# 特權指令

## 特權等級和特權指令

有一些系統方面的指令，只有特權等級為 0（權限最高）的程序才可以使用。如果一個 CPL 不為 0 的程序試圖執行這些指令，會導致 general-protection fault（#GP）。其中的一些指令則可以設定為可在 CPL 不為 0 的程序中執行。
下面列出這些特權指令：

- LGDT - 載入 GDTR。
- LLDT - 載入 LDTR。
- LTR - 載入工作暫存器（task register）。
- LIDT - 載入 IDTR。
- MOV（控制 / 除錯暫存器） - 載入或儲存控制 / 除錯暫存器（CRx 和 DRx）。
- LMSW - 載入 MSW（Machine Status Word）。
- CLTS - 清除 CR0 中的 task-switched 旗標。
- INVD - 將 cache 設為無效，不寫回資料。
- WBINVD - 將 cache 設為無效，寫回資料。
- INVLPG - 將 TLB 的 entry 設為無效。
- HLT - 停止處理器動作。
- RDMSR - 讀取 MSR（Model-Specific Registers）。
- WDMSR - 寫入 MSR。
- RDPMC - 讀取 PMC（Performance-Monitoring Counter）。
- RDTSC - 讀取 TSC（Time-Stamp Counter）。

把 CR4 的 PCE 旗標（第 4 bit）設為 1，可以使 RDPMC 指令可在任何 CPL 下執行。把 CR4 的 TSD 旗標（第 2 bit）設為 1，則可使 RDTSC 指令可在任何 CPL 下執行。
在 EFLAGS 旗標中的 IOPL（第 12 bit 和第 13 bit），設定存取輸出入位址空間（I/O address space）所需的最低權限。例如，如果 IOPL 設為 1，則只有 CPL 為 0 和 1 的程序可以執行 I/O 指令，和存取 I/O 記憶體。這個旗標只能在 CPL 為 0 的程序中，利用 POPF 或 IRET 命令更改。