Linux Containers Overview & Roadmap

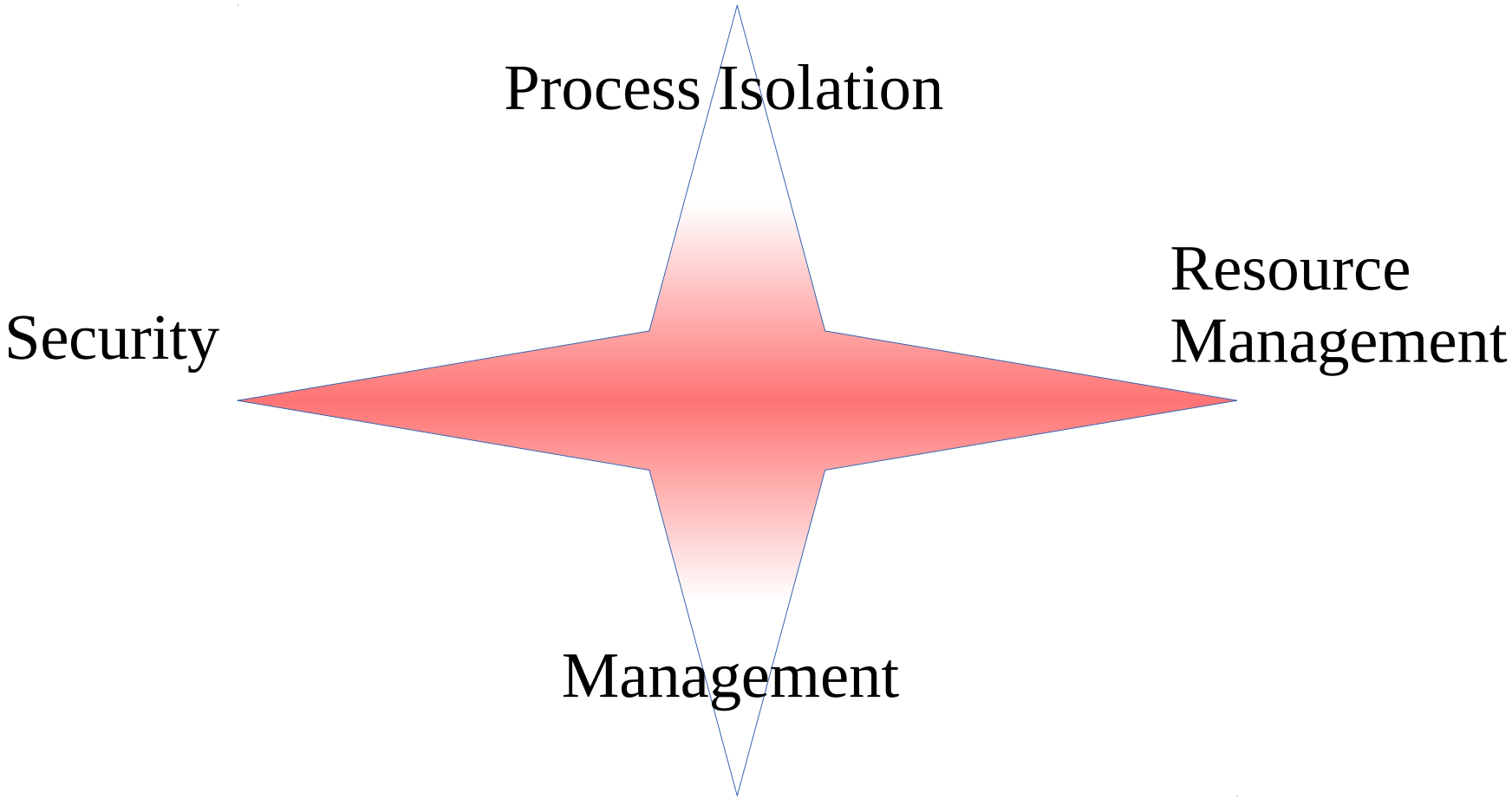
Bhavna Sarathy
Senior Product Manager, Red Hat

Dan Walsh
Senior Principal Software Engineer, Red Hat

June 12 2013

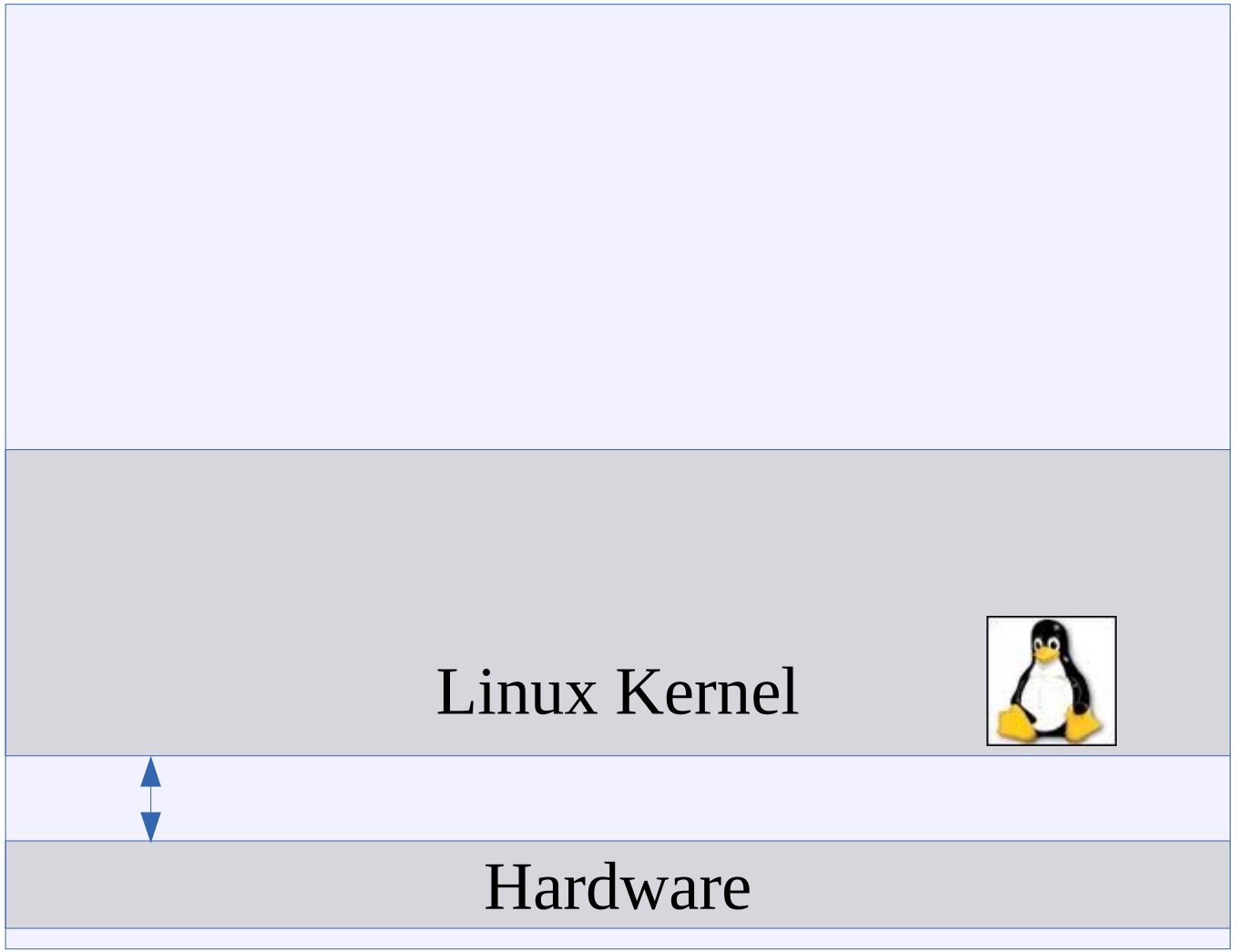
redhat.

Key elements of Linux Containers

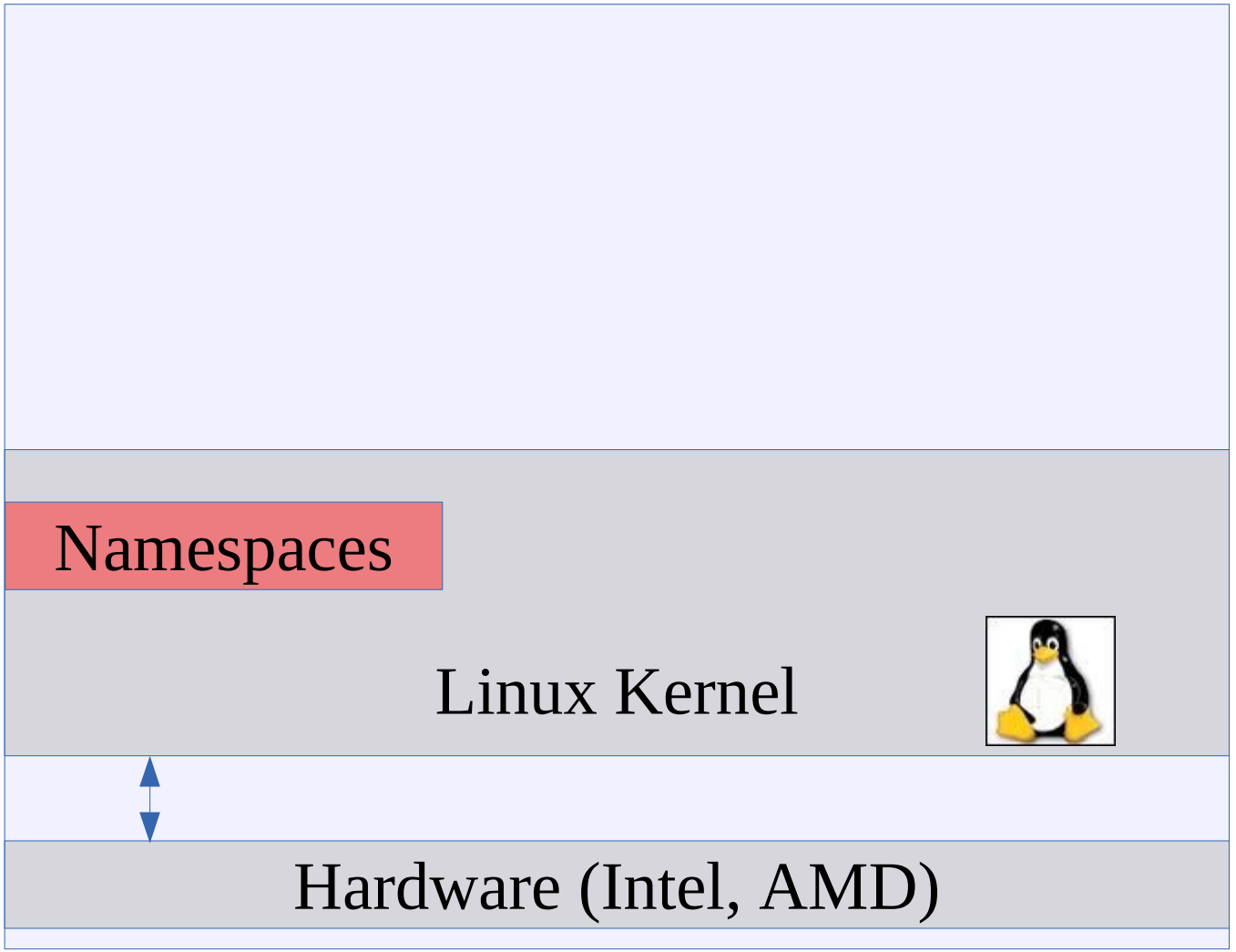


Linux Container Architecture

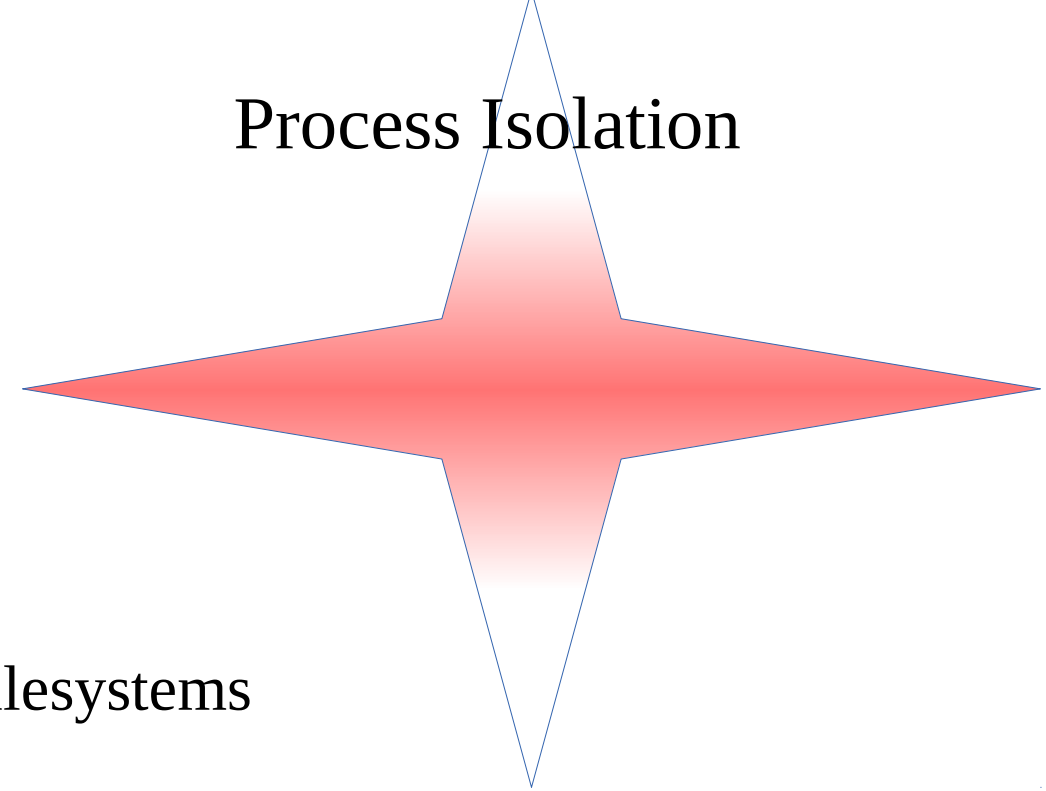
Red Hat Enterprise Linux Container Architecture



Red Hat Enterprise Linux Container Architecture

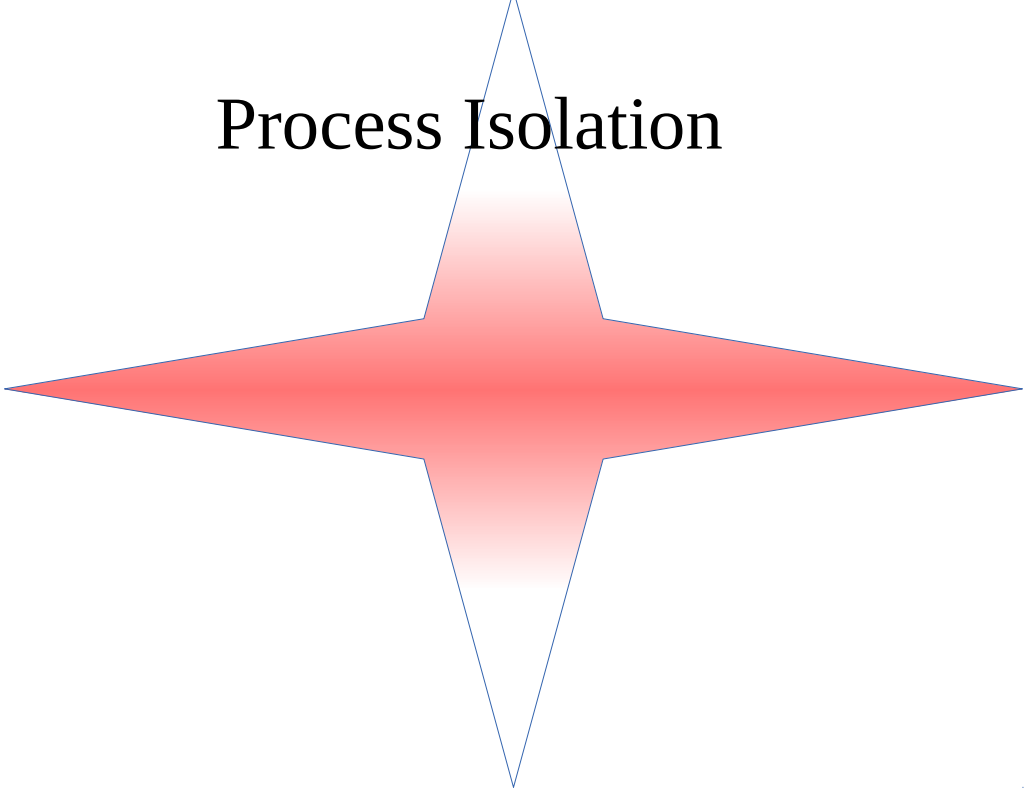


Namespaces



Mount : mounting/unmounting filesystems
UTS : hostname, domainname
IPC : SysV message queues, semaphore/shared memory segments
Network: IPv4/IPv6 stacks, routing, firewall
PID: Private /proc, multiple pid 1's
User: (UID) Just showing up in the Kernel now.

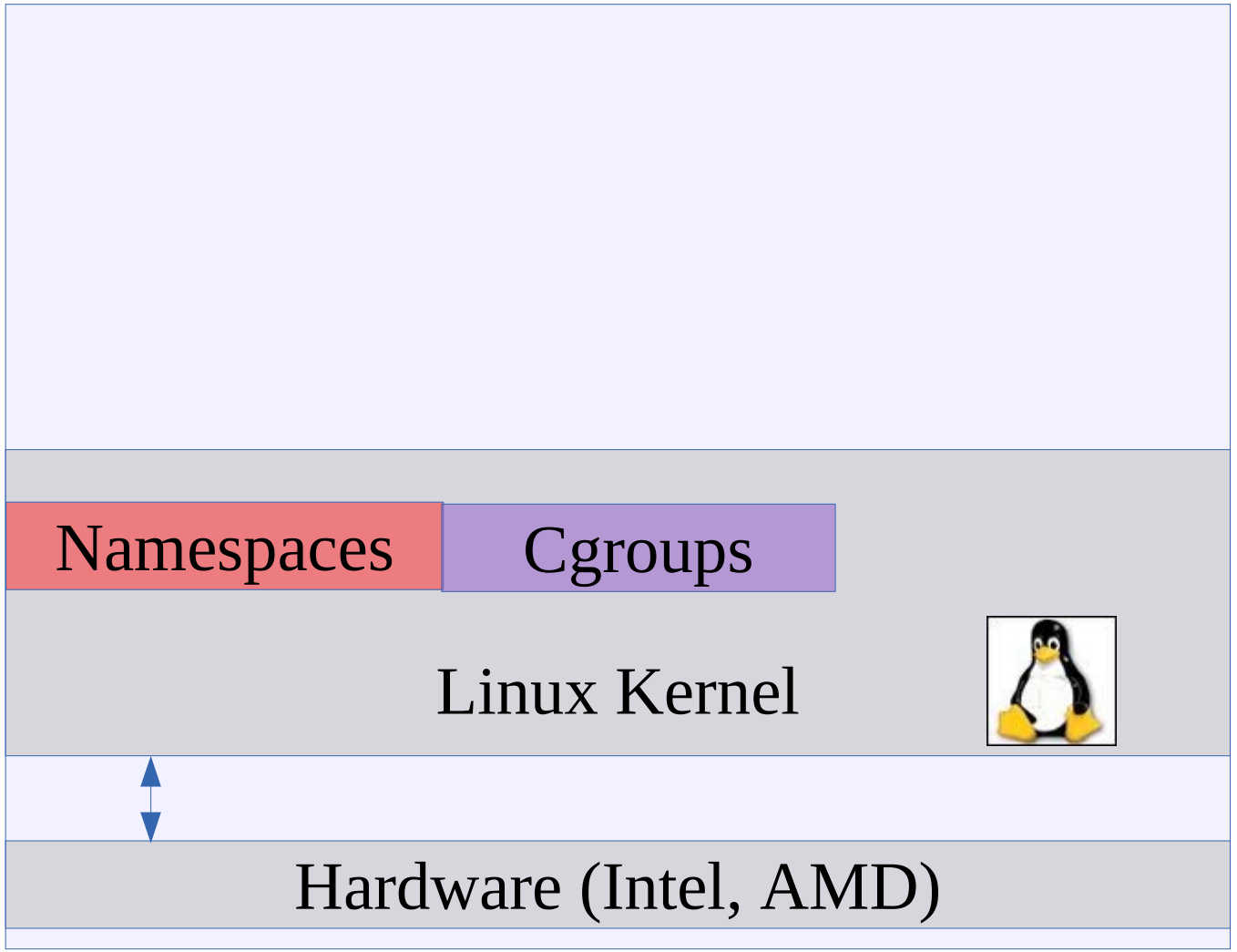
- Not planning on supporting in RHEL7.



Namespace Use

- pam_namespace - RHEL5/6
- SELinux sandbox - RHEL6
- SystemD - Fedora 17
  - UnitFile: PrivateTmp, PrivateNetwork
- Openshift - RHEL6
  - Pam_namespace : Private /tmp

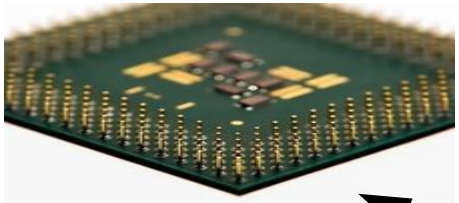
Red Hat Enterprise Linux Container Architecture



Resource Management with Cgroups

Memory

Network



CPU

Block IO

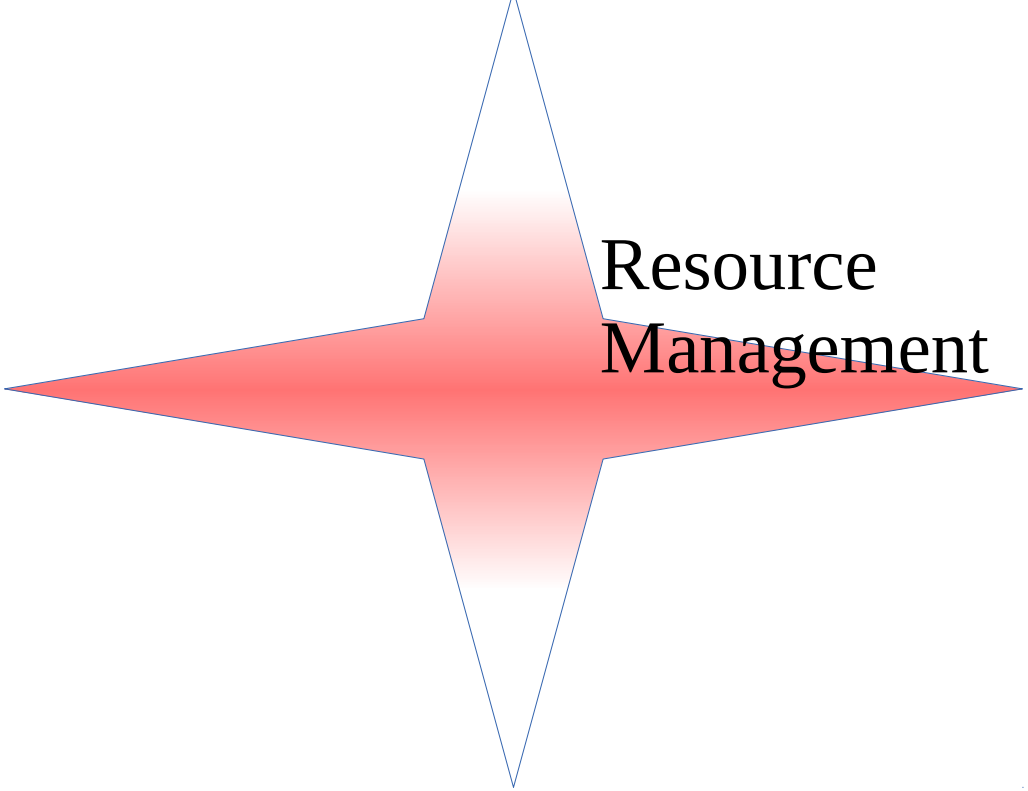
Namespaces

Cgroups

Linux Kernel

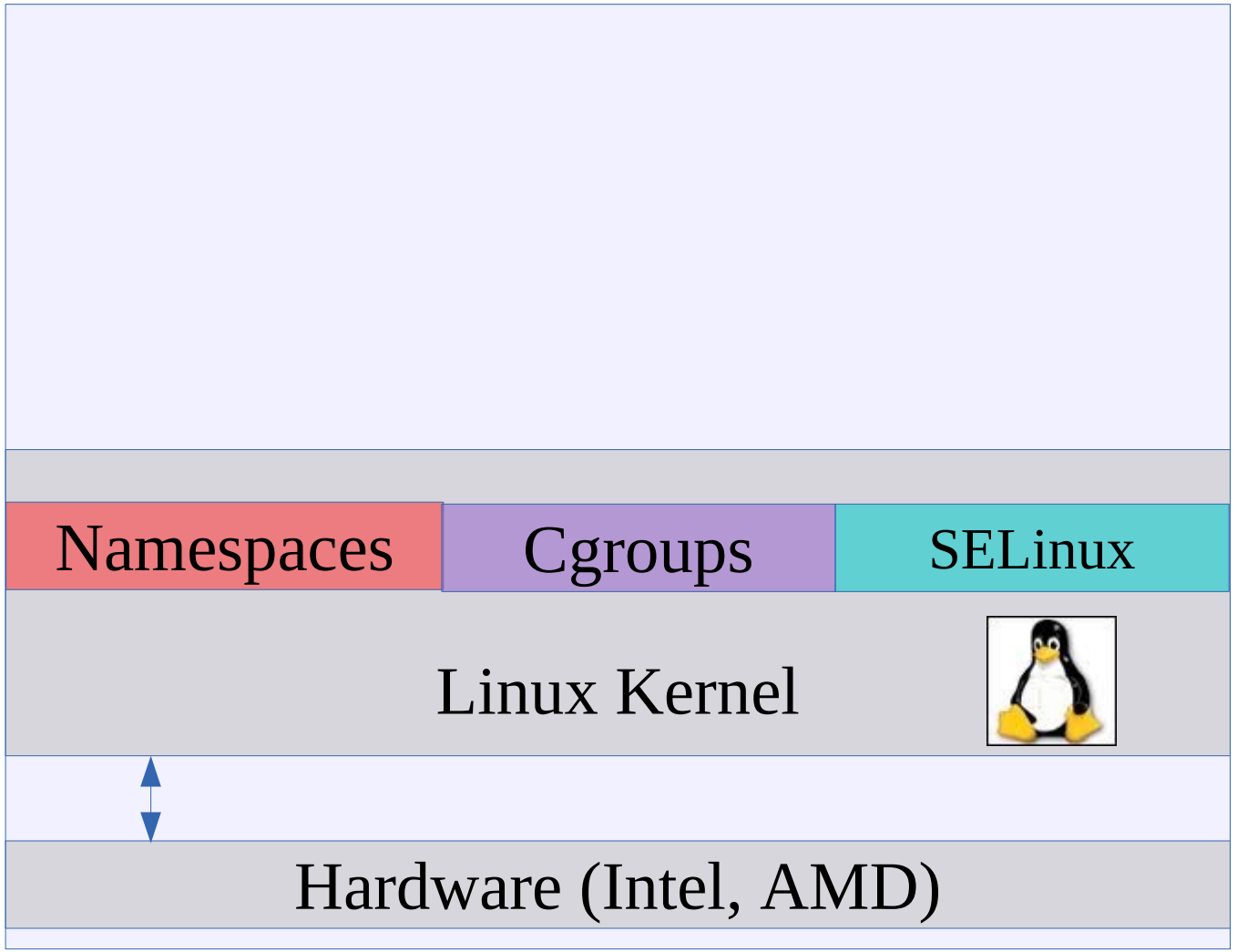
Hardware (Intel, AMD)

Cgroup Use

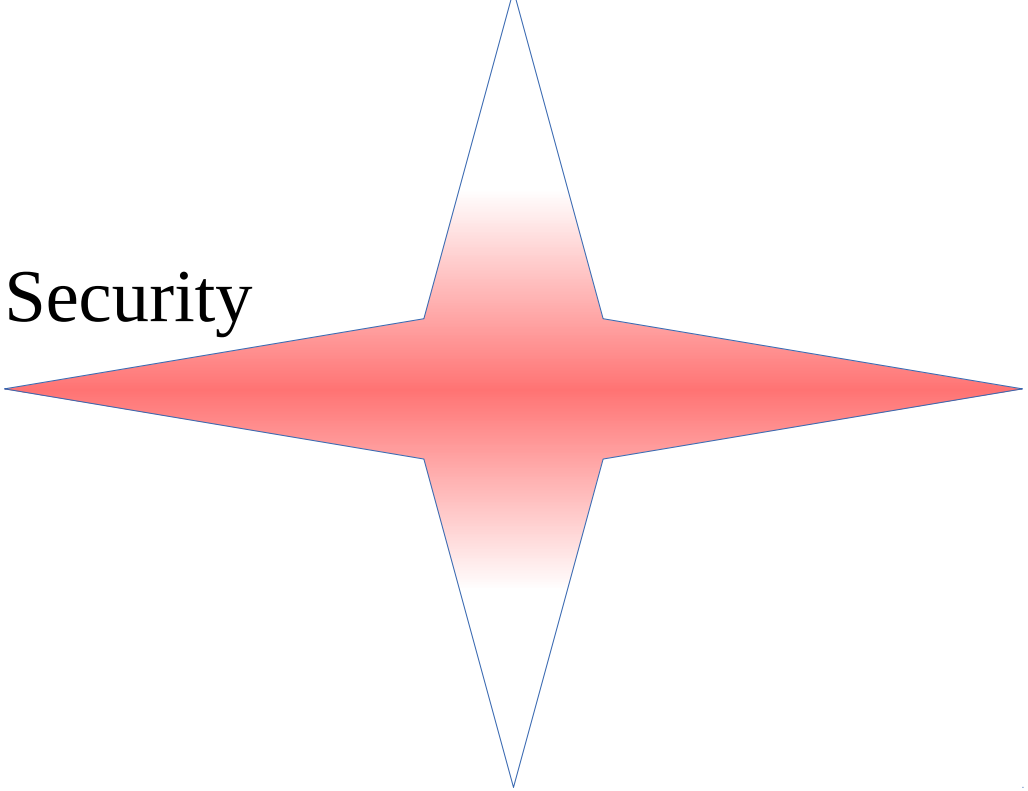


- Libvirt/qemu – RHEL6
- OpenShift - RHEL6
- SystemD - Fedora 18
  - UnitFile: ControlGroup*
- Red Hat Storage Server
  - Gluster - RHEL6

Red Hat Enterprise Linux Container Architecture

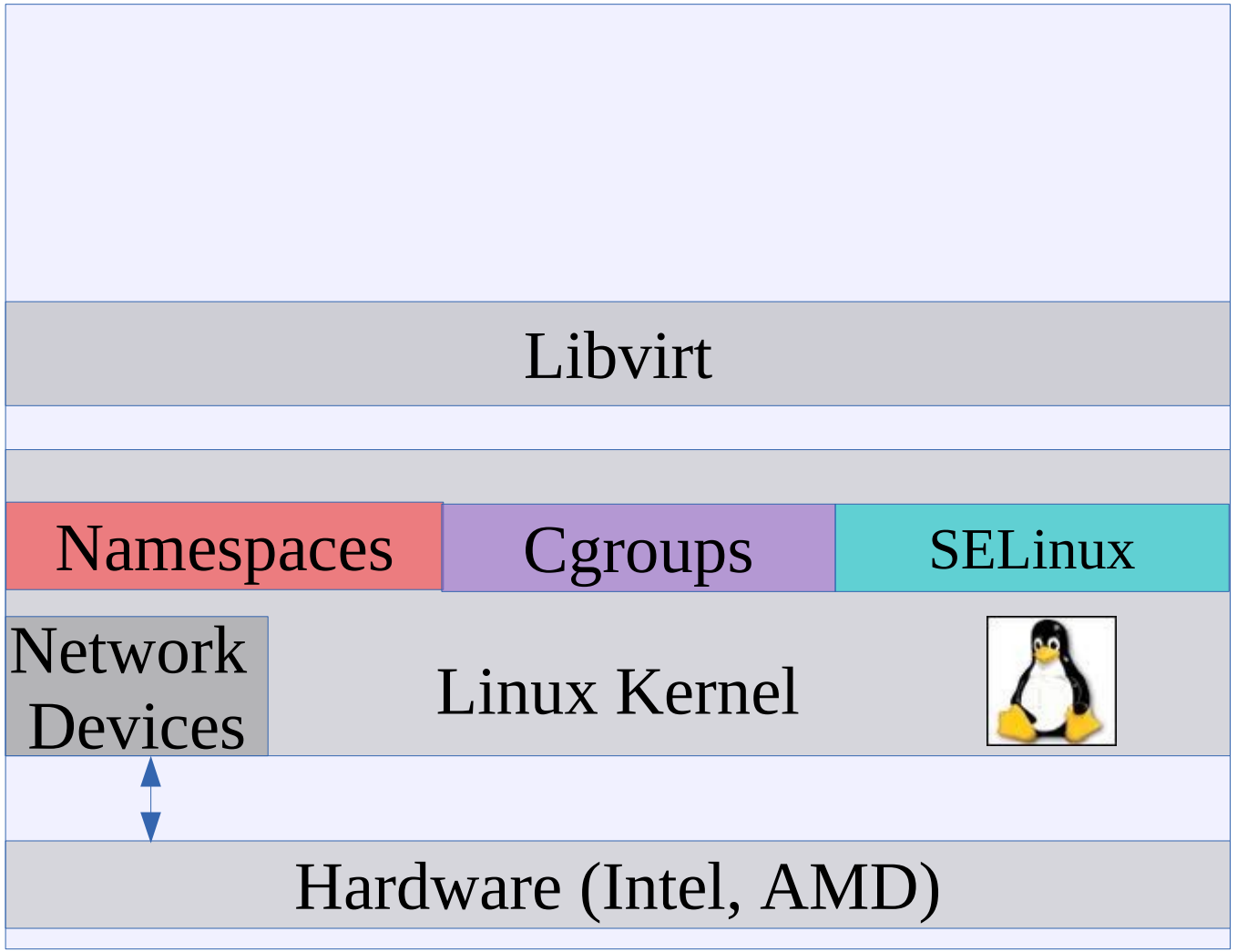


SELinux Use

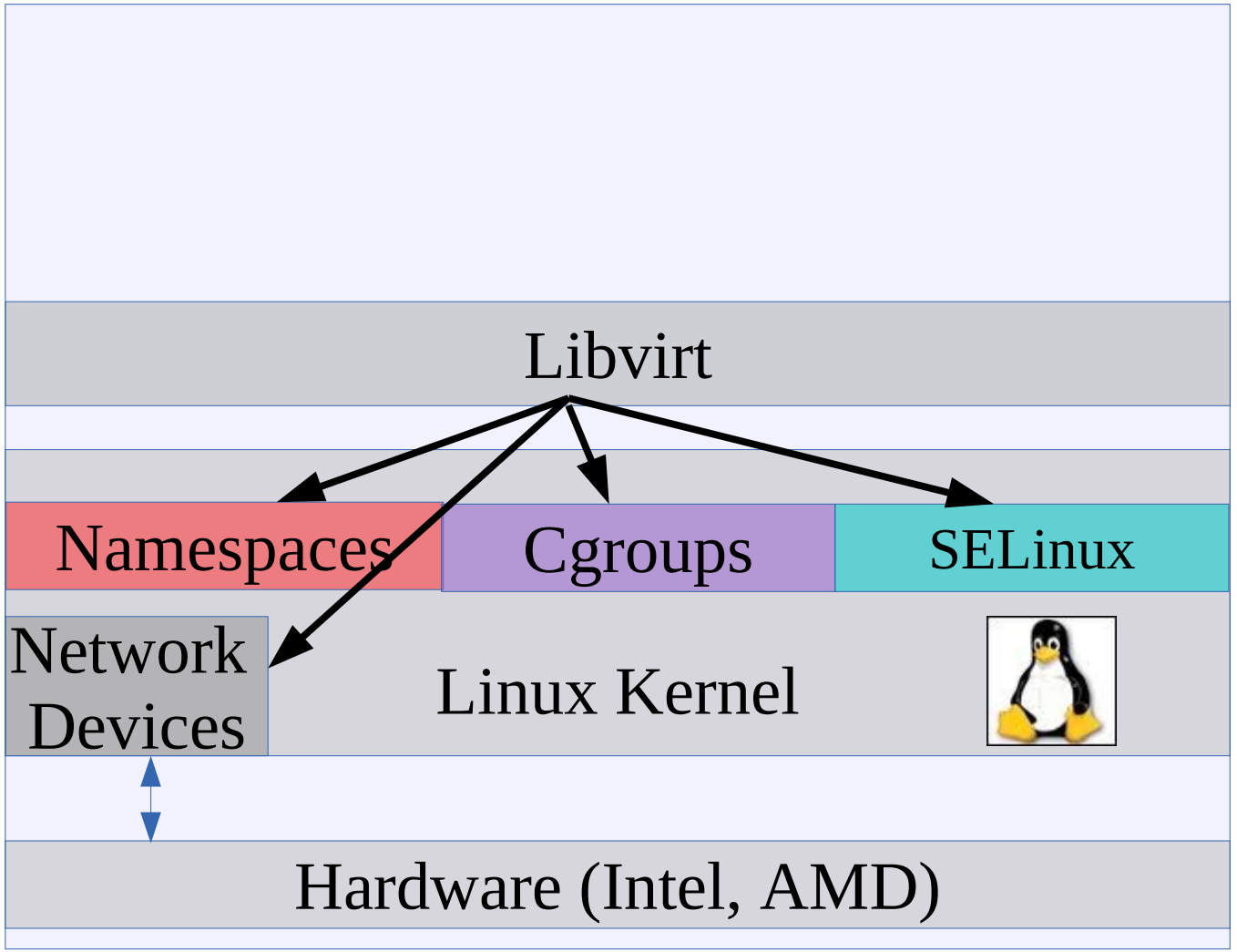


- Targeted - RHEL4
- MLS – RHEL5
- Targeted/MCS - RHEL6
  - sVirt
  - OpenShift
  - sandbox -X

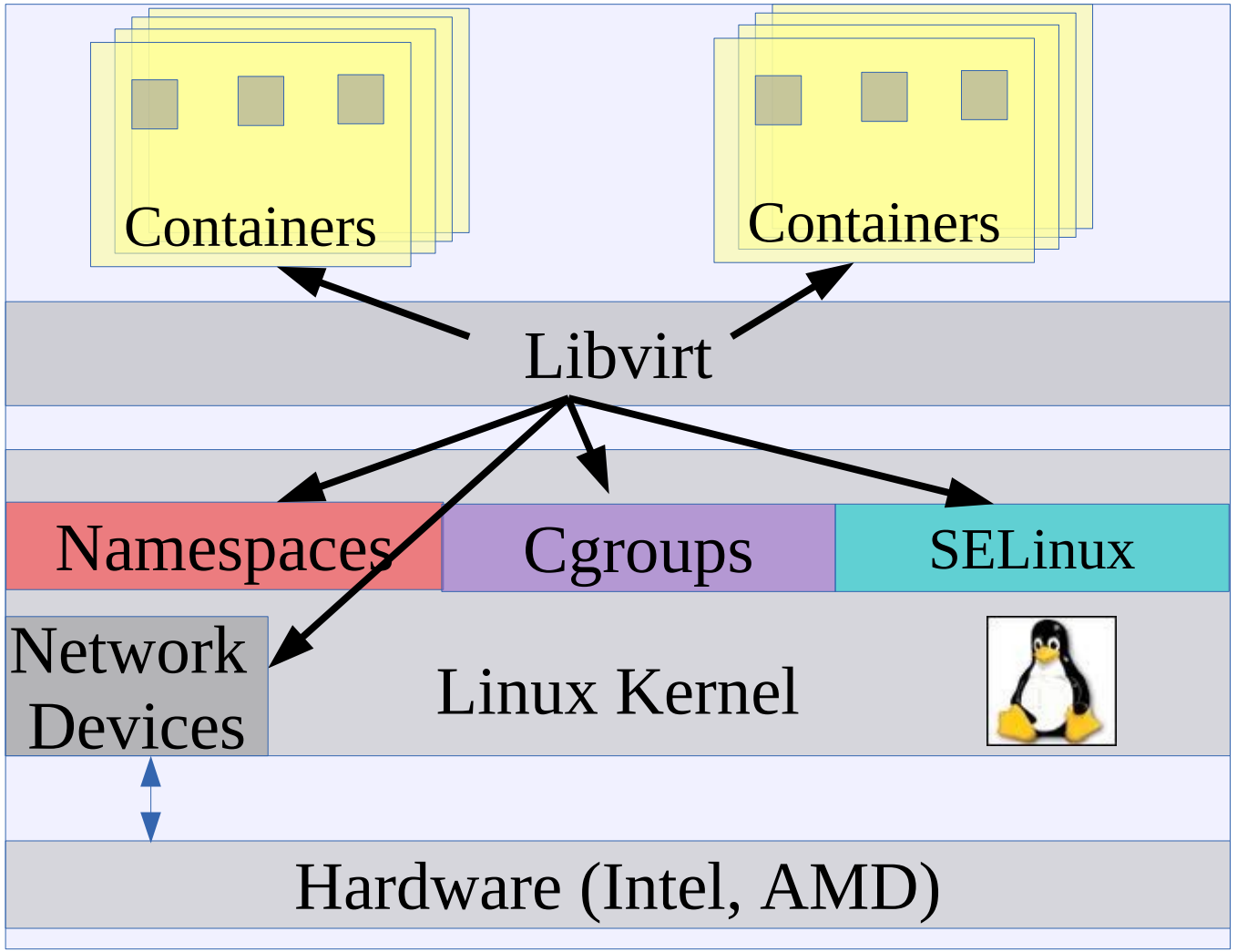
Red Hat Enterprise Linux Container Architecture



Red Hat Enterprise Linux Container Architecture



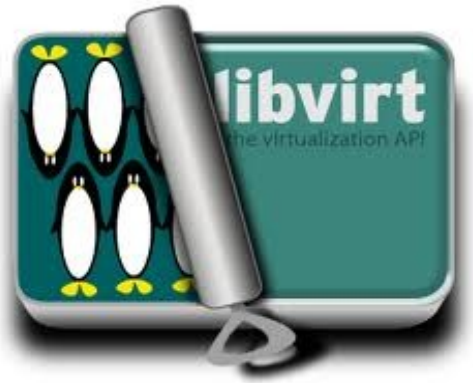
Red Hat Enterprise Linux Container Architecture



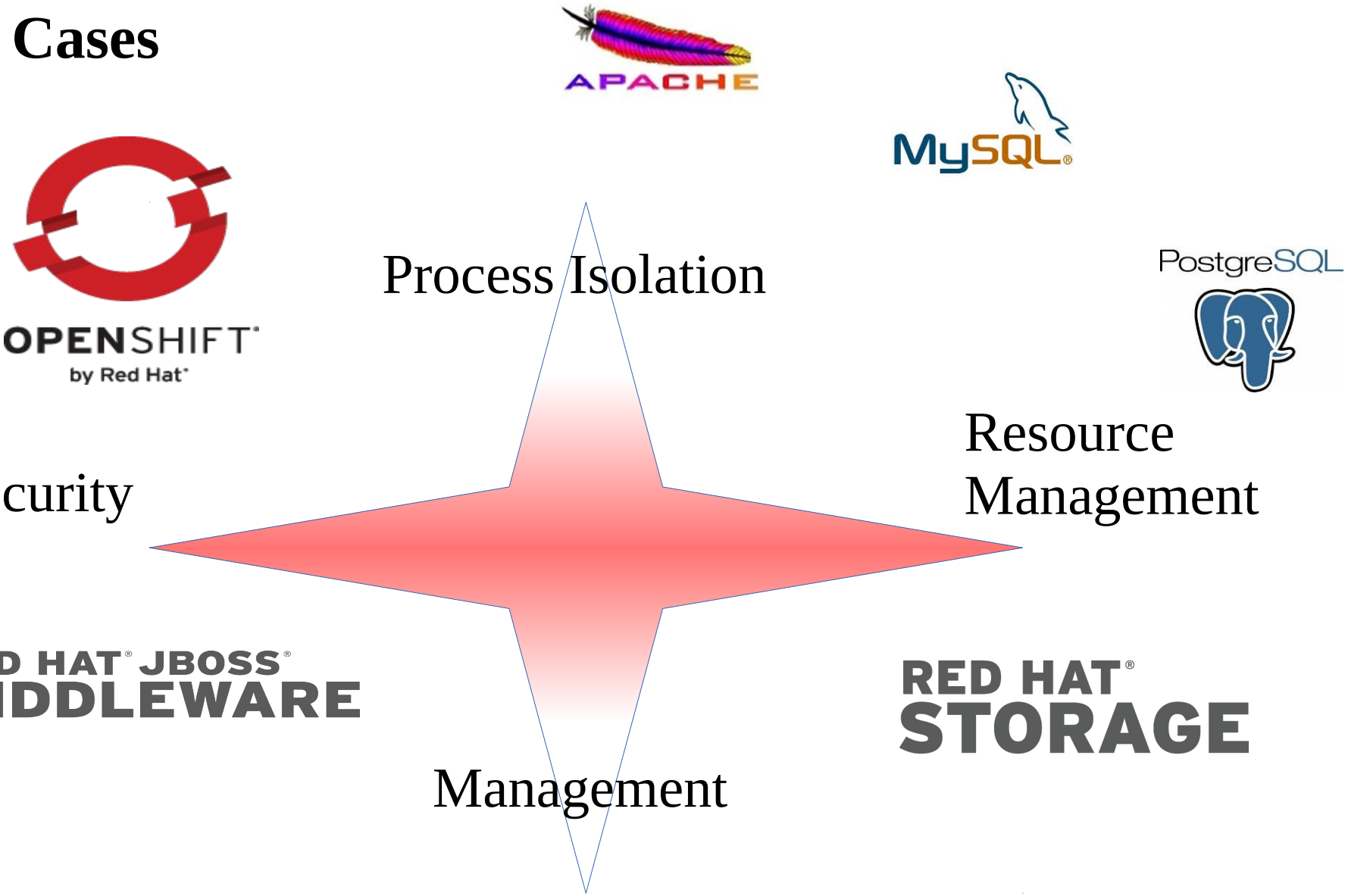
Libvirt Use

- Libvirt - RHEL5, RHEL6
  - Launch Virtual Machines
- Libvirt-lxc – RHEL6.4
  - Launch Containers

Management



Linux Container Use Cases



Containers use cases

Shared RHEL Host Software

- Generic Application Container
- Systemd Application Container

Containers use cases

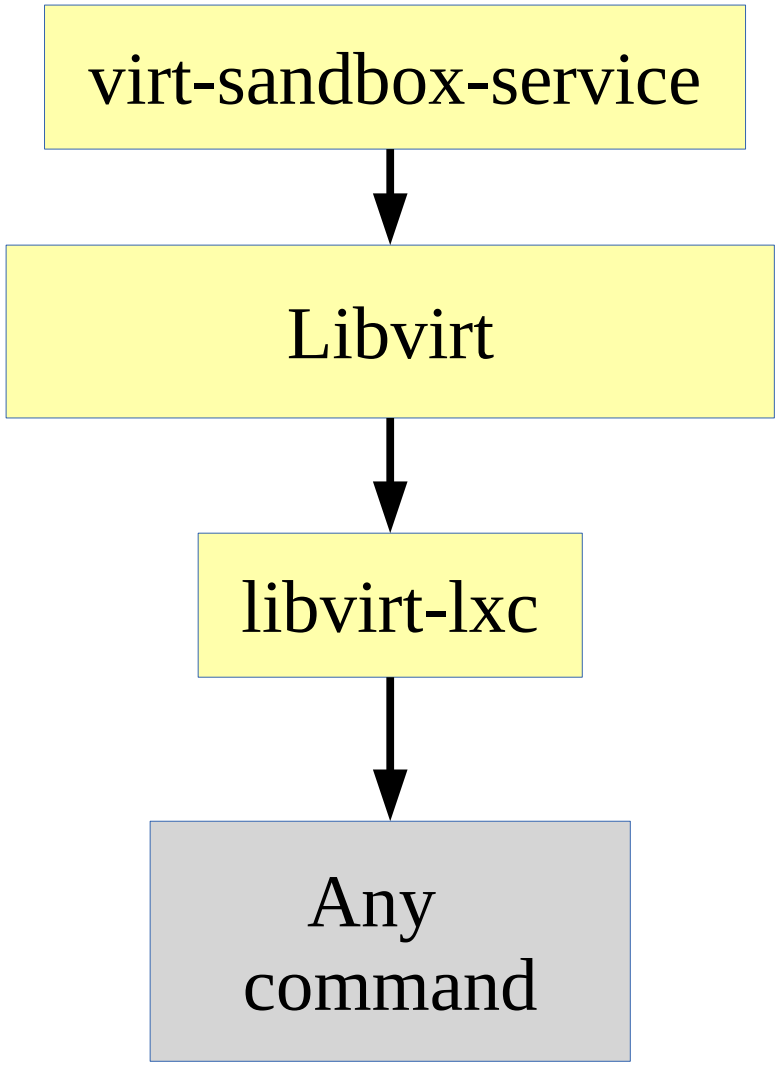
Shared RHEL Host Software

- Generic Application Container
- Systemd Application Container

Unshared OS Software

- Chroot Application Container
- Booted OS Container

Generic Application Container

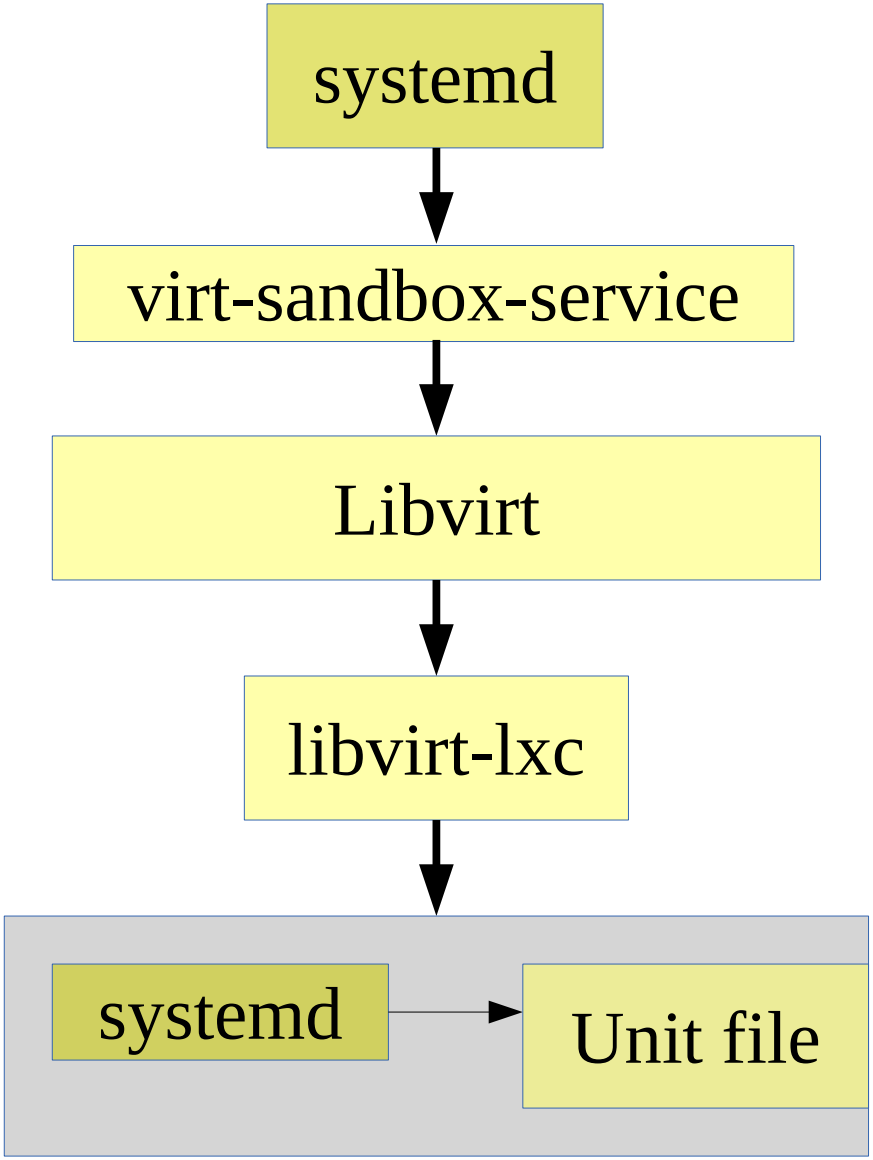


Planned for RHEL 7.0

RED HAT® STORAGE

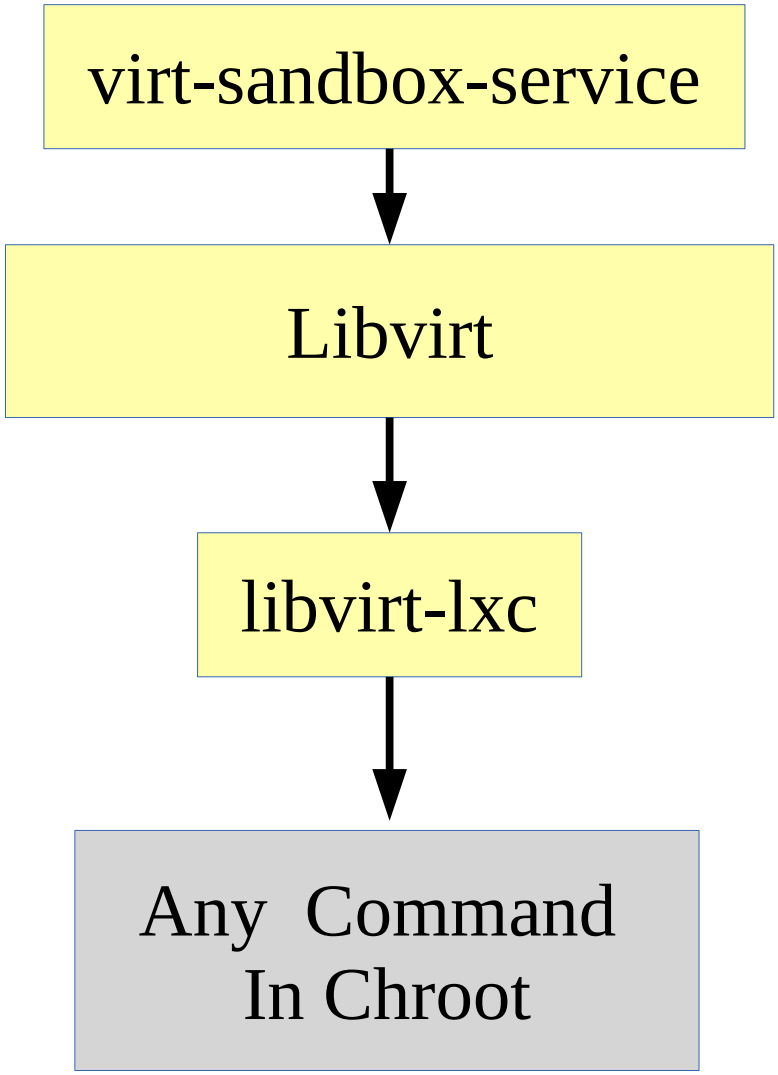
OPENSHIFT by Red Hat®

Systemd Application Container



Planned for RHEL 7.0

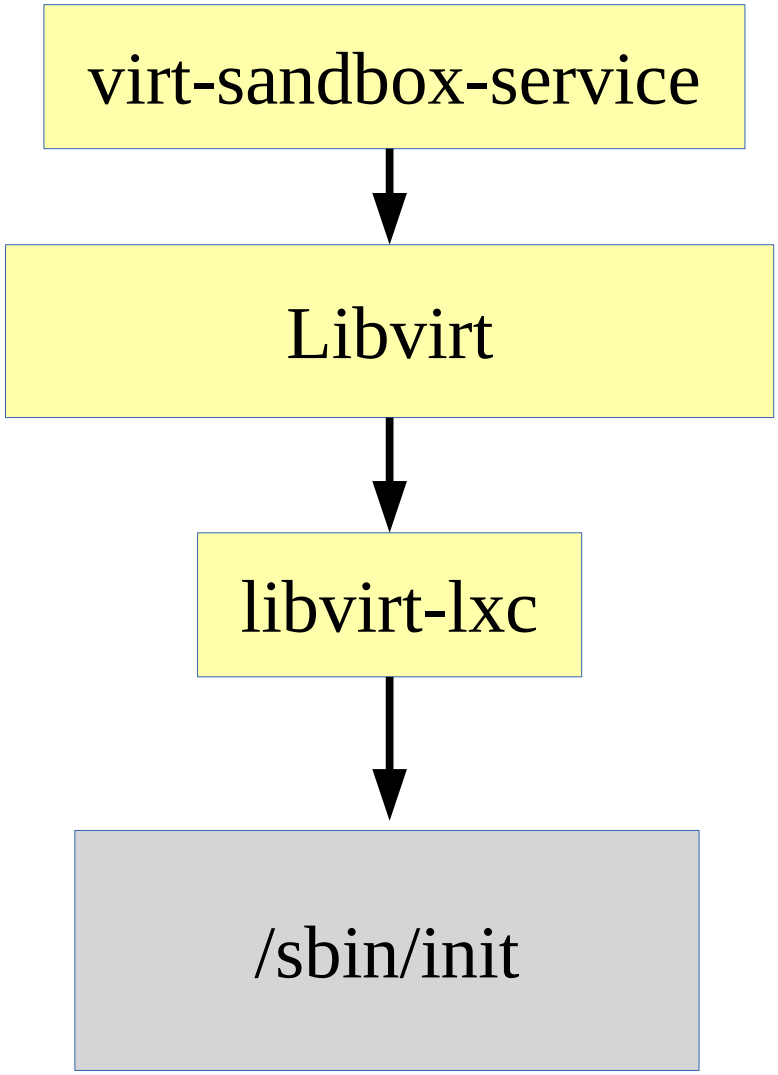
Chroot Application Container



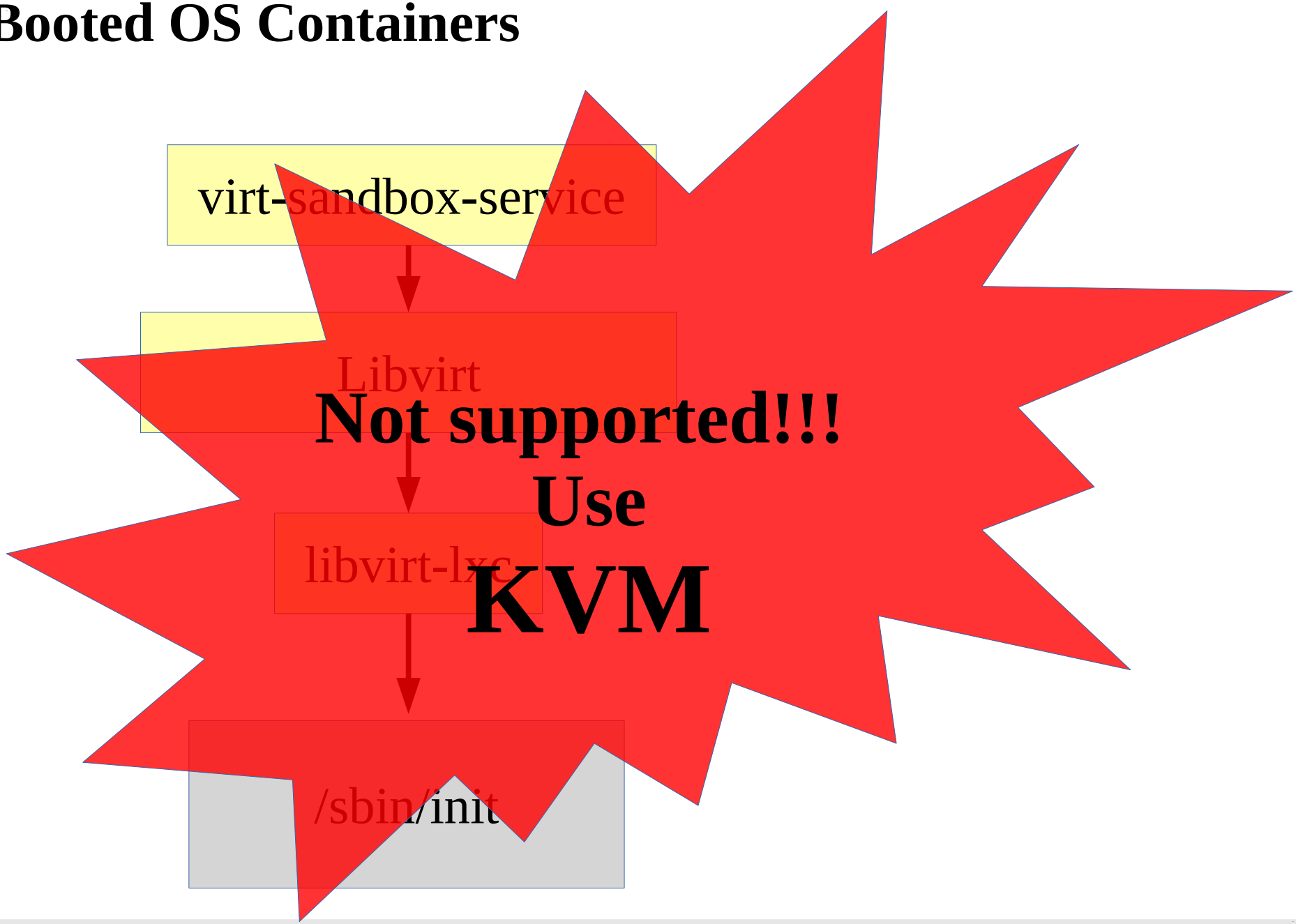
Support TBD in RHEL 7.*

RED HAT® ENTERPRISE LINUX®

Booted OS Container



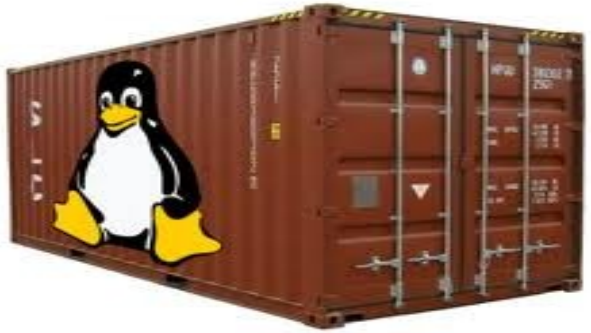
Booted OS Containers



Containers vs KVM Virtualization

When should I use containers and when should I use KVM?

Containers vs KVM Virtualization



- Startup and shutdown speed
- Ease of Maintainance
- Easy to create
- System-wide changes visible in each container
  - For RHEL Shared OS Containers
- Scalability: Number of containers
  - Process Memory Sharing

KVM Virtualization vs Containers

- Boot multiple Different Operating Systems
  - Including Windows
- Separate kernel
  - Better Security
  - Kernel crash does not take down host
- Guest Isolation from host changes
- Full Separation
- Features such as live migration, live storage migration

Linux Containers : Scalability

How many containers can you run?

- Theoritical
  - Scales to 6000 containers and 12000 bind mounts of root filesystem directories
- Practical
  - Running real workloads, containers doing work in parallel

Linux Containers Demo

Future

- Seccomp – Linux syscall restriction
- Better audit support/logging support
- Working UnionFS.
- What's going to break?????

Questions?

Related Summit Sessions

Managing SELinux in the Enterprise

- Wed 4:50 pm, Rm 312

Secure Development Practices

- Thu 1:20 pm, Rm 306

Under the Hood of OpenShift, Turbocharged by RHEL

- Thu 3:40 pm, Rm 304

KVM Hypervisor Roadmap & Technology Update

- Thu 10:40am, Rm 304

Hypervisor Technology Comparison & Migration

- Fri 9:45am, Rm 313

Contact Info

Dan Walsh

Email: dwalsh@redhat.com

Blog: danwalsh.livejournal.com

Twitter: @rhatdan

Bhavna Sarathy

Email: bsarathy@redhat.com