微云点
vcloudpoint

《AppLocker 组策略》

微信公众号

AppLocker 组策略

限制云终端用户运行与安装软件

AppLocker 组策略功能说明：

AppLocker 组策略为 Windows 系统自带组策略，用于限制指定用户或用户组运行和安装指定路径的应用程序。

一般情况下，只有 admin 管理员才有权限安装程序。云终端用户为普通用户，无法自行安装程序，但绿色软件或某些软件安装包（例如，搜狗浏览器）不需要 admin 管理员权限也能运行和安装，因此使用 AppLocker 组策略直接限制用户打开应用程序，能更有效限制云终端用户擅自使用其他程序。

指导文档系统环境：

Windows 7 x64 旗舰版

磁盘分区：

C 盘——系统+软件盘

D 盘——公共盘

E 盘——私有盘

温馨提示：

- AppLocker 组策略需与用户账户控制（UAC）搭配使用，可参考《**用户账户控制（UAC）**》开启 UAC；
- 设置 Applocker 前请规范软件安装路径，务必将软件安装在 **C:\Program Files** 或 **C:\Program Files (x86)**路径下，因为 Program Files 文件夹是系统创建的文件夹，专门用来存放应用程序，有特定的权限限制，普通用户无法随意读写；
- AppLocker 适用操作系统：Windows 7（旗舰版、企业版），Windows 8.1 企业版，Windows 10 企业版，Server 2008R2（Standard、企业版、Datacenter），Server 2012R2（Standard、Datacenter），Server 2016（Standard、Datacenter）。

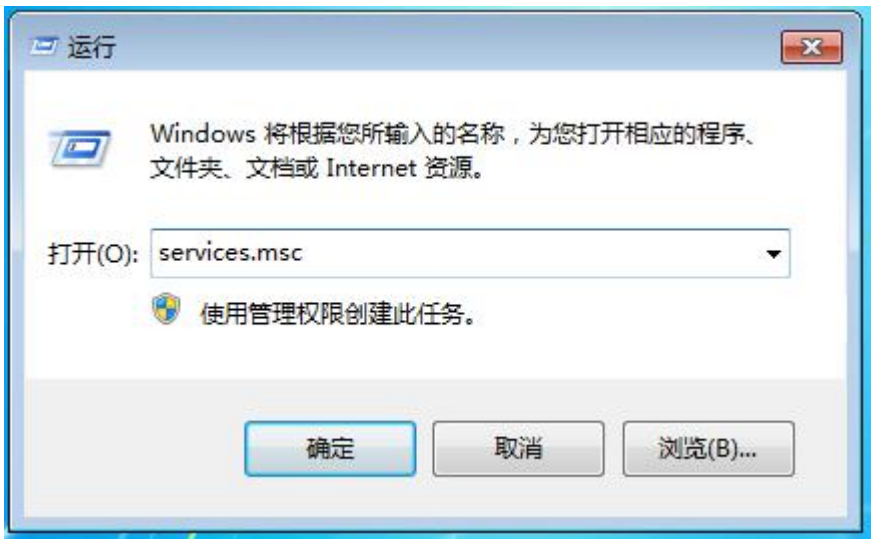
Applocker 配置简易步骤：

1) **Application Identity** 服务项设置为自启
2) 进入**本地组策略编辑器—AppLocker**
3) **可执行规则**，**Windows 安装程序规则**，**脚本规格**都**创建默认规则**
4) **AppLocker** 开启**配置规则强制**
5) 重启主机，组策略生效

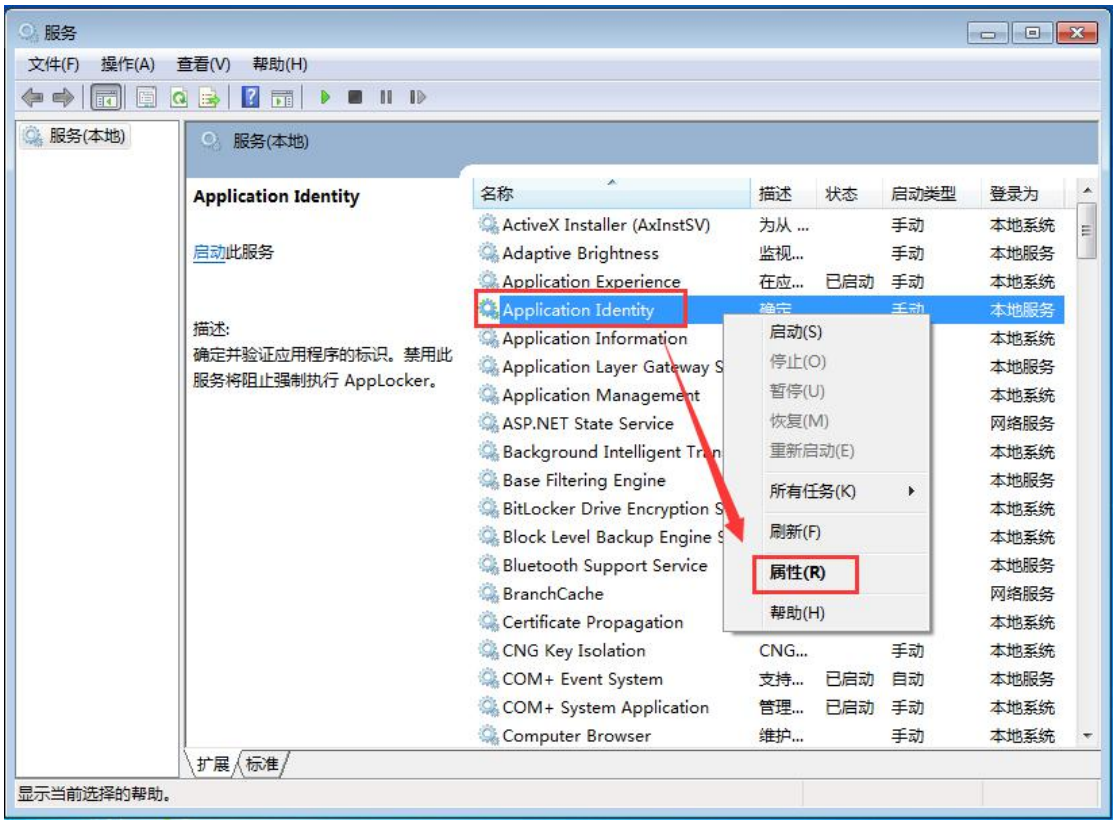
目录

AppLocker 限制云终端用户详细步骤

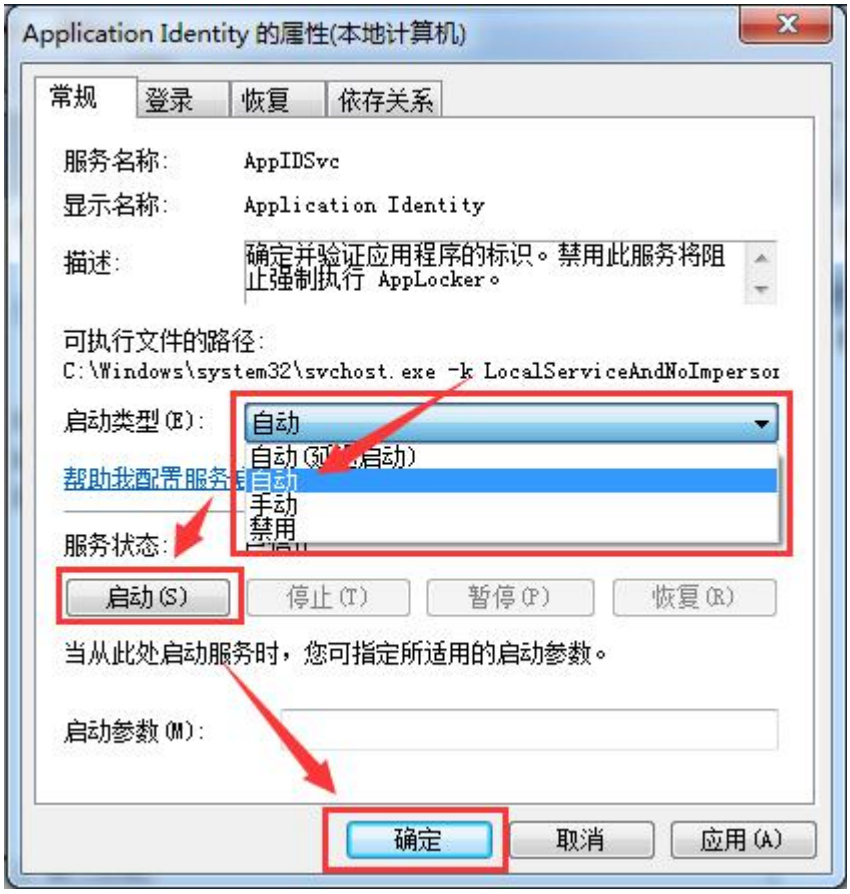
1) **admin 账号**运行 **services.msc**



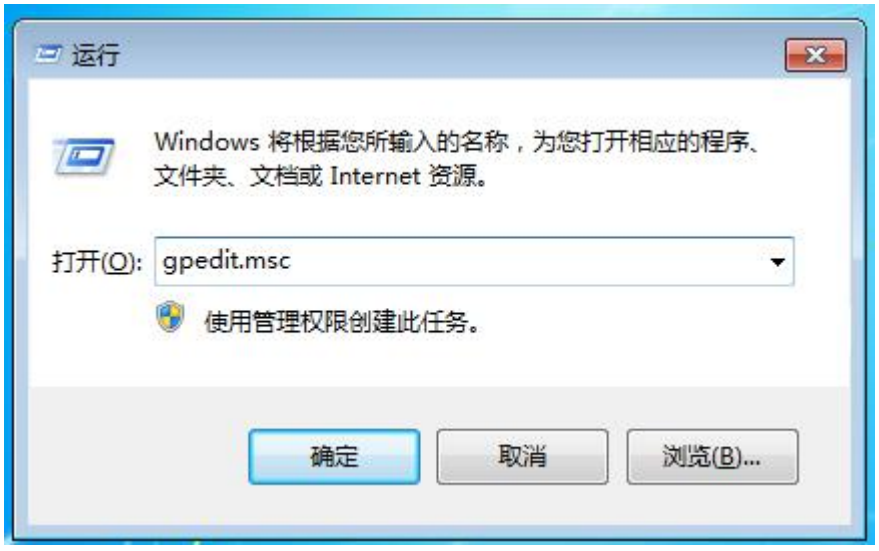
2) 进入**服务**，右键 **Application Identity**，进入**属性**



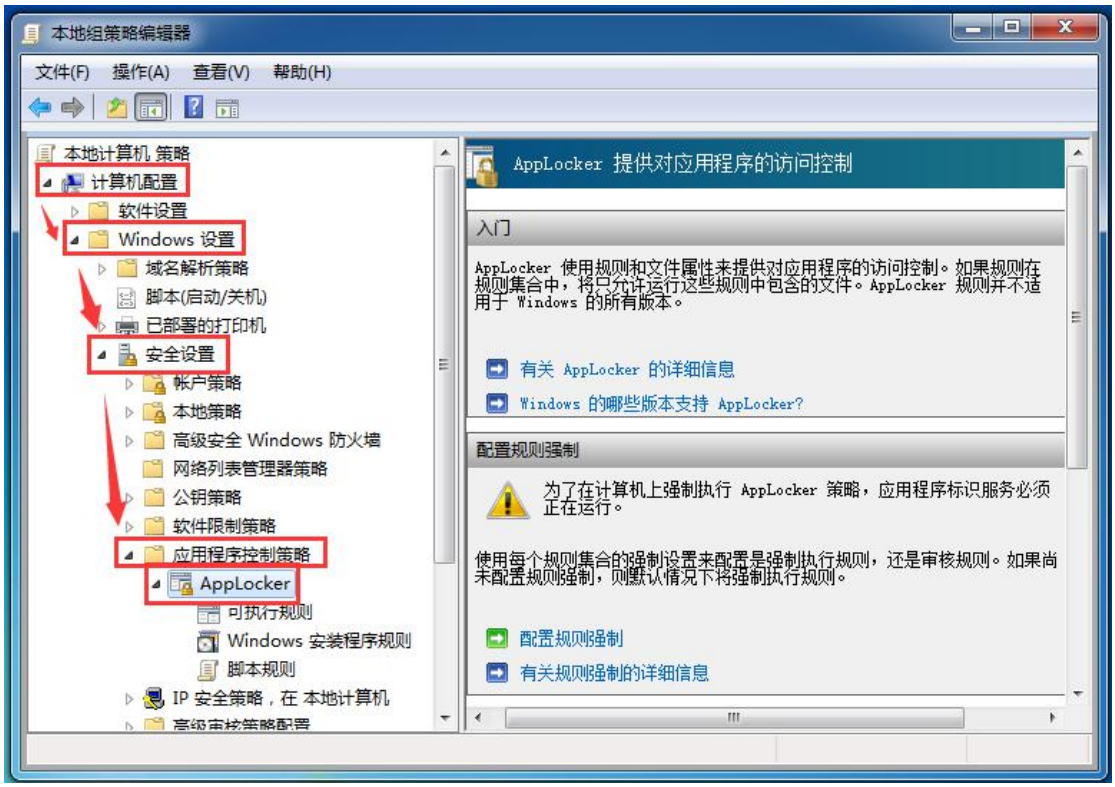
3) **启动类型**设置为**自动**，并**启动**服务



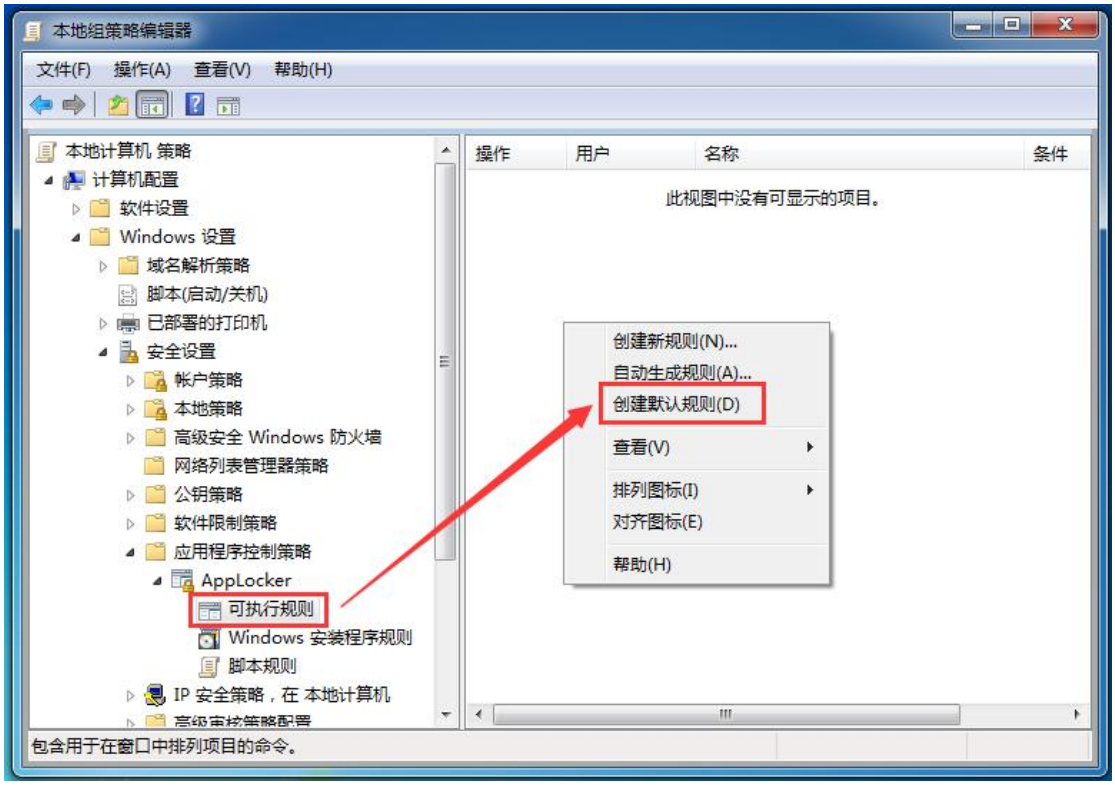
4) **admin 账号**运行 **gpedit.msc**，进入本地组策略编辑器



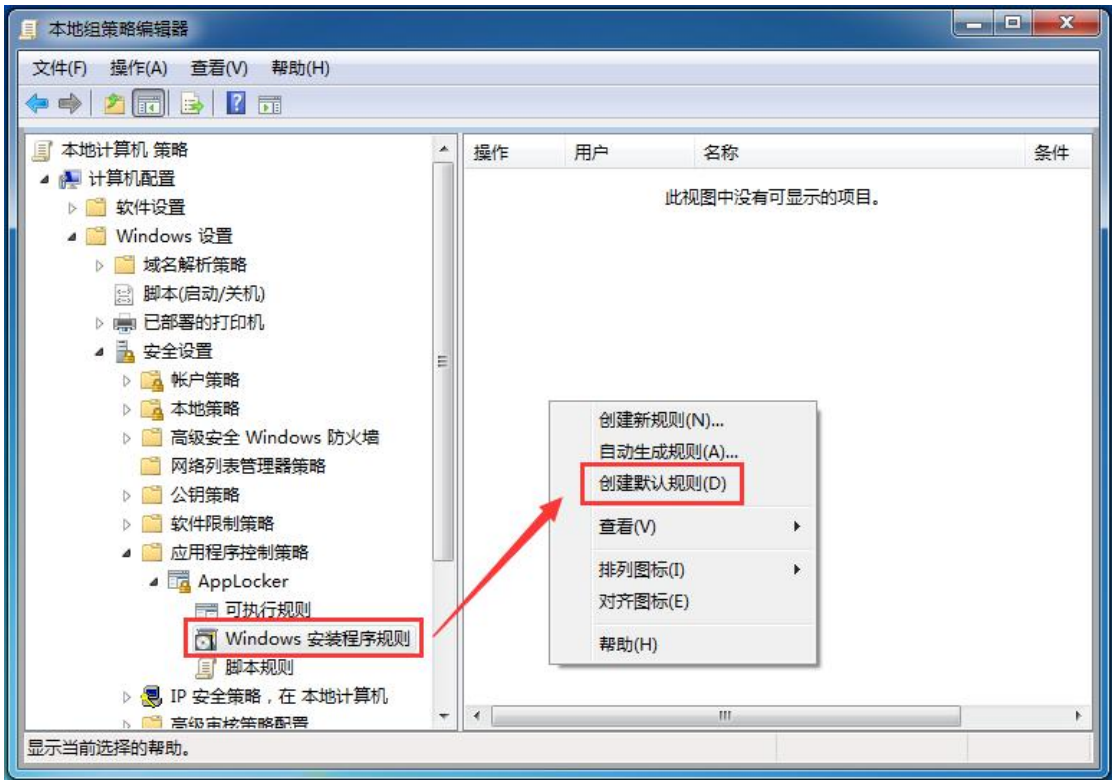
5) 找到 **AppLocker**（本地计算机策略-计算机配置-Windows 设置-安全设置-应用程序控制策略-AppLocker）



6) 选中**可执行规则**，右边框空白处鼠标右键，选择**创建默认规则**（该默认规则为：所有用户只能运行 C:\Program Files 或 C:\Program Files (x86)路径下的程序）

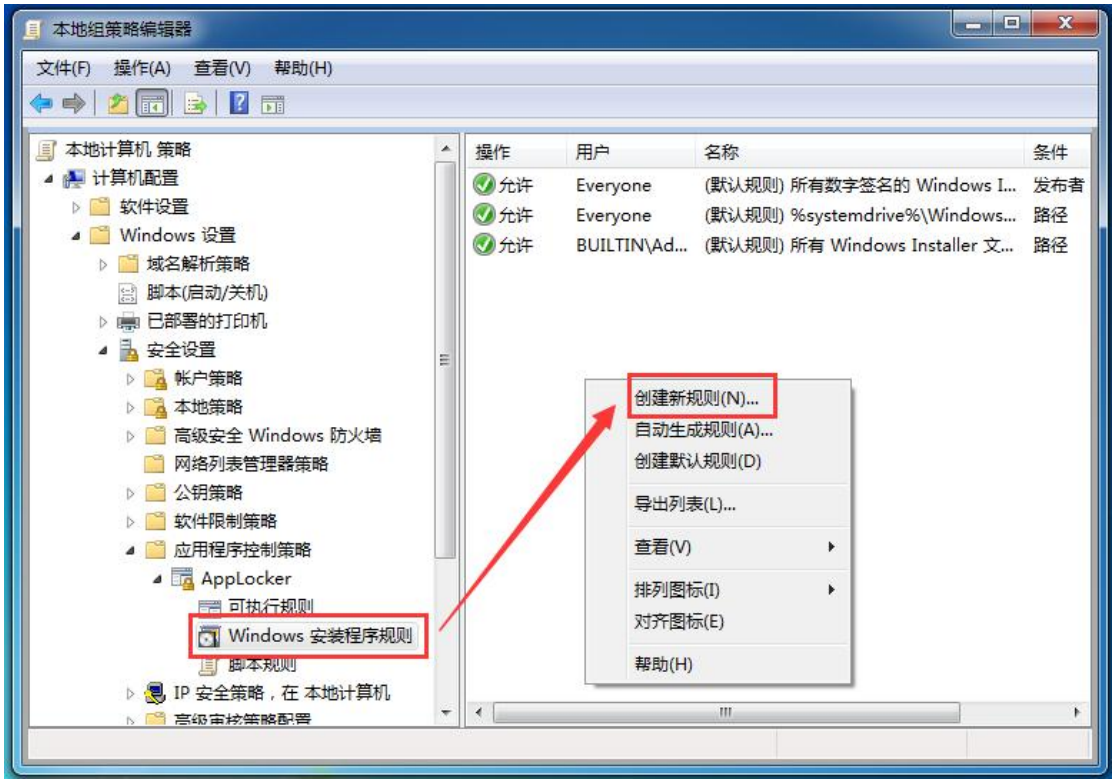


7) 选中 **Windows 安装程序规则**，在右边框空白处鼠标右键，**创建默认规则**（该默认规则为：仅管理员可运行.exe/.msi 安装程序）

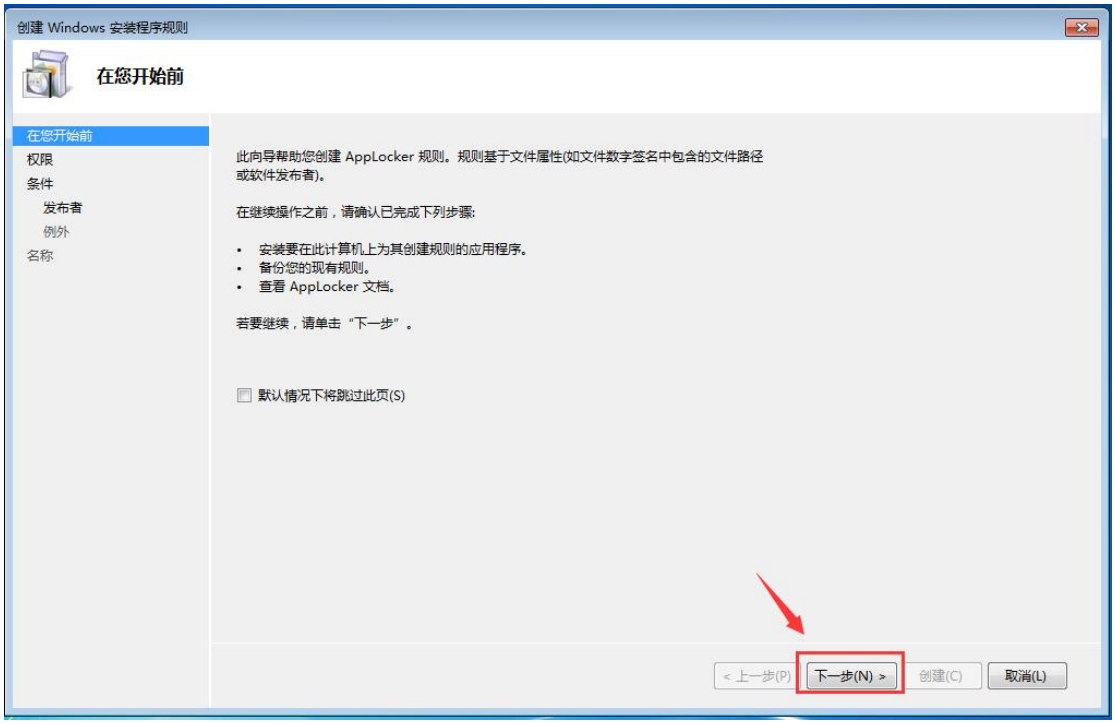


注意：为更有效阻止普通用户安装程序，需创建新规则，将所有磁盘盘符设置为拒绝，请参考步骤 8~20，禁止云终端用户在 C、D、E 盘安装软件

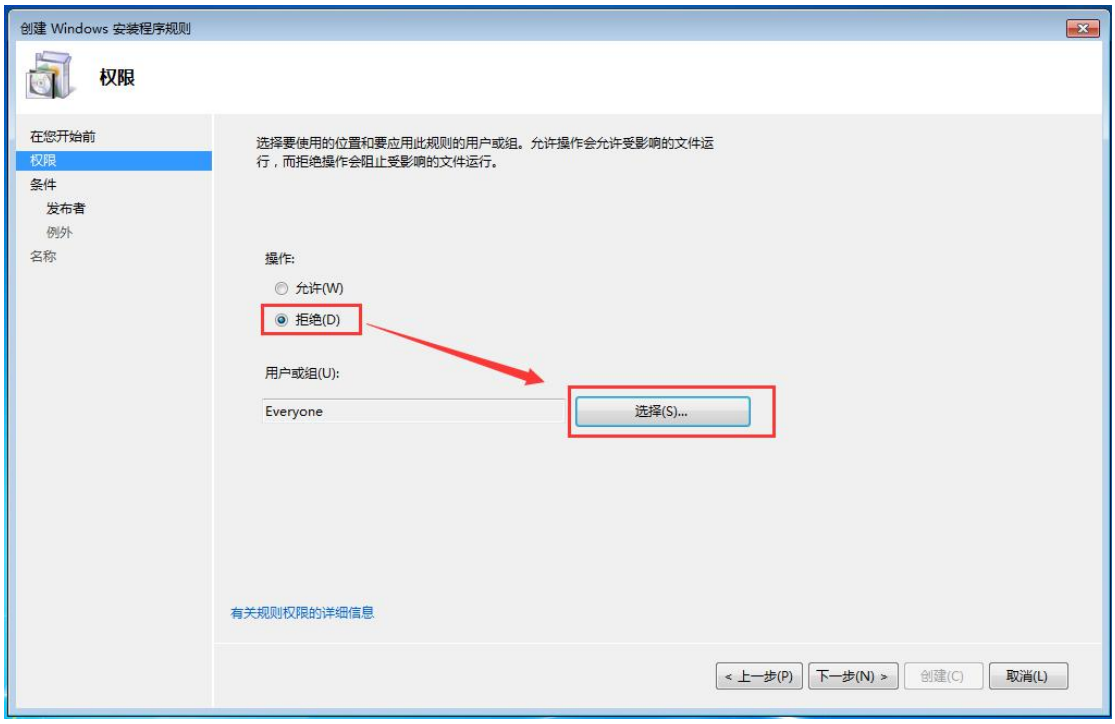
8) 在右边框空白处鼠标右键，**创建新规则**



9) **下一步**

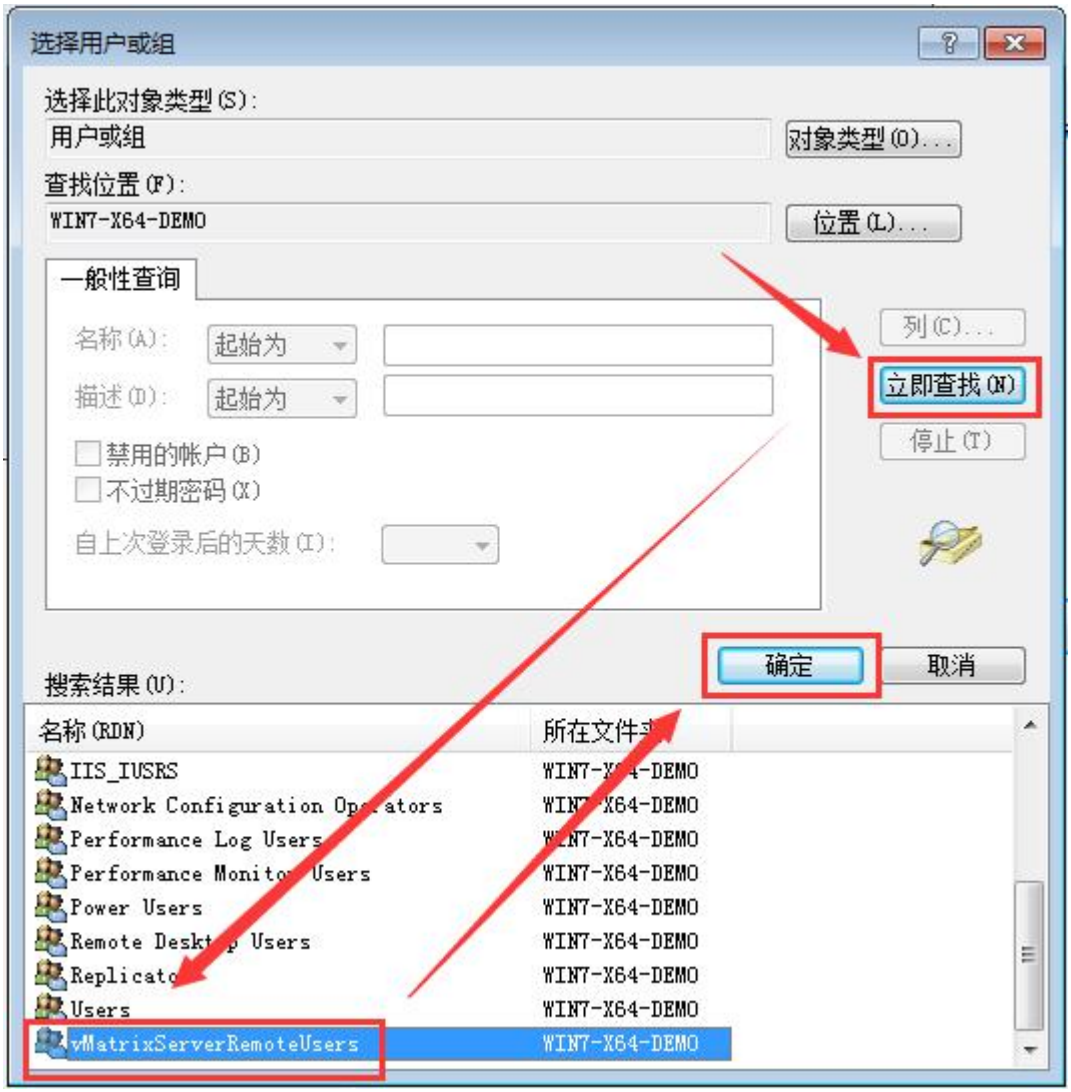


10) 选择**拒绝**，并**选择**需要拒绝的用户组



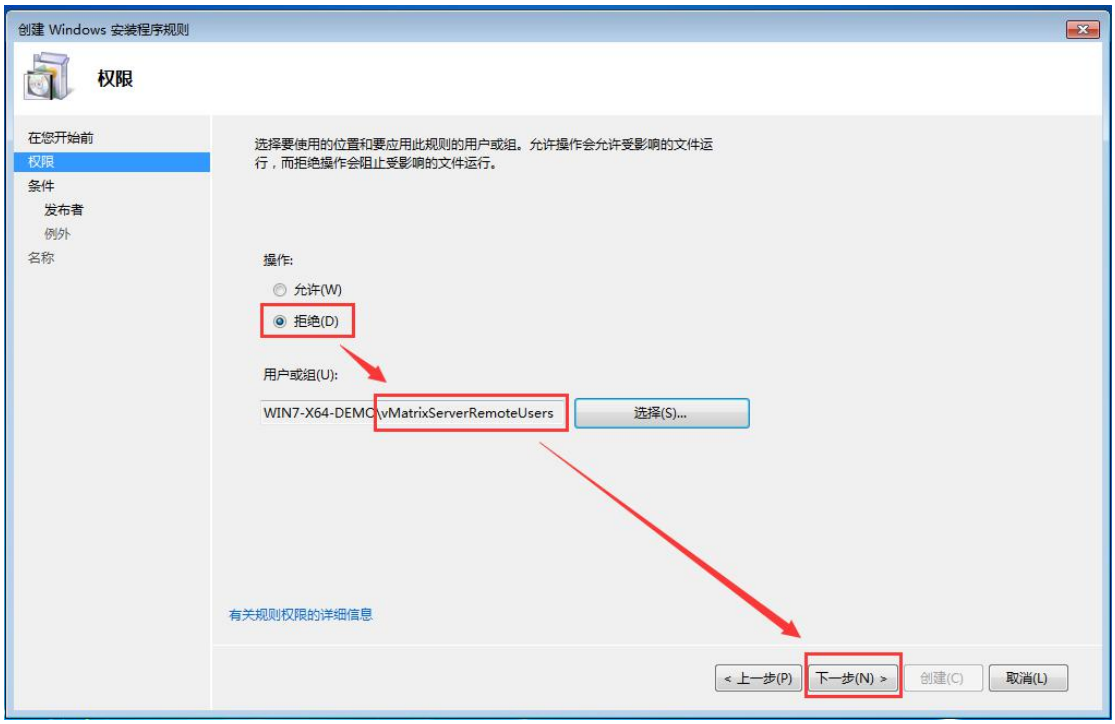
11) 点击**高级**

12) **立即查找**，选中 **vMatrixServerRemoteUsers** 用户组，**确定**

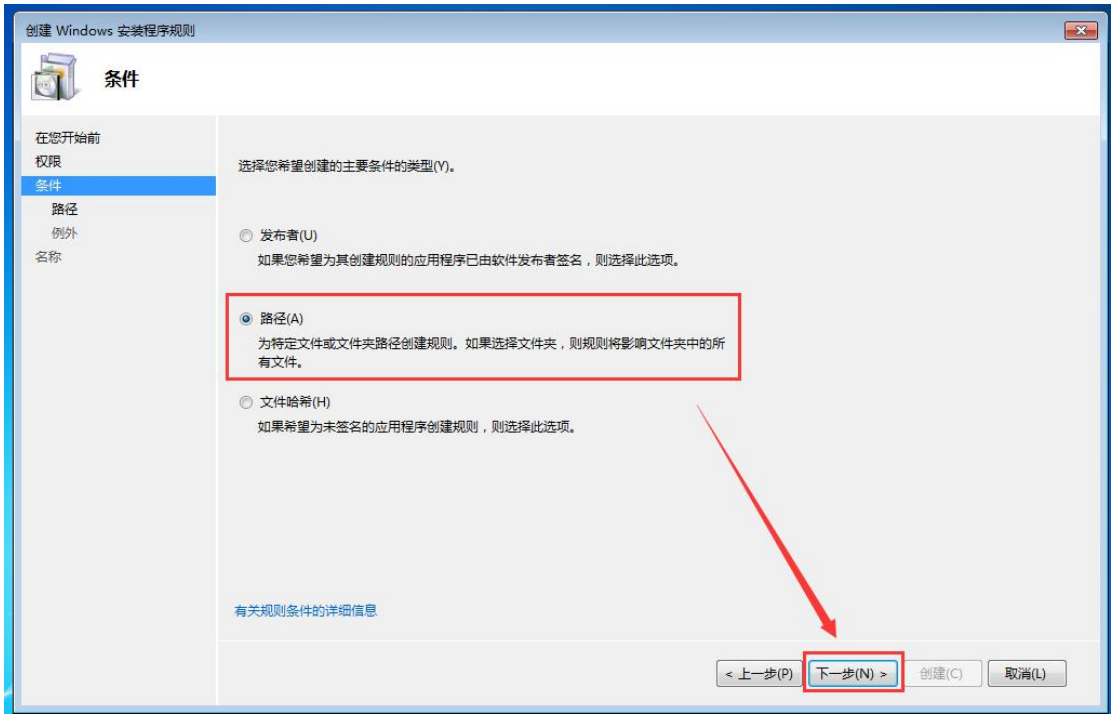


13) 再次确认选择的是 **vMatrixServerRemoteUsers** 用户组，**确定**

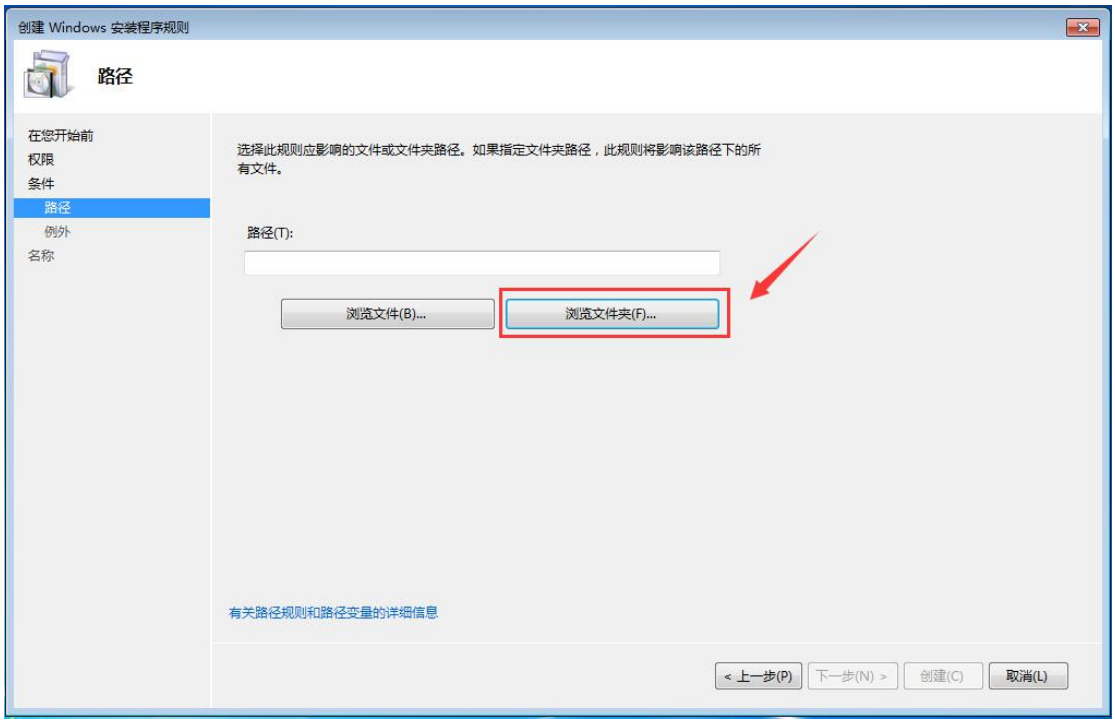
14) 确认选择了**拒绝**，**下一步**



15) 选择**路径**类型，**下一步**

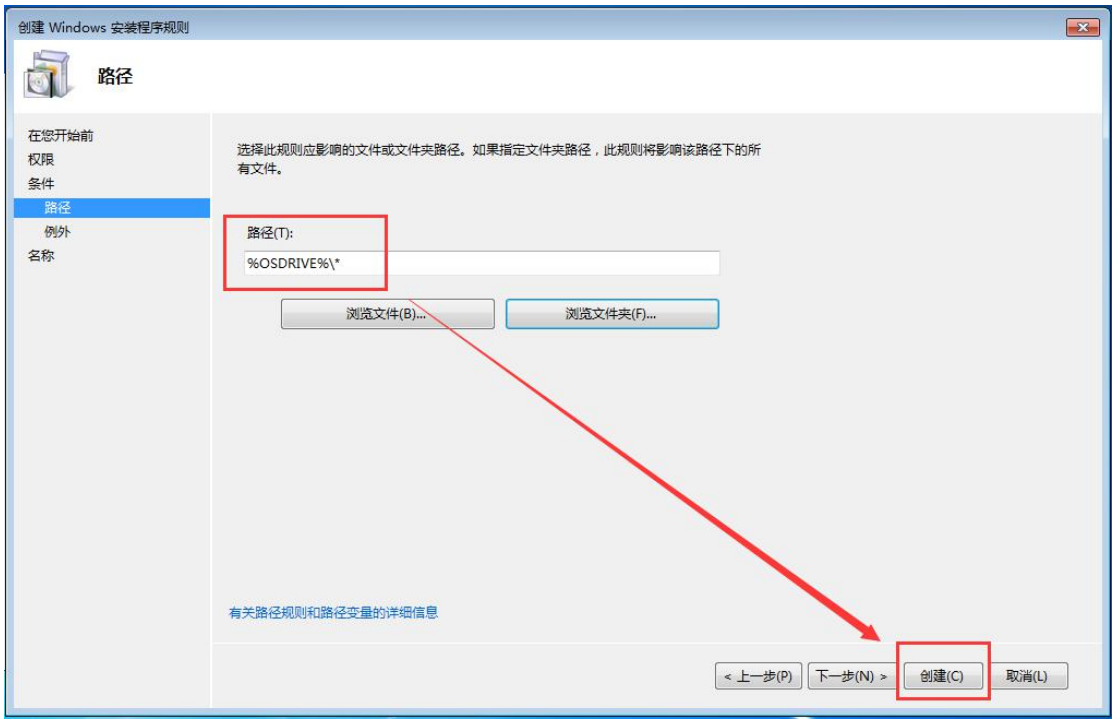


16) 选择**浏览文件夹**

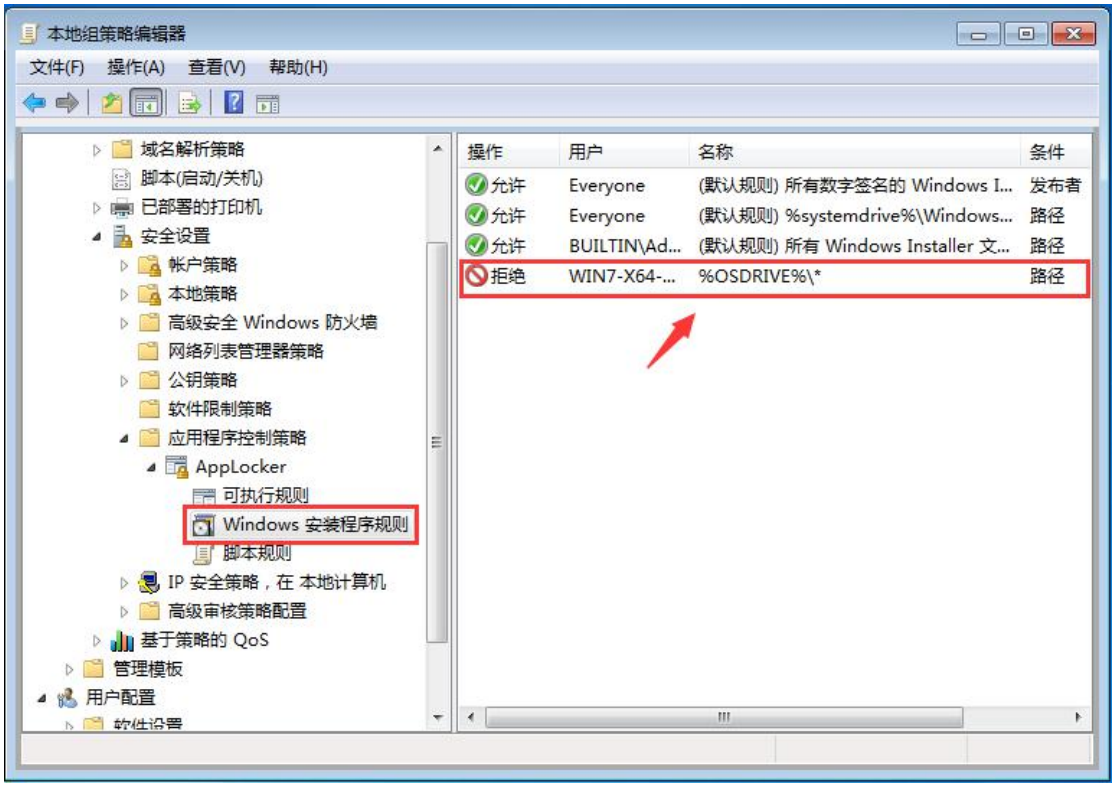


17) 选择 **C 盘**根目录，**确定**

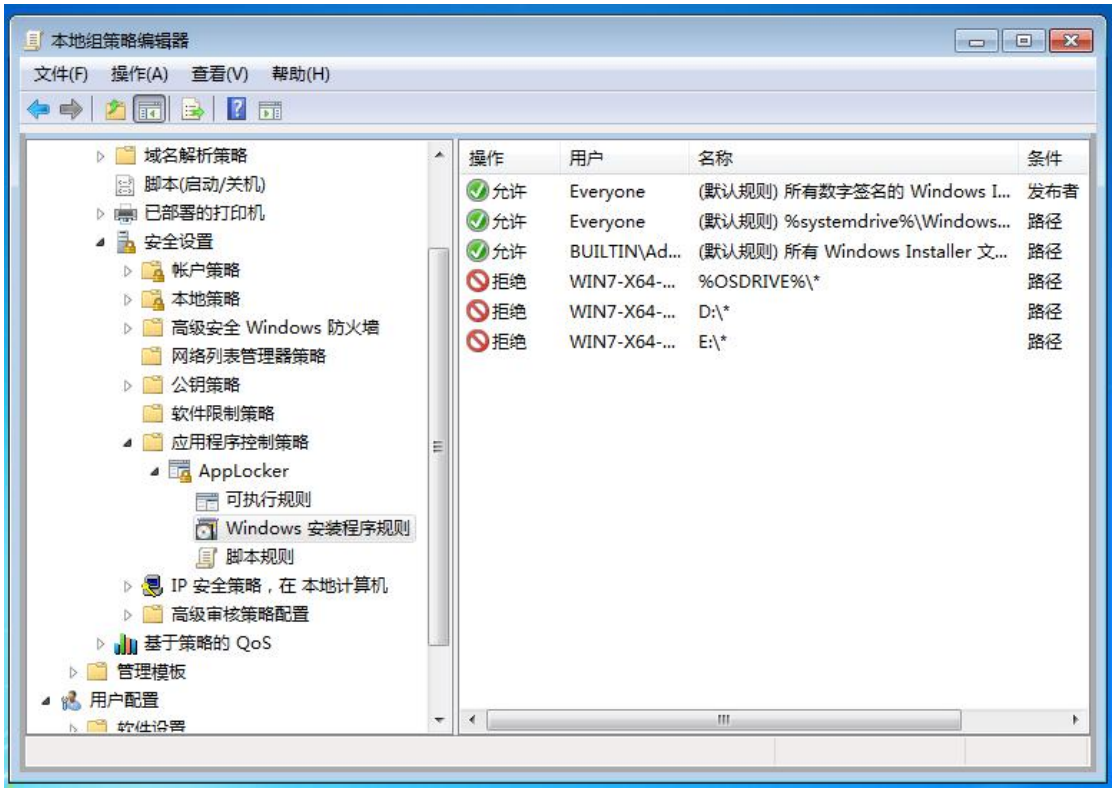
18) 确认**路径**（C 盘根目录显示为%OSDRIVE%），**创建**



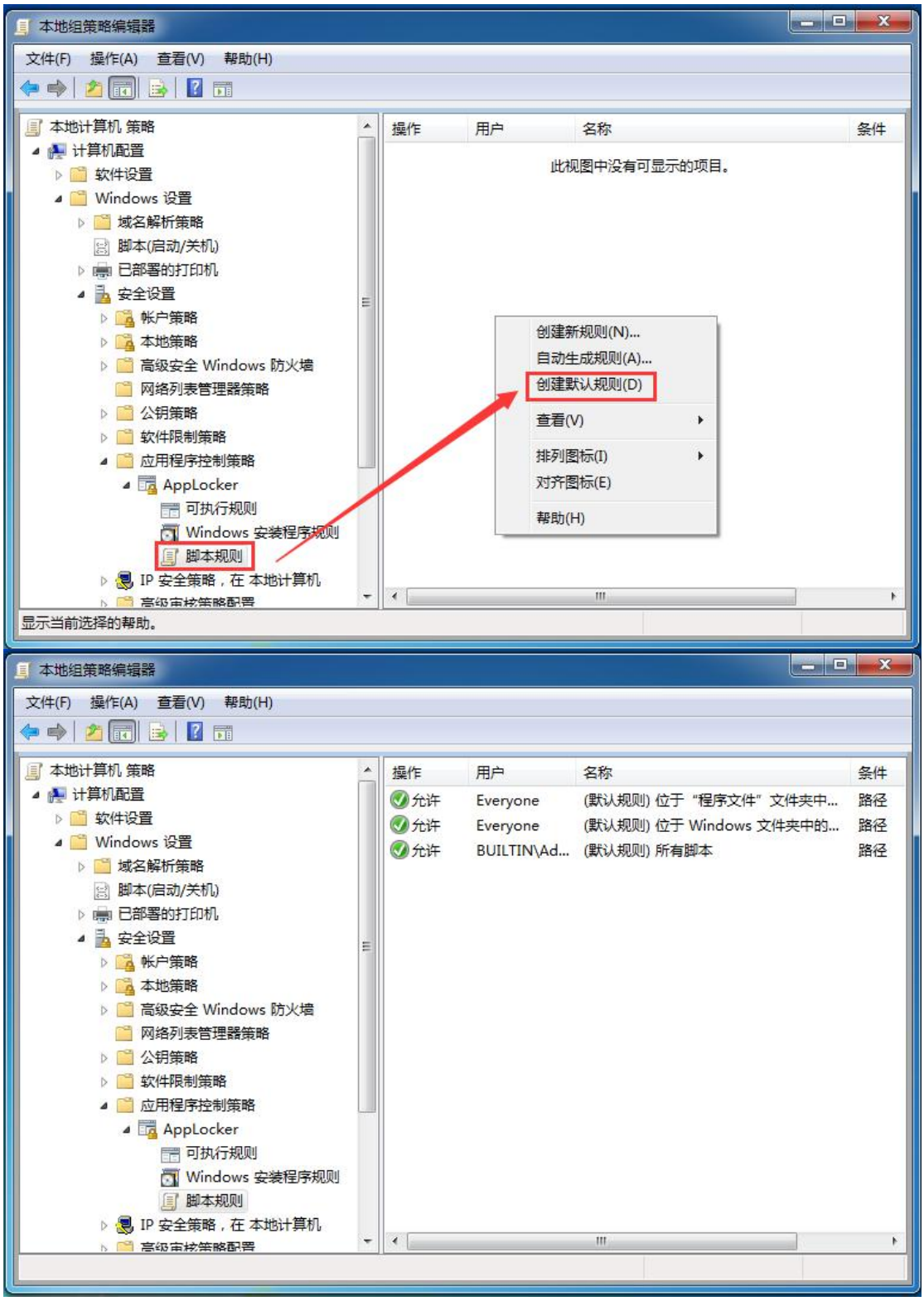
19) 可以看到自创建的**拒绝**规则



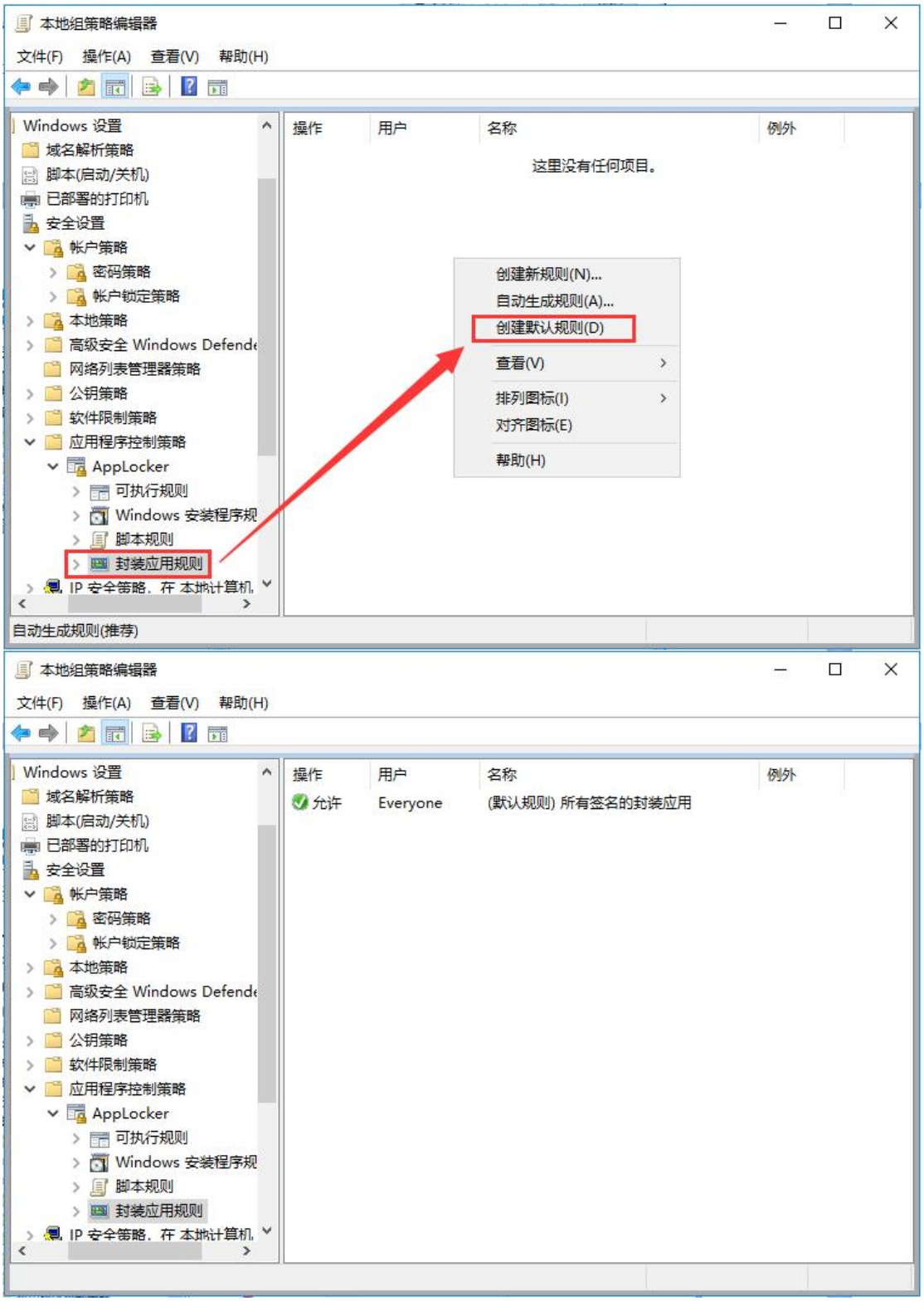
20) 重复以上步骤 8~19，把**其余的盘符**（公共盘，私有盘...）也添加到**拒绝**规则，限制普通用户在其他盘符下安装软件



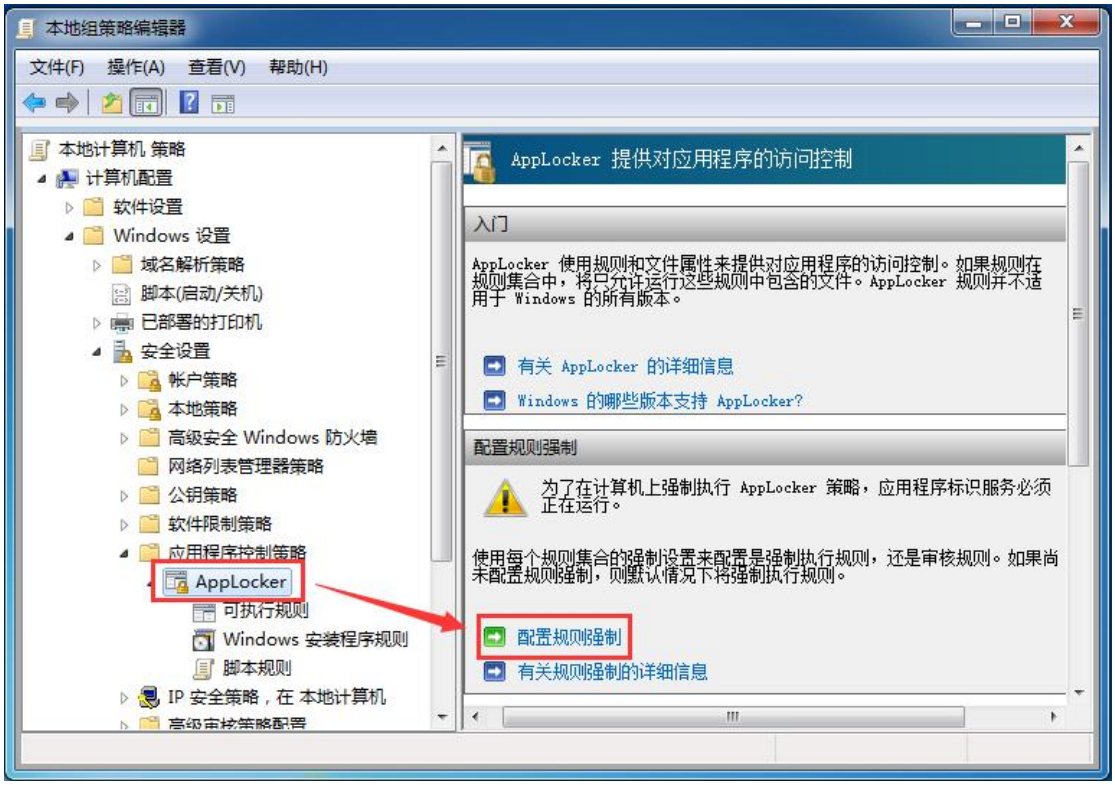
21) 选中**脚本规则**，右键空白处，**创建默认规则**（该默认规则为：所有用户只能执行默认规则路径下的脚本）



22) 选中**封装应用规则**（win8/server2012 或更高版本系统），右边框空白处鼠标右键，**创建默认规则**（该默认规则为：所有用户只能执行默认规则路径下的脚本）



23) 选中 **AppLocker**，点击**配置规则强制**



24) **强制**项的规则，全部勾选已配置，**确定**（win8/server2012 或更高版本系统，封装应用规则也勾选）

25) AppLocker 设置完成，建议**重启主机**

测试是否生效：

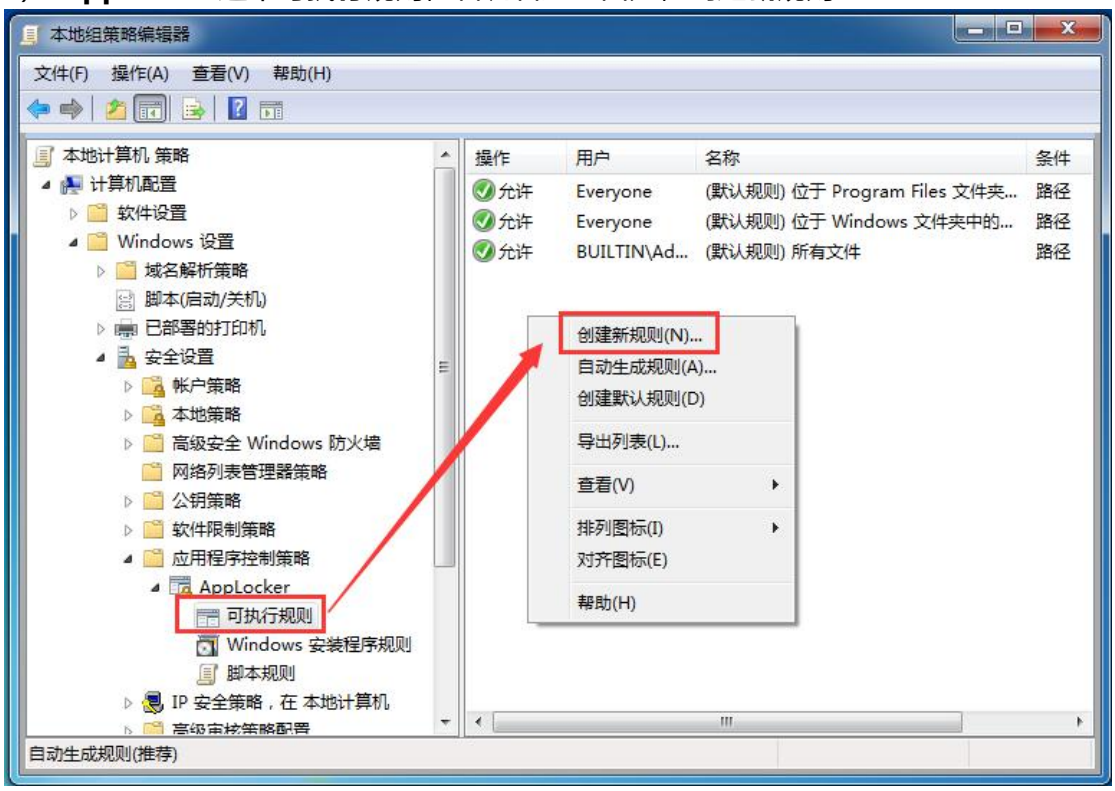
- 在云终端登录用户，运行需要使用的软件（C:\Program Files 或 C:\Program Files (x86)路径下的软件），是否正常运行；
- 在云终端登录用户，试运行.exe/.msi 程序安装包或者绿色程序包，是否无法打开，并弹出阻止提示

温馨提示：用户桌面（C:\Users\用户名\Desktop）只能通过快捷方式打开程序，无法打开.exe 文件。

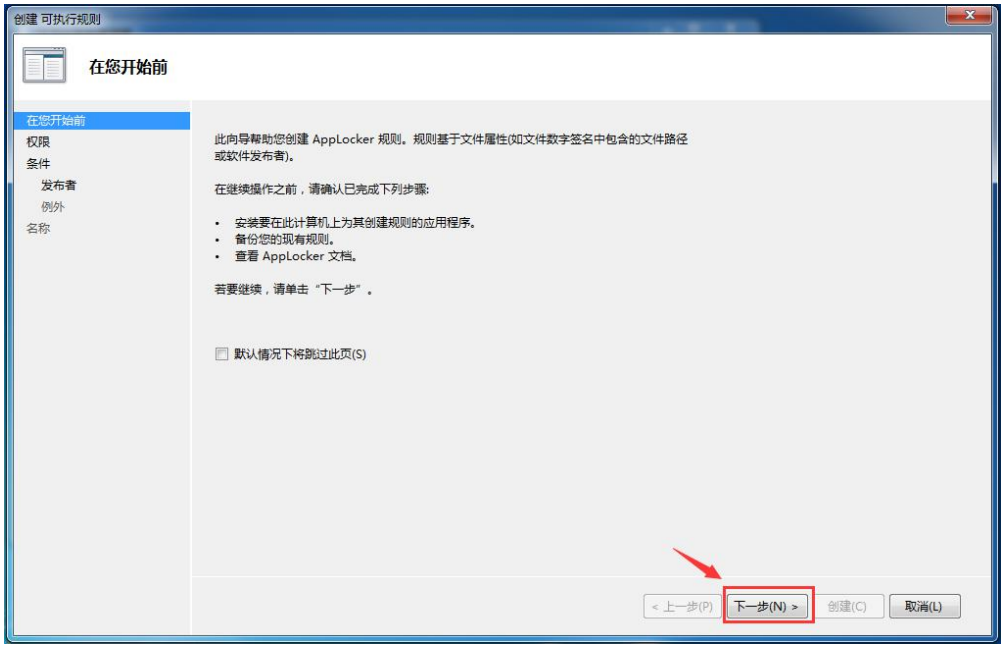
附加 1：允许运行其他路径的应用程序

某些软件安装路径比较特殊，无法安装在 **C:\Program Files** 和 **C:\Program Files (x86)**路径下（例如，百度网盘，C 盘默认安装用户路径下或者非 C 盘路径），一般会安装到其他盘（例如，手动创建的 **D:\Program Files**），通过**可执行规则**中**创建新规则**（步骤 1~7）添加允许路径，或者**自动生成规则**（步骤 8~13），通过文件哈希来允许运行特殊软件。

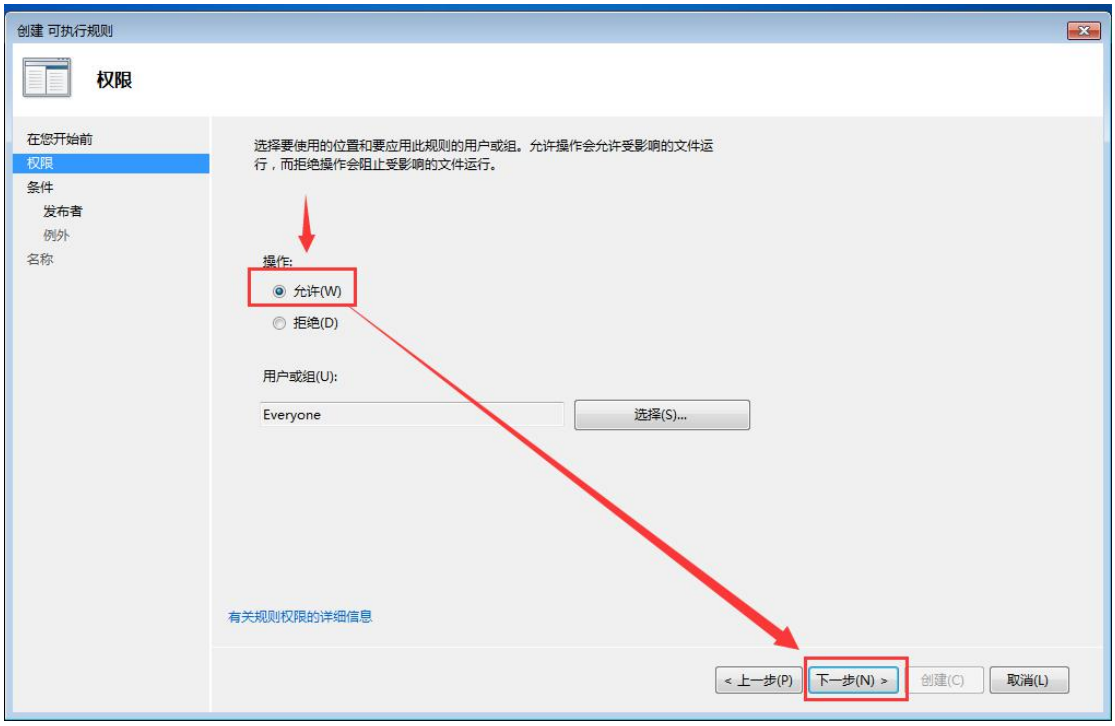
1） **Applocker** 选中**可执行规则**，右键右边空白处，**创建新规则**



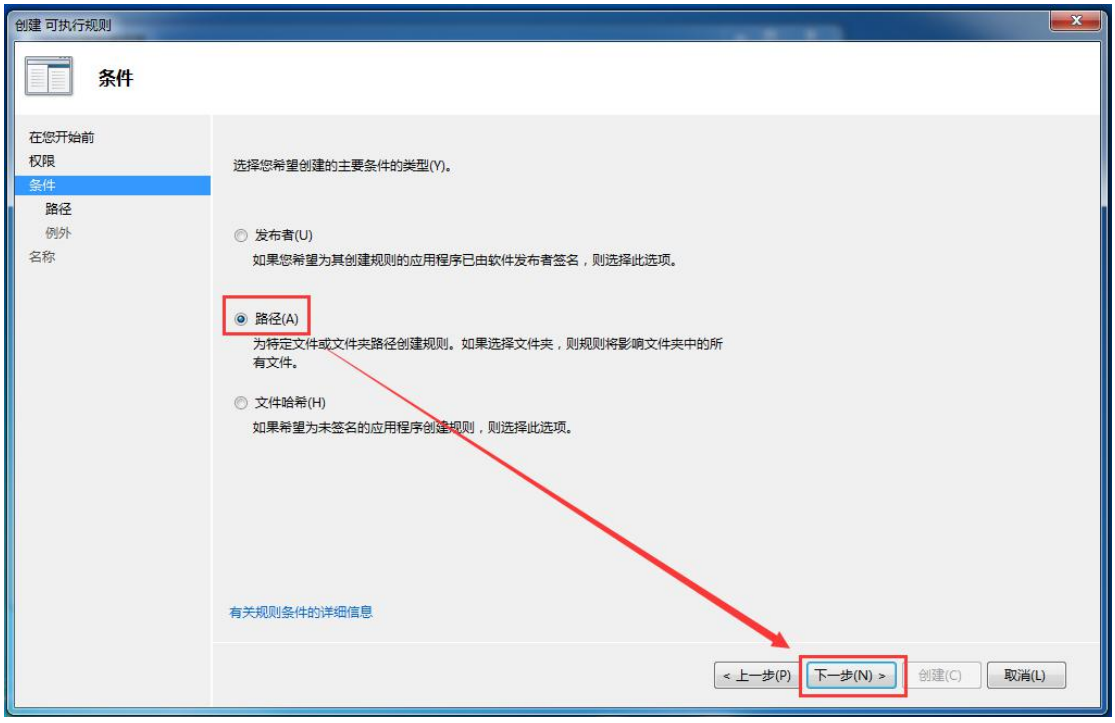
2） **下一步**



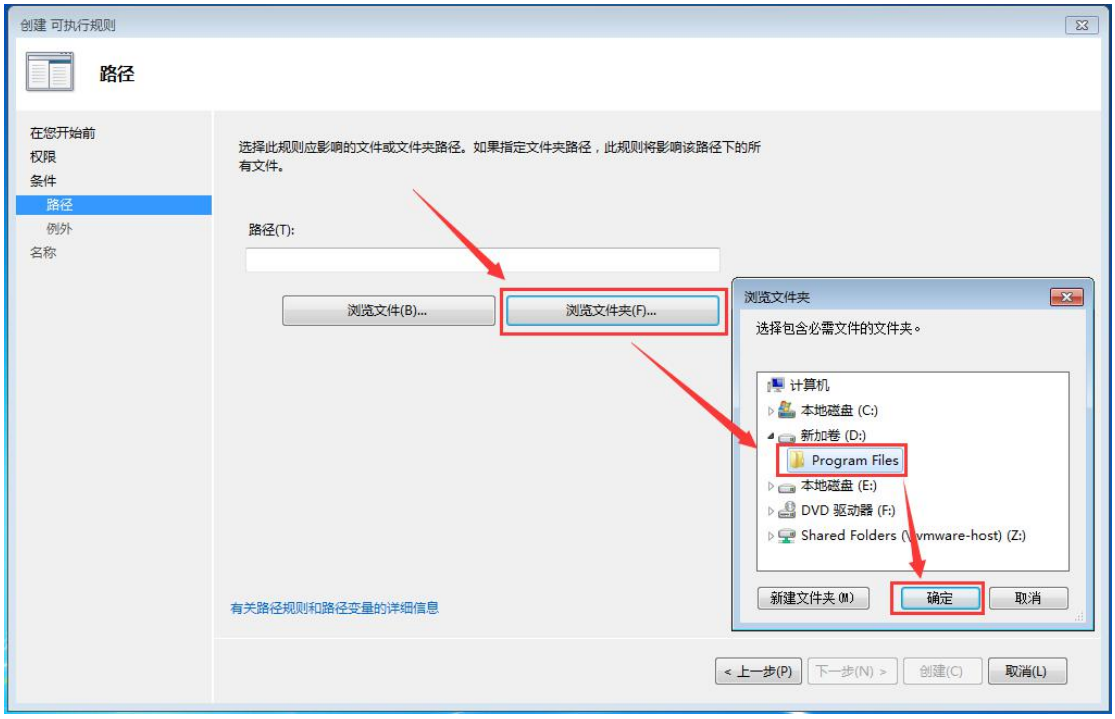
3) 选择**允许**，**下一步**



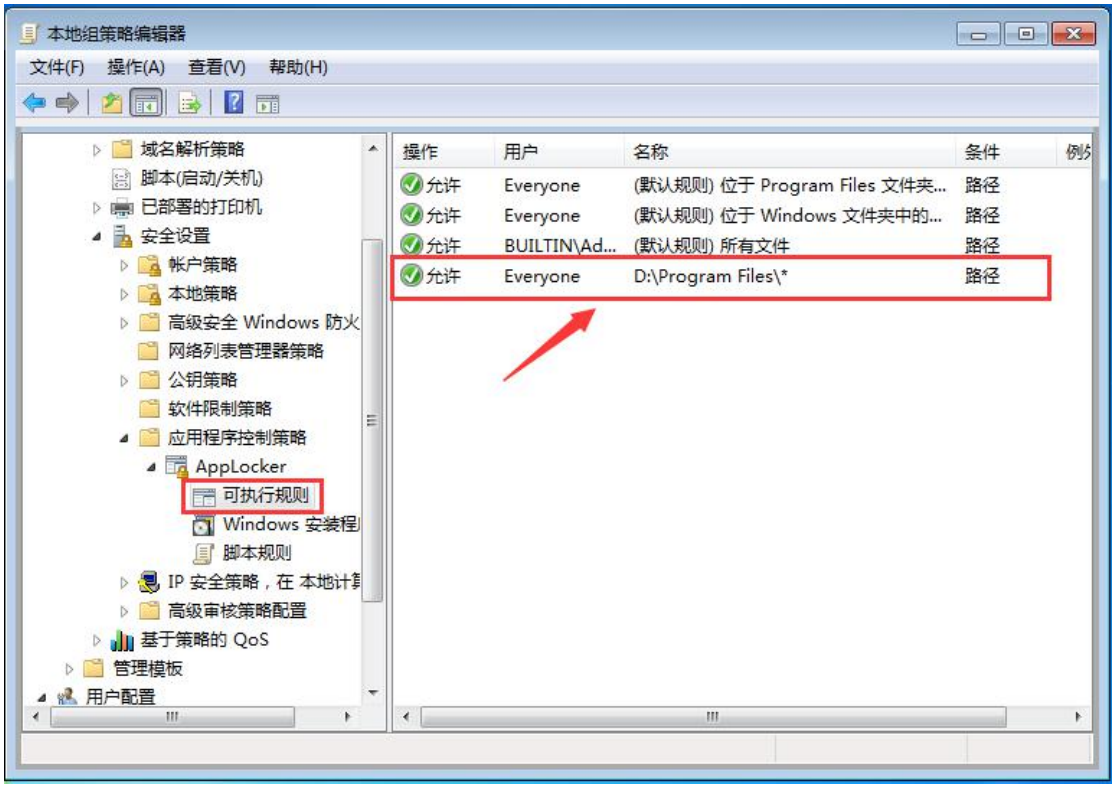
4) 选择**路径**，**下一步**



5) **浏览文件夹**，选择 D 盘 **Program Files** 文件夹，**确定**，**创建**新规则



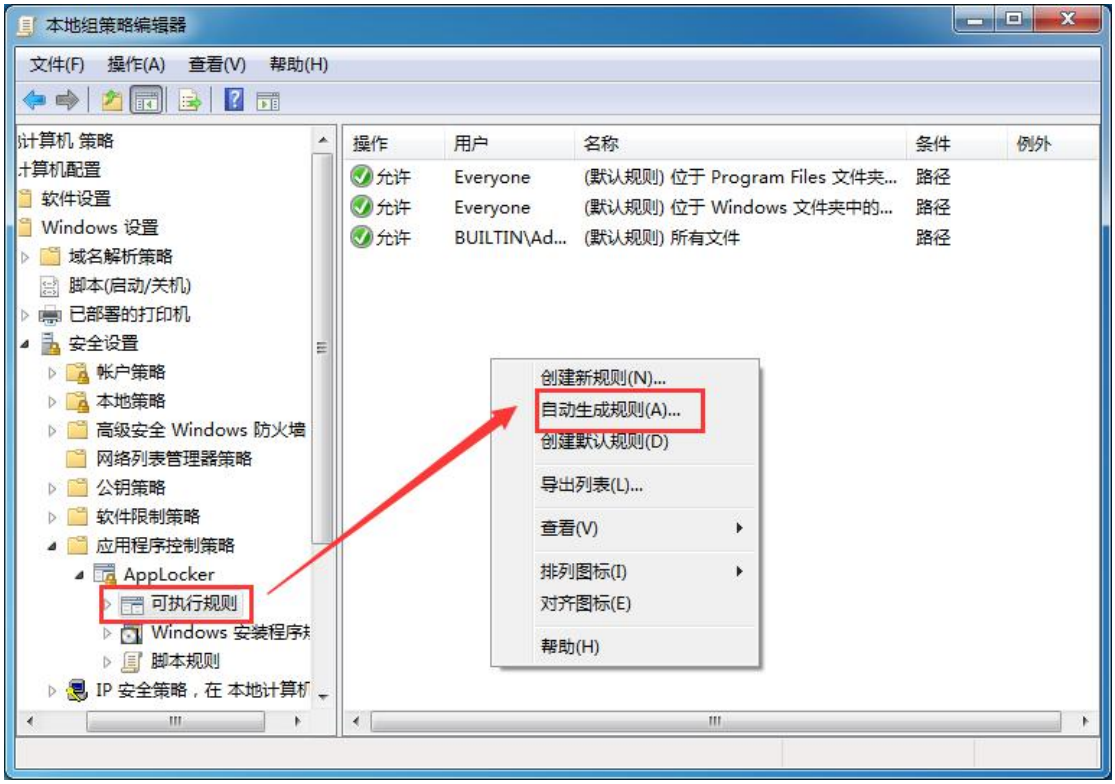
6) 在**可执行规则**里，已创建新的**允许**规则



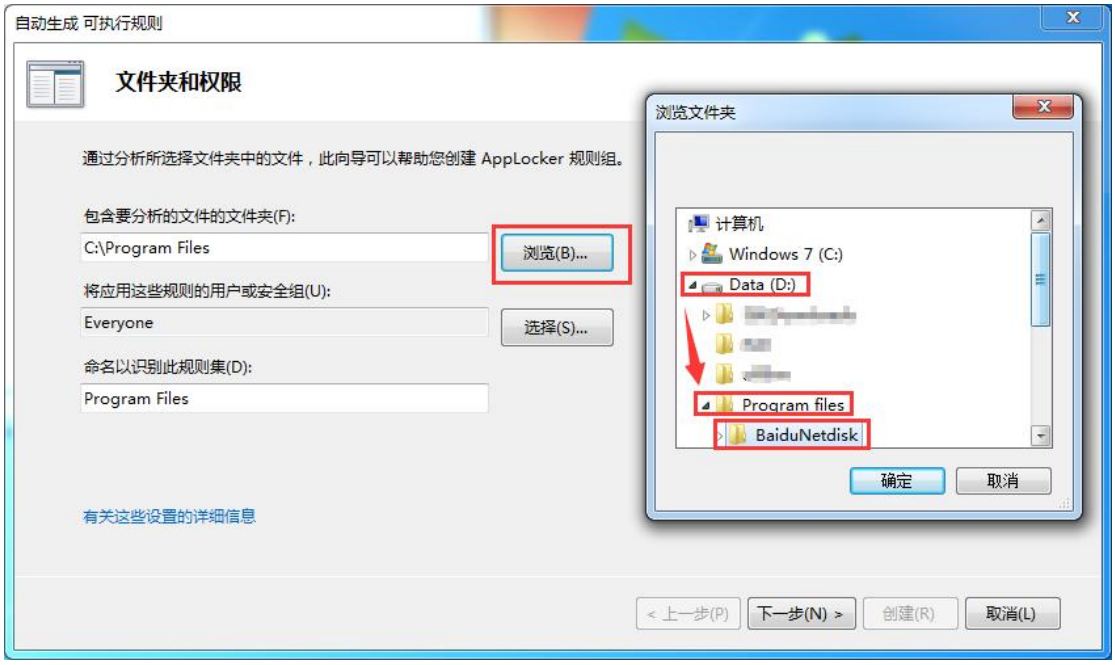
7) 允许规则后，在云终端上试运行该路径的程序，确认规则生效

注意：允许 **D:\Program Files** 路径下运行程序，有可能出现用户将绿色软件放置于 D:\Program Files 里打开使用的情况。而**自动生成规则**，通过文件哈希判断程序，只允许指定的程序可被打开，有效阻止用户使用绿色软件

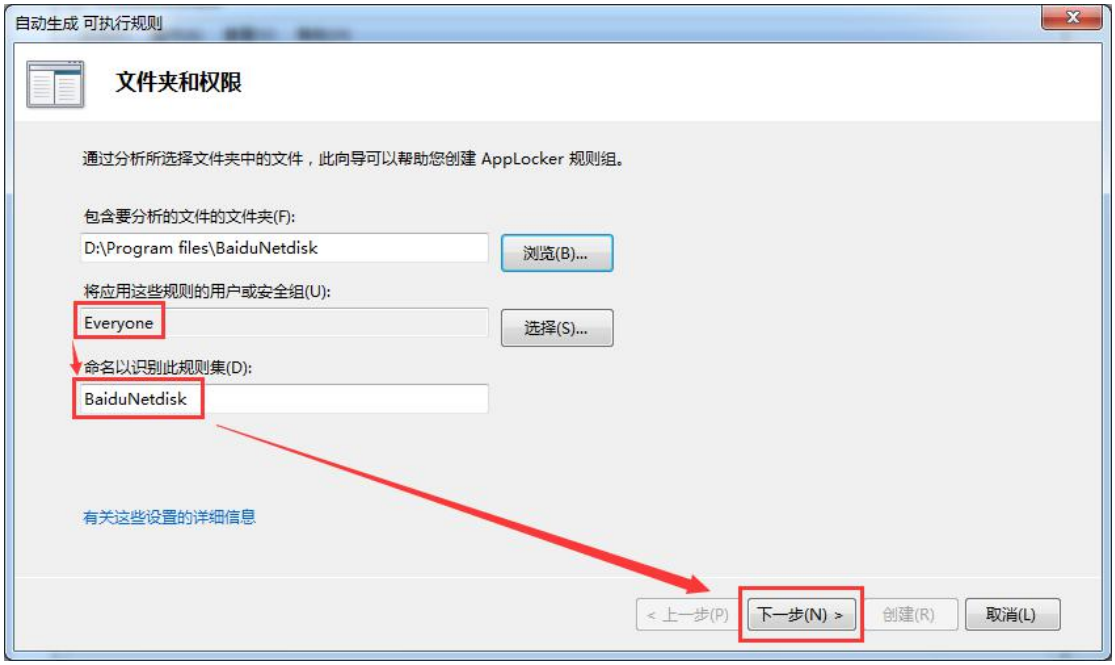
8) **Applocker** 选中**可执行规则**，右键右边空白处，**自动生成规则**



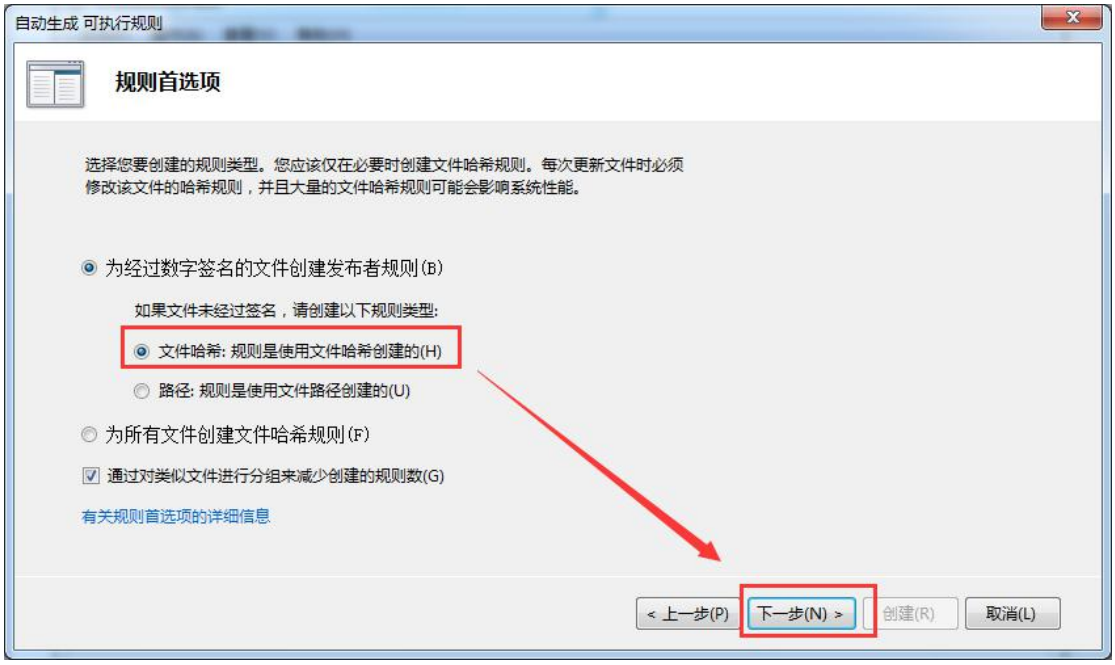
9) **浏览**，选择程序路径，（例如，安装在 D:\Program Files 的百度网盘）



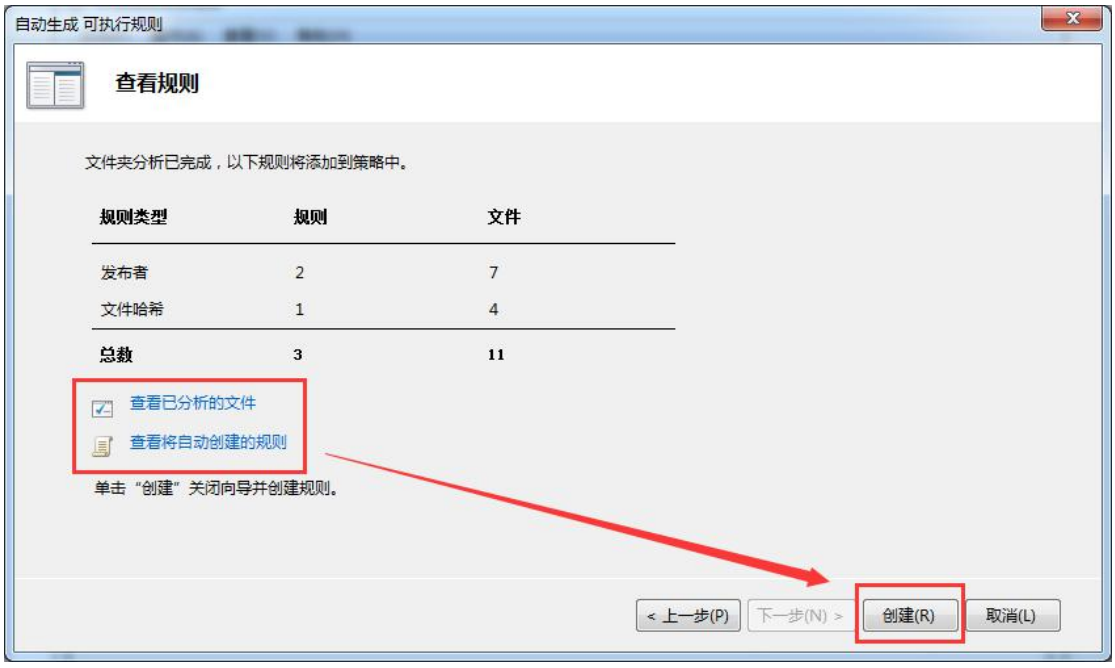
10) 选择程序路径后，将以程序文件夹名 BaiduNetdisk 来识别规则，**下一步**



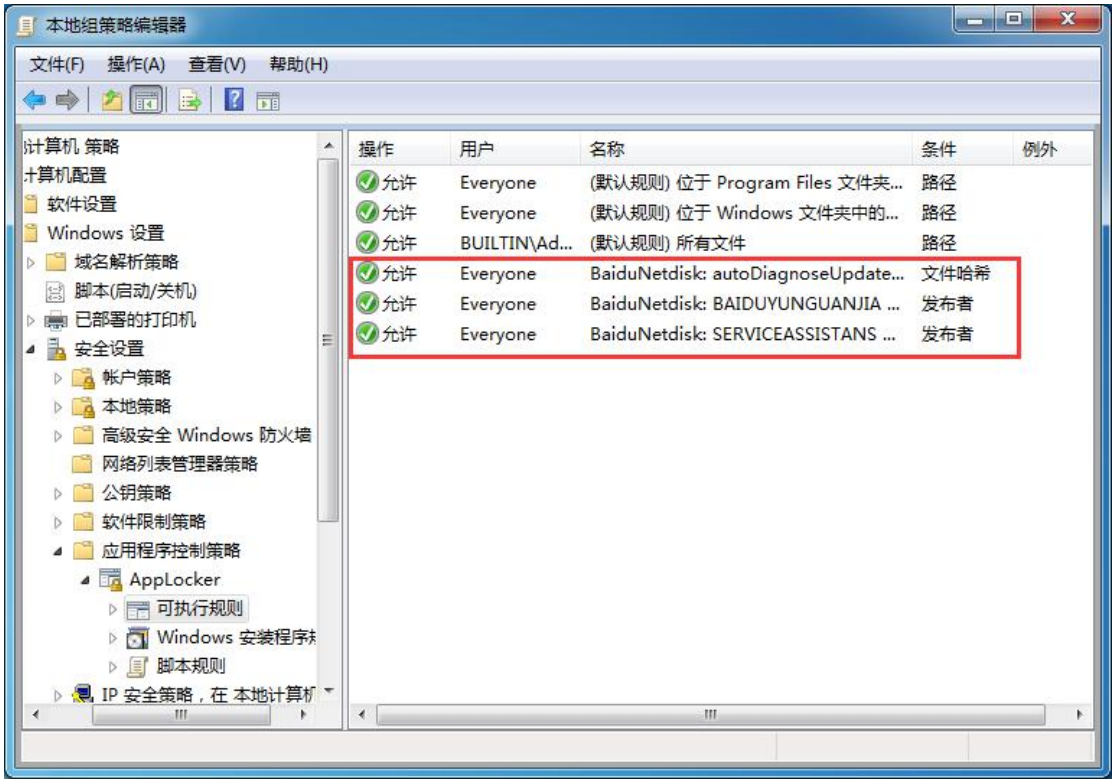
11) 默认勾选**文件哈希**创建规则，下一步



12) 生成规则后，点**创建**即可（或**查看已分析的文件**和**查看将自动创建的规则**，自行修改）



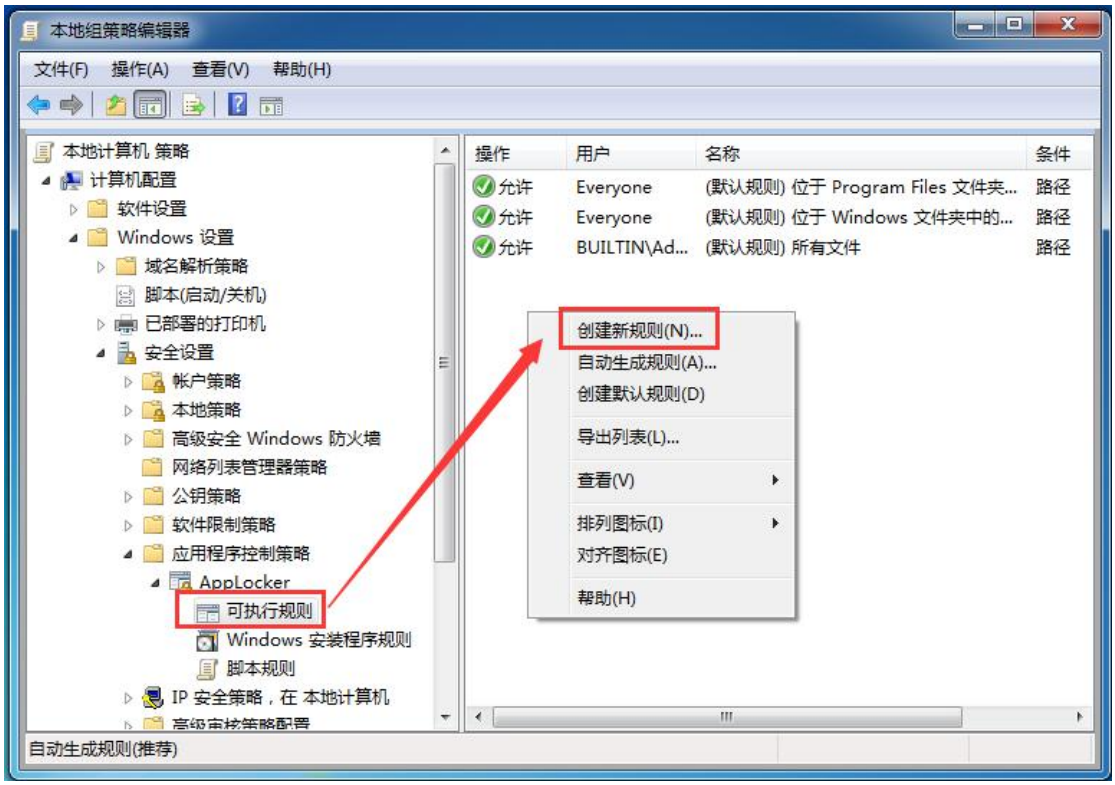
13) 已生成允许规则，云终端用户试运行百度网盘



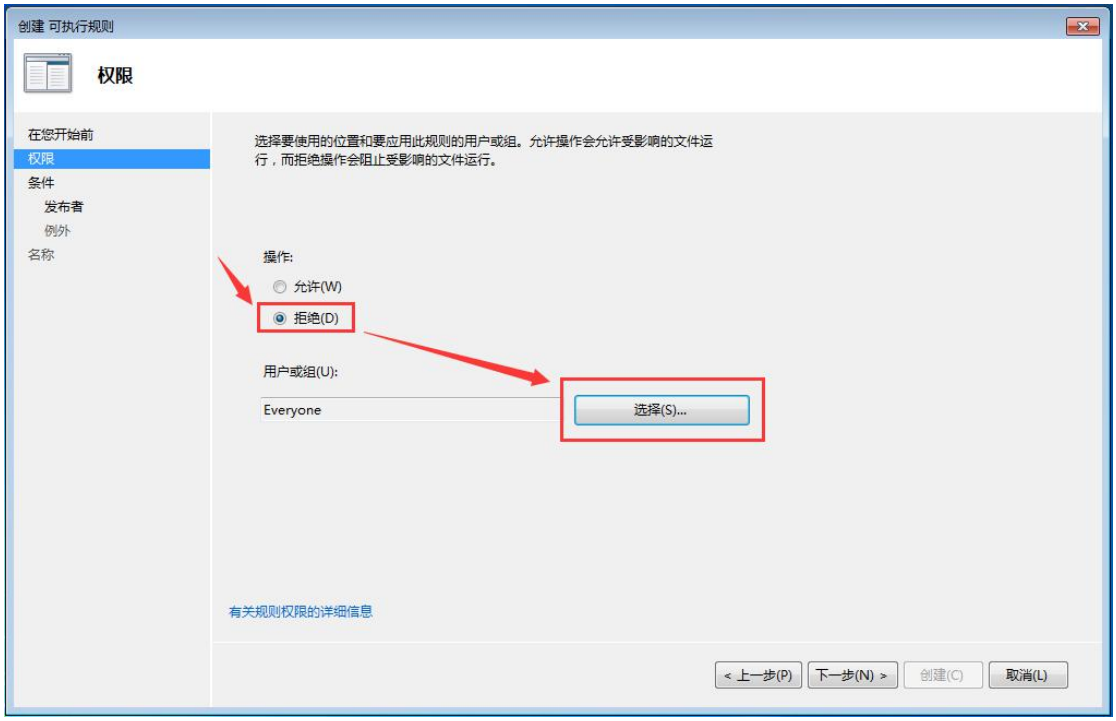
附加 2：限制指定用户/用户组使用某个软件

如需对某用户（例如 user1）限制使用某个软件（例如 QQ），通过**可执行规则**中创建拒绝规则进行限制。

1） **Applocker** 选中**可执行规则**，右键右边空白处，**创建新规则**

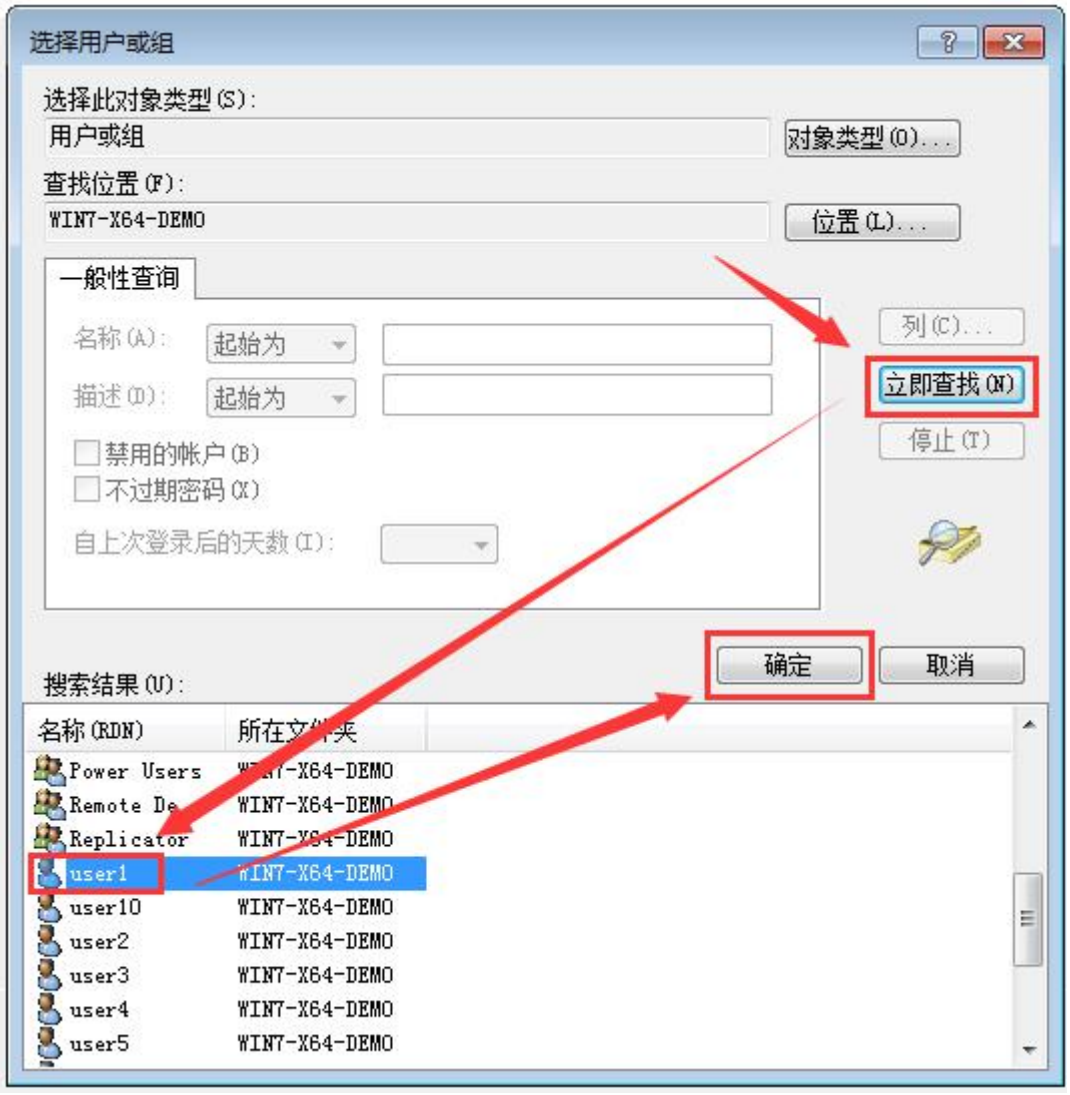


2） 选择**拒绝**，**选择**用户



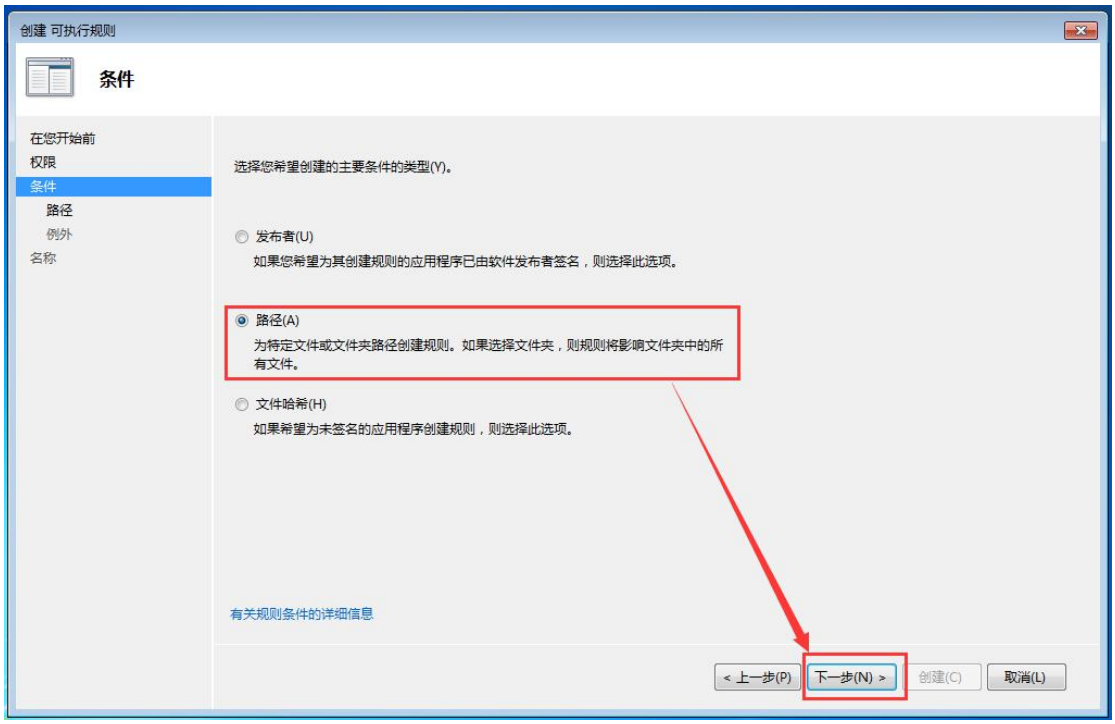
3) 点击**高级**

4) **立即查找**，找到并选中 **user1**，**确定**

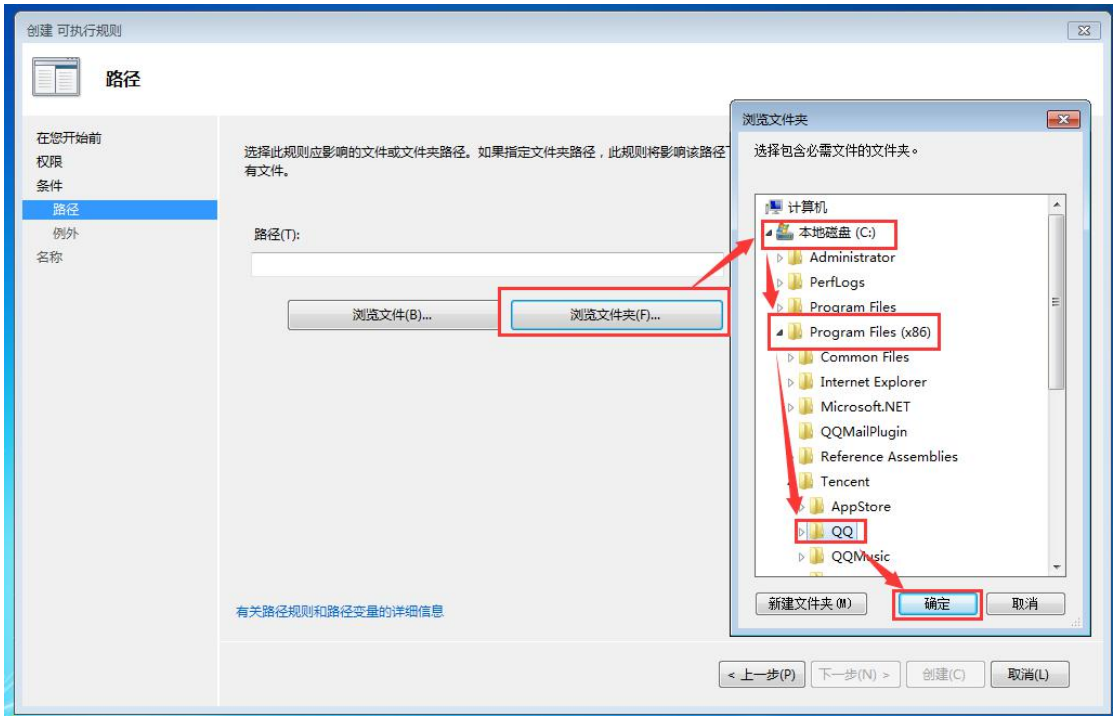


5) 选择**拒绝**，**user1**，**下一步**

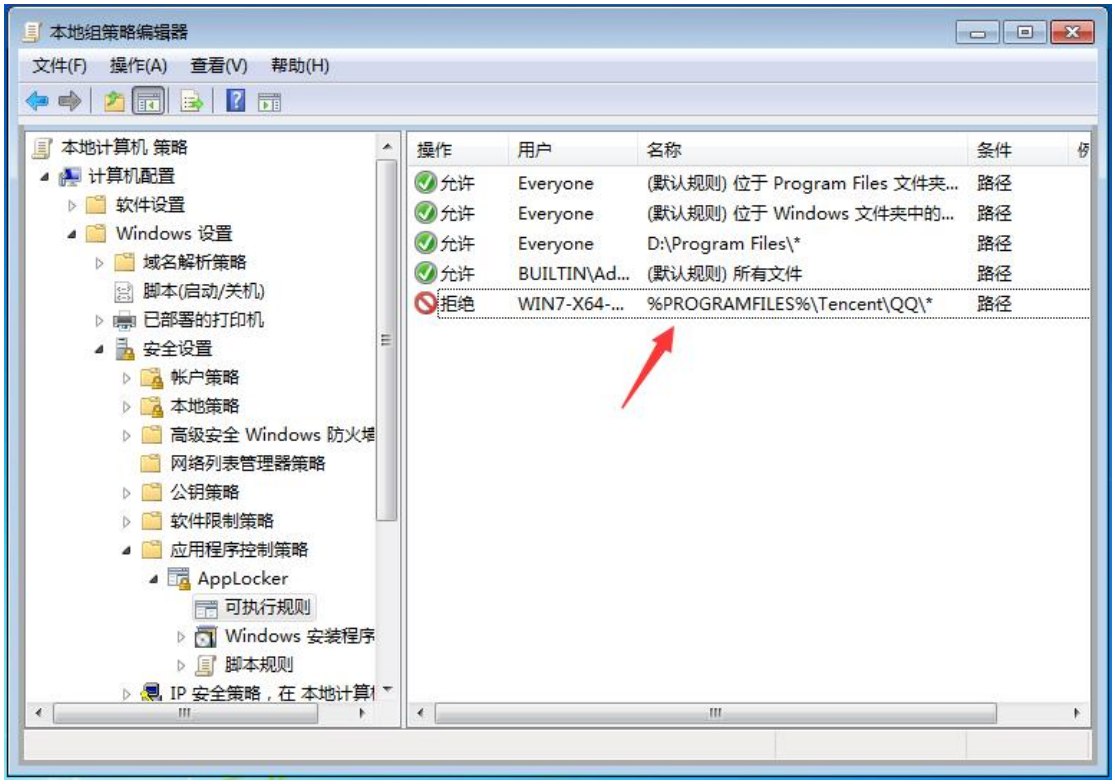
6) 选择**路径**，**下一步**



7) **浏览文件夹**，选择 **QQ 的安装路径**，**确认**并**创建**



8) 已添加拒绝规则



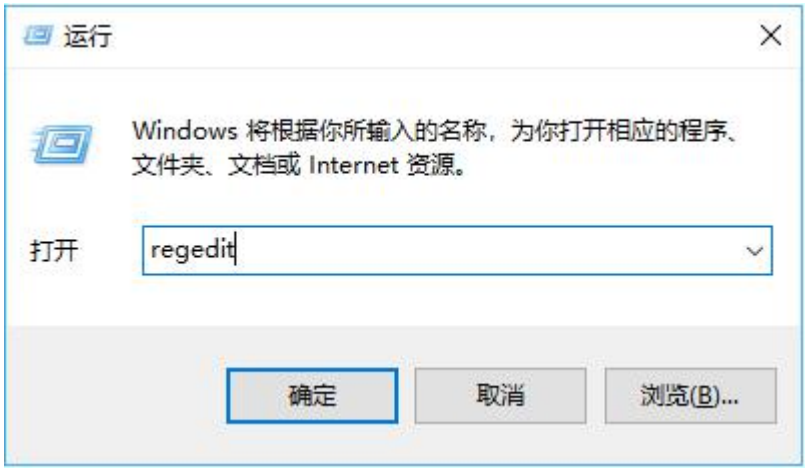
9) User1 用户运行 QQ 时，弹出提示，无法打开

10) 如需对部分用户进行限制，先创建一个普通用户组，将用户添加进该用户组，再对该用户组做限制

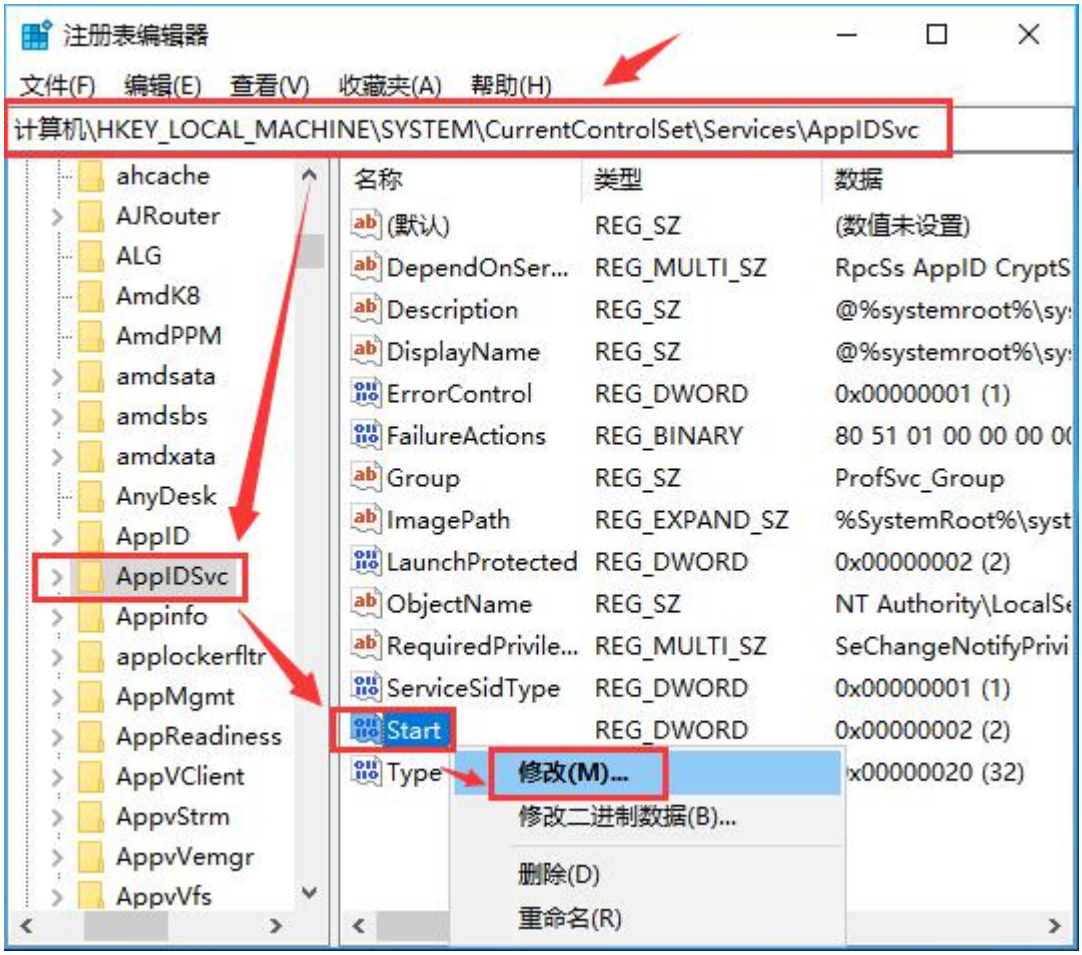
附加 3：Win10/Server 2016 Application Identity 开启方式

Win10/Server 2016 无法在服务中直接将 Application Identity 服务设置为自动启动，需要通过修改注册表，将 Application Identity 服务设置为自启。

1) **admin 账号**运行 **regedit**，打开注册表编辑器



2) 找到 **AppIDSvc**，右键 Start，**修改**数据
(HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AppIDSvc)



3) 将数值数据修改为 **2**，**确定**

4) Application Identity 服务已设置为自启