Universitatea Polithenica București
Facultatea de Automatică și Calculatoare
Arhitectura Sistemelor de Calcul

Intel VT-x vs. AMD-V

virtualizare hardware pentru desktop

Ioan-Alexandru EFTIMIE
Grupa: 332CC

alex@eftimie.ro

2 iunie 2009

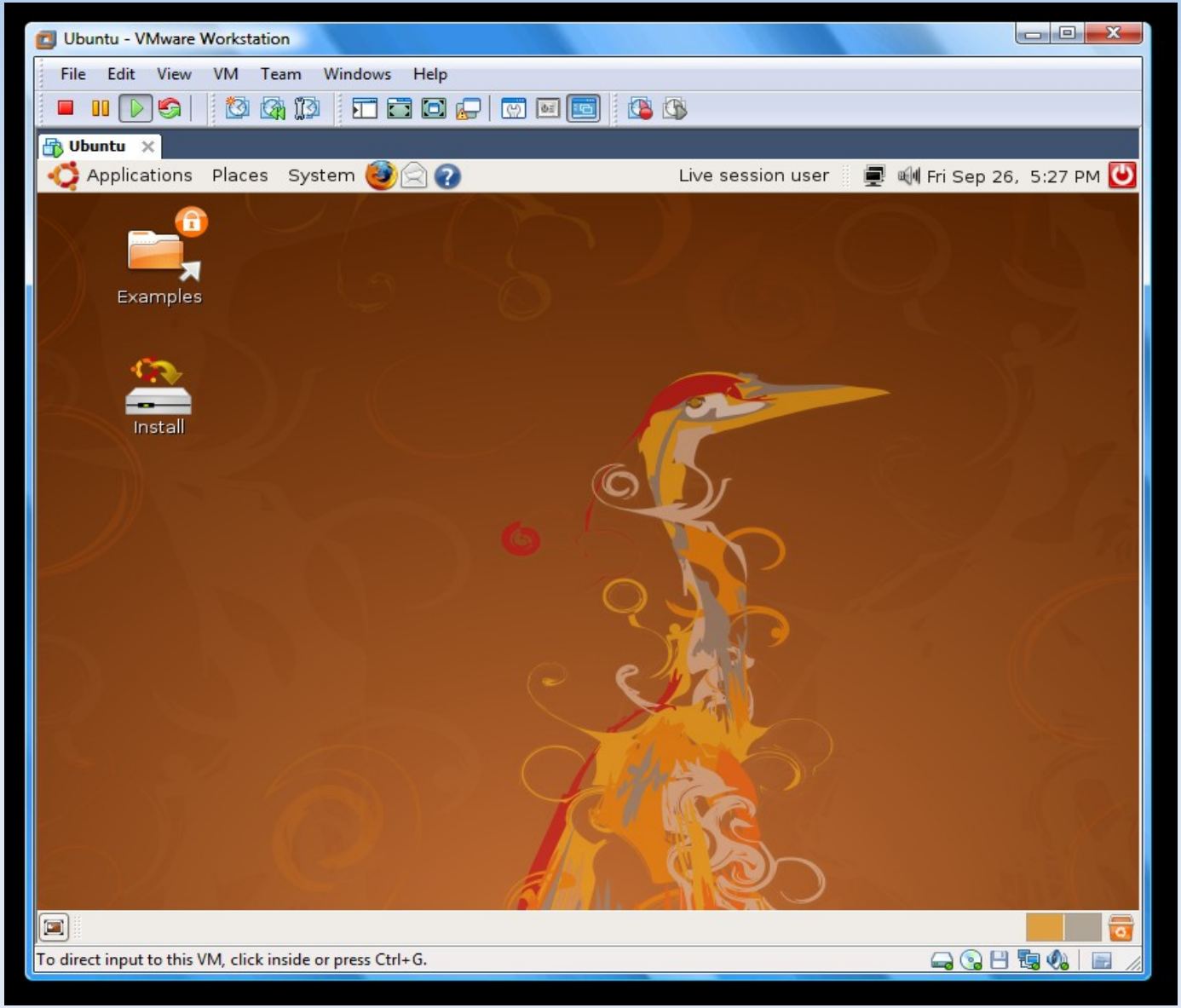
Cuprins

Introducere

- De ce virtualizare?

- De ce hardware?

Introducere (2)



Istoric

- 1999, VMware - primul hypevisor pentru x86
  - Translatare binară, overhead de performanță
- 2001, Microsoft – Virtual PC pentru Mac OS și Windows
- 2002, VMware – patentează „VMware Virtual Platform”
- 2005, alternative Free – Qemu, VirtualBox
- Xen, Denali, L4 - paravirtualizare

Istoric (2)

- Răspuns hardware
  - 2005, Intel VT-x
  - 2006, AMD-V
- Nu sunt intercompatibile
- Respectă modelul Popek & Goldberg
- Rulează SO musafir nemodificat

Modelul Popek și Goldberg

- 1974, *„Formal Requirements for Virtualizable Third Generation Architectures”*
- Presupuneri; aplicații pe IBM 360, Honeywell 6000, DEC PDP-10
- Trei condiții:
  - **Echivalența**
  - **Controlul resurselor**
  - **Eficiența**
- Instruction Set Architecture
- User mode/System mode

Modelul Popek și Goldberg (2)

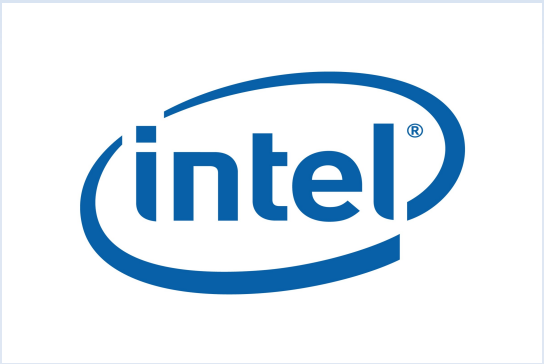
- ISA:
  - Instrucțiuni privilegiate
  - Instrucțiuni sensibile la control
  - Instrucțiuni sensibile la comportament
- Teorema 1:
  - Pentru orice computer modern, o mașină virtuală poate fi construită dacă setul de instrucțiuni sensibile este un subset al celor privilegiate.
- Teorema 2:
  - Un computer modern este virtualizabil recursiv, dacă:

    1. este virtualizabil

    2. permite construcția pe el a unei mașini virtuale fără constrângeri legate de temporizare (timing).

Intel VT-x

- Codename „Vanderpool”
- Pentium 4, Pentium D, Core 2, Core 2 Duo, Xeon, Atom
- Nu pe low-end (Celeron, Pentium)
- Avantaje:
  - Comprimare spațiu adresă
  - Eliminare aliasuri în inel
  - Acces stări privilegiate fără fault (VMM)
  - Apeluri de sistem de pe musafir
  - Acces la stări ascunse (registre nedocumentate)



Intel VT-x (2)

- EPT (Extended Page Tables)
  - Arhitectura Nehalem
  - Virtualizare tabele pagini de memorie

AMD-V

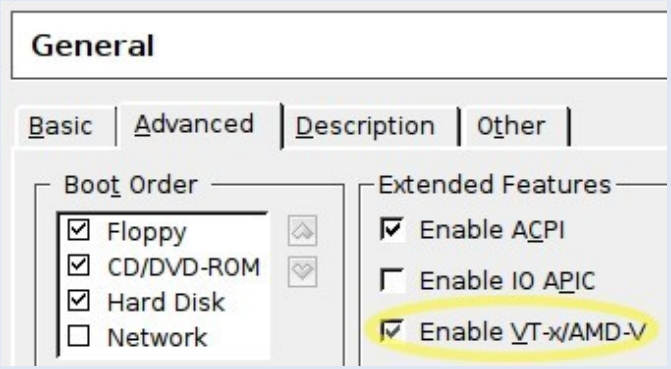
- Codename „Pacifica”
- X86 pe 64 de biți
- Avantaje:
  - Lățime mare de bandă și scalabilitate
  - Management memorie VM în hardware
  - Management consum
  - TLB etichetat (comutare rapidă)
  - AMD-V™ Extended Migration – permite migrarea mașinii virtuale pe orice procesor din gama Opteron

AMD-V (2)

- Suport în:
  - Athlon 64 „Orleans”
  - Athlon 64 FX „Windsor”
  - Turion 64 X2
  - Opteron, Phenom
- Nu în: Sempron

Aplicații

- KVM (Kernel-based Virtual Machine), Xen
- VirtualBox, Sun xVM
- VMware Workstation 6, VMware Fusion, VMware Server
- Hyper-V
- Microsoft Virtual Server
- Oracle VM
- Parallels Workstation
- Virtual Iron, TenAsys, Blue Pill



Hands-On

- Pentru a putea utiliza AMD-V, Intel VT-x trebuie activat din BIOS
- Pentru a vedea dacă procesorul suportă:

```
egrep '(vmx|svm)' /proc/cpuinfo
```

Concluzii

- Tehnologie tânără
  - Implicit dezactivată, soluții de virtualizare software mai rapide
- Tendințe orientate înspre platforma mobilă
  - Intel Atom, AMD Turion 64 X2
- Avantaje evidente
  - Rulare transparentă simultană

Bibliografie

- „x86 virtualization” - Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/X86_virtualization
- Gerald J. Popek and Robert P. Goldberg (1974). "Formal Requirements for Virtualizable Third Generation Architectures".
- „Intel Virtualization Technology” - http://www.intel.com/technology/itj/2006/v10i3/1-hardware/6-vt-x-vt-i-s
- „AMD Virtualization Technology” - http://www.amd.com/us-en/0,,3715_15781_15785,00.html
- Tombuntu - „Should you enable VT-x in VirtualBox” (2007) - http://tombuntu.com/index.php/2007/10/01/should-you-enable-intels-vt