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

avinto

cFT

APPLICATION MIGRATION

TRANSITIVE

BACKUP

zmanda

DATABASE

INGRES

GRID COMPUTING

Voltaire

IDENTITY MANAGEMENT

Centrify

Likewise

HIGH AVAILABILITY/DISASTER RECOVERY

MARATHON

SteelEye TECHNOLOGY INC

Double-Take Software

NETWORK HARDWARE

TEHUTI NETWORKS

Chelsio Communications

ServerEngines

SOLARFLARE Communications

Mellanox TECHNOLOGIES

P2V CONVERSION

LEOSTREAM

invirtus

PLATESPIN

PROVISIONING

DATA Mountain View Data

SCALENT

egenera

SAN HARDWARE

QLOGIC

BROCADE

EMULEX

ISILON SYSTEMS

compellent

NetApp

DataCore SOFTWARE

LeftHand NETWORKS

FalconStor Software

STONEFLY

SECURITY

CATBIRD NETWORKS

REFLEX SECURITY

SignaCert

SERVICE LEVEL AUTOMATION

Enigmatec CORPORATION

SYSTEM HARDWARE

SUPERMICRO

Verari systems

SYSTEM MANAGEMENT

ConVirt

Avocent The Power of Being There.

embotics

enomaly open source consulting

HYPERIC

Qlusters

evident Software

virtugo

TroutVirtual

VIRTUALIZATION MGMT

Cassatt

Platform

AVAILIGENT

VIRTUAL APPLIANCES

JumpBox

virtual appliances

rPath The Software Appliance Company

VIRTUAL LAB MANAGEMENT

VMLogix

Surgient

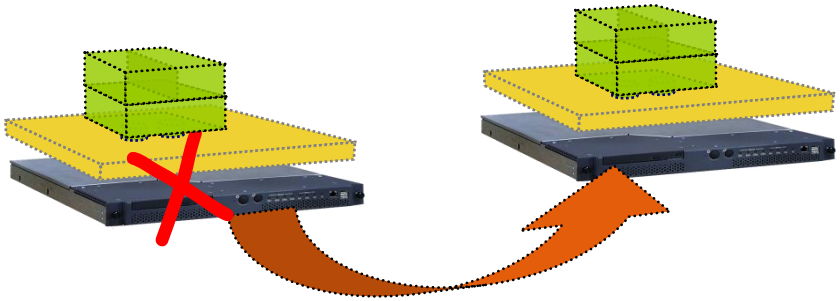
Why Virtualization is ‘Hot’

- 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

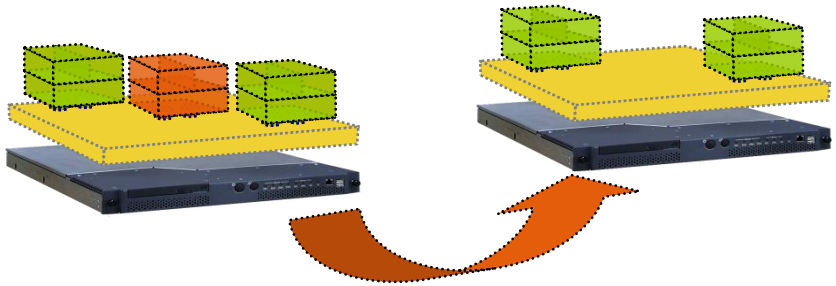
First Virtualization Benefits

- 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

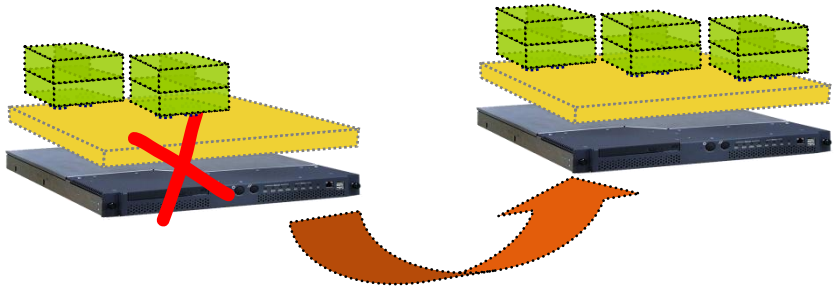


- **Avoid planned downtime with VM Relocation**

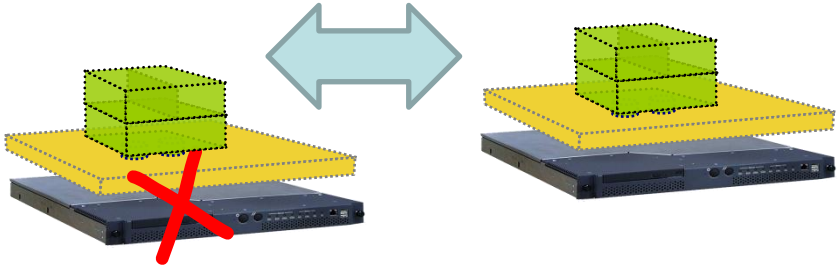


- **Dynamically re-balance workload to meet app SLAs or to saver power**

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

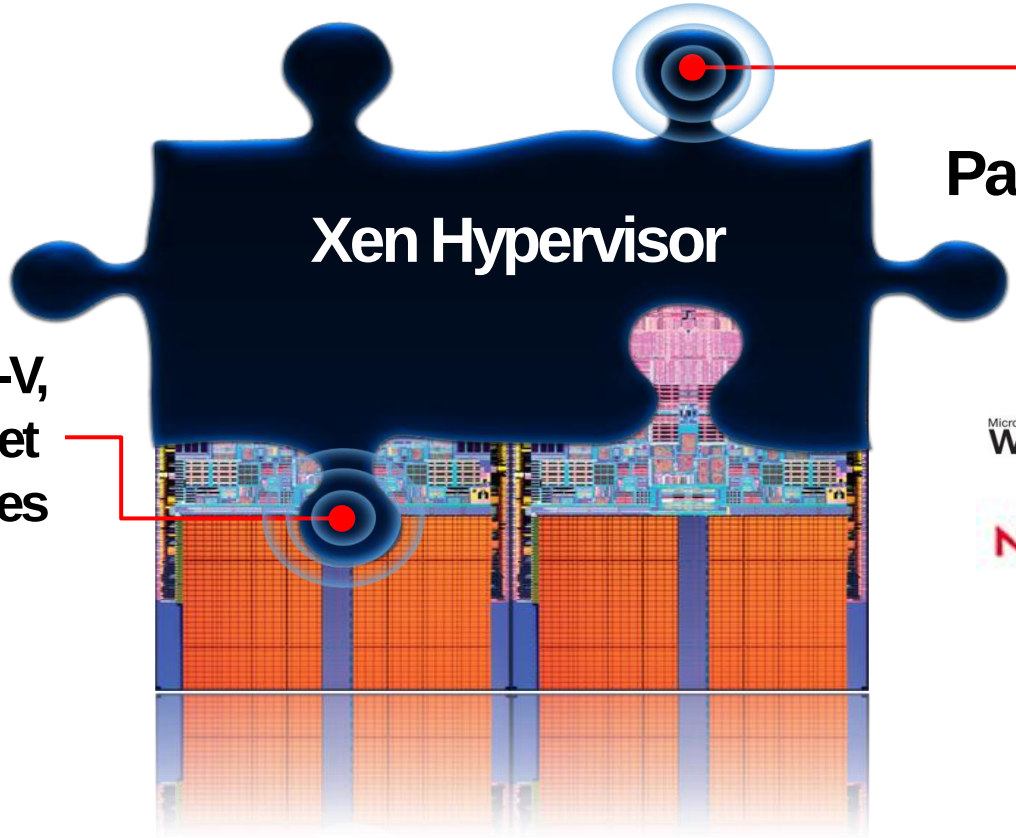
Improving Security with Virtualization

- 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



Paravirtualization

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

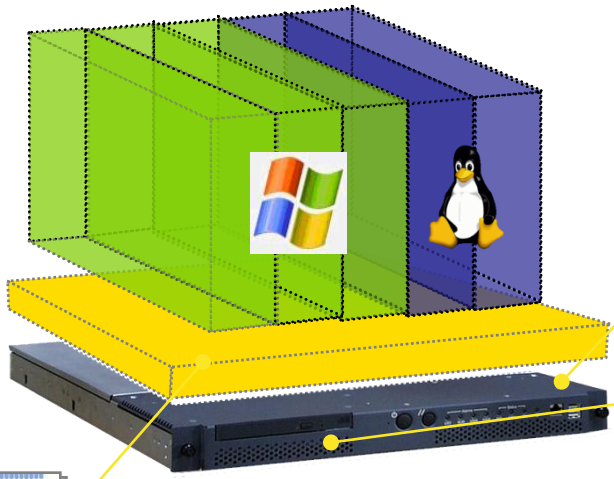
Microsoft Windows

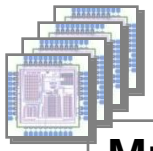
redhat

Novell

Sun microsystems

Unlocking Hardware Innovation





Multi-core Processors

- More efficient utilization
- Hides complexity from guests

Enhanced Security

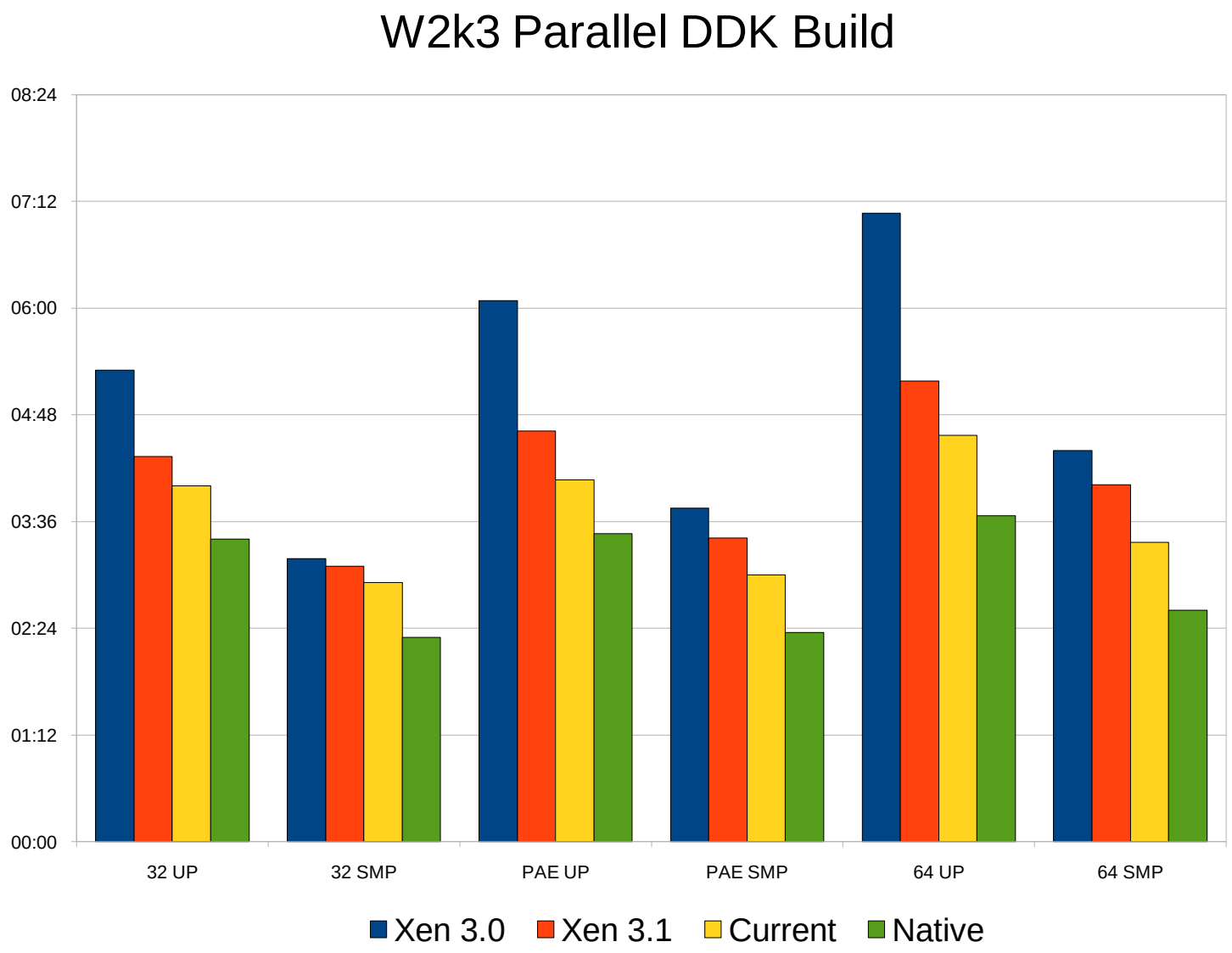
- TPM and secure boot (TXT)
- IOMMU **to protect device DMA accesses**
- **Full Execute-Disable (NX/XD)**

Hardware Virtualization Support

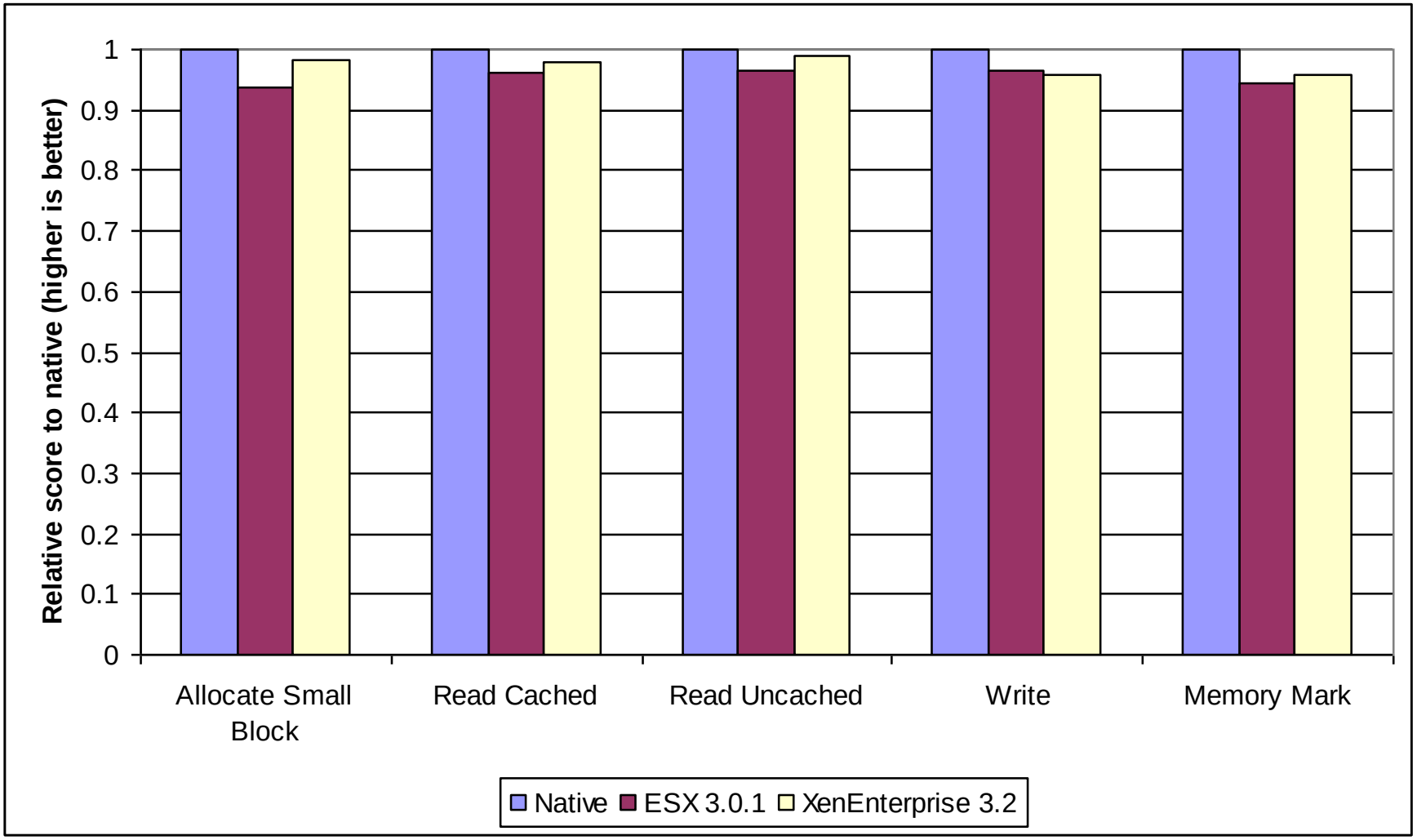
- Nested Page Tables (VT2/VMI)
- FlexPriority, FlexMigrate
- Smart NICs (e.g. VT-C/VMDq) and HBAs

Only a hypervisor can deliver the benefits of the new hardware

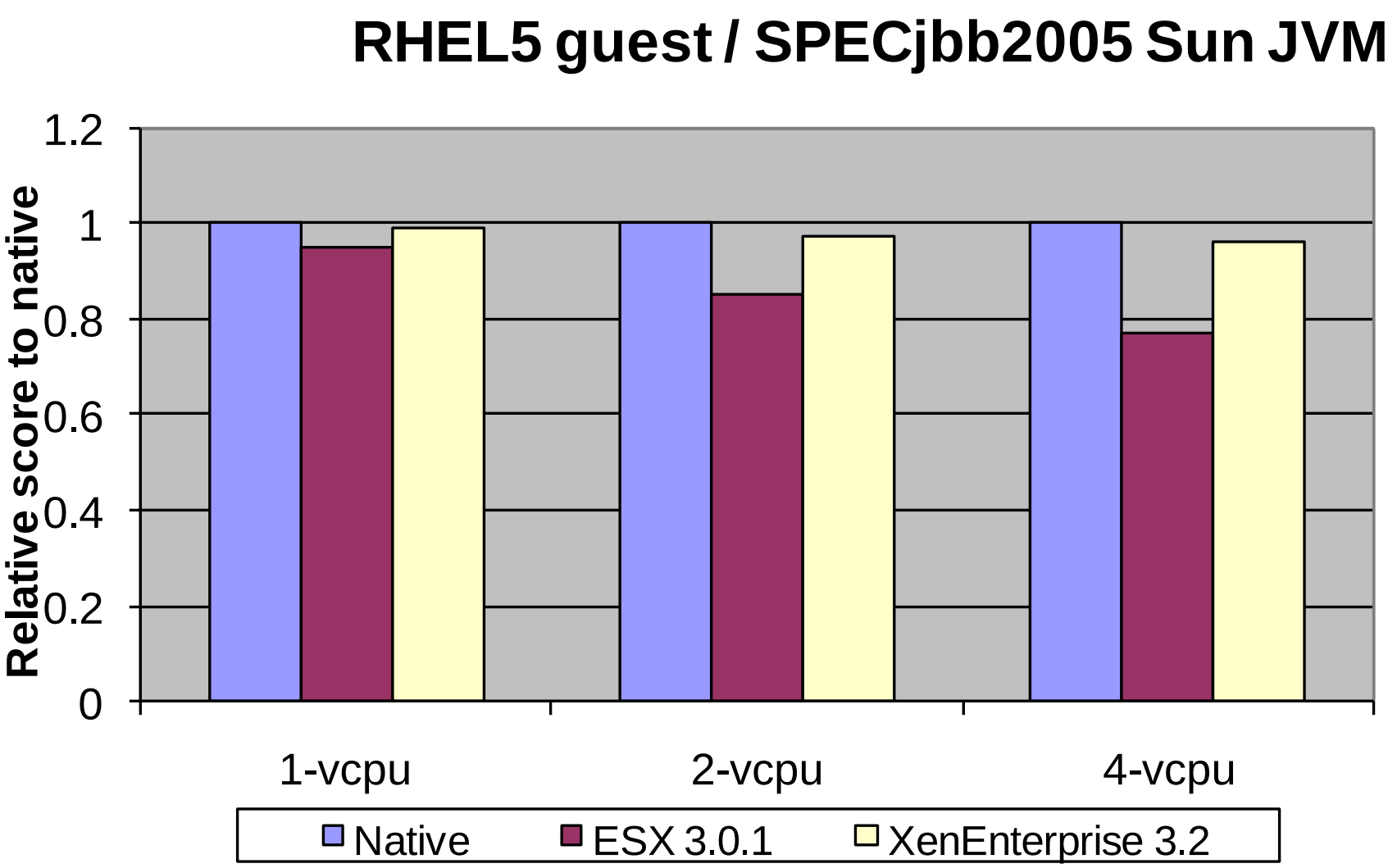
Peformance


W2k3 Parallel DDK Build
08:24
07:12
06:00
04:48
03:36
02:24
01:12
00:00
32 UP
32 SMP
PAE UP
PAE SMP
64 UP
64 SMP
Xen 3.0
Xen 3.1
Current
Native

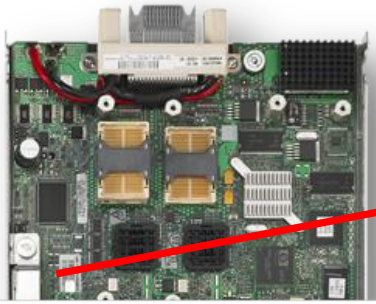
w2k3 Passmark memory results



SPECjbb2005 (Sun JVM)



Embedding Xen



“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

i n v e n t

- **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**

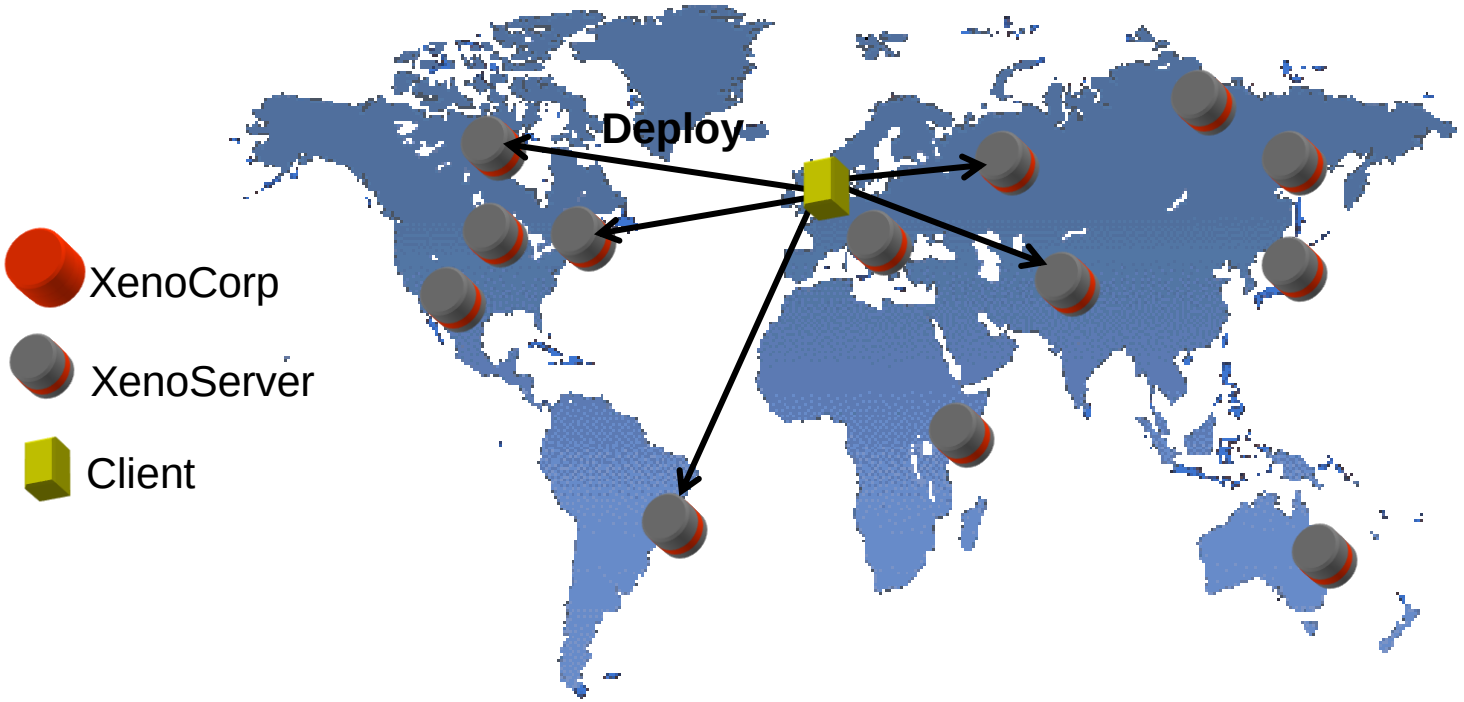
Xen Client : A Hypervisor for Client Devices

- 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

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. redhat Novell Sun ORACLE
- Platform-integrated virtualization
  - OS-agnostic; "virtual machine hosting appliance"
  - E.g. CITRIX VirtualIron hp invent DELL symantec.
- Xen for clients
  - E.g. phoenix technologies NEOCLEUS Virtualizing Endpoints 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