

Linux Containers Roadmap

Red Hat Enterprise Linux 7 RC

Bhavna Sarathy

Senior Technology Product Manager, Red Hat

Linda Wang

Senior Eng. Manager, Red Hat

Bob Kozdemba

Principal Soln. Architect, Red Hat

Define the problem

Benefits

Architecture

Q & A



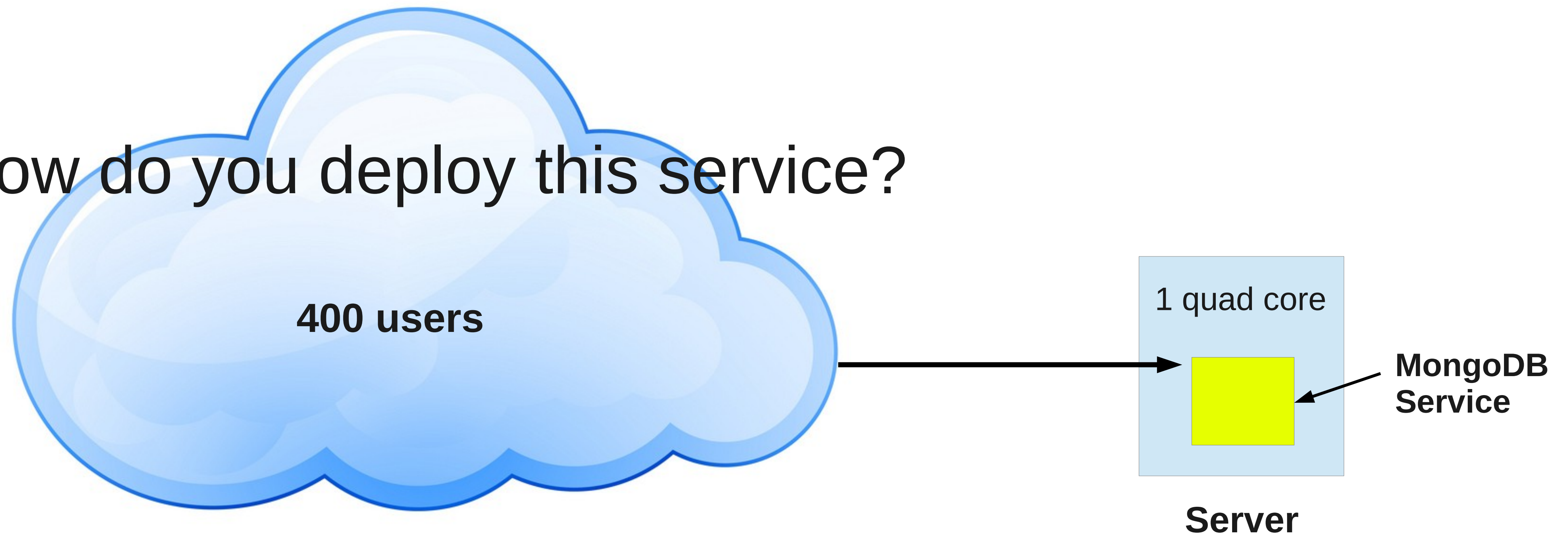
Use Cases

Building Blocks

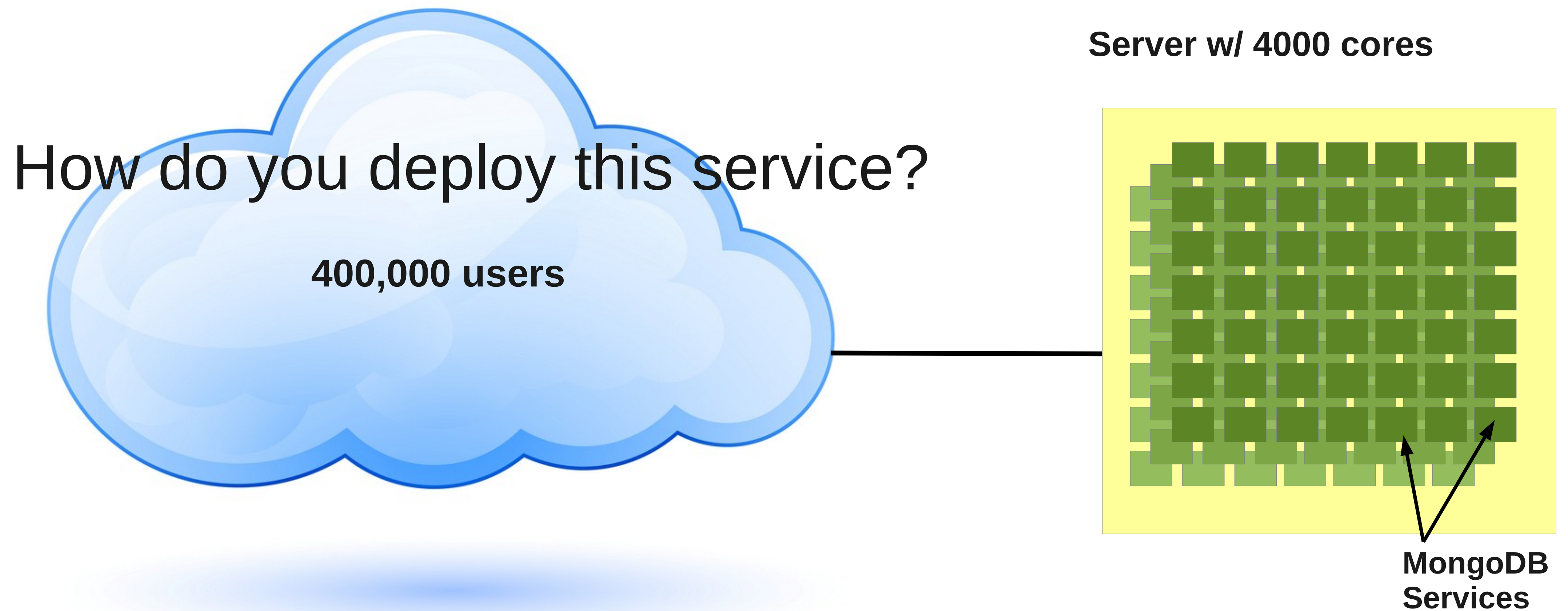
Demo

Defining the problem space

How do you deploy this service?



Defining the problem space

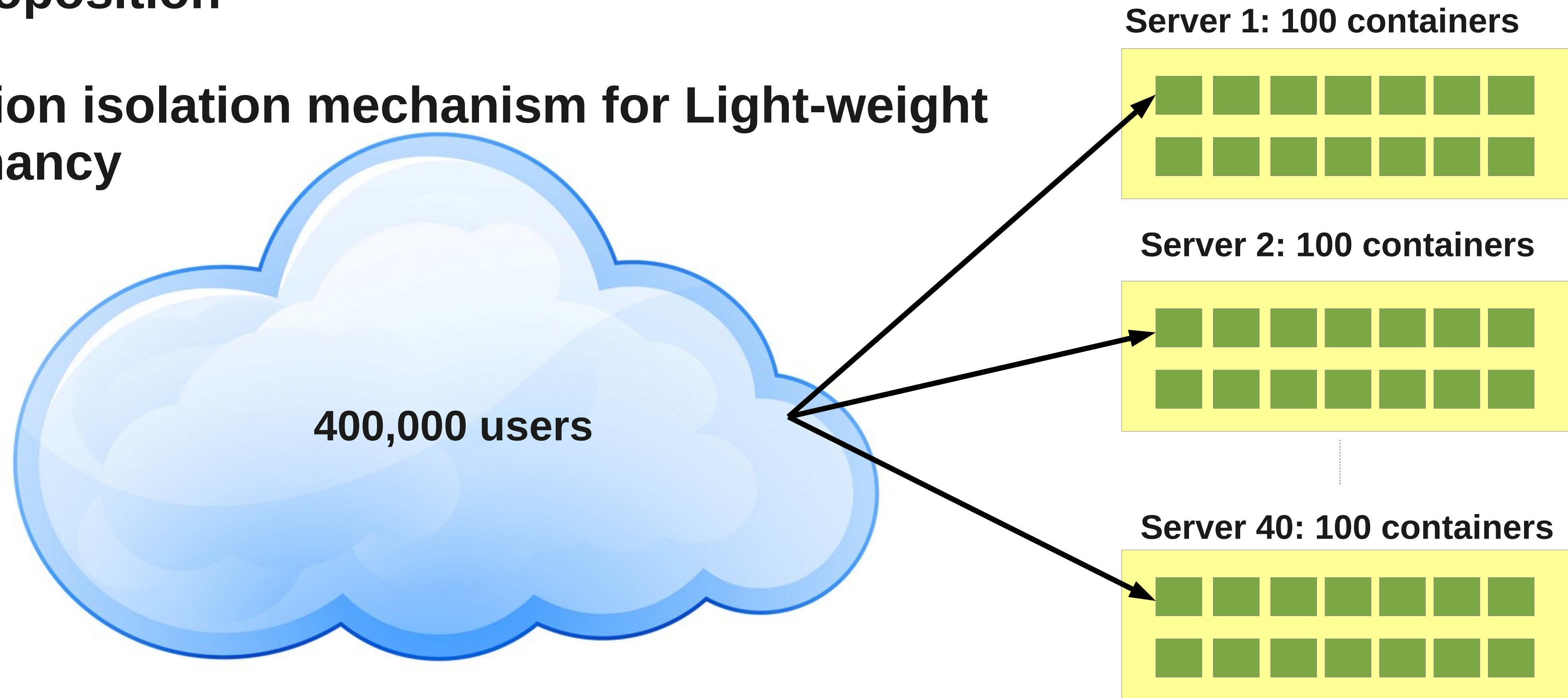




How about Red Hat Linux Containers?

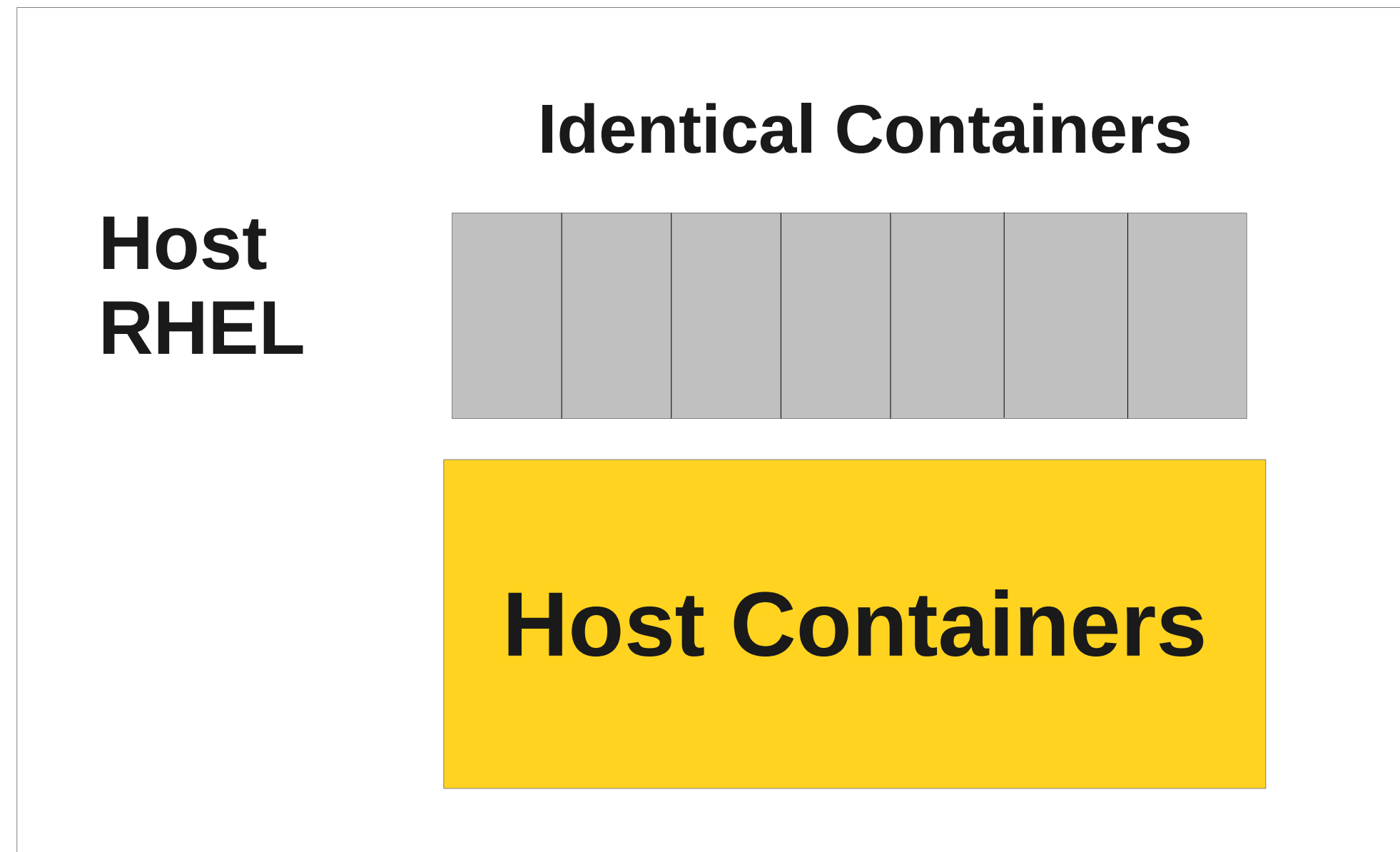
Value Proposition

Application isolation mechanism for Light-weight multi-tenancy



RHEL 7 Linux Containers Use Case 1

Host Containers



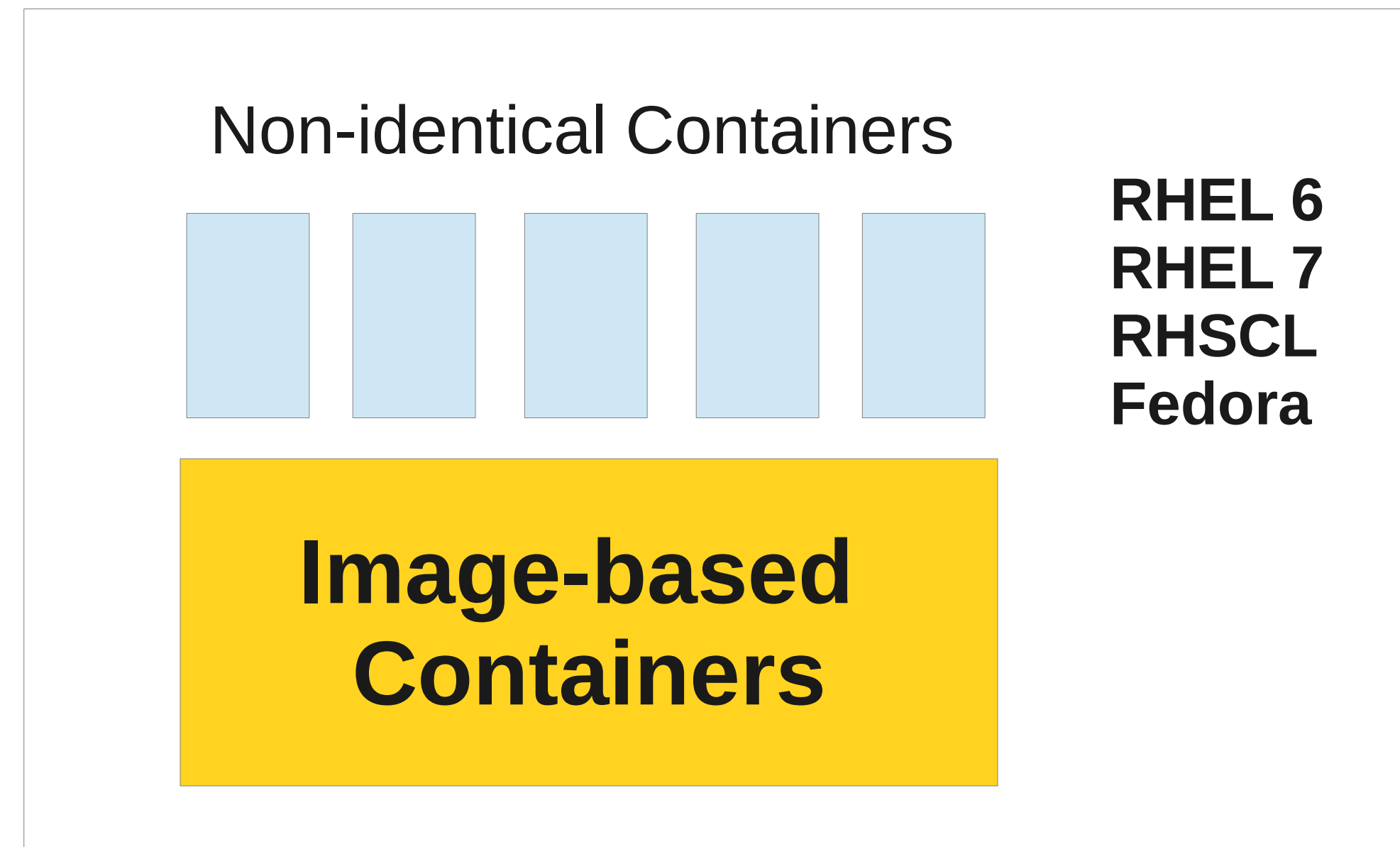
- RHEL 7 host carved into secure containers
- Each container running RHEL 7 userspace
- Pro : Security erratas can be applied easily with “yum update”
- Con : Limited to RHEL 7 runtimes

RHEL 7 Linux Containers Use Case 2

Image-based Containers

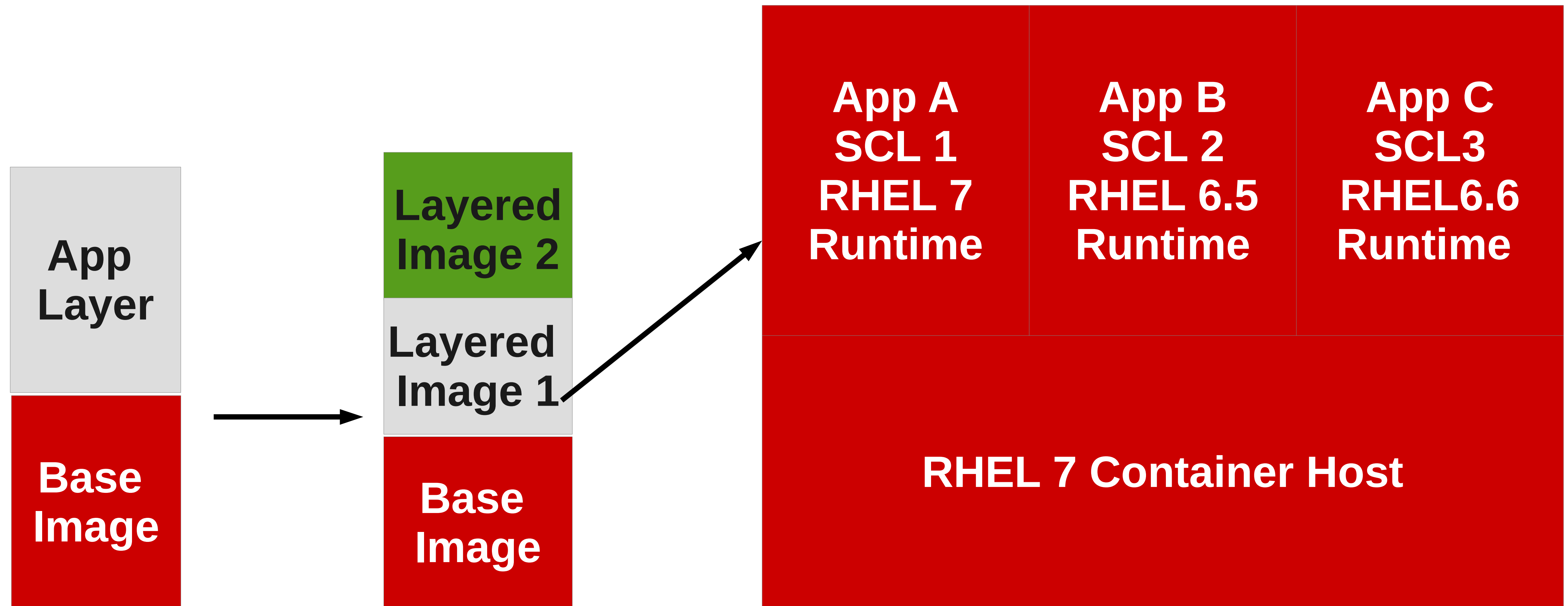


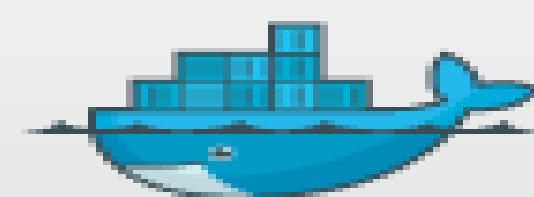
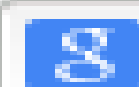
Docker format



- Docker builds on Linux Containers and provides format for content distribution
- Docker includes the userspace runtime of an application

Image-based Containers with Docker technology





docker



September 19, 2013

RED HAT AND DOCKER COLLABORATE

We are thrilled to [announce](#) the collaboration between [Docker](#) and [Red Hat](#).

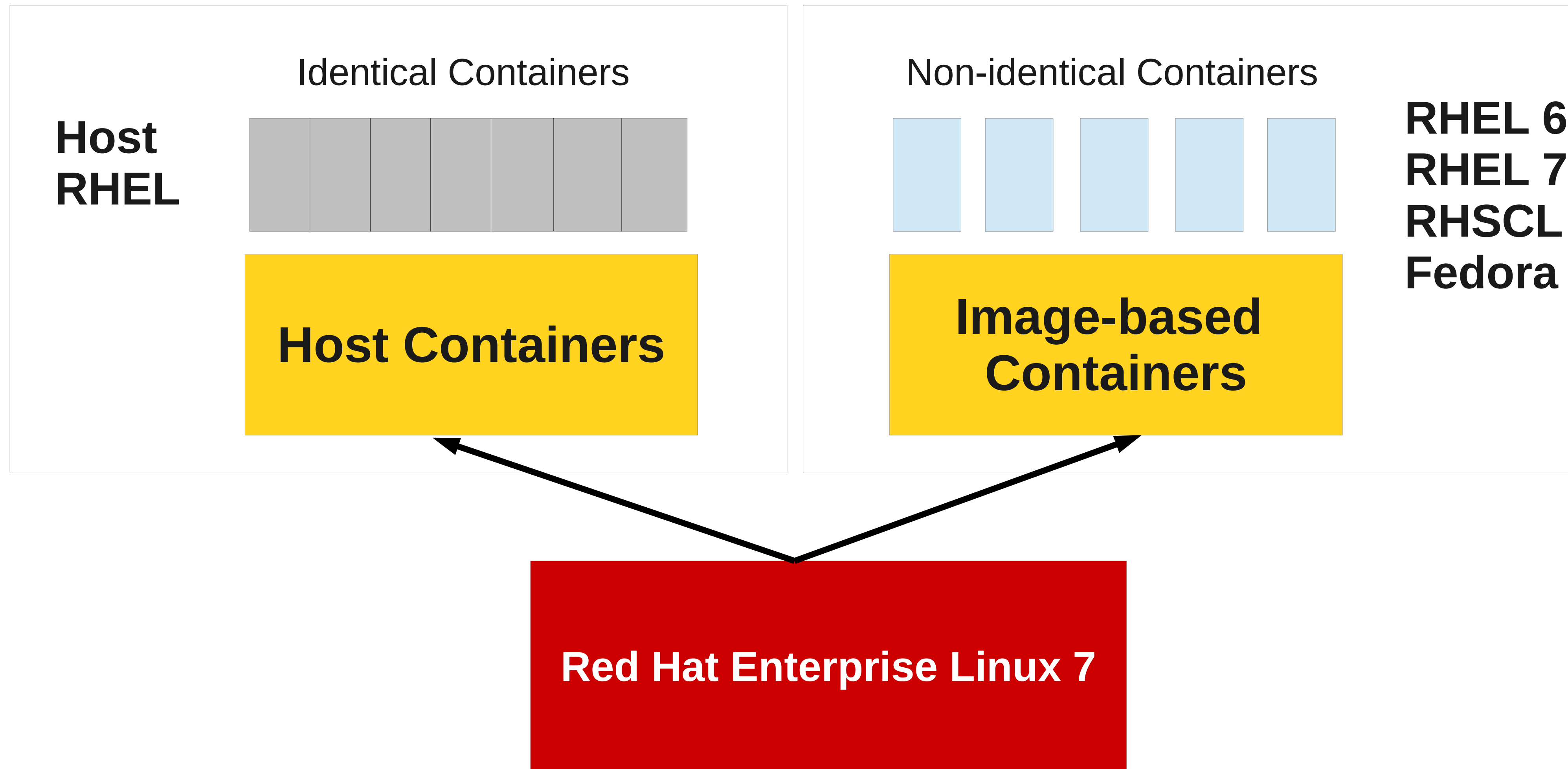
Collaboration with Red Hat is important for a number of reasons, including:

- Driving compatibility with the most widely deployed Linux distributions
- Enabling integration with one of the most prominent and important PaaS solutions
- Collaborating with the most prominent, pure open source company

First, it is critically important for us to make Docker work seamlessly with Red Hat Enterprise Linux and related Linux distributions, such as Fedora.

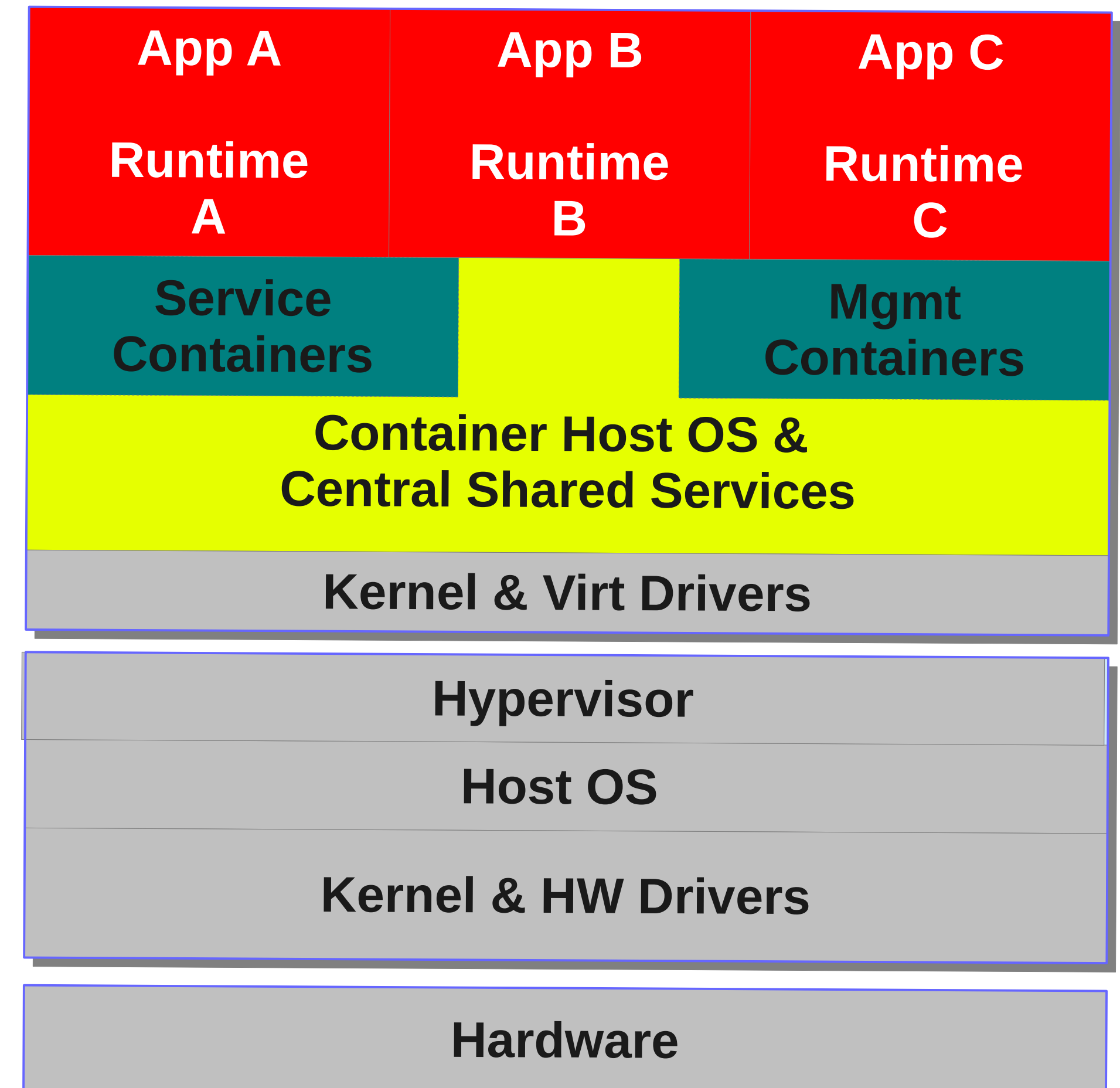
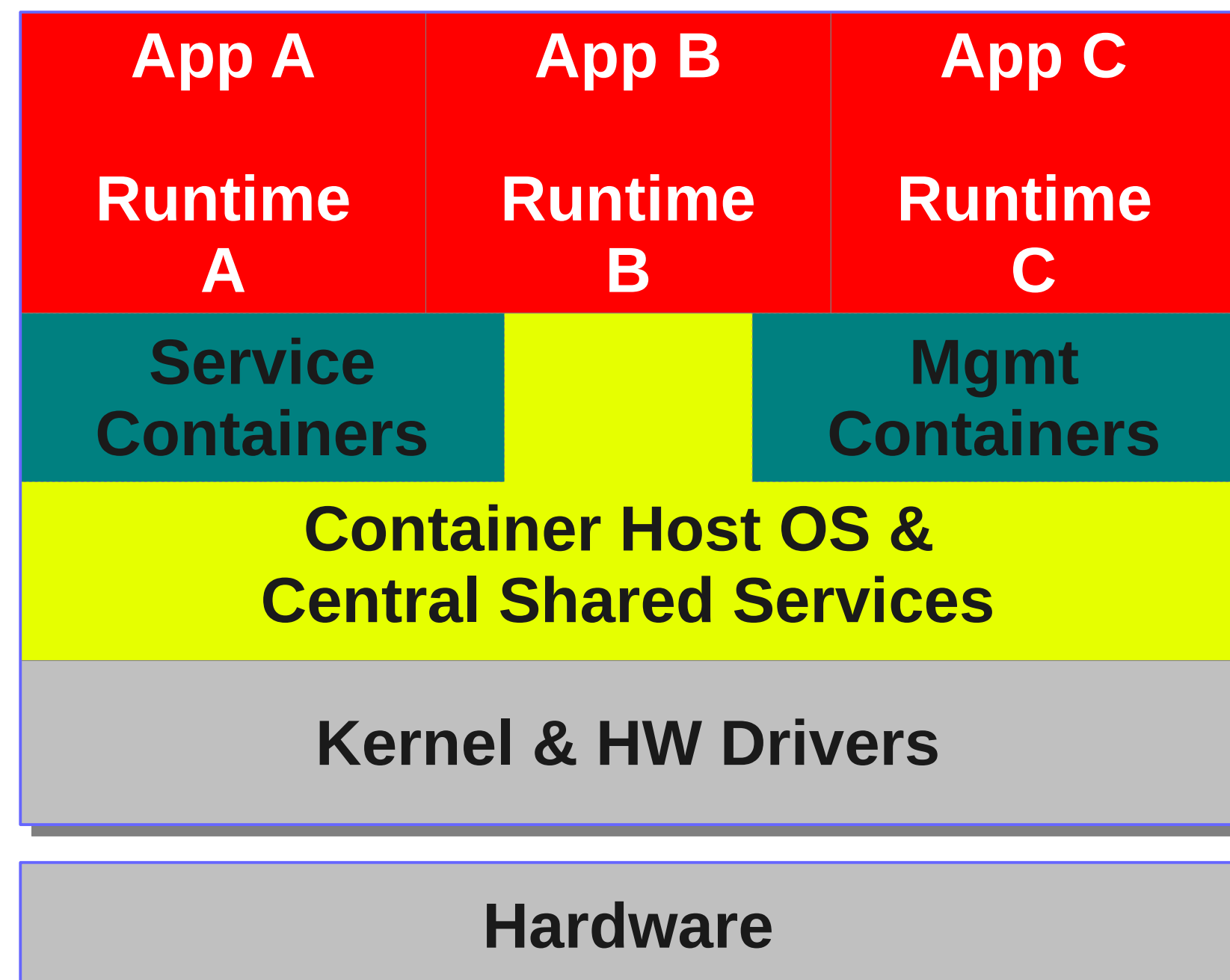
This is the #1 requested enhancement for Docker, and is obviously a major concern for people who want to deploy Docker in mainstream production environments. Our teams have been working together to package Docker for Fedora in time for the next release of Docker (0.7). Red Hat and dotCloud are planning to make Docker available for all Fedora users with upcoming releases, and we look forward to the initial release of Docker on Red Hat Enterprise Linux.

Linux Containers in Red Hat Enterprise Linux 7

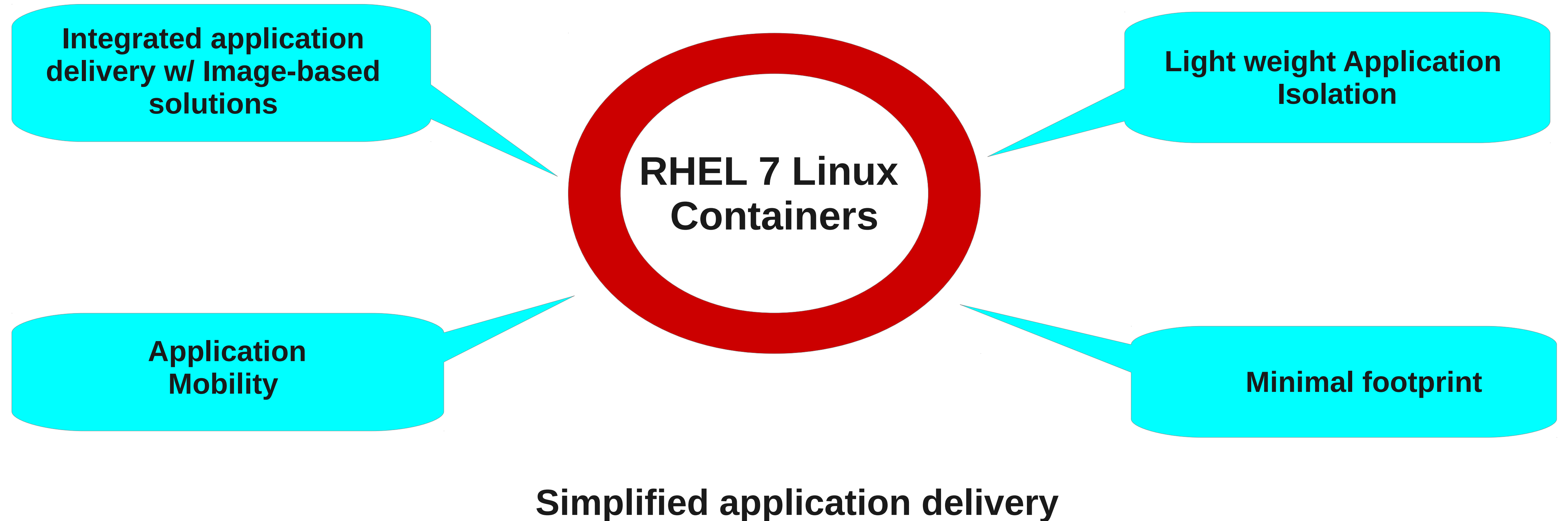


RHEL 7 Deployment Models

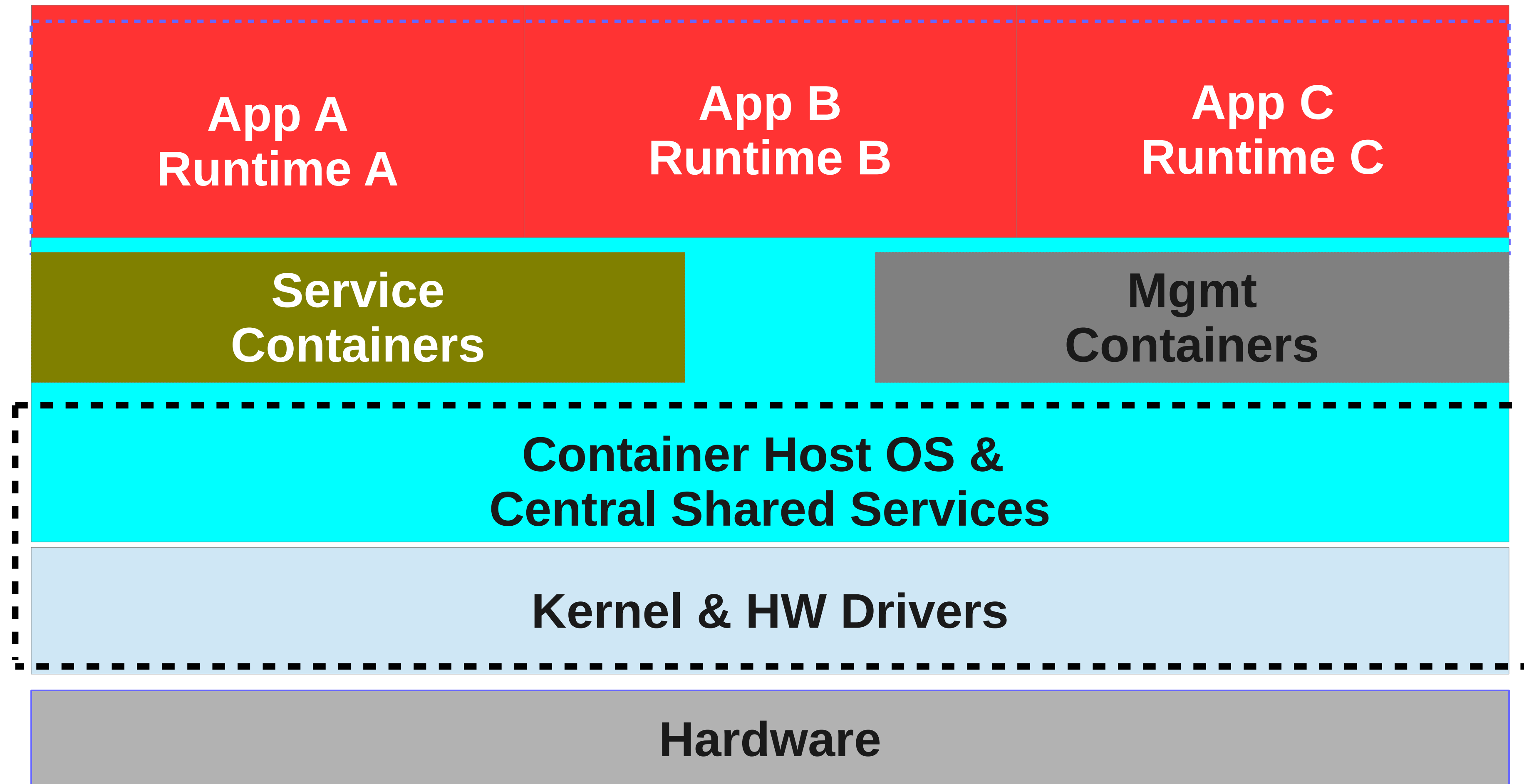
- Containers can be deployed in baremetal or virtual
- RHEL 7 supports both Virtualization with KVM and Linux Containers



RHEL 7 Linux Containers Benefits



RHEL 7 Container Host



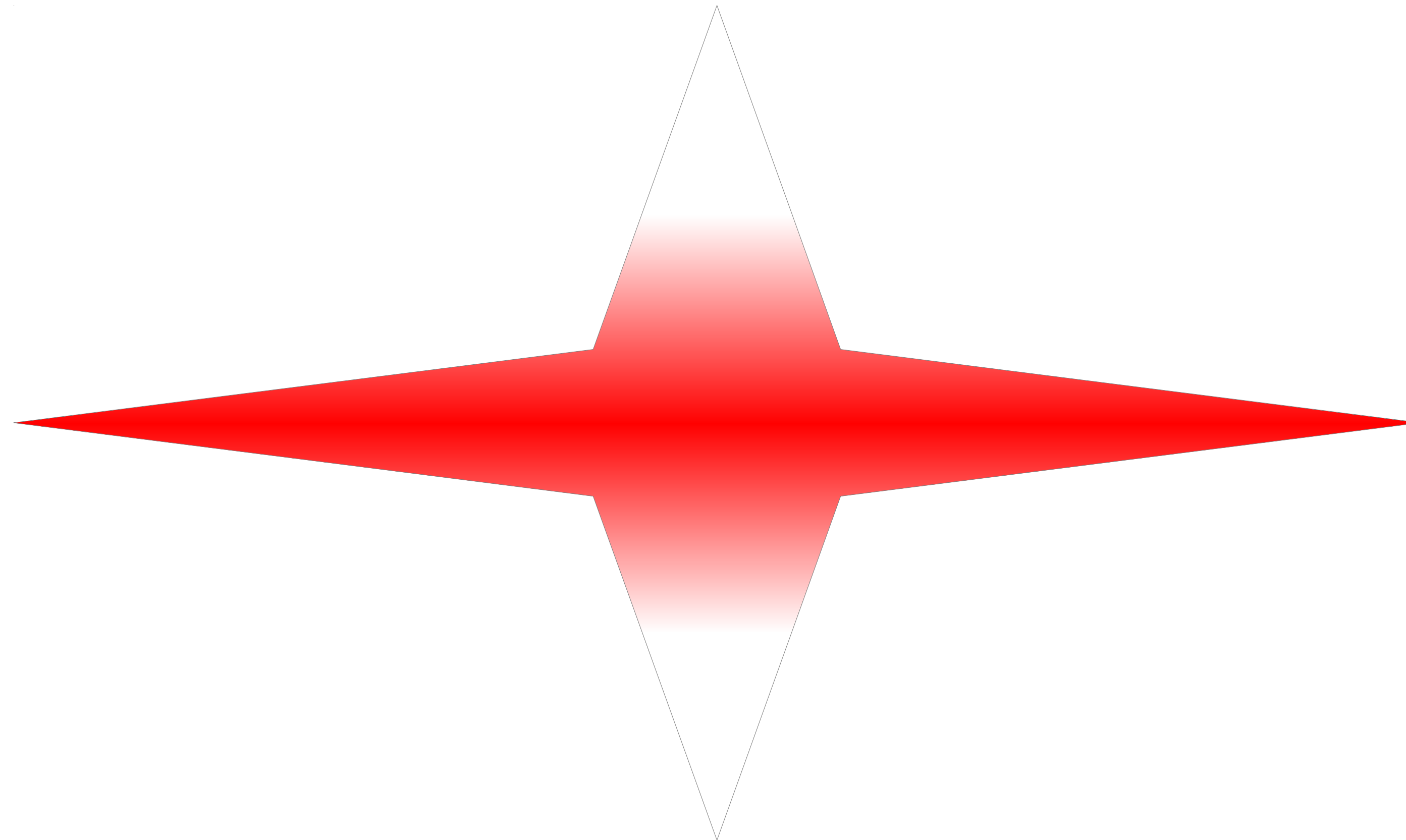
RHEL 7 Linux Containers - Building Blocks

Process Isolation

**Resource
Management**

Security

Management

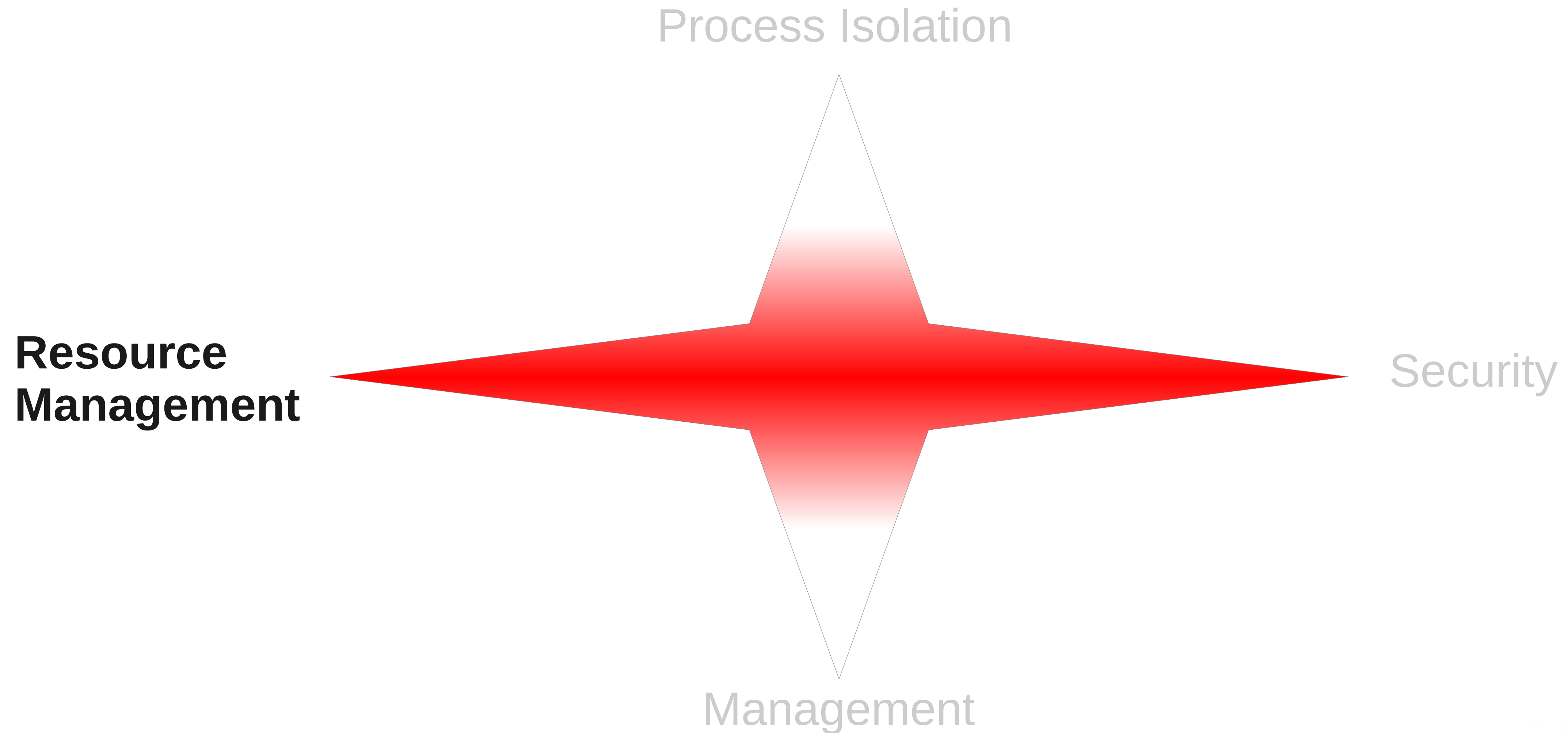


RED HAT
SUMMIT

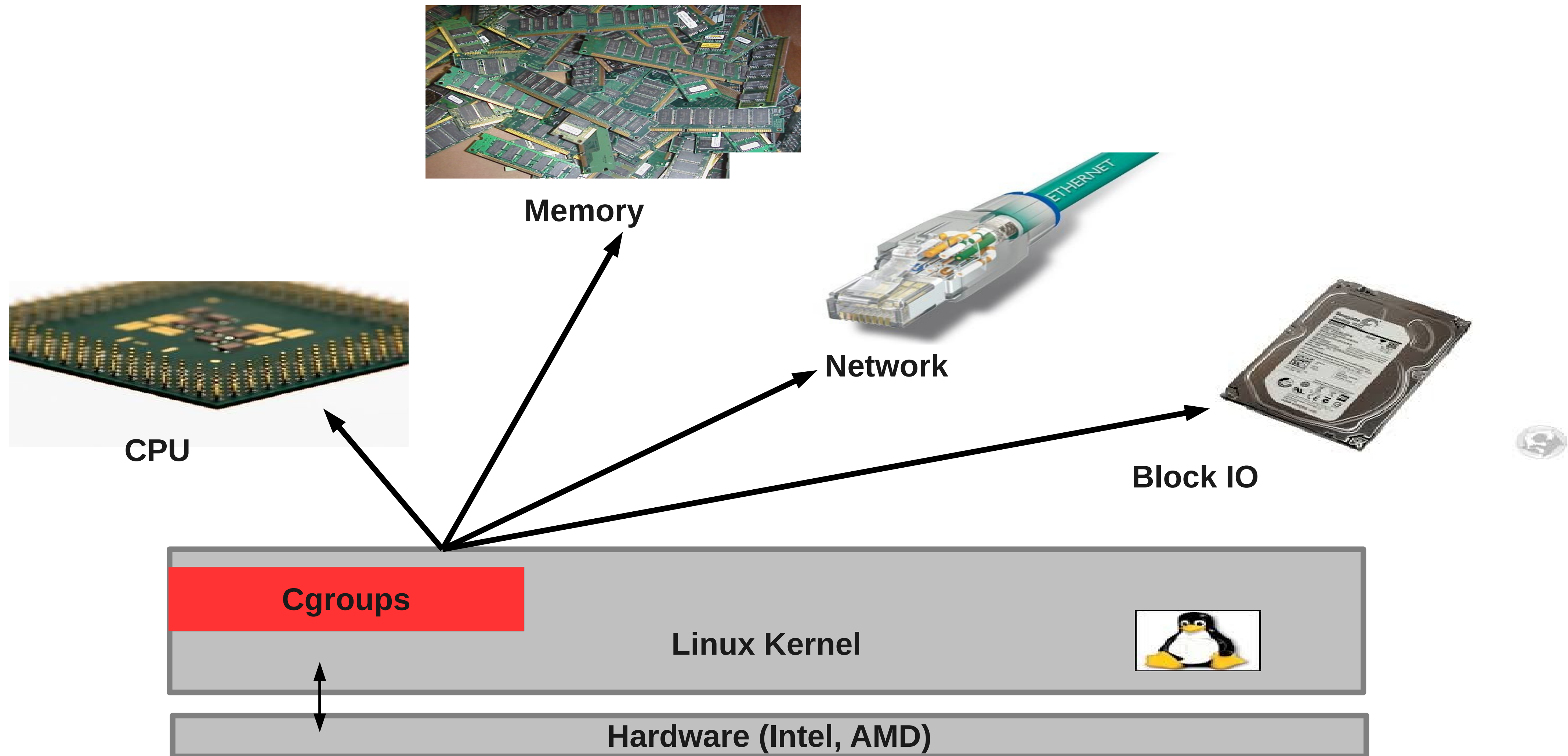
10 YEARS *and counting*
SAN FRANCISCO | APRIL 14-17, 2014

Linux Containers Features and Architecture

Linux Containers – Resource Management



Resource Management – Control Groups



Control Groups – In a Container Environment



Control Groups – Resource Control



Control Groups - Usability Improvements

- RHEL6 Any privileged process can manage Cgroups
 - No coordination and with unexpected results
 - Kernel moving to single writer mode
 - Kernel does not enforce this yet...
- RHEL7 systemd will manage cgroups
 - Recommended to use systemd APIs in RHEL7
 - New concept of Scopes/Slices

<https://www.youtube.com/watch?v=MSG4jW187Is>

<http://www.freedesktop.org/wiki/Software/systemd/ControlGroupInterface>

Control Groups - Usability Improvements: Scopes

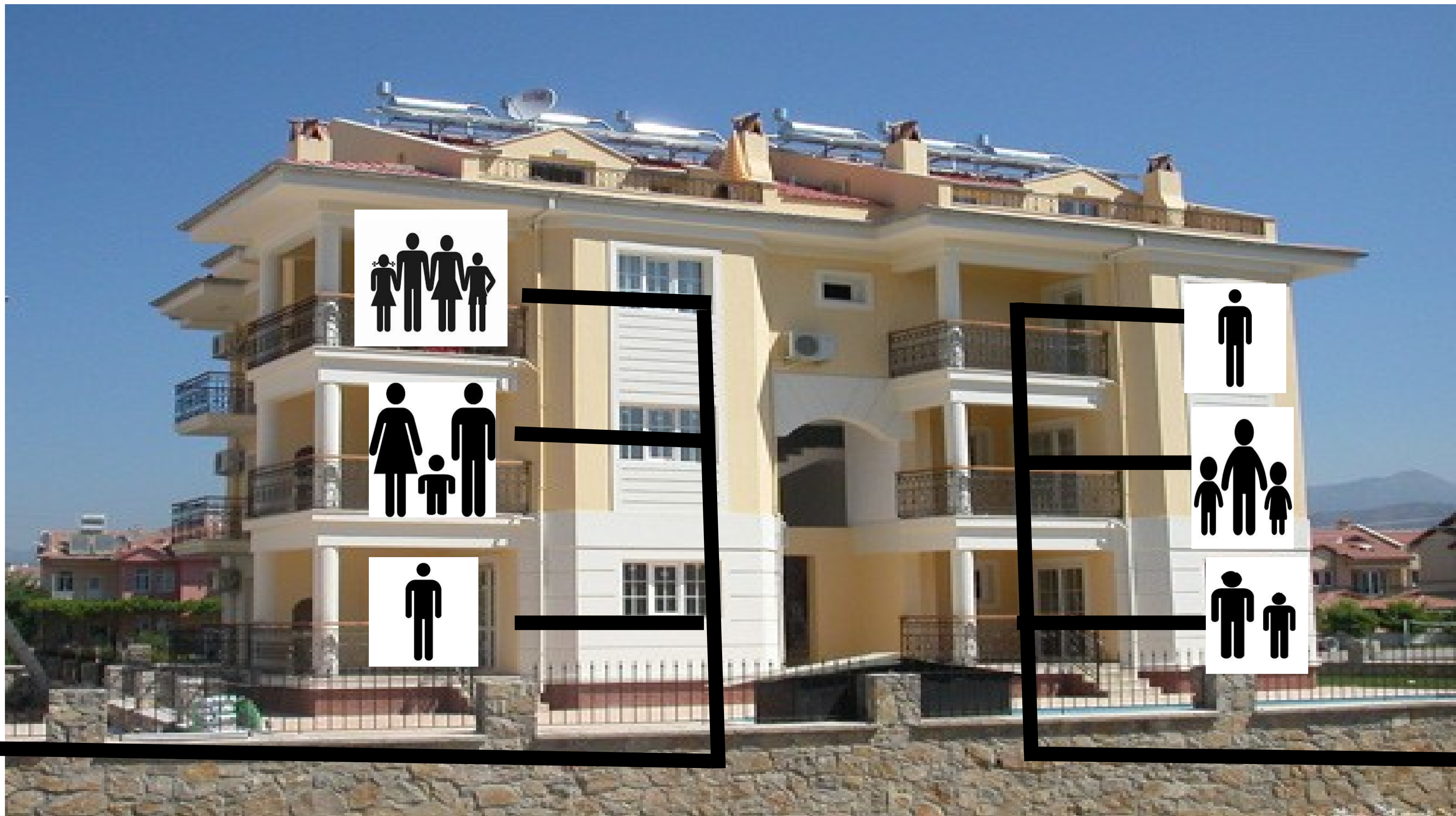
Systemd puts all related worker PIDs into cgroup called a 'scope'.

- Services
 - Apache processes in same services/apache scope
 - Mysql processes in same services/Mysql scope
 - Apache/Mysql get an equal "slice" of the system
- Users accounts
 - All users get an equal "slice"
- Machines
 - All containers/VMs get an equal "slice"
- No service/user/machine can dominate system

Control Groups – Systemd’s “Scope”



Control Groups – Systemd’s “Slice”



Control Groups - Usability Improvements: Slices

Special unit file for assigning resource constraints

Slices get assigned to scopes

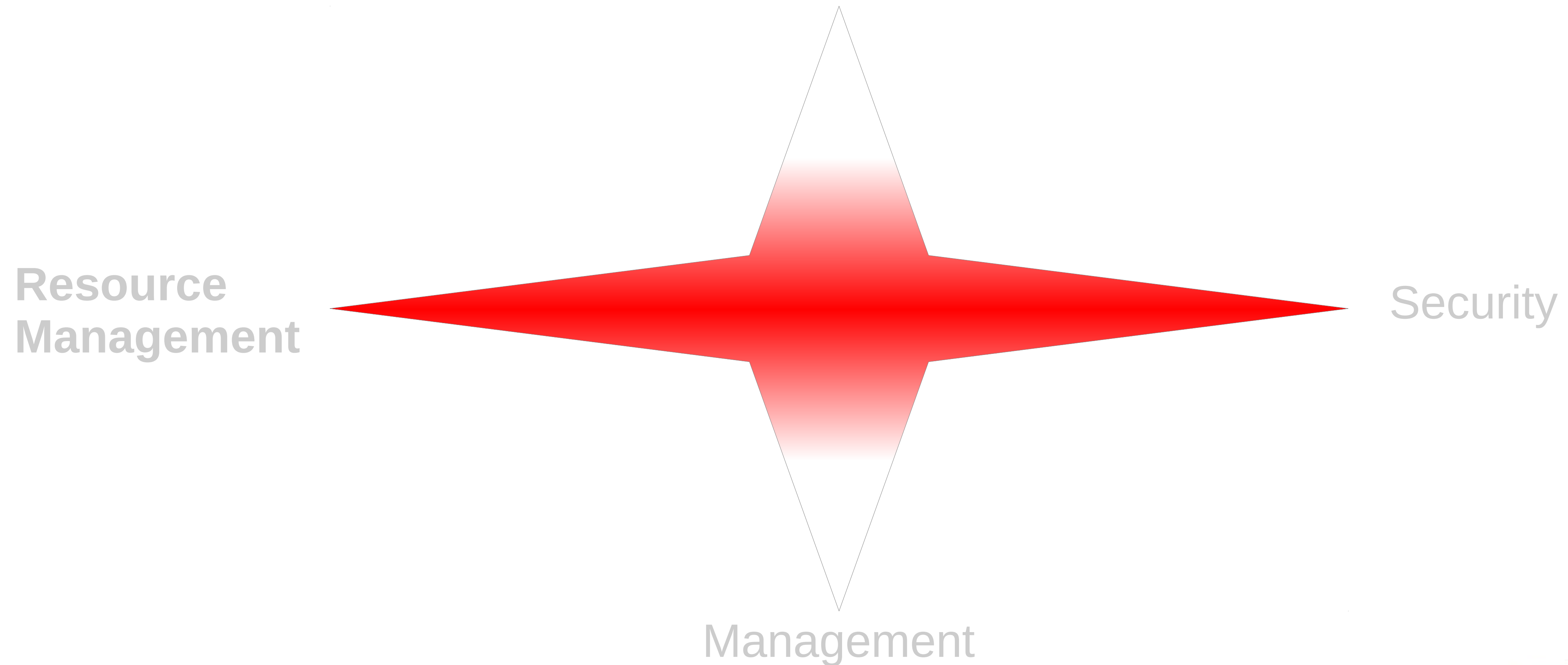
- Systemd automatically assigns services to system.slice
- You can override resource with Unit file configuration
 - MemoryLimit=1g
- Command Line

#> systemctl set-property httpd.service CPUShares=524 MemoryLimit=500M

- Systemd will assign Containers to machine.slice
 - You can override by editing
 - /etc/systemd/system/big-machine.slice

Linux Containers – Process Isolation

Process Isolation



Process Isolation - Namespaces



Process Isolation - Namespaces

- Isolate processes
 - Create a new environment with a Subset of the resources
- Once set up, namespaces are transparent for processes
- Can be used in custom and complex scenarios
- Supported Namespaces
 - ipc, pid, mnt, net, uts
 - Future Red Hat Enterprise Linux 7: user namespace

Process Isolation - Namespaces

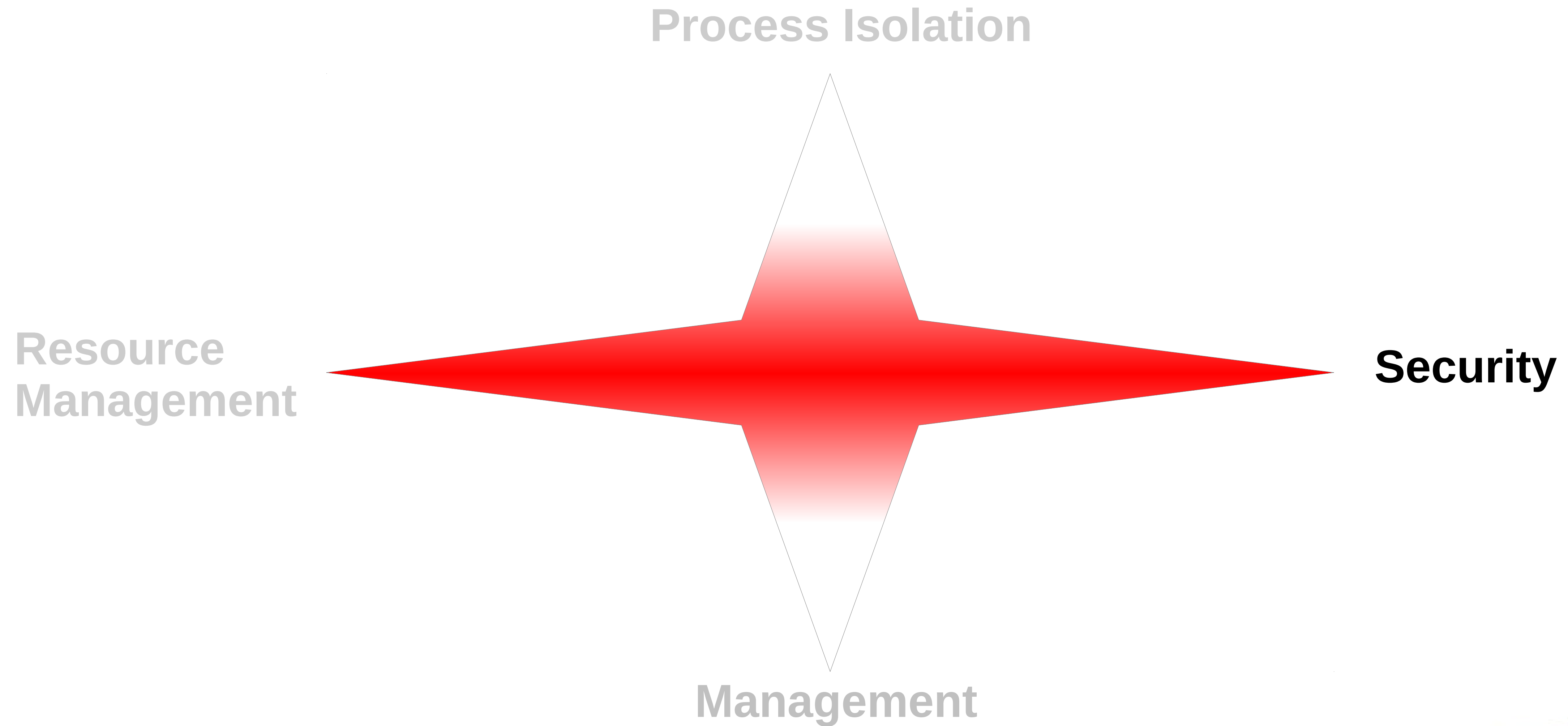
Namespaces	Functionality	What does it mean?
Mount	Isolate the set of FS mount points seen by processes	/tmp in container can be different in ns' Remount '/' read only within namespace
PID (process ID)	Process can have same PID in different NS (include PID1)	Process in NS can't see/interact with process outside All processes are visible in 'root' PID NS
Network	Isolate the networking stack: ip addr, routes, netfilter iptable rules	Each NS has its own private loopback IF Commonly used with virtual ethernet IF pair
UTS	Set a different host and domain names for NS	No impact to the rest of the system Useful when combined with Network NS
IPC	Private inter-process communication environment: message queues, semaphores, shared memory	Resources are only accessible within the Namespace

Process Isolation - User Namespace

May be enabled in future releases...

- Mapping between UIDs and GIDs
 - 5000-6100 on Root Namespace
 - 0-1100 in User Namespace
- Super user (UID 0) possible inside the Namespace
 - Configuring network on a network namespace
 - Binding to ports < 1024
 - Treated as unprivileged UID 5000 outside namespace

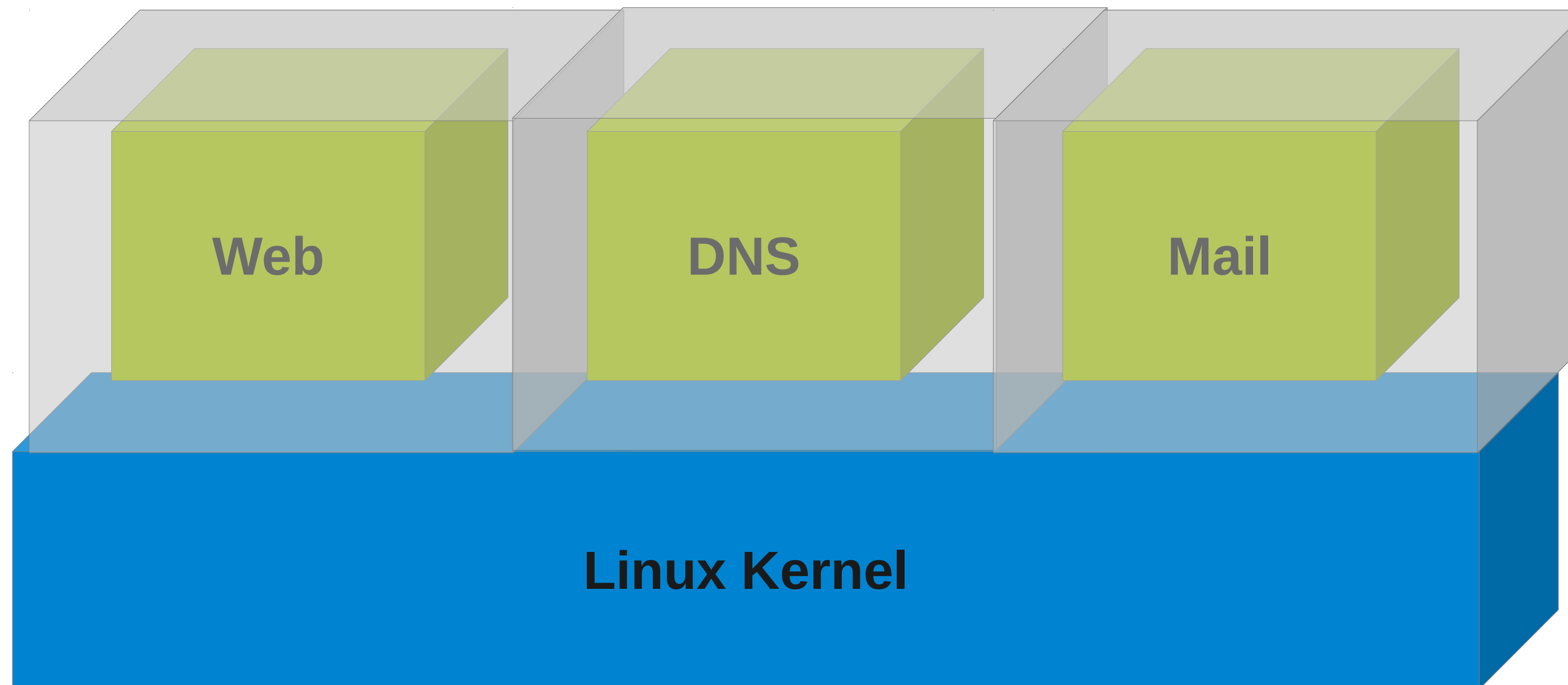
Linux Containers - Security



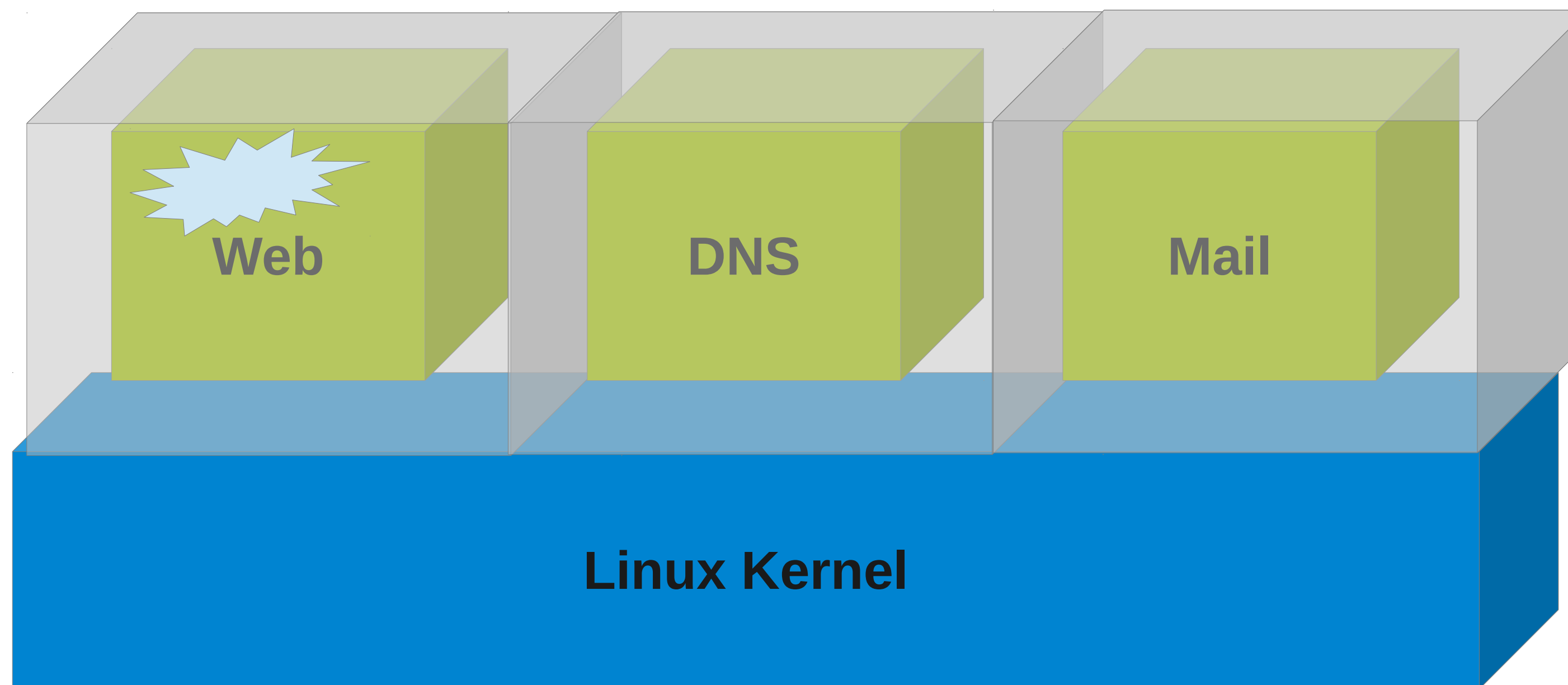
SELinux – Security



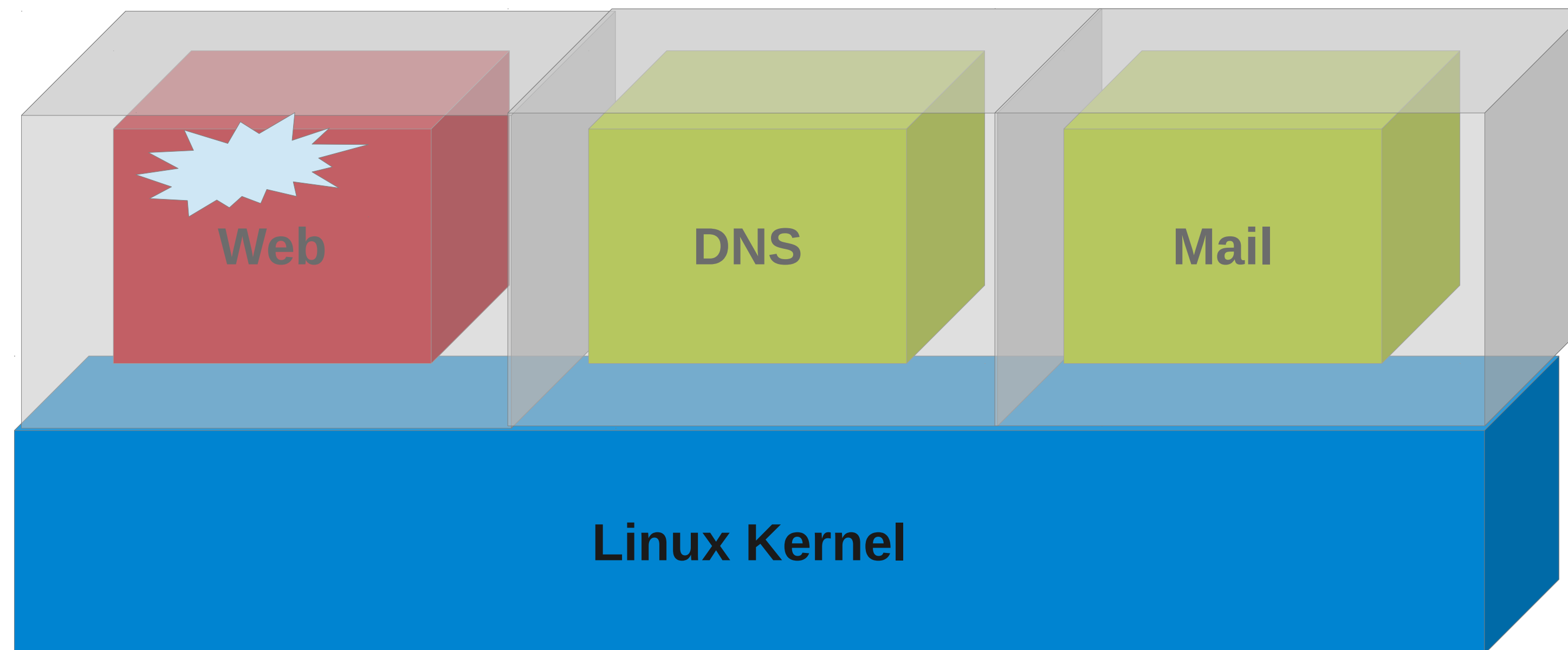
SELinux - Security



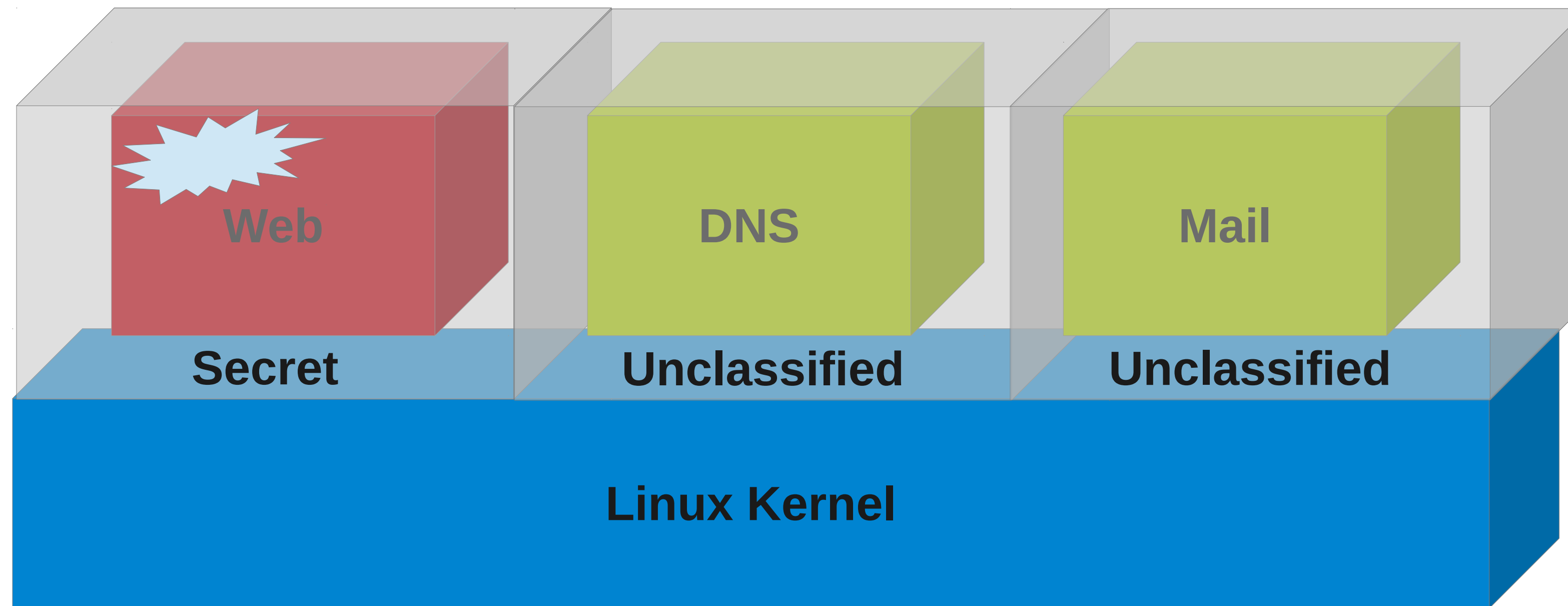
Each container process is confined in its own sandbox distinct from other the other processes



When a process is attacked.....

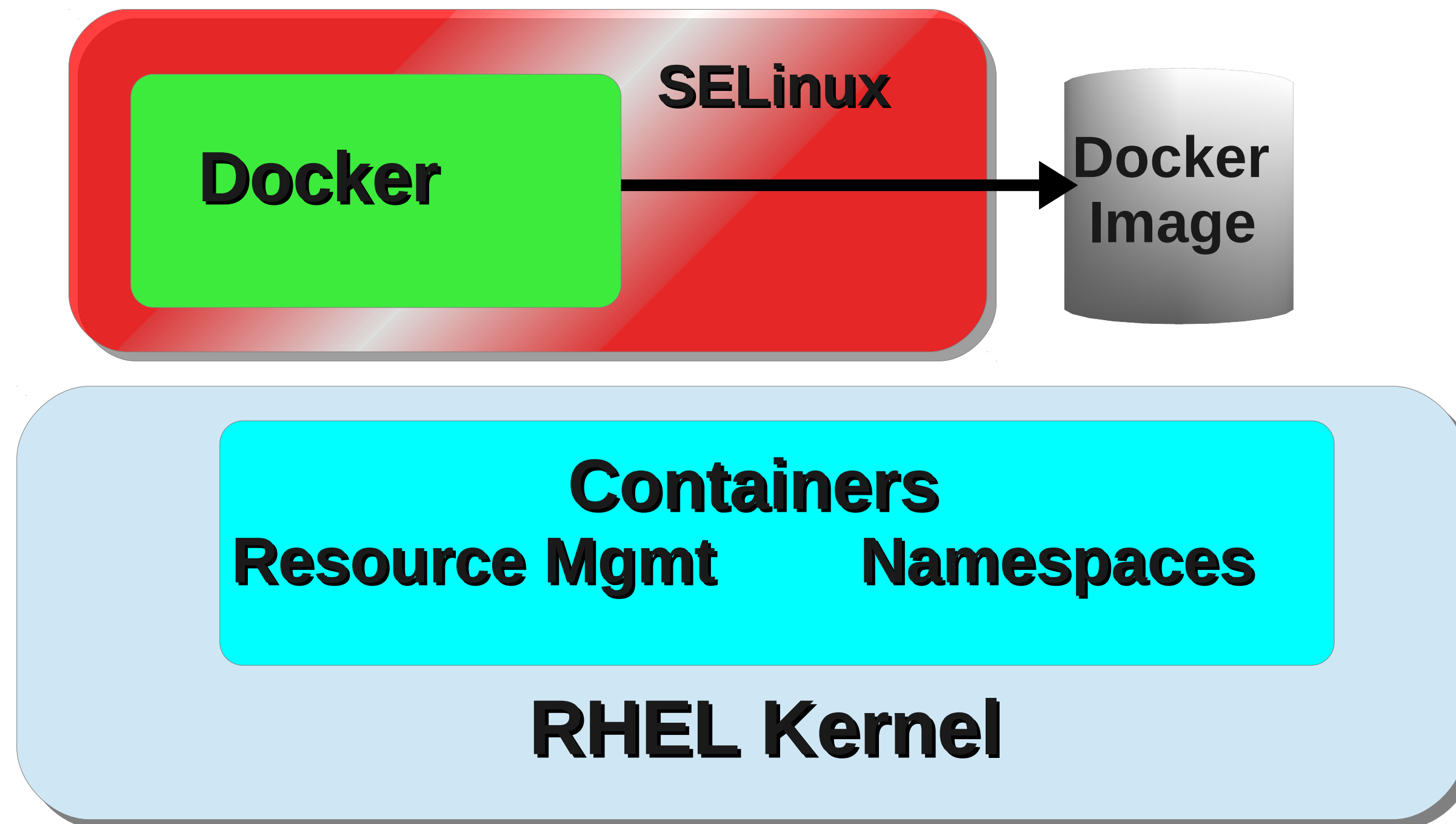


...and compromised, there is far less exposure. Only the container process is lost – lose the process not the system.



Label the container process with multiple level using SELinux Multi Level Security (MLS)

SELinux and Docker



Linux Containers - Management

Process Isolation

Resource
Management

Security

Management

System and Container Management



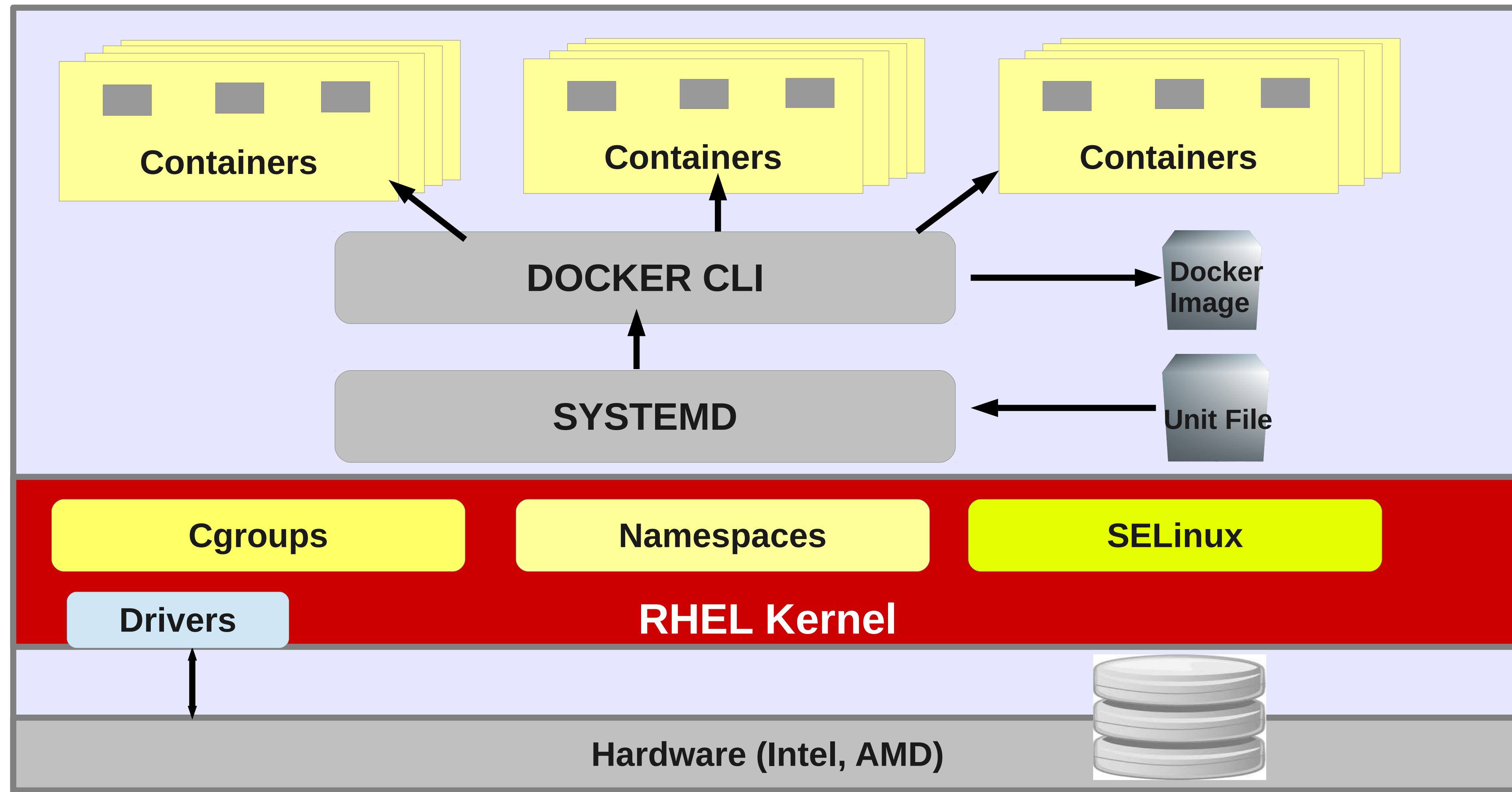
Docker CLI



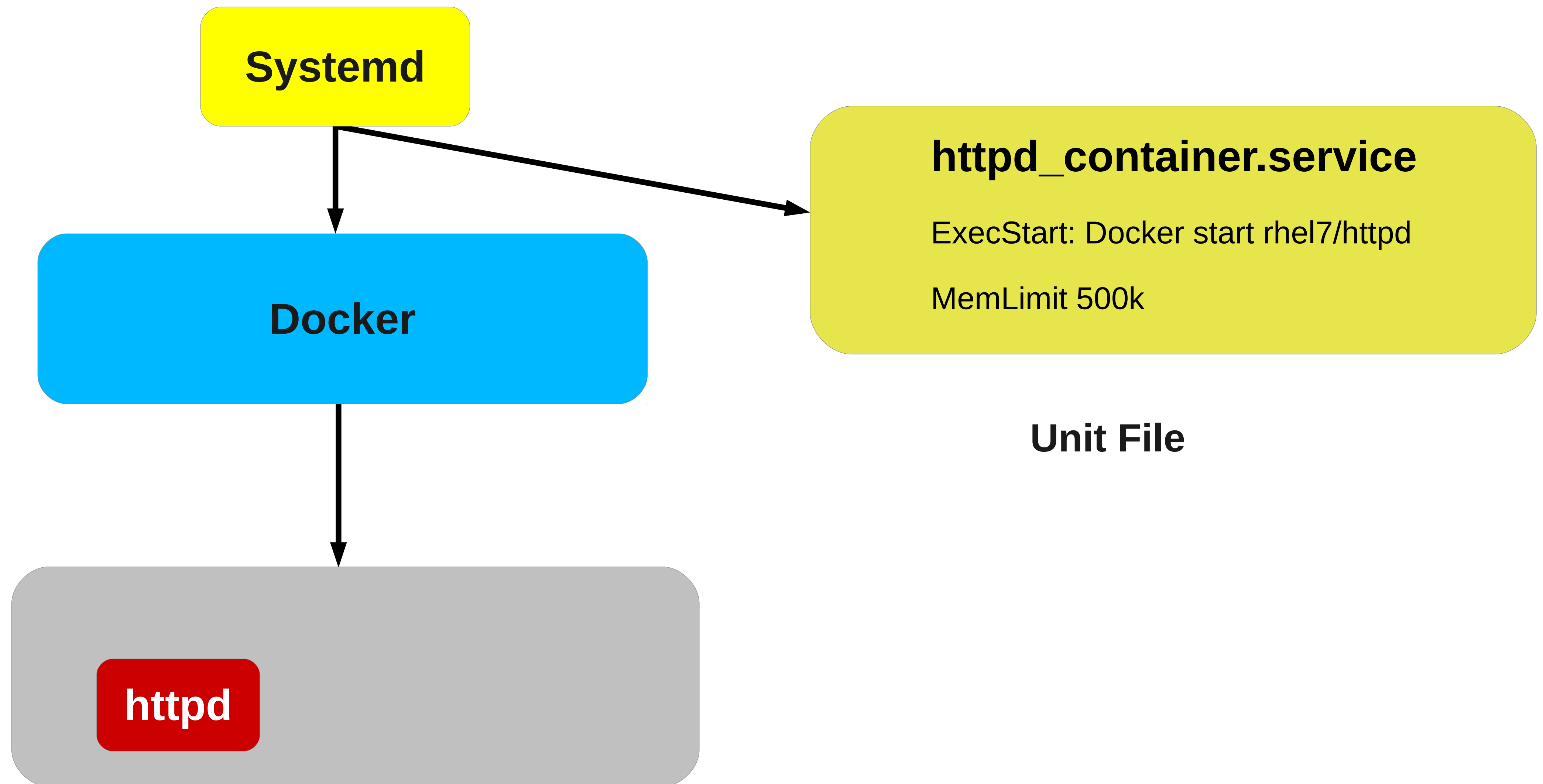
Docker format

- Tool to package an application and its runtime dependencies for deployment into a Linux Container
- Docker 0.9 includes libContainer, native LXC implementation

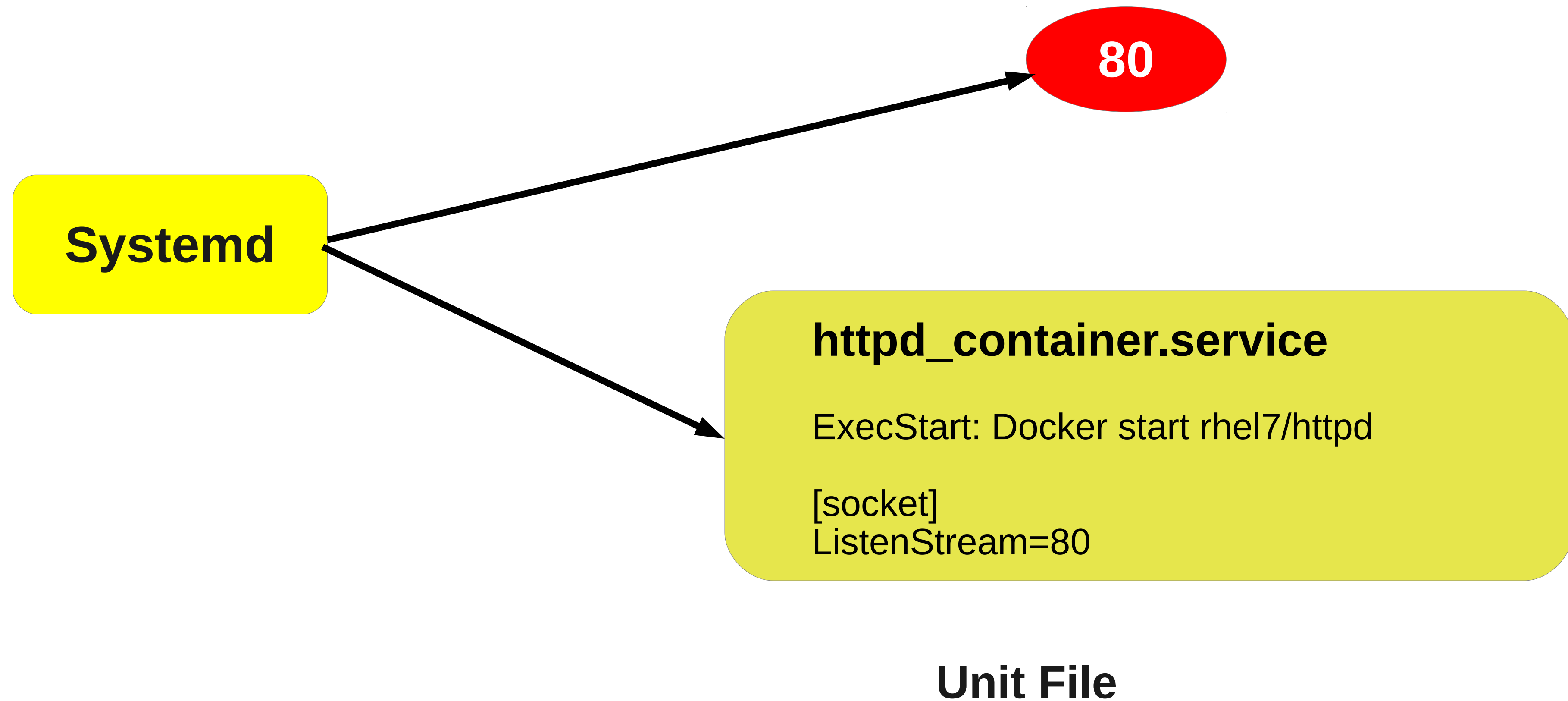
Red Hat Enterprise Linux 7 Containers Architecture with Docker CLI



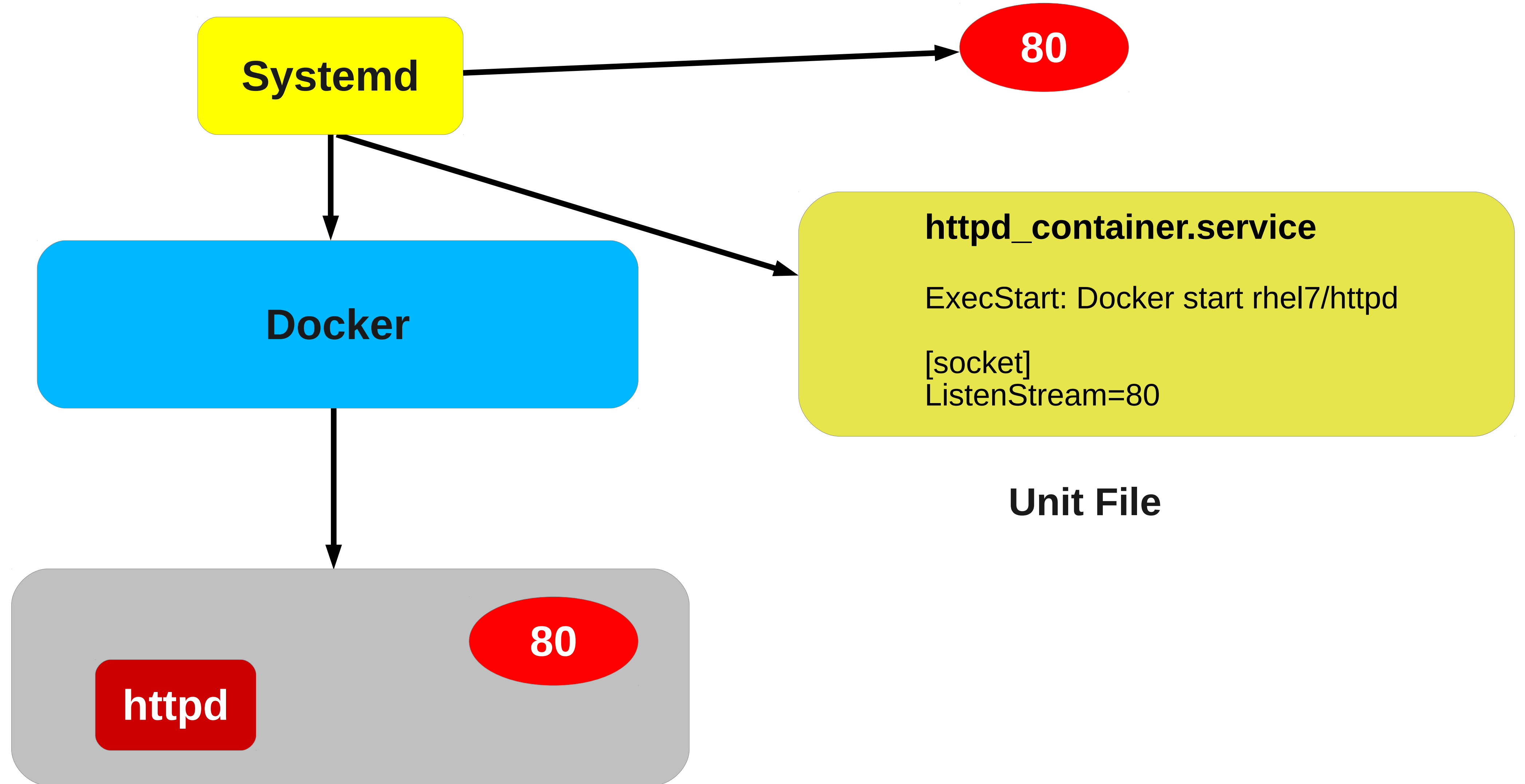
Systemd Cgroup Configuration passed to Docker



Systemd Socket Activation of Docker Containers



Systemd Socket Activation of Docker Containers



Red Hat Certification for Containerized Apps

The screenshot shows a web browser window with the URL www.redhat.com/about/news/press-archive/2014/3/red-hat-announces-certification-for-containerized-applications-extends-customer-confidence-and-trust-to-the-cloud. The page features the Red Hat logo and a navigation bar with links: United States, Customer Portal, Resource library, Find a partner, Buy online, and Contact sales. A search bar is also present. The main content area is titled "ABOUT RED HAT" and includes a navigation menu with links to PRODUCTS, SOLUTIONS, SUPPORT, TRAINING, and CONSULTING. The article title is "Red Hat Announces Certification for Containerized Applications, Extends Customer Confidence and Trust to the Cloud". The article is dated March 11, 2014, and is from Raleigh, NC. The article text states: "Red Hat Container Certification delivers secure, consistent and simplified platform for ISVs to take advantage of containers in Docker format". The article also mentions that the certification extends the confidence customers have with Red Hat Enterprise Linux, which currently supports thousands of certified applications, to certified containers running on certified container hosts. The pending release of Red Hat Enterprise Linux 7 and Red Hat's OpenShift Platform-as-a-Service (PaaS) offering will both be certified container hosts, with Docker as a primary supported container format. The right sidebar contains a "Share" button, a "CONTACT RED HAT PR" button, a "SEARCH NEWS" button, and three featured content blocks: "RED HAT NEWS", "THE RED HAT WAY", and "ARE YOU RIGHT FOR RED HAT?".

Red Hat | Red Hat Announ x

www.redhat.com/about/news/press-archive/2014/3/red-hat-announces-certification-for-containerized-applications-extends-customer-confidence-and-trust-to-the-cloud

LOG IN

United States • Customer Portal • Resource library • Find a partner • Buy online • Contact sales

I want to... Type to search

ABOUT RED HAT

PRODUCTS SOLUTIONS SUPPORT TRAINING CONSULTING

About Red Hat > News and press releases > Press Release March 2014 >

Share 6

+ CONTACT RED HAT PR

+ SEARCH NEWS

RED HAT NEWS
Press, announcements, and more.

THE RED HAT WAY
It's better to share. Watch now.

ARE YOU RIGHT FOR RED HAT?
Apply now.

2014

January
February
March
April
May
June
July
August
September
October
November
December

2013

2012

Red Hat Announces Certification for Containerized Applications, Extends Customer Confidence and Trust to the Cloud

Raleigh

March 11, 2014
Red Hat Container Certification delivers secure, consistent and simplified platform for ISVs to take advantage of containers in Docker format

Raleigh, NC – March 11, 2014 – Red Hat, Inc. (NYSE: RHT), the world's leading provider of open source solutions, today announced the extension of its application certification program to include containerized applications. The Red Hat Container Certification ensures that application containers built using Red Hat Enterprise Linux will operate seamlessly across certified container hosts. Designed with the needs of independent software vendors (ISVs), service providers and their enterprise customers in mind, the certification extends the confidence customers have with Red Hat Enterprise Linux, which currently supports thousands of certified applications, to certified containers running on certified container hosts. The pending release of Red Hat Enterprise Linux 7 and Red Hat's OpenShift Platform-as-a-Service (PaaS) offering will both be certified container hosts, with Docker as a primary supported container format.

<http://www.redhat.com/about/news/press-archive/2014/3/red-hat-announces-certification-for-containerized-applications-extends-customer-confidence-and-trust-to-the-cloud>

RED HAT
SUMMIT

10 YEARS *and counting*
SAN FRANCISCO | APRIL 14-17, 2014

Demo

Linux Containers in RHEL 7 - Key Takeaways

- Application isolation mechanism for Light-weight multi-tenancy
- Application centric packaging w/ Docker image-based containers
- Linux Containers Productization
 - Key kernel enablers – full support in RHEL 7 GA
 - Docker 1.0 – shipped with RHEL 7 GA
- Linux Container Certification
- Red Hat and Docker partnership to build enterprise grade Docker containers

Linux Container Sessions, Demos and Labs

Time	Title	Venue
Wed 1:20 PM – 2:20 PM	Portable, lightweight and interoperable Docker containers across Red Hat Solutions	Room 236
Wed 3:50 PM – 5:50 PM	Containers & resource management in Red Hat Enterprise Linux 7 Beta (Hand-on Lab)	Room 105
Wed 11:00 AM – 1:00 PM	Linux Containers and Application Isolation Demo	Red Hat Booth (Infrastructure Pod 1)
Wed 1:20 PM – 3:20 PM	Implementing & managing OpenShift Enterprise	Labs II
Wed 11:30 AM – 2:00 PM	Next Generation Container Management Demo	Emerging Technologies Red Hat Booth (Pod 31)



10 YEARS *and counting*
SAN FRANCISCO | APRIL 14-17, 2014

Questions?