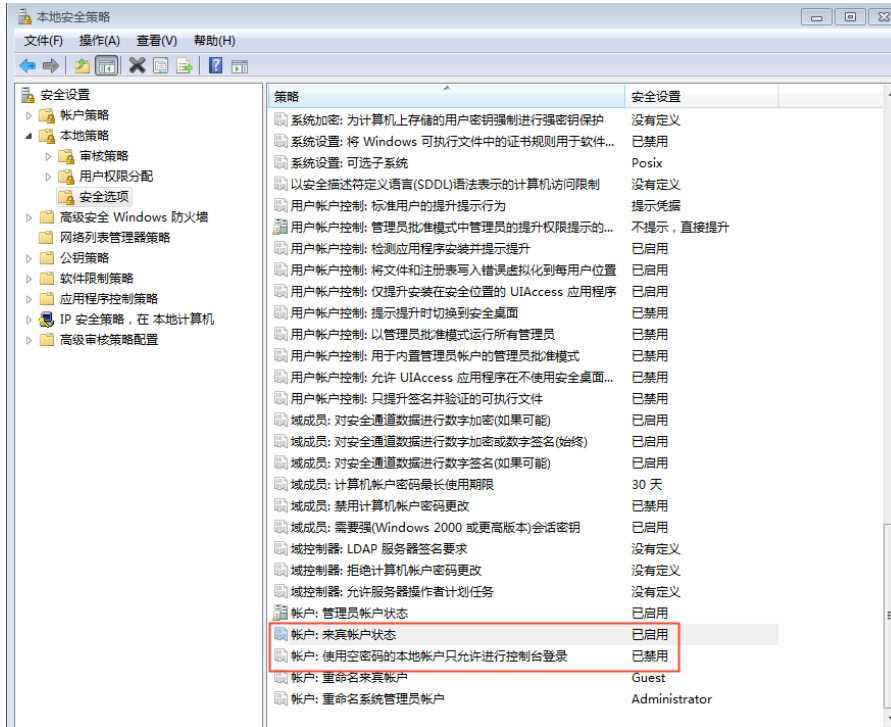


3、服务器端配置，修改中间层的本地安全策略

- (1) 打开【控制面板】→【管理工具】→【本地安全策略】，将【本地策略】→【安全选项】中的“网络访问: 本地帐户的共享和安全模型”修改为【经典-本地用户以自己的身份验证】；



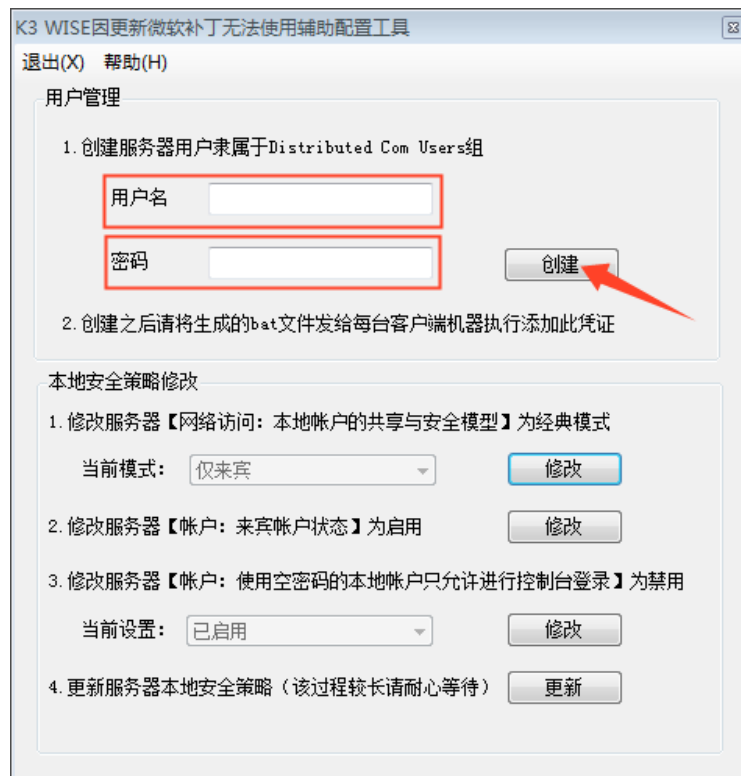
- (2) 在本地安全策略中“帐户: 来宾帐户状态”设置为【已启用】；
- (3) 帐户: 使用空密码的本地帐户只允许进行控制台登录，设置为【已禁用】；



(4) 更新组策略: 打开 cmd->输入 gpupdate 回车。

二、自动配置工具

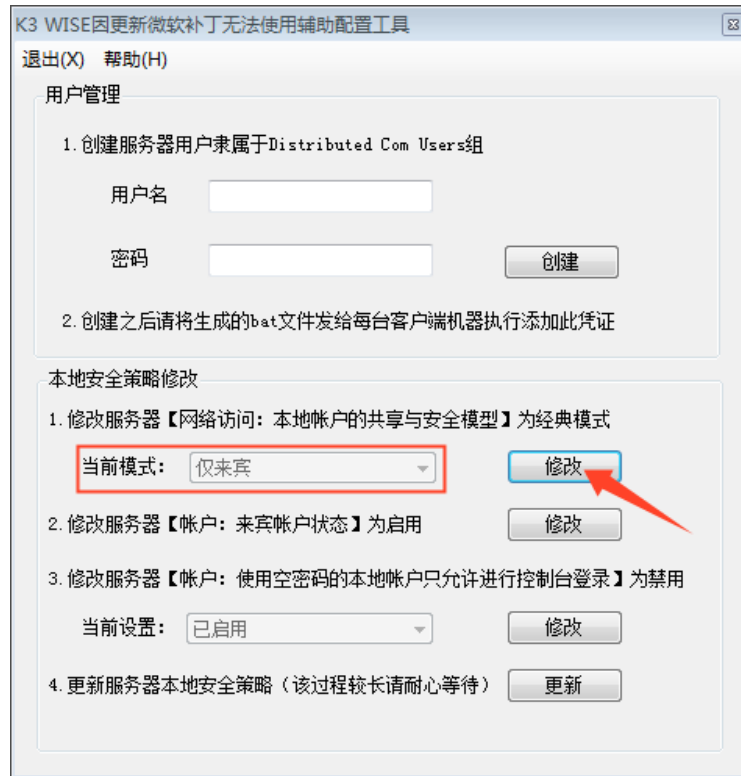
- 1、 下载并将附件中的“K3WISE 因更新微软补丁无法使用辅助配置工具.rar”解压，双击（或以管理员身份运行）打开“K3WISE 因更新微软补丁无法使用辅助配置工具.exe”；
- 2、 在服务器创建用户，输入用户名和密码（须满足机器所设置的密码策略要求），点击【创建】按钮，如下图所示；



- 3、 创建用户成功后（建议不再随意修改该用户密码，避免客户端添加的凭据失效），弹出文件界面，将生成的“客户端添加凭据.bat”文件发送给每台客户端机器执行添加凭据（客户端双击运行该文件即可），如下图所示；

名称	修改日期	类型
 reg.reg	2022/11/1 19:02	注册表项
 reg1.reg	2022/11/10 11:24	注册表项
 Windows10系统更新微软补丁后K3 WIS...	2022/11/3 10:40	Foxit PDF Reade...
 客户端添加凭据.bat	2022/11/8 15:26	Windows 批处理...

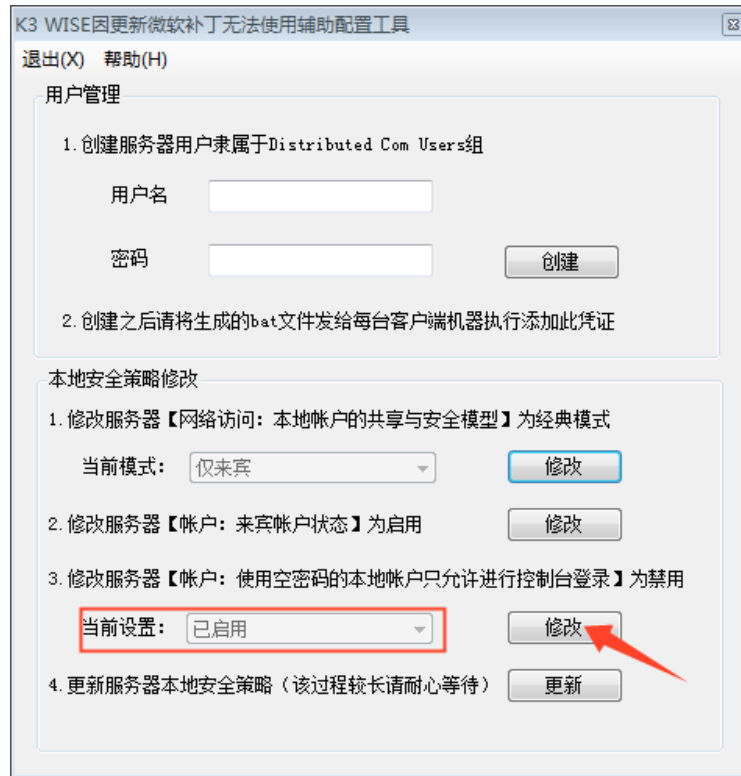
- 4、所有客户端添加凭据完成后，修改服务器【网络访问：本地帐户的共享与安全模式】为经典模式，若当前模式为“仅来宾”，则点击【修改】按钮，如下图所示；



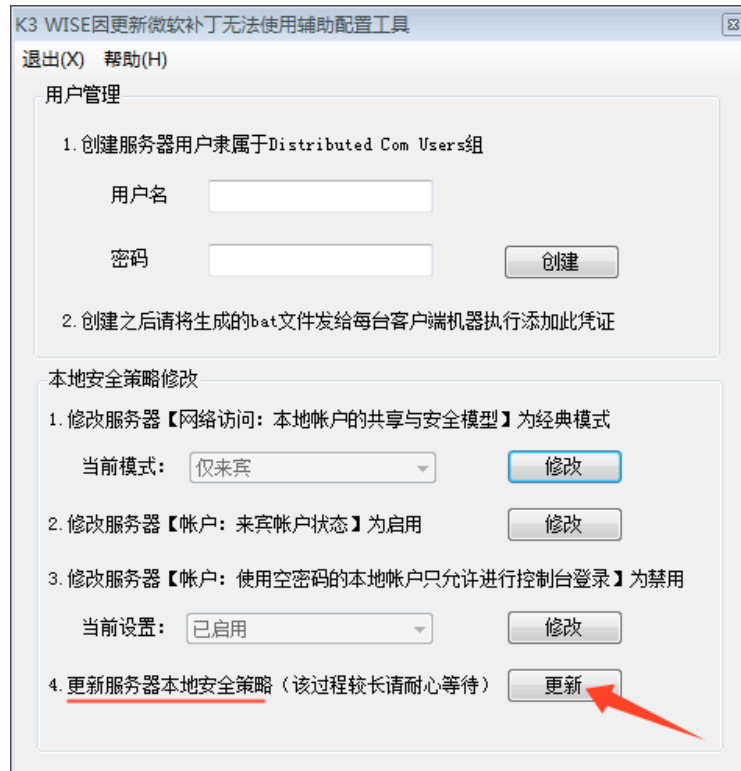
- 5、修改服务器【帐户：来宾帐户状态】为启用，点击【修改】按钮，如下图所示；



- 6、修改服务器【帐户：使用空密码的本地帐户只允许进行控制台登录】为禁用，若当前设置为“已启用”，则点击【修改】按钮，如下图所示；



- 7、更新服务器本地安全策略，点击【更新】按钮，如下图所示。



注意事项:

- (1) 客户端登录用户请不要与服务器端已有用户同名，否则将以客户端登录用户身份进行认证，由于密码极可能不相同，将导致认证失败。**

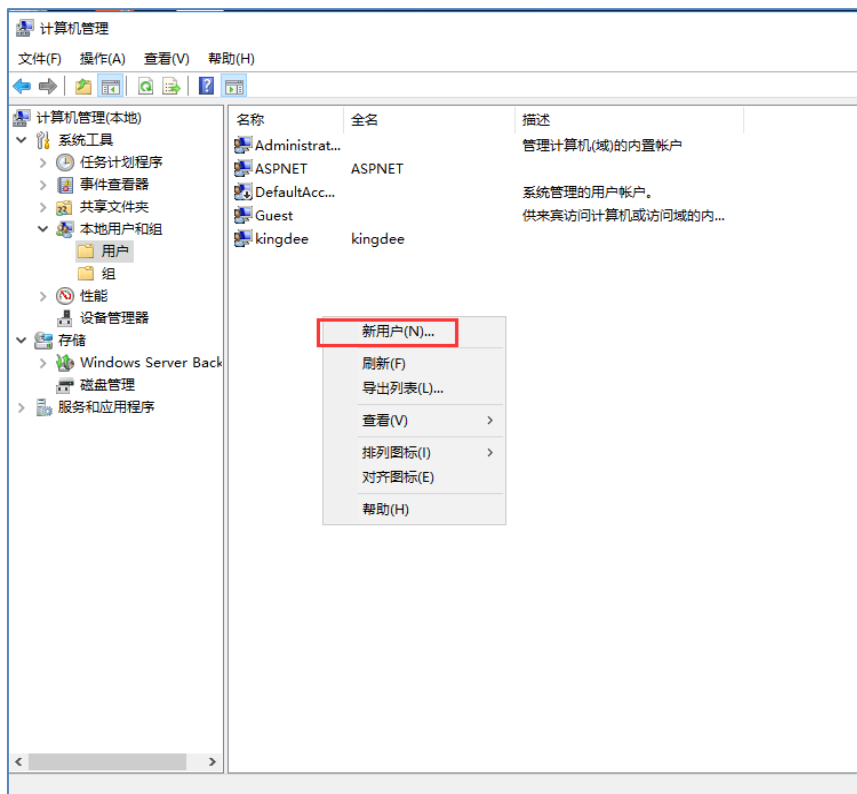
例如：服务器端用户名为 administrator，客户端登录用户名也为 administrator，会导致认证失败，需要修改客户端用户名，附件提供了批处理修改客户端用户名的文件，请下载解压后右键编辑文档，在需要修改的位置填入修改前的用户名以及修改后的用户名，修改后保存，在客户端双击运行，完成后需重启客户端生效。

- (2) 若按以上步骤操作以后 win10 客户端还是无法连接，请确认电脑的版本号是否为 20H2 以下版本，例如 1909 或 1803 版本的电脑，都需要将电脑更新到 20H2 以上版本（例如 21H2 版本都是可以的）。**

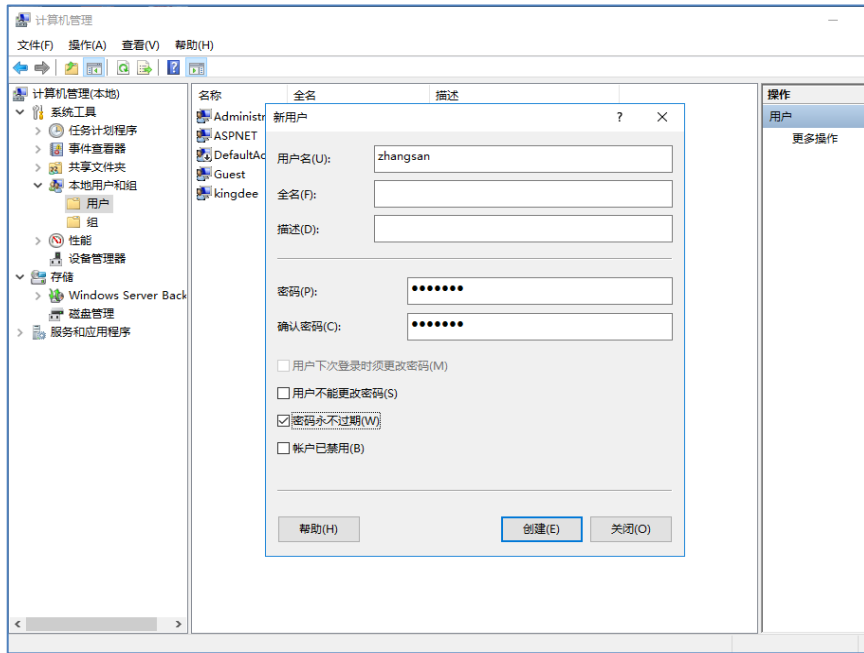
方案三：设置同名同密码用户（客户端登录用户在服务器端存在，且用户名与密码完全相同）

在服务器的用户管理中，添加每个客户端电脑的 Windows 的登录用户，并保持与客户端登录用户的用户名、密码完全相同，使客户端的 Windows 登录用户能够通过网络身份认证。

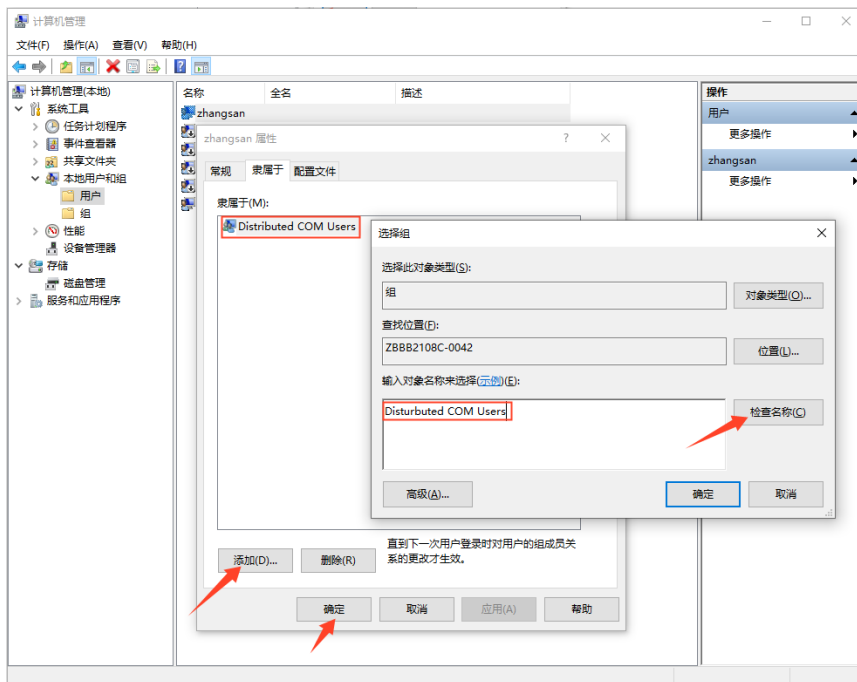
- 1、 右键点击计算机弹出快捷菜单选择【管理】->【计算机管理】或 Win+R 快捷键打开运行输入 compmgmt.msc 点击确定后可打开计算机管理；
- 2、 在服务器端添加客户端的登录用户，并保证与客户端的用户的密码一致；



- 3、 添加用户信息、用户名和密码，注意勾选【密码永不过期】选项，其他选项均不勾选，点击创建，如下图所示；



- 4、设置用户权限，将用户添加进 Disturbed COM Users 组，设置好之后建议重启一下中间层服务器，如下图所示。（建议仅保留该用户组权限，其它用户组清理，以保证服务器安全）



注意事项：若按照方案三操作客户端还是无法连接中间层，请再按照方案二操作。