Red Hat Update for System z

Shawn Wells, RHCE

EMail: swells@redhat.com

Lead, Linux on System z

Agenda

45min Update on Red Hat

- Today
- Tomorrow
- Together

Introductions

- Shawn Wells
  W/W Lead, Linux on System z
  - Solutions Architect
  - Business Development, Presentations & Demos, Interface to Prod Mgmt, etc

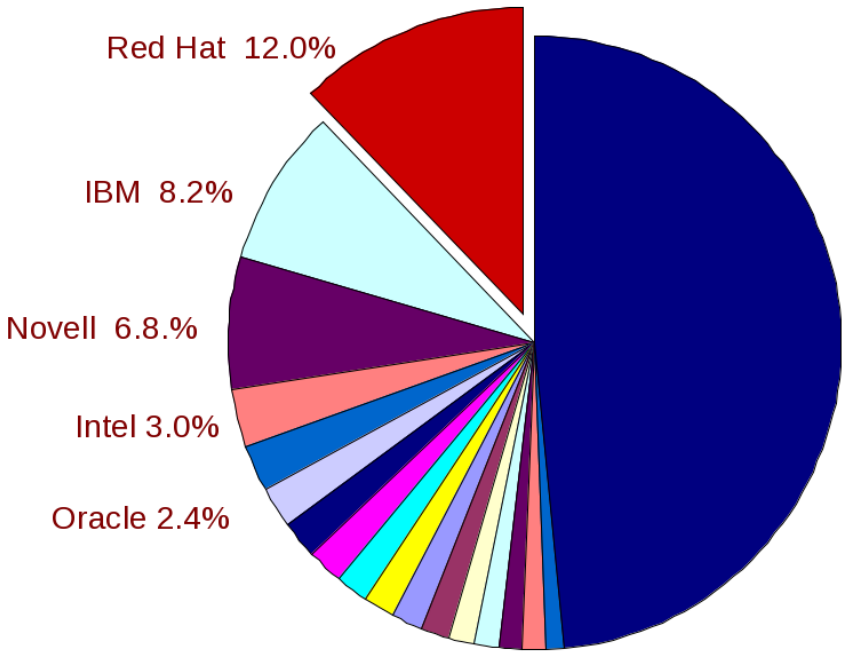
Introductions

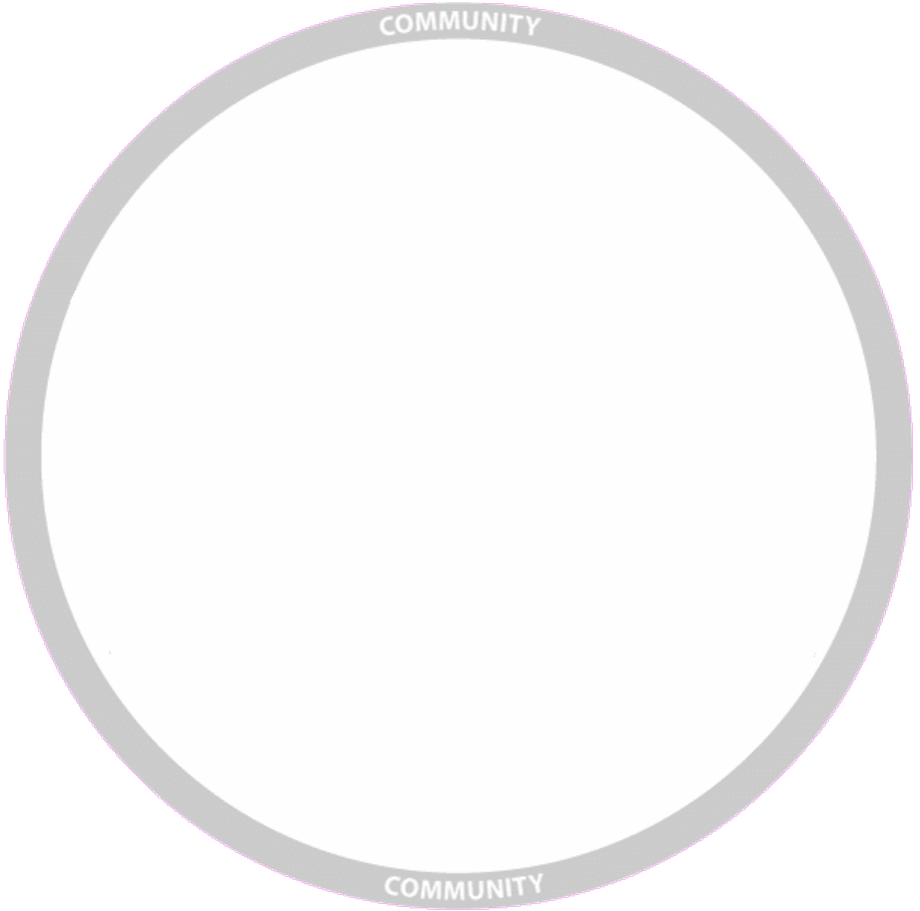
- Shawn Wells
  W/W Lead, Linux on System z
  - Solutions Architect
  - Business Development, Presentations & Demos, Interface to Prod Mgmt, etc
- Also here at T3.....
  - Brad Hinson
    Lead, Linux on System z Technical Support
  - Justin Payne
    Sr Technical Support Engineer, Linux on System z

Red Hat Development Model

Community

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

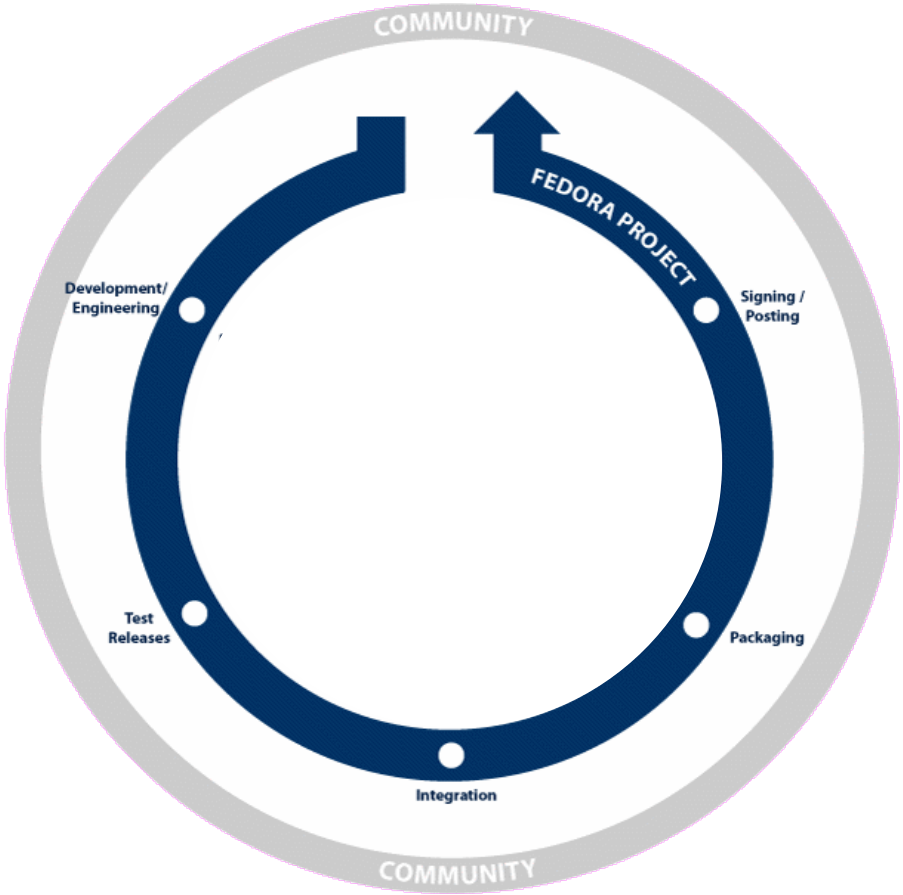




Red Hat Development Model

Fedora

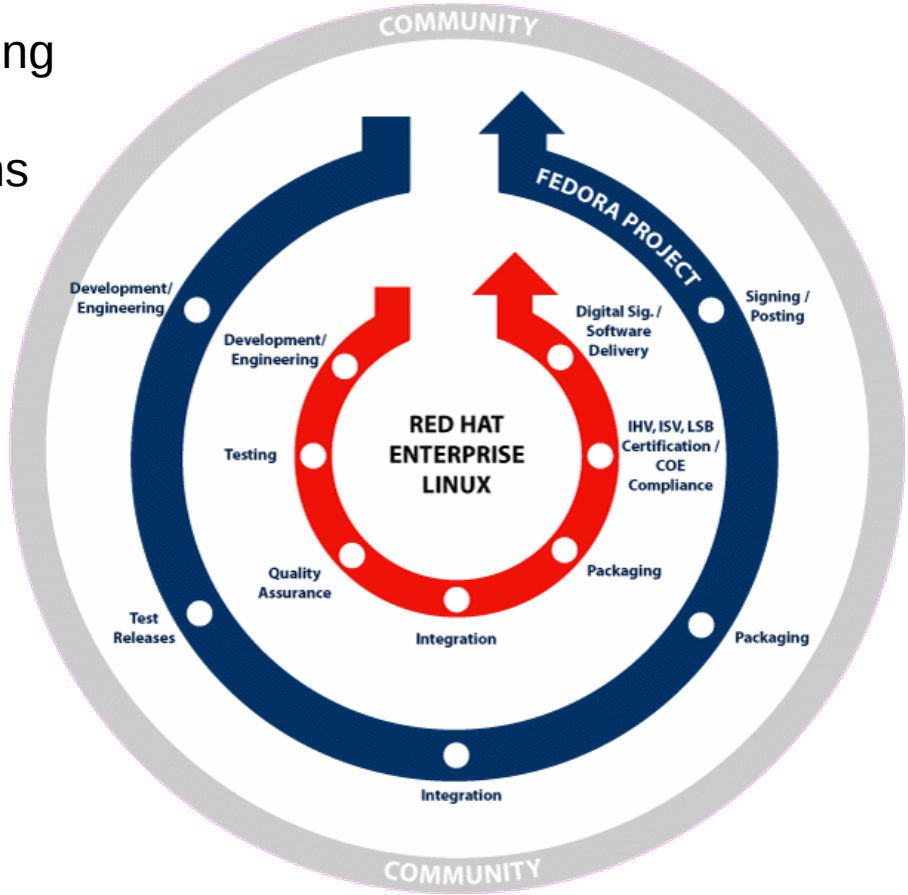
- Rapid innovation
- Latest technologies
- Community Supported
- Released ~6mo cycles



Red Hat Development Model

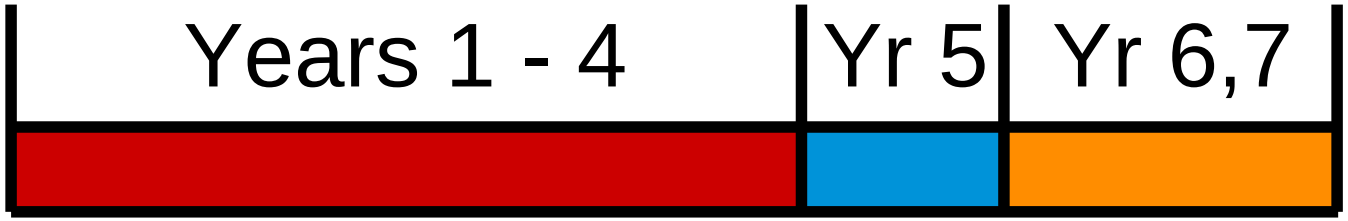
Red Hat Enterprise Linux

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



Red Hat Today: *Announcements*

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**		

Red Hat Today: *Announcements*

Red Hat Enterprise Linux 4.7

Announced Thursday, July 24 2008

- 2.6.9-78 Kernel Stream
- Added AIDE
- Ability to generate SHA-256 and SHA-512 password hashes
- Updated zFCP driver to include bugfixes
- Updated qdio driver to fix zFCP/SCSI write to IO stagnates on LPAR
- /proc/sys/vm/nfs-writeback-lowmem-only param to fix NFS read performance
- /proc/sys/vm/write-mapped to help select faster NFS read performance
- autofs5

- *N_PIV is waiting development acceptance for 4.8 (Already in RHEL5)*

Download @ https://rhn.redhat.com/network/software/download_isos_full.pxt

Red Hat Today: *Announcements*

What is AIDE?

- Intrusion Detection program
- Ships with RHEL5, now in 4.7

 # yum install aide
 # aide –init

Red Hat Today: *Announcements*

What is AIDE?

- Intrusion Detection program
- Ships with RHEL5, now in 4.7

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

Red Hat Today: *Announcements*

What is AIDE?

- Intrusion Detection program
- Ships with RHEL5, now in 4.7

```
# 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

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

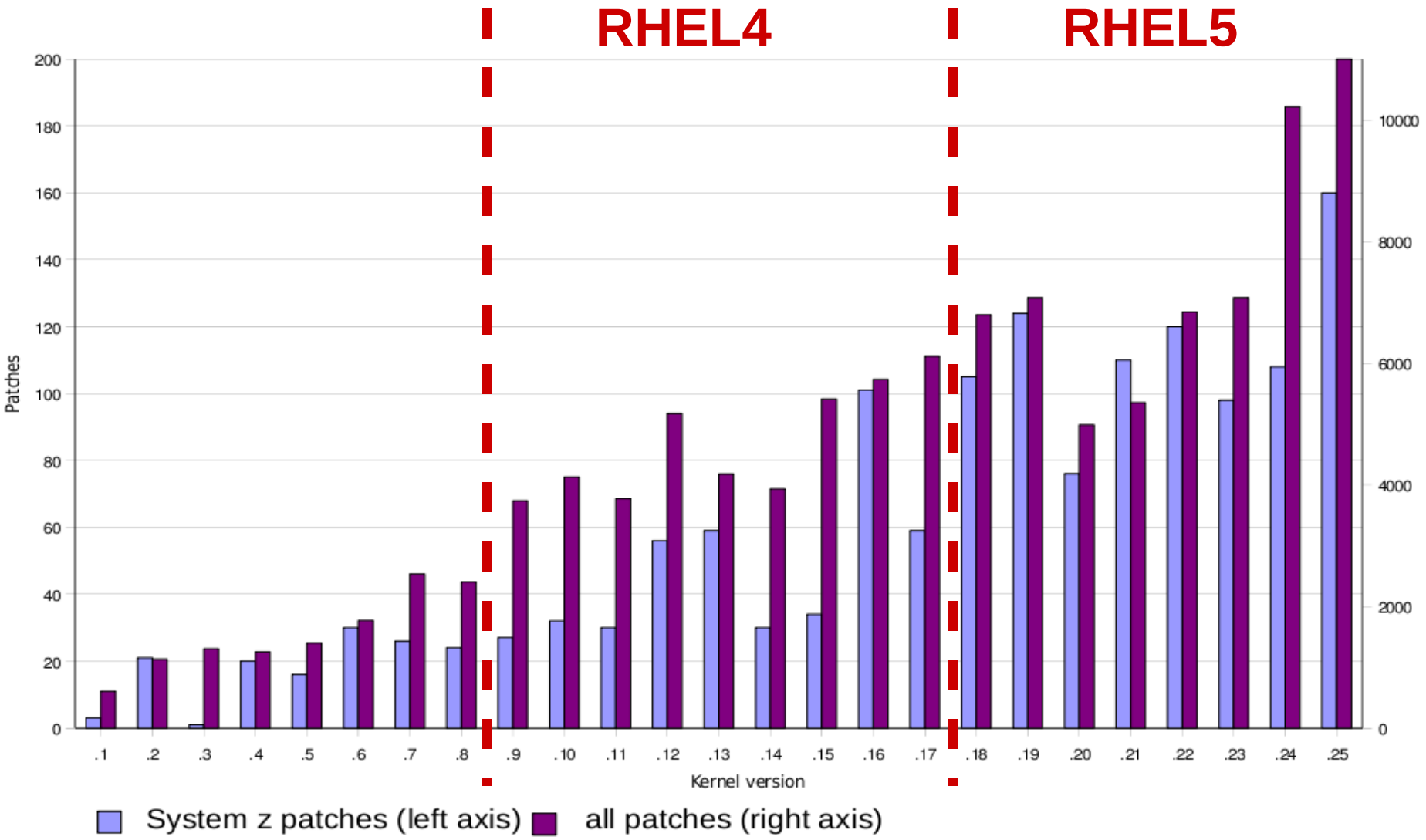
Marketing & Sales Perspective

- 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

the proof is in the pudding...

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

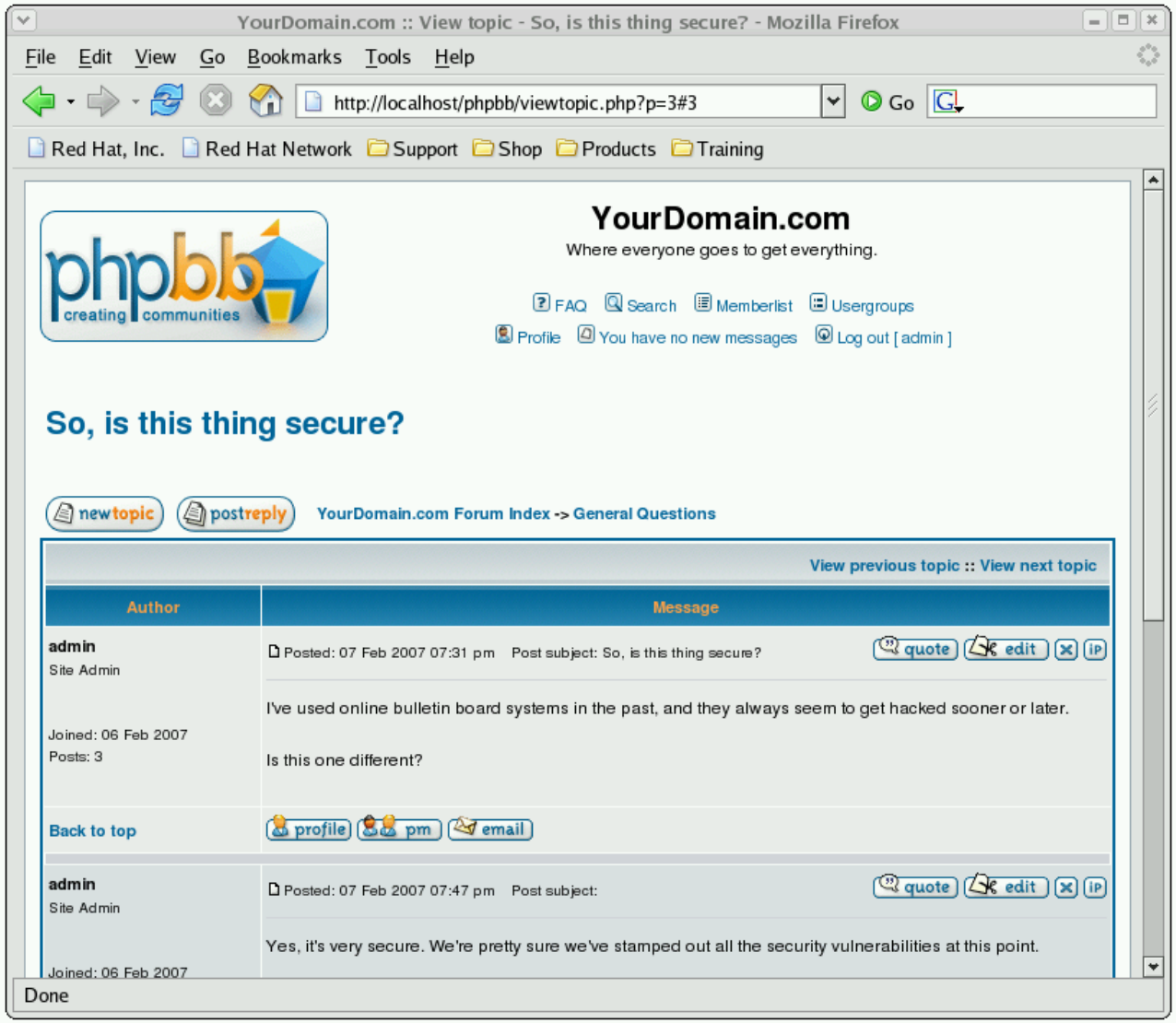
- **In kernel crypto**
  - S/390 implementation of SHA-384 and SHA-512 digests
  - Improved encryption performance (i.e. encrypted filesystems)
- **libica library**
  - Support for updated OpenSSL, PKCS#11, GSKit, and kernel crypto APIs
  - Device driver performance updates
- **Crypto2 Express Support**

Red Hat Today: *RHEL Security Status*

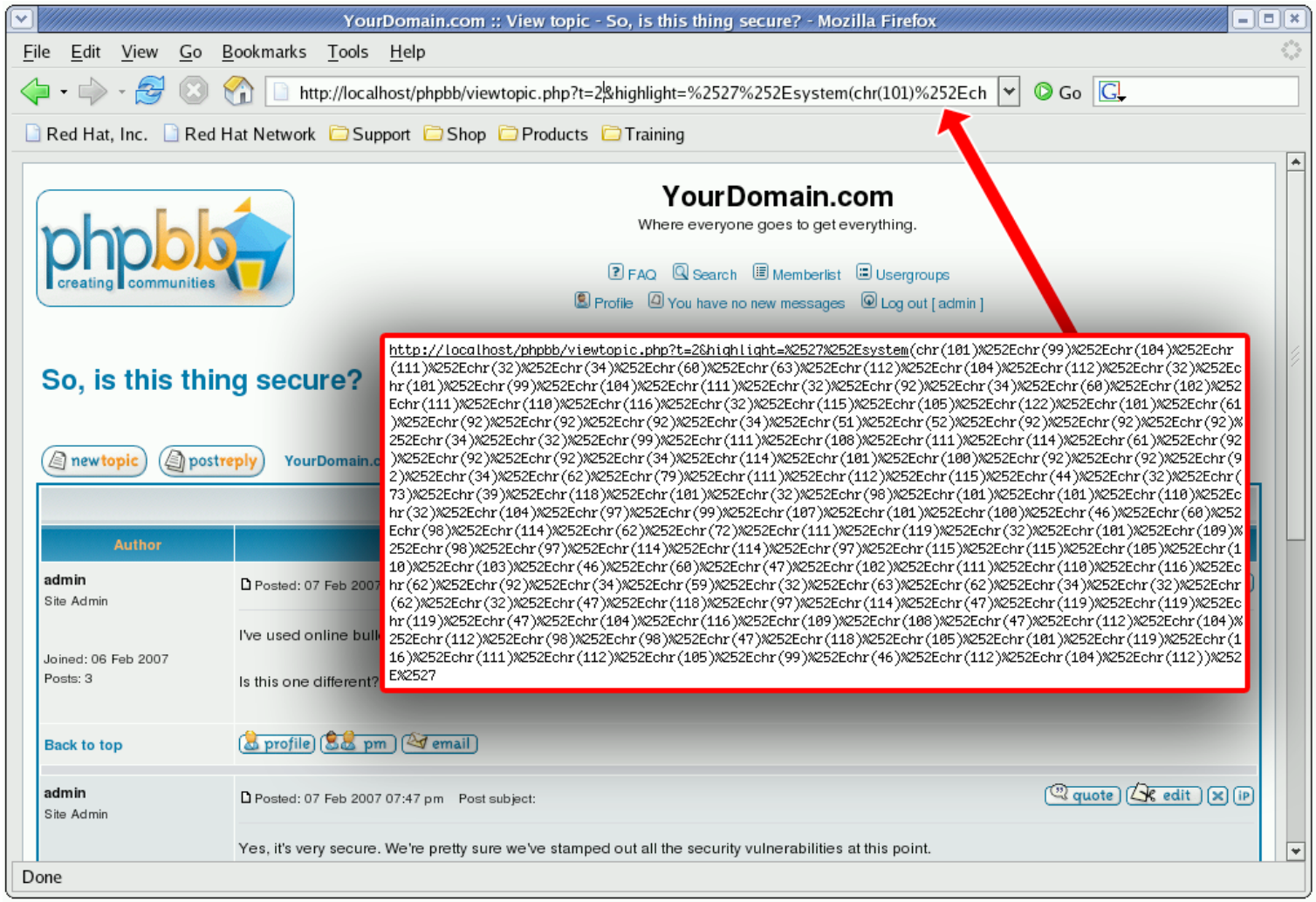
Kernel Enablement

- **SELinux**
  - Policies { targeted, strict, MLS }
  - Contexts { root:system_r:httpd_sys_script_t }
  - Roles { system_r, object_r }
- **ExecShield, FORTIFY_SOURCE, and Canary Values**
  - kernel.exec-shield (/proc/sys/kernel/exec-shield)
- **ACL Lists**
  - setfactl, getfacl

Red Hat Today: *SELinux Use Case*



Red Hat Today: *SELinux Use Case*



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 Today: *RHEL Security Status*

SELinux

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**

Red Hat Today: *RHEL Security Status*

Who cares about SELinux Loadable Policy Modules?

Red Hat Today: *RHEL Security Status*

Who cares about SELinux Loadable Policy Modules?

or

I just turn off SELinux anyway

Red Hat Today: *RHEL Security Status*

SELinux

- 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

Red Hat Today: *RHEL Security Status*

SELinux

<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

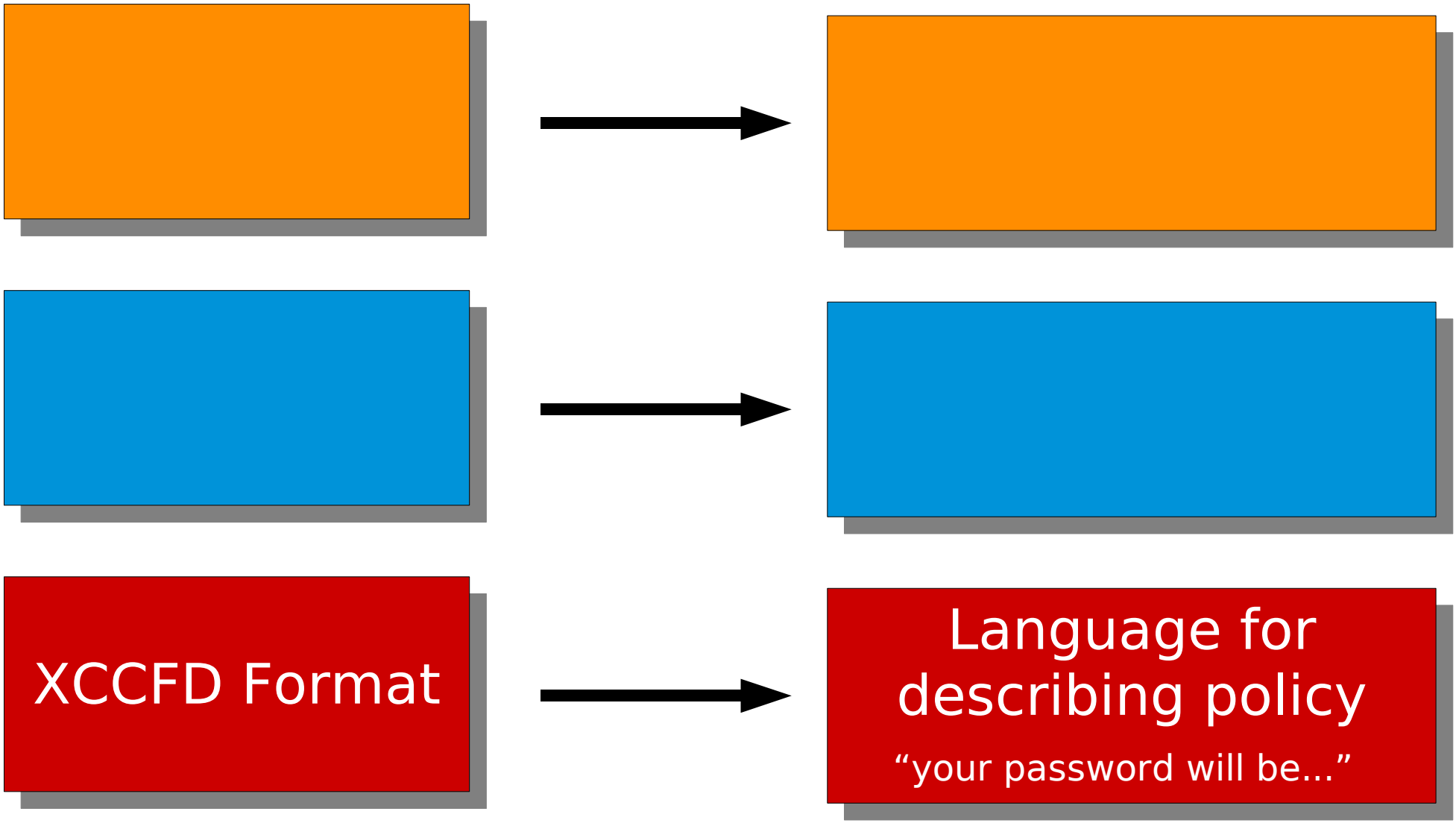
.....

</snip>

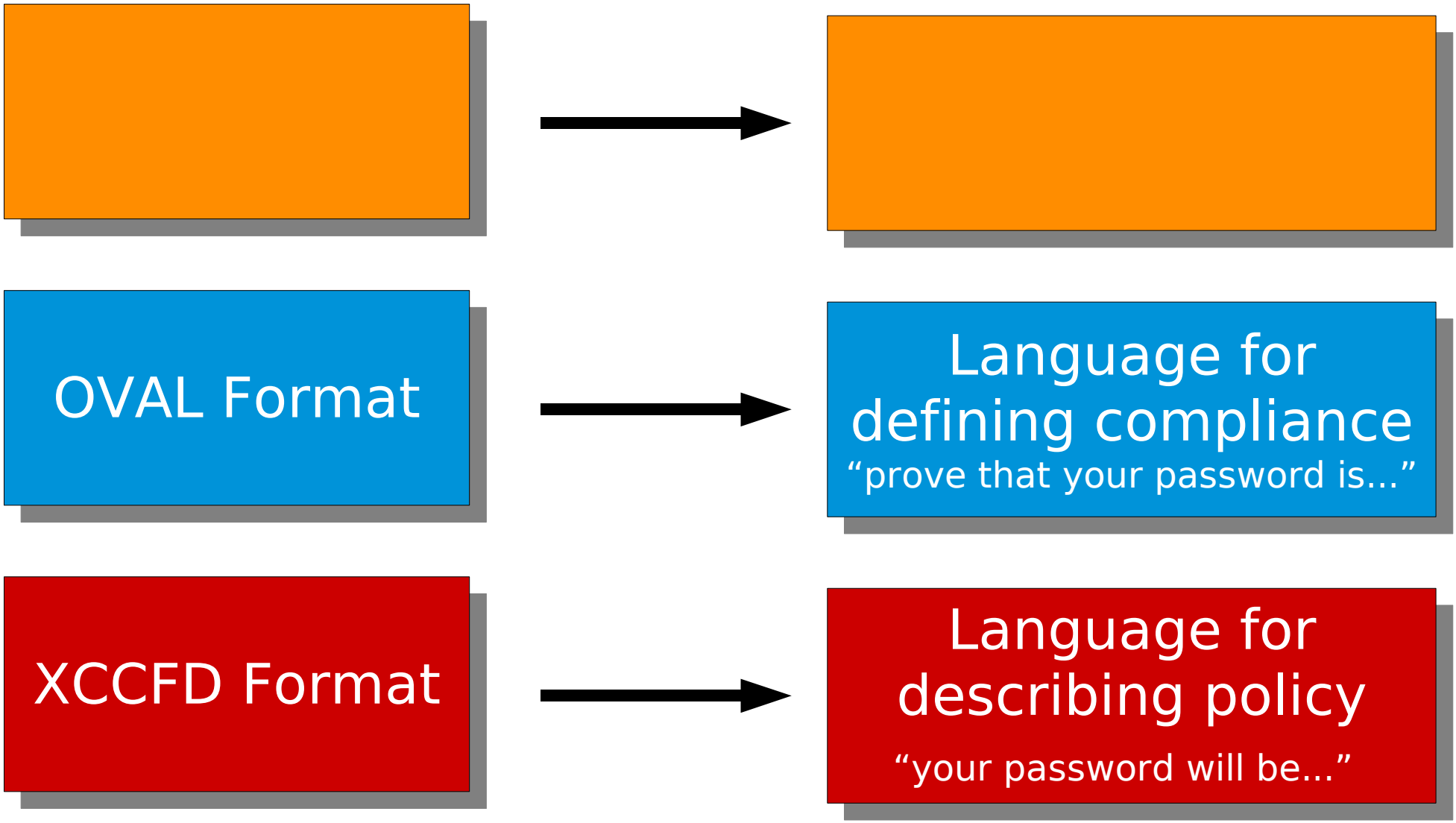
 # ausearch -x "/sbin/ip" | audit2allow -M myVPNfix

 # semodule -i myVPNfix

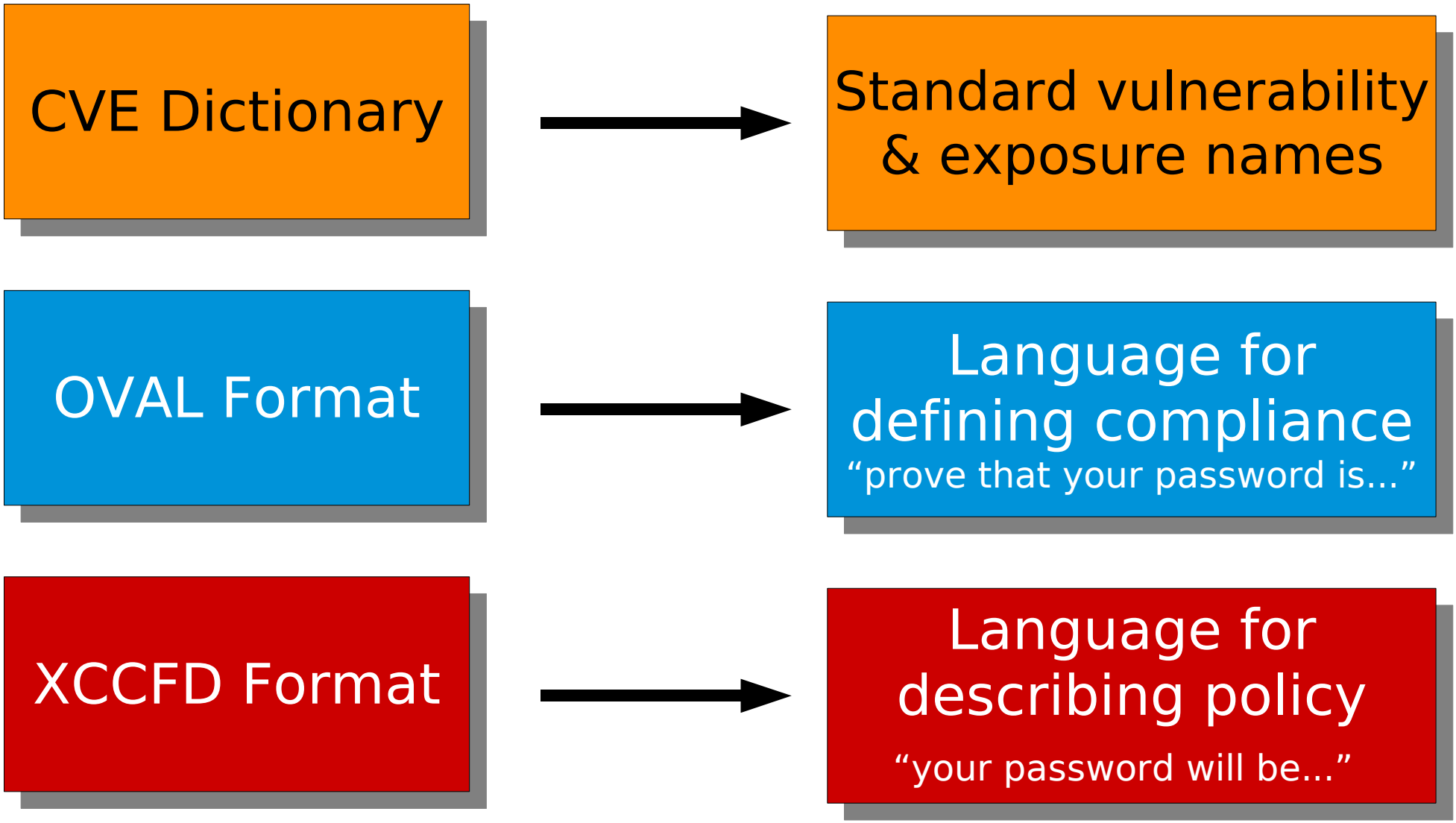
Red Hat Tomorrow: *Here comes XCCDF*



Red Hat Tomorrow: *Here comes XCCDF*



Red Hat Tomorrow: *Here comes XCCDF*



Red Hat Tomorrow: Using *XCCDF*

```
<definitions>
   <definition class="vulnerability" id="OVAL9999" instance="1">
      <affected family="Linux">
         <linux:platform>Red Hat Enterprise Linux</linux:platform>
          <product>RHEL5.2</product>
      </affected>
      <description>SELinux is turned off</description>
      <reference source="CVE">CVE-SELinux-test</reference>
      <status>ACCEPTED</status>
      <version>1</version>
      <criteria result="1">
         <criteria comment="SELinux Turned off. Turn back on." test_ref="XCCDF-
         Section1" version="1"/>
      </criteria>
   </definition>
</definitions>
```

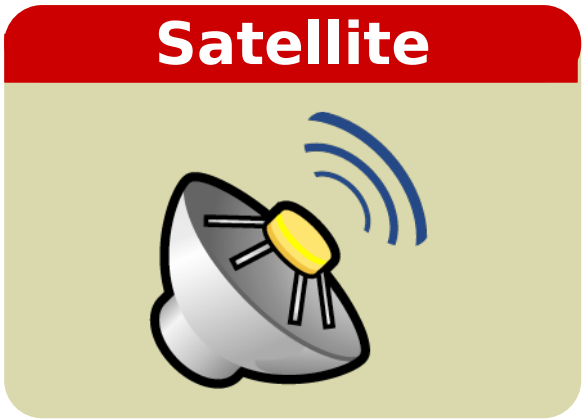
Red Hat Today: *Systems Management*

Red Hat Network

A systems management platform designed to provide complete life cycle management of the operating system and applications.

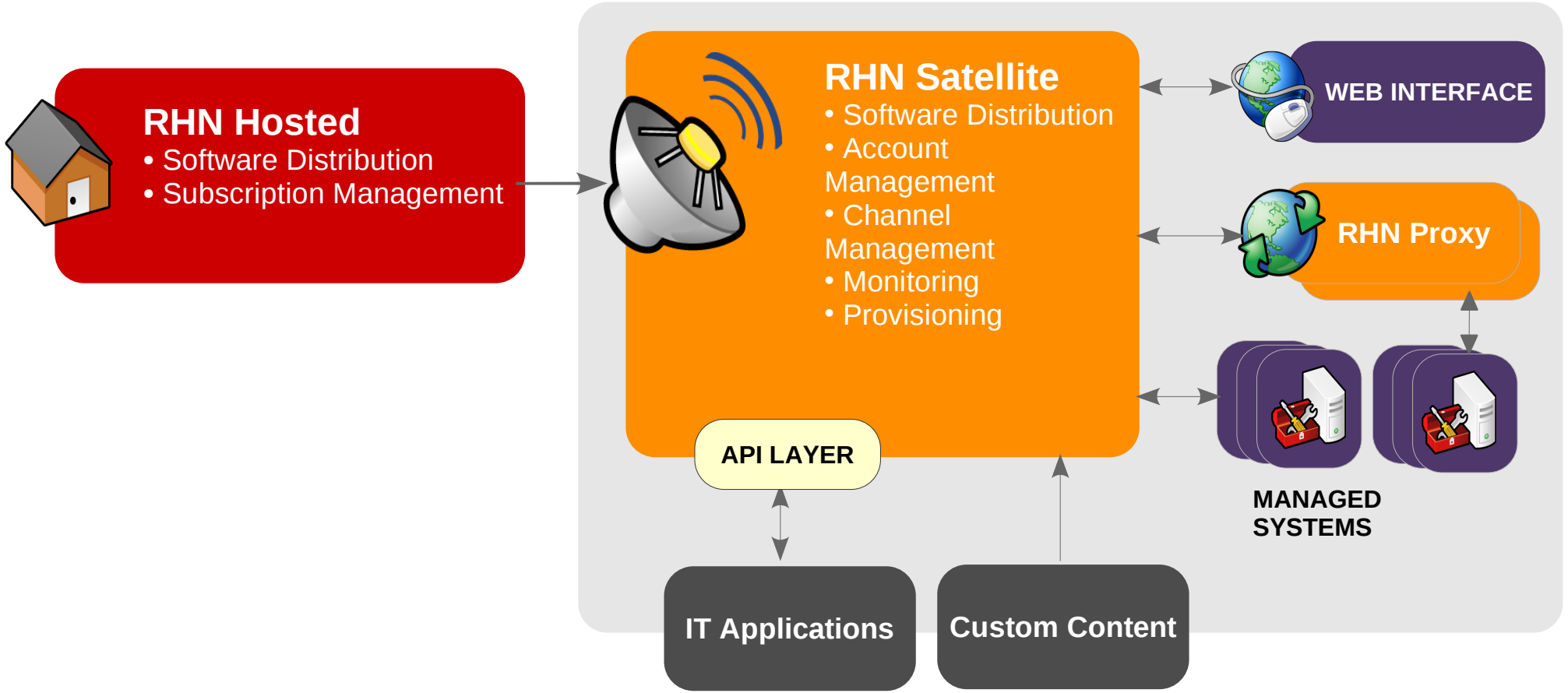
- Provision/re-provision machines without touching them
- Manage 1,000 systems as easily as 1
- Ensure security fixes / config changes applied consistently across enterprise

What is Red Hat Network?

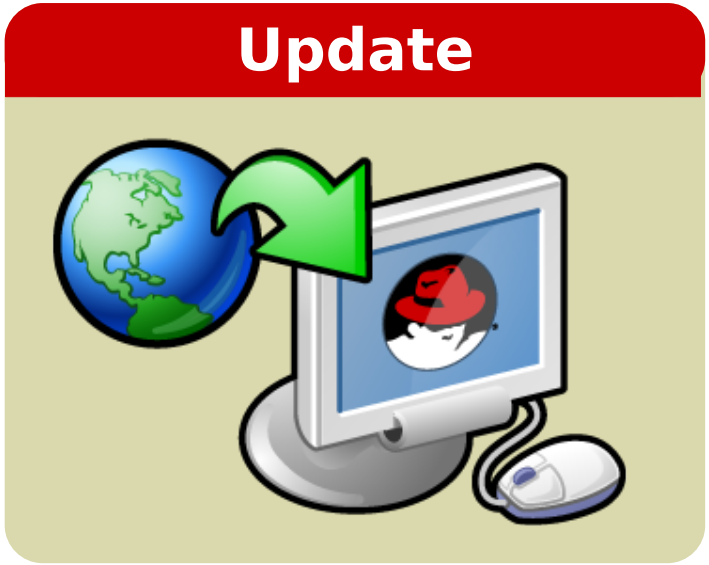


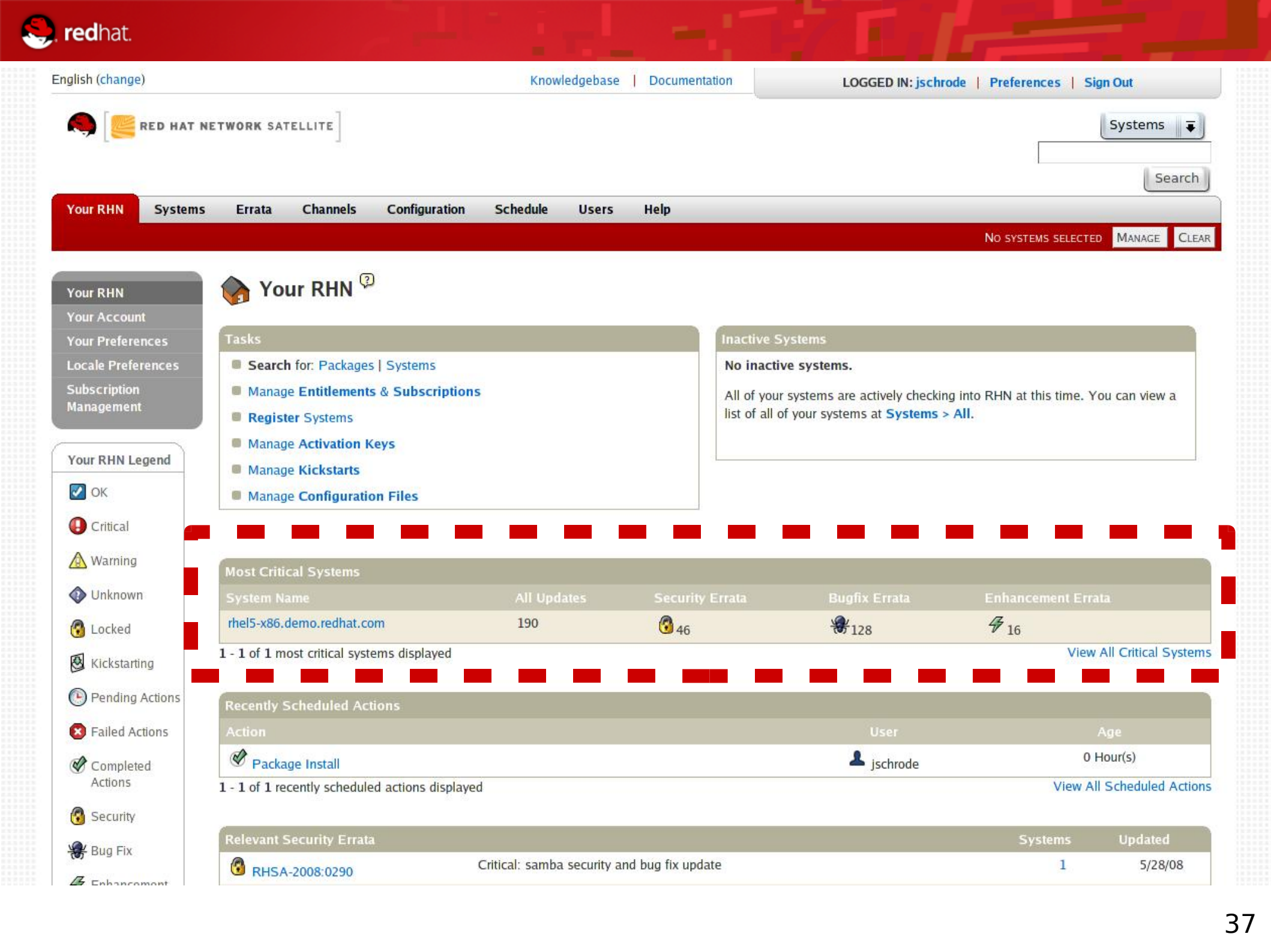
- Enterprise solution, enhanced control
- All system information stored locally on your network
- Custom content distribution
- Ability to run disconnected from internet

RHN Satellite Deployment Model



What is Red Hat Network?

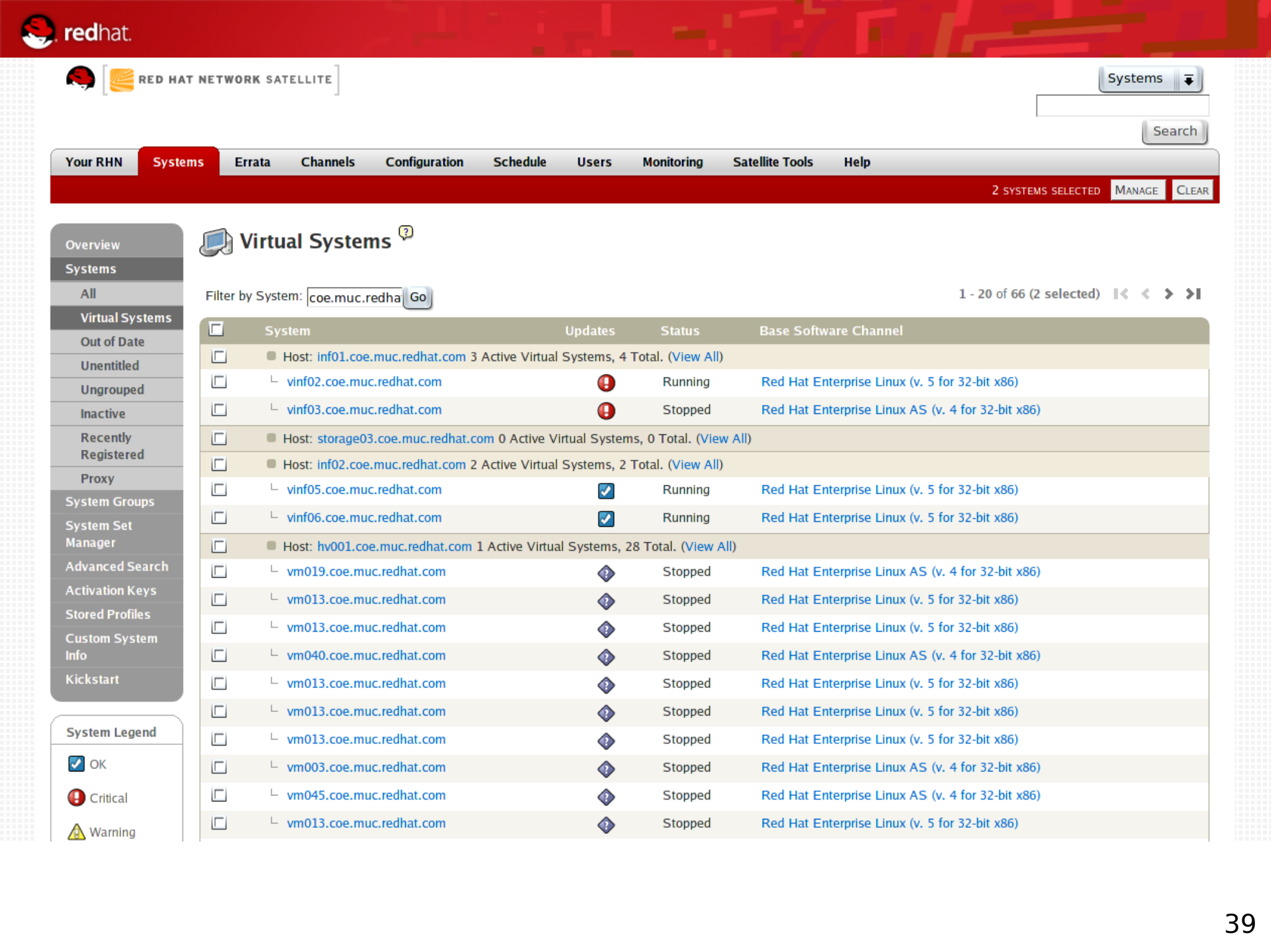



redhat
English (change)
Knowledgebase | Documentation
LOGGED IN: jschrode | Preferences | Sign Out
RED HAT NETWORK SATELLITE
Systems
Search
Your RHN
Systems
Errata
Channels
Configuration
Schedule
Users
Help
NO SYSTEMS SELECTED
MANAGE
CLEAR
Your RHN
Your Account
Your Preferences
Locale Preferences
Subscription Management
Your RHN Legend
OK
Critical
Warning
Unknown
Locked
Kickstarting
Pending Actions
Failed Actions
Completed Actions
Security
Bug Fix
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.
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

What is Red Hat Network?

Update

Manage


redhat
RED HAT NETWORK SATELLITE
Systems
Search
Your RHN
Systems
Errata
Channels
Configuration
Schedule
Users
Monitoring
Satellite Tools
Help
2 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
System Legend
OK
Critical
Warning
Virtual Systems
Filter by System: coe.muc.redha Go
1 - 20 of 66 (2 selected)
System
Updates
Status
Base Software Channel
Host: inf01.coe.muc.redhat.com 3 Active Virtual Systems, 4 Total. (View All)
vinf02.coe.muc.redhat.com Running Red Hat Enterprise Linux (v. 5 for 32-bit x86)
vinf03.coe.muc.redhat.com Stopped Red Hat Enterprise Linux AS (v. 4 for 32-bit x86)
Host: storage03.coe.muc.redhat.com 0 Active Virtual Systems, 0 Total. (View All)
Host: inf02.coe.muc.redhat.com 2 Active Virtual Systems, 2 Total. (View All)
vinf05.coe.muc.redhat.com Running Red Hat Enterprise Linux (v. 5 for 32-bit x86)
vinf06.coe.muc.redhat.com Running Red Hat Enterprise Linux (v. 5 for 32-bit x86)
Host: hv001.coe.muc.redhat.com 1 Active Virtual Systems, 28 Total. (View All)
vm019.coe.muc.redhat.com Stopped Red Hat Enterprise Linux AS (v. 4 for 32-bit x86)
vm013.coe.muc.redhat.com Stopped Red Hat Enterprise Linux (v. 5 for 32-bit x86)
vm013.coe.muc.redhat.com Stopped Red Hat Enterprise Linux (v. 5 for 32-bit x86)
vm040.coe.muc.redhat.com Stopped Red Hat Enterprise Linux AS (v. 4 for 32-bit x86)
vm013.coe.muc.redhat.com Stopped Red Hat Enterprise Linux (v. 5 for 32-bit x86)
vm013.coe.muc.redhat.com Stopped Red Hat Enterprise Linux (v. 5 for 32-bit x86)
vm013.coe.muc.redhat.com Stopped Red Hat Enterprise Linux (v. 5 for 32-bit x86)
vm003.coe.muc.redhat.com Stopped Red Hat Enterprise Linux AS (v. 4 for 32-bit x86)
vm045.coe.muc.redhat.com Stopped Red Hat Enterprise Linux AS (v. 4 for 32-bit x86)
vm013.coe.muc.redhat.com Stopped Red Hat Enterprise Linux (v. 5 for 32-bit x86)

What is Red Hat Network?

Update

Manage

Provision

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
```

What is Red Hat Network?

Update

Manage

Provision

Monitor

RHN Satellite Is Now Open Source

http://spacewalk.redhat.com

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

Thank You

Shawn Wells
Solutions Architect
Lead, Linux on System z

Email: swells@redhat.com
Phone: +1 443 534 0130

http://redhat.com/z

Useful Links

- Technical mailing list (linux-390@vm.marist.edu)
  - Subscribe: http://www2.marist.edu/htbin/wlvindex?linux-390
  - Archive: http://www.mail-archive.com/linux-390@vm.marist.edu/
- RHEL 5 Virtualization Cookbook
  - http://www.linuxvm.org/present/misc/virt-cookbook-RH5.pdf
  - Update to 5.2 coming soon (currently under technical review)
- Presentations from SHARE user conferences and other links
  - http://www.linuxvm.org/present/
  - http://www.linuxvm.org/

http://www.redhat.com/z

Open Discussion

Supplemental:
Red Hat Use Case

System z Use Case: How Red Hat Uses Z

- IBM zSeries 2094 (z9)
- IBM zSeries 2084 (z990)
- Shark storage (ESS unit 2105, 16 full drawers of disk)
  - Provided via FCP layer emulation
- Fully loaded z10 comes July '08

System z Use Case: How Red Hat Uses Z

- **Training (internal/external)**
- **Development VMs**
  - s390-utils, kernel, integrating DeveloperWorks, etc
- **Quality Engineering**
  - VM for each RHEL distro released since RHEL 4 (4.0, 4.1..... 5.1)
- **Support Desk**
  - Emulating user problems

System z Use Case: How Red Hat Uses Z

- **JBoss Development (dev, test, prod)**
- **Red Hat Network Development (dev, test, prod)**
- **Enterprise IPA Development (dev, test, prod)**
- **Cross compilation of all RHEL architectures**
- **Staff accounts (sandbox environments, demos)**

System z Use Case: How Red Hat Z

- **Red Hat Network for deployment of new VMs, patching**
  - Managed by one staff member
    - Allows patching, reprovision z/VM guests, etc

Most Critical Systems

System Name	All Updates	Security Errata
beltbuckle	226	46
RHT_Laptop	246	41
IAD_DevBox	204	32
IAD_DevBox1	161	19
RHT-IAD_turtle	7	5

1 - **5** of **5** 'Most Critical' systems displayed

System z Use Case: How Red Hat Z

- **RHN for Z: Lesson Learned**
  - When configuring the kickstart through the web interface, choose Static IP instead of DHCP.
  - In the Extra Kernel Parameters text box, enter the information normally found in the CMS CONF file.
    - Single line!

```
DASD=100 HOSTNAME=example IPADDR=192.168.5.100 ...
```

Documented at:

http://kbase.redhat.com/faq/FAQ_49_12902.shtm

Supplemental:
RHEL 5.2 Bug Fixes

RHEL 5.2 Bug Fixes, Installer Related

- BZ: https://bugzilla.redhat.com/show_bug.cgi?id=237508 [Private]
  - Summary: LCS device not found at install
- BZ: https://bugzilla.redhat.com/show_bug.cgi?id=305331 [Private]
  - Summary: sudo-1.6.8p12-10 segfaults when using ldap on s390
- BZ: https://bugzilla.redhat.com/show_bug.cgi?id=354661 [Private]
  - Summary: multipath paths fail using PAV Devices on DS8000 DS6000
- BZ: https://bugzilla.redhat.com/show_bug.cgi?id=279201 [Private]
  - Summary: zfcpconf.sh fails in rc.sysinit if / partition and /usr partition are separated

RHEL 5.2 Bug Fixes, Storage Related

- BZ: https://bugzilla.redhat.com/show_bug.cgi?id=360701 [Private]
  - Summary: swap_dup: Bad swap file entry <xxxxxxxx> without swap configured
- BZ: https://bugzilla.redhat.com/show_bug.cgi?id=360611 [Private]
  - Summary: FICON DS8000: File ID Miscompare after CHPID off via HMC

RHEL 5.2 Bug Fixes, I/O Related

- BZ: https://bugzilla.redhat.com/show_bug.cgi?id=360821 [Private]
  - Summary: qdio: too many interrupts on qdio-driven devices
- BZ: https://bugzilla.redhat.com/show_bug.cgi?id=360631 [Private]
  - Summary: qdio: time calculation is wrong
- BZ: https://bugzilla.redhat.com/show_bug.cgi?id=354801 [Private]
  - Summary: cio: Disable channel path measurements on shutdown/reboot
- BZ: https://bugzilla.redhat.com/show_bug.cgi?id=354831 [Private]
  - Summary: cio: Handle invalid subchannel set id in stsch
- BZ: https://bugzilla.redhat.com/show_bug.cgi?id=354821 [Private]
  - Summary: cio: Device status validity

RHEL 5.2 Bug Fixes, Networking Related

- BZ: https://bugzilla.redhat.com/show_bug.cgi?id=281241 [Private]
  - Summary: tcpdump does not show outgoing packets with fake_ll=1
- BZ: https://bugzilla.redhat.com/show_bug.cgi?id=354891 [Private]
  - Summary: qeth: recognize/handle RC=19 from Hydra 3 OSA
- BZ: https://bugzilla.redhat.com/show_bug.cgi?id=354851 [Private]
  - Summary: qeth: increment sequence number for incoming packets
- BZ: https://bugzilla.redhat.com/show_bug.cgi?id=267381 [Private]
  - Summary: QDIO based network connections hang with QIOASSIST ON

RHEL 5.2 Bug Fixes, Stability Related, p1

- BZ: https://bugzilla.redhat.com/show_bug.cgi?id=360591 [Private]
  - Summary: Operating System Message: Kernel panic - not syncing: Fatal exception in interrupt
- BZ: https://bugzilla.redhat.com/show_bug.cgi?id=253275 [Private]
  - Summary: Placing a kprobe on 'bc' instruction can crash the system
- BZ: https://bugzilla.redhat.com/show_bug.cgi?id=354811 [Private]
  - Summary: I/O stall, system crash due to scanning for units from FC transport class
- BZ: https://bugzilla.redhat.com/show_bug.cgi?id=354871 [Private]
  - Summary: qdio: System hang with zfcp in case of adapter problems

RHEL 5.2 Bug Fixes, Stability Related, p2

- BZ: https://bugzilla.redhat.com/show_bug.cgi?id=350861 [Private]
  - Summary: Kernel panic with lcs interface as dhcp server
- BZ: https://bugzilla.redhat.com/show_bug.cgi?id=330211 [Private]
  - Summary: qeth: crash during reboot after failing online setting
- BZ: https://bugzilla.redhat.com/show_bug.cgi?id=380981 [Private]
  - Summary: Kernel Panic during activation of OSA-devices with fake_ll
- BZ: https://bugzilla.redhat.com/show_bug.cgi?id=325451
  - Summary: ptrace compatibility problem with PTRACE_{PEEK,POKE}USR_AREA