Red Hat Technology & Roadmap

Introduction

- **Lynne Corddry (lcorddy@redhat.com)**
  Vice President, Business Development

- **Tim Demski (tdemksi@redhat.com)**
  Director, Business Development

- **Shawn Wells (swells@redhat.com)**
  Government Solutions Architect

Agenda

- Red Hat Enterprise Linux Update
- SOA Direction / Application Stack
- Future Direction (Emerging Technologies)
- Summary & Close

Red Hat, Inc

- Headquarters: Raleigh, NC
- Founded 1993
- Public 1999 (NYSE: RHT)
- Operating in 27 countries
- Over 2800 Employees worldwide
- Over 50% are engineers
- $1.3B cash reserves
- $400M FY07 Revenue

58 OFFICES IN 26 COUNTRIES

NORTH AMERICA

Toronto
Atlanta
Austin
Chicago
Dallas
Denver
Hunstville
Minneapolis
Marlton
Mountain View
New York
Raleigh
St Louis
Tullahoma
Tysons Corner
Westford

LATIN AMERICA

Buenos Aires
São Paulo
Mexico City

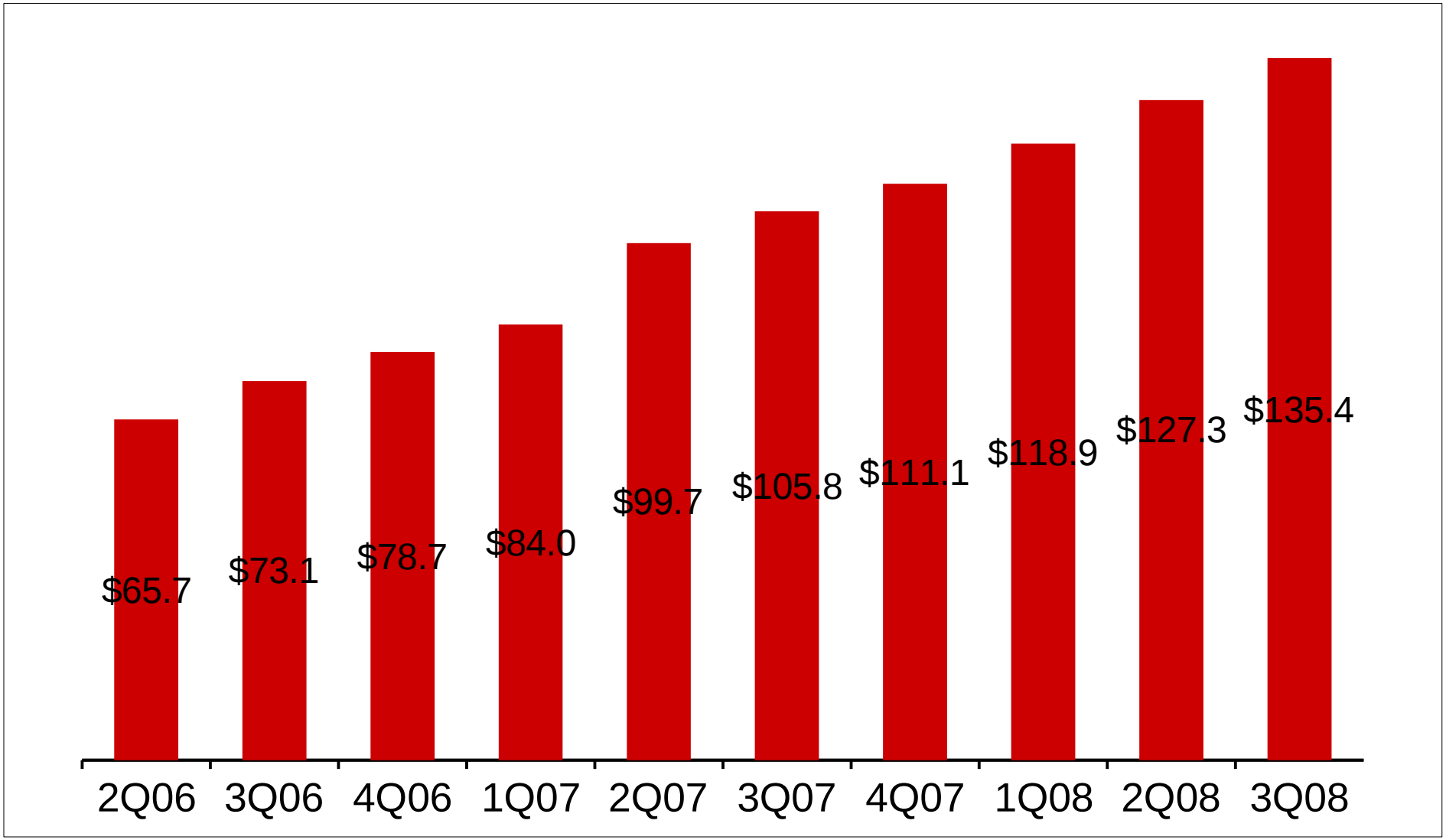
EUROPE, MIDDLE EAST, AFRICA

Turnhout
Brno
Helsinki
Nanterre
Berlin
Frankfurt
Munich
Stuttgart
Cork
Milan
Amersfoort
Madrid
Stockholm
Neuchâtel
Cambridge
Farnborough
London
Newcastle

ASIA PACIFIC

Brisbane
Melbourne
Sydney
Beijing
Guangzhou
Shanghai
Shenzhen
Hong Kong
Bangalore
Chennai
Kolkata
Mumbai
New Delhi
Pune
Tokyo
Seoul
Kuala Lumpur
Singapore
Sri Lanka

Quarterly Revenue



In millions

Red Hat & LMCO

- Master Partner Agreement At IS&GS Level
- Major participant in LMCO labs (NEXGEN, LIGHTHOUSE)
- Web Services Factory
- Partner on major programs
  - NGA GEOSCOUT
  - NASA ORION
  - Air Force TMOS and GCSS
  - NAVY Q70
  - ARMY WIN-T
  - FBI NGEN

#1 IN VALUE. #1 AGAIN.

CIO INSIGHT

#1 FOUR YEARS RUNNING IN ENTERPRISE SOFTWARE

#1 MEETING COMMITMENTS ON TIME AND ON BUDGET

97% said they would buy FROM RED HAT AGAIN.

#1 OVERALL IN 3 OF THE LAST 4 YEARS

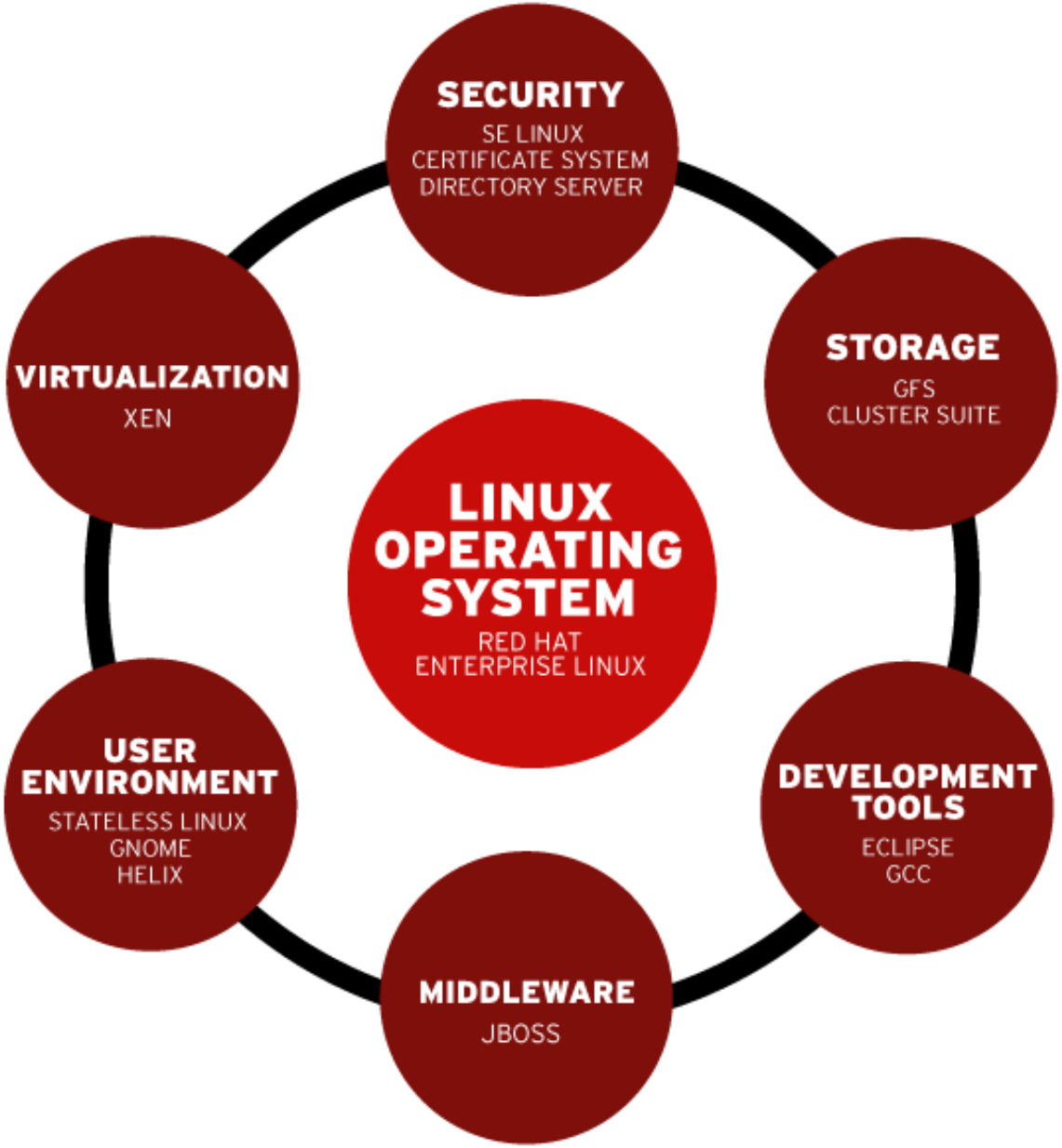
#1 MEETING EXPECTATIONS FOR LOWERING COST

TOP 10 FOR ENTERPRISE SOFTWARE 2007

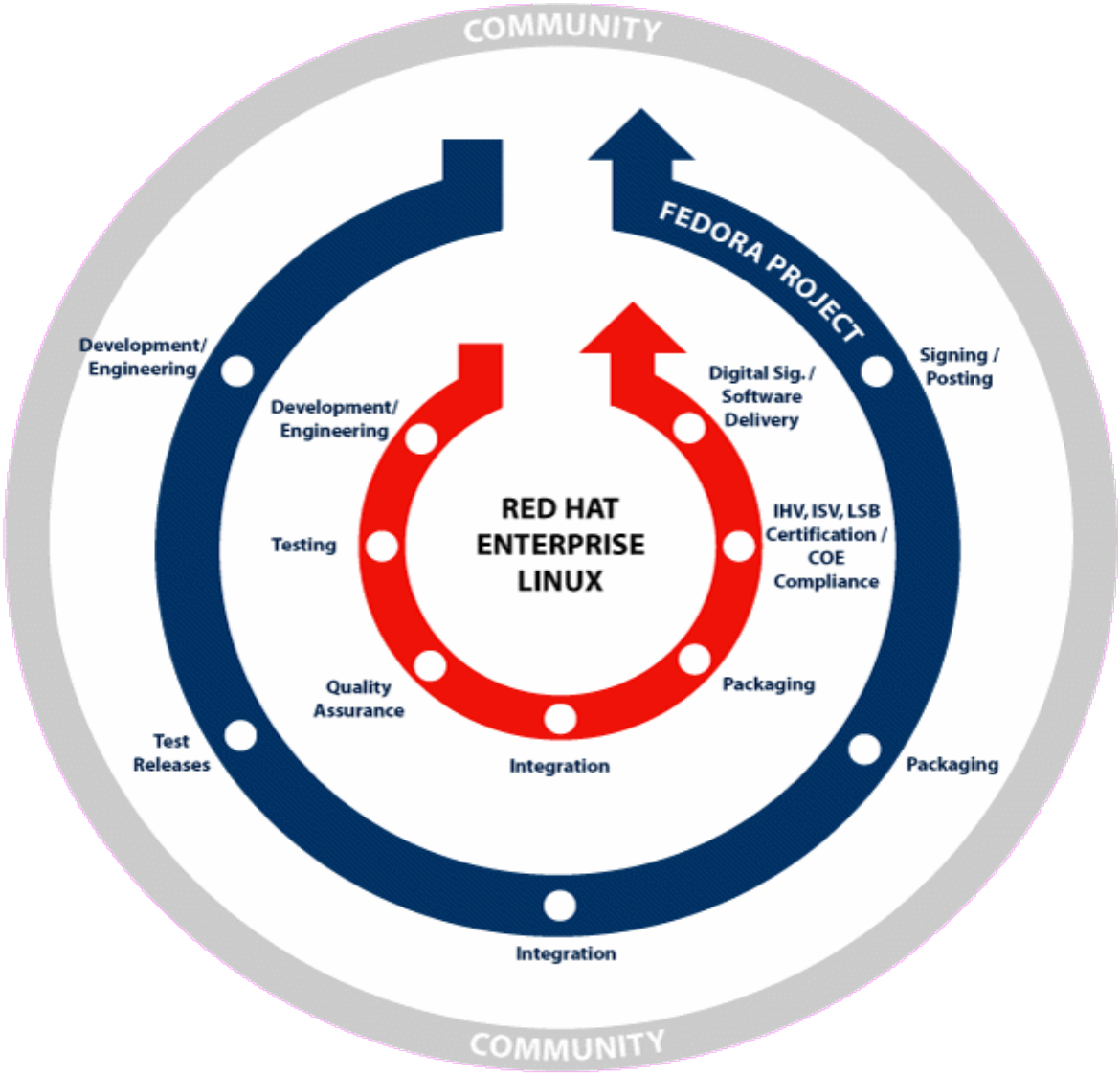
RANK 07	RANK 06	RANK 05	VENDOR	OVERALL 07	VALUE	RELIABILITY	WOULD CONTINUE TO DO BUSINESS (%YES)
1	**1**	**1**	**RED HAT**	**80%**	**80%**	**80%**	**97%**
2	2	2	Citrix Systems	76%	76%	76%	93%
3	-	-	Adobe	73%	71%	76%	91%
4	7	6	SAP	64%	66%	62%	89%
5	6	7	Microsoft	62%	62%	61%	84%
6	8	3	Business Objects	61%	60%	62%	83%
7	5	5	Novell	60%	60%	60%	70%
8	8	10	Oracle *(Including Hyperion)*	58%	57%	59%	79%
9	11	9	CA	52%	51%	54%	68%
10	10	8	Cognos	51%	50%	52%	80%

Visit http://www.redhat.com/promo/vendor for more information

- BEA WebLogic
- Veritas
- VMWare
- EMC Powerpath
- SUN Solaris



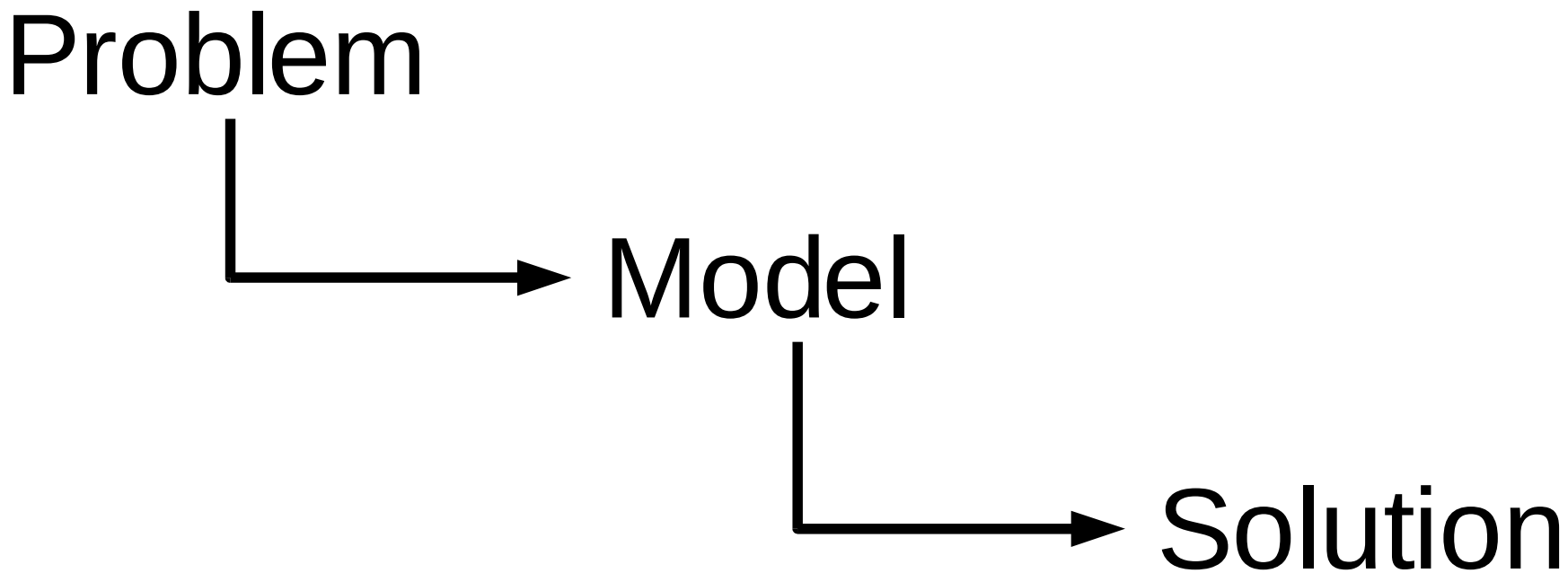
Red Hat Development Model



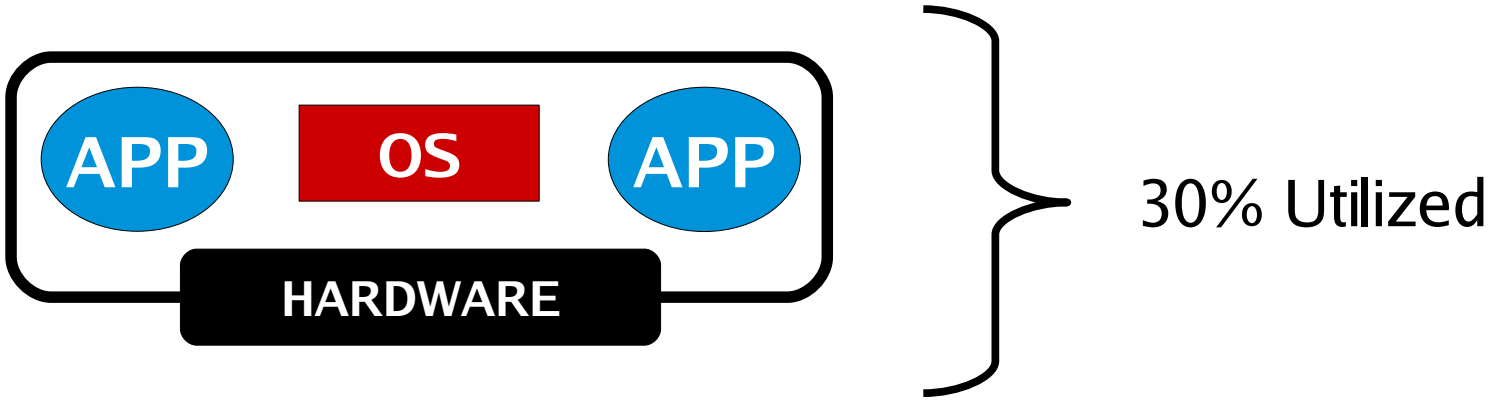
Red Hat Enterprise Linux Update

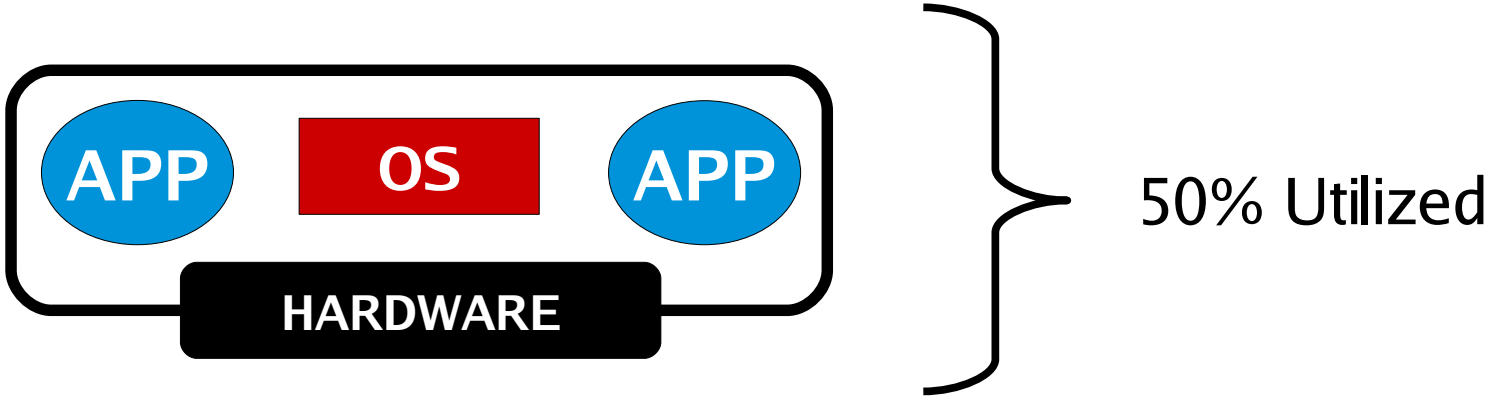
Virtualization

Virtualization

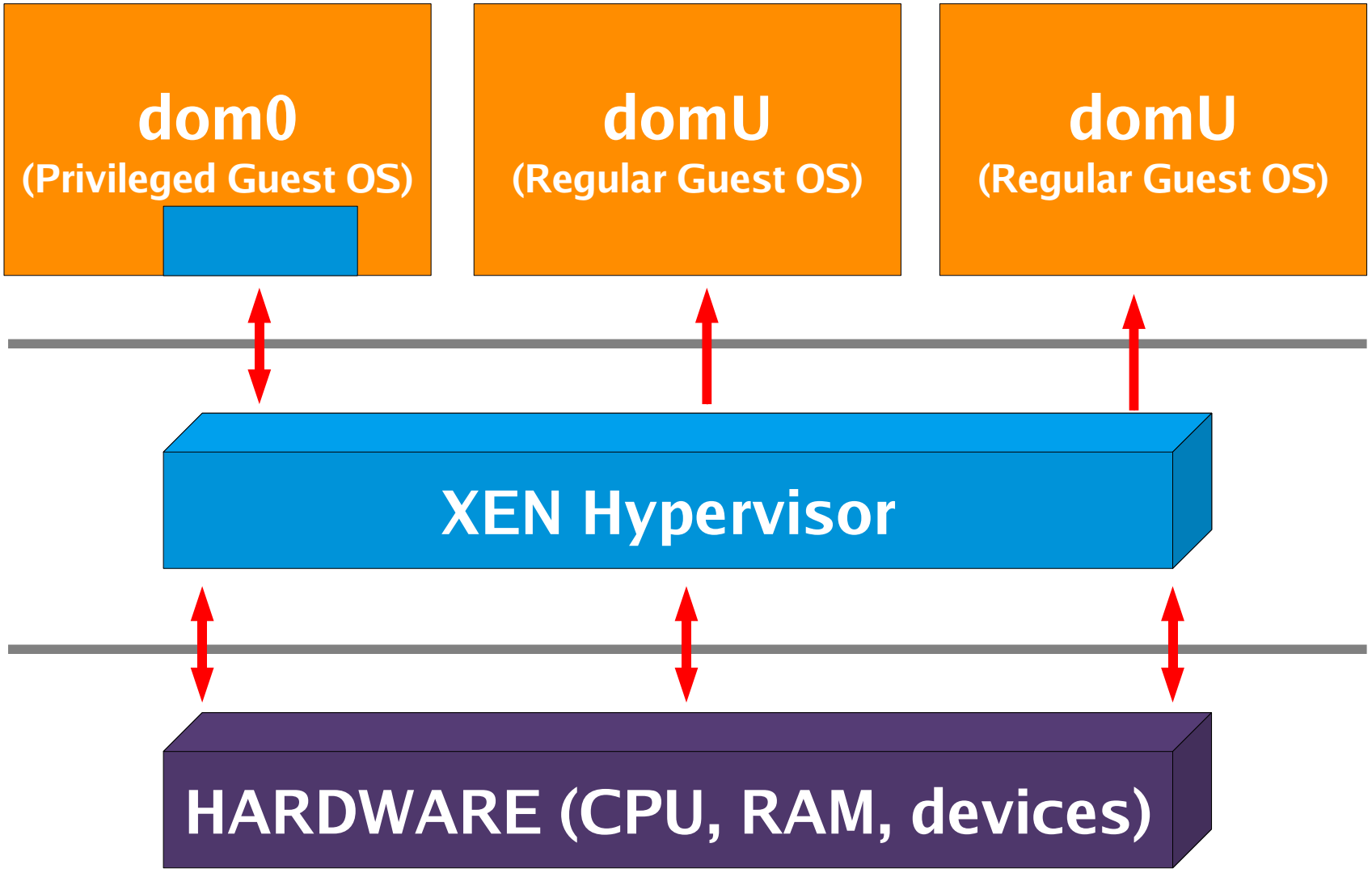


Virtualization: Define the Problem





Virtualization: Modeling the Problem via Xen



The Xen Hypervisor

Advantages

- Flexible IT Services
- Disaster Tolerance
- Life Cycle Management
- Live Migration

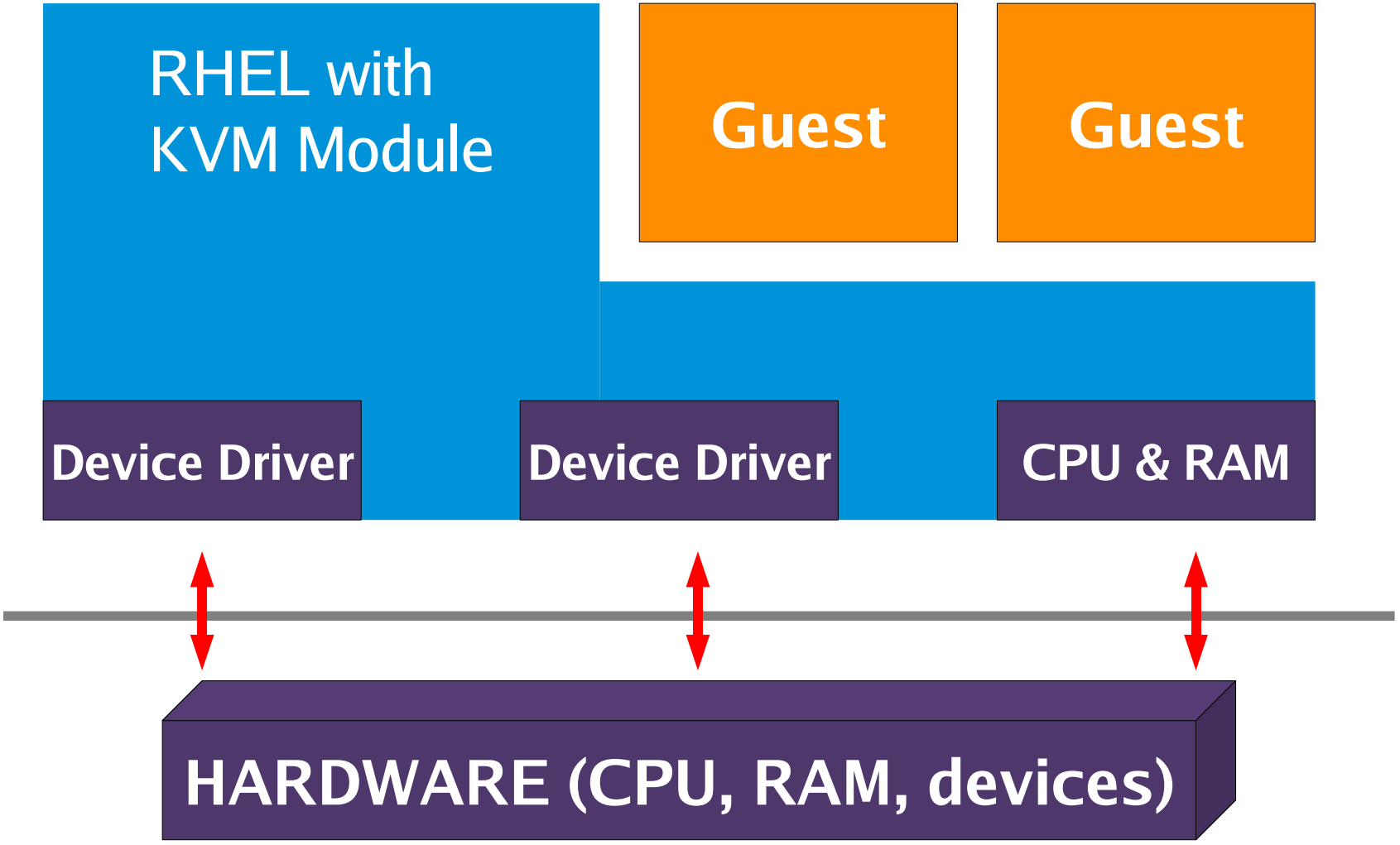
Disadvantages

- Power Management
- 2x Privileged Entities

Options

- Fully Virtualized
- Para Virtualized

Virtualization: Modeling the Problem via KVM



The Xen Hypervisor

Advantages

- 80-100% Native Performance
- Specjbb2005: 95-100% Native Performance
- Stable

Disadvantages

- Power Management
- 2x Privileged Entities

Options

- Fully Virtualized
- Para Virtualized

The KVM Hypervisor

Advantages

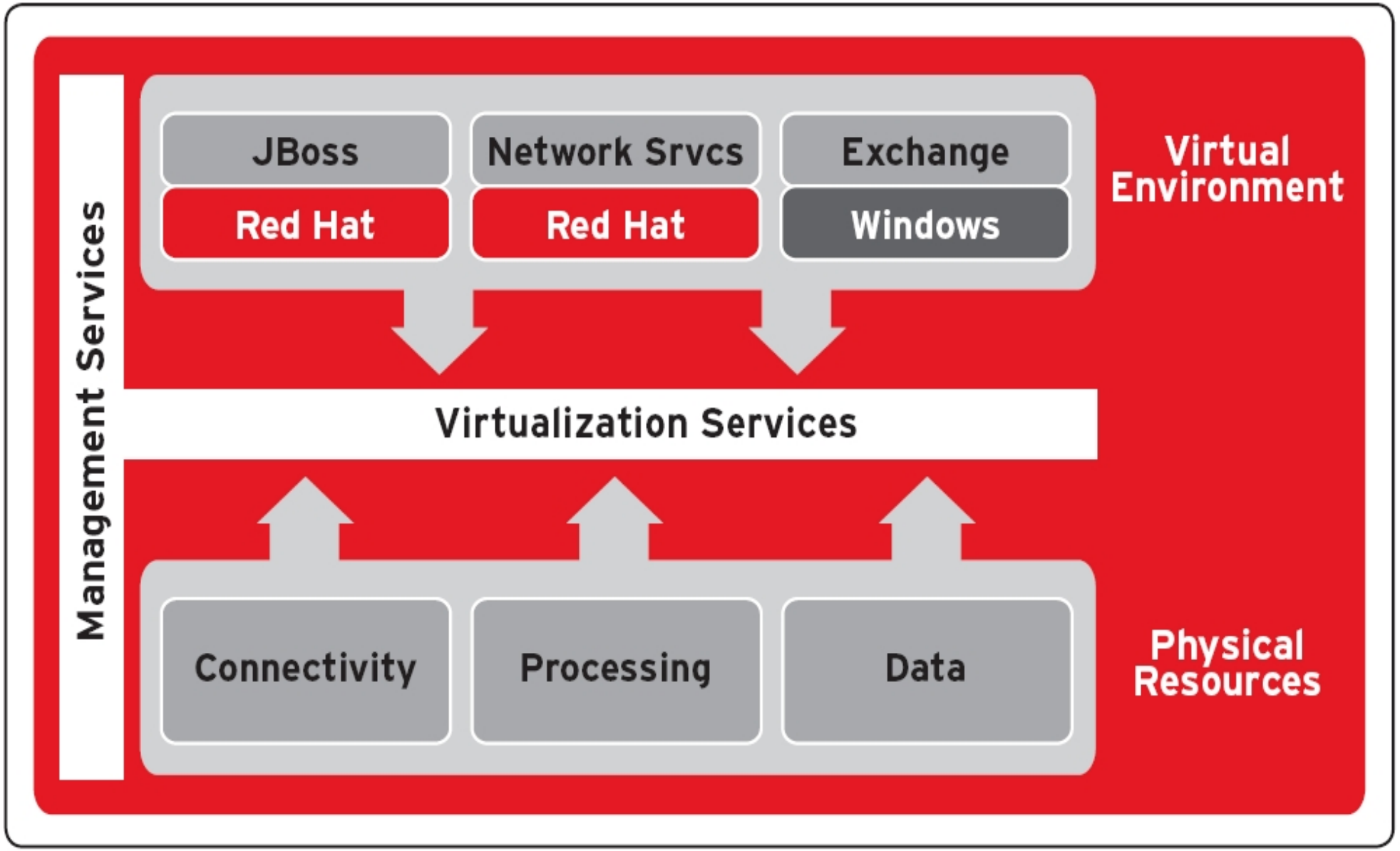
- One Privileged Entity
- All Advantages of RHEL
- KVM in Upstream Kernel

Disadvantages

- Not production worthy, target RHEL6
- CPU Intensive, 50-100%

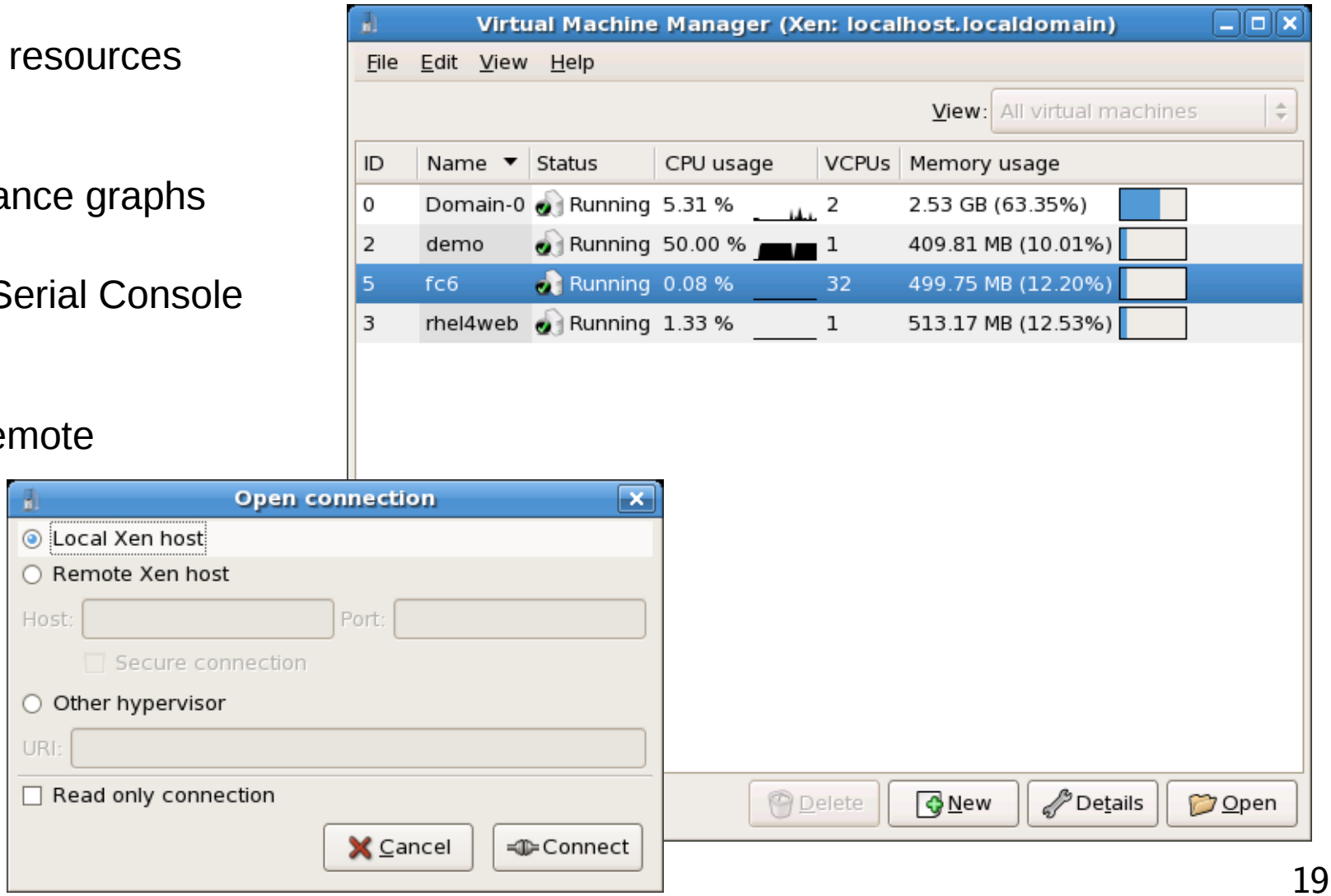
Future

- Xen guests compatible with KVM


Management Services
JBoss
Red Hat
Network Srvcs
Red Hat
Exchange
Windows
Virtual Environment
Virtualization Services
Connectivity
Processing
Data
Physical Resources

Introduction to virt-manager

- Graphical virtual guest management
- Add/Remove resources dynamically
- Live performance graphs
- Graphical & Serial Console Emulation
- Connect to remote hosts

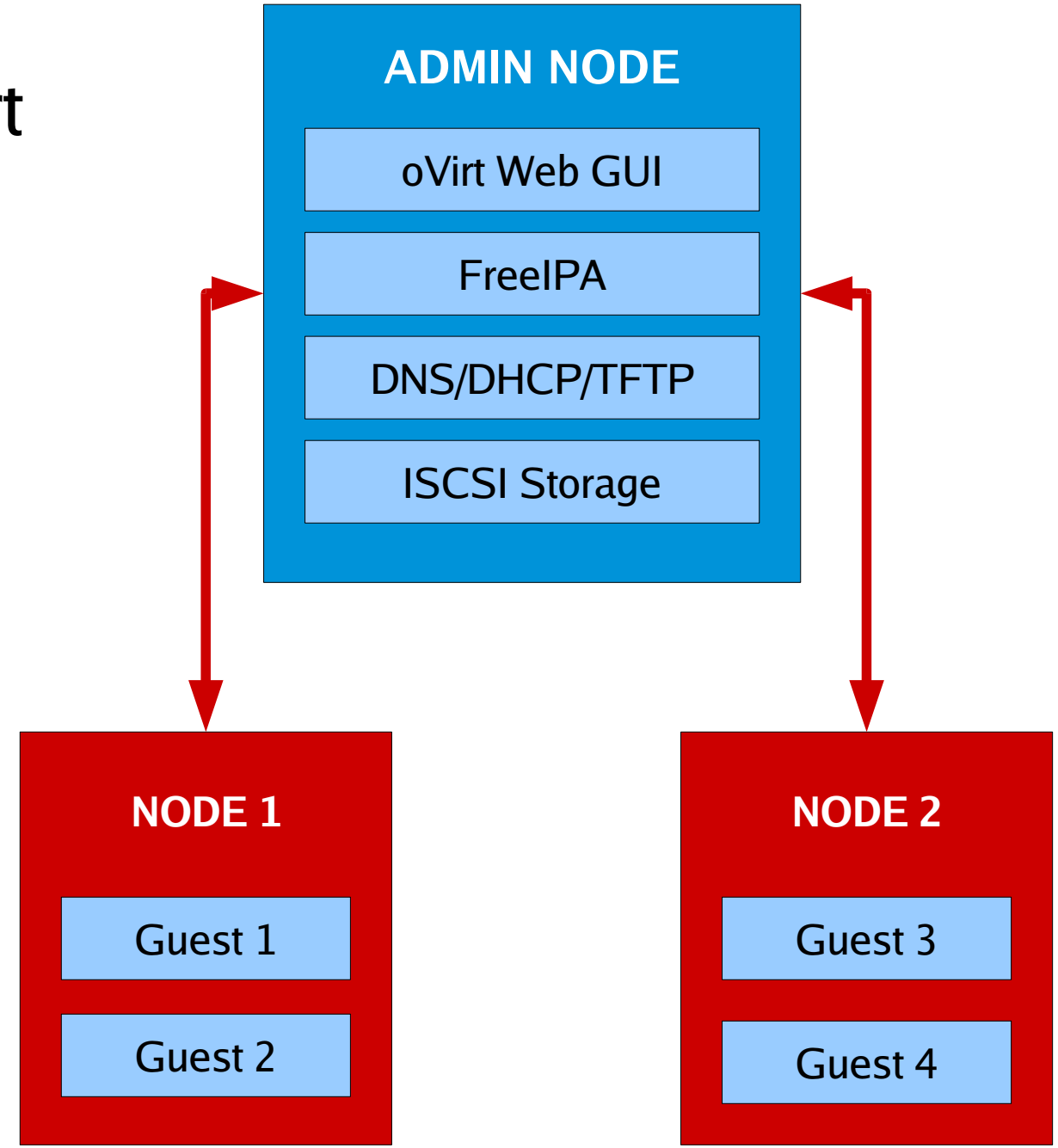


Introduction to libvirt API

- Hypervisor agnostic
- Stable API for tool/app development
  - CIM providers; Python, C bindings, scriptable
- Allows authenticated/encrypted sessions to remote hypervisors
- Current support for
  - Xen Hypervisor
  - KVM Hypervisor
  - QEMU Hypervisor

Introduction to oVirt

- Currently ***in development***
- Utilizes libvirt
- Web-Based GUI
- Automate clustering, load balancing, and SLA maintenance
- Designed for enterprise management
- Built on Ruby on Rails
- Performance tools built-in



Red Hat Enterprise Linux Update

Security

Open Source as a Security Innovation

1. More eyes on the code, therefore less security bugs

Bugs per 1000 Lines of Code		
Linux 2.6 Kernel	0.17	Stanford University/Cover
Proprietary Software	10 to 20	Carnegie Mellon Cylab

Wired Magazine, Dec 2004

2. Red Hat's rapid response to any vulnerabilities

Time from a critical issue being known to the public until the day that a fix is available via RHN
Red Hat Enterprise Linux 4, Feb 2005-Feb 2006

Red Hat Security Certifications

- **NIAP/Common Criteria: The most evaluated operating system platform**
  - Red Hat Enterprise Linux 2.1 – EAL 2 (Completed: February 2004)
  - Red Hat Enterprise Linux 3 EAL 3+/CAPP (Completed: August 2004)
  - Red Hat Enterprise Linux 4 EAL 4+/CAPP (Completed: February 2006)
  - Red Hat Enterprise Linux 5 EAL4+/CAPP/LSPP/RBAC (Completed: June 2007)

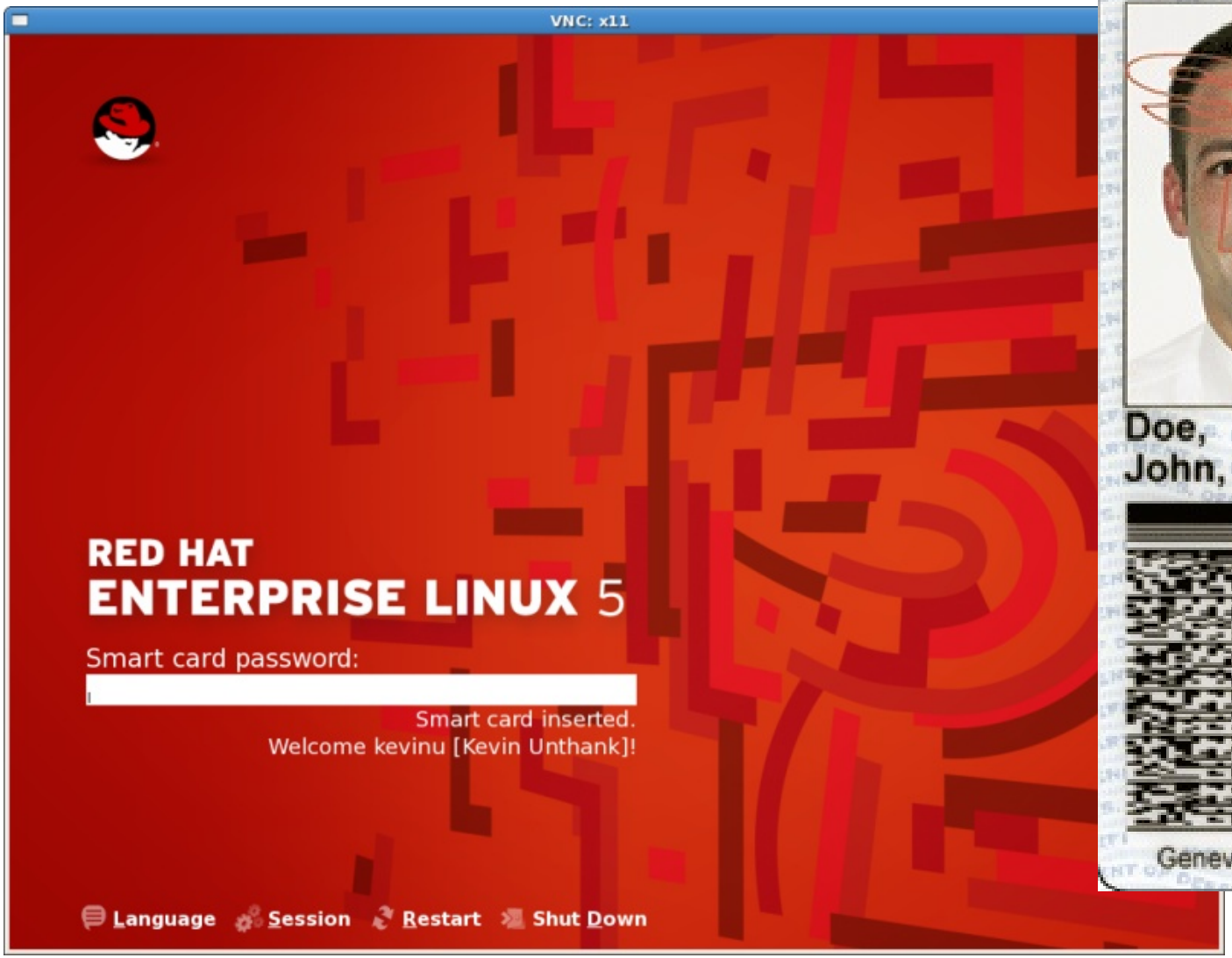
- **DII-COE**
  - Red Hat Enterprise Linux 3 (Self-Certification Completed: October 2004)
  - Red Hat Enterprise Linux: First Linux platform certified by DISA

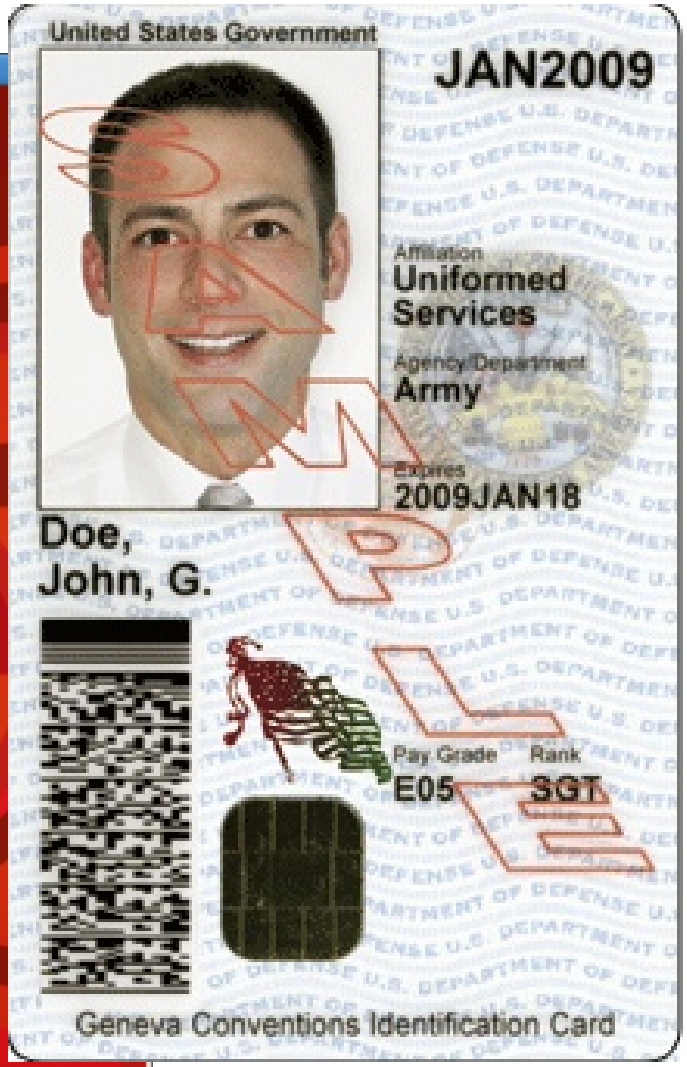
- **DCID 6/3**
  - Currently PL3/PL4: ask about kickstarts.
  - Often a component in PL5 systems

- **DISA SRRs / STIGs**
  - **Ask about kickstarts**

- **FIPS 140-2**
  - Red Hat / NSS Cryptography Libraries certified Level 2

RHEL5 Security: DoD Access Cards

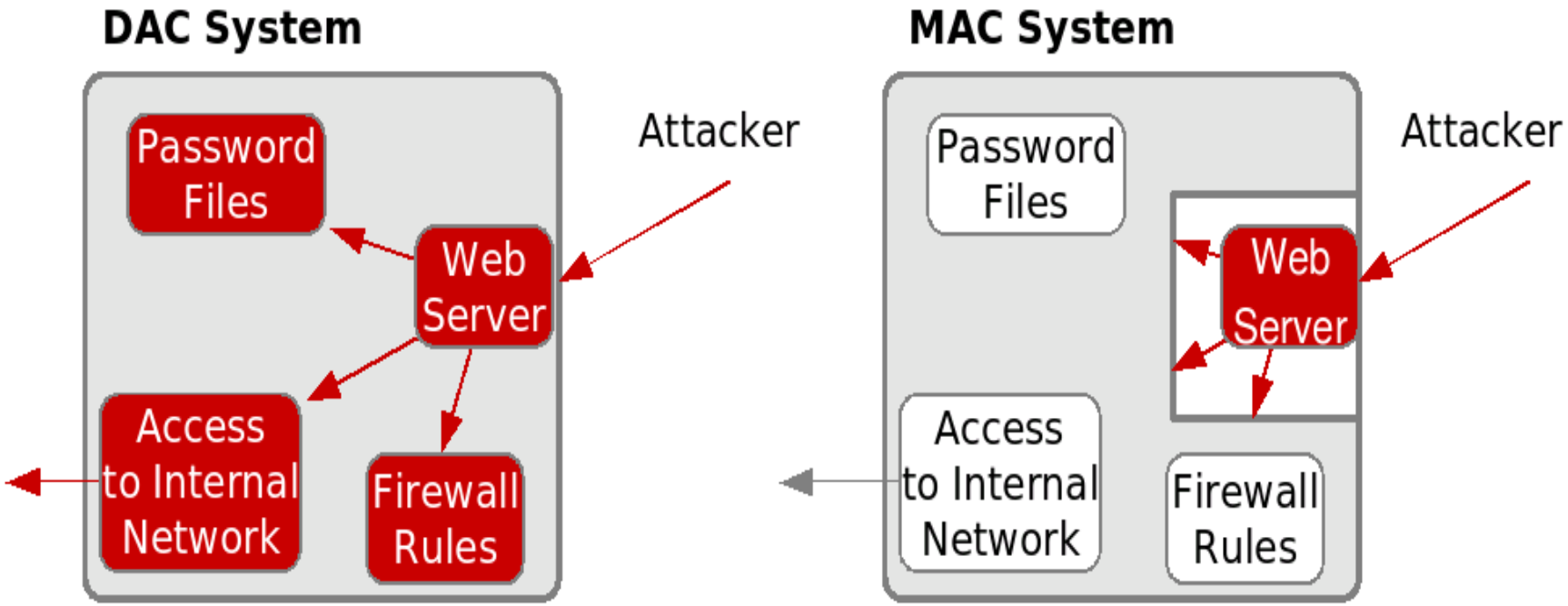




RHEL5 Security: NIST Standards Work

- Extensible Configuration Checklist Description Format (XCCDF)
  - Enumeration for configuration requirements
  - DISA FSO committed to deploying STIG as XCCDF
  - Others working with NIST
  - Security policy becomes one file

RHEL5 Security: Basics of SELinux



RHEL5 Security: SELinux Policies

- Targeted Policy (Default)
  - Applications run unconfined unless explicitly defined policy exists
- Strict Policy
  - All application actions explicitly allowed through SELinux, else actions denied
- MLS
  - Polyinstantiated file systems
  - Allows for different “views” based on clearance level

RHEL5 SELinux Enhancements

- **Expanded SELinux targeted policy coverage**
  - Provides coverage for all core system services, versus 11 in Red Hat Enterprise Linux 4
  - Includes support for Multi Level Security (MLS) enforcement model
    - In addition to existing RBAC and TE models
- **An additional level of protection against security exploits**
  - Fine-grained policies via kernel-enforced mandatory access controls
  - Limits the scope of security vulnerabilities
  - Beyond what any other general-purpose OS can deliver

RHEL5 SELinux Enhancements

- **ExecShield**
  This enhancement can prevent any memory that was writable from becoming executable. This prevents an attacker from writing his code into memory and then executing it

- **Stack Smashing protection (Canary values)**
  The system will place a canary value at a randomized point above the stack. This canary value is verified during normal operation. If the stack has been smashed, the canary value will have been overwritten, indicating that the stack has been smashed. This is a method to detect buffer overflows early.

- **FORTIFY_SOURCE GCC option**
  When the compiler knows the size of a buffer, functions operate on the buffer to make sure it will not overflow at runtime. This works to help catch format string flaws as well as buffer overflows.

RHEL5 SELinux Enhancements

Loadable Policy Modules

- In the past, all policy changes had to be made to the policy source
  - Required the entire policy re-compiled
  - Requiring a full set of policy development tools on production systems.

- Modules allow for the creation of self-contained policy modules
  - Safely linked together to create system policies
  - Add policy on the fly
  - Remove policy on the fly

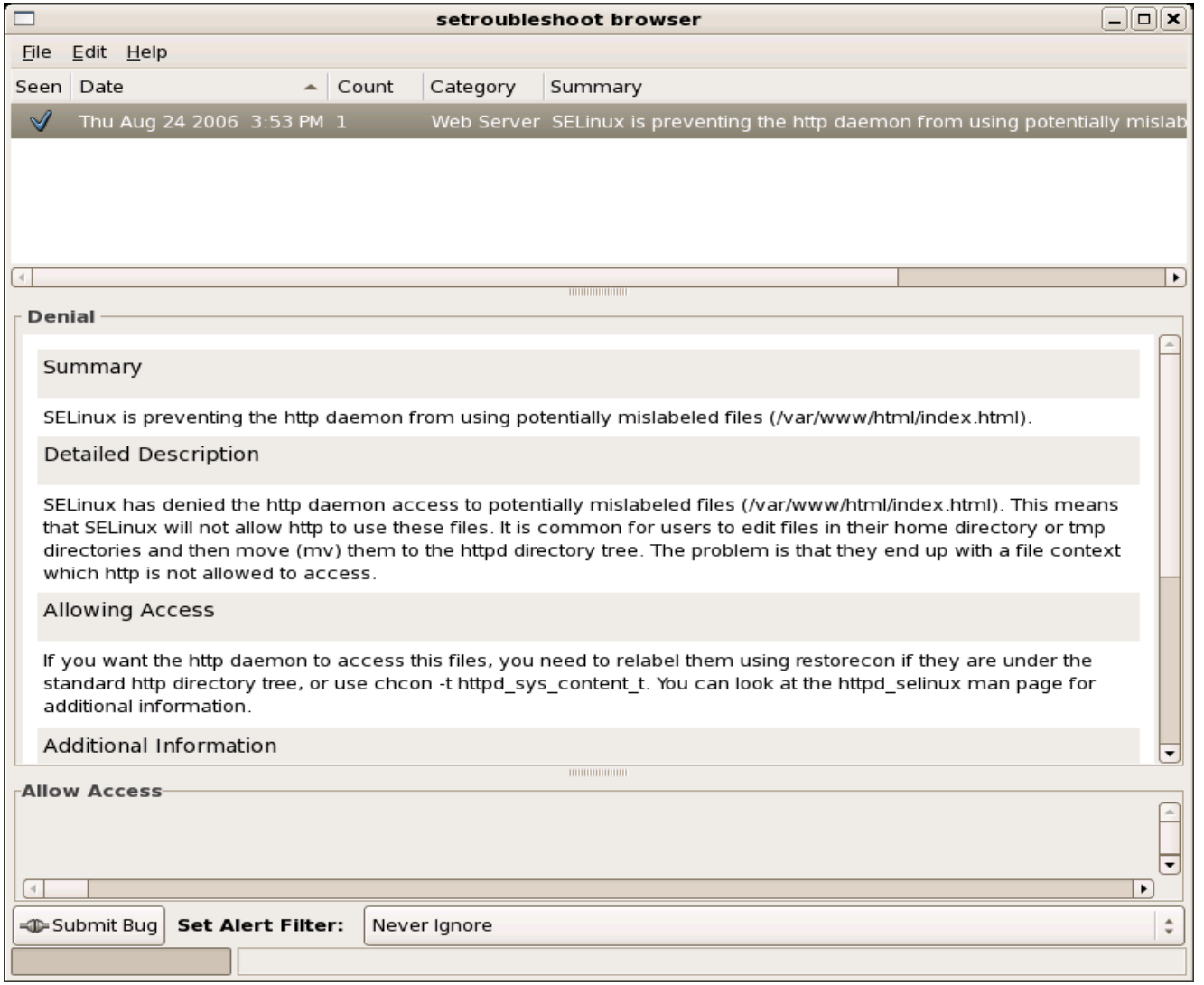
- Framework to allow ISV/OEM partners to ship their own modular SELinux policy

Further Information

- http://sepolicy-server.sourceforge.net/index.php?page=module-overview

RHEL5 SELinux Enhancements

- New troubleshooting tool provides clear, easy-to-understand, GUI-based, security violation notifications
- Over 60 events defined today

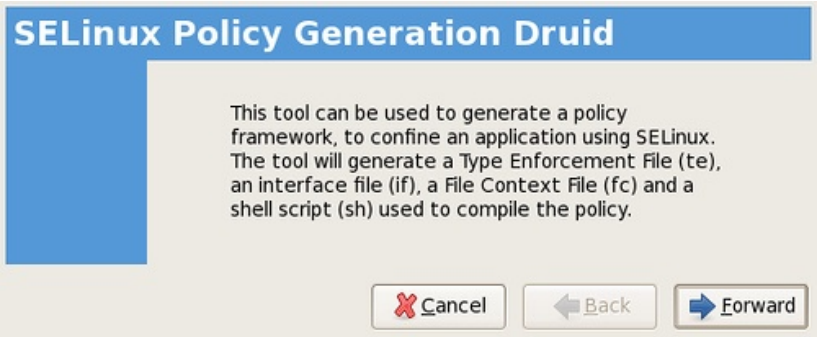


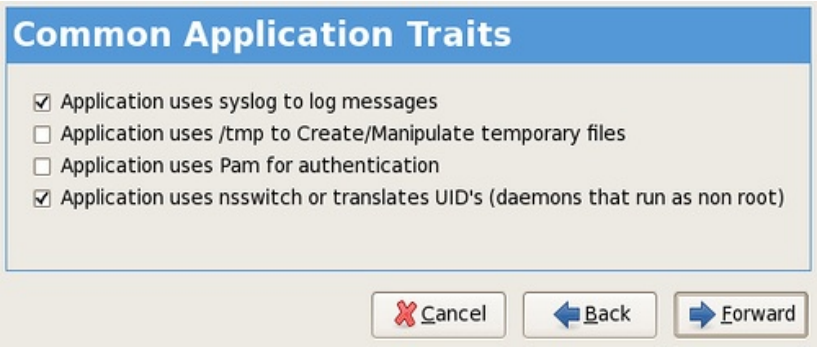
RHEL5 SELinux Enhancements

Policy creation now a two-step process

1) system-config-selinux
   - Creates template policy (network, filesystem read/write, etc)

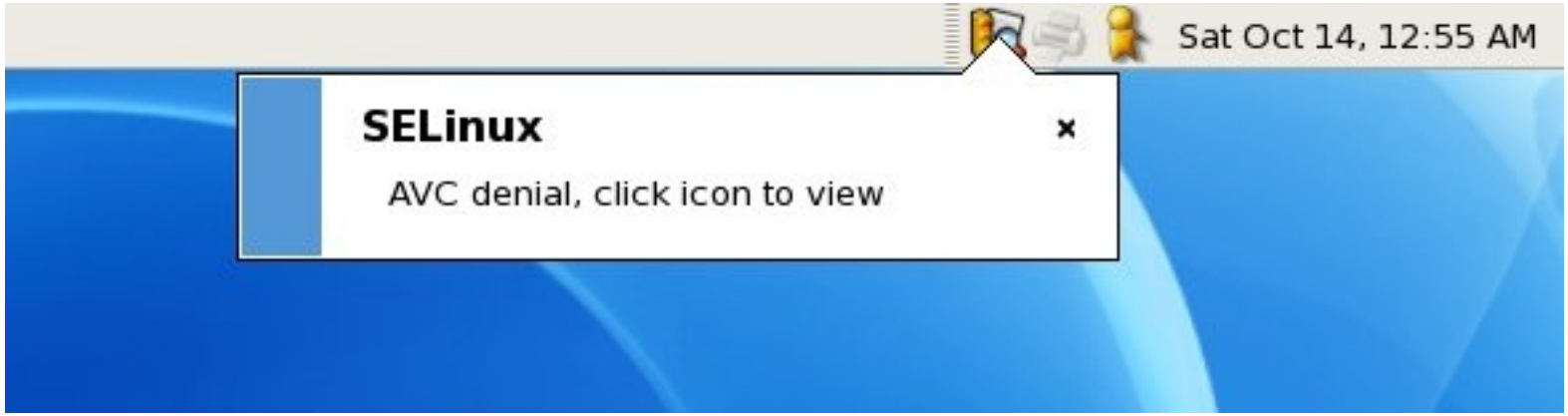
2) audit2allow
   - Traces application, ensuring proper accesses





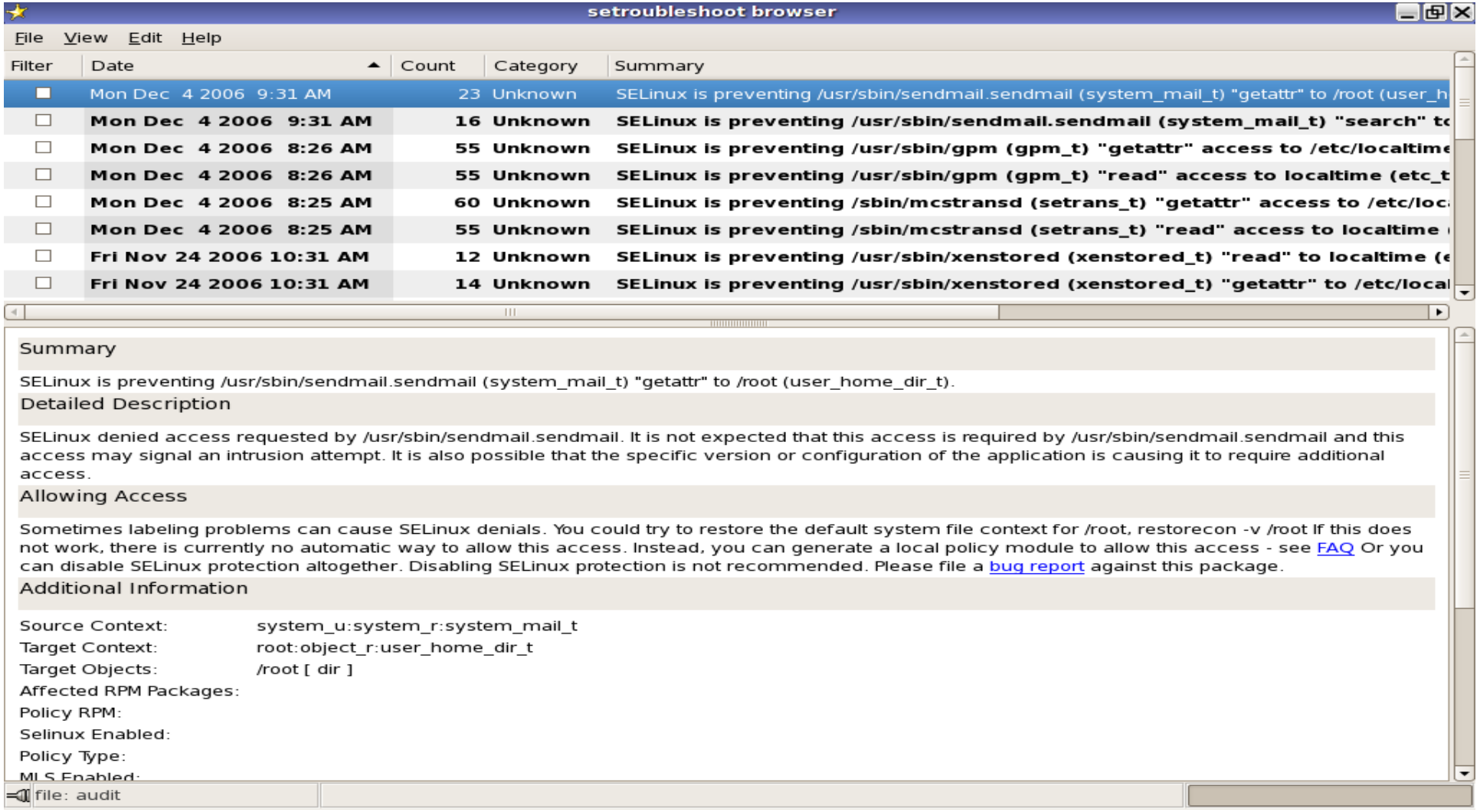
SELinux: End-User View

- sealert Notification



SELinux: End-User View

- sealert Browser



SELinux: System Administrator View

- Audit Log Analysis GUI
- Management GUI
- Policy Analysis GUI
- Policy Difference GUI
- Troubleshooter GUI

SELinux: System Administrator View

- Using audit2allow & semanage
  - You are experiencing SELinux errors
  - You know that these errors are blocking legitimate usage

Be aware that changes to your SELinux policy could compromise the security of your system.

SELinux: System Administrator View

- Red Hat gives employees a “Corporate Standard Build”
  - Customized RHEL Desktop
  - Includes VPN Configuration

- VPN Broke in last update!

time->**Wed Mar 5 07:22:55 2008**

type=SYSCALL msg=audit(1204719775.306:738): arch=40000003 syscall=54 success=no exit=-19 a0=4 a1=8933 a2=bfcec1bc a3=bfcec1bc items=0 ppid=3900 pid=5003 auid=501 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) comm="ip" exe="/sbin/ip" subj=user_u:system_r:ifconfig_t:s0 key=(null)

type=AVC msg=audit(1204719775.306:738): avc: denied { sys_module } for pid=5003 comm="ip" capability=16 scontext=user_u:system_r:ifconfig_t:s0 tcontext=user_u:system_r:ifconfig_t:s0 tclass=capability

SELinux: System Administrator View

<snip>

.....

comm="ip" exe="/sbin/ip" subj=user_u:system_r:ifconfig_t:s0 key=(null)

type=AVC msg=audit(1204719775.306:738): avc: denied { sys_module } for pid=5003 comm="ip" capability=16 scontext=user_u:system_r:ifconfig_t:s0 **tcontext=user_u:system_r:ifconfig_t:s0 tclass=capability**

.....

</snip>

 # ausearch -x "/sbin/ip" | audit2allow -M myVPNfix

 # semodule -i myVPNfix

SELinux: Auditor View

- Centralized Logging is a must!

aureport

- # aureport –summary

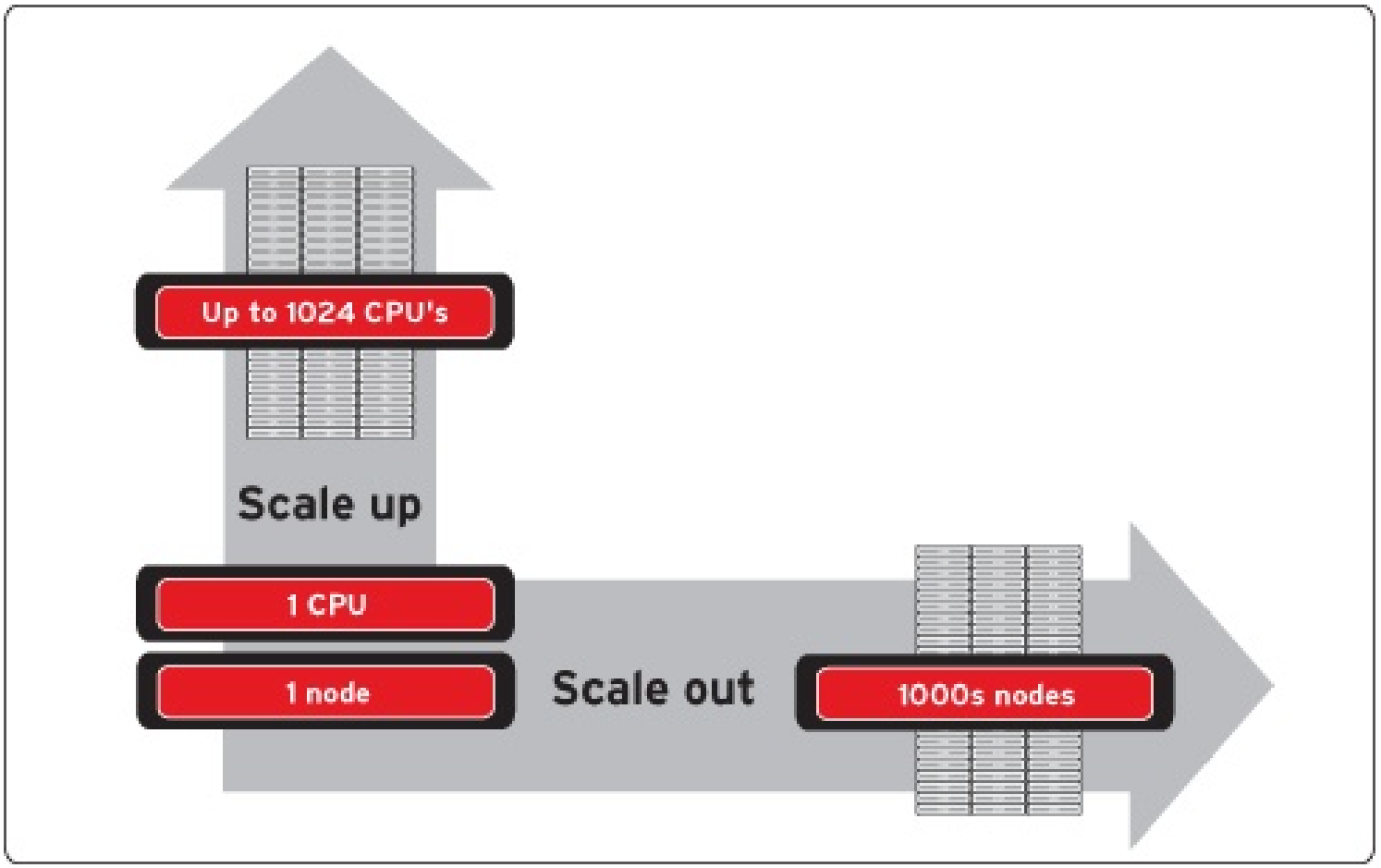
ausearch

- # ausearch -ul swells

Red Hat Enterprise Linux Update

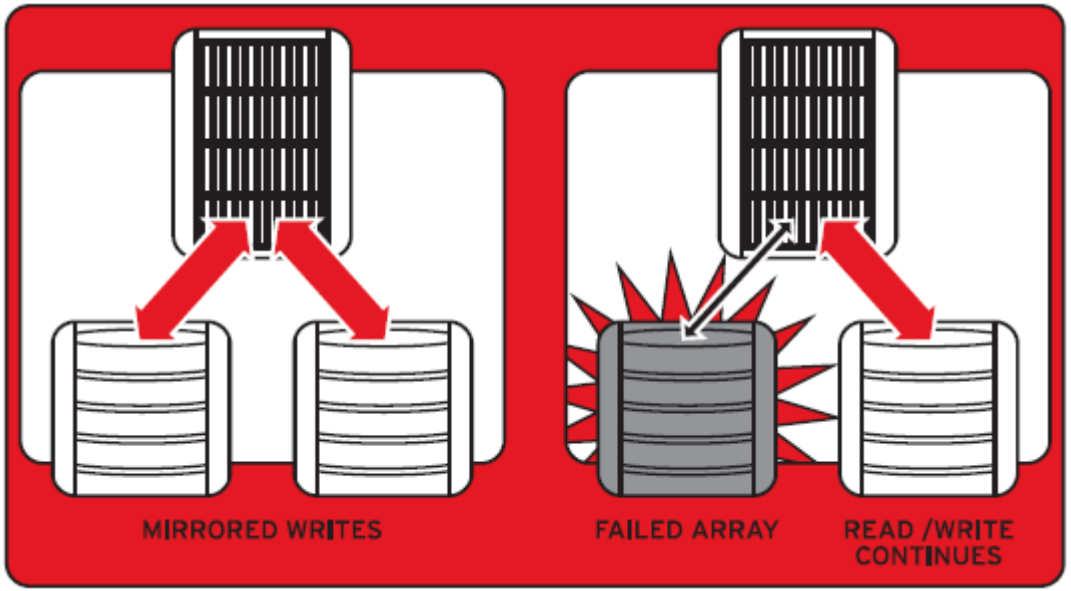
High Availability

RHEL5 High Availability: Mature Scaling



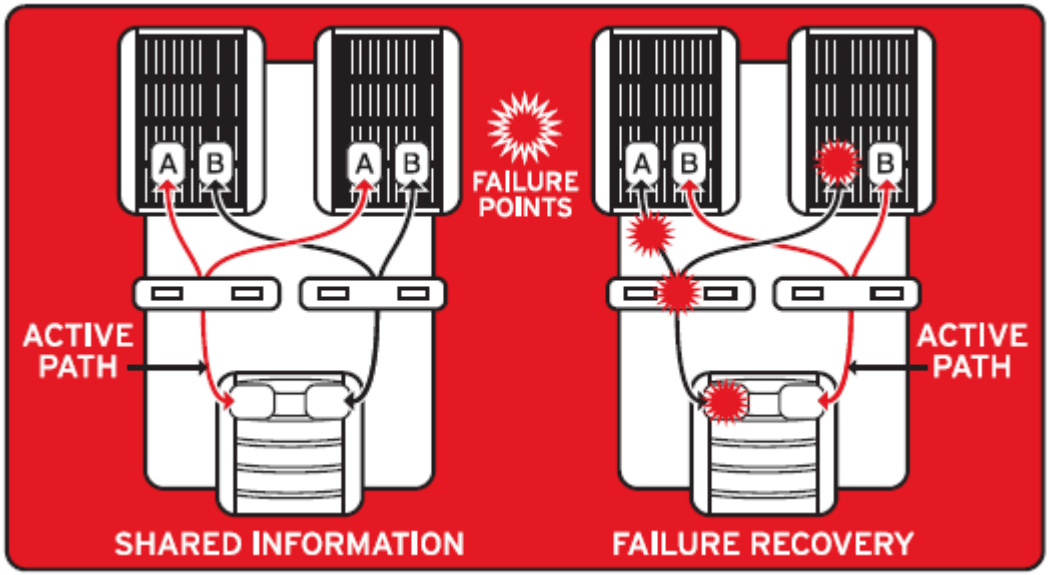
LVM Host-Based Synchronous Mirroring

- Each write is simultaneously written to 2 or more local or SAN disks (RAID1)
- LVM automatically detects failure, uses the identical, mirrored disks or LUN
- Upon restoration, recovery process begins in background
- If minor outage, transaction log rapidly replays missed I/O



Device Mapper Multipath IO (MPIO)

- Connects & manages multiple paths through SAN to storage array
- Upon component failure, MPIO redirects traffic via redundant pathing
- Active/Active array support
- Bundled into RHEL



GFS

- Red Hat GFS is an open source, POSIX-compliant, cluster file system.
- It provides a consistent file system image across the server nodes in a cluster, allowing Red Hat Enterprise Linux servers to simultaneously read and write to a single shared filesystem.
- Red Hat GFS also includes Red Hat Cluster Suite providing integrated application high availability and failover.

Red Hat Enterprise Linux Update

Directory Server

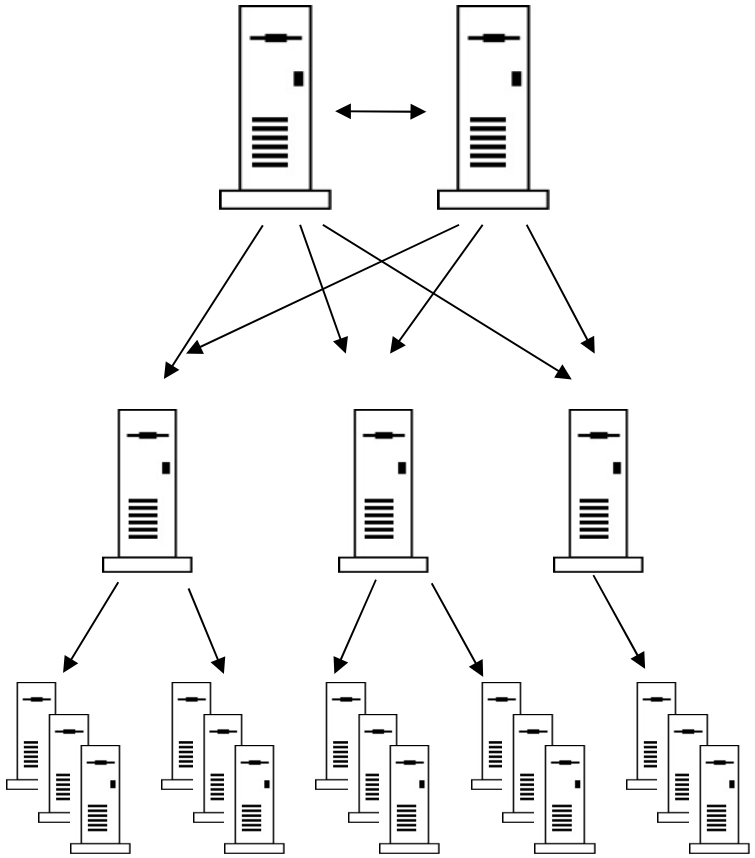
Certificate Server

Red Hat Authentication History

- On December 8, 2004, Red Hat acquired assets from AOL's Netscape Security Solutions business unit, including currently shipping products:
  - Netscape Certificate Management System (Red Hat Certificate System)
  - Netscape Directory Server (Red Hat Directory Server)
- Acquisition of JBoss in June 2006 now provides an extension for the identity management technologies into the Application and Web Services space.

What does Red Hat Directory Server provide?

- Standards Compliance (LDAP v2/v3)
- High Performance
  - Multi-Master Replication
  - WAN Replication
  - Load Balancing
  - Data Redundancy
  - Fault Tolerance
- Windows User Synchronization
- SASL Authentication
- Fine Grained ACL



What does Red Hat Certificate System provide?

- Standards Based PKI
- Unmatched Scalability
  - 14,000 certificate issuances/hour
  - 12M certificates issued < 35 days
  - Largest public CRL: 1.2M
- Government Support
  - FIPS-140 Certified
  - EAL4/CIMC Protection Profile
- Replaces Passwords, Single Sign-On
- Smart Card Support
- Integrated with RHEL & Windows

Certificate Server Scalability

- 25M+ Certificates issued from the DoD PKI CAs, 1999-Present
- 3.5M – 4M “active” smart cards, most with 3 certificates
- Issuing lifetime of individual CAs governed by the size of the database managed by the CA
  - As number of certificates issued increased, number of revocations increased, resulting in large CRLs
  - CMS 4.2 and CMS 6.1 on Solaris – approximately 1.5M issued certificates per CA
  - Red Hat CS 7.1 on Linux [deployed in 2006] – DT&E Testing prior to fielding demonstrated 3M issued certificates per CA with large CRL

PKI and Kerberos: Independently Successful

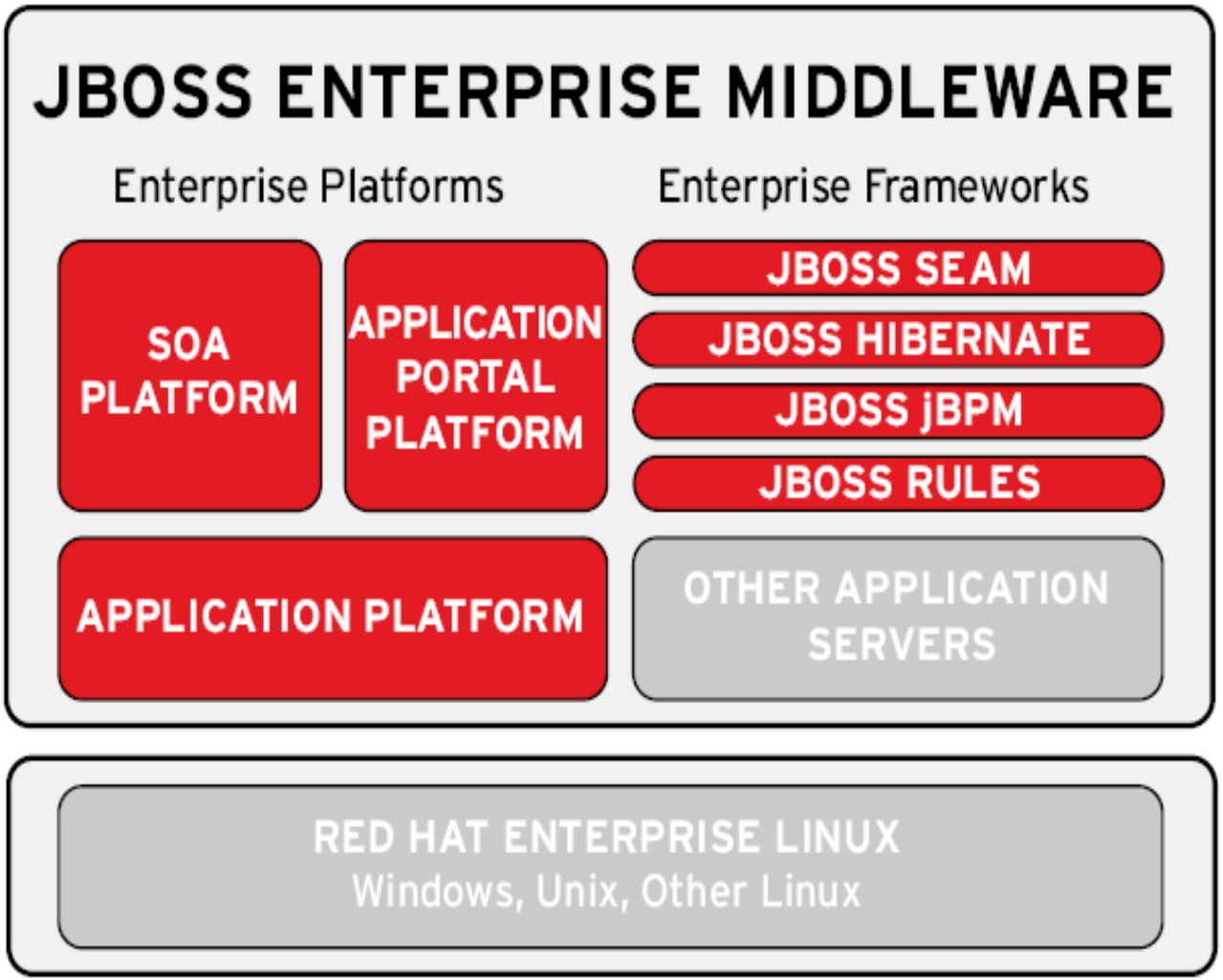
- PKI
  - Smart card authentication
  - Web services
    - TLS, SSL
  - Encryption
  - Signing
  - Data integrity
  - Non Repudiation
  - Asymmetric keys
- Kerberos
  - System Login
  - Secure Filesystem access
    - NFSv4, CIFS
  - Email server access
  - Printing
  - Symmetric keys

Directory & Certificate Server tie them together

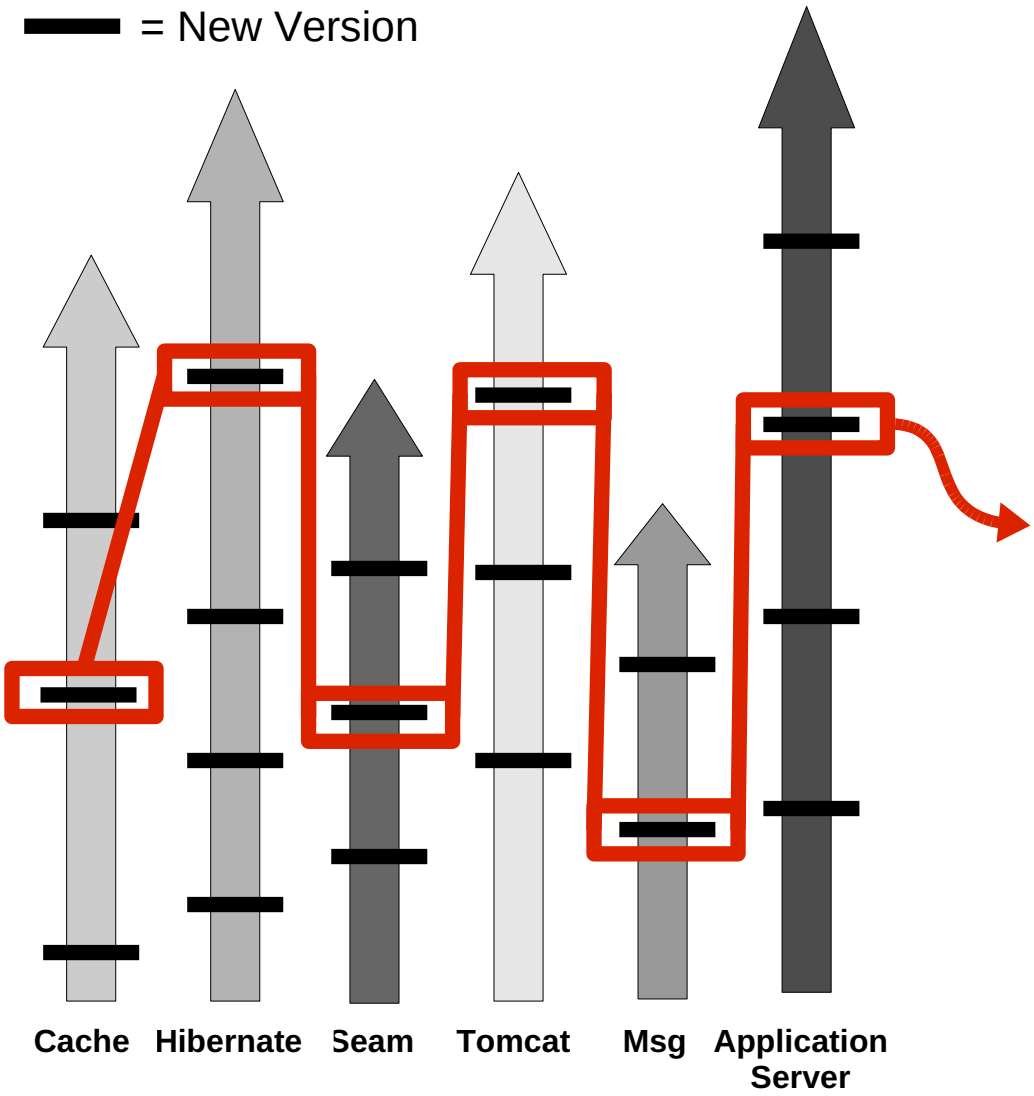
Red Hat Middleware Update

JBoss

MetaMatrix


JBOSS ENTERPRISE MIDDLEWARE
Enterprise Platforms
Enterprise Frameworks
SOA PLATFORM
APPLICATION PORTAL PLATFORM
JBOSS SEAM
JBOSS HIBERNATE
JBOSS jBPM
JBOSS RULES
APPLICATION PLATFORM
OTHER APPLICATION SERVERS
RED HAT ENTERPRISE LINUX
Windows, Unix, Other Linux

JBoss Enterprise: Stability & Performance



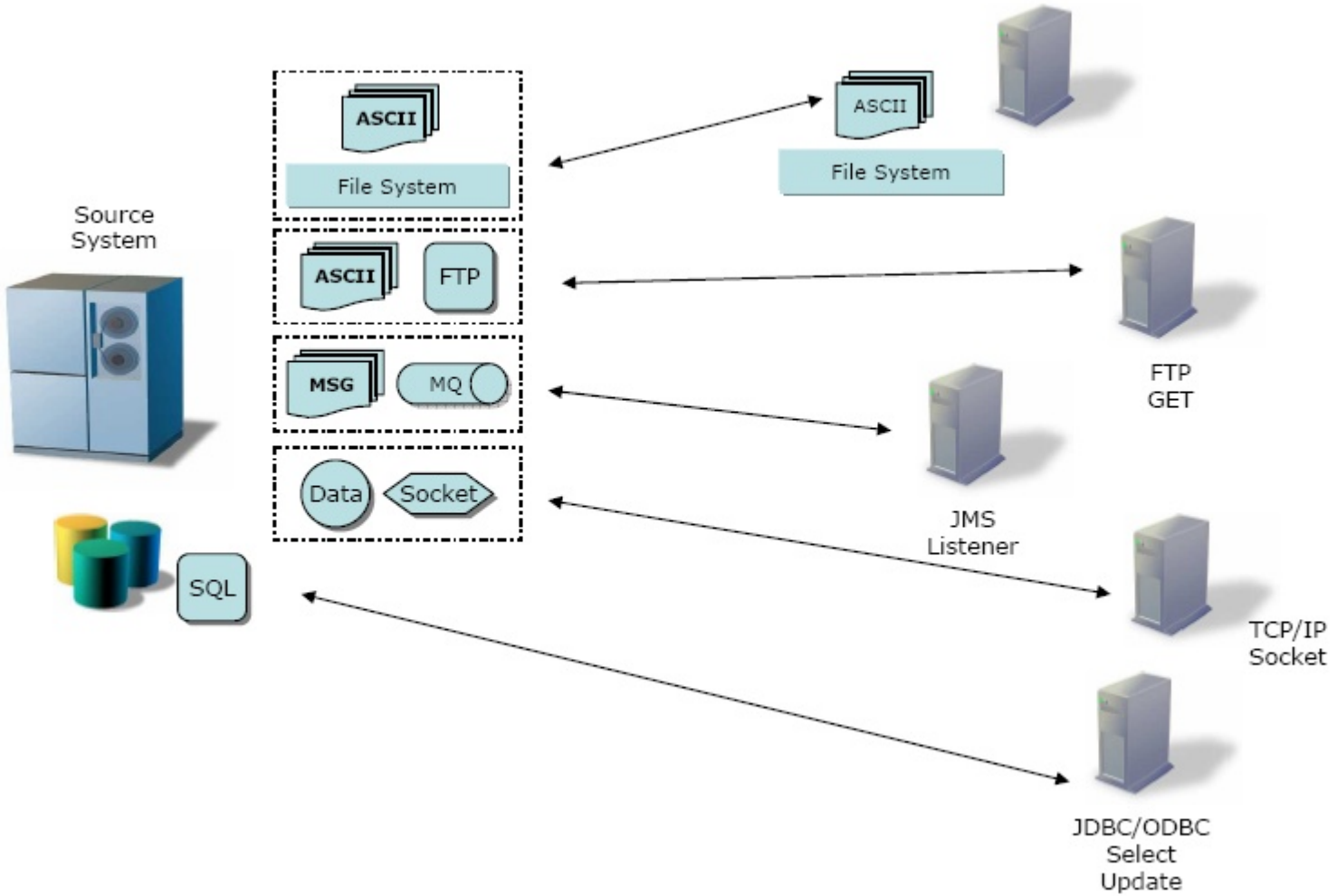
Corporate Challenge:

- Integrate Multiple Versions
- Coordinate 100,000 developers

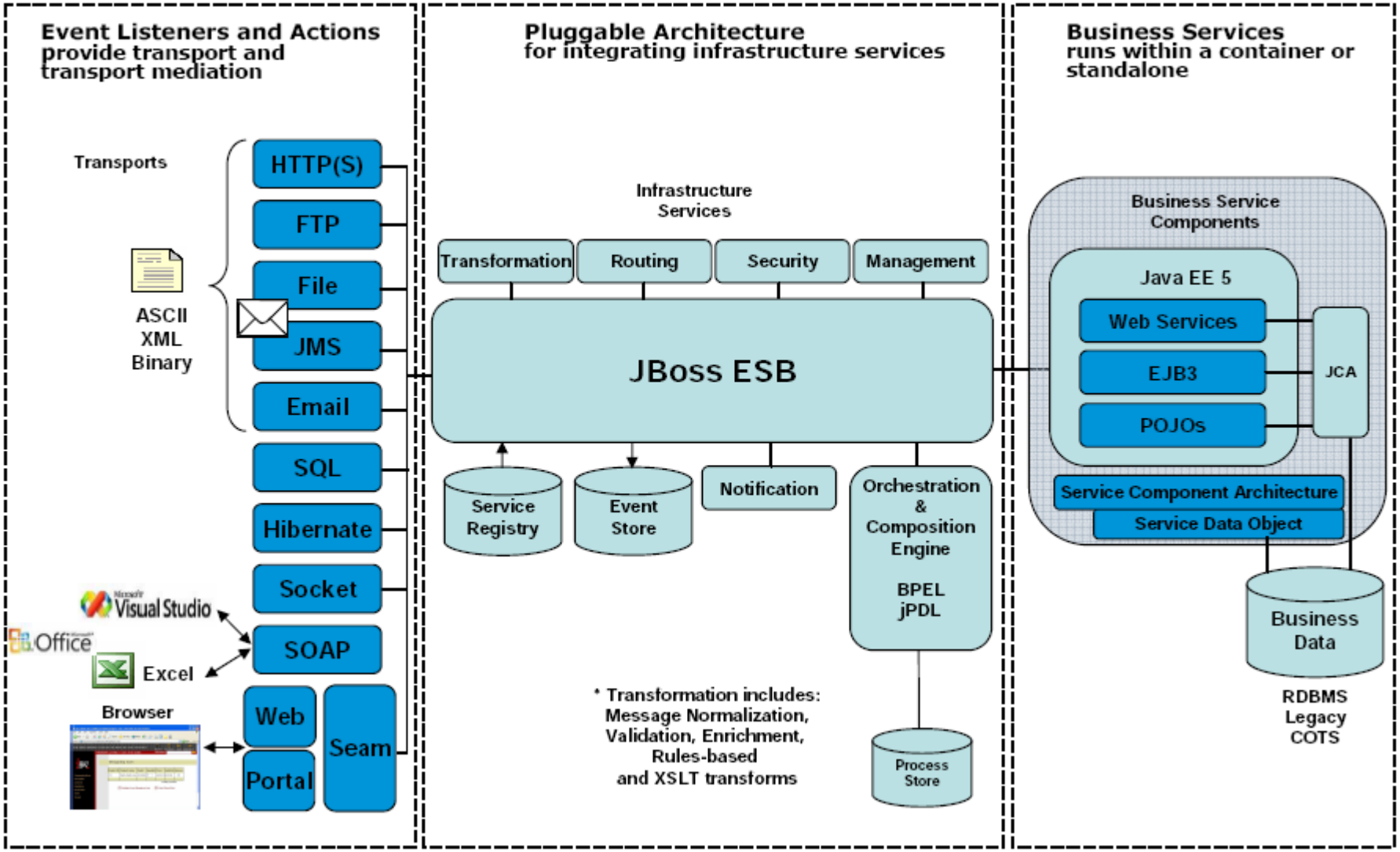
Solution: JBoss Enterprise Platforms

- Single, integrated, certified distributions
- Extensive Q/A Process
- Industry-leading Support
- Documentation
- Secure, Production-level Configurations
- Multi-year Errata Policy

JBoss ESB: Before (Stovepipes)

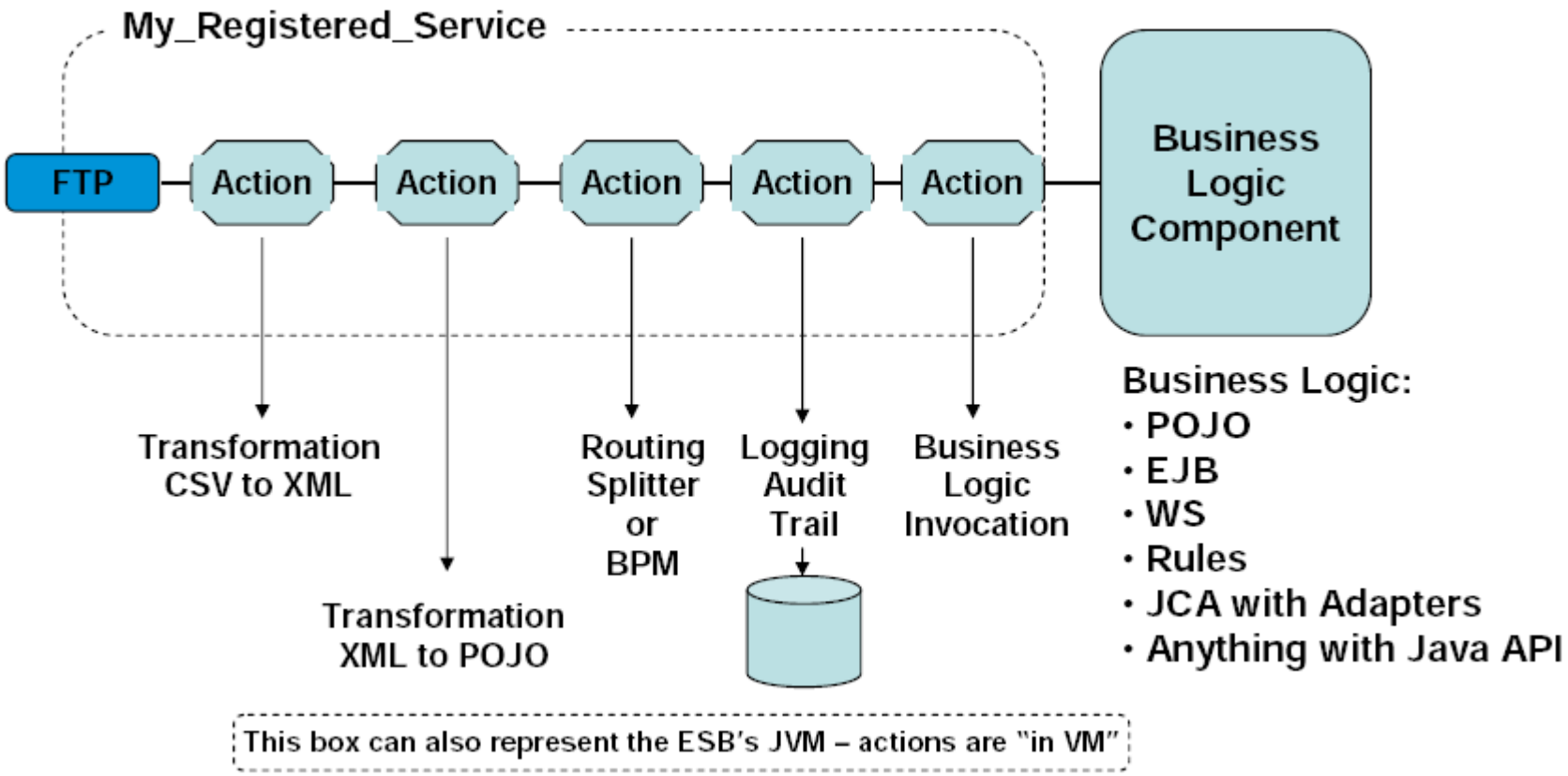


JBoss ESB: After (Anything-To-Anything)

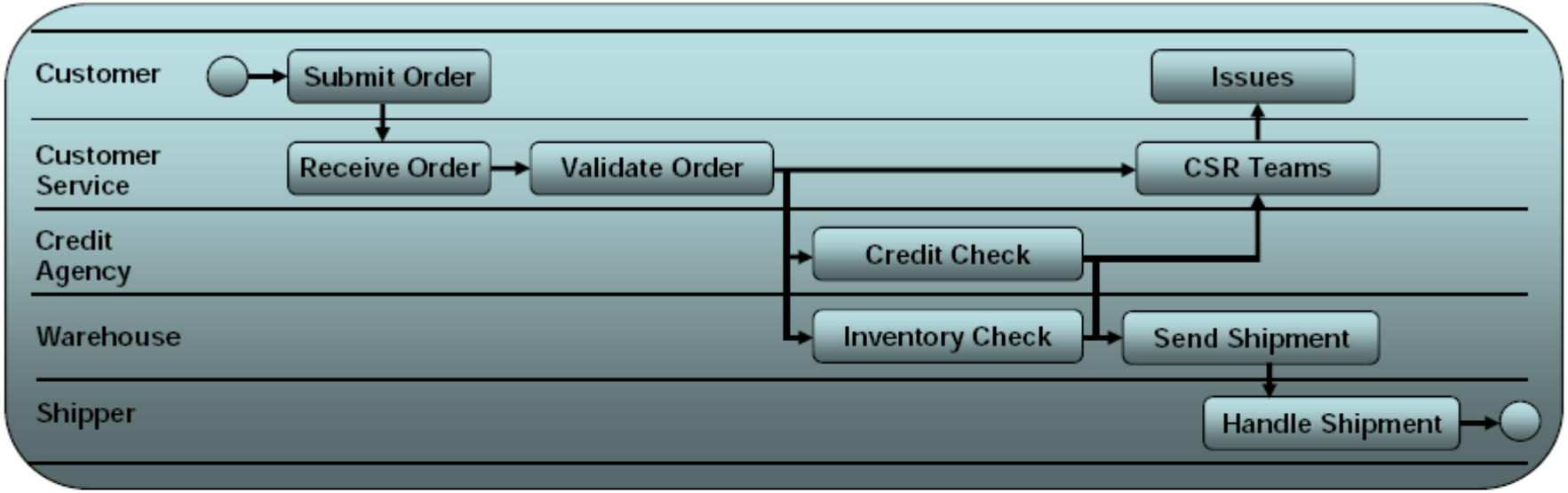


JBoss Action Pipeline

- Actions are reusable components that can be chained together to form capabilities of a registered service. Can be dynamically added/removed at runtime.



JBoss Rules



Validate Order
- a Parse XML
- b Transform
- c Apply Business Rules

Credit Check
- a Create Outbound Msg
- b Handle Response
- c Apply Business Rules

Send Shipment
- a Determine Shipper(s)
- b Print Labels
- c Print Pick Tickets
- d Create & Send ASNs

Inventory Check
- a Send to N Warehouses
- b Handle N Responses
- c Determine Best WHSEs
- d Handle Drop-Ships

ESB Mediates & Provides Services

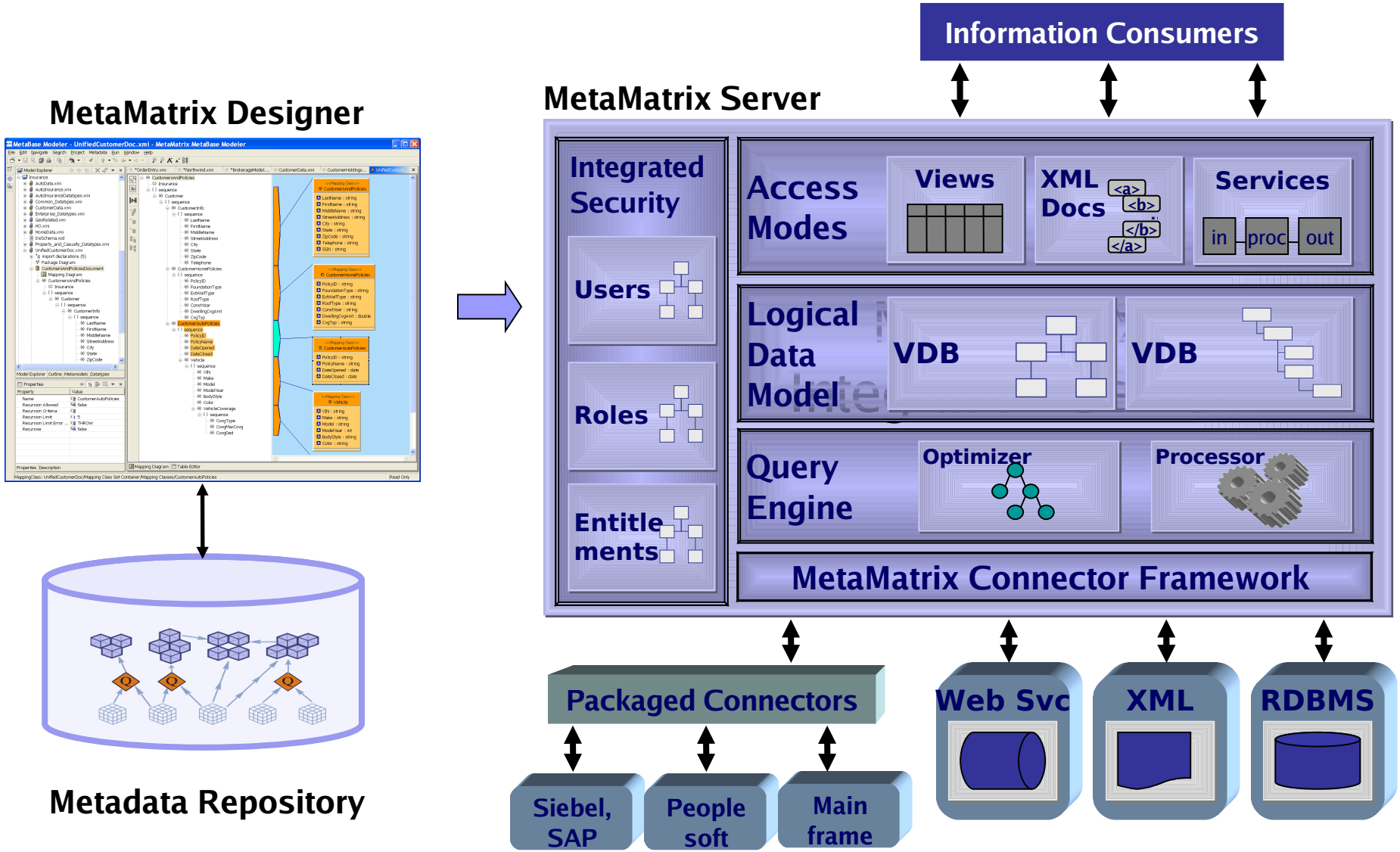
JBoss Conclusion

- Open Source makes JBoss SOA happen
  - ESB
  - Hibernate
  - SEAM
- ESB is a solution for application/process integration
- ESB is about service intermediation
- Ask about getting evaluation copies!

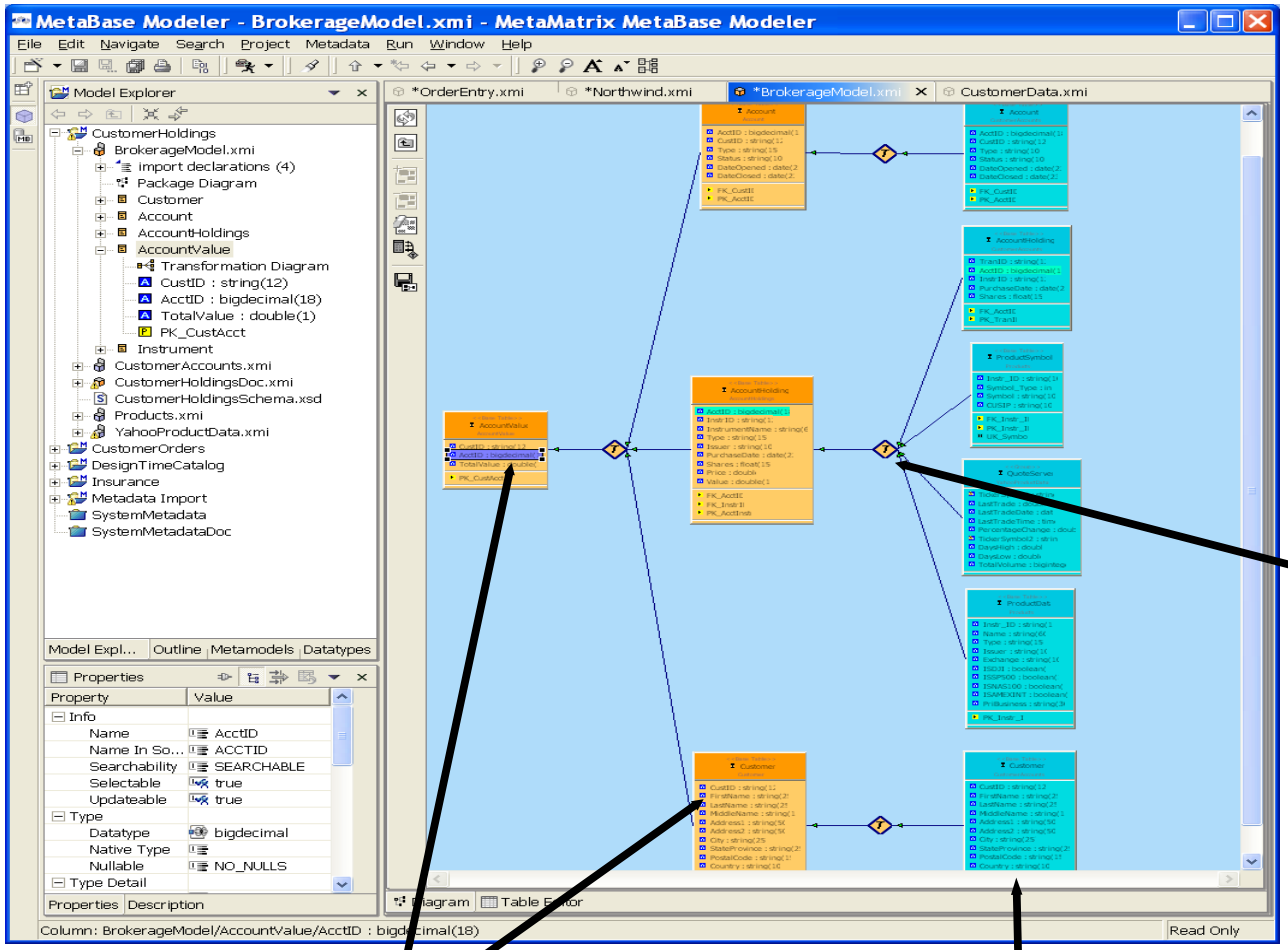
MetaMatrix Background

- On-demand access to distributed information
  - Real time integration of diverse data
  - Avoid unnecessary data replication
- Metadata-Driven
  - Integration in days, not weeks
  - Reduce “long tail” of application maintenance
- Improved data agility
- Abstracts data into a “single view” without need to move data between databases
  - Single view of Customer – CRM
  - Single view of Supplier – Supply Chain
  - Single view of Employee – HR Consolidation
- SOA Enabler
  - Consume/Produce Web Services
  - ..... and still provide support for ODBC, JDBC, and legacy!

MetaMatrix: How it works



MetaMatrix Enterprise Designer



Defined by Models, not code

Transformations:

- Select
- Join/Aggregate
- Filter
- Functions
- Text/String
- Numeric
- Decode
- User Defined

Logical Models

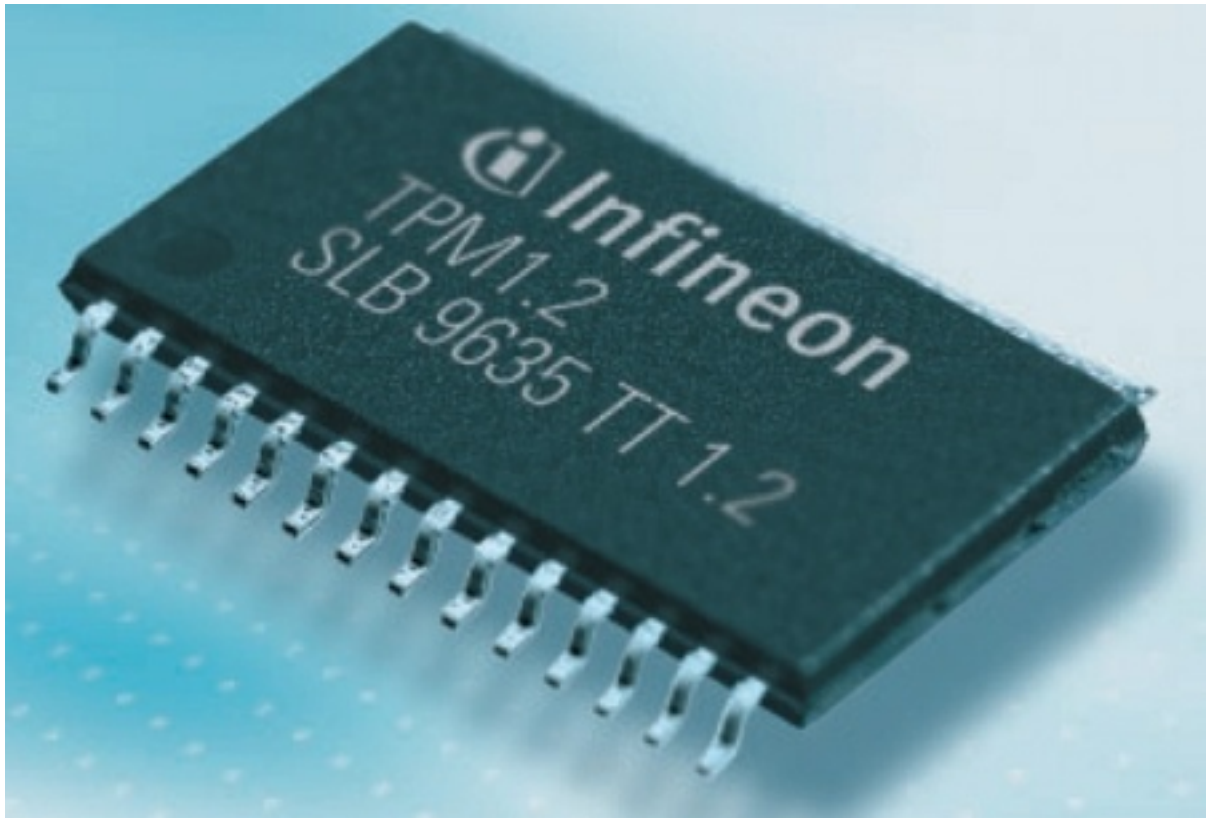
Physical Models representing actual data sources

Red Hat Emerging Technologies

- Virtualization Updates
- MRG/Realtime, Messaging, Grid
- freeIPA

Trusted Platform Module

- What functionality would you like to see?
- What functionality would you use?

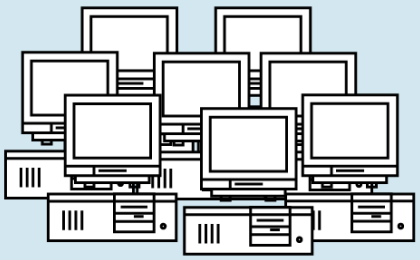


Deploy apps at scale to any resource

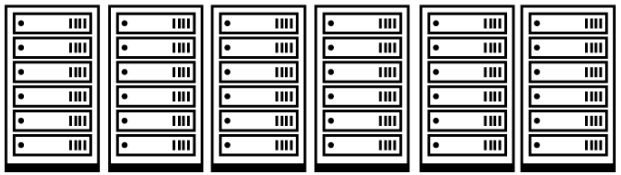
Run with Realtime performance

Interoperate and send data with fast, reliable, AMQP-compliant messaging

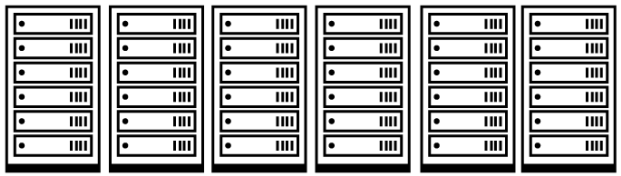
RED HAT ENTERPRISE MRG



Desktop PC Cycle-Stealing



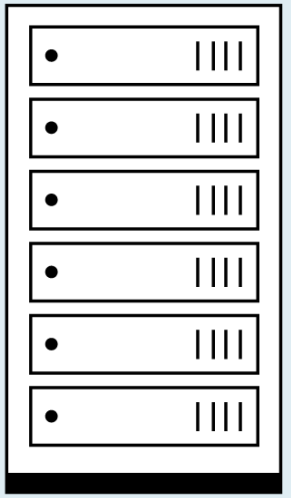
Local Grid



Remote Grid

Remote Cloud

Remote Server



MRG Realtime

- **Determinism**
  Ability to schedule high priority tasks predictably and consistently

- **Priority**
  Ensure that highest priority applications are not blocked by low priority

- **Quality Of Service** (QoS)
  Trustworthy, consistent response times

- **Proven results**
  - Average of 38% improvement over stock RHEL5
  - Timer event precision enhanced to µs level, rather than ms

MRG: Messaging

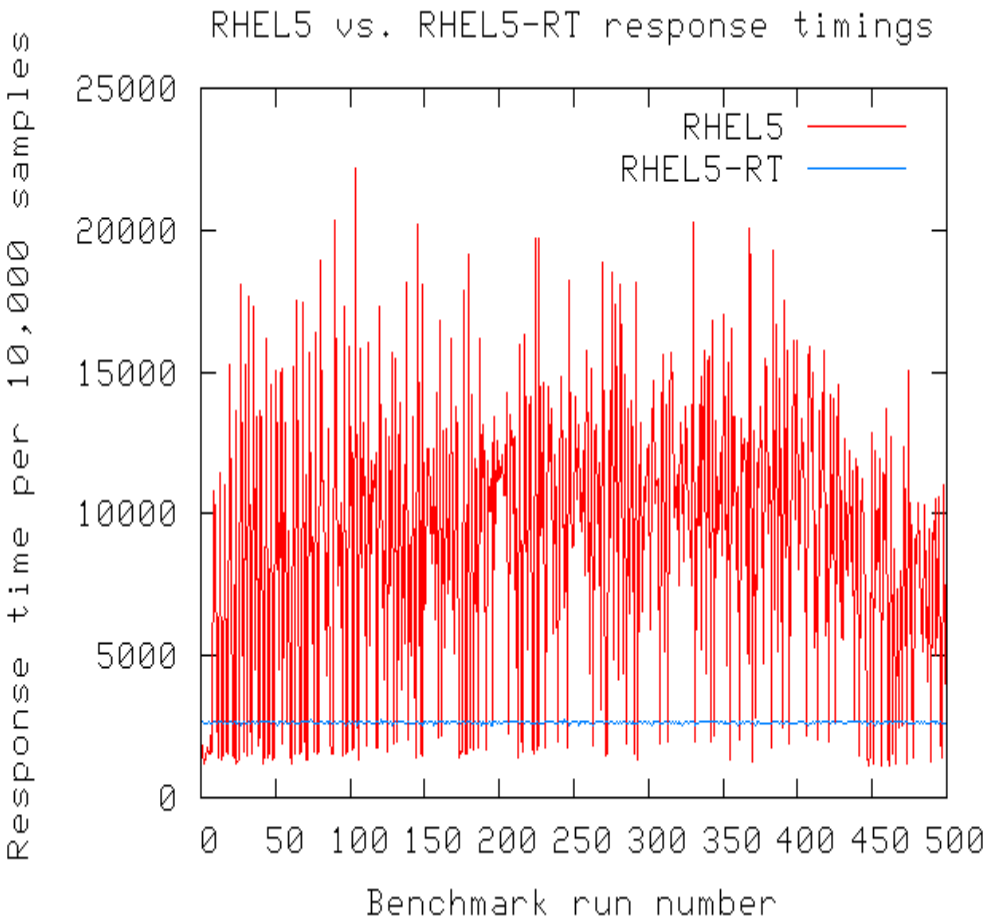
- Provides messaging that is up to 100-fold faster than before
- Spans fast messaging, reliable messaging, large-file messaging
- Implements AMQP, the industry's first open messaging standard, for unprecedented interoperability that is cross-language, cross-platform, multi-vendor, spans hardware and software, and extends down to the wire level
- Uses Linux-specific optimizations to achieve optimal performance on Red Hat Enterprise Linux and MRG Realtime
  - Takes advantage of RHEL clustering, IO, kernel, and more
  - Includes new high-performance AIO Journal for durable messaging
  - Provides native infiniband support for transient messaging

About AMQP

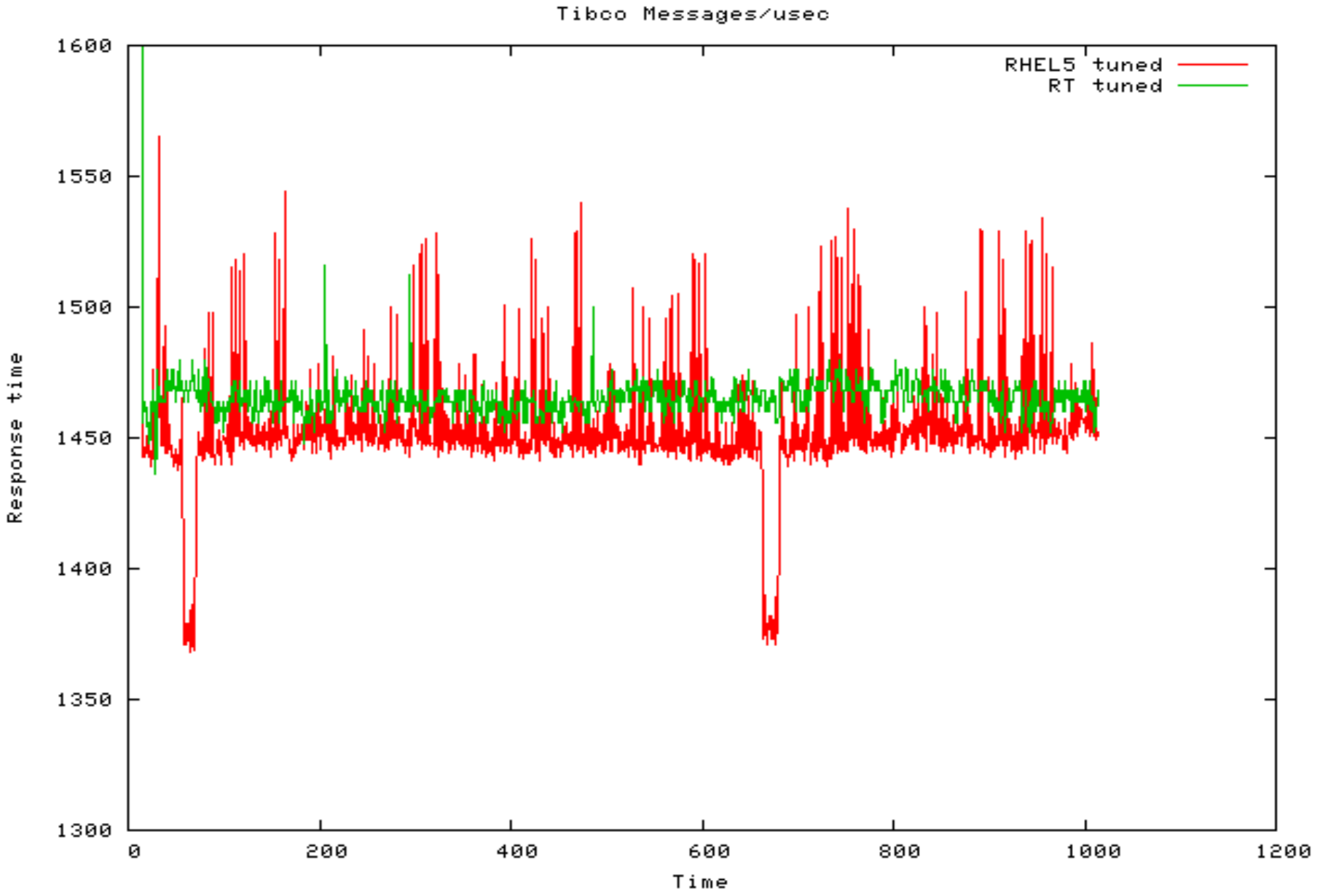
- AMQP is an open specification for messaging
  - It is a complete specification
  - Anyone may use the AMQP specification to create useful implementations without being charged for the IP rights to do so
- AMQP aims to be technology and language-neutral
  - Available in C, C++, Java, JMS, .NET, C#, Ruby, Python, etc.
  - Requires IP, and can be used with TCP, UDP, SCTP, Infiniband, etc.
- Products complying with AMQP are inter-operable
  - AMQP is a Wire-Level protocol based on the ubiquitous IP
  - Wire-level compatibility means it can be embedded in the network
  - Applications written to Product X will plug into servers running Product Y
- Red Hat is a founding member of the AMQP Working Group

MRG: Realtime

- Enables applications and transactions to run predictably, with guaranteed response times
  - Provides microsecond accuracy
- Provides competitive advantage & meets SLA's
  - Travel web site: missed booking
  - Program trading: missed trades
  - Command & Control: life & death
- Provides replacement kernel for RHEL 5.1+; x86/x86_64
- Preserves RHEL Application Compatibility



Detail zoom-in of RHEL5 vs MRG Realtime



MRG: Realtime Tools

- **MRG includes a new MRG Realtime Latency Tracer**
  - Runtime trace capture of longest latency codepaths – both kernel and application. Peak detector
  - Selectable triggers for threshold tracing
  - Detailed kernel profiles based on latency triggers
- **Existing standard RHEL5 based performance monitoring tools remain relevant**
  - Gdb, OProfile Frysk – source level debuggers & profiler
  - SystemTap, kprobe – kernel event tracing and dynamic data collection
  - kexec/kdump standard kernel dump/save core capabilities

MRG: Realtime Breakthroughs

- **Red Hat engineers succeed at mainstream acceptance**
  - Methodical multi-year implementation
  - Incrementally added features beneficial to all use cases
  - Iteratively worked to cooperatively build an inclusive realtime community
- **MRG Realtime is COTS (Commercial Off The Shelf) operating system**
  - Standard RHEL5.1 OS
  - Replacement kernel
- **Integrated with distributed high speed messaging & grid scheduler**
  - MRG Messaging, MRG Grid

MRG: Grid

- Brings advantages of scale-out and flexible deployment to any application
- Delivers better asset utilization, allowing applications to to take advantage of all available computing resources
- Dynamically provisions additional peak capacity for “Christmas Rush”-like situations
- Executes across multiple platforms and in virtual machines
- Provides seamless and flexible High Throughput Computing (HTC) and High Performance Computing (HPC) across
  - Local grids
  - Remote grids
  - Remote clouds (Amazon EC2)
  - Cycle-stealing from desktop PCs

MRG: Grid based off Condor

- MRG Grid is based on the Condor Project created and hosted by the University of Wisconsin, Madison
- Red Hat and the University of Wisconsin have signed a strategic partnership around Condor:
  - University of Wisconsin makes Condor source code available under OSI-approved open source license
  - Red Hat & University of Wisconsin jointly fund and staff Condor development on-campus at the University of Wisconsin
- Red Hat and the University of Wisconsin's partnership will:
  - Add enhanced enterprise features, management, and supportability to Condor and MRG Grid
  - Add High Throughput Computing capabilities to Linux

Red Hat Enterprise MRG Availability

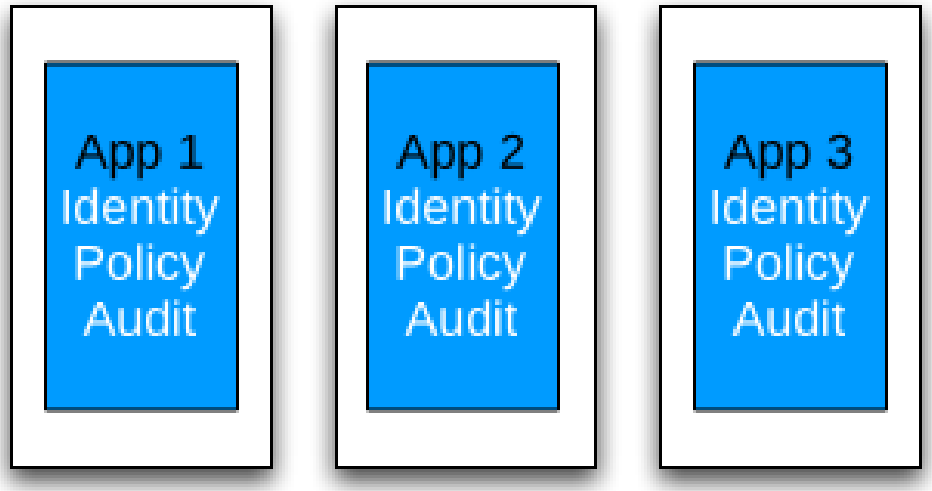
- MRG Announcement & Beta Launch: December 2007
  - Public beta
- MRG v1.0: Early 2008
  - RHEL-only support for MRG Messaging broker
  - MRG Grid Technology Preview
- MRG v1.1: Late 2008
  - Multi-platform support for MRG Messaging Java-based broker
  - AMQP support updated to newly available AMQP version (1.0)
  - MRG Grid support available

Additional Information:

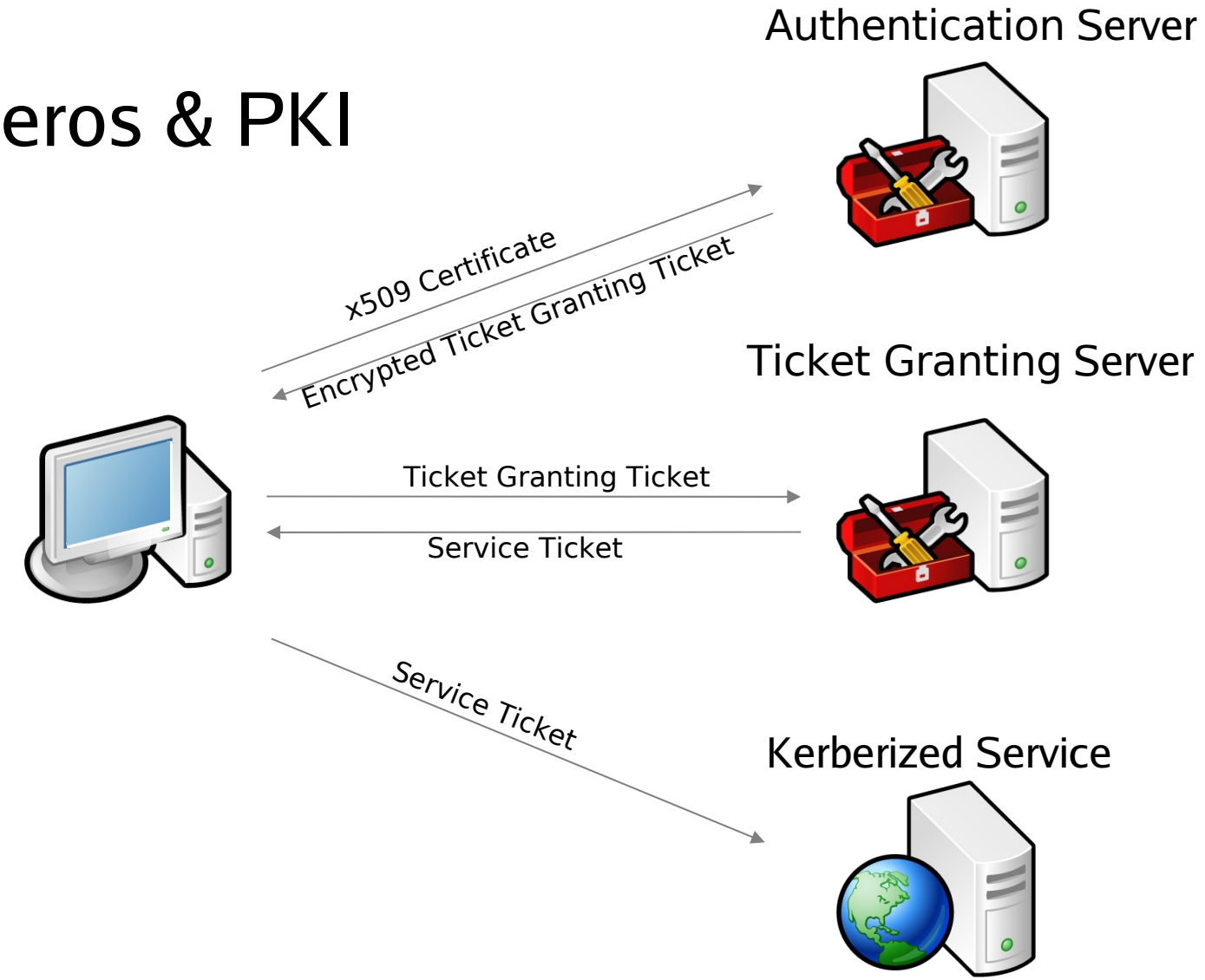
http://www.redhat.com/mrg/

Security Information Situation Today

- Many security and security management applications store and manage their own vital security information
  - Identity
  - Policy
  - Audit
- Difficult to analyze across applications, so organizations can't
  - Form a full picture of their security stance
  - Comply with government regulations
  - Protect themselves sufficiently
  - Efficiently enable their operations
- Example: Identity silos



Kerberos & PKI



- Enterprise Single Sign-on
- Strong authentication with strong credentials

What is needed?

To enable this:

Maximize freedom

Maximize efficiency

Vital security information (IPA) should be:

- Open (You own it)
- Inter-operable
- Manageable

Need a way to make it possible for vital security information

- Identity
- Policy
- Audit

to enable the freedom and efficiency of next generation IT infrastructure

- Project
  - Open Source
  - www.freeipa.org
  - Started and contributed to by Red Hat
  - Open to all
  - IPA = Identity, Policy, Audit
- Big vision
  - Start with centralized user identity management for UNIX/Linux
  - Add robust, shared sense of machine, service and data identity
  - Provide centrally managed admin access control for UNIX/Linux
  - Give ability to externalize policy and add to it easily
  - Add centralized audit
  - With this you can enable flexible cross-enterprise policy and rational audit

freeIPA
identity | policy | audit

IPAv1 (February target) will provide

Single Sign on for users

- Tie together Directory and Kerberos
- User Kerberos ticket for SS) to UNIX/Linux, JBoss, other apps

Centralized authentication point for IT

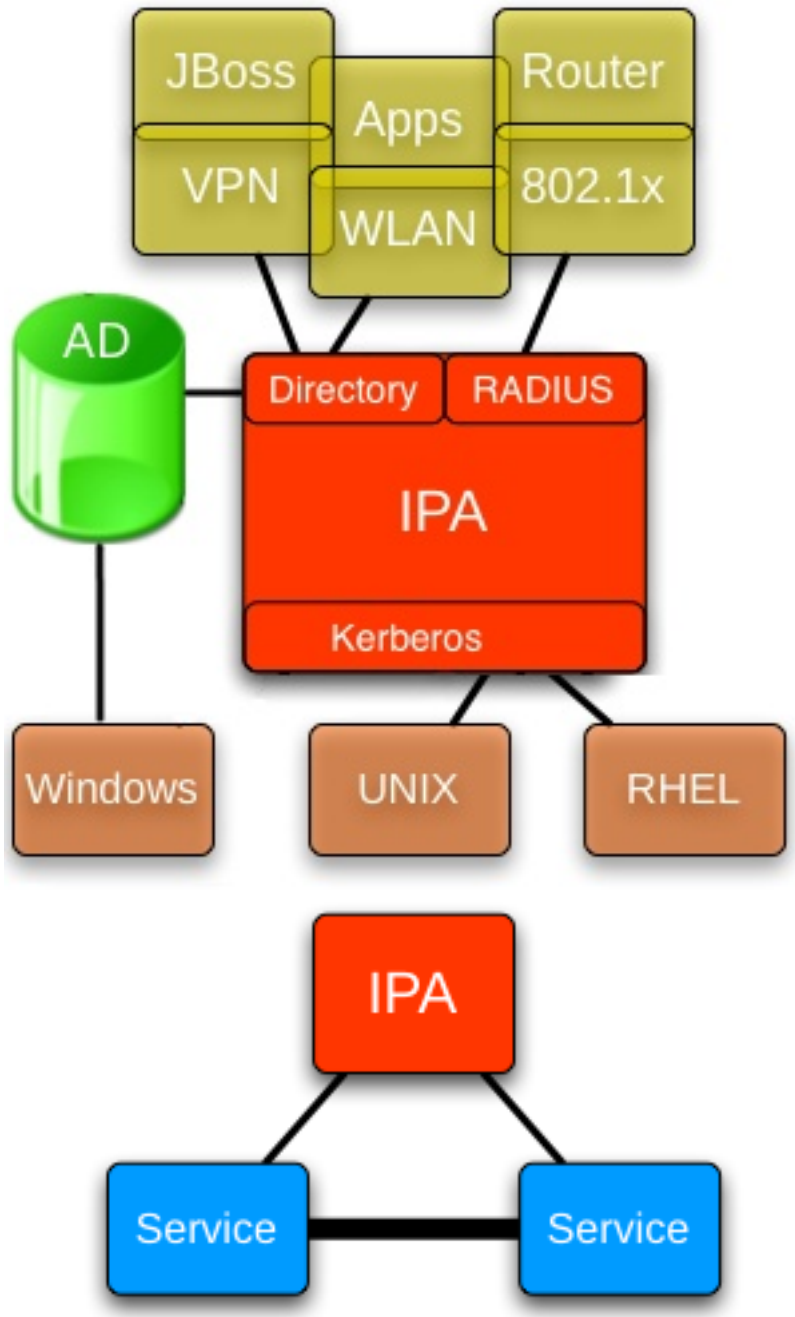
- Unite Directory, Kerberos, RADIUS servers, SAMBA
- From Apps, UNIX/Linux, VPNs, WLANs

Easy for IT to set up, migrate to, and manage

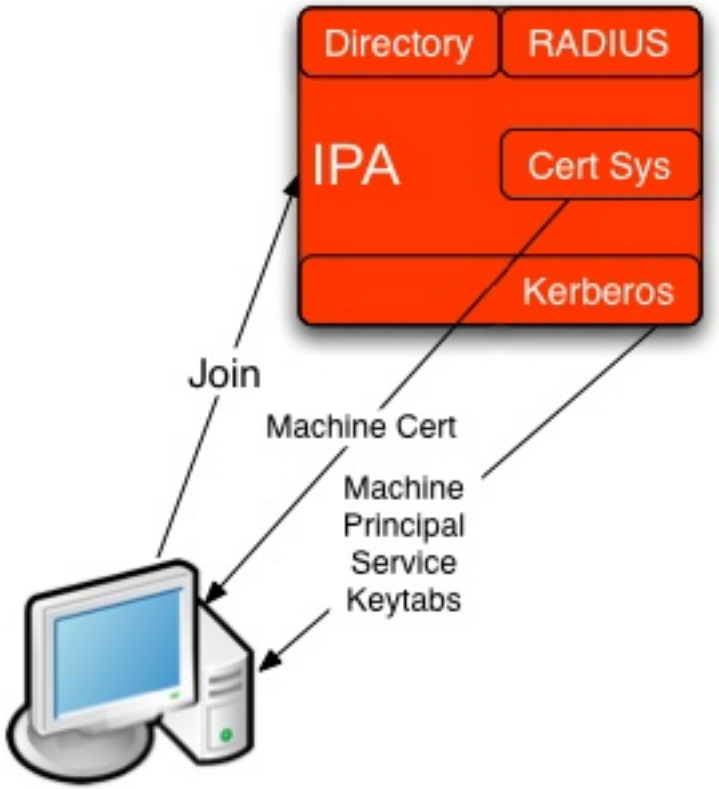
- Simple IPA install
- Intuitive web interface, Command line
- Tools migrate from NIS

Key Data replicated via Directory

Process identity via a Kerberos principal



freeIPA
identity | policy | audit



IPAv2 (July target) will provide

Identify and group machines, Vms, services

Simplified service authentication and establishment of secure communication

- Machine identity via Kerberos, certificate
- Process identity via Kerberos principal

Management of machine certificate

Centrally managed access control

- Extensible policy framework
- Set policy of which users can access which apps on which machines
- Centrally managed scoped admin control

Central audit database

- Centrally audit security event, logs, keystrokes (?), compliance with lockdown

Open Discussion