From big iron to IoT

Julien Grall <julien.grall@arm.com>

Linaro Connect US 2016

© ARM 2016
Xen

- Type-1 hypervisor
- Supported architecture
  - x86-64
  - ARMv7 and ARMv8 with virtualization extensions
Type-1 vs Type-2

VM1
Applications
Guest Operating System

Type-1 Hypervisor
Hardware (CPU, Memory, Interrupts)

VM2
Applications
Guest Operating System

Applications
Guest Operating System

Applications
Type-2 Hypervisor
Native Operating System

Hardware (CPU, Memory, Interrupts)
Architecture

- Dom0
  - PV backends
  - HW drivers
- DomU
  - PV Frontends
- DomU
  - PV Frontends
- DomU
  - PV Frontends

Xen

Hardware
Architecture - 2
Para-Virtualized drivers
Para-Virtualized drivers

- Pair of drivers: backend/frontend
- Available for a wide range of devices
  - Console
  - Framebuffer
  - SCSI
  - Block
  - ...

© ARM 2016
PV: Architecture

Dom0

PV backends

HW drivers

DomU

PV Frontends

DomU

PV Frontends

DomU

PV Frontends

Xen

Hardware
How it works

Backend
Request Consumer

Request Producer

Response Consumer

Response Producer

Frontend
Virtualization on ARM
Virtualization

- ARMv7 and ARMv8
- Provides virtualization interfaces for
  - Timer
  - Interrupt Controller
  - Page Table
Virtualization - 2

Device Tree describes …

<table>
<thead>
<tr>
<th>GT</th>
<th>GIC v2</th>
<th>2 stage MMU</th>
</tr>
</thead>
</table>

EL0

EL1

HVC

EL2
Xen ARM
A perfect match

Device Tree describes …

Dom0 only

I/O

Any Xen guest VM

EL0

EL1

GT  GIC v2  2 stage MMU

HVC

EL2

Xen Hypervisor
Clean architecture

- It is NOT a straight 1:1 port of x86
- No device emulation
- One kind of guest supported
- Exploit virtualization support in hardware
- Easier to support new OS
## Small code base

<table>
<thead>
<tr>
<th></th>
<th>common</th>
<th>ARMv7</th>
<th>ARMv8</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>xen/arch/arm</td>
<td>16390</td>
<td>2394</td>
<td>2394</td>
<td>21216</td>
</tr>
<tr>
<td>C</td>
<td>15247</td>
<td>1664</td>
<td>1763</td>
<td>17338</td>
</tr>
<tr>
<td>ASM</td>
<td>143</td>
<td>730</td>
<td>669</td>
<td>3878</td>
</tr>
<tr>
<td>xen/include/asm-arm</td>
<td>4297</td>
<td>611</td>
<td>724</td>
<td>5632</td>
</tr>
<tr>
<td><strong>Total ARM</strong></td>
<td>20687</td>
<td>3005</td>
<td>3118</td>
<td>26848</td>
</tr>
<tr>
<td><strong>x86_64</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>xen/arch/x86</td>
<td></td>
<td></td>
<td></td>
<td>100970</td>
</tr>
<tr>
<td>xen/include/asm-x86</td>
<td></td>
<td></td>
<td></td>
<td>13119</td>
</tr>
<tr>
<td><strong>Total x86_64</strong></td>
<td></td>
<td></td>
<td></td>
<td>114089</td>
</tr>
</tbody>
</table>

`sloccount on Xen 4.7-rc2`
Secure

- Isolation, disaggregation and partitioning
- No device emulation, no QEMU
- Small surface of attack
Xen 4.8 will be released in December 2016.

Readiness:

- EFI guest and host support
- ACPI guest (Linaro is working on it) and host support
- Support for guest with 64K, 16K and 4K page granularity
- New hardware and platform support
- All main features present
Resources
Using Xen

- **user ML:** xen-user@lists.xenproject.org
- **wiki:** https://goo.gl/9qsfMf
- **whitepaper:** https://goo.gl/TcuqXd
Contributing to Xen

- **devel ML:** xen-devel@lists.xenproject.org
- **#xenarm or #xendevel on freenode**
Questions?