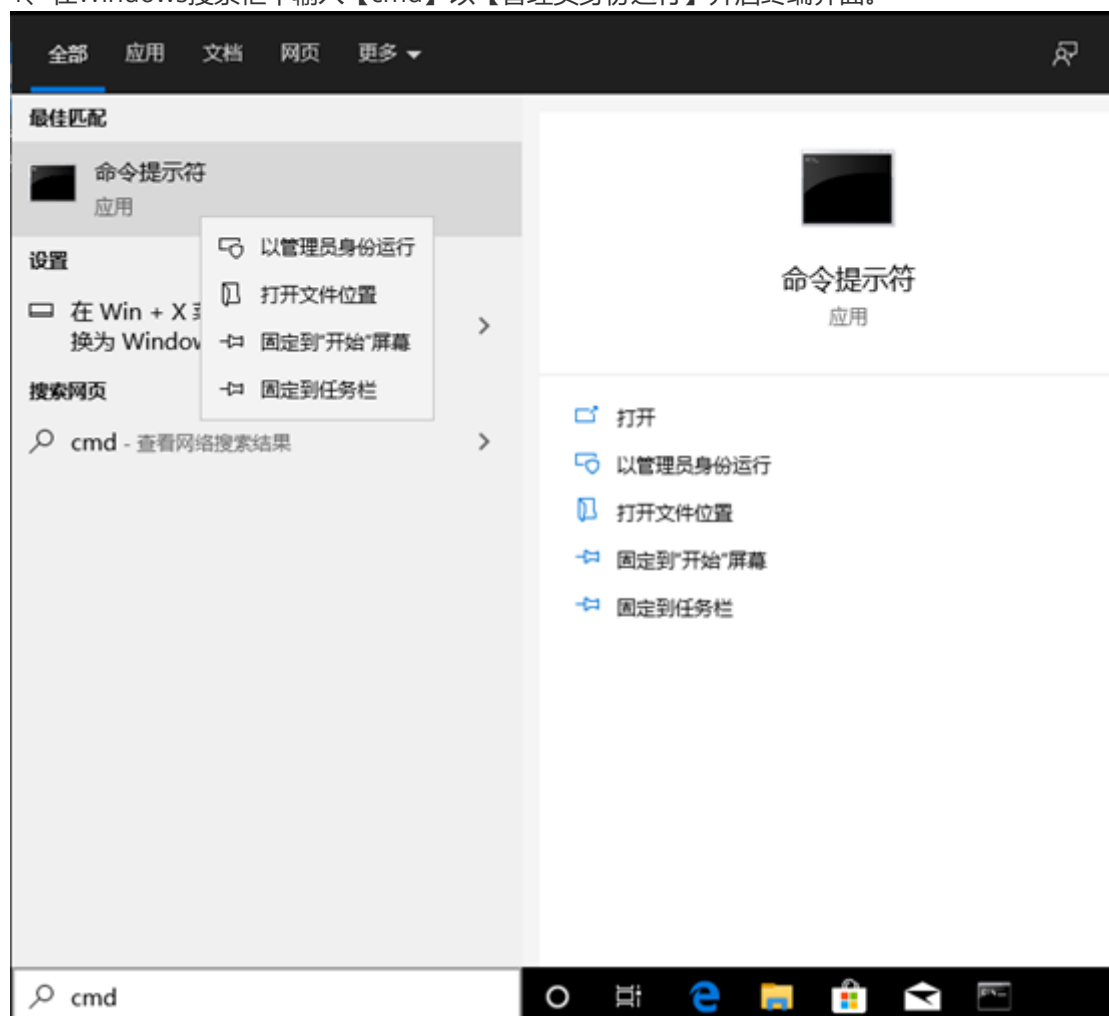


# Windows注册表操作 实验步骤

## 使用reg命令管理注册表

1、在Windows搜索框中输入【cmd】以【管理员身份运行】开启终端界面。



2、打开Windows的dos界面，并使用reg命令创建注册表。使用命令 `reg add hkcu\test /v hello /t REG_SZ /d "this is test!" /f`。在HKEY\_CURRENT\_USER根键中新建一个子键名为test，新建键值名称为hello，值为this is test，值的类型为REG\_SZ。

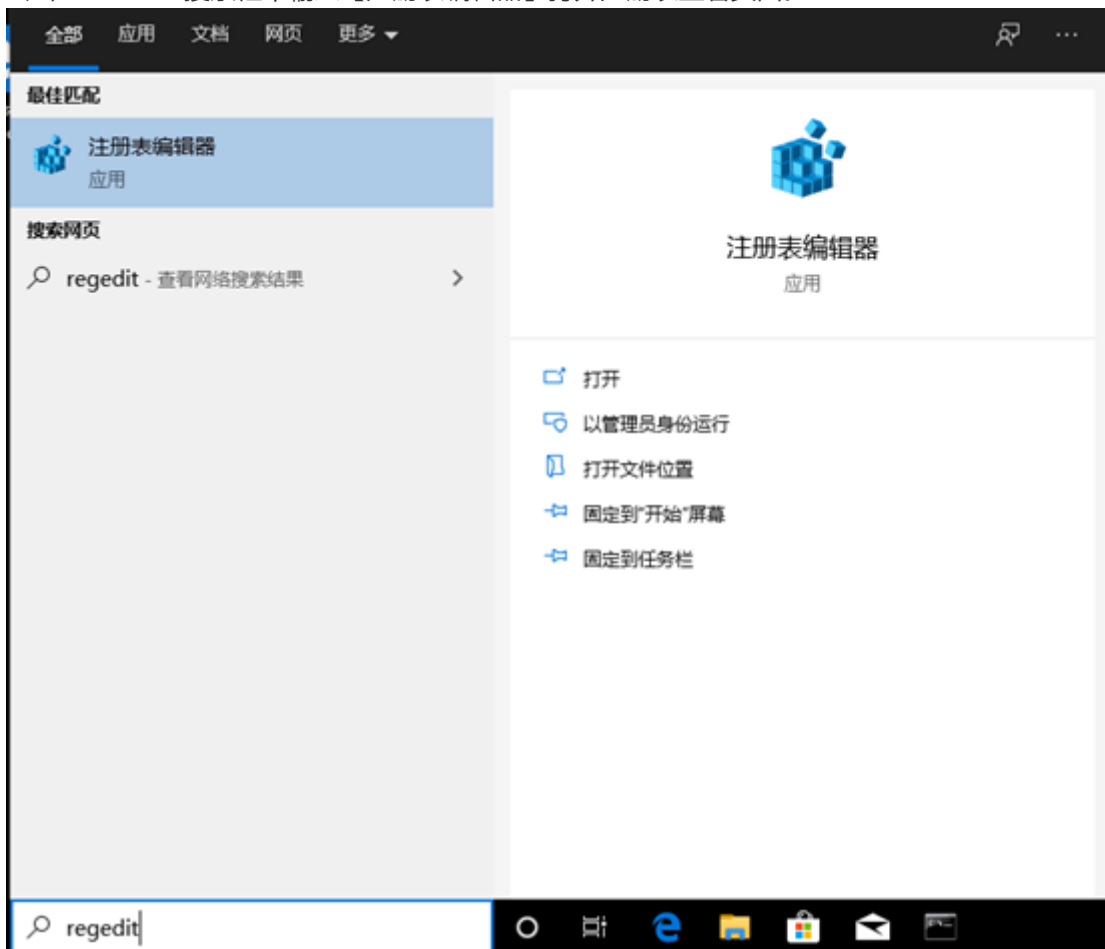
/v表示需要创建的值的名称，/t表示值的类型，/d表示这个值的数据，/f表示强制不提示。

在reg中将注册表进行了简写，简写方法如下：

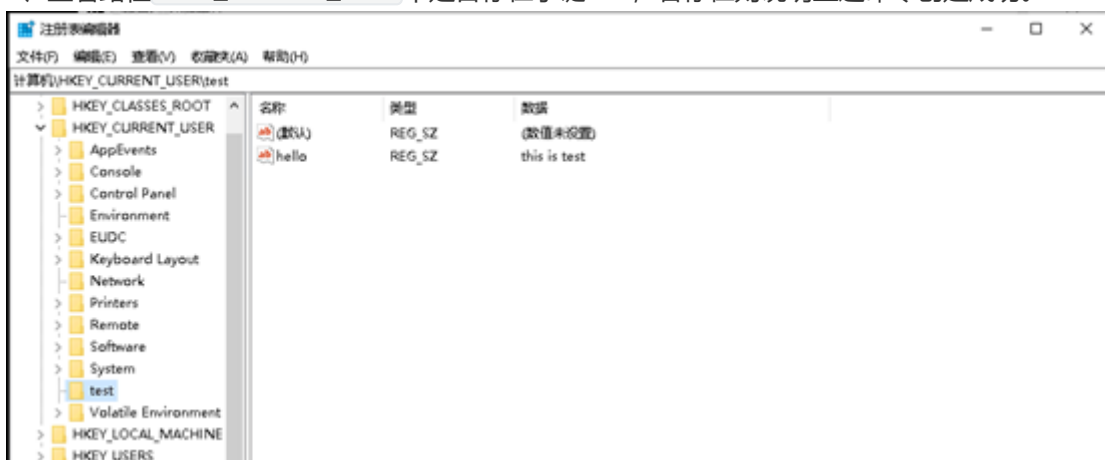
```
HKCU--->HKEY_CURRENT_USER;
HKLM--->HKEY_LOCAL_MACHINE;
HKU--->HKEY_USERS;
HKCC--->HKEY_CURRENT_CONFIG。
```



3、在Windows搜索框中输入【注册表编辑器】打开注册表查看页面。

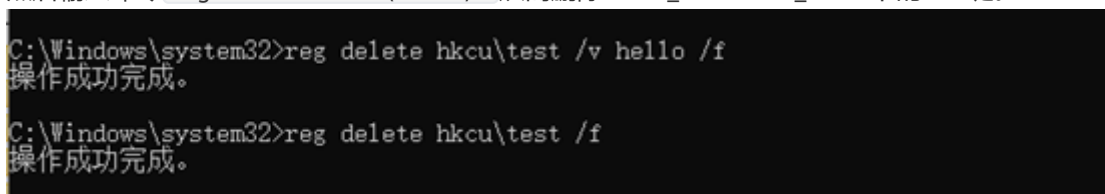


4、查看路径 HKEY\_CURRENT\_USER 中是否存在子键test，若存在则说明上述命令创建成功。



5、在Windows的dos界面中输入命令 `reg delete hkcu\test /v hello /f` 从而删除 HKEY\_CURRENT\_USER 下test键的hello值。

然后输入命令 `reg delete hkcu\test /f` 从而删除HKEY\_CURRENT\_USER下的test键。



# 使用reg命令启动Windows的远程桌面连接功能

1、使用reg命令查看Windows系统的远程桌面是否开启。

使用命令 `reg query HKLM\SYSTEM\CurrentControlSet\Control\Terminal" "Server /v fDenyTSConnections`。

查询fDenyTSConnections值为“0x1”，这说明该主机远程桌面功能处于关闭状态。

```
C:\Windows\system32>reg query HKLM\SYSTEM\CurrentControlSet\Control\Terminal" "Server /v fDenyTSConnections
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server
fDenyTSConnections    REG_DWORD    0x1
```

2、使用reg命令将Windows系统的远程桌面修改为开启。（也就是将上文fDenyTSConnections值从0x1修改为0x0）

使用命令 `reg add HKLM\SYSTEM\CurrentControlSet\Control\Terminal" "Server /v fDenyTSConnections /t REG_DWORD /d 00000000 /f`。

```
C:\Windows\system32>reg add HKLM\SYSTEM\CurrentControlSet\Control\Terminal" "Server /v fDenyTSConnections /t REG_DWORD /d 00000000 /f
操作成功完成。
```

3、使用reg命令查看Windows系统中远程桌面功能对应的端口号。

使用命令 `reg query HKLM\SYSTEM\CurrentControlSet\Control\Terminal" "Server\WinStations\RDP-Tcp /v PortNumber`。

查询PortNumber值为“0xd3d”（该值为十六进制），转换为十进制值为3389。

```
C:\Windows\system32>reg query HKLM\SYSTEM\CurrentControlSet\Control\Terminal" "Server\WinStations\RDP-Tcp /v PortNumber
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp
PortNumber    REG_DWORD    0xd3d
```

4、验证功能。在Windows搜索框中输入【此电脑】，然后右键点击【属性】->【远程设置】，查看Windows系统的远程功能选项从之前的【不允许远程连接到此计算机】切换到了【允许远程连接到此计算机】。

