Red Hat Update for System z

Shawn Wells

EMail: swells@redhat.com

Phone: (+1) 443 534 0130

Lead, Linux on System z

Agenda

- **Red Hat Intro & Company Overview**
- **Red Hat Technology Update**
  - **Enterprise Linux Update**
  - **Long Range Virtualization Plan**
  - **Security/MLS/Common Criteria**
- **System z Specifics**
  - **Hardware Exploitation**
  - **Roadmap**
- **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
- 85% Government/Commercial Linux Market Share
- 40+% Year over Year Growth (For 24 straight quarters)

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

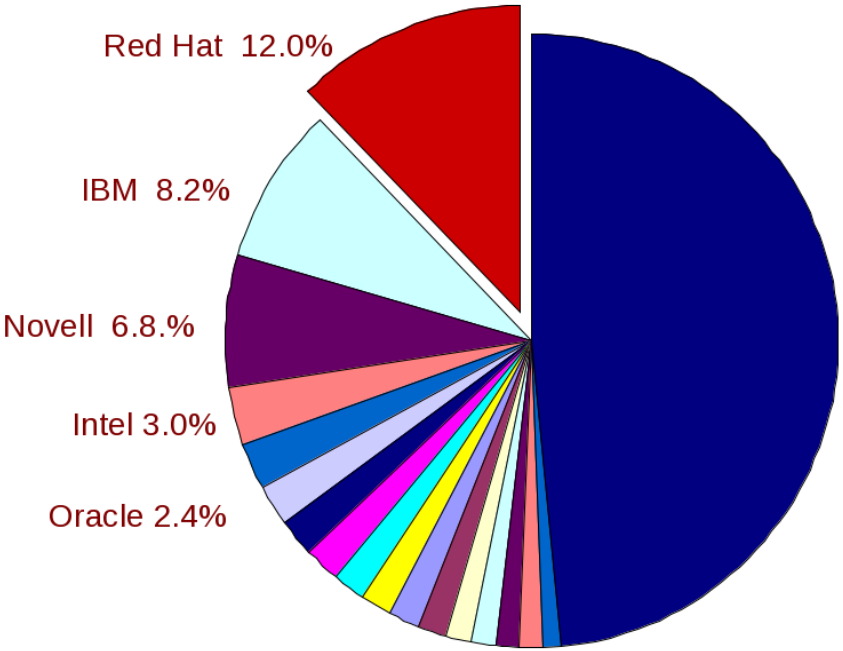
ASIA PACIFIC

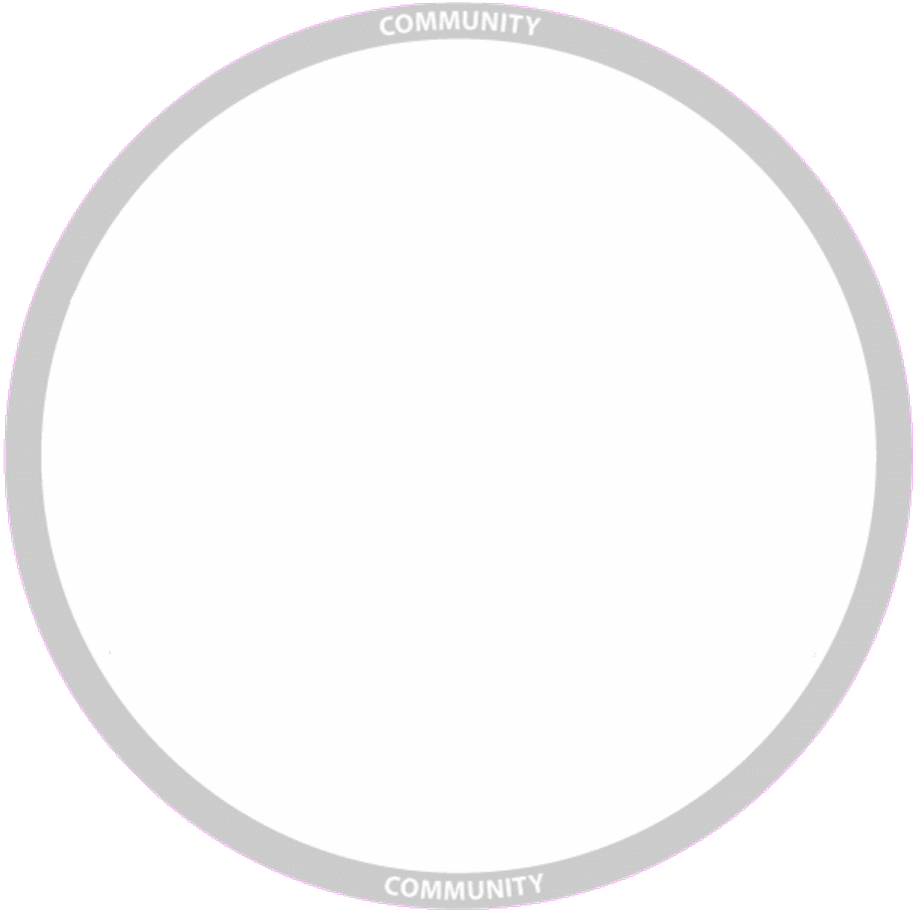
Brisbane
Melbourne
Sydney
Beijing
Guangzhou
Shanghai
Shenzhen
Hong Kong
Bangalore
Chennai
Kolkata
Mumbai
New Delhi
Pune
Tokyo
Seoul
Kuala Lumpur
Singapore
Sri Lanka

Red Hat Development Model

Community

- Development with “upstream” communities
- Kernel, glibc, etc
- Collaboration with partners, IBM, open source contributors

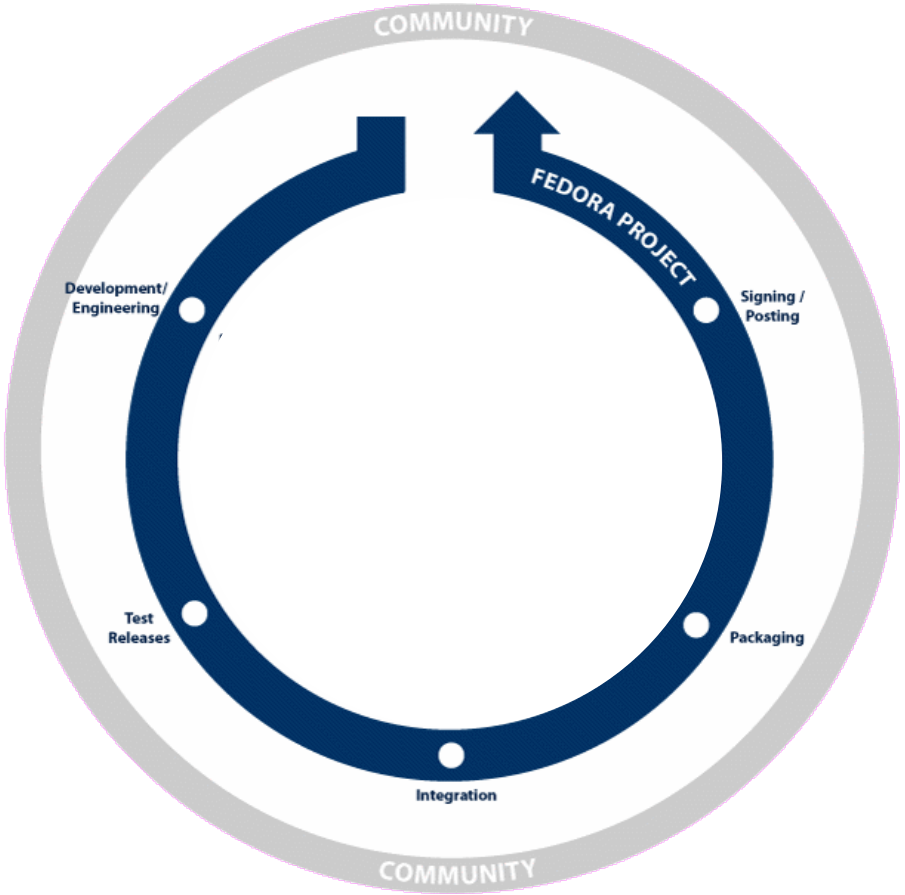




Red Hat Development Model

Fedora

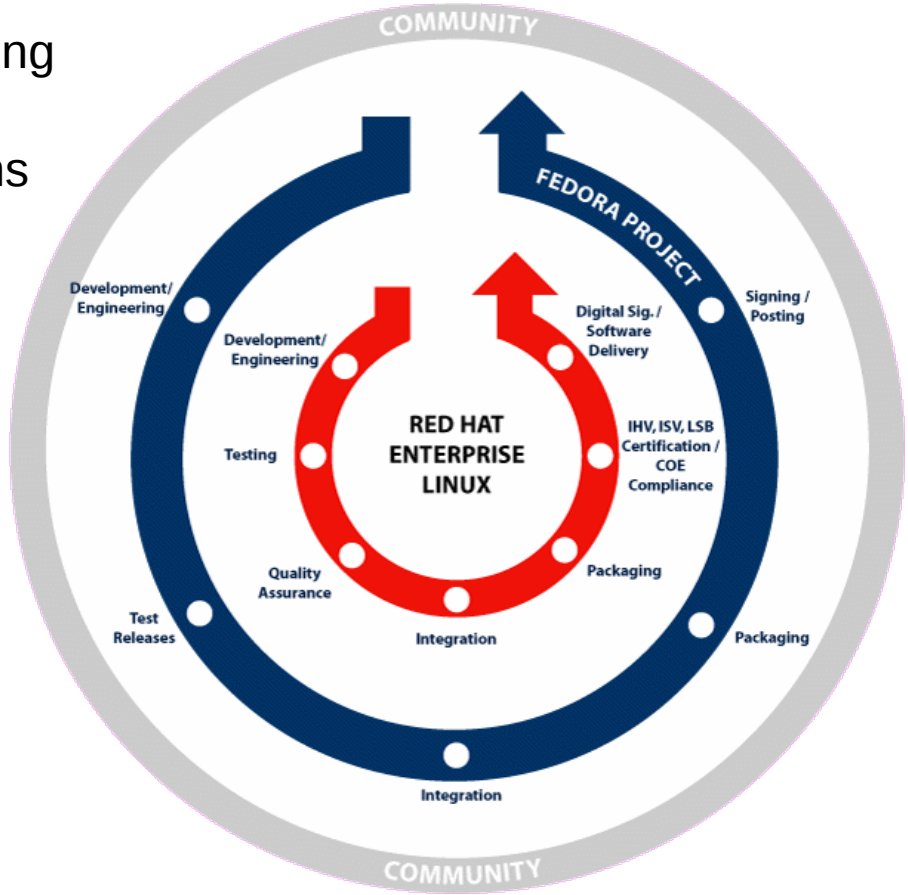
- Rapid innovation
- Latest technologies
- Community Supported
- Released ~6mo cycles



Red Hat Development Model

Red Hat Enterprise Linux

- Stable, mature, commercial product
- Extensive Q&A, performance testing
- Hardware & Software Certifications
- 7yr maintenance
- Core ABI compatibility guarantee
- Major releases 2-3yr cycle

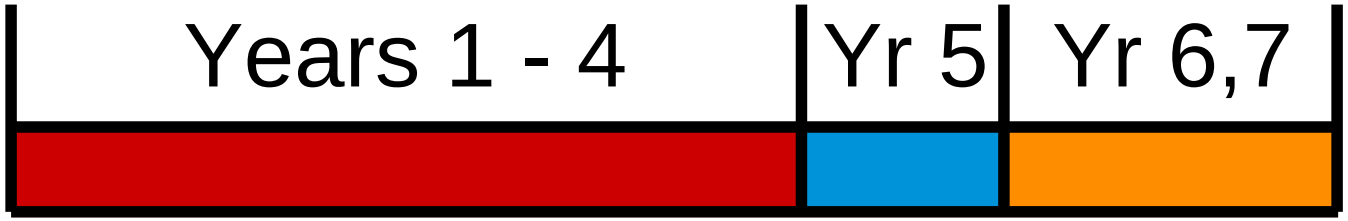


Fedora for System z

http://unc.rdu.redhat.com/fc9-s390x/

Support Cycle

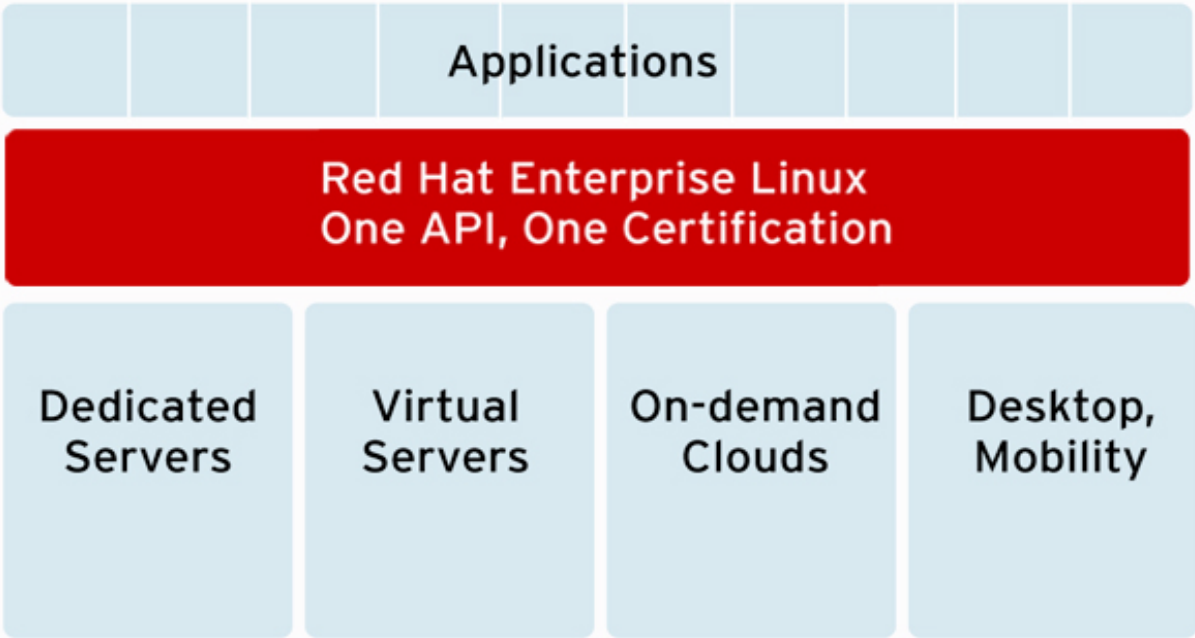
Extended Product Lifecycle



	Production 1	Production 2	Production 3
Security Patches	X	X	X
Bug Fixes	X	X	X
Hardware Enablement	**Full**	**Partial**	**None**
Software Enhancements	X		

CERTIFY ONCE, DEPLOY ANYWHERE

Reduces costs, complexity, administration, and management overhead.
Red Hat Enterprise Linux supported applications run everywhere.



Red Hat Enterprise Linux Update

RHEL Kernel Updates

- High resolution timers (2.6.16)
  - Provide fine resolution and accuracy depending on system configuration and capabilities - used for precise in-kernel timing
- Modular, on-the-fly switchable I/O schedulers (2.6.10)
  - Only provided as a boot option in RHEL4
  - Improved algorithms (esp. for CFQ)
  - Per-Queue selectable (previously system-wide)
- New Pipe implementation (2.6.11)
  - 30-90% perf improvement in pipe bandwidth
  - Circular buffer allow more buffering rather than blocking writers

Monitoring Features

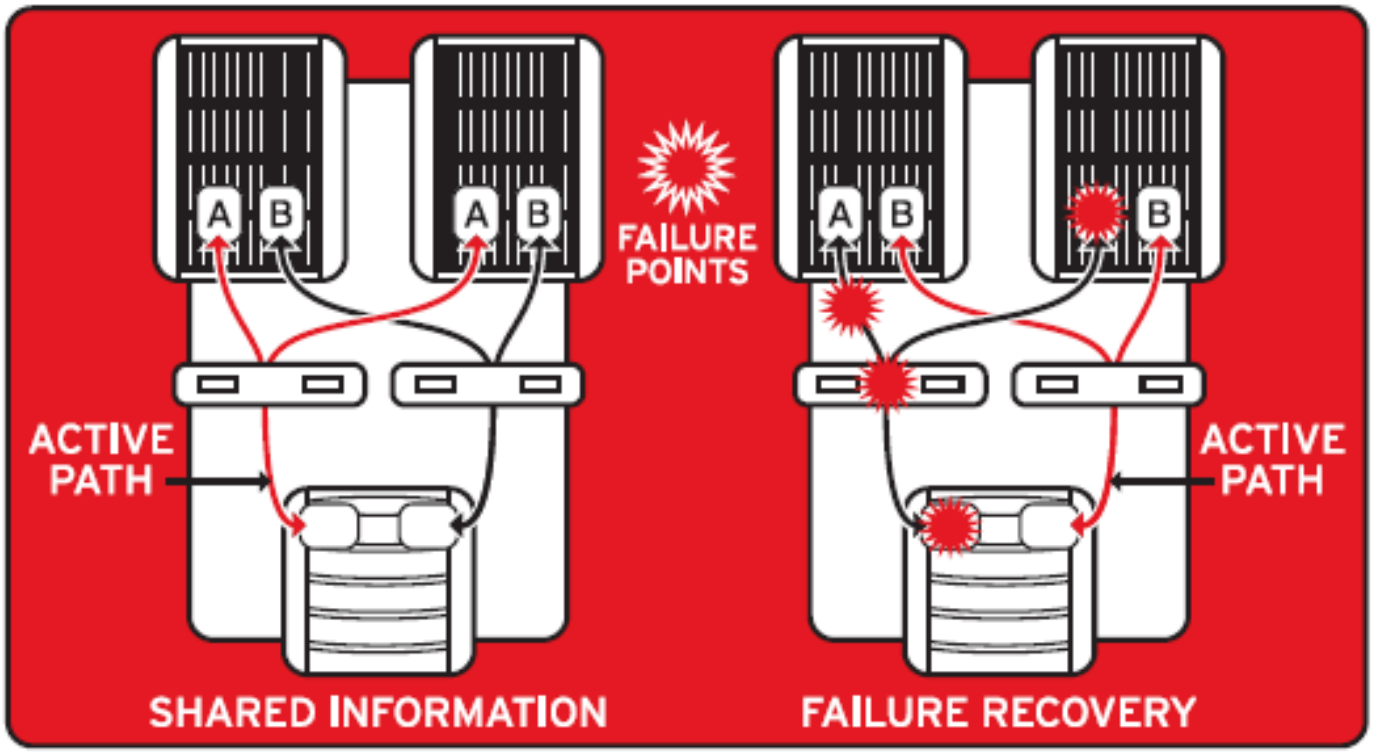
- Inotify (2.6.13)
  - New file system event monitoring mechanism (replaces dnotify)
  - Ideal for security and performance monitoring
- Process Events Connector (2.6.15)
  - Reports fork, exec, id change, and exit events for all processes to userspace
  - Useful for accounting/auditing (e.g. ELSA), system activity monitoring, security, and resource management
- Blktrace
  - Block queue IO tracing – monitor block device queue traffic (2.6.17)

File System Features

- EXT3
  - Ext3 block reservation & on-line growth (2.6.10 & RHEL4)
  - Extended Attributes in the body of large inode
    - Saves space and improves performance (2.6.11)
  - Increases maximum ext3 file-system size from 8TB to 16TB (2.6.18)
- ACL support for NFSv3 and NFSv4 (2.6.13)
- NFS
  - Support large reads and writes on the wire (2.6.16)
  - Linux NFS client supports transfer sizes up to 1MB
- ***Device mapper multipath support***

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



Security Features

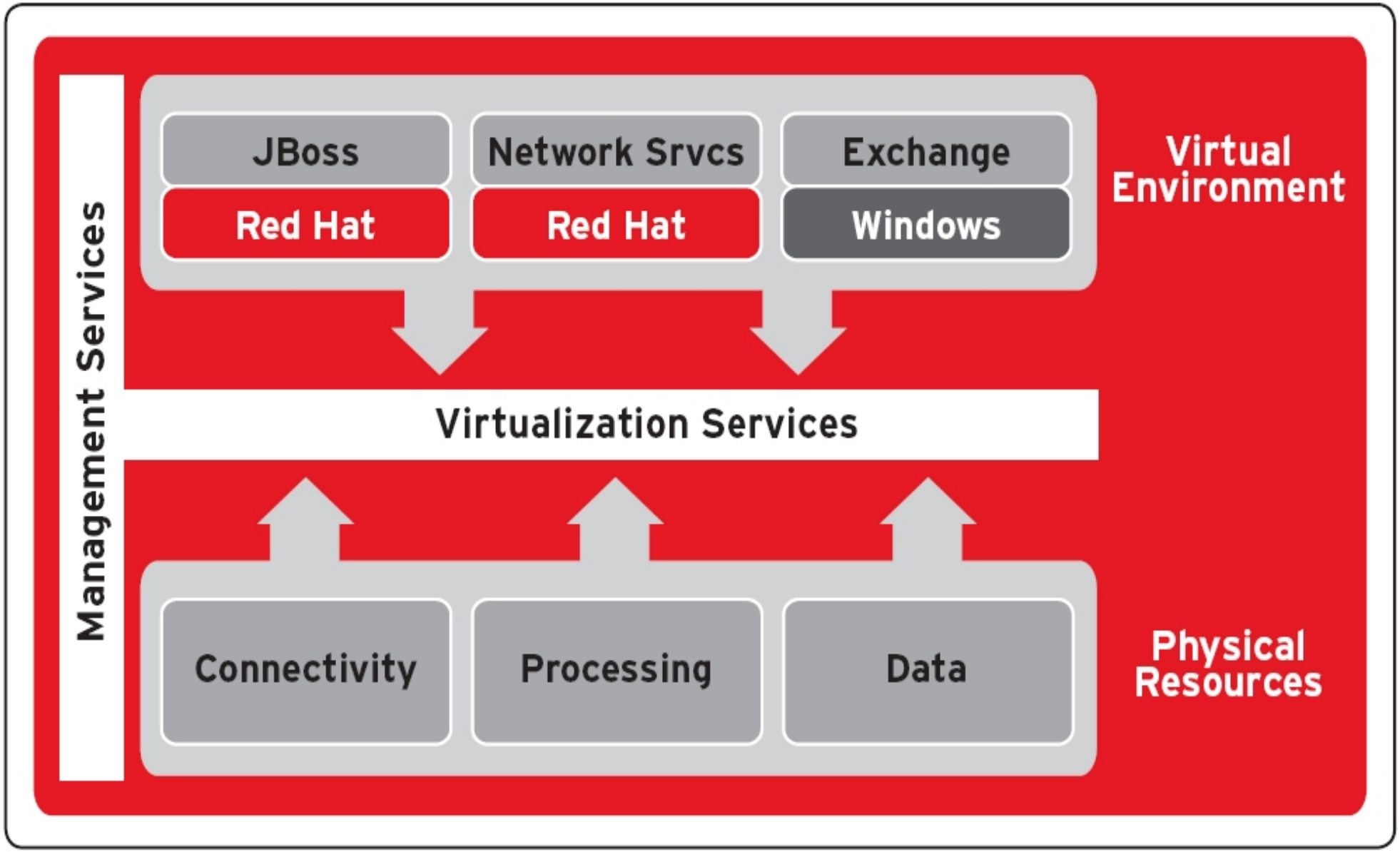
- Address space randomization:
  - Address randomization of multiple entities – including stack & mmap() region (used by shared libraries) (2.6.12; more complete implementation than in RHEL4)
  - Greatly complicates and slows down hacker attacks
- Multilevel security (MLS) implementation for SELinux (2.6.12)
  - Third policy scheme for SELinux, with RBAC & TE
- Audit subsytem
  - Support for process-context based filtering (2.6.17)
  - More filter rule comparators (2.6.17)
- TCP/UDP getpeersec
  - Enable a security-aware application to retrieve the security context of an IPSec security association a particular TCP or UDP socket in using (2.6.17)

Networking

- Add nf_conntrack subsystem: (2.6.15)
  - Common IPv4/IPv6 generic connection tracking subsystem
  - Allows IPv6 to have a stateful firewall capability (not previously possible)
    - Enables analysis of whole streams of packets, rather than only checking the headers of individual packets
- **SELinux per-packet access controls**
  - **Replaces old packet controls**
  - **Add Secmark support to core networking**
    - **Allows security subsystems to place security markings on network packets (2.6.18)**
- IPv6
  - RFC 3484 compliant source address selection (2.6.15)
  - Add support for Router Preference (RFC4191) (2.6.17)
  - Add Router Reachability Probing (RFC4191) (2.6.17

Red Hat Enterprise Linux

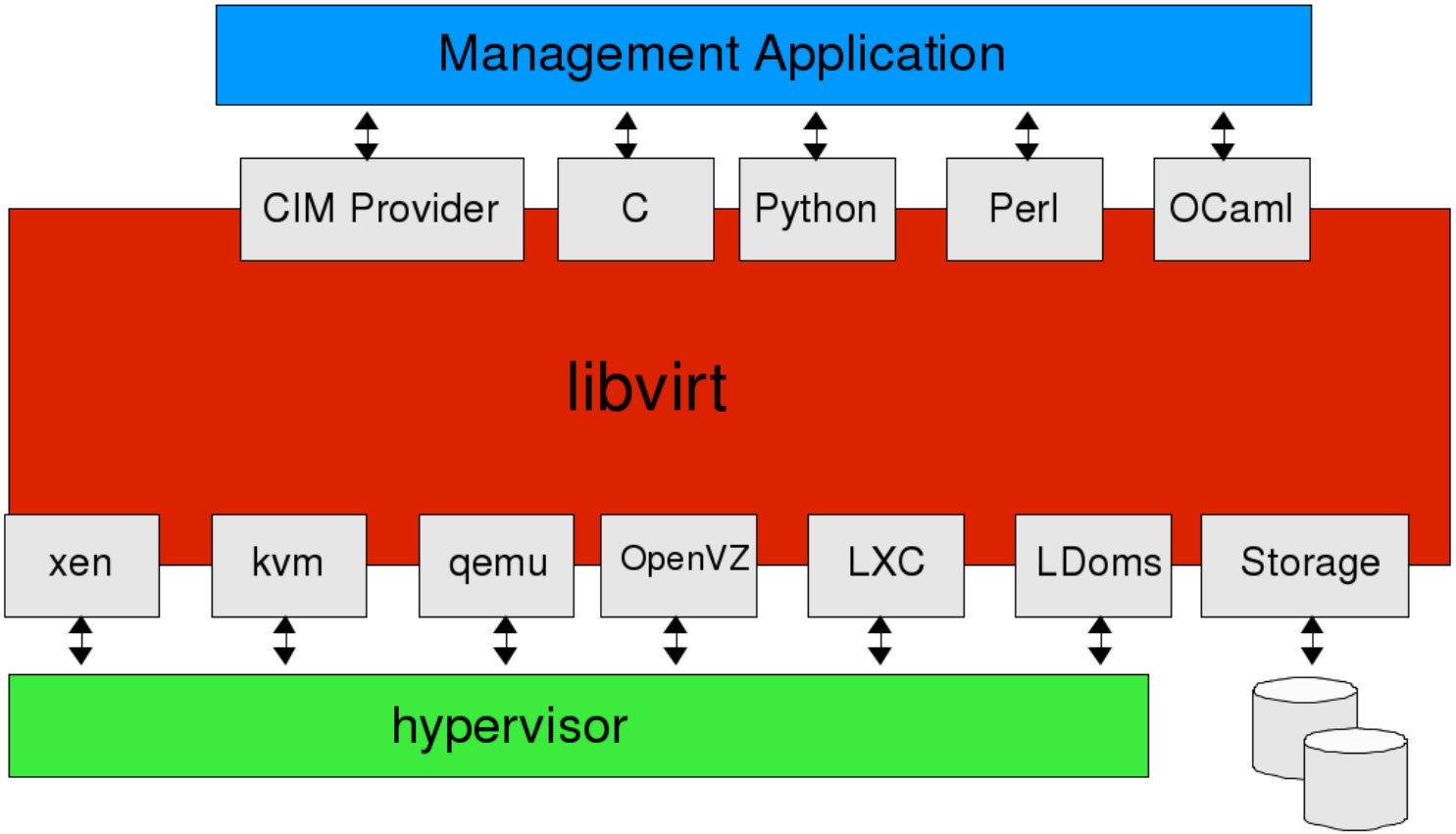
Future Virtualization Update


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

Introduction to libvirt API

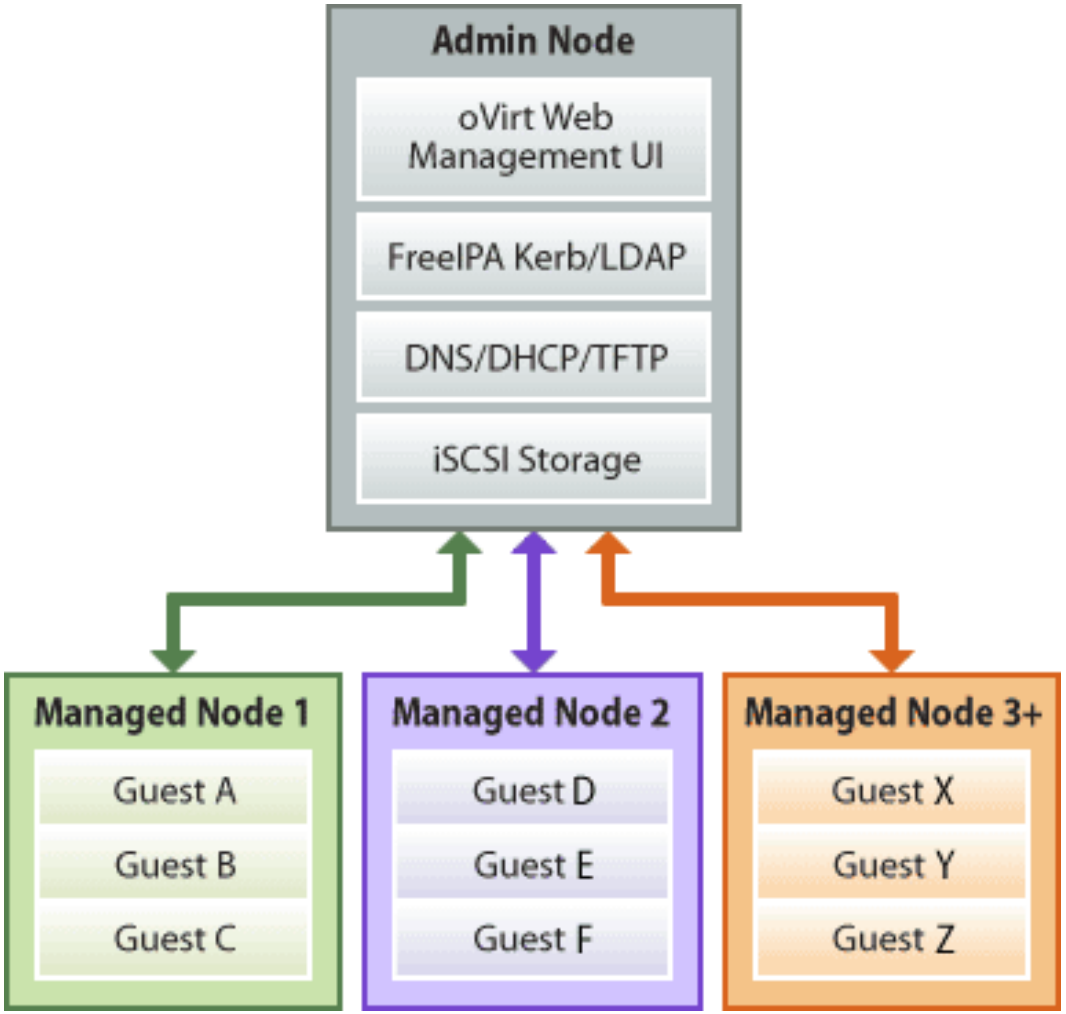
- Hypervisor agnostic
- Stable API for tool/app development
  - CIM providers; Python, C bindings, scriptable
- Allows authenticated/encrypted sessions to remote hypervisors
- Current support for
  - Xen Hypervisor
  - KVM Hypervisor
  - QEMU Hypervisor

Introduction to libvirt API



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 Security Update

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

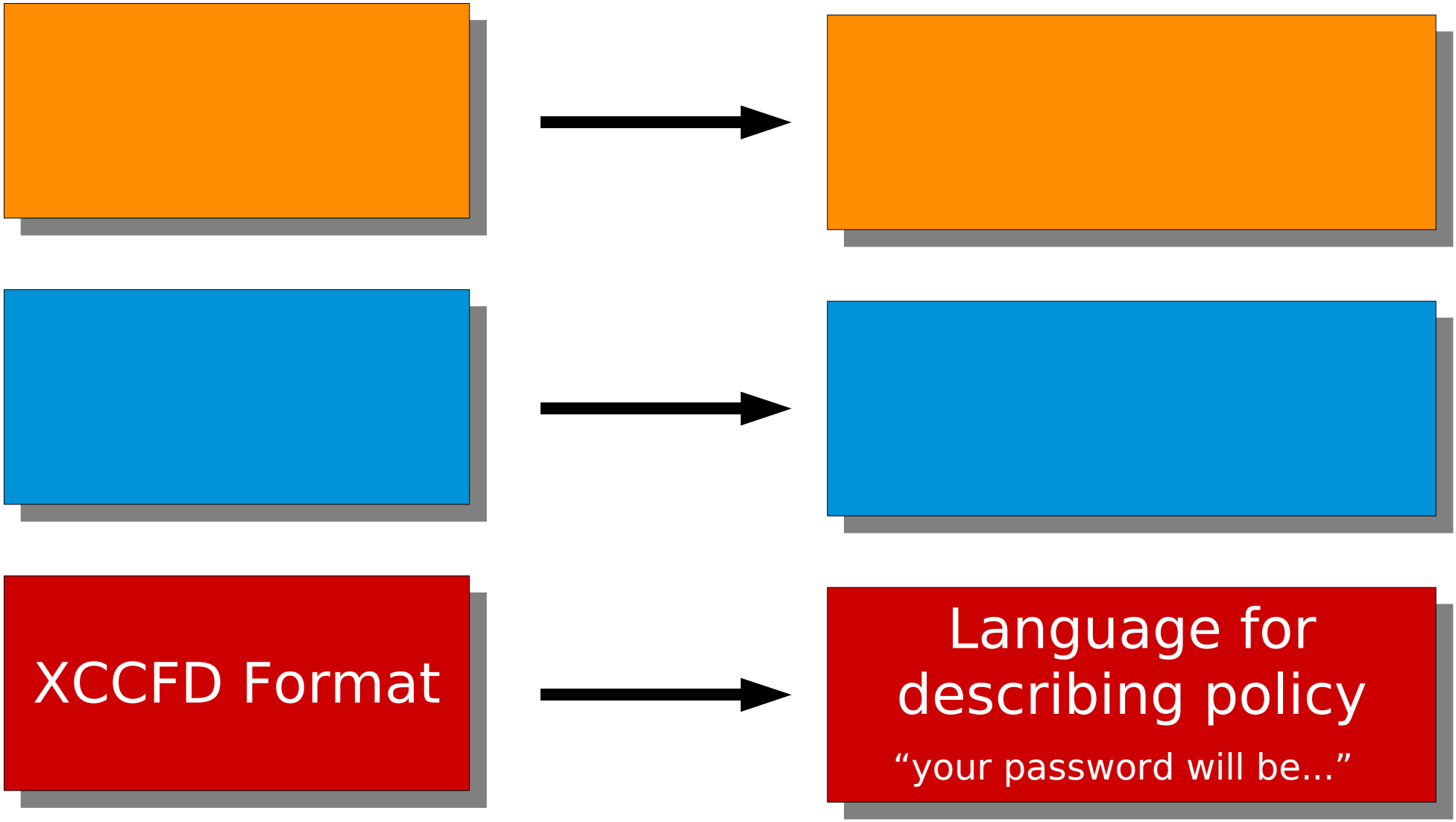
- **DISA SRRs / STIGs**
  - Ask about kickstarts.

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

RHEL5 Security: 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

Red Hat Tomorrow: *Here comes XCCDF*



Red Hat Tomorrow: *Here comes XCCDF*

OVAL Format → Language for defining compliance
"prove that your password is..."

XCCFD Format → Language for describing policy
"your password will be..."

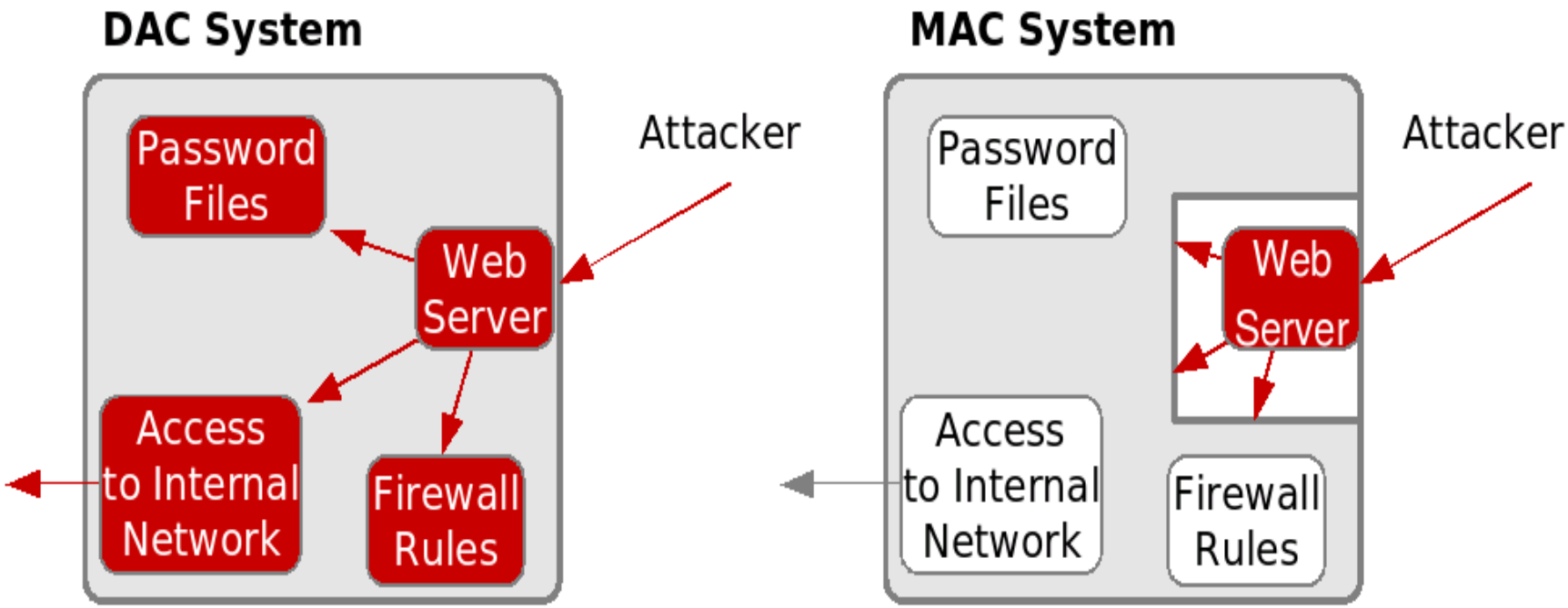
Red Hat Tomorrow: *Here comes XCCDF*

CVE Dictionary → Standard vulnerability & exposure names

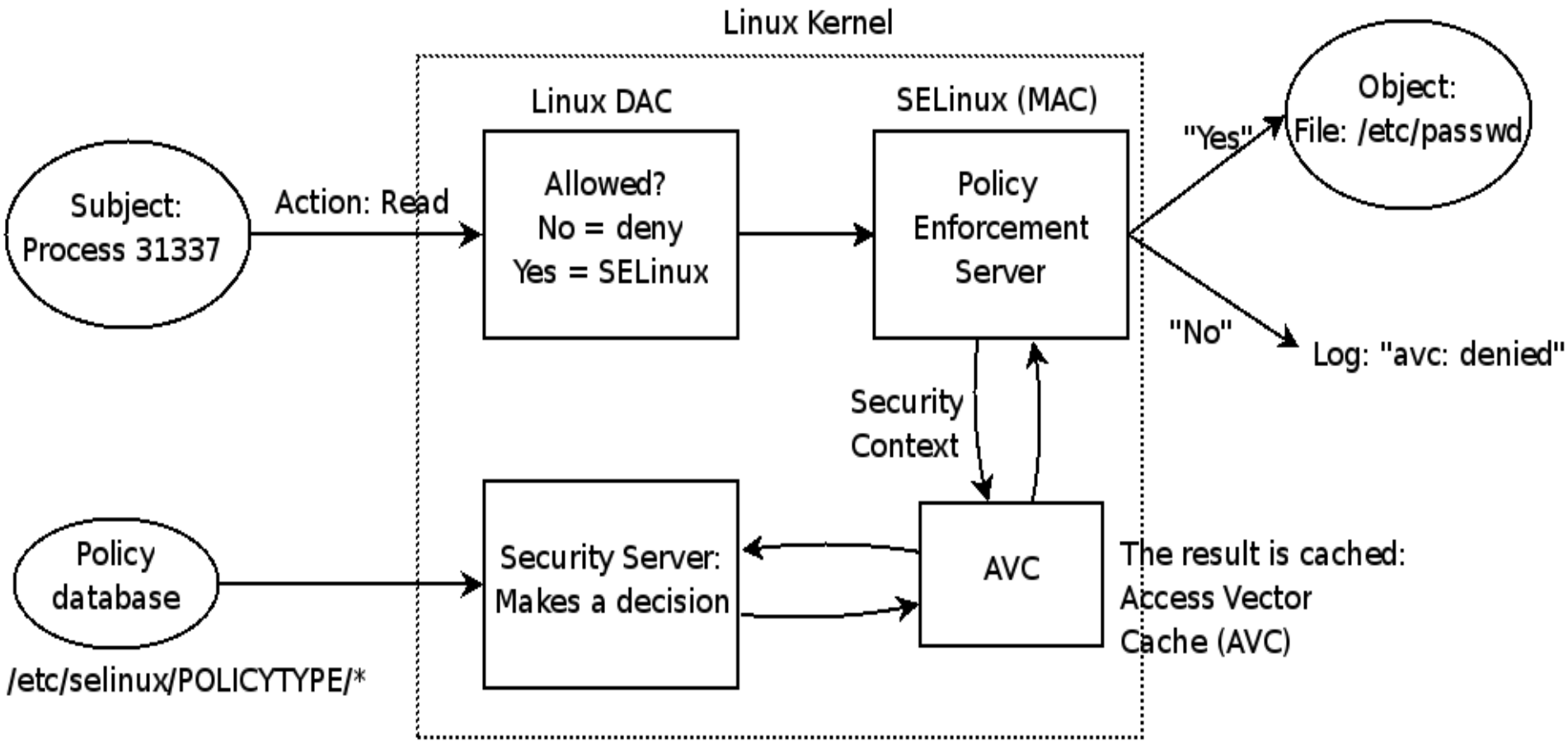
OVAL Format → Language for defining compliance
"prove that your password is..."

XCCFD Format → Language for describing policy
"your password will be..."

RHEL5 Security: Basics of SELinux



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

SELinux Contexts

user_u:object_r:context_t

Examples:

Apache_u:ApacheBackup_r:ApacheDataFiles_t

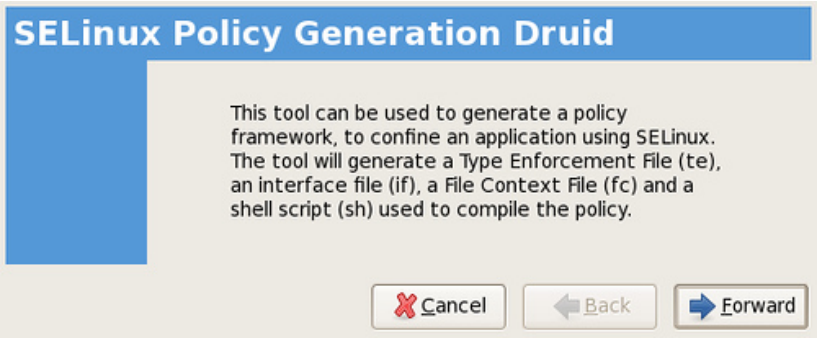
Apache_u:ApacheConfig_r:ApacheConfigFiles_t

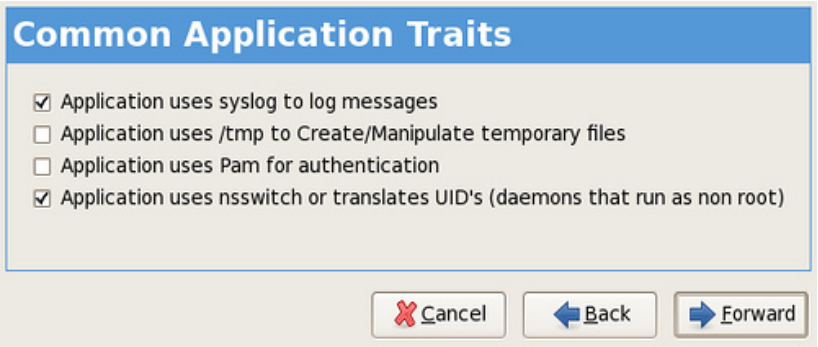
RHEL5 SELinux Enhancements

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





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

Red Hat Today: *SELinux Use Case*

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

Red Hat, Inc. | Red Hat Network | Support | Shop | Products | Training

phpbb creating communities

YourDomain.com

Where everyone goes to get everything.

FAQ | Search | Memberlist | Usergroups

Profile | You have no new messages | Log out [admin]

So, is this thing secure?

newtopic | postreply | 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? quote edit 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	profile pm email
admin Site Admin Joined: 06 Feb 2007	Posted: 07 Feb 2007 07:47 pm Post subject: quote edit Yes, it's very secure. We're pretty sure we've stamped out all the security vulnerabilities at this point.

Done

Red Hat Today: *SELinux Use Case*

YourDomain.com :: View topic - So, is this thing secure? - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

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

Go

Red Hat, Inc. Red Hat Network Support Shop Products Training

phpbb creating communities

YourDomain.com

Where everyone goes to get everything.

FAQ Search Memberlist Usergroups

Profile You have no new messages Log out [admin]

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)%252Echr(101)%252Echr(99)%252Echr(104)%252Echr(111)%252Echr(32)%252Echr(92)%252Echr(34)%252Echr(60)%252Echr(102)%252Echr(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(92)%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)%252Echr(32)%252Echr(104)%252Echr(97)%252Echr(99)%252Echr(107)%252Echr(101)%252Echr(100)%252Echr(46)%252Echr(60)%252Echr(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(110)%252Echr(103)%252Echr(46)%252Echr(60)%252Echr(47)%252Echr(102)%252Echr(111)%252Echr(110)%252Echr(116)%252Echr(62)%252Echr(92)%252Echr(34)%252Echr(59)%252Echr(32)%252Echr(62)%252Echr(34)%252Echr(32)%252Echr(62)%252Echr(32)%252Echr(47)%252Echr(118)%252Echr(97)%252Echr(114)%252Echr(47)%252Echr(119)%252Echr(119)%252Echr(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(116)%252Echr(111)%252Echr(112)%252Echr(105)%252Echr(99)%252Echr(46)%252Echr(112)%252Echr(104)%252Echr(112))%252E%2527

So, is this thing secure?

new topic post reply YourDomain.c

Author	
admin Site Admin Joined: 06 Feb 2007 Posts: 3	Posted: 07 Feb 2007 I've used online bull Is this one different?
Back to top	profile pm email
admin Site Admin	Posted: 07 Feb 2007 07:47 pm Post subject: quote edit IP Yes, it's very secure. We're pretty sure we've stamped out all the security vulnerabilities at this point.

Done

Red Hat Today: *SELinux Use Case*

Red Hat Today: *RHEL Security Status*

SELinux Use Case

- 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

Red Hat Enterprise Linux System z Update

Red Hat Today: *Announcements*

Red Hat / IBM Alliance

Technical Perspective

- Dedicated Partner Managers
- IBM on-site kernel engineers at Red Hat
- Weekly calls with IBM System z Product Mgmt
- Emphasis on IBM access to code (making it easier to work together)
- Weekly reviews of open bugs & feature requests
- Proof of Concept Support

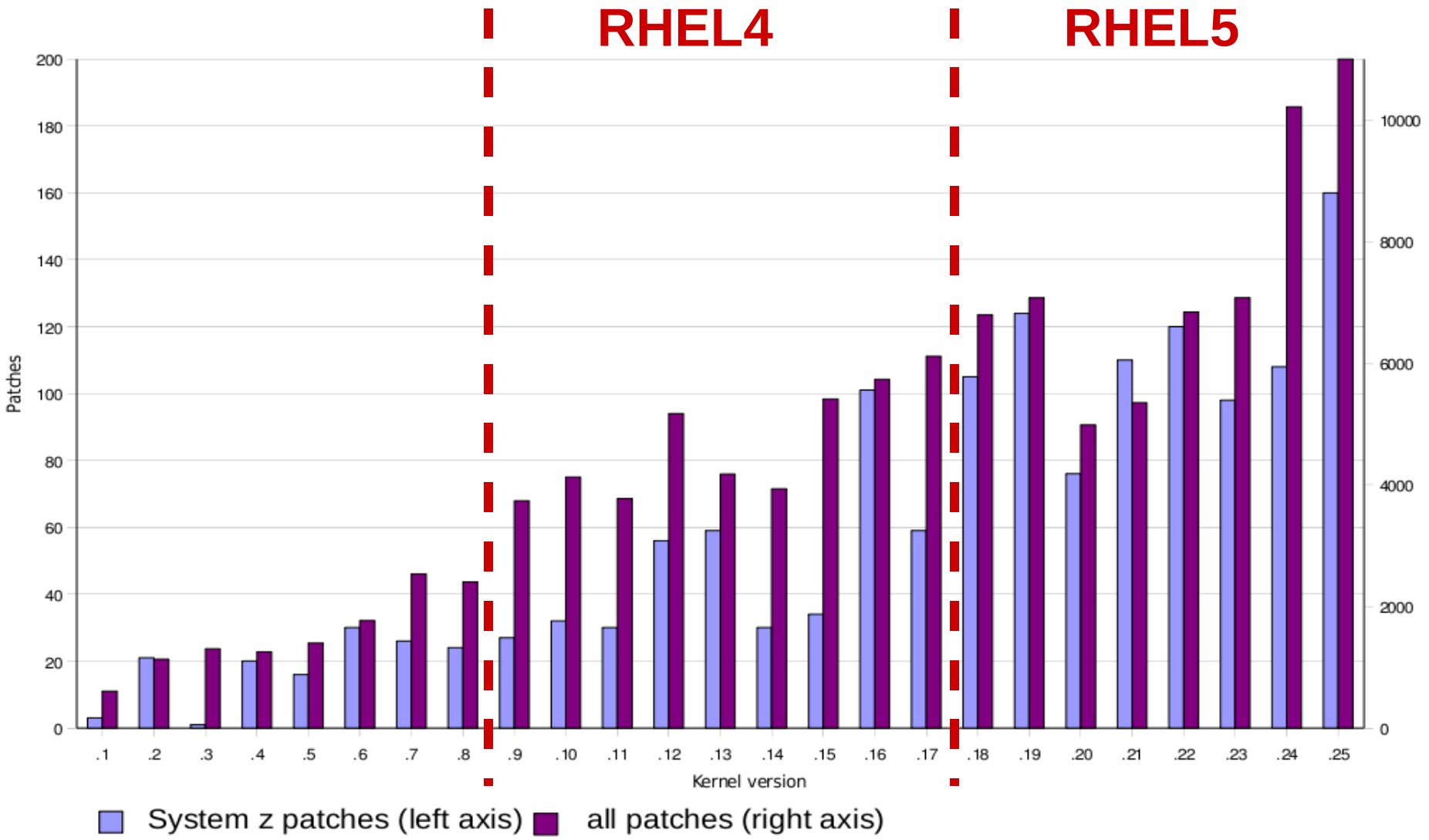
Marketing & Sales Perspective

- Joint World-Wide Tour
- Marist, zNTP, T3, SHARE, zExpo, etc

Business Perspective

- Dedicated staff from helpdesk to executive

IBM Changes to 2.6.x Kernel



Red Hat Today: *RHEL Status*

Upstream of Code

- DASD Drive Updates
- zFCP Driver Updates
  - zFCP multipathing support in RHEL5 installer
- Crypto2 Express Support
- Hugetblfs
- Layer-2 IPv6 support for Hipersockets

Marketing Perspective

- Joint World-Wide Tour
- Marist, zNTP, T3, SHARE, zExpo, etc

Sales Perspective

- Joint sales calls

Red Hat Today: *RHEL Status*

RHEL 5.1

- Improved z/VM scheduling
- Improved performance with key recompiled libraries

RHEL 5.2

- Support for new IBM z10
- Improved IBM Director support to support fast connection to z/VM
- Improved Virtual Server Management
- Implementation of SCSI dump infrastructure
- Support for Dynamic CHPID reconfiguration
- Better network configuration tool support for System z network adapters
- Improved install experience with support for “ssh -X” with VNC
- Better network performance with skb scatter-gather support
- Implemented device-multipath support for xDR/GDPS

RHEL 5.3

- NSS, CPU Affinity, ETR support planned
- Suggestions? swells@redhat.com

Red Hat Today: *RHEL Security Status*

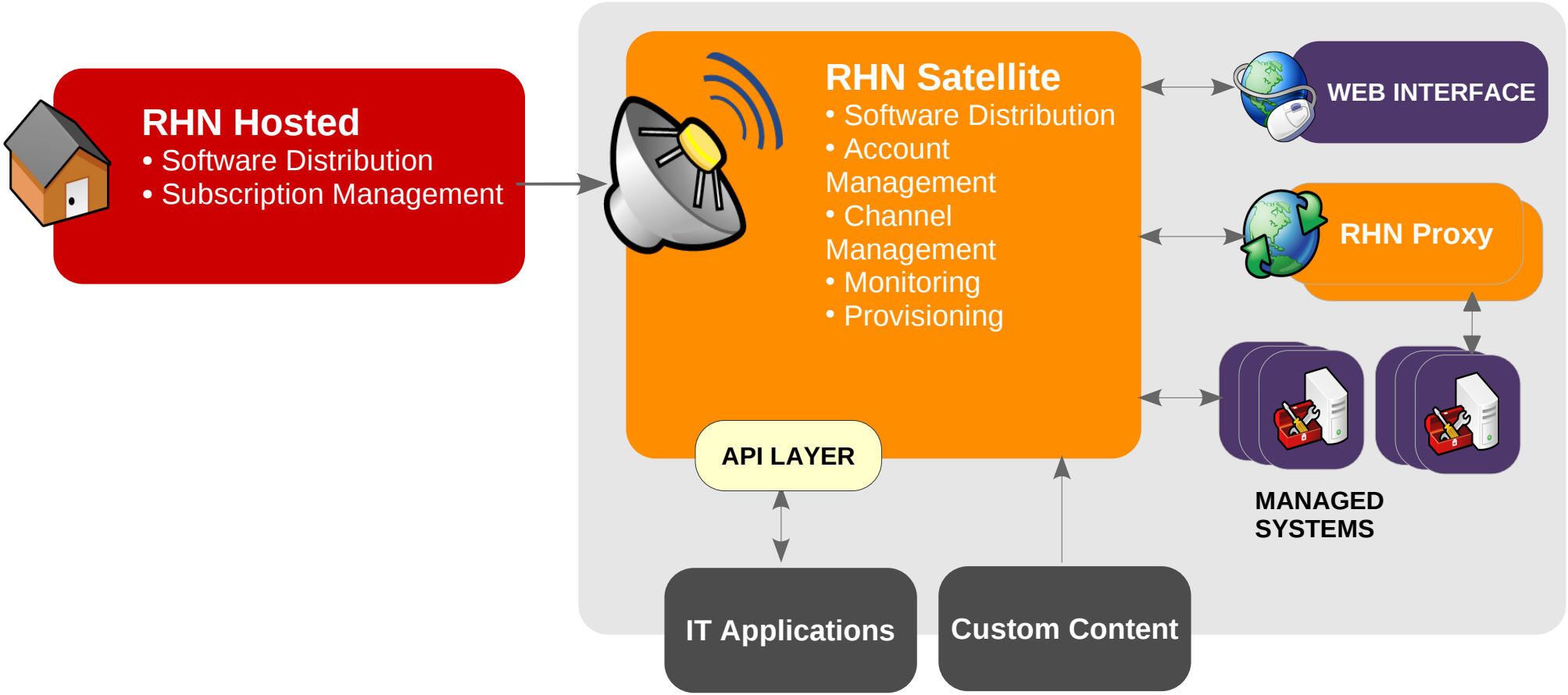
Hardware Enablement

- **In kernel crypto**
  - S/390 implementation of SHA-384 and SHA-512 digests
  - Improved encryption performance (i.e. encrypted filesystems)
- **libica library**
  - Support for updated OpenSSL, PKCS#11, GSKit, and kernel crypto APIs
  - Device driver performance updates
- **Crypto2 Express Support**

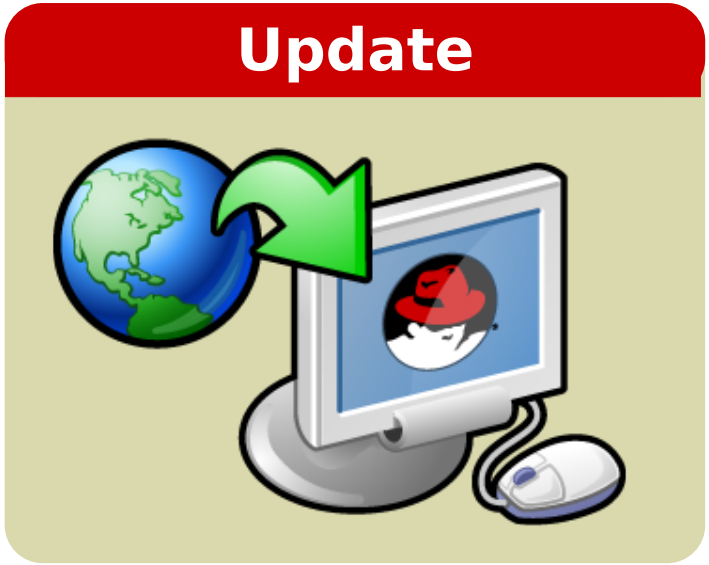
Red Hat Enterprise Linux Update

Red Hat Network

RHN Satellite Deployment Model



What is Red Hat Network?



What is Red Hat Network?

Update

Manage

What is Red Hat Network?

Update

Manage

Provision

What is Red Hat Network?

Update

Manage

Provision

Monitor

redhat

English (change) | Knowledgebase | Documentation | LOGGED IN: jschrode | Preferences | Sign Out

RED HAT NETWORK SATELLITE

Systems

Search

Your RHN | Systems | Errata | Channels | Configuration | Schedule | Users | Help

NO SYSTEMS SELECTED | MANAGE | CLEAR

- Your RHN
- Your Account
- Your Preferences
- Locale Preferences
- Subscription Management

Your RHN

Tasks

- **Search** for: Packages | Systems
- Manage **Entitlements** & **Subscriptions**
- **Register** Systems
- Manage **Activation Keys**
- Manage **Kickstarts**
- Manage **Configuration Files**

Inactive Systems

No inactive systems.

All of your systems are actively checking into RHN at this time. You can view a list of all of your systems at **Systems > All**.

Your RHN Legend

- OK
- Critical
- Warning
- Unknown
- Locked
- Kickstarting
- Pending Actions
- Failed Actions
- Completed Actions
- Security
- Bug Fix
- Enhancement

Most Critical Systems

System Name	All Updates	Security Errata	Bugfix Errata	Enhancement Errata
rhel5-x86.demo.redhat.com	190	46	128	16

1 - 1 of 1 most critical systems displayed

View All Critical Systems

Recently Scheduled Actions

Action	User	Age
Package Install	jschrode	0 Hour(s)

1 - 1 of 1 recently scheduled actions displayed

View All Scheduled Actions

Relevant Security Errata

		Systems	Updated
RHSA-2008:0290	Critical: samba security and bug fix update	1	5/28/08

redhat

Knowledgebase | Documentation

RED HAT NETWORK SATELLITE

Systems

Search

Your RHN | Systems | Errata | Channels | Configuration | Schedule | Users | Help

NO SYSTEMS SELECTED MANAGE CLEAR

- Overview
- Systems
  - All
  - Virtual Systems
  - Out of Date
  - Unentitled
  - Ungrouped
  - Inactive
  - Recently Registered
  - Proxy
- System Groups
- System Set Manager
- Advanced Search
- Activation Keys
- Stored Profiles
- Custom System Info
- Kickstart

rhel5-x86.demo.redhat.com

delete system

Details | Software | Groups | Events

Pending | History

System History

The following history events have been noted for this system.

Please note that this system has no pending events.

1 - 5 of 5

Type	Status	Summary	Time
		Package Install scheduled by jschrode	2008-06-03 20:44:29 CEST
	(n/a)	subscribed to channel rhel-i386-server-vt-5	2008-06-03 20:42:17 CEST
	(n/a)	subscribed to channel rhn-tools-rhel-i386-server-5	2008-06-03 20:42:16 CEST
	(n/a)	added system entitlement	2008-06-03 20:37:14 CEST
	(n/a)	subscribed to channel rhel-i386-server-5	2008-06-03 20:37:11 CEST

1 - 5 of 5

Event Type Legend

- Package Event
- Errata Event
- Preferences Event

redhat

Your RHN | Systems | Errata | Channels | Configuration | Schedule | Users | Help

No systems selected | Manage | Clear

- Overview
- Systems
- System Groups
- System Set Manager
- Advanced Search
- Activation Keys
- Stored Profiles
- Custom System Info
- Kickstart
  - Profiles
  - Bare Metal
  - GPG and SSL Keys
  - Distributions
  - File Preservation

Kickstart: rhel-5-i386-server_default_part_novirt

Kickstart Details | System Details | Software | Activation Keys | Scripts | Kickstart File

Kickstart File

The kickstart file generated by this kickstart profile is viewable below:

Download Kickstart File

```
# Kickstart config file generated by RHN Config Management
#
# Profile Name  : rhel-5-i386-server_default_part_novirt
# Profile Label : rhel-5-i386-server_default_part_novirt
# Date Created  : 2008-06-03 20:40:03.0
#

install
text
network --bootproto dhcp
url --url http://devel13.z900.redhat.com/ty/MwPJrTGI
lang en_US
langsupport --default en_US en_US
keyboard us
mouse none
zerombr yes
clearpart --all
part /boot --fstype=ext3 --size=200
part pv.01 --size=1000 --grow
part swap --size=1000   --maxsize=2000
volgroup myvg pv.01
logvol / --vgname=myvg --name=rootvol --size=1000 --grow
bootloader --location mbr
timezone America/New_York
auth --enablemd5 --enableshadow
rootpw --iscrypted $1$OKAzMj1I$VO5gL5mVVj9T09GidA/Y6/
selinux --permissive
reboot
firewall --disabled
skipx
repo --name=Cluster --baseurl=http://devel13.z900.redhat.com/kickstart/dist/ks-rhel-i386-server-5-u1/Cluster
repo --name=ClusterStorage --baseurl=http://devel13.z900.redhat.com/kickstart/dist/ks-rhel-i386-server-5-u1/ClusterStorage
repo --name=VT --baseurl=http://devel13.z900.redhat.com/kickstart/dist/ks-rhel-i386-server-5-u1/VT
repo --name=Workstation --baseurl=http://devel13.z900.redhat.com/kickstart/dist/ks-rhel-i386-server-5-u1/Workstation
```

RHN Satellite Is Now Open Source

http://spacewalk.redhat.com

- Announced at Red Hat Summit 2008
  - .... remember the Fedora -> RHEL model?

Open Discussion