HANDLE OpenProcess(

DWORD dwDesiredAccess, //渴望得到的访问权限(标志)

BOOL bInheritHandle, // 是否继承句柄

DWORD dwProcessId// 进程标示符

);

dwDesiredAccess说明

PROCESS\_ALL\_ACCESS 给予进程所有可能允许的权限.

PROCESS\_DUP\_HANDLE允许使用DuplicateHandle函数进行进程句柄的复制操作.

PROCESS\_QUERY\_INFORMATION允许函数GetExitCodeProcess 或函数GetPriorityClass functions 查询进程的信息时使用该句柄.

PROCESS\_SET\_INFORMATION允许函数SetPriorityClass使用此句柄进行优先级设置.

PROCESS\_TERMINATE允许函数TerminateProcess 使用此句柄关闭进程.

PROCESS\_VM\_OPERATION 允许函数VirtualProtectEx使用此句柄修改进程的[虚拟内存](http://baike.so.com/doc/4993788-5217767.html" \t "http://baike.so.com/doc/_blank).

PROCESS\_VM\_READ or PROCESS\_VM\_WRITE 允许函数访问和写入权限

SYNCHRONIZE Windows NT 专用: 允许同步函数使用此句柄.

bInheritHandle: 指定返回的句柄是继承dwProcessId指定的进程..

dwProcessId:指定打开需要打开的进程的PID.

### [折叠](http://baike.so.com/doc/6840318-7057593.html)返回值

如成功，返回值为指定进程的句柄。

如失败，返回值为空，可调用GetLastError获得错误代码。

例：

HANDLE hRemoteProcess;

//打开远程线程

if ((hRemoteProcess = OpenProcess(PROCESS\_CREATE\_THREAD | //允许远程创建线程

PROCESS\_VM\_OPERATION | //允许远程VM操作

PROCESS\_VM\_WRITE, //允许远程VM写

FALSE, dwRemoteProcessId)) == NULL)

{

MessageBox(NULL, L"打开指定进程失败!", L"错误提示", MB\_OK);

return FALSE;

}