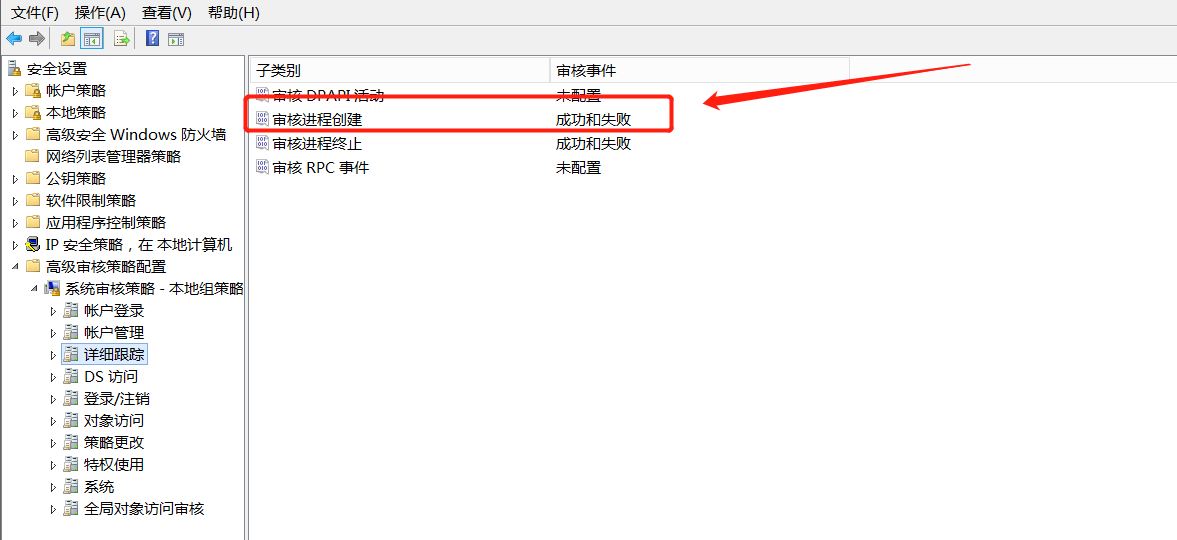
# Windows审核进程创建

在Windows系统中，此审核策略只适用于Windows2012R2和Windows8NT以上的系统。审核进程创建记录cmd命令行参数，但是记录的范围是有限制的。

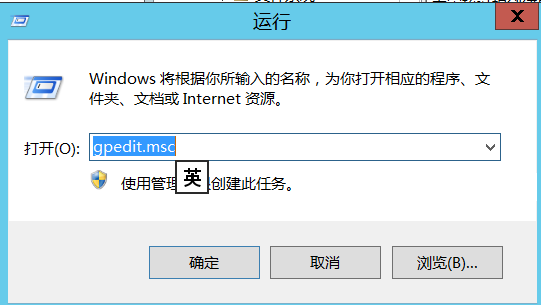
## 开启过程

### 开启审核进程创建策略：

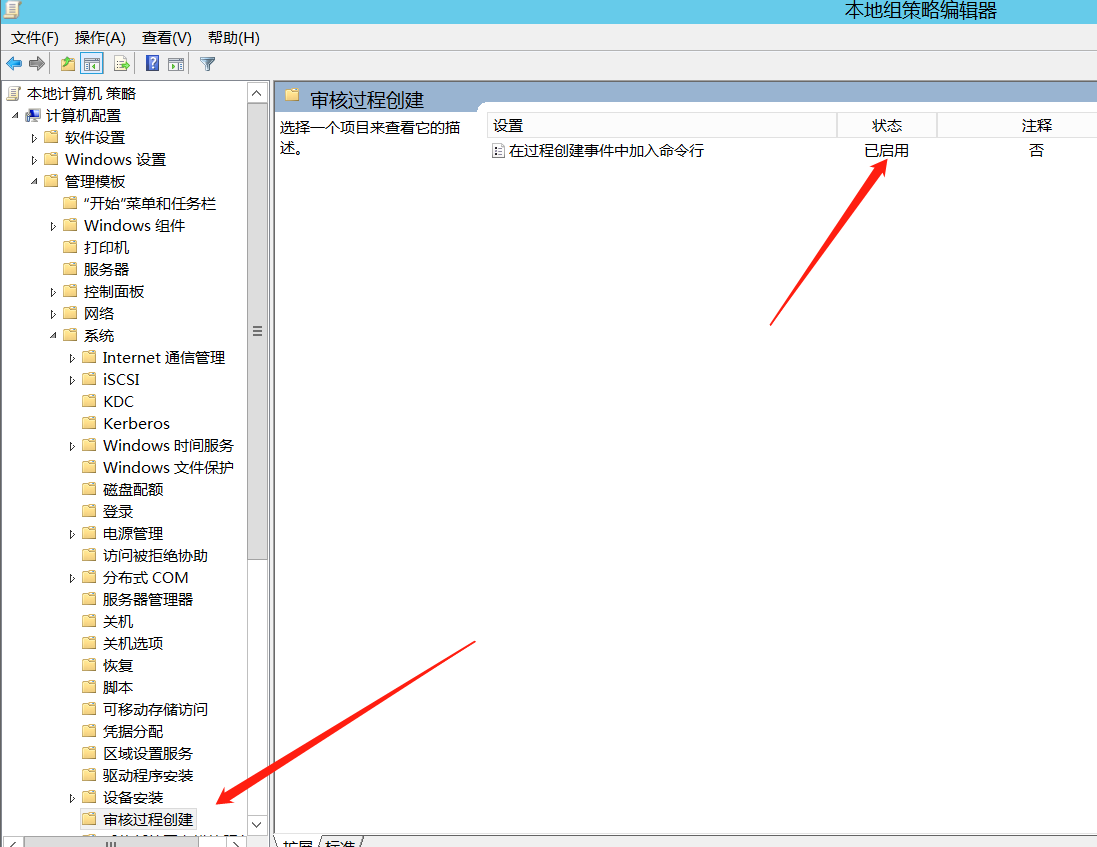
* 需要打开本地安全策略中的高级审核策略，如下：



* Win+R打开运行窗口，输入gpedit.msc



* 计算机配置>管理模板>系统>审核过程创建----开启

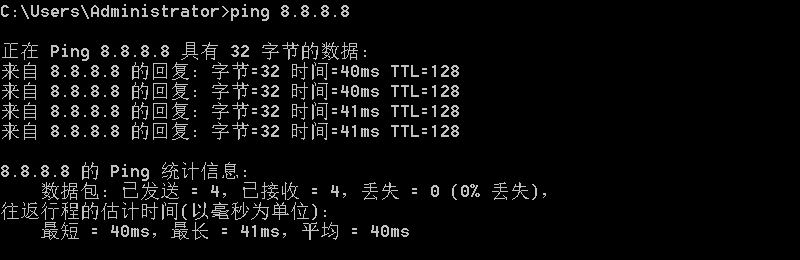


## 实验测试：

只记录在Windows系统中存在EXE可执行程序的进程调用以及设计到此进程的命令行参数。

例如：

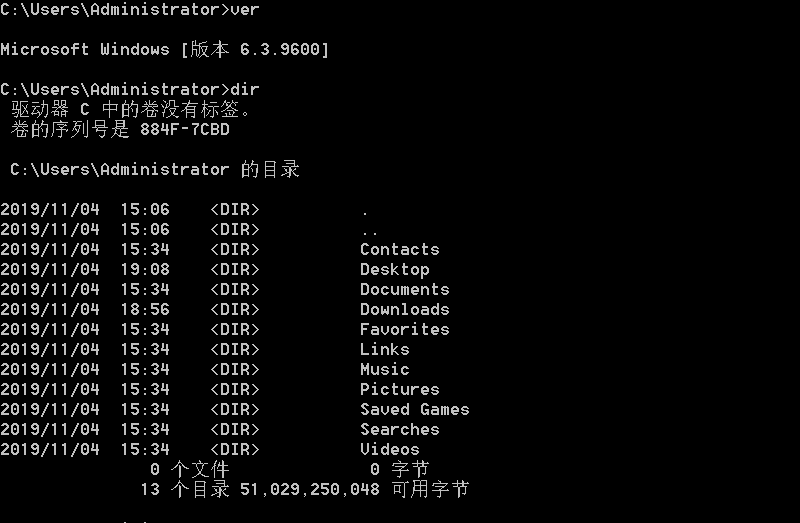
开启策略后，调用ping.exe来发现测试。





日志可以很清楚的记录。

但是我们尝试使用单纯的命令形式：



在日志中并不会发现此命令的执行。

注：在Sysmon中可以记录此命令行参数