

Exécution de plusieurs systèmes d'exploitation sur une puce manycore CC-Numa sécurisée

Jean-Baptiste BRÉJON

Encadrant : Quentin MEUNIER
Lip6 - SoC - ALSOC

10 Septembre 2015

- 1 Contexte et Sujet
- 2 Définition des problèmes et solutions
- 3 Procédure de recette
- 4 Démarrage d'une VM
- 5 Démarrage de 2 VMs ALMOS sur la plateforme finale
- 6 Conclusion et perspectives

Contexte du stage

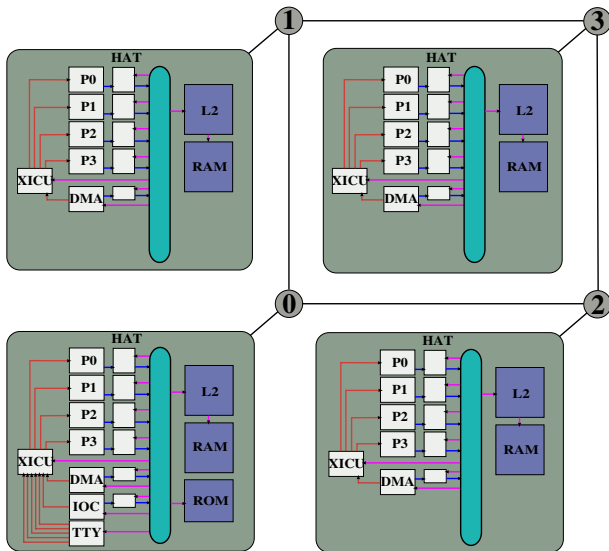
- Projet ANR TSUNAMY - LIP6 (Alsoc)
- Partenaires : Lab-STICC (Lorient), CEA LIST, Laboratoire Hubert Curien (St Etienne)
- Thèmes du projet
 - Architecture manycore
 - Cloud computing
 - Problématiques de sécurité
- Apports du LIP6
 - Architecture TSAR (CC-NUMA)
 - Système d'exploitation ALMOS

Contexte

Terminologie

- Système d'exploitation (OS) : ALMOS (utilisé dans le cadre de se stage).
- Instance d'un OS : Spécialisation d'un OS, qui comporte un système de fichiers, un code kernel binaire et un bootloader.
- Machine virtuelle (VM) : Sous-ensemble de clusters associé à une instance d'OS.

Sujet : Démarrer 2 ALMOS sur une plateforme à 4 clusters



Problèmes et solutions 1/3

Composant IOC : contrôleur de disque → composant MUTLI_IOC

- Un seul canal → multi-canal
- Un seul disque → un disque par canal

Routage des interruptions → composant IOPIC

Pas d'accès à l'intérieur de l'instance pour l'hyperviseur

- Concentre les interruptions des périphériques non-répliqués
- Envoi d'IPI (Inter-process-interrupt), interruption logicielle
- La cible est configurable par logiciel

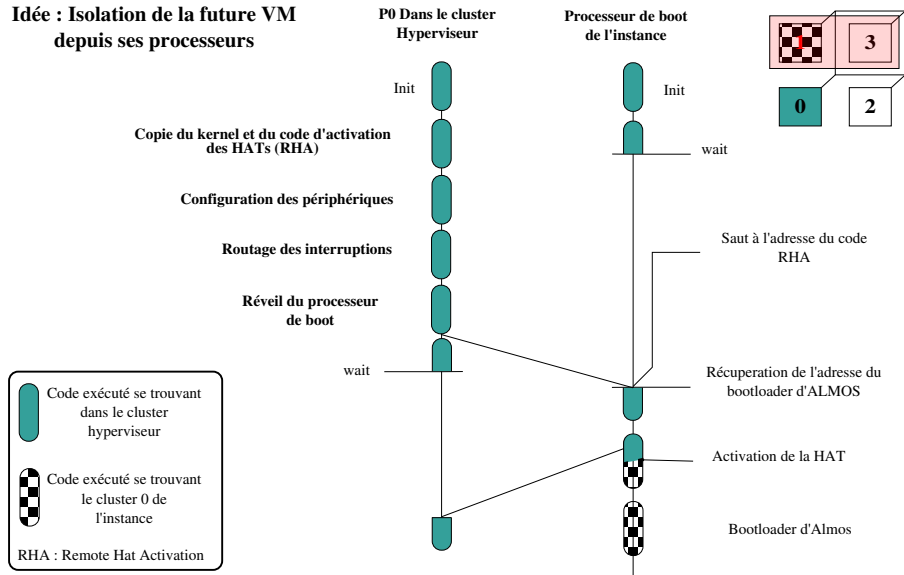
Problèmes et solutions 2/3

Composant MULTI_TTY → Composant MULTI_TTY_VT

- Une fenêtre par canal → création de sous-canaux
- → N sous-canaux par canal
- → Une fenêtre affiche le contenu d'un sous-canal
- → Choix du sous-canal affiché effectué par le logiciel
- → Fort couplage avec l'IOPIC

Problèmes et solutions 3/3 - Isoler $\leftarrow \rightarrow$ Réveiller

Idée : Isolation de la future VM depuis ses processeurs



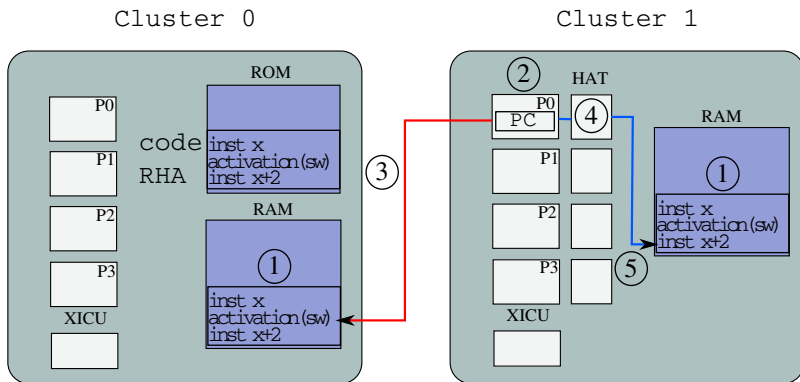
Procédure de recette

- ❶ Lancement d'un ALMOS sur 1 cluster sans IOPIC
- ❷ Lancement d'un ALMOS sur 1 cluster avec IOPIC
- ❸ Démarrage de deux ALMOS
 - Développement MULTI_IOC
- ❹ Démarrage des VMs en utilisant le Shell hyperviseur
 - Développement MULTI_TTY_VT
- ❺ Lancement de l'application "hello" sur les deux VMs

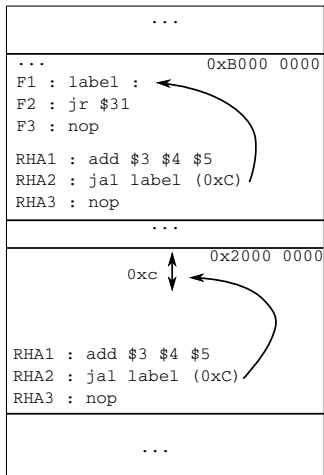
Différence avec la spécification

- Ajout du composant MULTI_HAT devant le composant MULTI_IOC
- Procédure de démarrage d'une VM plus complexe

Copie du code RHA dans la RAM



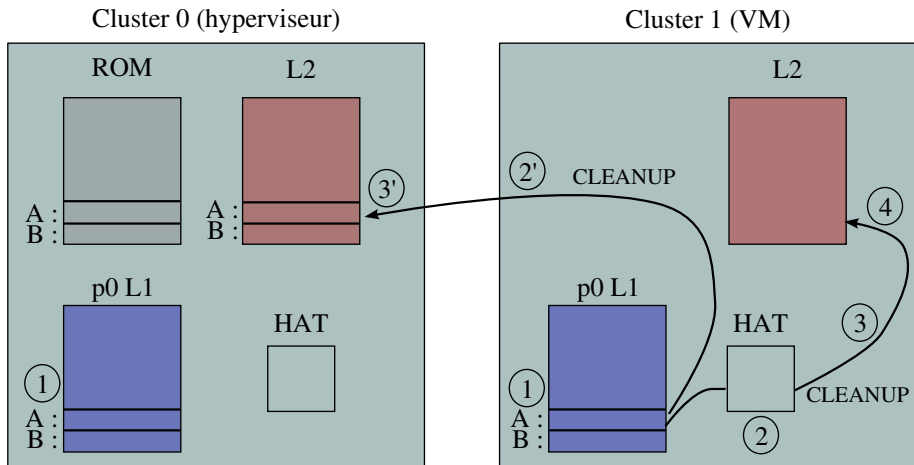
Appel de fonctions dans le code RHA



JAL ADDR28

RA = PC + 8; PC = PC_{31:28} :: ADDR28^⓪JALR R_D, R_SR_D = PC + 8; PC = R_S

Cohérence des caches



État initial

```
term0
[]

term1
[]

term2
[]

term3
[]

term4
tsarboot 1.3 (brejon@rythm Wed Aug 26 12:17:48 CEST 2015) (svn rev
0x3DFC000 - 0x3DFF000
hypev0 $ run 1 0[]
```

Lancement de la première VM

```

term0_1.txt
Wake up all processors                                IPI SENDS                                [ addr 0x1f
#80004 jump at 0x100000 ]
IPI SENDS                                [ addr 0x1ff80008 jump at 0x100000 ]
IPI SENDS                                [ addr 0x1ff8000c jump at 0x100000 ]
QM: gid : 0 -- hw_id : 16 -- lid : 0 -- cid : 0 -- outirq : 0
QM: gid : 1 -- hw_id : 17 -- lid : 1 -- cid : 0 -- outirq : 4
QM: gid : 2 -- hw_id : 18 -- lid : 2 -- cid : 0 -- outirq : 8
QM: gid : 3 -- hw_id : 19 -- lid : 3 -- cid : 0 -- outirq : 12
cluster_init: cid 0: start_addr 0x200000, limit_addr 0x3e00000, start_vaddr 0x80000
000
PPM 0 [ 15360, 14938, 11950, 2240, 746 ]
PPM 0 pages_tbl [0, 1, 2, 0, 1, 2, 2, 1, 1, 28]
Mapping Region <0x1ff80000 - 0x1ff81000> -> <0xff800000 - 0xff801000>
Found Device: XICU (Interrupt Control Unite With Integrated RT-Timers)
Base <0xff800000> Size <0x1000> Irq <-1>
Mapping Region <0x1ff00000 - 0x1ff01000> -> <0xff801000 - 0xff802000>

term1_1.txt
7 found
[/]>exec hello

term2_1.txt
[]

term3_1.txt
[]

term4
launching almos 0 on 1
lp = 3, gp = 19, cxy_id 1, bootentry addr = 0x100000
hypev0 $ run 2 1

```

Lancement de la seconde VM

```

tern0_2.txt
Kernel Entry Point @0x800ca44

Initialization of 2 Online Clusters [ 152259178 ]
Mapping Region <0x0 - 0x3e00000> : <0x80000000 - 0x83e00000>
Mapping Region <0x80000000 - 0x83e00000> -> <0x83e00000 - 0x87c00000>

Wake up all processors IPI SENDS [ addr 0x1ff80004 ju
mp at 0x100000 ]
IPI SENDS [ addr 0x1ff80008 jump at 0x100000 ]
IPI SENDS [ addr 0x1ff8000c jump at 0x100000 ]
IPI SENDS [ addr 0x9ff80000 jump at 0x100000 ]
IPI SENDS [ addr 0x9ff80004 jump at 0x100000 ]
IPI SENDS [ addr 0x9ff80008 jump at 0x100000 ]
IPI SENDS [ addr 0x9ff8000c jump at 0x100000 ]
QM: gid : 1 -- hw_id : 33 -- lid : 1 -- cid : 0 -- outirq : 4
QM: gid : 0 -- hw_id : 32 -- lid : 0 -- cid : 0 -- outirq : 0
QM: gid : 2 -- hw_id : 34 -- lid : 2 -- cid : 0 -- outirq : 8
QM: gid : 3 -- hw_id : 35 -- lid : 3 -- cid : 0 -- outirq : 12
QM: gid : 5 -- hw_id : 49 -- lid : 1 -- cid : 1 -- outirq : 4
QM: gid : 6 -- hw_id : 50 -- lid : 2 -- cid : 1 -- outirq : 8
QM: gid : 4 -- hw_id : 48 -- lid : 0 -- cid : 1 -- outirq : 0
QM: gid : 7 -- hw_id : 51 -- lid : 3 -- cid : 1 -- outirq : 12
cluster_init: cid 0: start_addr 0x200000, limit_addr 0x3e00000, start_vaddr 0x80000

tern1_2.txt
7 found
[/]>exec hello

tern2_2.txt

tern3_2.txt

tern4
launching almos 1 on 2
lp = 3, gp = 51, cxy_id 3, bootentry addr = 0x100000
hypev0 $

```

Conclusion et perspectives

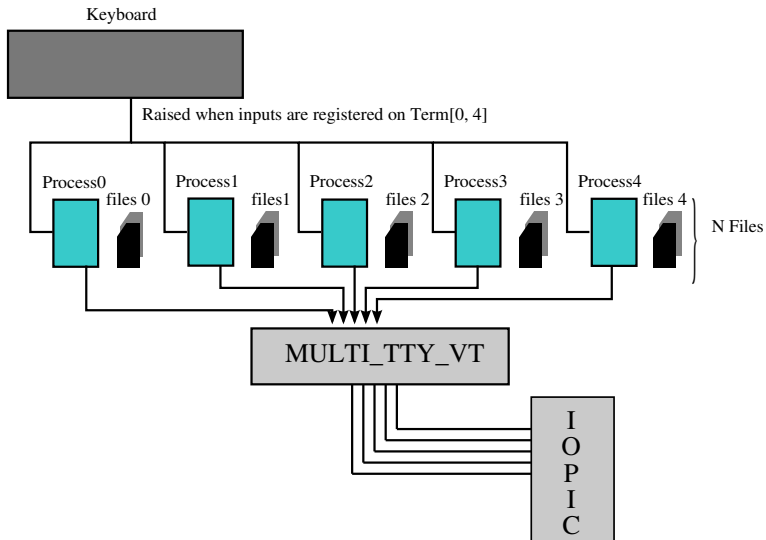
Conclusion

- L'hyperviseur, couplé aux composants, permet de lancer plusieurs VMs sur la même machine, objectif du stage atteint
- Les VMs sont isolées entre elles et ne peuvent pas accéder à l'hyperviseur
- Migration vers une plateforme plus réaliste (IOB 40bits)

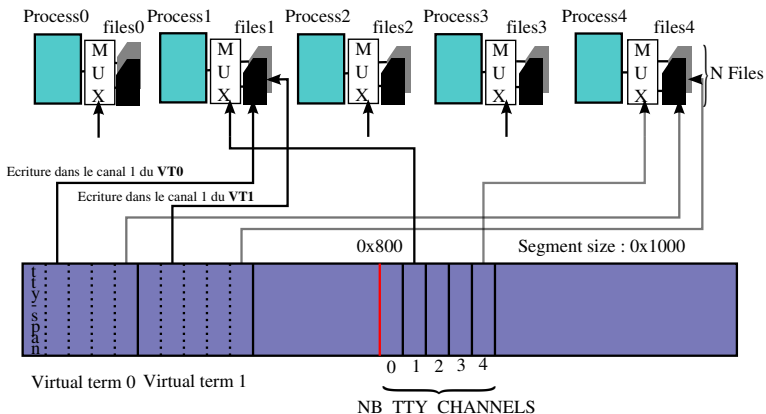
Perspectives

- Destruction des VMs
- Isolation complète des VMs

Solution pour affichage des machines virtuelles - Lecture



Solution pour affichage des machines virtuelles - Écriture



Exemple complet : séquence de démarrage

