What is Xen?

- The only open-source type-1 hypervisor
- For Unix and Unix-like OS
  - Linux, NetBSD and OpenSolaris
- From ancient greek term Xenos (ξένος), "guest-friends"
- Developed by the University of Cambridge, now by the Linux Foundation
- GNU General Public License (GPL2)
- Programming language: C
What is a hypervisor?

- Hypervisor = virtual machine monitor (VMM)
- Computer software/firmware/hardware that creates and runs virtual machines

- Host machine – the computer a hypervisor runs on
- Guest machine – each virtual machine

- Types:
  - Type-1, native or bare-metal hypervisors
    - Runs directly on the real hardware
  - Type-2 or hosted hypervisors
    - Runs on the OS
History of Xen

- **Late 1990s**
  - Xen hypervisor created by Keir Fraser and Ian Pratt as part of the Xenoserver research project at Cambridge University in the late 1990s

- **2002**
  - The Xen hypervisor was open sourced
History of Xen

2004

- Xen 1.0 was officially released, followed a short time later by Xen 2.0
- Ian Pratt and others founded XenSource, Inc.
  - Goal to convert Xen hypervisor from a research tool into a competitive product for enterprise computing.
  - Xen hypervisor remained an open source solution
History of Xen

- **2006**
  - Microsoft and VMWare adopted the concept of Paravirtualization, first introduced by the Xen community

- **2007**
  - Citrix Systems, Inc. acquired XenServer in August for $500 million
History of Xen

- 2006
  - Microsoft and VMWare adopted the concept of Paravirtualization, first introduced by the Xen community

- 2007
  - Citrix Systems, Inc. acquired XenServer in August for $500 million
History of Xen

- **2009**
  - The Xen community announced a new initiative for Cloud Computing, Xen Cloud Platform

- **2010**
  - Xen 4.0. released
  - A community contest has selected a mascot
History of Xen

- 2011
  - The Xen community delivered the first version of the Xen Cloud Platform
  - Linux 3.x, contains full support for Xen Dom0 and DomU
  - Major Linux distributions announce that they will re-introduce Xen into their distributions

- 2012
  - The Xen Cloud Platform packages for Linux are released
History of Xen

- **2013**
  - The Xen ARM port becomes functional
  - Xen becomes part of the Linux Foundation as a Linux Foundation Collaborative Project
  - Trademark "Xen Project" is issued to the Linux Foundation
  - First user-centric event – Xen Project User Summit
Xen management consoles

- Third-party tools to facilitate the common tasks of administering a Xen host
  - configuring, starting, monitoring and stopping of Xen guests.
- Non-commercial:
  - Web-based HyperVM
  - Web-based ConVirt
  - OpenNebula
  - openSUSE YaST and virt-man
  - ...
- Commercial:
  - Citrix XenServer
  - Huawei FusionSphere[70]
  - Oracle VM Server for x86
  - ...
What is a hypervisor?

- Hypervisor = virtual machine monitor (VMM)
- Computer software/firmware/hardware that creates and runs virtual machines

- Host machine – the computer a hypervisor runs on
- Guest machine – each virtual machine

- Types:
  - Type-1, native or bare-metal hypervisors
    - Runs directly on the real hardware
  - Type-2 or hosted hypervisors
    - Runs on the OS
What is a hypervisor useful for?

- Server virtualization
- Software development (including the development of operating systems)
  - No need to reboot the physical computer whenever a bug occurs
- Computer-security research
  - Sandboxing
- Various pieces of software may require different operating systems
Uses of virtual servers

- consolidation => increased utilization
- dynamic fault tolerance against software failures
  - (through rapid bootstrapping or rebooting)
- hardware fault tolerance
  - (through migration of a virtual machine to different hardware)
- secure separation of operating systems
- support of legacy software and OS instances on the same computer
- Xen supports virtual machine live migration from one host to another
  - workload balancing and the avoidance of downtime
Xen virtualization

- **5 types of virtualization:**
  - HVM (hardware virtual machine)
  - HVM with PV drivers
  - PVHVM (paravirtualization with full hardware virtualization, i.e. HVM with PVHVM drivers)
  - PVH (PV in an HVM container)
  - PV (paravirtualization)
The Paravirtualization Spectrum

- **Virtualized (V)**
- **Paravirtualized (P)**

<table>
<thead>
<tr>
<th></th>
<th>Disk / Network</th>
<th>Interrupts, Timers</th>
<th>Emulated Motherboard</th>
<th>Privileged Instructions and page tables</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Virtualization</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
</tr>
<tr>
<td>FV with PV disk,</td>
<td>P</td>
<td>V</td>
<td>V</td>
<td>V</td>
</tr>
<tr>
<td>network</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PVHVM</td>
<td>P</td>
<td>P</td>
<td>V</td>
<td></td>
</tr>
<tr>
<td>PVH</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>V</td>
</tr>
<tr>
<td>Full Paravirtualized</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
</tr>
</tbody>
</table>

- **HVM mode**
- **PV mode**
<table>
<thead>
<tr>
<th>x86 Shortcut</th>
<th>Mode</th>
<th>With</th>
<th>Interrupts &amp; Timers</th>
<th>Privileged Instructions</th>
<th>Page Tables</th>
<th>QEMU Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>HVM / Fully Virtualized</td>
<td>HVM</td>
<td></td>
<td>VS</td>
<td>VS</td>
<td>VS</td>
<td>VH</td>
</tr>
<tr>
<td>HVM + PV drivers</td>
<td>HVM</td>
<td>PV Drivers Installed</td>
<td>VS</td>
<td>VS</td>
<td>VS</td>
<td>VH</td>
</tr>
<tr>
<td>PVHVM</td>
<td>HVM</td>
<td>PVHVM Capable Guest</td>
<td>PV</td>
<td>PV2</td>
<td>VS</td>
<td>VH</td>
</tr>
<tr>
<td>PVH</td>
<td>PVH</td>
<td>PVH Capable Guest</td>
<td>PV</td>
<td>HA3</td>
<td>PV4</td>
<td>VH</td>
</tr>
<tr>
<td>PV</td>
<td>PV</td>
<td></td>
<td>PV</td>
<td>PV</td>
<td>PV5</td>
<td>PV</td>
</tr>
<tr>
<td>ARM</td>
<td>N/A</td>
<td></td>
<td>PV</td>
<td>VH</td>
<td>PV6</td>
<td>VH</td>
</tr>
</tbody>
</table>

PV = Paravirtualized
VS = Software Virtualized (QEMU)
VH = Hardware Virtualized
HA = Hardware Accelerated
Paravirtualization

- Guest knows it's a guest on the host
- Guests run a modified operating system
  - The guests are modified to use a special hypercall application binary interface (ABI)
- High performance even on Xen’s host architecture (x86)
- Xen can run PV guests even on CPUs without support for virtualization
- No need to emulate a full set of hardware and firmware services
  - Simpler to manage
  - Reduces the exposed attack surface
- Hard (almost impossible) to modify the kernel of closed-source operating systems like Windows to use this method
HVM

- Full virtualization
- Can run almost all the operating systems without any modifications
- HVM virtualization extensions from the host CPU to virtualize guests
- HVM requires Intel VT or AMD-V hardware extensions
- The hypervisor emulates PC hardware, including BIOS, IDE disk controller, VGA graphic adapter, USB controller, network adapter etc.
- Virtualization hardware extensions are used to boost performance of the emulation
- For older host operating systems, fully virtualized guests are usually slower than paravirtualized guests
- Inefficient
- Paravirtualization on HVM
  - Full virtualization with paravirtualization drivers
Xen hosts

- Xen can be shipped in a dedicated virtualization platform, such as Citrix XenServer Enterprise Edition
- Xen is available for and distributed with:
  - Alpine Linux, Arch Linux, Debian GNU/Linux, FreeBSD, Gentoo, Mageia, NetBSD
  - OpenSolaris-based distributions, openSUSE, Qubes OS, SUSE Linux Enterprise Server, Solaris, Ubuntu
Xen guests

- Paravirtualized
  - Linux, FreeBSD, OpenBSD, NetBSD, MINIX, GNU/Hurd, Plan 9 from Bell Labs
- Full virtualization only
  - Anything else, including Windows
Xen alternatives

- VirtualBox
- KVM (Kernel-based Virtual Machine)
- OpenStack
- Portable Virtualbox
- VMware vSphere Hypervisor
- Microsoft Hyper-V Server
- Citrix XenServer
- Danube Cloud
- ...