Red Hat Security Seminar

Shawn D. Wells (swells@redhat.com)

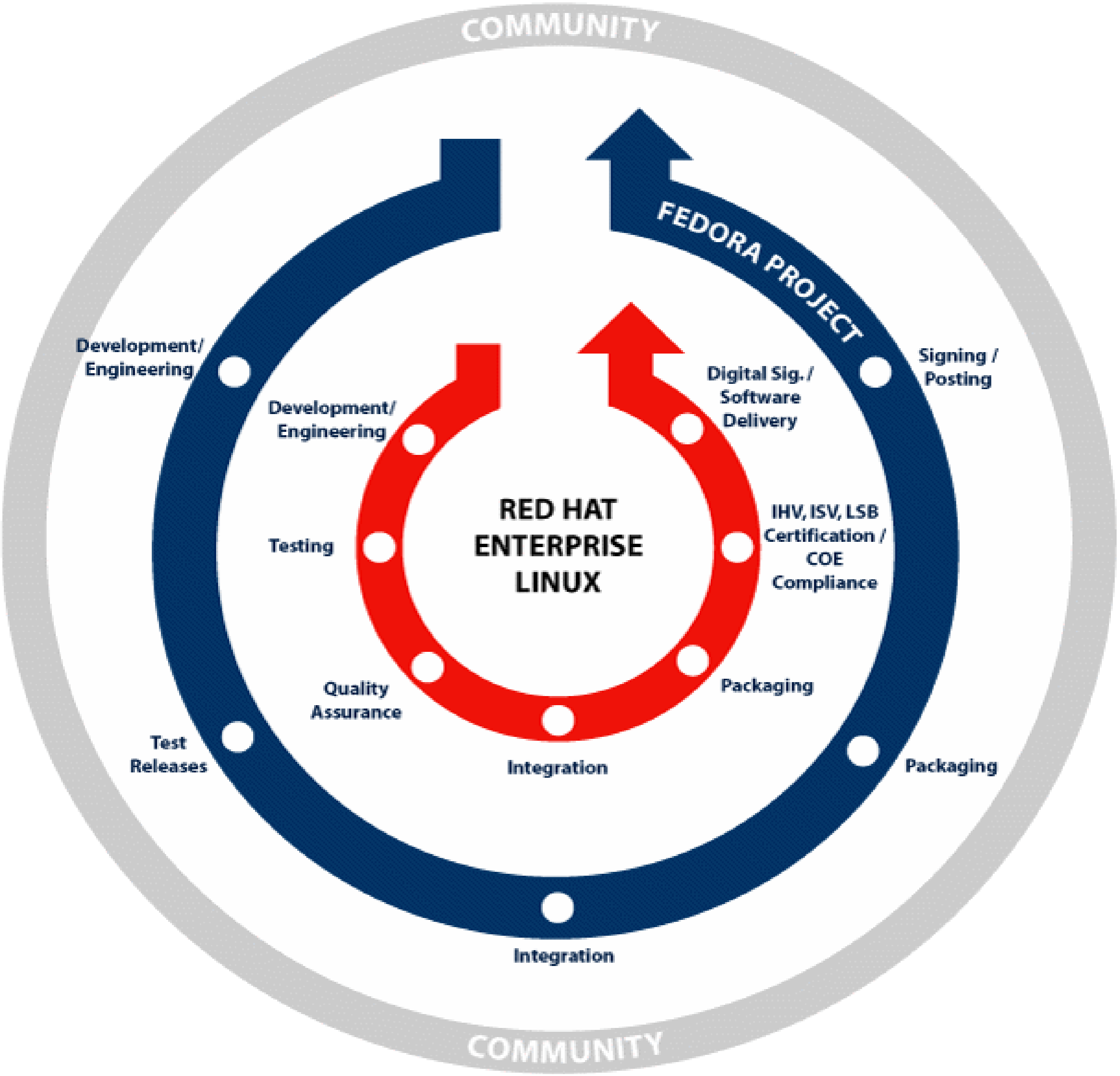
Solutions Architect, Federal Team

Agenda

- Start: 10:30 am
- End: 1:00 pm, ish
- Red Hat Emerging Technologies
- Red Hat Security
- Summary & Close

Hands On & Labs

Red Hat Development Model



Open Source – A Better Way

- Returns control
- Security reinforced through transparency
- Multiplies the development capacity

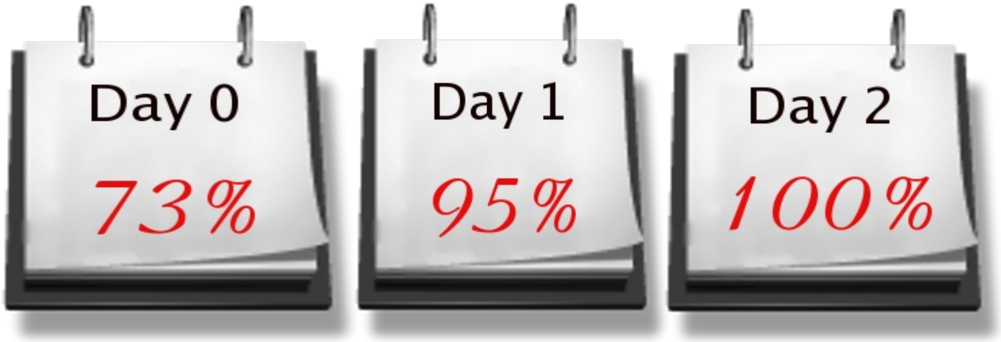
Bugs per 1000 Lines of Code

Linux 2.6 Kernel	0.17	Stanford University/Cover
Proprietary Software	10 to 20	Carnegie Mellon Cylab

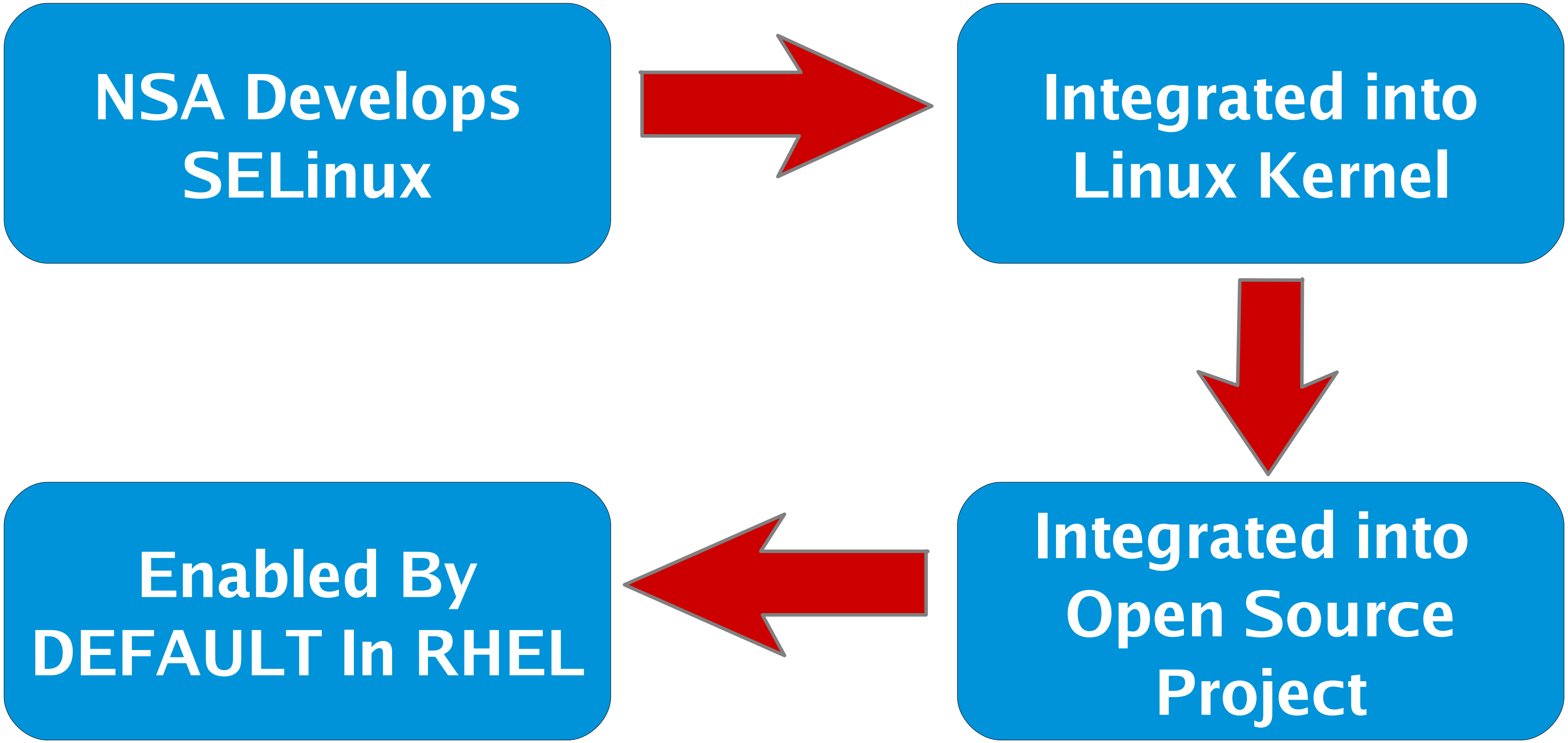
Wired Magazine, Dec 2004

Open Source as a Security Innovation

- Time from a critical issue being known to the public until the day that fix available
  - Red Hat Enterprise Linux 4
  - FEB 2005 – FEB 2006



SELinux: Building Security Openly



NSA Develops SELinux

Integrated into Linux Kernel

Integrated into Open Source Project

Enabled By DEFAULT In RHEL

Customers, NSA, Community, and Red Hat continue evolution

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

Security 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

Open Vulnerability & Assessment Language (OVAL)

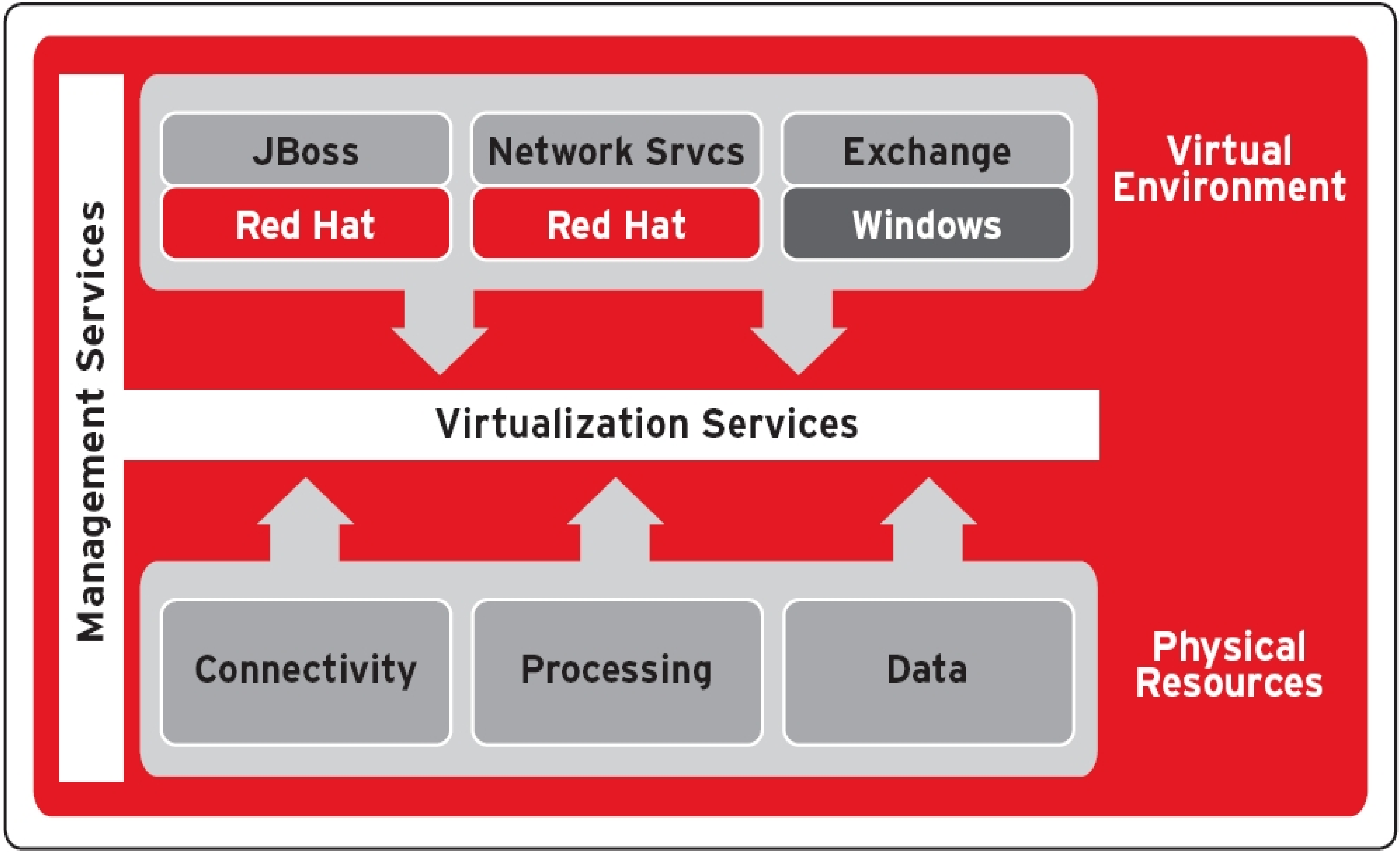
- Machine-readable versions of security advisories

Common Vulnerability and Exposures (CVE) Compatibility

- Trace a vulnerability through multiple vendors

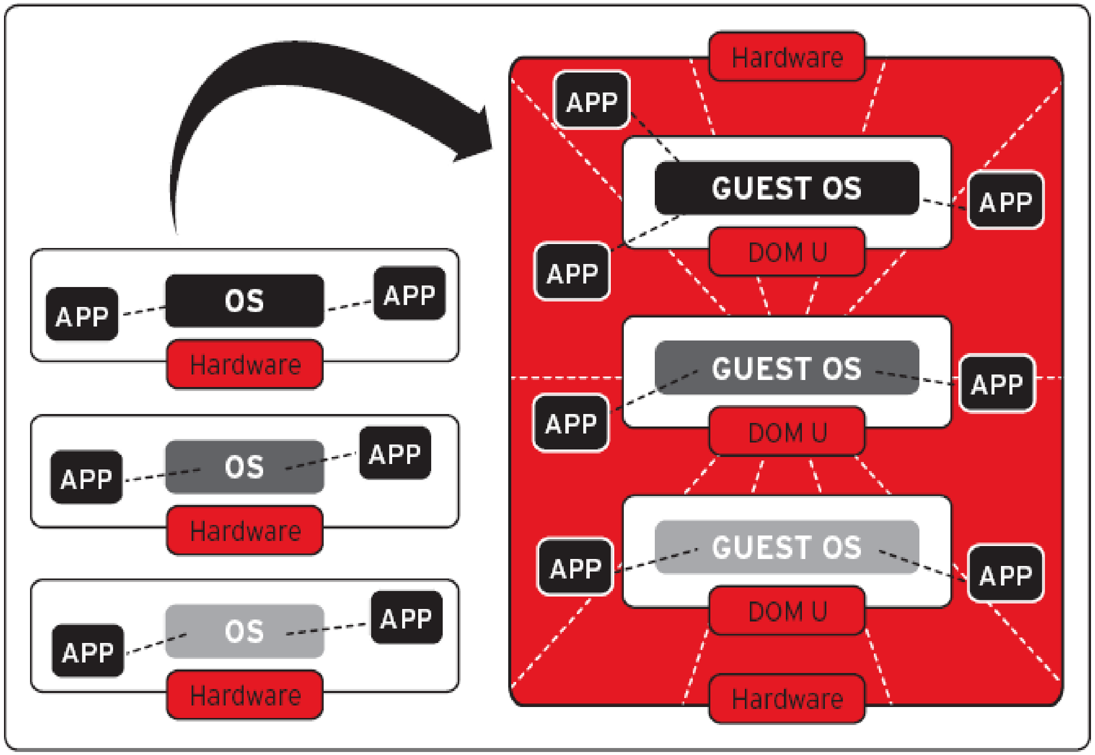
Questions?

Red Hat Emerging Technologies


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

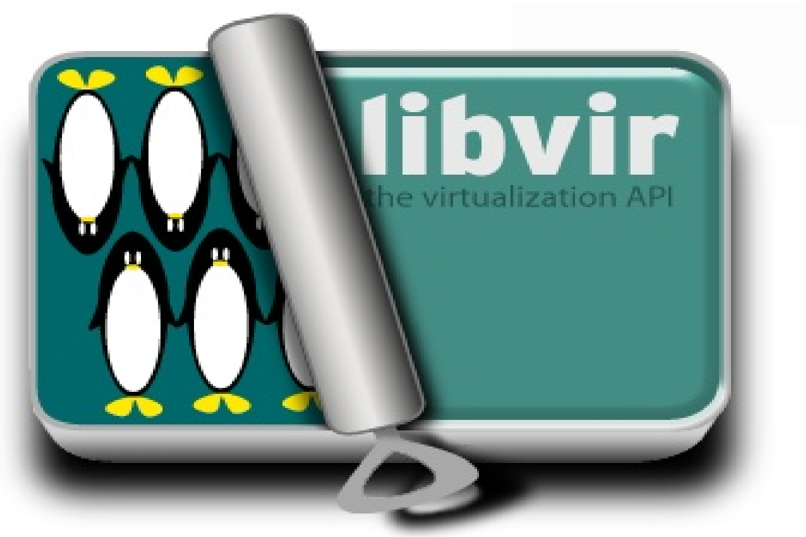
The Xen Hypervisor

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



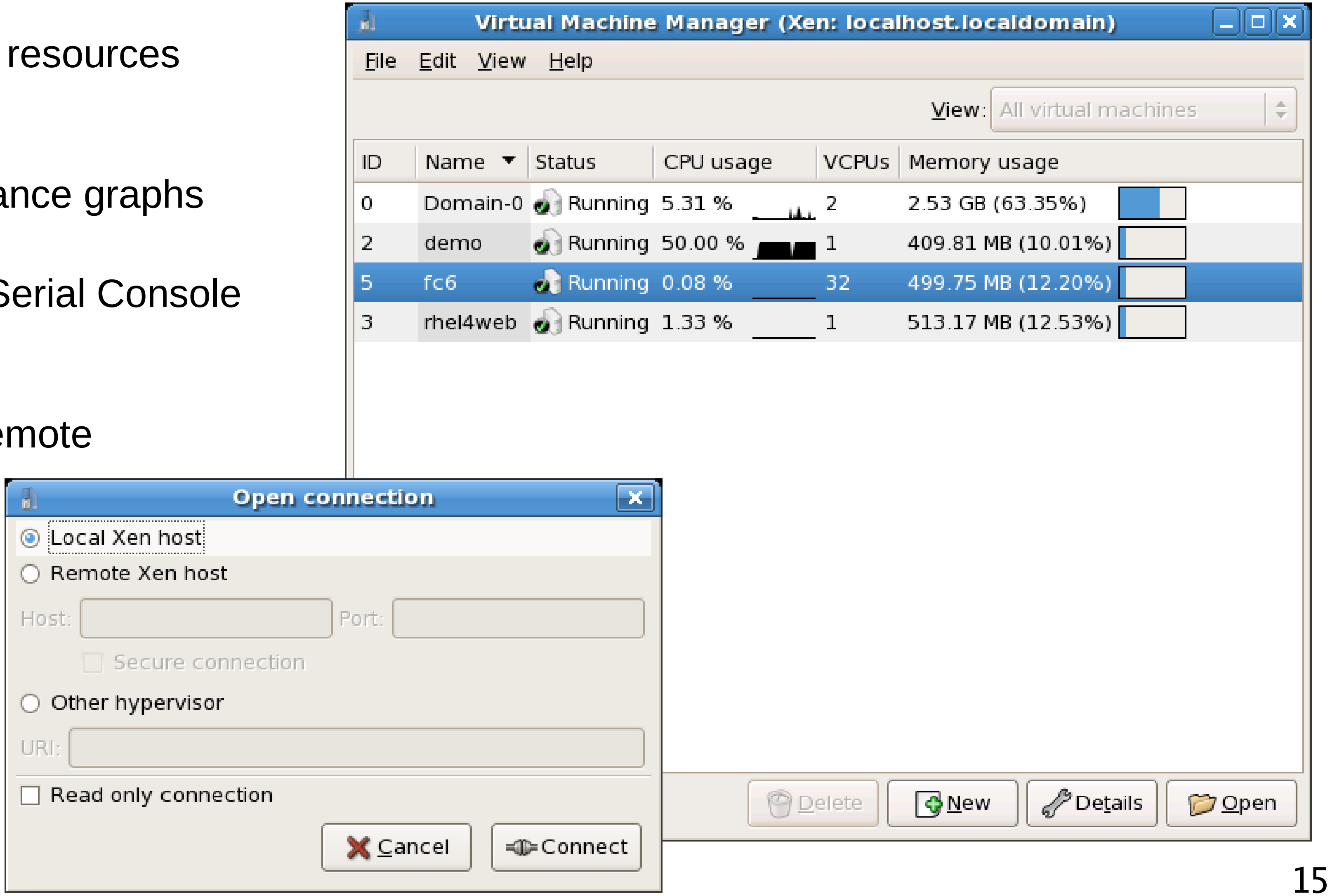
Introduction to libvirt API

- 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 virt-manager

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



Virtual Machine Manager (Xen: localhost.localdomain)

ID	Name	Status	CPU usage	VCPUs	Memory usage
0	Domain-0	Running	5.31 %	2	2.53 GB (63.35%)
2	demo	Running	50.00 %	1	409.81 MB (10.01%)
5	fc6	Running	0.08 %	32	499.75 MB (12.20%)
3	rhel4web	Running	1.33 %	1	513.17 MB (12.53%)

Open connection

● Local Xen host

○ Remote Xen host

Host: Port:

□ Secure connection

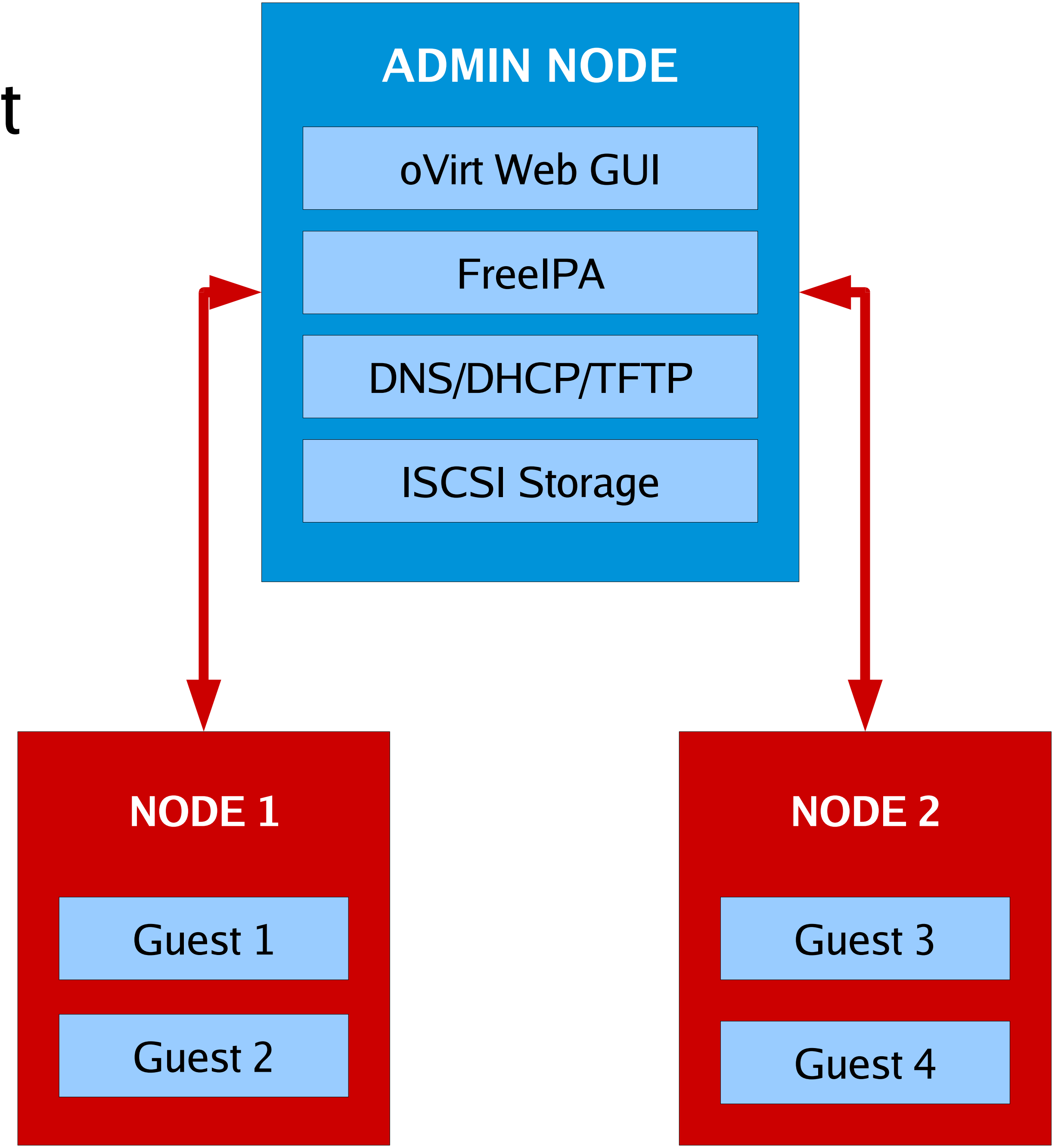
○ Other hypervisor

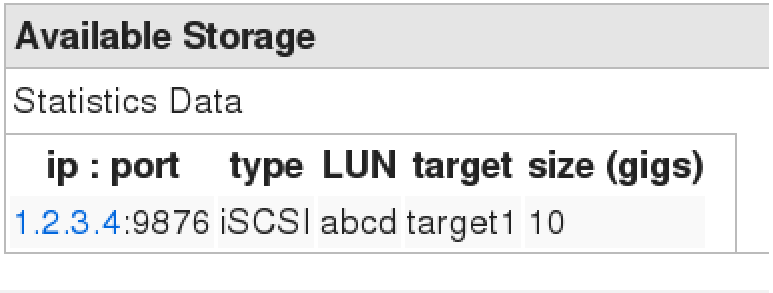
URI:

□ Read only connection

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

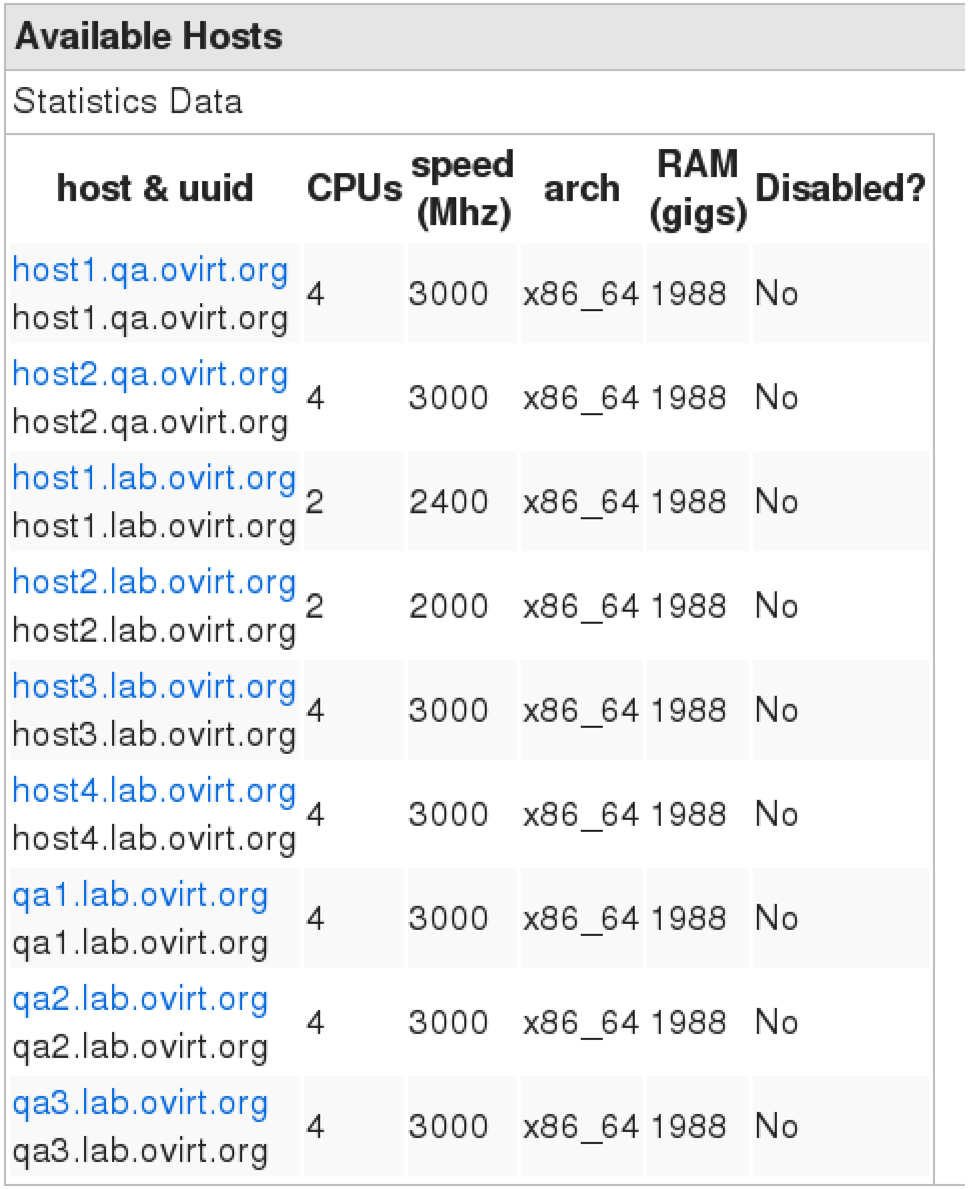




Available Storage

Statistics Data

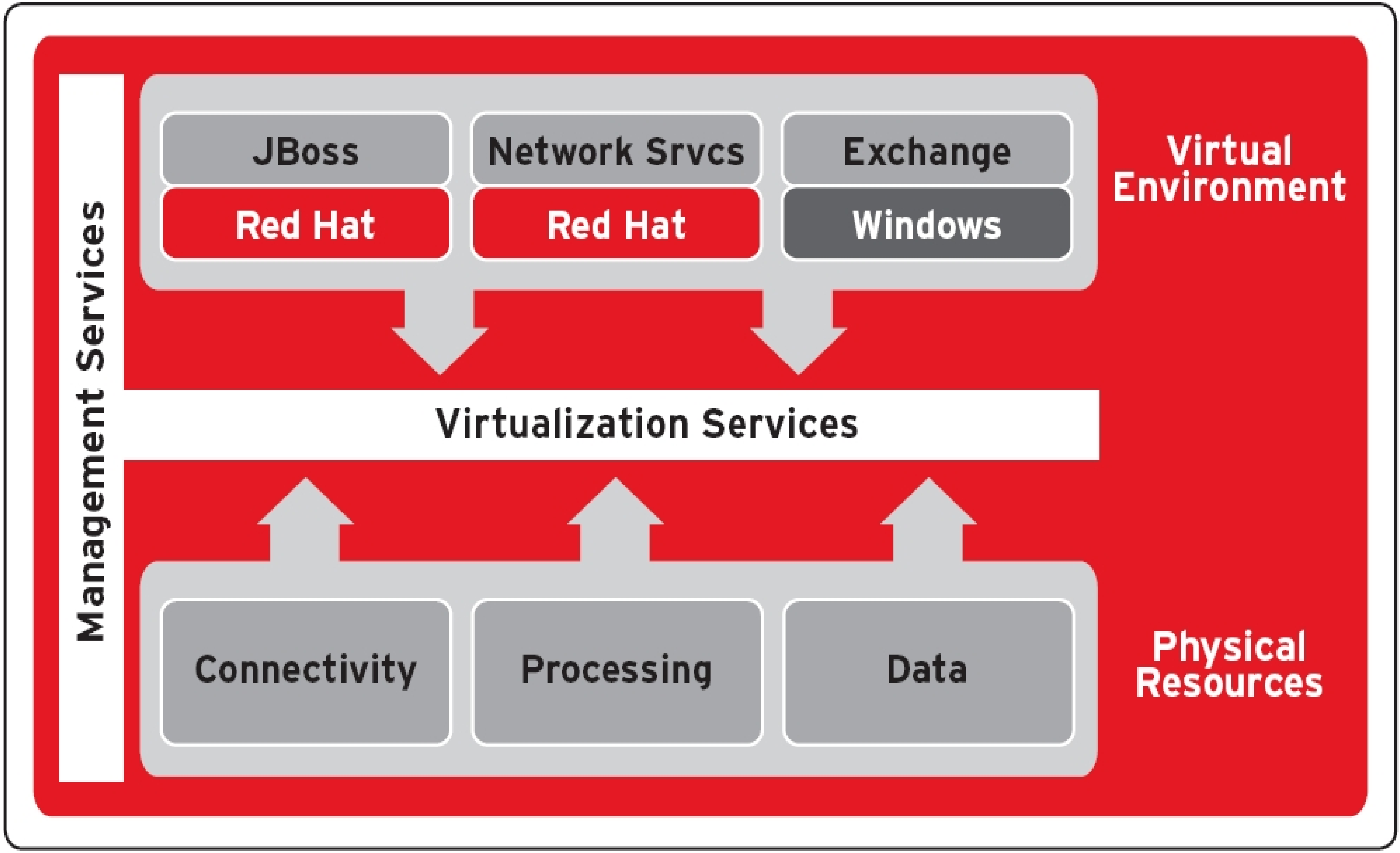
ip : port	type	LUN	target	size (gigs)
1.2.3.4:9876	iSCSI	abcd	target1	10

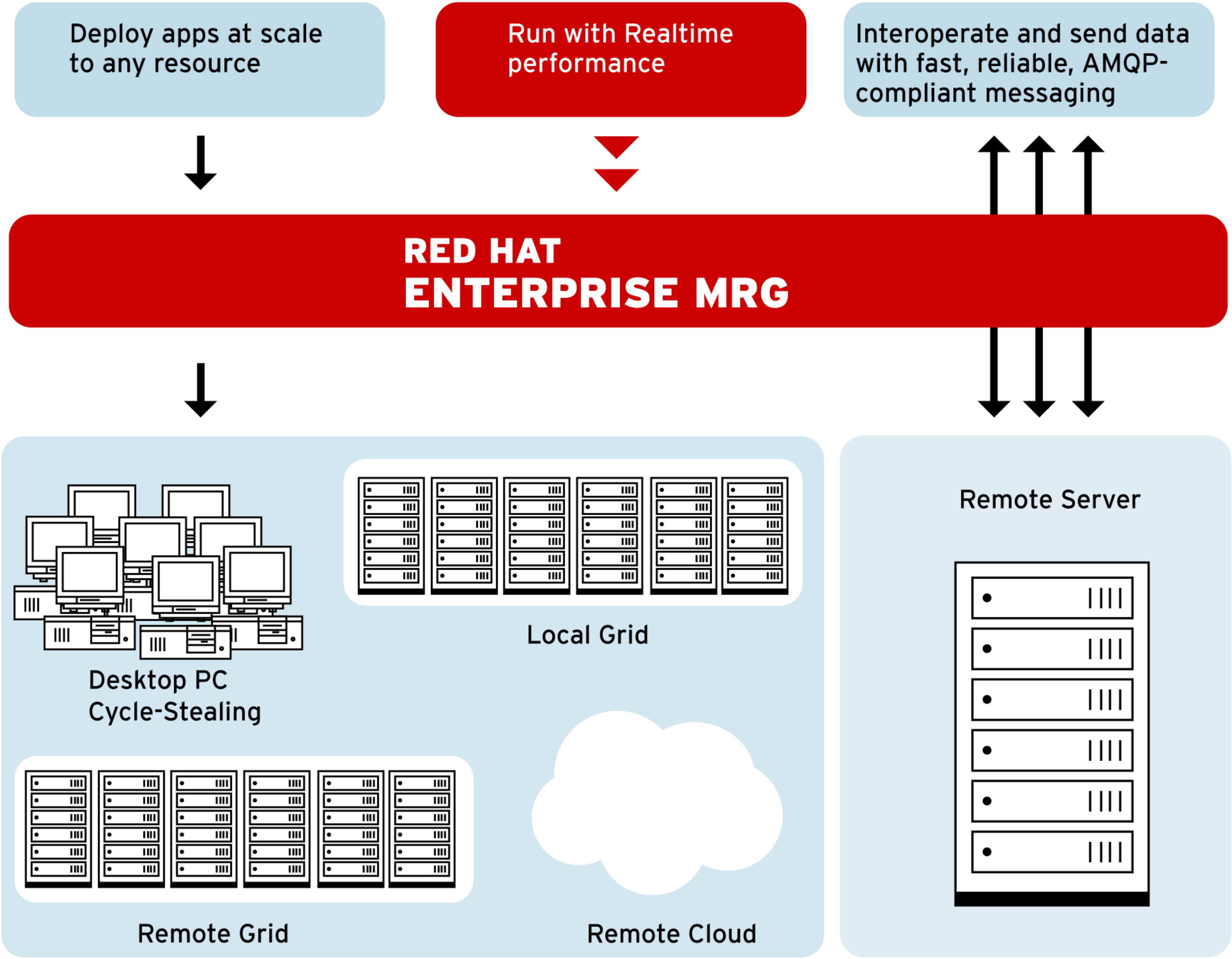


Available Hosts

Statistics Data

host & uuid	CPUs	speed (Mhz)	arch	RAM (gigs)	Disabled?
host1.qa.ovirt.org host1.qa.ovirt.org	4	3000	x86_64	1988	No
host2.qa.ovirt.org host2.qa.ovirt.org	4	3000	x86_64	1988	No
host1.lab.ovirt.org host1.lab.ovirt.org	2	2400	x86_64	1988	No
host2.lab.ovirt.org host2.lab.ovirt.org	2	2000	x86_64	1988	No
host3.lab.ovirt.org host3.lab.ovirt.org	4	3000	x86_64	1988	No
host4.lab.ovirt.org host4.lab.ovirt.org	4	3000	x86_64	1988	No
qa1.lab.ovirt.org qa1.lab.ovirt.org	4	3000	x86_64	1988	No
qa2.lab.ovirt.org qa2.lab.ovirt.org	4	3000	x86_64	1988	No
qa3.lab.ovirt.org qa3.lab.ovirt.org	4	3000	x86_64	1988	No


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



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: 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

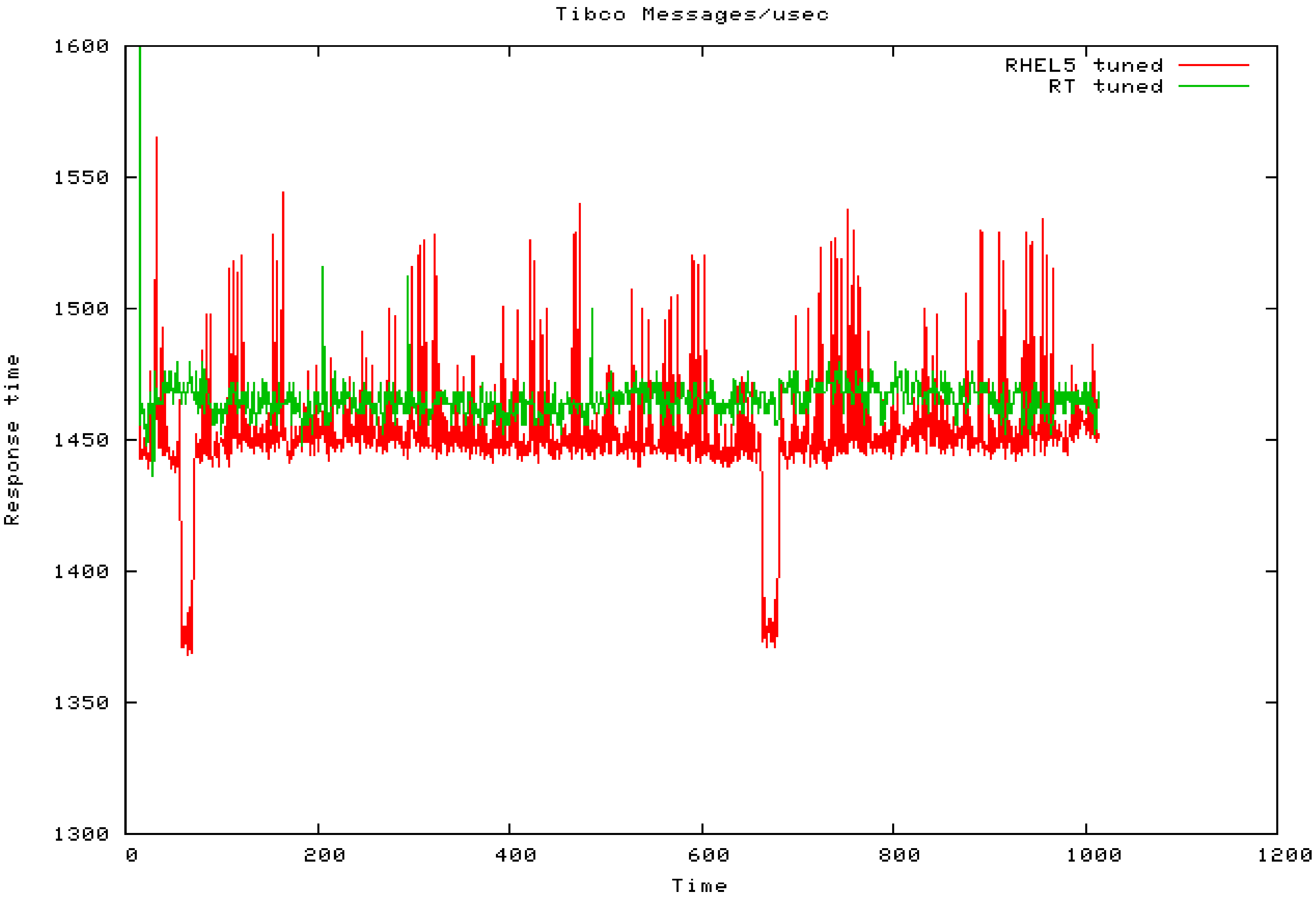
MRG Realtime

- **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


Tibco Messages/usec
RHEL5 tuned
RT tuned
Response time
1600
1550
1500
1450
1400
1350
1300
0
200
400
600
800
1000
1200
Time

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

Condor High Throughput Computing

- 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

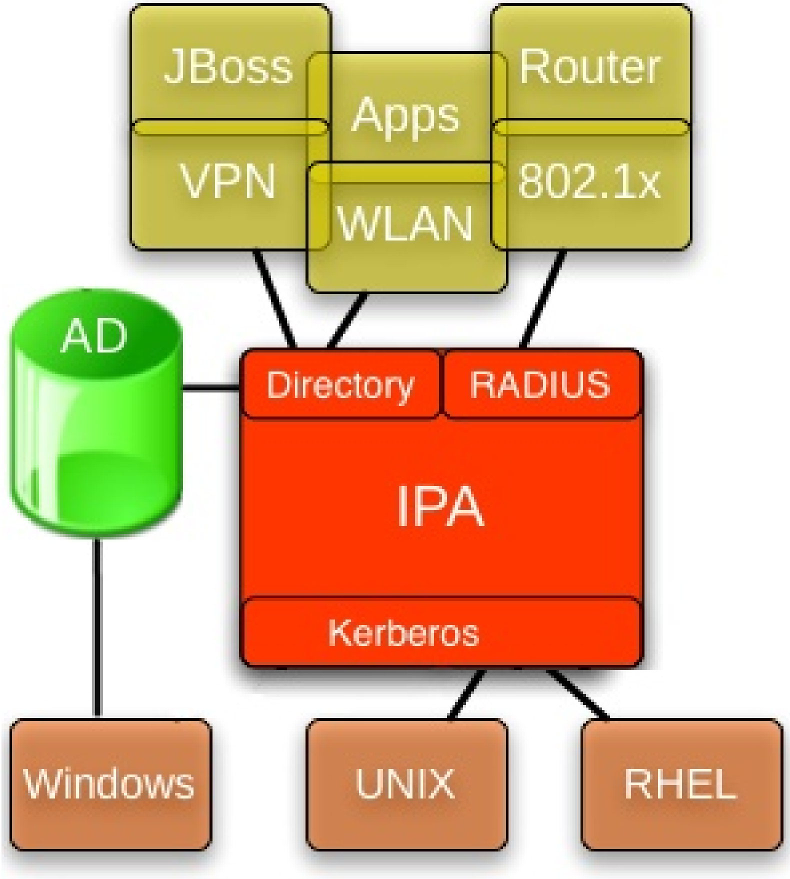
- Unite Directory, Kerberos, RADIUS servers, SAMBA
- From Apps, UNIX/Linux, VPNs, WLANs

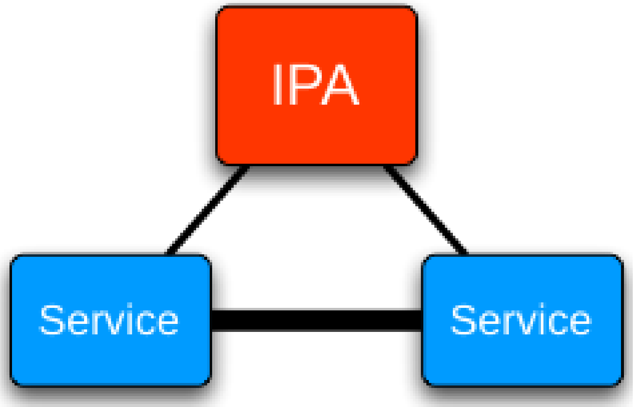
Easy for IT to set up, migrate to, and manage

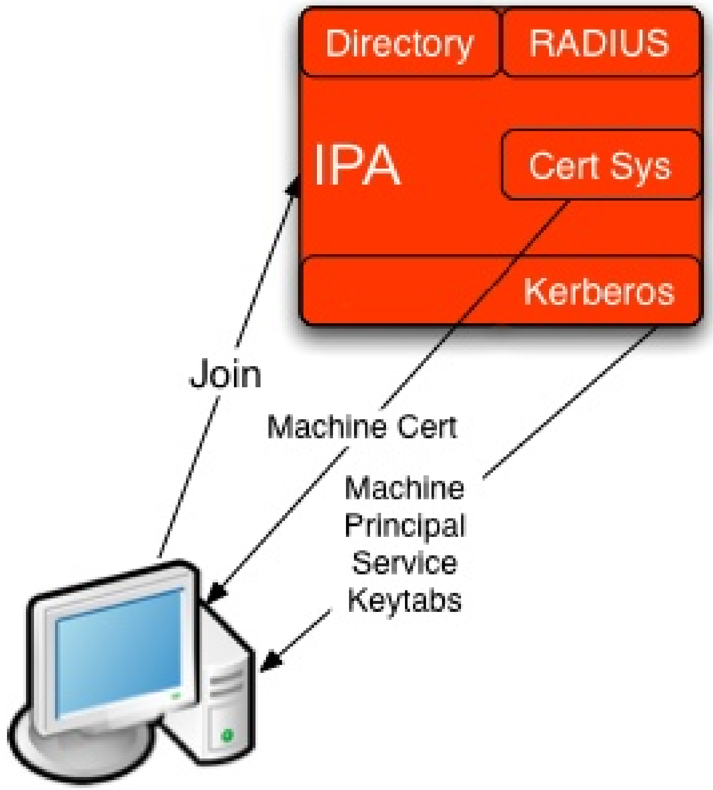
- Simple IPA install
- Intuitive web interface, Command line
- Tools migrate from NIS

Key Data replicated via Directory

Process identity via a Kerberos principal







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

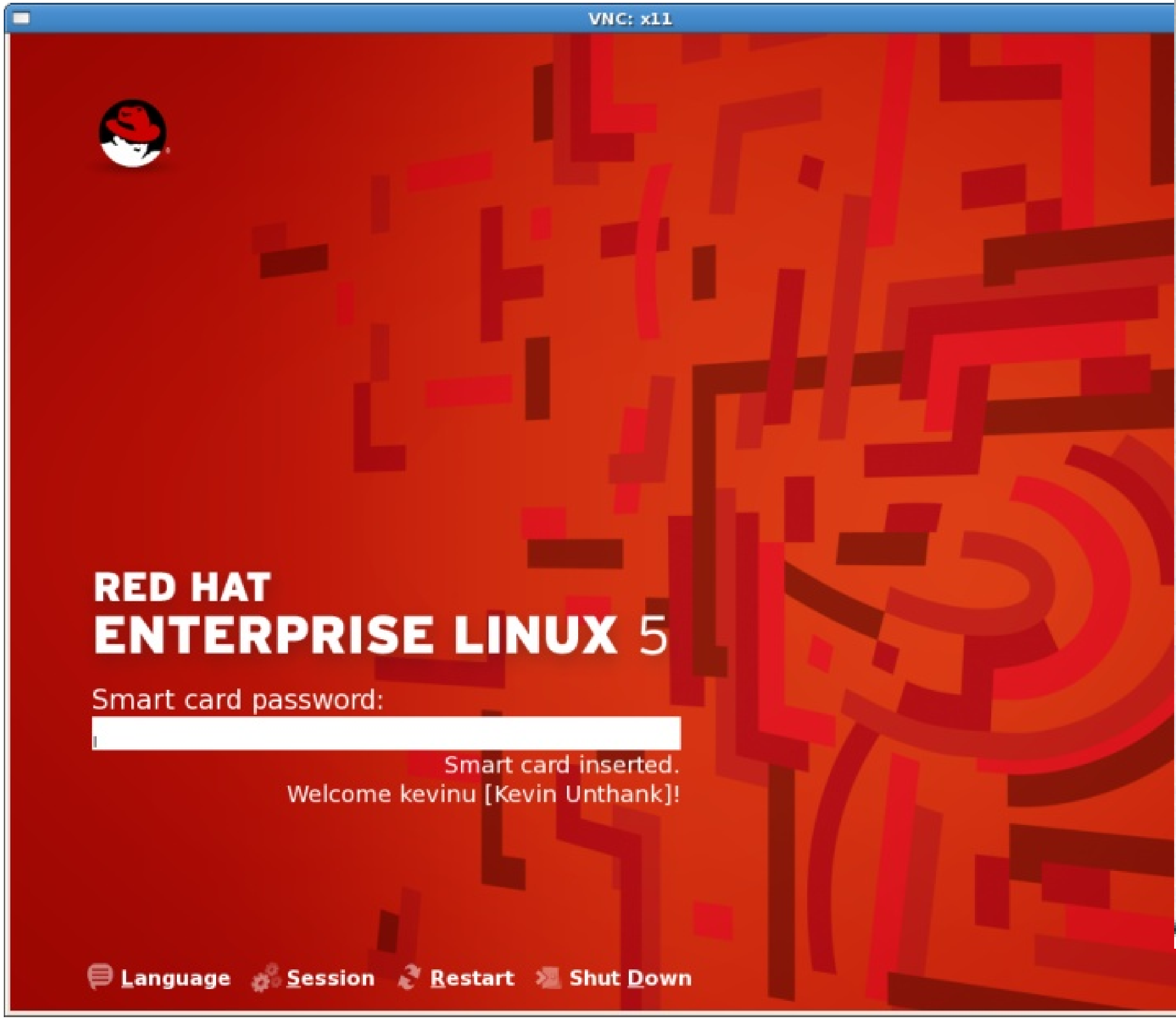
Centrally managed access control

- 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

RHEL5 Security: Smart Card Support



VNC: x11

RED HAT
ENTERPRISE LINUX 5

Smart card password:

Smart card inserted.
Welcome kevinu [Kevin Unthank]!

United States Government

JAN2009

Affiliation
Uniformed Services

Agency/Department
Army

Expires
2009JAN18

Doe,
John, G.

Pay Grade
E05

Rank
SGT

Geneva Conventions Identification Card

Questions?

SELinux

A Wonderland of Obscure Subsystems

Access Control Mechanisms (ACMs)

- Control which users and processes can access different files, devices, interfaces, etc., in a computer system.

- This is a primary consideration when securing a computer system or network of any size.

  - Discretionary Access Control (DAC)
  - Access Control Lists (ACLs)
  - SELinux
    - Mandatory Access Control (MAC)
    - Role-Based Access Control (RBAC)
    - Multi-Level Security (MLS)

Discretionary Access Controls (DAC)

- Basic access controls for objects in a filesystem
- Typical access control provided by file permissions, sharing, etc
- Access is generally at the discretion of the owner of the object (file, directory, device, etc.).

```
# ls -L /demos/Harris/
```

Access Control Lists (ACLs)

- Evolution of DAC
- Delegate access decisions to specific user/groups/subsets
- -rw-rw-r--**+**

```
# sudo -u hr_worker cat HR_PayrollData
# setfacl -m u:hr_worker:r HR_PayrollData
# sudo -u hr_worker cat HR_PayrollData
```

SELinux Basics: Goals

- **Systems Must Be Tamperproof**

There must be no way for attackers or others on the system to intentionally or accidentally disable it or otherwise interfere with its operation

- **Systems Must Be Nonbypassable**

There must be no way to gain access to system resources except through mechanisms that use the reference monitor to make access control decisions

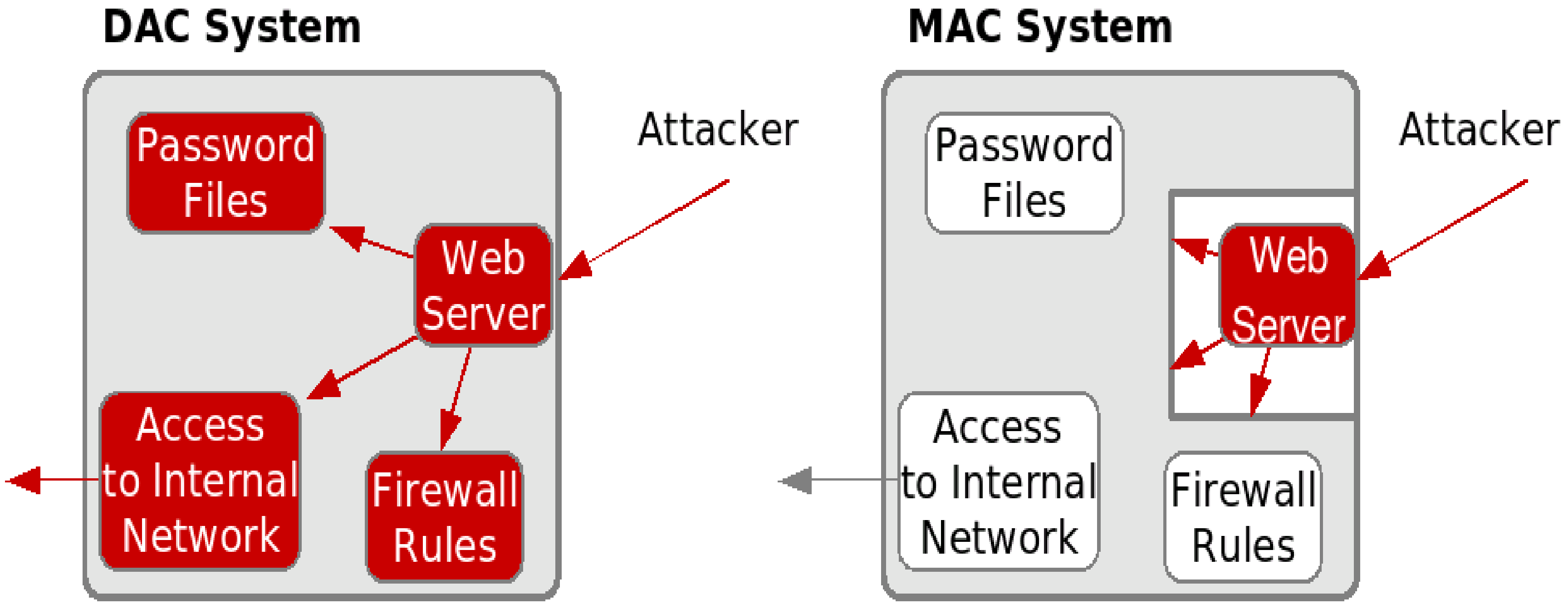
- **Access Must Be Verifiable**

There must be a way to convince third-party evaluators (i.e. Auditors) that the system will always enforce MLS correctly

- **No Covert Channels**

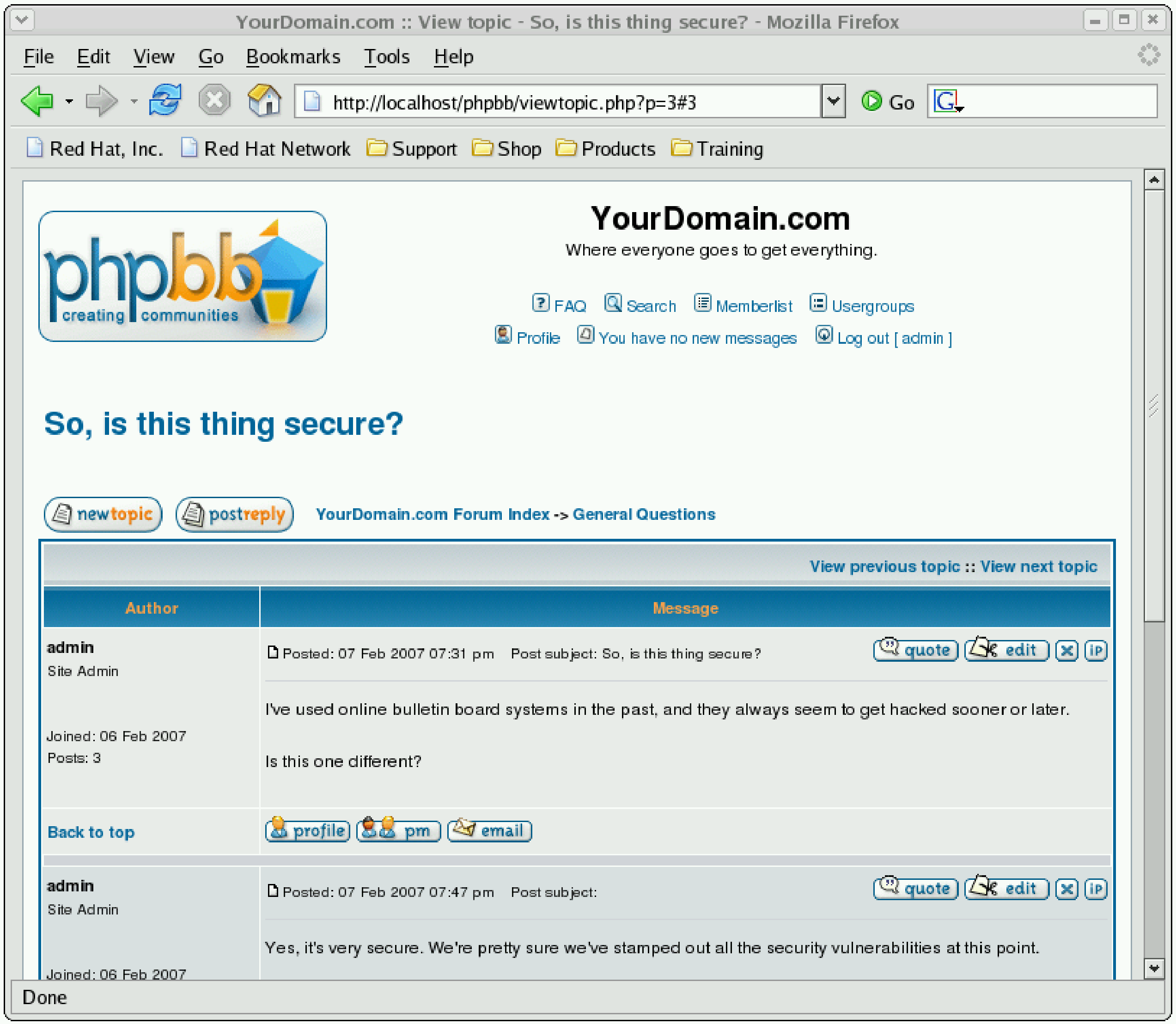
Eliminate footprints of other processes on the system (process threads, resource utilization, disk activities, etc)

SELinux Basics: MAC vs DAC



- DAC does not clearly separate the privileges of users and applications action on the users behalf, increasing the damage that can be caused by application exploits.

Recent SELinux Examples


YourDomain.com :: View topic - So, is this thing secure? - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://localhost/phpbb/viewtopic.php?p=3#3
Go
Red Hat, Inc.
Red Hat Network
Support
Shop
Products
Training
phpbb creating communities
FAQ
Search
Memberlist
Usergroups
Profile
You have no new messages
Log out [admin]
newtopic
postreply
quote
edit
profile
pm
email
Done

YourDomain.com

Where everyone goes to get everything.

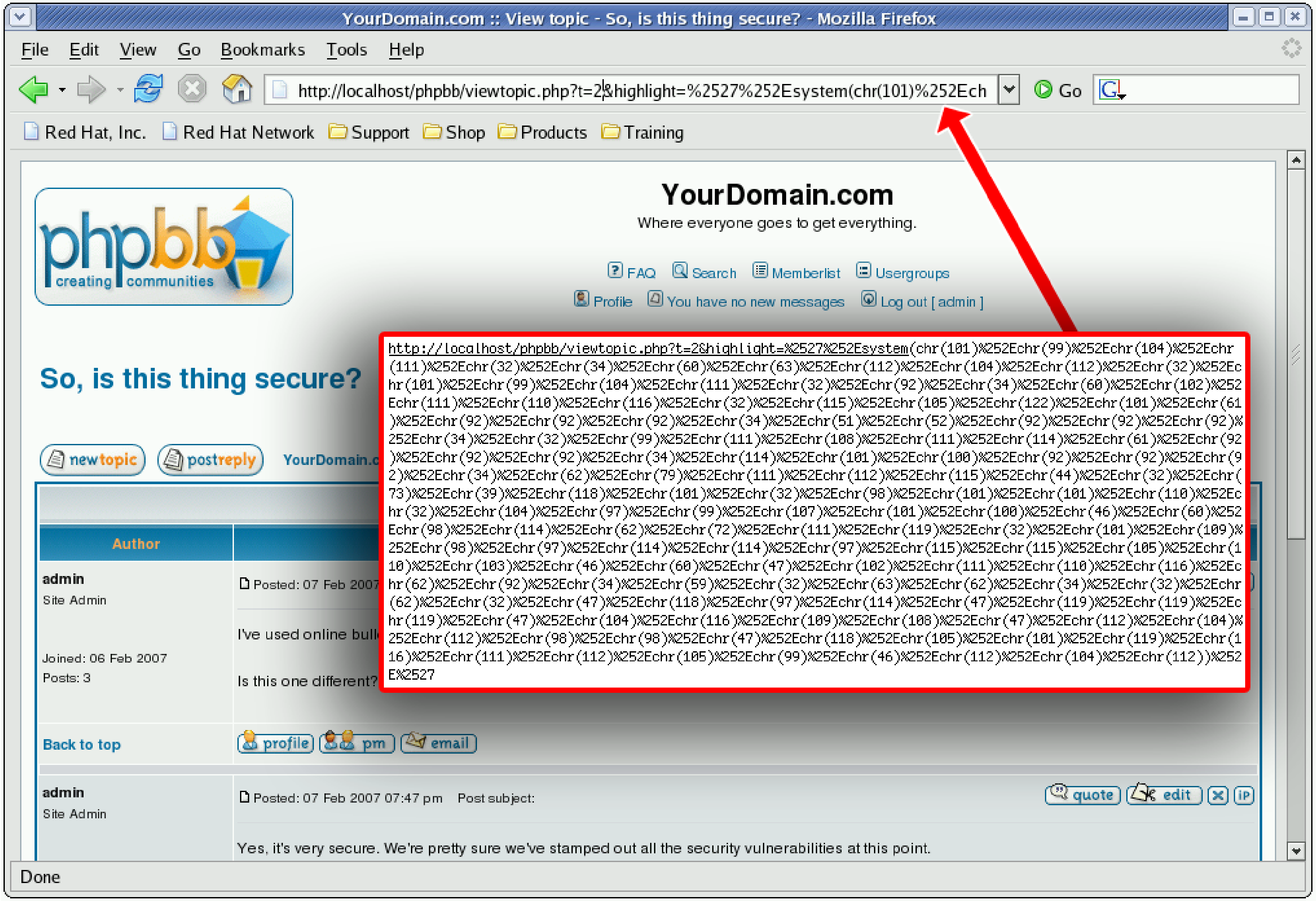
So, is this thing secure?

YourDomain.com Forum Index -> General Questions

View previous topic :: View next topic

Author	Message
admin Site Admin Joined: 06 Feb 2007 Posts: 3	Posted: 07 Feb 2007 07:31 pm Post subject: So, is this thing secure? I've used online bulletin board systems in the past, and they always seem to get hacked sooner or later. Is this one different?
Back to top	
admin Site Admin Joined: 06 Feb 2007	Posted: 07 Feb 2007 07:47 pm Post subject: Yes, it's very secure. We're pretty sure we've stamped out all the security vulnerabilities at this point.

Recent SELinux Examples



http://localhost/phpbb/viewtopic.php?t=2&highlight=%2527%252Esystem(chr(101)%252Ech

YourDomain.com

Where everyone goes to get everything.

So, is this thing secure?

YourDomain.c

```
http://localhost/phpbb/viewtopic.php?t=2&highlight=%2527%252Esystem(chr(101)%252Echr(99)%252Echr(104)%252Echr
(111)%252Echr(32)%252Echr(34)%252Echr(60)%252Echr(63)%252Echr(112)%252Echr(104)%252Echr(112)%252Echr(32)%252Ec
hr(101)%252Echr(99)%252Echr(104)%252Echr(111)%252Echr(32)%252Echr(92)%252Echr(34)%252Echr(60)%252Echr(102)%252
Echr(111)%252Echr(110)%252Echr(116)%252Echr(32)%252Echr(115)%252Echr(105)%252Echr(122)%252Echr(101)%252Echr(61
)%252Echr(92)%252Echr(92)%252Echr(92)%252Echr(34)%252Echr(51)%252Echr(52)%252Echr(92)%252Echr(92)%252Echr(92)%
252Echr(34)%252Echr(32)%252Echr(99)%252Echr(111)%252Echr(108)%252Echr(111)%252Echr(114)%252Echr(61)%252Echr(92
)%252Echr(92)%252Echr(92)%252Echr(34)%252Echr(114)%252Echr(101)%252Echr(100)%252Echr(92)%252Echr(92)%252Echr(9
2)%252Echr(34)%252Echr(62)%252Echr(79)%252Echr(111)%252Echr(112)%252Echr(115)%252Echr(44)%252Echr(32)%252Echr(
73)%252Echr(39)%252Echr(118)%252Echr(101)%252Echr(32)%252Echr(98)%252Echr(101)%252Echr(101)%252Echr(110)%252Ec
hr(32)%252Echr(104)%252Echr(97)%252Echr(99)%252Echr(107)%252Echr(101)%252Echr(100)%252Echr(46)%252Echr(60)%252
Echr(98)%252Echr(114)%252Echr(62)%252Echr(72)%252Echr(111)%252Echr(119)%252Echr(32)%252Echr(101)%252Echr(109)%
252Echr(98)%252Echr(97)%252Echr(114)%252Echr(114)%252Echr(97)%252Echr(115)%252Echr(115)%252Echr(105)%252Echr(1
10)%252Echr(103)%252Echr(46)%252Echr(60)%252Echr(47)%252Echr(102)%252Echr(111)%252Echr(110)%252Echr(116)%252Ec
hr(62)%252Echr(92)%252Echr(34)%252Echr(59)%252Echr(32)%252Echr(63)%252Echr(62)%252Echr(34)%252Echr(32)%252Echr
(62)%252Echr(32)%252Echr(47)%252Echr(118)%252Echr(97)%252Echr(114)%252Echr(47)%252Echr(119)%252Echr(119)%252Ec
hr(119)%252Echr(47)%252Echr(104)%252Echr(116)%252Echr(109)%252Echr(108)%252Echr(47)%252Echr(112)%252Echr(104)%
252Echr(112)%252Echr(98)%252Echr(98)%252Echr(47)%252Echr(118)%252Echr(105)%252Echr(101)%252Echr(119)%252Echr(1
16)%252Echr(111)%252Echr(112)%252Echr(105)%252Echr(99)%252Echr(46)%252Echr(112)%252Echr(104)%252Echr(112))%252
E%2527
```

admin
Site Admin

Joined: 06 Feb 2007
Posts: 3

Posted: 07 Feb 2007

I've used online bull

Is this one different?

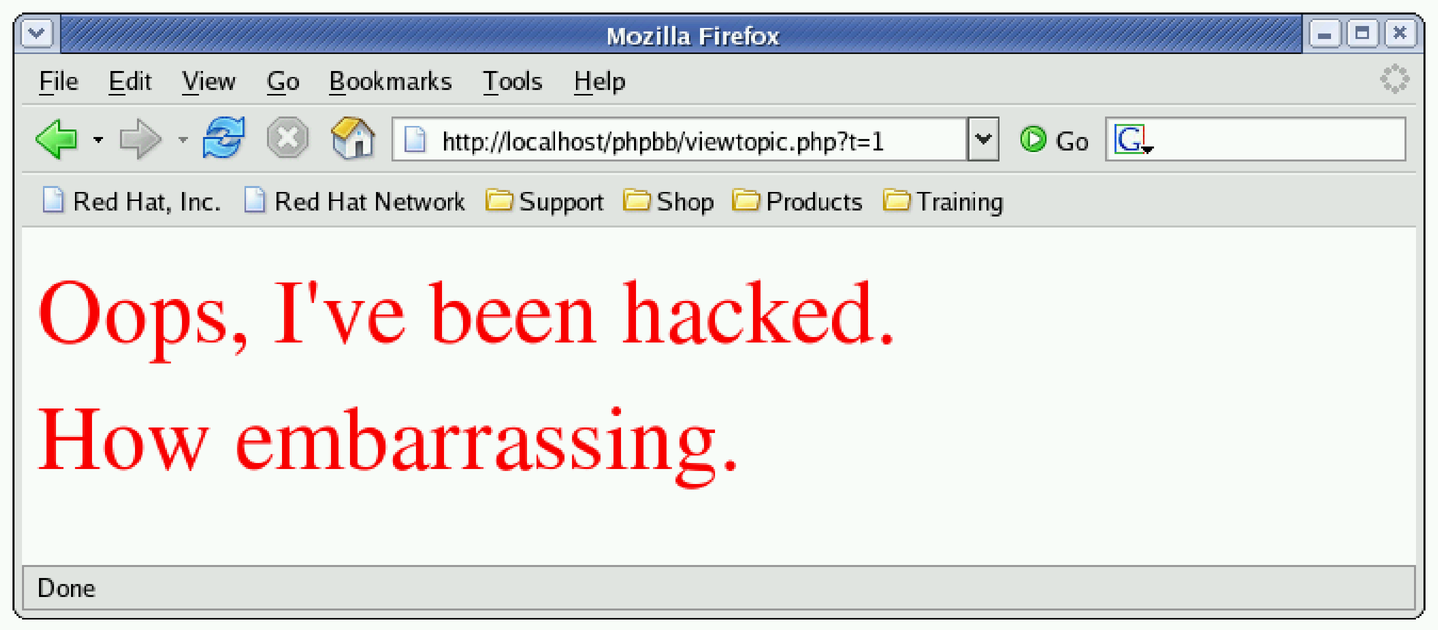
admin
Site Admin

Posted: 07 Feb 2007 07:47 pm Post subject:

Yes, it's very secure. We're pretty sure we've stamped out all the security vulnerabilities at this point.

Recent SELinux Examples

- The Result


Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://localhost/phpbb/viewtopic.php?t=1
Go
Red Hat, Inc. Red Hat Network Support Shop Products Training

Oops, I've been hacked.

How embarrassing.

Using SELinux...

- Apache should not be allowed to overwrite content
  - Therefore, Apache – and any program started by Apache – is not given write access to the data
  - SELinux constrains the program, regardless of the user running executable
  - The content is protected, even if the Apache PHP/CGI user owns the files
- When attacker uses the same exploit, with SELinux turned on:

```
Mar  3 23:02:04 rhel4-u4-as kernel: audit(1170820924.171:108):
  avc:  denied  { write } for  pid=26760 comm="sh"
  name="phpbb" dev=dm-0 ino=1114119
  scontext=root:system_r:httpd_sys_script_t
  tcontext=root:object_r:httpd_sys_content_t tclass=dir
```

Key Points

- The attack would have been prevented simply by turning SELinux on, without any further configuration!
- SELinux implements comprehensive control over all resources, including files, directories, devices, sockets, networking, IPC, etc.
- SELinux and Linux DAC are orthogonal (both security checks must pass)

SELinux Basics: RHEL5 Improvements

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

SELinux Basics: RHEL5 Improvements, *Cont*

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

SELinux Basics: RHEL5 Improvements, *Cont*

ExecShield

- Prevent any memory that was writable from becoming executable.
- Prevents an attacker fromwriting his code into memory and then executing it

Stack Smashing protection (Canary values)

- Places 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.

SELinux Basics: RHEL5 Improvements, *Cont*

FORTIFY_SOURCE GCC option

- 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.

Unconfined Memory

- Unconfined is a domain that was added to SELinux specifically to allow applications in this domain to run as if they were not running on an SELinux system.
- With RHEL5, memory protections have been added to the unconfined domain.

SELinux Compatible Applications

- SELinux can control all Linux applications.
- Since policy dictates how processes will access domains, all one needs to do is construct a policy for their application.
- Once the policy is constructed, it can be loaded, tested, and distributed with the application.

SELinux Basics: Policy Types

- **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

SELinux: Exploring Contexts

- All objects have a *security context*
  - `user:role:type[:sensitivity:category]`
  - Stored as extended attribute on the inode

User

- Strict: `audit_u`, `admin_u`, etc.
- Targeted: `root`, `system_u`, `user_u`

Role

- Targeted: files are `object_r`, processes are `system_r`

Type

- Type v. domain: `httpd_exec_t` v. `httpd_t`

- *Sensitivity*: s0-s15, aka “SystemLow-SystemHigh”
- *Category*: c0-c1023
  - Set math!

SELinux: Exploring Contexts

# ps -axZ

Notice context of ntpd, versus bash

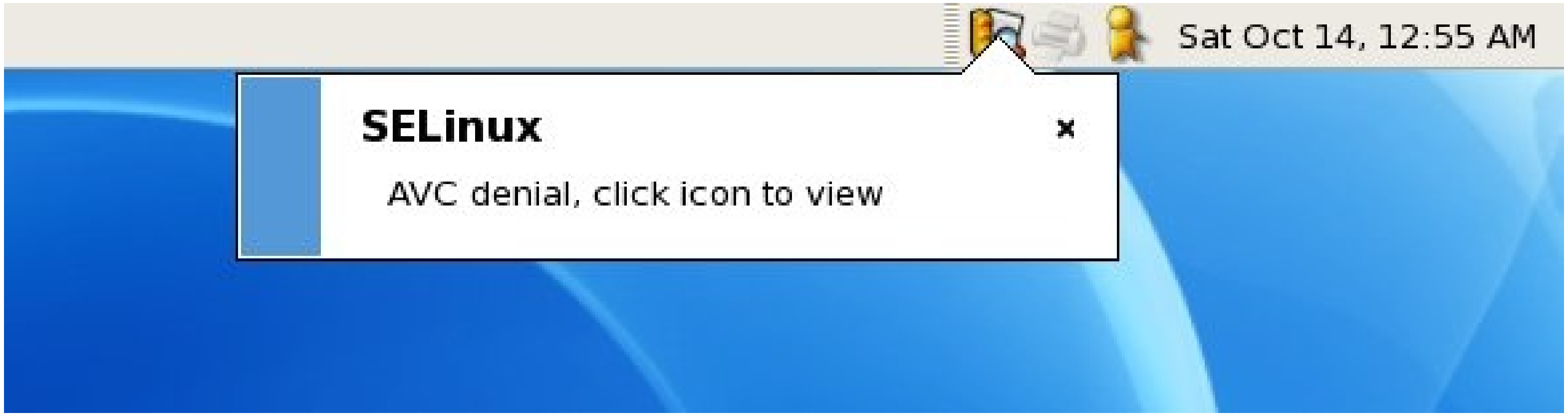
# ls -Z /home

Notice context of ntpd, versus bash

Apache Example

SELinux: End-User View

- sealert Notification

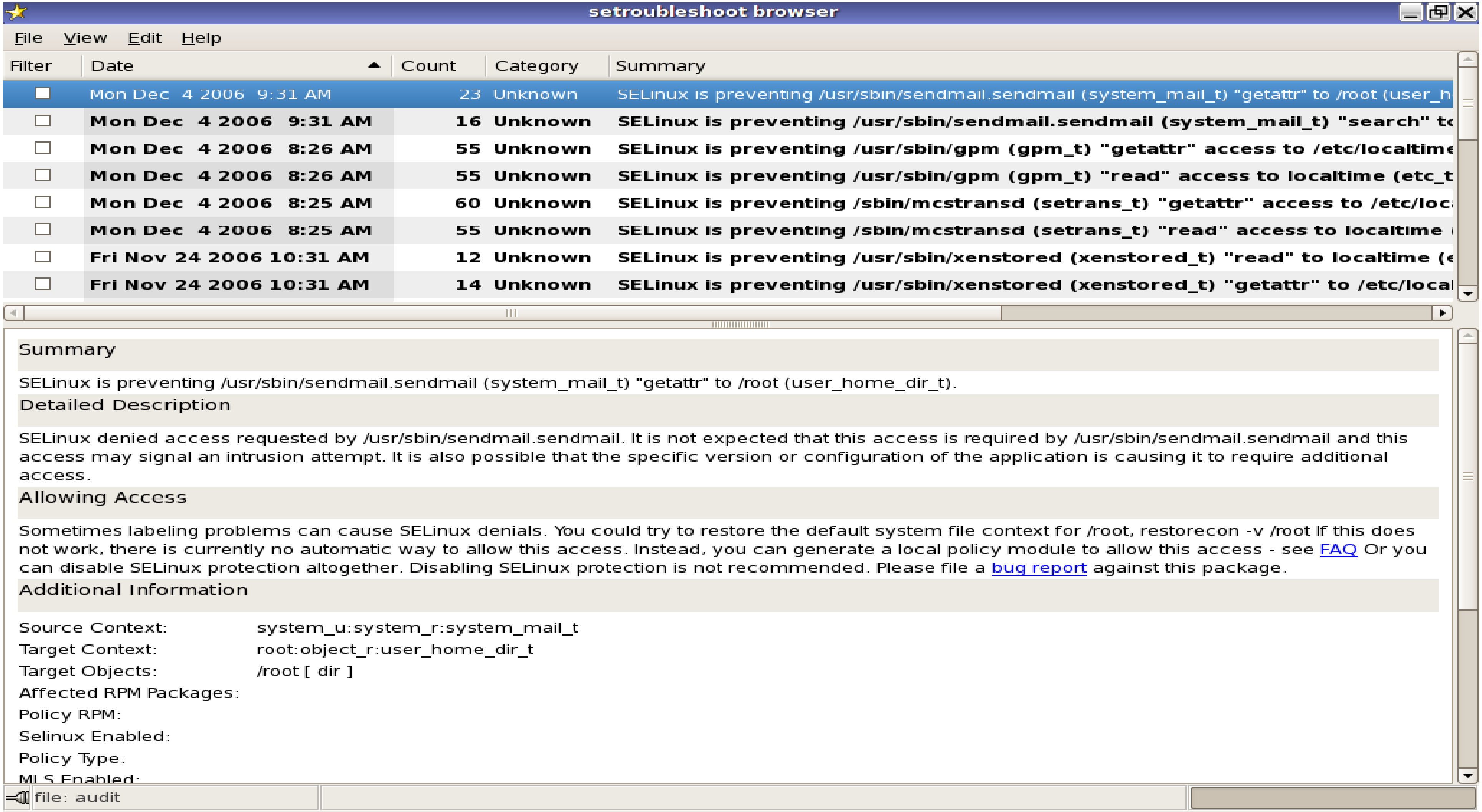


SELinux

AVC denial, click icon to view

SELinux: End-User View

- sealert Browser



Filter	Date	Count	Category	Summary
□	Mon Dec 4 2006 9:31 AM	23	Unknown	SELinux is preventing /usr/sbin/sendmail.sendmail (system_mail_t) "getattr" to /root (user_h
□	Mon Dec 4 2006 9:31 AM	16	Unknown	SELinux is preventing /usr/sbin/sendmail.sendmail (system_mail_t) "search" to
□	Mon Dec 4 2006 8:26 AM	55	Unknown	SELinux is preventing /usr/sbin/gpm (gpm_t) "getattr" access to /etc/localtime
□	Mon Dec 4 2006 8:26 AM	55	Unknown	SELinux is preventing /usr/sbin/gpm (gpm_t) "read" access to localtime (etc_t
□	Mon Dec 4 2006 8:25 AM	60	Unknown	SELinux is preventing /sbin/mcstransd (setrans_t) "getattr" access to /etc/loc
□	Mon Dec 4 2006 8:25 AM	55	Unknown	SELinux is preventing /sbin/mcstransd (setrans_t) "read" access to localtime (
□	Fri Nov 24 2006 10:31 AM	12	Unknown	SELinux is preventing /usr/sbin/xenstored (xenstored_t) "read" to localtime (e
□	Fri Nov 24 2006 10:31 AM	14	Unknown	SELinux is preventing /usr/sbin/xenstored (xenstored_t) "getattr" to /etc/local

Summary

SELinux is preventing /usr/sbin/sendmail.sendmail (system_mail_t) "getattr" to /root (user_home_dir_t).

Detailed Description

SELinux denied access requested by /usr/sbin/sendmail.sendmail. It is not expected that this access is required by /usr/sbin/sendmail.sendmail and this access may signal an intrusion attempt. It is also possible that the specific version or configuration of the application is causing it to require additional access.

Allowing Access

Sometimes labeling problems can cause SELinux denials. You could try to restore the default system file context for /root, restorecon -v /root If this does not work, there is currently no automatic way to allow this access. Instead, you can generate a local policy module to allow this access - see FAQ Or you can disable SELinux protection altogether. Disabling SELinux protection is not recommended. Please file a bug report against this package.

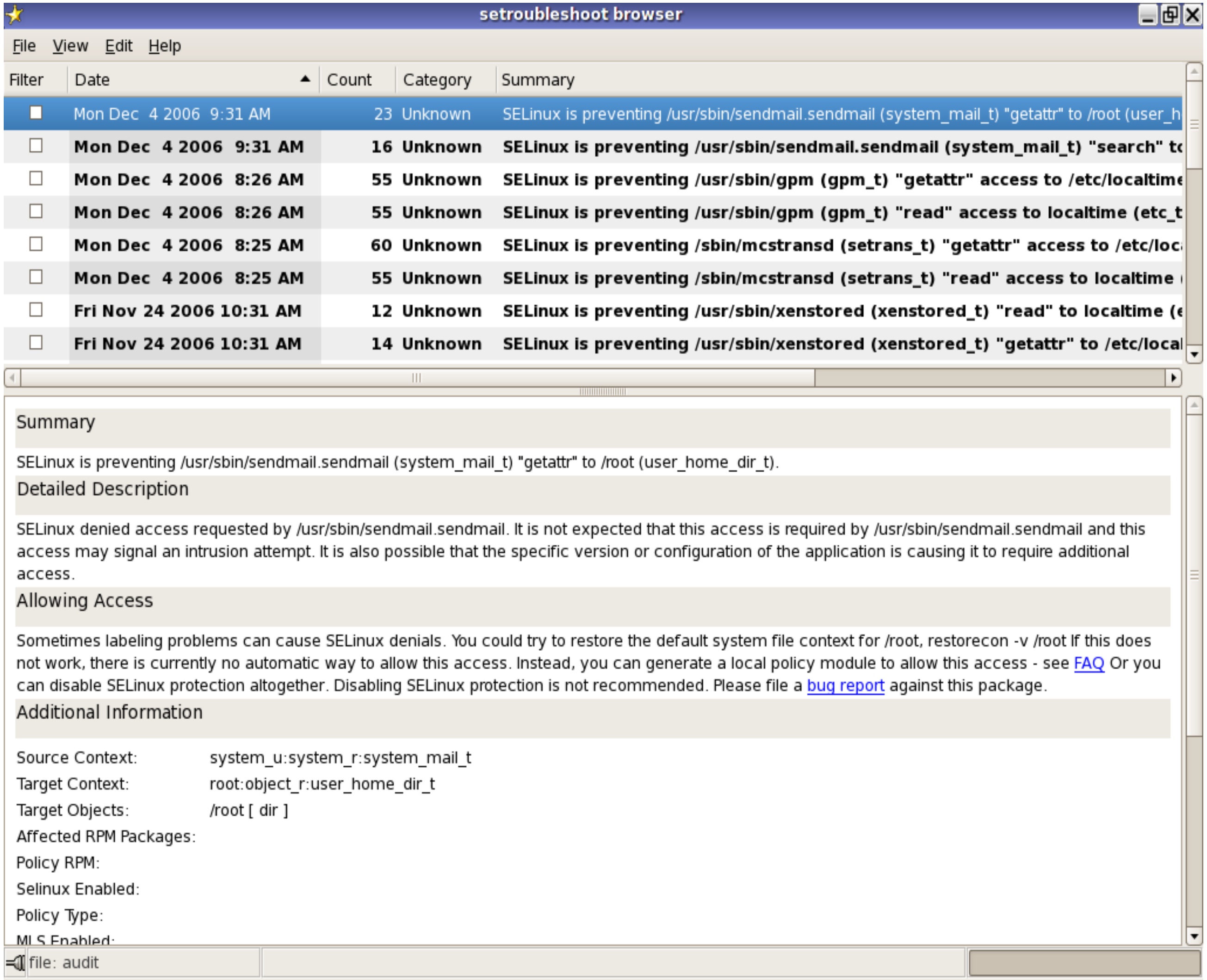
Additional Information

```
Source Context:          system_u:system_r:system_mail_t
Target Context:          root:object_r:user_home_dir_t
Target Objects:          /root [ dir ]
Affected RPM Packages:
Policy RPM:
Selinux Enabled:
Policy Type:
MLS Enabled:
```

file: audit

SELinux: System Administrator View

- sealert Browser



Filter	Date	Count	Category	Summary
☐	Mon Dec 4 2006 9:31 AM	23	Unknown	SELinux is preventing /usr/sbin/sendmail.sendmail (system_mail_t) "getattr" to /root (user_h
☐	Mon Dec 4 2006 9:31 AM	16	Unknown	SELinux is preventing /usr/sbin/sendmail.sendmail (system_mail_t) "search" to
☐	Mon Dec 4 2006 8:26 AM	55	Unknown	SELinux is preventing /usr/sbin/gpm (gpm_t) "getattr" access to /etc/localtime
☐	Mon Dec 4 2006 8:26 AM	55	Unknown	SELinux is preventing /usr/sbin/gpm (gpm_t) "read" access to localtime (etc_t
☐	Mon Dec 4 2006 8:25 AM	60	Unknown	SELinux is preventing /sbin/mcstransd (setrans_t) "getattr" access to /etc/loc
☐	Mon Dec 4 2006 8:25 AM	55	Unknown	SELinux is preventing /sbin/mcstransd (setrans_t) "read" access to localtime
☐	Fri Nov 24 2006 10:31 AM	12	Unknown	SELinux is preventing /usr/sbin/xenstored (xenstored_t) "read" to localtime (e
☐	Fri Nov 24 2006 10:31 AM	14	Unknown	SELinux is preventing /usr/sbin/xenstored (xenstored_t) "getattr" to /etc/local

Summary

SELinux is preventing /usr/sbin/sendmail.sendmail (system_mail_t) "getattr" to /root (user_home_dir_t).

Detailed Description

SELinux denied access requested by /usr/sbin/sendmail.sendmail. It is not expected that this access is required by /usr/sbin/sendmail.sendmail and this access may signal an intrusion attempt. It is also possible that the specific version or configuration of the application is causing it to require additional access.

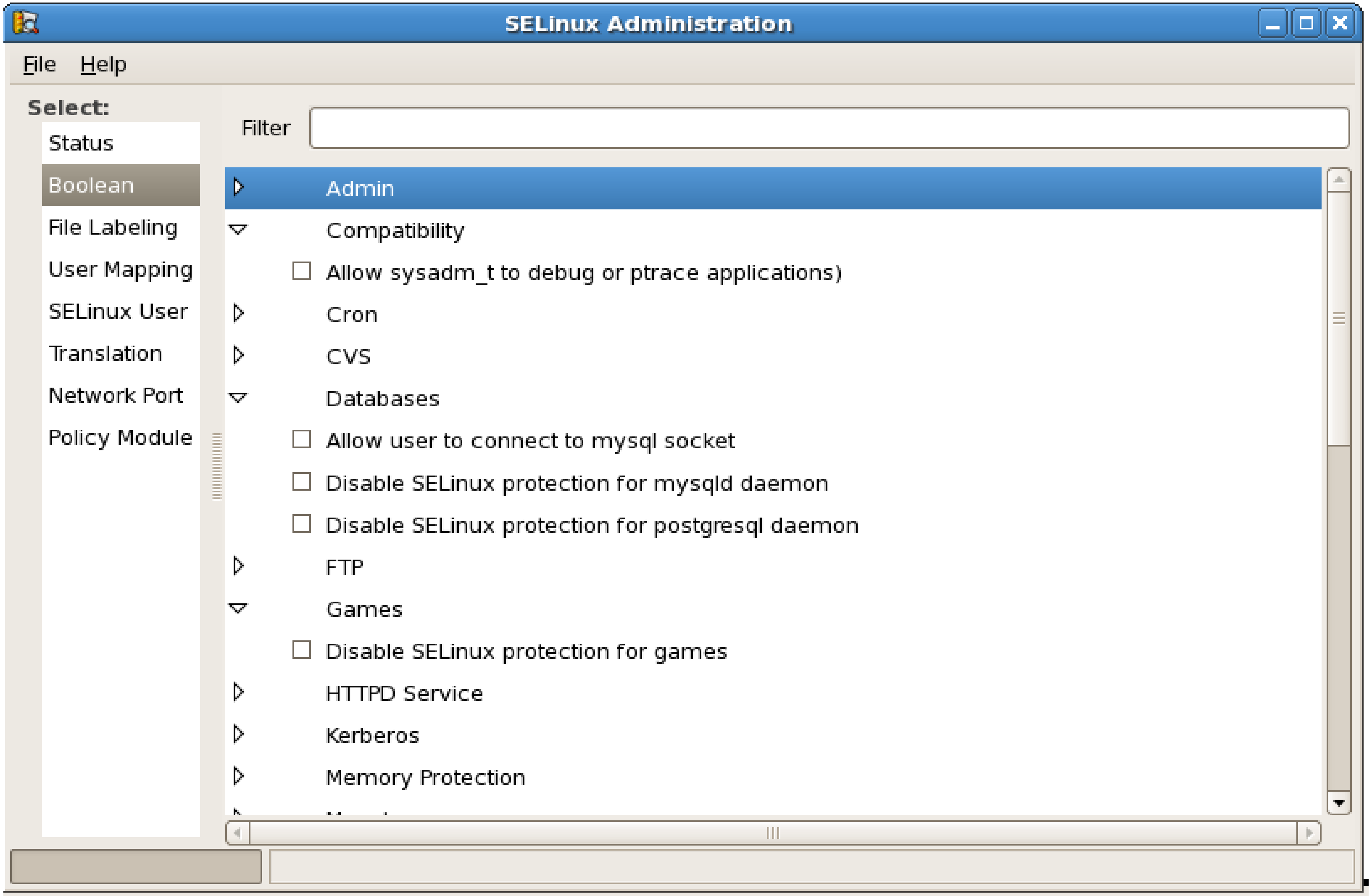
Allowing Access

Sometimes labeling problems can cause SELinux denials. You could try to restore the default system file context for /root, restorecon -v /root If this does not work, there is currently no automatic way to allow this access. Instead, you can generate a local policy module to allow this access - see FAQ Or you can disable SELinux protection altogether. Disabling SELinux protection is not recommended. Please file a bug report against this package.

Additional Information

Source Context:	system_u:system_r:system_mail_t
Target Context:	root:object_r:user_home_dir_t
Target Objects:	/root [dir]
Affected RPM Packages:	
Policy RPM:	
Selinux Enabled:	
Policy Type:	
MLS Enabled:	

SELinux: System Administrator View



▷ Admin

▽ Compatibility

□ Allow sysadm_t to debug or ptrace applications)

▷ Cron

▷ CVS

▽ Databases

□ Allow user to connect to mysql socket

□ Disable SELinux protection for mysqld daemon

□ Disable SELinux protection for postgresql daemon

▷ FTP

▽ Games

□ Disable SELinux protection for games

▷ HTTPD Service

▷ Kerberos

▷ Memory Protection

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

aide

- Intrusion Detection program
- Ships with RHEL5

```
# yum install aide
# aide –init
# chmod 777 /etc/hosts
# aide - -check

    AIDE found differences between database and filesystem!!
    Changed files:
    changed:/etc/hosts
    Detailed information about changes:

    File: /etc/hosts
    Permissions: -rw-r--r-- , -rwxrwxrwx
```

aide v auditd

- auditd built into RHEL
- Used in Common Criteria, DCID, STIG compliance

```
-a exit,possible -S chmod -F arch=${ARCH} -F success=0 -F success!=0

-a exit,always -S open -S pipe -S mkdir -S creat -F arch=${ARCH} -F success=0

-a exit,always -S rename -F arch=${ARCH} -F success!=0
```