Panoramica su Cloud Computing targata Red Hat

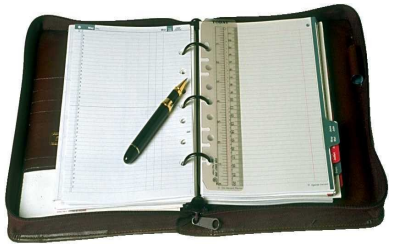
AIPSI Meeting 2010

Giuseppe “Gippa” Paterno'
Solution Architect
EMEA Security Expert
gpaterno@redhat.com

Who am I

- Currently Solution Architect and EMEA Security Expert in Red Hat
- Visiting Researcher at Trinity College Dublin
- Previously Security Solution Architect in Sun and also in IBM
- Red Hat Certified Security Specialist (RHCSS), RH Architect (RHCA) and Cisco Certified Network Professinal (CCNP)
- Part of the italian security community *sikurezza.org*
- Forensic analisys for local govs
- More on:
  - http://www.gpaterno.com/
  - http://www.scss.tcd.ie/Giuseppe.Paterno/
  - http://www.linkedin.com/in/gpaterno

Agenda



- Cloud computing
- Red Hat Virtualization Strategy
- Cloud Security (Gippa's hardcore security :)

What is a cloud?

"A computing capability that provides an abstraction between the computing resource and its underlying technical architecture (e.g., servers, storage, networks), enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction."

(from Wikipedia)

Build your own cloud!

To summarize:

efficient usage of YOUR resources

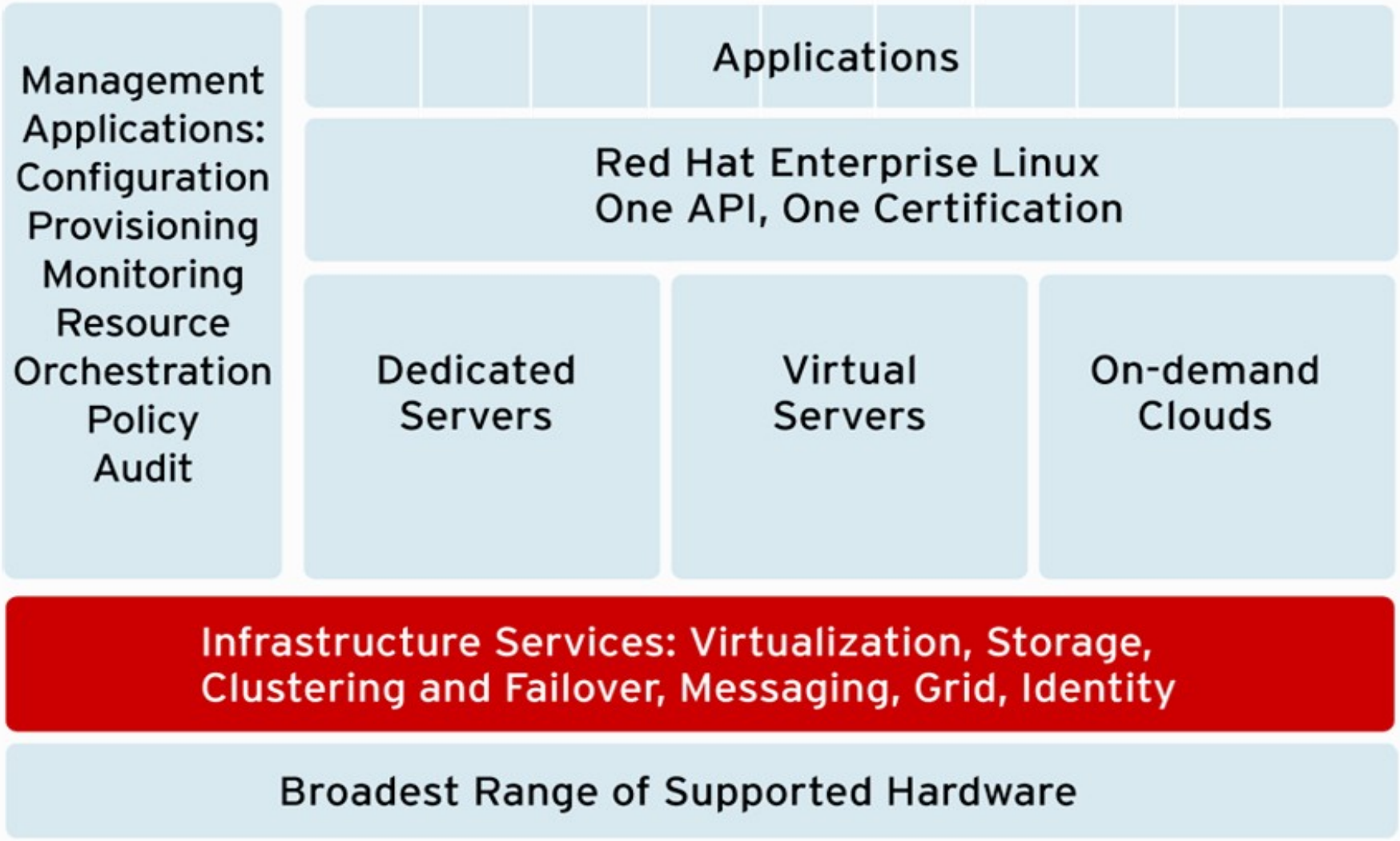
Let's build your own cloud with the following characteristics: lower the costs, agility, reliability, scalability, accountability and

.... security!!!

Red Hat Virtualization Portfolio

RED HAT'S LINUX AUTOMATION ARCHITECTURE

Any application, anywhere, anytime

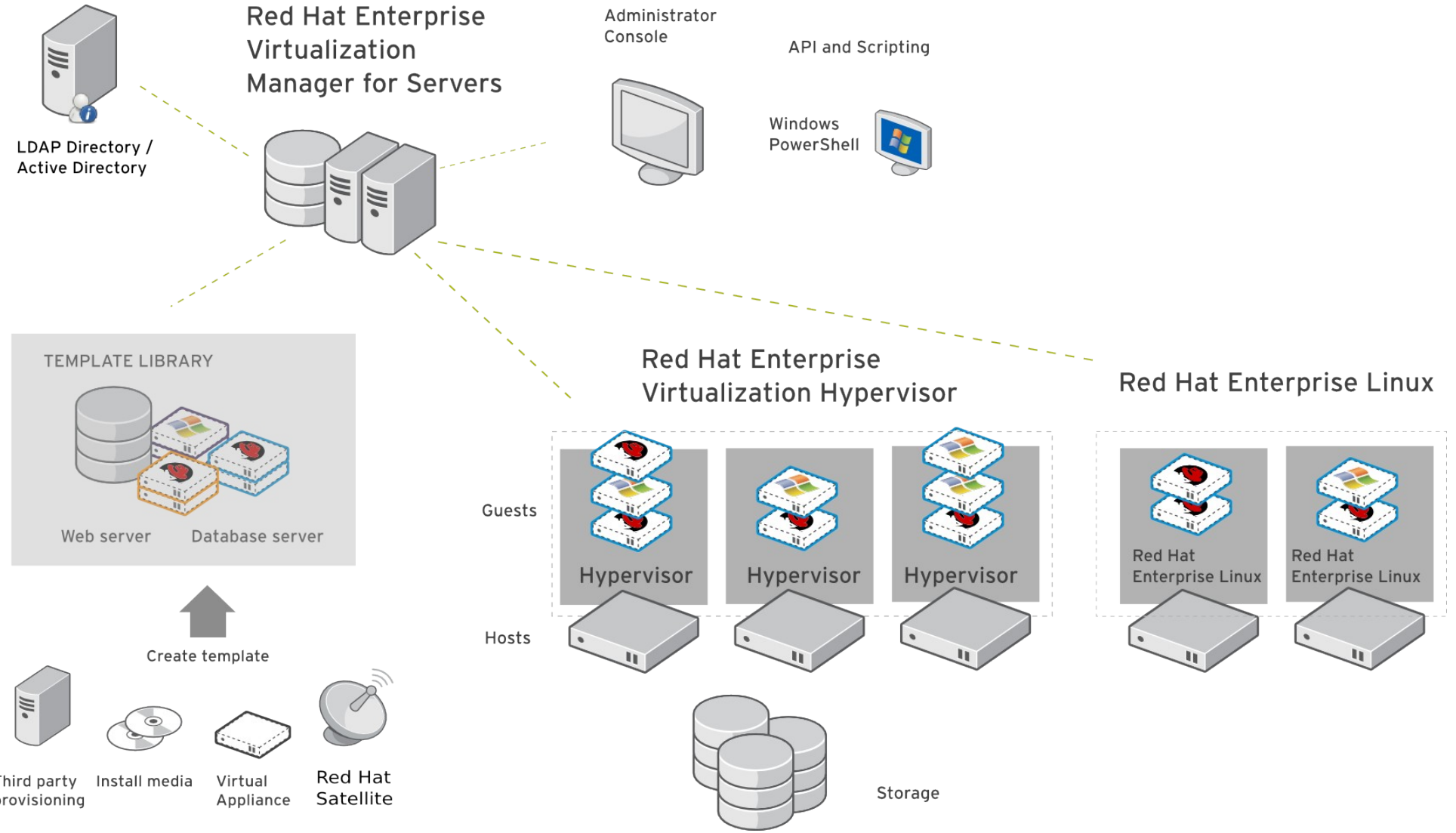


RED HAT ENTERPRISE VIRTUALIZATION (RHEV)

- **RHEV MANAGER FOR SERVERS**
  - Enterprise grade server management system
- **RHEV MANAGER FOR DESKTOPS** **(beta)**
  - Virtual Desktop Infrastructure with SPICE

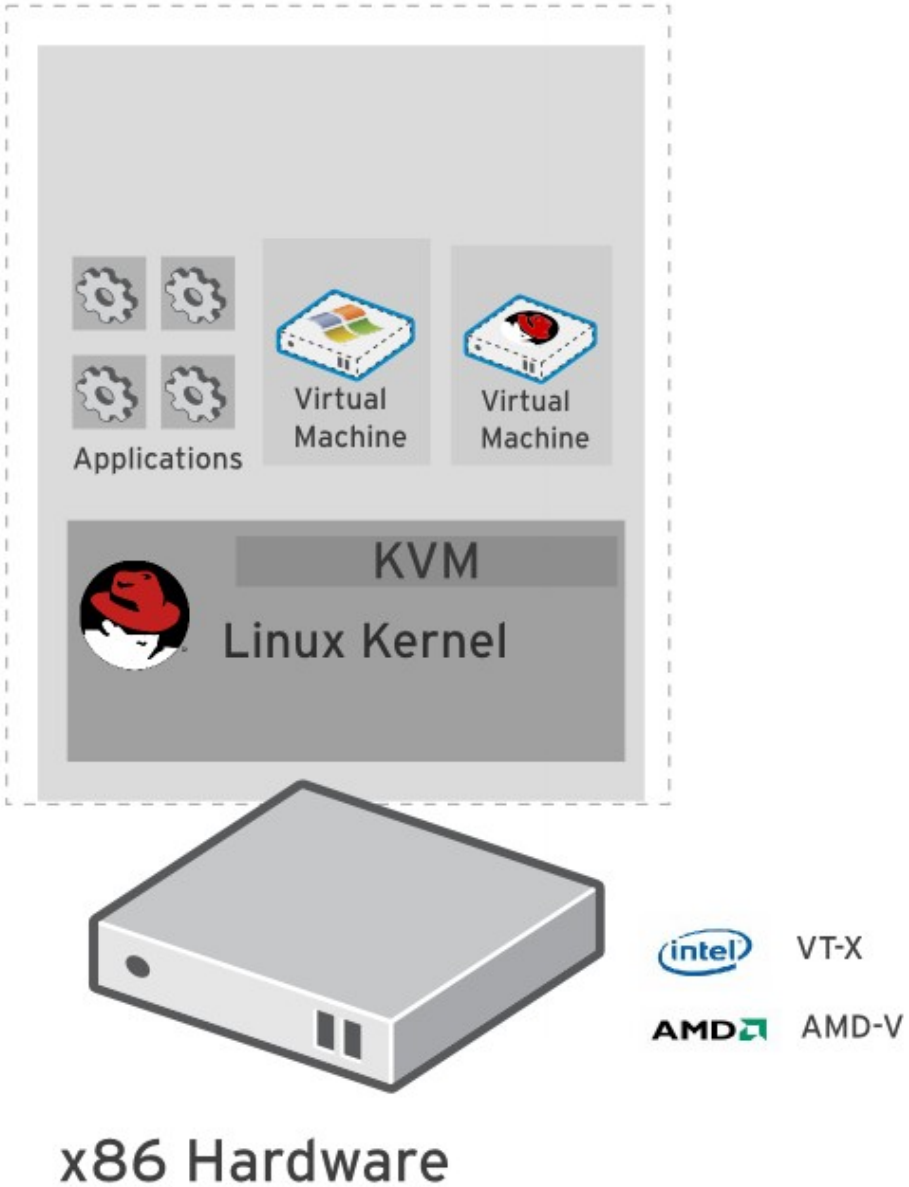
- **RHEV HYPERVISOR**
  - Small footprint, high performance dedicated hypervisor
    Available only with RHEV Manager
- **RED HAT ENTERPRISE LINUX** (with KVM)
  - High Performance, security, integrated hypervisor

RED HAT ENTERPRISE VIRTUALIZATION ARCHITECTURE



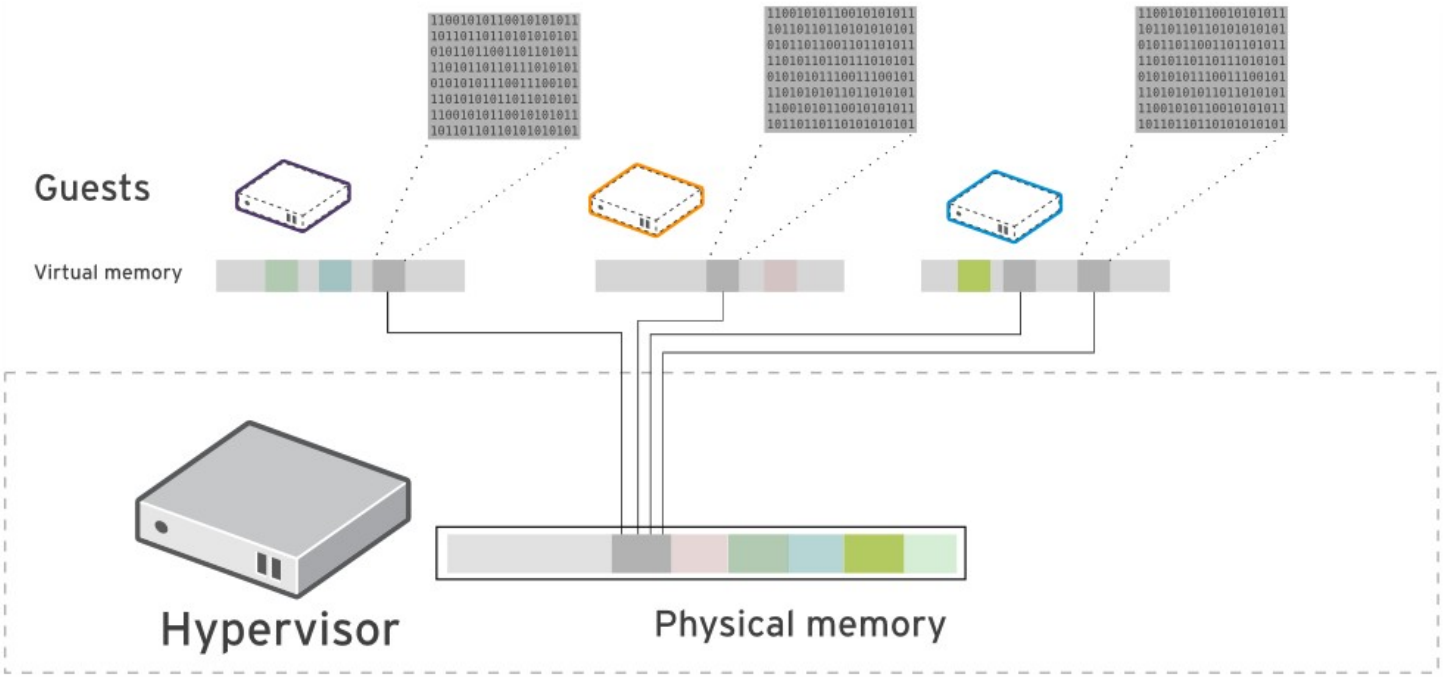
KERNEL-BASED VIRTUAL MACHINE (KVM)

- Included in Linux kernel since 2006
- Runs Linux, Windows and other operating system guests
- Advanced features
  - Live migration
  - Memory page sharing
  - Thin provisioning
  - PCI Pass-through
- KVM architecture provides high "feature-velocity" – leverages the power of Linux



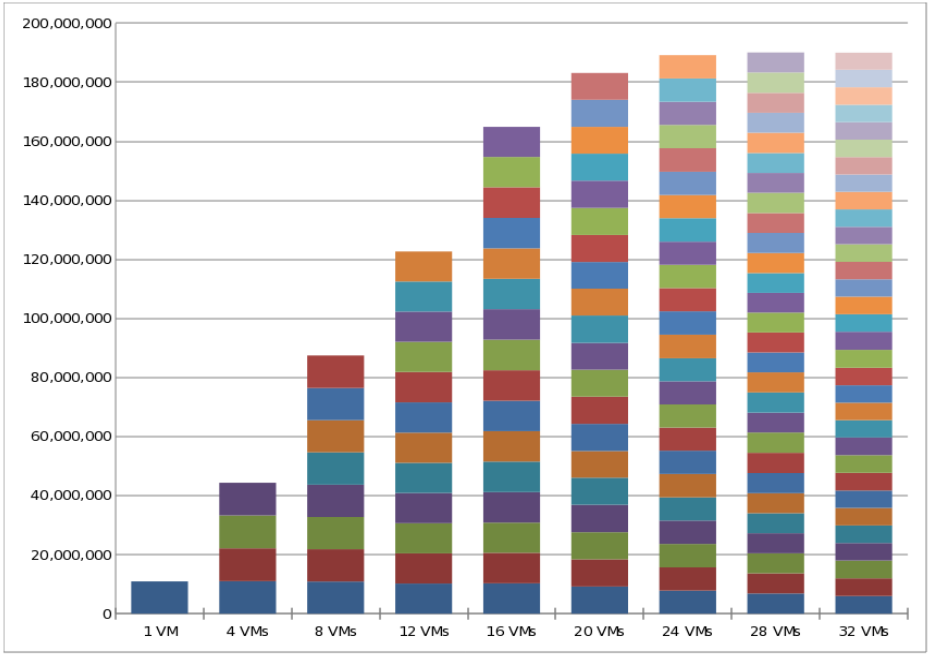
KVM HYPERVISOR – ADVANCED FEATURES

- Kernel Same-Page Merging (KSM)
  - Memory Page Sharing
  - Securely shares identical memory pages between virtual machines



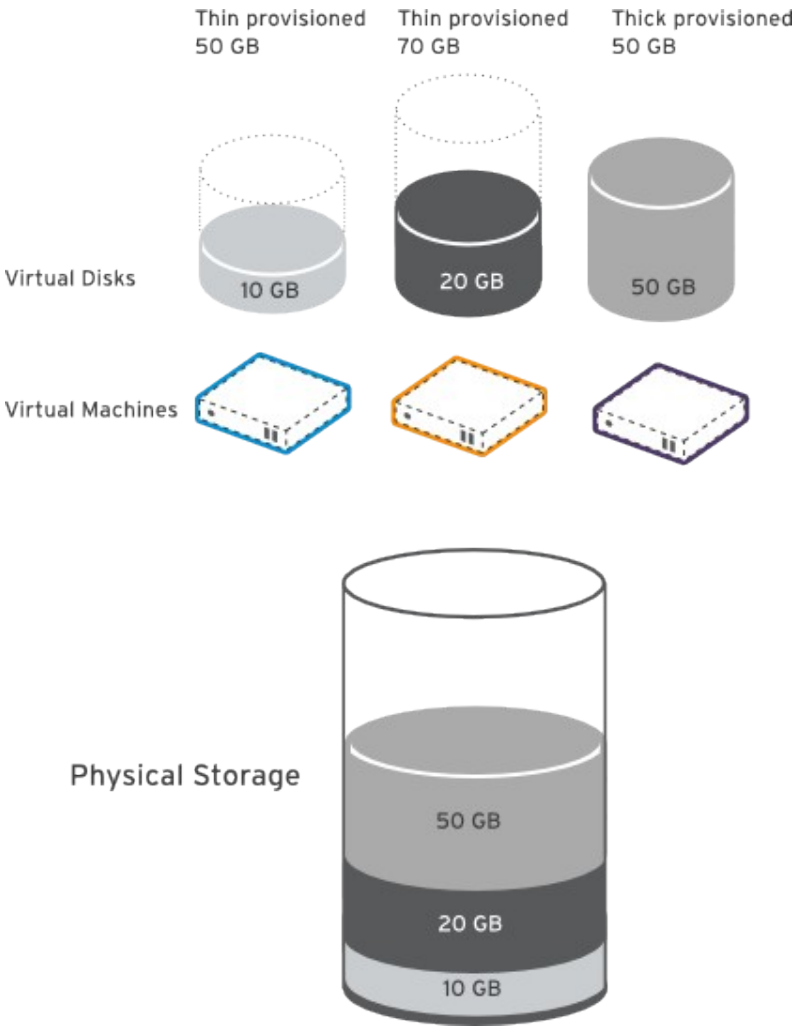
KVM HYPERVISOR – ADVANCED FEATURES

- Kernel Same-Page Merging (KSM)
  - Enterprise Java workload benchmark
  - Intel Xeon Processor X5550 with 24GB ram
  - Running multiple 3GB Windows 2003 VMs
  - Scaling up to 200% over-commit

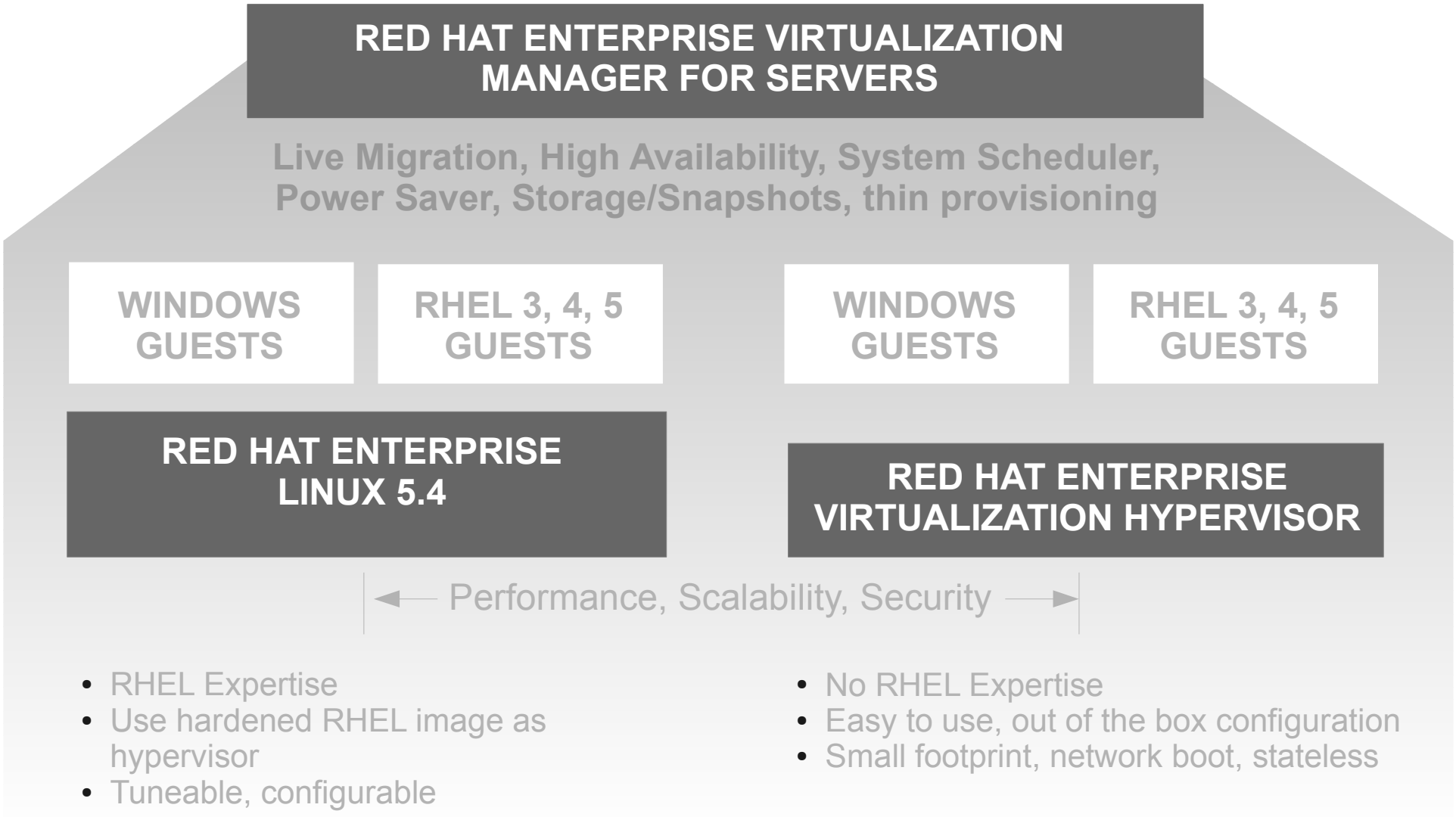


KVM HYPERVISOR – ADVANCED FEATURES

- Thin Provisioning
  - Allocate storage only when needed
  - Oversubscribe storage
  - Transparent to virtual machine
  - Improve Storage Utilization
  - Reduced Storage Costs
  - Works with NFS, iSCSI and Fiber Channel
  - Storage reporting and alerting



RED HAT ENTERPRISE VIRTUALIZATION CHOICE OF HYPERVISOR PLATFORMS



RED HAT ENTERPRISE VIRTUALIZATION
GUEST SUPPORT

- Support for Red Hat Enterprise Linux guests
  - Red Hat Enterprise Linux 3 - (32 and 64 bit)
  - Red Hat Enterprise Linux 4 - (32 and 64 bit)
  - Red Hat Enterprise Linux 5 - (32 and 64 bit)

- Para-virtualized drivers for high performance network and disk I/O
  - Uses standard VirtIO interface
    - Included as part of Linux kernels > 2.6.25
  - Backported into RHEL 4.8+ and RHEL 5.3+ kernels
  - Available as download for RHEL 3

RED HAT ENTERPRISE VIRTUALIZATION
GUEST SUPPORT & INTEROPERABILITY

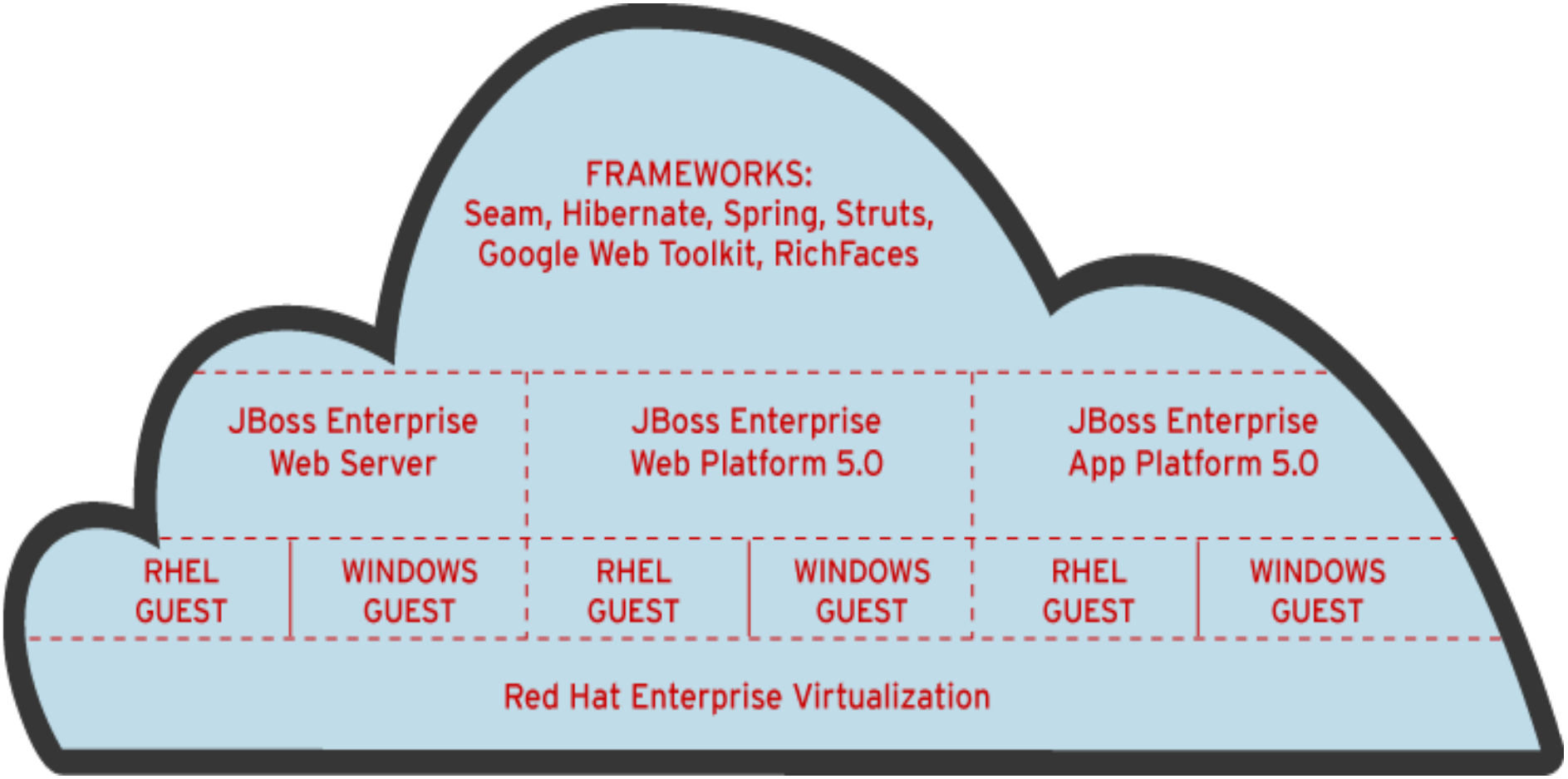
- Support for Microsoft Windows Server guests
  - Windows Server 2003 & 2003R2 - (32 and 64bit)
  - Windows Server 2008 & 2008R2 - (32 and 64 bit)
  - Server Virtualization Validation Program (SVVP) Certification from Microsoft
    - Both RHEL 5.4 and RHEV-H Certified on AMD and
    - Ensures fully supported environment
- Para-virtualized drivers for high performance network and disk I/O
  - WHQL Certified “signed” drivers
  - Included on Windows Update for seamless user experience

RED HAT ENTERPRISE VIRTUALIZATION MANAGEMENT FEATURES

Feature	Description
High Availability	Restart guest VMs from failed hosts automatically on other hosts
Live Migration	Move running VM between hosts with zero downtime
System Scheduler	Continuously load balance VMs based on resource usage/policies
Power Saver	Concentrate virtual machines on fewer servers during off-peak hours
Maintenance Manager	No downtime for virtual machines during planned maintenance windows
Image Management	Template based provisioning, thin provisioning and snapshots
Monitoring and Reporting	For all objects in system – VM guests, hosts, networking, storage etc.

Gippa's vision of Cloud Security

How a Cloud stack is (vendors/labels apart)



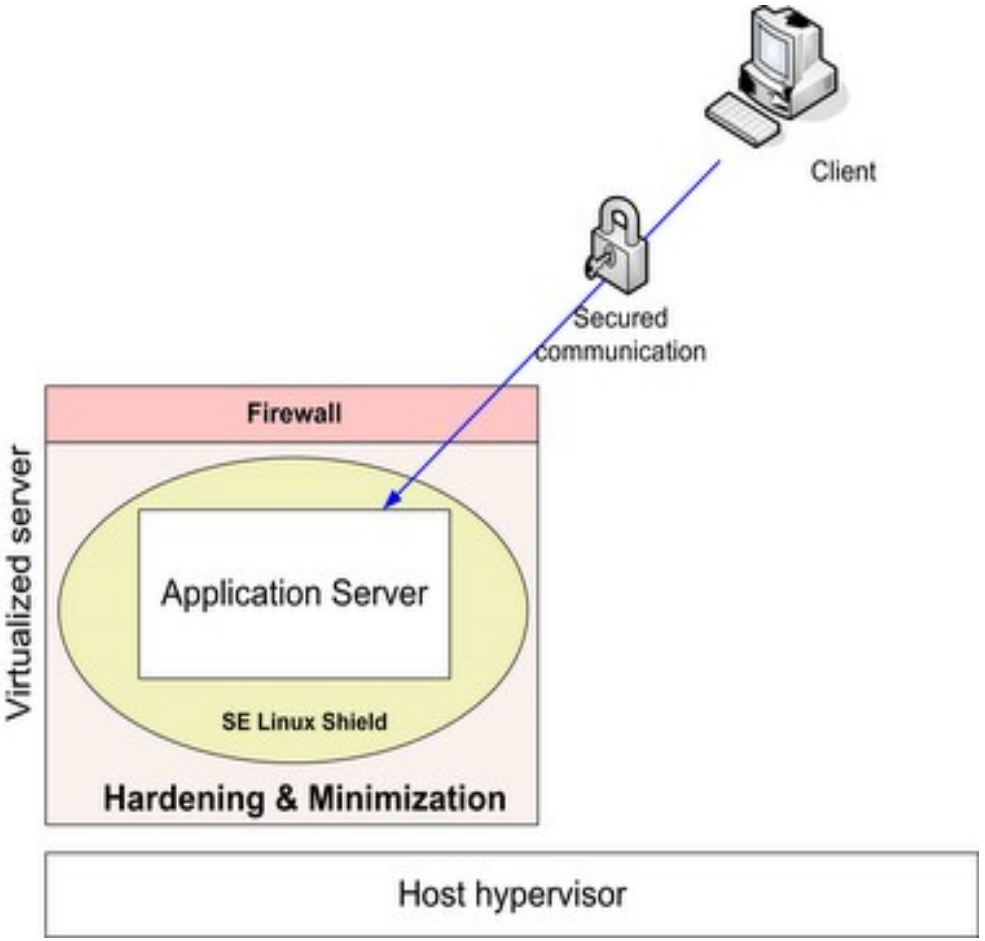
Issues on security in a Cloud

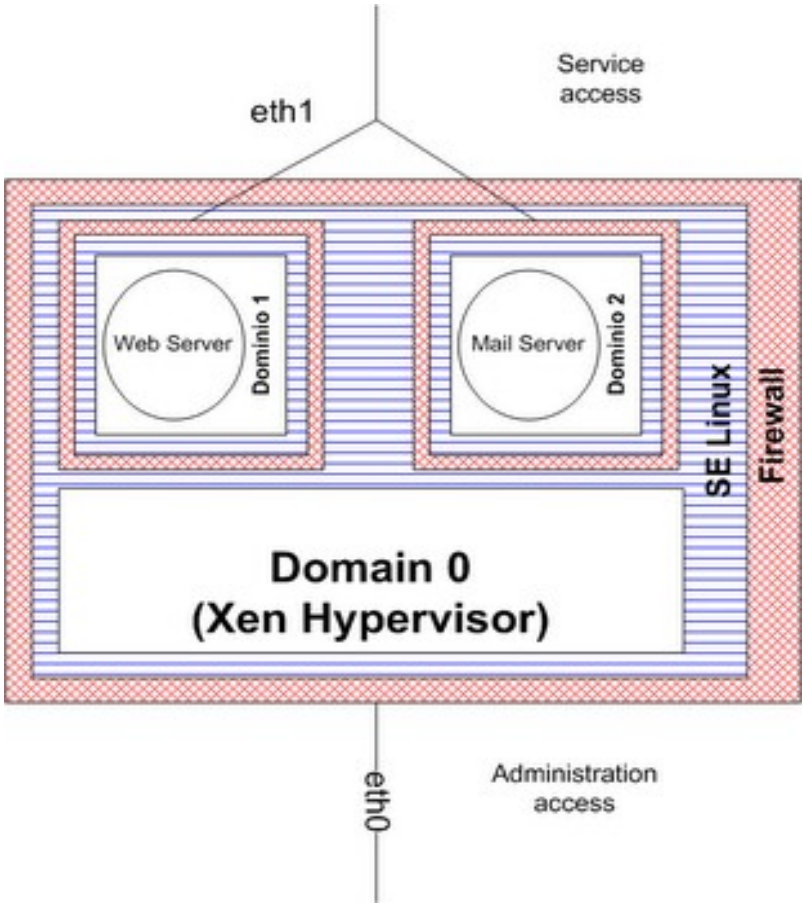
Not any different from a Service Oriented Architecture, but more dynamic. What are the aspects on security in a cloud?

- Hypervisor isolation
- Operating System security
- Network segregation and encryption
- Data encryption and isolation
- Strong authentication and authorization
- J2EE container protection
- Web content protection (XSS, javascript/AJAX, etc...)
- Secure Web Services
- Database hardening and content encryption
- .... and a lot more!

Too much for a presentation, let's talk about hypervisor protection and isolation.

How's Defense in Depth in a Cloud





KVM HYPERVISOR – ADVANCED FEATURES

- Security: inherits security features of Linux
- Includes support for SELinux
  - Provides protection and isolation for virtual machines and host
  - Compromised virtual machine cannot access other VMs or host
- sVirt Project
  - Sub-project of NSA's SELinux community
  - Provides “hardened” hypervisors
  - Contain any hypervisor breaches
  - Will be included in RHEL 6

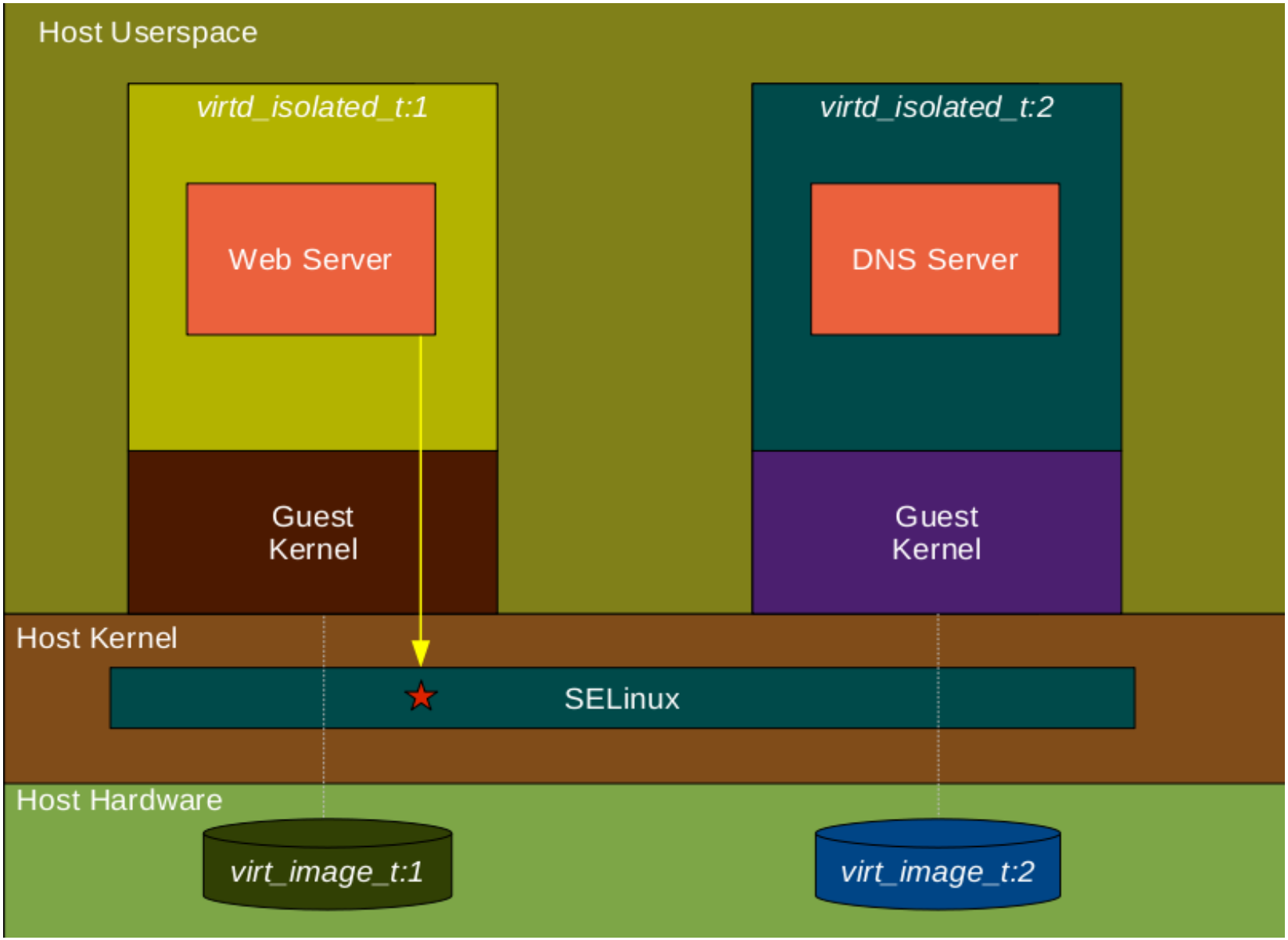
MAC and SE Linux

- Mandatory Access Control (MAC) is a kind of access control defined by the Trusted Computer System Evaluation Criteria
  - “[...] restricting access to objects based on the sensitivity of the information contained in the objects and the formal authorization (i.e., clearance) of subjects to access information of such sensitivity". (from Wikipedia)
- The most used MAC system in Linux is Security Enhanced Linux (SE Linux)
  - Developed initially by NSA (National Security Agency)
  - Several contributors, such as Red Hat, Tresys, IBM, ...
  - Certified Common Criteria (EaL4+) and used by military
    - When used in “stricted” mode is even more secure
  - Based on policies that confine user programs and system services to the minimum amount of privilege they require to do their jobs

sVirt Project

- MAC in process-based virtualization (KVM, OpenVZ, etc...)
  - Isolate guests using MAC security policy
  - Contain hypervisor breaches
  - Supports MAC security schemes (SELinux, SMACK)
- Provides:
  - Strong isolation between active VMs
  - Improved control over access to VM resources
  - Improved control over access to shared resources
  - Fine-grained interaction with the host
  - MAC containment of Vms
  - Interface with label networking/CIPSO
- Heavy usage of the MCS framework:
  - system_u:object_r:virt_image_t:c<UUID>

sVirt, the big picture



Check out document

“Virtualizzazione e Sicurezza” on

http://www.gpaterno.com/pubblicazioni/

(available in italian)

Q&A
Thank you!

Giuseppe “Gippa” Paterno'
Solution Architect
gpaterno@redhat.com