Ubiquitous Xen

Ian Pratt, Chairman of Xen.org, Citrix Systems Inc.
Outline

• A brief history of Xen
• Why virtualization matters
• The Xen Advantage
• New Frontiers
The Xen Story

• Apr 2002 Xen hypervisor development starts
• Oct 2003 Xen SOSP paper
• Apr 2004 Xen 1.0 released
• Jun 2004 First Xen developer’s summit
• Nov 2004 Xen 2.0 released
• 2004 Hardware vendors start taking Xen seriously
• 2005 RedHat, Novell, Sun and others adopt Xen
• Dec 2005 Xen 3.0 released
• 2006 VMware and Microsoft adopt paravirtualization
• May 2008 Xen embedded in Flash on HP/Dell servers
• Aug 2008 Xen 4.0 released
Xen Project Mission

• Build the industry standard OSS hypervisor
  – Core "engine" that is incorporated into multiple vendors’ products

• Maintain Xen’s industry-leading performance
  – Be first to exploit new hardware acceleration features
  – Help OS vendors paravirtualize their OSes

• Maintain Xen’s reputation for stability and quality
  – Security is paramount

• Support multiple CPU types
  – From server to client to mobile phone

• Foster innovation

• Drive interoperability
Xen Community: Strong & Productive

• Over 250 contributors to the 3.x series
• Vendors optimize Xen for their products
  – CPU and I/O vendors; OSVs; Mgmt vendors
• Research community
  – Develop new Xen features
  – Explore entire new uses of virtualization
  – Many Universities, IBM, HP, Intel, NSA
• User community
  – Amazon, Google, Oracle, MySpace, hosting providers
• Xen.org and the new Xen Advisory Board
  – Management oversight, trademark policy etc
## Xen Community and ISVs

### Application Appliances
- avinti®
- CFT
- Marathon
- SteelEye Technology, Inc.
- Double-Take Software

### Application Migration
- Transitive®

### Backup
- Zmanda

### Database
- Ingres®

### Grid Computing
- Voltaire

### Identity Management
- Centrify
- Likewise

### Provisioning
- Data Mountain View Data®
- Scalent
- egenera

### High Availability/Disaster Recovery
- Marathon
- SteelEye Technology, Inc.
- Double-Take Software

### Network Hardware
- Toxmi Networks
- Chelsio Communications
- Mellanox Technologies

### P2V Conversion
- LeoStream
- Invirut

### System Management
- Avocent
- Evident
- ToutVirtual

### System Hardware
- Supermicro
- Verari Systems®

### Virtual Appliance
- JumpBox

### Virtual Lab Management
- VMLogix

### Xen Community and ISVs

### System Hardware
- Supermicro
- Verari Systems®

### Virtualization Management
- Availigent
- Cassatt

### Service Level Automation
- Enigmatic

### Security
- Reflex Security
- SignaCert

### Virtual Appliances
- JumpBox

### Virtualization Management
- Availigent
- Cassatt

### Xen Community and ISVs
Why Virtualization is ‘Hot’

• Clearing up the mess created by the success of ‘scale-out’
  – One Application per commodity x86 server
  – Leads to ‘server sprawl’
  – 5-15% CPU utilization typical

• Failure of popular OSes to provide
  – Full configuration isolation
  – Temporal isolation for performance predictability
  – Strong spatial isolation for security and reliability
  – True backward app compatibility
First Virtualization Benefits

• Server consolidation
  – Consolidate scale-out success
  – Exploit multi-core CPUs

• Manageability
  – Secure remote console
  – Reboot / power control
  – Performance monitoring

• Ease of deployment
  – Rapid provisioning

• VM image portability
  – Move image between different hardware
  – Disaster Recovery
2nd Generation Virtualization Benefits

- Avoid planned downtime with VM Relocation
- Dynamically re-balance workload to meet app SLAs or to save power
Virtualization enables High-Availability

- **Restart-HA** monitors hosts and VMs to keep apps running

- **Hardware Fault Tolerance** with deterministic replay or checkpointing
Virtualization Security

- Virtualization adds more software and thus increases the potential attack surface
  - Network-facing control stack
  - VM containment

- Xen smaller and more defensible than an OS
  - True hypervisor architecture
  - Need a “strength in depth” approach
    - Disaggregate, De-privilege, narrow interfaces
    - Xen Security Modules (XSM) from the NSA
  - Secure Xen launch with TPM TXT/SKINIT
Improving Security with Virtualization

• Virtualization allows administrative policy enforcement from outside of the OS
  – Firewalls, IDS, malware scanning etc
    • More robust as not so easily disabled
    • Provides protection within a network rather than just at borders
  – Hardening OSes with immutable memory, taint tracking, logging and replay
  – Backup policy, multi-path IO, HA, FT etc
    • Availability and Reliability

• Reducing human effort required to admin all the VMs is the next frontier
Virtualization and Application Stacks

• Simplifies Application-stack certification
  – Certify App-on-OS; OS-on-HV; HV-on-h/w
  – Enables Virtual Appliances

• Virtual hardware greatly reduces the effort to modify/create new OSes
  – Application-specific OSes
    • Slimming down and optimization of existing OSes
    • “Native execution” of Apps
  – Great opportunity for Linux
Maximizing Performance

Xen Hypervisor

Intel VT & AMD-V, Smart IO & chipset Technologies

Paravirtualization
Unlocking Hardware Innovation

Only a hypervisor can deliver the benefits of the new hardware

Enhanced Security
- TPM and secure boot (TXT)
- IOMMU to protect device DMA accesses
- Full Execute-Disable (NX/XD)

Hardware Virtualization Support
- Nested Page Tables (VT2/VMI)
- FlexPriority, FlexMigrate
- Smart NICs (e.g. VT-C/VMDq) and HBAs

Multi-core Processors
- More efficient utilization
- Hides complexity from guests
Performance

W2k3 Parallel DDK Build

8/25/2008
w2k3 Passmark memory results

Allocate Small Block
Read Cached
Read Uncached
Write
Memory Mark

Relative score to native (higher is better)

Native
ESX 3.0.1
XenEnterprise 3.2
SPECjbb2005 (Sun JVM)

RHEL5 guest / SPECjbb2005 Sun JVM

Relative score to native

1.2
1.0
0.8
0.6
0.4
0.2
0.0

1-vcpu
2-vcpu
4-vcpu

Native
ESX 3.0.1
XenEnterprise 3.2
“HP will offer the Citrix XenServer HP Select Edition as the preferred and recommended solution for virtualization on Proliant Systems”

Scott Farrand, VP Software, HP Industry Standard Servers

- Xen embedded into system firmware
- Closely coupled and optimized for h/w
  - Dedicated hypervisor better able to meet the rapid h/w product cycle than a full OS, and thus best placed to fully enable new hardware features
Xen Client : A Hypervisor for Client Devices

- Security, Manageability and Supportability
- “Embedded IT” virtual appliances
  - IDS, Malware detection, remote access, backup etc.
- Building Multi-level secure systems
  - Run multiple guest VMs with very controlled information flow
    - Enables Bring-Your-Own-PC model
    - Corporate VM; VM for web browsing; VM for banking
    - Seamless merging of VM displays
    - Migration of VMs between datacentre and laptops for offline use
- Security requires a true hypervisor architecture
  - Intel TXT / AMD SKINIT and Trusted Platform Module
From Laptops to Phones

- Smart phones and portable devices
  - Xen ARM
  - Smart phones now suffer from many of the same problems as PCs

- Simple restricted use cases:
  - Three VMs running on one CPU:
    - Real time VM for controlling the radio
    - VM for vendor/operator - supplied s/w
    - VM for user-downloaded software
XenoServers: University Project from 1999

- Incremental rollout
- Flexible platform
- Unified management

- Global services and apps
- Exploit network topology
- Open commercial platform

Deploy

- XenoCorp
- XenoServer
- Client
XenoServers Vision is Becoming Reality

Industry’s largest production use of virtualization

Amazon has thousands of servers running Xen
- Server consolidation and workload management
- EC2 (Elastic Computing Cloud) “Rent a VM”
Augmenting IT infrastructure with Cloud

• Dynamic infrastructure as a service
  – 100% virtualized, and fully manageable
  – Pay as you use - no long-term contracts

• Initial applications for Cloud
  – End-user facing applications (e.g. Web) - take advantage of Cloud’s global presence and fat pipes
  – Test and Dev environments, Disaster Recovery

• Extending the Data Center into the Cloud
  – Seamless movement on Xen VMs
Where to get Xen?

• Incorporate OSS Xen in to your custom OS install
  – Common among virtual server hosting providers
  – Large Enterprises with tens of thousands of machines,
    E.g. Amazon.com Google

• OS-integrated Xen
  – Attractive if you’re primarily running one OS
  – E.g. Red Hat Novell Sun Oracle

• Platform-integrated virtualization
  – OS-agnostic; “virtual machine hosting appliance”
  – E.g. Citrix Virtual Iron HP Dell Symantec

• Xen for clients
  – E.g. Phoenix Technologies NeoCLEUS Lenovo
Closing Remarks

• Virtualization is destined to become ubiquitous
  – Every machine, Every workload
  – Built in to the platform
  – Client devices as well as servers

• Xen offers the best performance and the most secure architecture
  – Xen is powered by a growing community with a diverse range of products and services