

?????

????????????? CPU ??,??? x86 ? CPU ??????????????,????????????,?? CPU ??????????,????????????????????.

????????????????? VMware ,?? 1999 ? 2 ?,VMware ??????? x86 ?????? "VMware Virtual Platform",?????? VMware ?????????????????????????????????????? Guest OS ?????????????????? full Virtualization ?????????,????? Binary translation ?? natively virtualizable architecture (? IBM System/370 or Motorola MC68020) ??.

????????? Xen ??????????,????? full virtualization ??????.????????????????????????????? Guest OS,????????? paravirtualization,????? Guest OS ?????????????? Guest OS ??????????????,????????? Linux ? FreeBSD ??????.Windows ??????????????????,?? Windows ?????????????????????????????????????? CPU ?????????????????????????????? paravirtualization ?? ??????? CPU ???,??? **Hardware-assisted virtualization** (Intel VT ? AMD-V) ,?????? Xen 3.0 ?????,????? CPU ? ?????? Xen ??????? full virtualization

?? Open-source ? VMware ? Microsoft ?? Connectix ?????????????????? Hyper-V,????? Hyper-V ???????Microsoft Virtual PC ? Microsoft Virtual Server.

**CPU**  
????? XEN full virtualization(Hardware-assisted virtualization) ?????,?????CPU ??????,? Intel ?? **VT(Virtualization Technology) ? AMD ? V Pacifica.** ?????????????????? CPU ?????????????? Hardware-assisted virtualization ??????????????????,????? Xen ?????????? hardware virtual machine (HVM), Virtual Iron ??? native virtualization.

**AMD virtualization (AMD-V)**  
AMD ??????? CPU ?????????? Pacifica ?????? Project code name.?????????? AMD Virtualization ???? AMD-V  
????? AMD CPU ??? AMD-V ???,??Athlon 64 ? Athlon 64 X2 ???? "F" ? "G" stepping ??????Turion 64 X2, Opteron 2nd generation[1] and 3rd-generation[2], Phenom ? Phenom II processors ??? AMD-V.????????? Sempron ?????? Sable ? Huron ?????? AMD-V.

????????????????? AMd ??????????

[http://www.amdtaiwan.com.tw/us-en/Processors/ProductInformation/0,,30\\_11...](http://www.amdtaiwan.com.tw/us-en/Processors/ProductInformation/0,,30_11...)

??? Linux ????????? CPU ? Flag.  
 ?????,???? Linux ??? CPU ? Flag.????

### AMD-V Pacifica ? Flag ? svm

```
[root@benjr ~]# cat /proc/cpuinfo | grep svm
```

???????? svm(Secure Virtual Machine) Flag ?????? AMD CPU ?????? ,?? CPU ?????? BIOS ??????????.??? BIOS ? CPU ?????????? virtualization???.????? AMD-V Pacifica ???? XEN ??????????????Full-Virtualization ?? Para-Virtualization.????? Full-virtualization(Hardware-assisted virtualization).

### Intel Virtualization Technology for x86 (Intel VT-x)

?? Intel ???? VT ??????????.VT-x ???? IA-32 ? Intel 64 ????.VT-i ???? Itanium ???,?? Intel VT ??? CPU ?????.

- Core Duo T2300, T2400, T2500, T2600, T2700 (Yonah)
- Core 2 Duo E6300, E6400, E6320, E6420, E6540, E6550, E6600, E6700, E6750, E6850 (Conroe)
- Core 2 Duo E8200, E8300, E8400, E8500, E8600 (Wolfdale)
- Mobile Core 2 Duo T5500, T5600, T7100, T7200, T7250, T7300, T7400, T7500, T7600, T7600G, T7700, T7800 (Merom)
- Mobile Core 2 Duo P7370, P8400, P8600, P8700, P8800, P9500, P9600, P9700, T8100, T8300, T9300, T9400, T9500, T9600, T9800, T9900 (Penryn)
- Core 2 Quad Q6600, Q6700 (Kentsfield)
- Core 2 Quad Q9300, Q9400, Q9400S, Q9450, Q9550, Q9550S, Q9650 (Yorkfield)
- Core 2 Extreme X6800 (Conroe\_XE)
- Core 2 Extreme QX6700, QX6800, QX6850 (Kentsfield\_XE)
- Core 2 Extreme QX9650, QX9770, QX9775 (Yorkfield\_XE)
- Xeon 3000, 5000, 7000 series
- Atom Z520, Z530, Z540, Z550, Z515 (Silverthorne)
- all Intel Core i7 processors
- Pentium Dual-Core E6300 and some version of the E5300 and E5400\*
- Celeron E3000 series

????????????? Intel ?????????.

<http://processorfinder.intel.com/Default.aspx>

?????,???? Linux ??? CPU ? Flag.????

### Intel VT ? flag ? vmx

```
[root@benjr ~]# cat /proc/cpuinfo | grep vmx
```

? AMD-V ????????? Flag ?????? Intel CPU ??????.

?? Intel ???? VT ??????????.

VT-x ???? IA-32 ? Intel 64 ???

VT-i ???? Itanium ???

VT-d refers to Intel VT for Directed I/O

?? Intel ??? CPU ?????????,???? Intel ??????.

VT-c refers to Intel VT for Connectivity

**Ring**

???????? full virtualization(Hardware-assisted virtualization) ??? CPU ?????????????????????????????????????  
"Ring", ? Intel x86 ? CPU ?????????? Ring 0,Ring 1,Ring 2 ? Ring 3. Ring 0 ???????,???????????? Ring0 ???,Ring  
0 ????????????? IO devices, CPU, Memory,??? Ring 1,?????? Kernel,driver ??? Ring 0.?? AP ?? Ring 3,?????????  
????????????????????????,?????? Window 3 ?????????,???????????? Crash ?.

????????????????????4??????,????????2???,? Linux ? Windows ???????,????????? supervisor / user-mode,?????  
Kernel ??? supervisor mode(Ring 0).? applications ?????? User mode(Ring 3).

?? user mode ? Application ?????????????? supervisor(Kernel) mode.???? system call ????.?? Ring 1 ? Ring 2 ?  
Linux ? Windows ??????????.????????? OS ???.

**VMM(Virtual Machine Monitor)**

??(Guest OS).?????? VMM(Virtual Machine Monitor).?????  
???????? OS ?????? Ring0.???????? Ring Deprivileging(??????),Ring 0 ??????? VMM(Virtual Machine Monitor)  
????? Hybervisor.??VMM ??????????????,??????

- ?????????????????? Guest OS
- ?????????? Guest OS
- ??? Guest OS ??????????????????

?????????? VMM ??? Privilege 0 ,Guest OS ??? Privilege 1(0/1/3??)

????????????????????,?????????? Ring 0 ????????????? IO devices, CPU, Memory ?? Ring 1 ? Guest OS ???????  
Binary translation( Full Virtualization) ??????????????????(nonvirtualizable instructions)VMM ??????????,????  
? VMM ???.VMM ???.

?????? VT ??? Xen ? VMM(virtual machine monitor) ??? Hybervisor ?????? Ring 0 ??,Dom0 ? kernel ?????  
Ring 1 (Dom0 ????? Xen ?????????).?????? DomU ?????? Ring 1 (?? Para-Virtualized).????? AP ?????? Ring  
3.Xen ? Paravirtualization ??????????????(Guest OS)???,?????????(Guest OS)????????????????(nonvirtualizable  
instructions)????? VMM ?????????(hypercall),?? VMM ??????????.?? Xen ? Paravirtualization ?????????????????????  
?????? Paravirtualization ??????(Guest OS)????.

???????? Host OS ??? Privilege 0,VMM ??? Privilege 3,Guest OS ??? Privilege 3(0/3/3??),????????????????????????,??

???????????????????????????????? Desktop ??.

### VMX & SVM

VMX ? SVM ? Intel VMX(Virtual Machine Extensions) ?? AMD svm(Secure Virtual Machine) ??? ????? CPU ?  
 ????? Intel ???? Guest OS ??????? Ring 0 ??? CPU ?????????????? forms(??)?? VMX root operation(??????),??  
 ??????? Ring -1(??) ?????????????? VMX root operation.??????? VMM(Virtual Machine Monitor) ?????  
 Hybervisor ???,?? VMX non-root operation(??????) ??????? Guest OS ???,???????? Ring ??? 4 ???  
 (Privileges levels).?? Guest OS ??????? Ring 0 ???,????????????( overhead )????.