# Kubernetes Performance-Sensitive Application Platform

Defining patterns and technology to run critical, high performance line-of-business applications on Kubernetes

Jeremy Eder, Derek Carr and Seth Jennings
OpenShift Engineering
May the Fourth, 2017



redhat.

# What is this?

Bring next generation development processes, agility, procedures and mindset to established industries



redhat.

# Why do this?

Current capabilities do a good job covering generic web hosting workloads (representing a fraction of workloads).

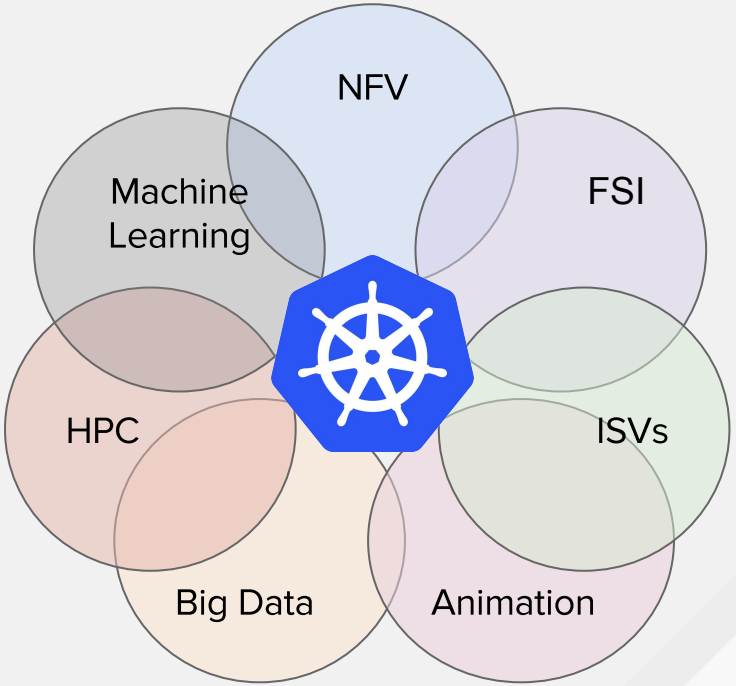


redhat.

# Why do this?

Kubernetes becomes the **single platform** to run any application:

- Old or new
- Monolithic/Microservice



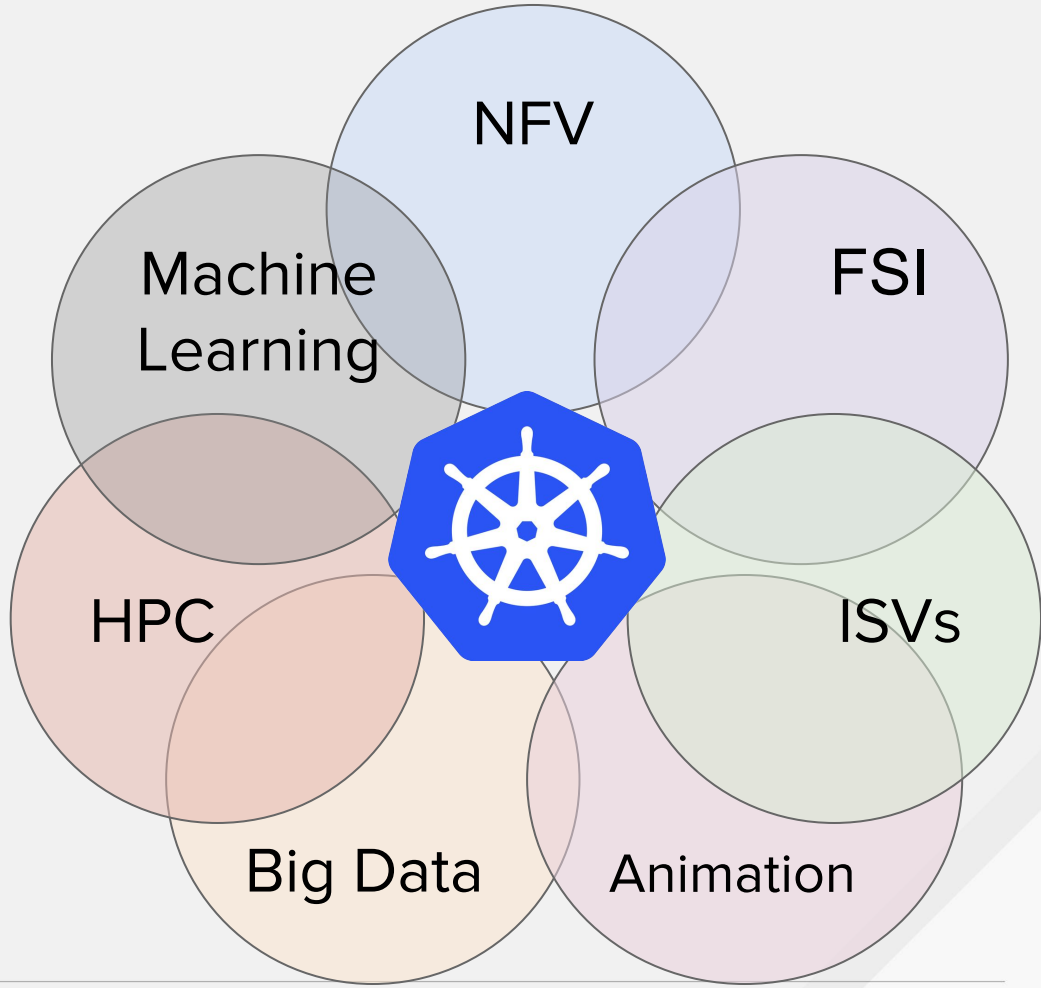



redhat.

So much overlap…

Coordinate, and plumb these generically.

Create primitives for ISV ecosystem to hook into.






redhat.

# Why do this?

## High performance customers want

- An industry-standard packaging format (OCI)
- A datacenter-wide workload scheduler (K8S)
- To use Open Source

## But they will not sacrifice performance to get it

- Not even a little



redhat.

# Why do this?

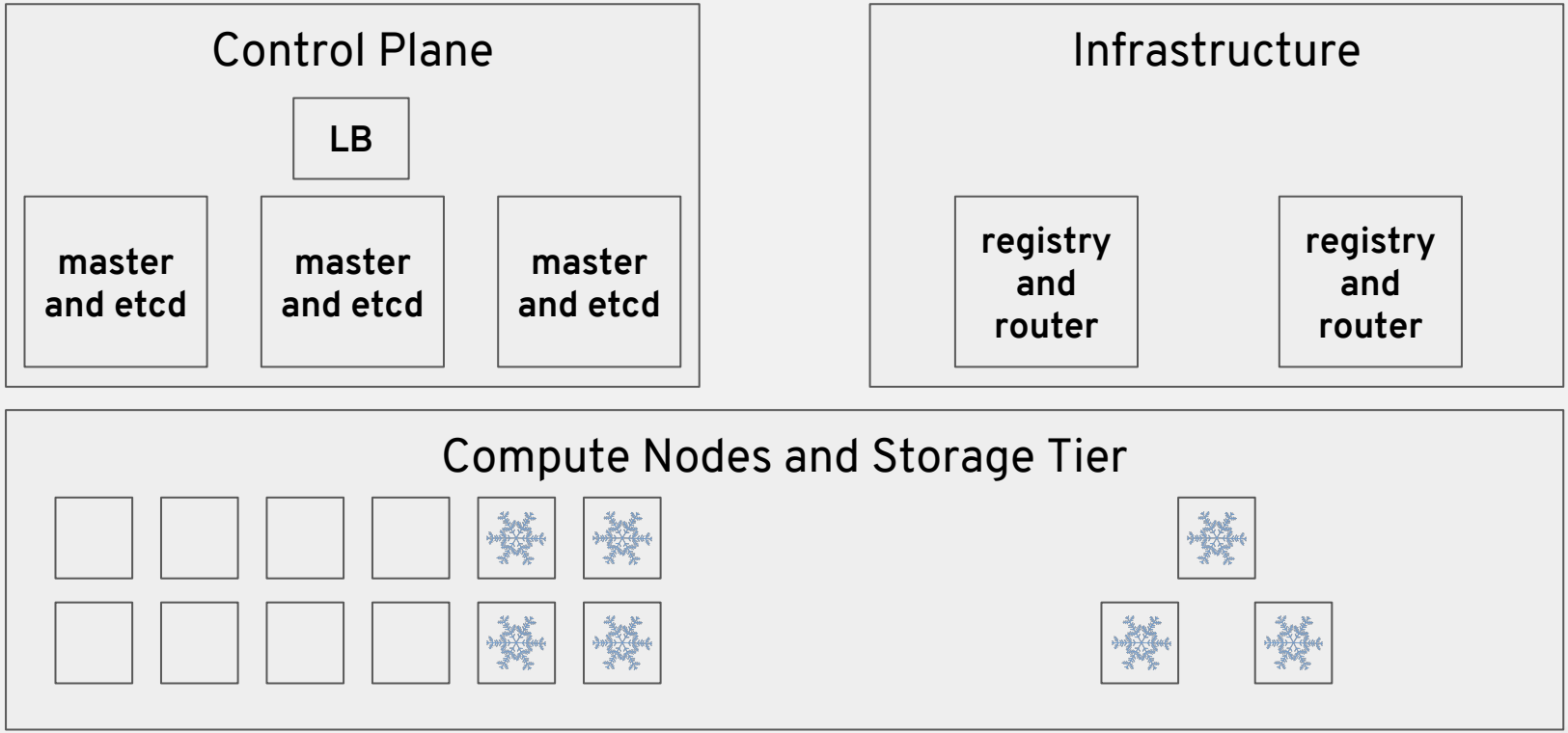
## Enable containerization of Infrastructure Software

- Software-defined Storage and Networking
- Packet switching and routing tiers
- Multi-workloads (very different) within a single cluster
  - Layered schedulers (HPC/grid)
- Many more...



redhat.

# Cluster Topology




redhat.

# Drill-down on overlap

| Feature | FSI | NFV | ISV | BD/ML | ANIM | HPC |
|---|---|---|---|---|---|---|
| NUMA (cpuset.cpus and cpuset.mems) | Yes | Yes | Yes | Maybe | Maybe | Yes |
| Device Passthrough (NIC and Disk, GPU etc…) | Yes | Yes | Yes | Maybe | Maybe | Yes |
| sysctl Support (non-namespaced too) | Yes | Yes | Yes | Yes | Yes | Yes |
| Separation of control- and data-plane | Yes | Yes | Yes | Yes | Yes | Yes |
| Node “fitness” (extended health info) | Yes | Yes | Maybe | Maybe | Maybe | Yes |
| Multi-homed pods | Yes | Yes | Maybe | Yes | Yes | Yes |
| Kernel Module loading/verification (DKMS-ish) | Yes | Yes | Maybe | Maybe | Yes | Maybe |
| Hugepages | Yes | Yes | Yes | Yes | Maybe | Maybe |



redhat.

# Kubernetes Resource Management Working Group

## Kicked off in January

- Define requirements for high performance workloads
- Design solutions to meet those needs
- First face to face this week, very productive!



redhat.

# Red Hat Container Catalog

## Consuming Container Images from Red Hat and its Ecosystem

Dirk Herrmann
Product Owner Container Catalog
May 2nd 2017

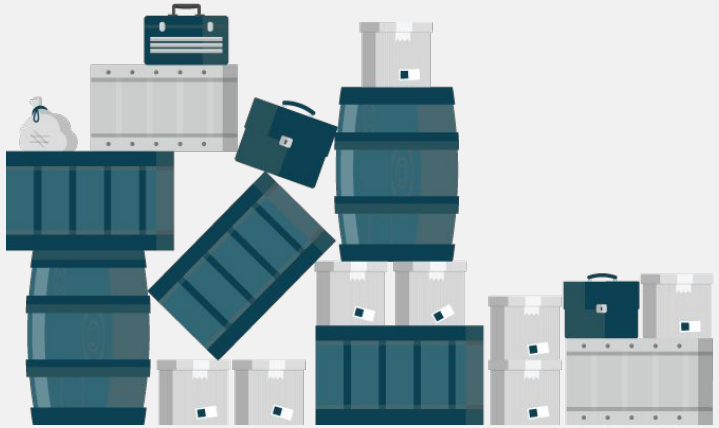


redhat.

# The Value & New Challenges

It’s quick and easy to pull a Linux container image from a public registry and get started.

In fact, too easy. There can be an explosion of different distributions, architectures, performance and security characteristics in different images.





redhat.

**Red Hat Registry Stats**

- 227 repositories
- 2,169 images
- 1+ TB storage

**Red Hat Security Statistics 2016**

- 97 critical RHSA
- 286 important RHSA
- 100% fixed in <1d *

**Red Hat Customer Portal Stats 2016**

- 13,100,00 visitors
- 2,400,000 searches
- 108,300,00 views

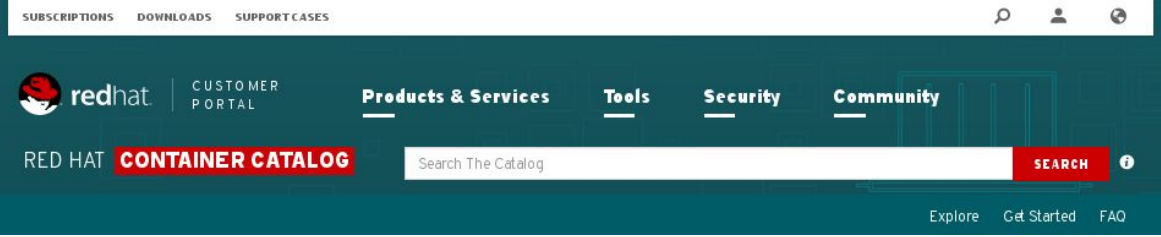
- Cross-team effort of 10 teams across 4 organizations
- Design driven approach focusing on end customer user experience

**RED HAT®**
CONTAINER CATALOG

- Container Health Index
- Extensive Image Metadata
- Image Documentation
- Image Advisories



* 100% of critical security flaws in RHEL have been fixed in less than one day: https://access.redhat.com/blogs/766093/posts/2957221




## Vision

Our vision is to help developers, architects, and IT operations realize the full potential of containers by transforming the way container-based applications are built, delivered, and consumed

1 Explore & Search

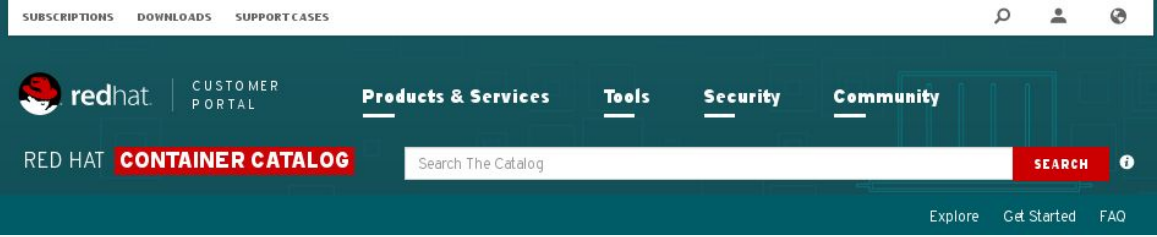
2 Evaluate & Select

3 Consume & Distribute

4 Use & Maintain

## Mission

Our mission is to provide customers and partners with the best experience when delivering and consuming container-based applications. This includes the right information and guidance to make intelligent decisions about which container images to consume



**Joe**

Architect

I want to explore what's inside the Red Hat Container Catalog

I want to search for a product and see all images belonging to it

**1** Explore & Search

**2** Evaluate & Select

**3** Consume & Distribute

**4** Use & Maintain

I'm searching for a database container image

I'm searching for Red Hat Enterprise Linux base image

**Jane**

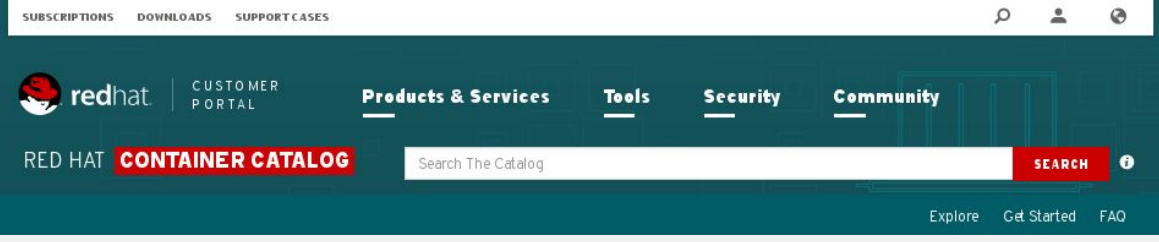
Developer

use our explore page to browse most relevant products and image categories

popular Red Hat and Ecosystem products

app categories such as database, programming language, logging

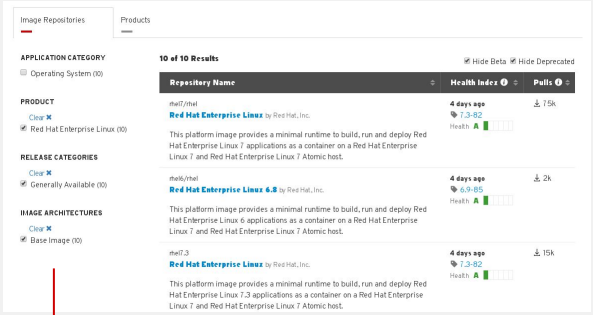
Base, Builder and Application Images



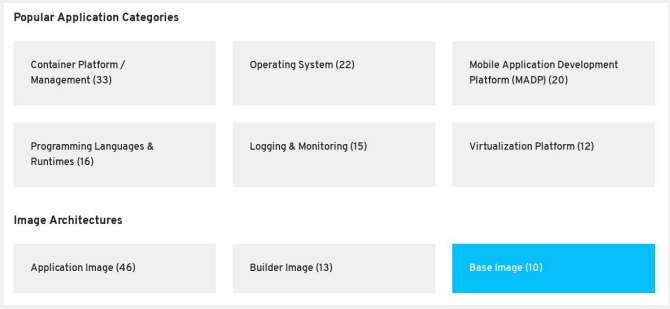
**Jane**

Developer

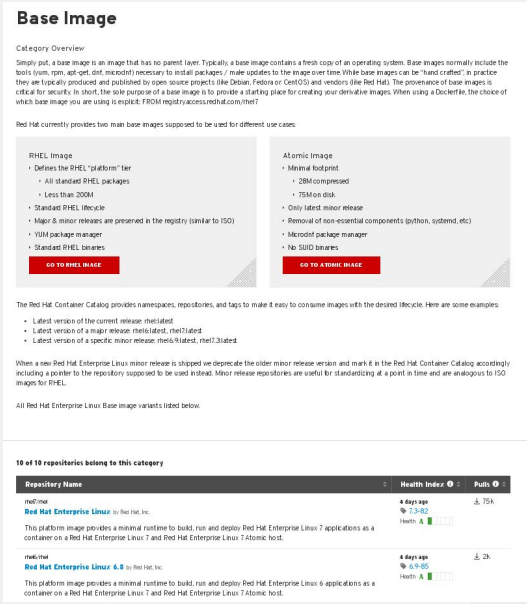
*I'm looking for a base image, what are my options?*




use the Base Images
filter on search page




or use Base Images
tile on explore page




to find our Red Hat base images

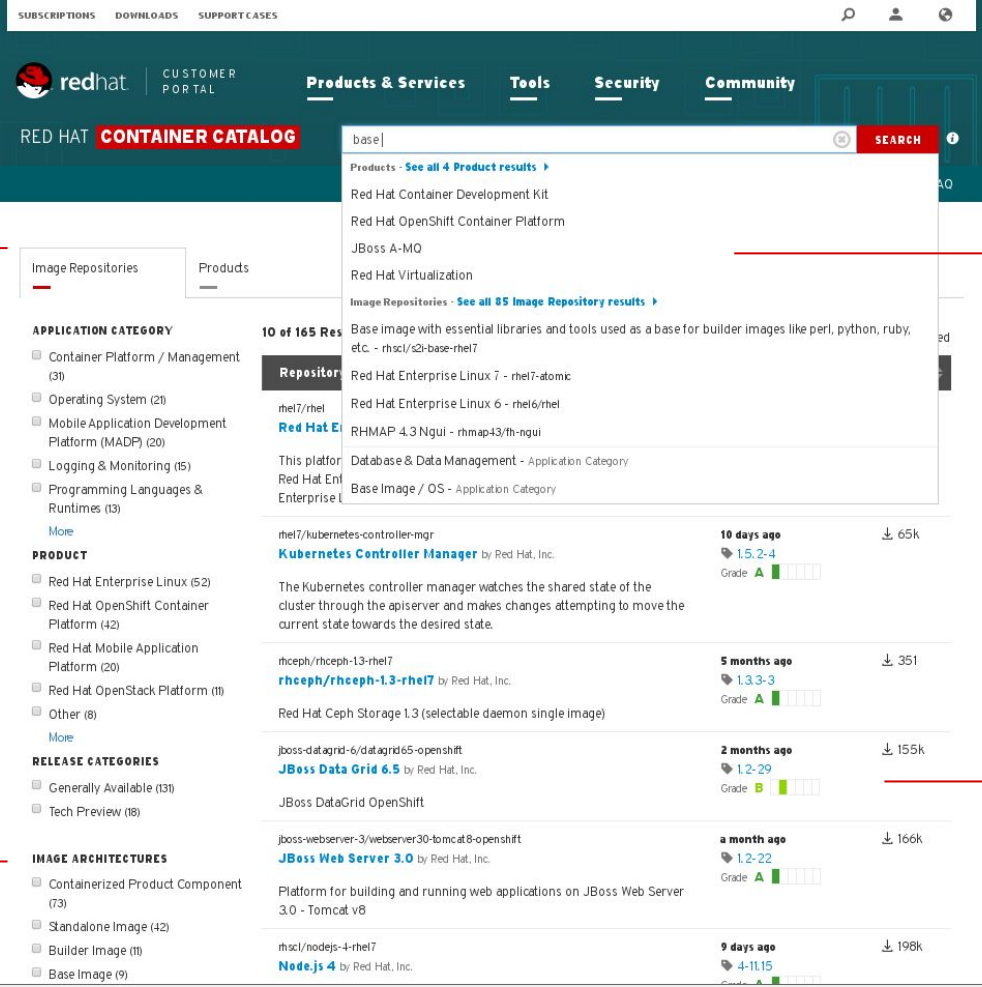


redhat.

You can search for:

- Images / Repos
- Products
- Image ID
- Advisory ID
- Categories
- Keywords
- etc.

Filter facets for multiple characteristics

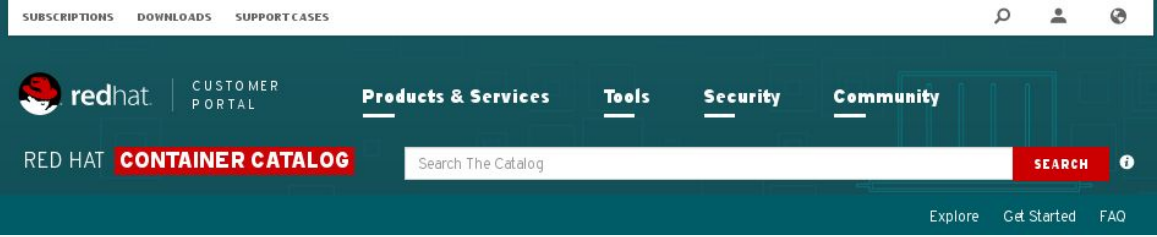



Type-ahead contains products, repositories and app categories

Search results with key data



redhat.



**Joe**

Architect

I want to see the key characteristics of an image.

Is there documentation available around an image?

1 Explore & Search

2 Evaluate & Select

3 Consume & Distribute

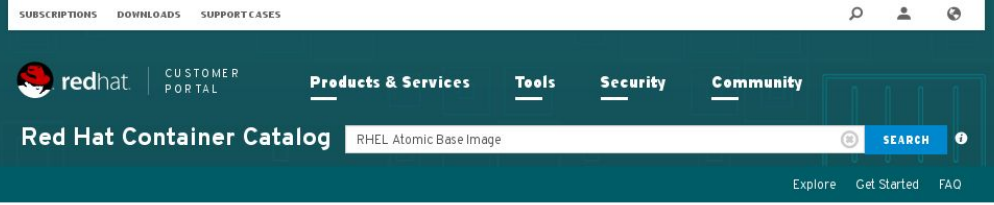
4 Use & Maintain

What are the environment variables defined inside the image?

I would like to learn how this images has been built.

**Jane**

Developer




# RHEL Atomic Base Image

by Red Hat, Inc. | in Product Red Hat Enterprise Linux

`registry.access.redhat.com/rhel-atomic` Updated 5 days ago 7.3-19 : Health Index A

Overview | Get this image | Tech Details | Documentation | Tags

## Description

The Red Hat Enterprise Linux 7 Atomic Base Image is designed to be a fully supported foundation for your custom developed applications which are built and updated rapidly, and don't require the extensive libraries or services in the operating system.This image is maintained by Red Hat and updated regularly, following the latest minor release cadence of Red Hat Enterprise Linux. It is designed for containerized applications that don't rely on a full, traditional Linux userspace, but wish to maintain complete runtime compatibility with RHEL. When used as the source for your containers, only one copy will ever be downloaded and cached in your production environment.Use this image just like you would a regular Red Hat Enterprise Linux distribution. Only a minimal set of tools are provided - components such as python, systemd, and yum are not included by default. Extra packages can be installed and updated with a simplified package manager called microdnf.

**Application Categories** Operating System

**Keywords** base rhel7 atomic

Hide Repository Specifications

| | |
|---|---|
| Registry | registry.access.redhat.com |
| Namespace/Repository | rhel-atomic |
| Release Category | Generally Available |
| Repository Size | 112.5 MB |
| Image Versions | 4 |
| Subscription Required | No |

## Most recent tag

View All Tags

Updated 5 days ago

7.3-19

**Health Index**

A

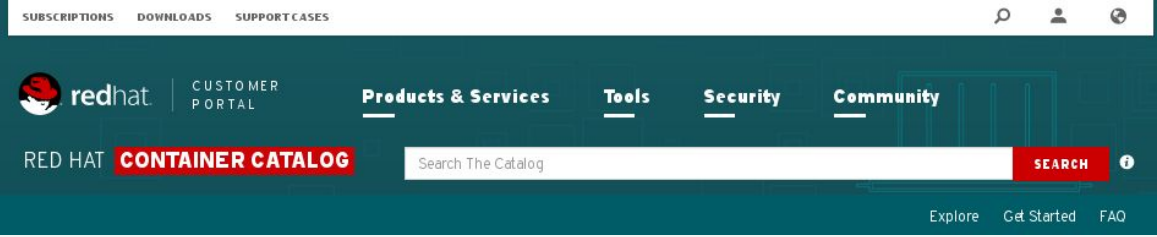
**ImageAdvisory**

RHBA-2017:1123

Show Image Specifications

overview page shows most relevant repository and latest image version data

additional tabs for consumption guidance, further technical details, surrounding documentation and tag index



**Joe**

Architect

I want to learn more how to consume and use this image.

Do I need a subscription or license to pull it?

1 Explore & Search

2 Evaluate & Select

3 Consume & Distribute

4 Use & Maintain

I want to pull this image, what do I need to do?

I'm using Red Hat Satellite 6, how can I sync the repository?

**Jane**

Developer

# RHEL Atomic Base Image

by Red Hat, Inc. | in Product Red Hat Enterprise Linux

`registry.access.redhat.com/rhel-atomic` Updated 11 days ago 7.3-15 : Freshness

Overview | Get this image | Tech Details | Documentation | Tags

**Choose your platform:**

Red Hat Satellite

See Acquiring Red Hat Container Images for general information on acquiring images listed in the Red Hat Container Catalog. Select "Choose your platform" for specific acquire paths.

Satellite 6 supports two different ways to distribute container images to its managed hosts:

A. **External Registries:** You can configure external registries by navigating to **Containers > Registries** in the Web UI of Satellite 6. Note that in this scenario Satellite 6 only triggers commands executed on the corresponding container host. This is a **pass-by** scenario because the image is neither pulled through Satellite 6 nor cached or stored inside Satellite 6. This also applies for the predefined external registry Docker Hub while creating a new container.
B. **Local Content:** Red Hat Satellite allows you to import / synchronize images from local and external registries. Satellite itself can act as an image registry for hosts. However, hosts cannot push changes back to the registry.

In this document we describe how to use Satellite 6 to synchronize external image repositories (**local content, scenario B**).

## 1 Prerequisites

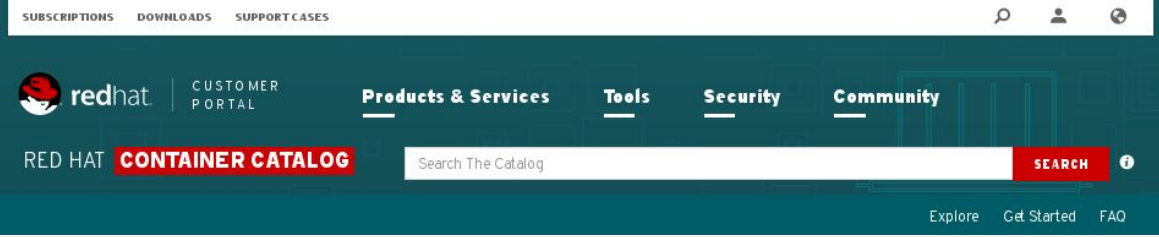
Before container images can be synchronized into Satellite 6 the following prerequisites have to be met:

- Red Hat Satellite 6 has been installed following the Satellite 6 Install Guide
- Subscription Manifest created and uploaded to Satellite 6 to access content
- For CLI Users only: hammer CLI installed and configured

## 2 Creating a Custom Product

consumption guidance for different container runtime env's and registries

consumption details including copyable command lines



**Carl**

Security

I want to see which updates are applicable to an image used by us

I want to see an actionable result for applicable security updates

1 Explore & Search

2 Evaluate & Select

3 Consume & Distribute

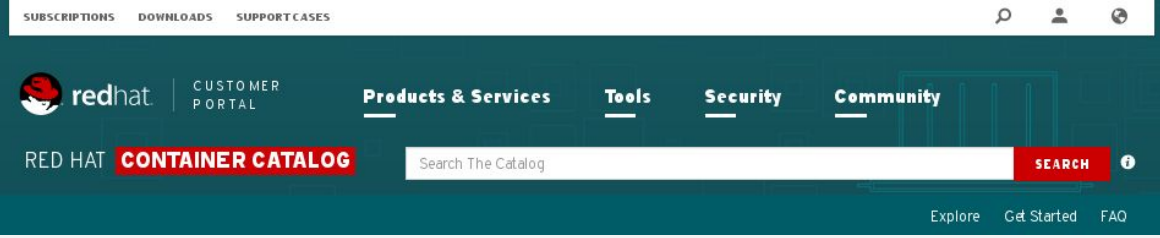
4 Use & Maintain

I want to get a list of all images associated with an advisory ID

I want to see an aggregated and simple freshness description

**Jane**

Developer

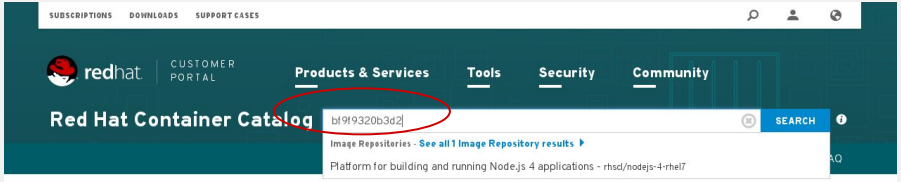


**Jane**

Developer

*How can I get more details around an image I'm using?*

```
[root@dherrman ~]# docker images | grep nodejs
registry.access.redhat.com/rhscl/nodejs-4-rhel7                4-11.14
                bf9f9320b3d2        9 weeks ago         444 MB
[root@dherrman ~]#
```



1 Get the image ID using CLI or registry UI

2 Use the container catalog search to find the image

3 Select the right image version and explore details

# Red Hat Sets New Standard for Trusted, Enterprise-Grade Containers with Industry's First Container Health Index

MAY 02, 2017

*Red Hat extends container inspection and tooling to ISV partner ecosystem; provides customers with enhanced security, reliability and support for deploying Linux containers at scale*

BOSTON--(BUSINESS WIRE)-- Red Hat, Inc. (NYSE:RHT), the world's leading provider of open source solutions, today introduced the industry's first Container Health Index, setting a new standard for enterprise-grade Linux containers. Based upon Red Hat's track record of delivering enterprise-grade open source technologies, including the world's leading enterprise Linux platform, the Container Health Index provides the most comprehensive image detail of any enterprise container service. The index grades all of Red Hat's containerized products as well as the Red Hat base layer of containers from certified independent software vendor (ISV) partners, with Red Hat planning to certify containerized products from 20 ISVs within the next 90 days.

While container-based applications have begun moving into production, not all containers are created or maintained equally. Every container starts with a Linux base layer, which means that every ISV building container images is distributing Linux content. For these containers to be used in production environments, this content needs to be free from known

**Red Hat Registry Stats**

- 227 repositories
- 2,169 images
- 542,525 RPMs

images are static content bundles

**but**

security issues emerge frequently

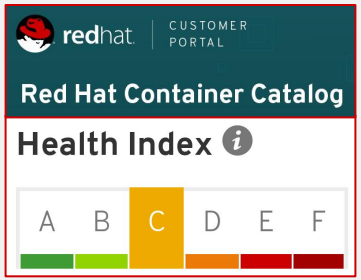
**Red Hat Security Statistics 2016**

- 3134 advisories
- 5075 unique CVEs
- 2016: 97 crit RHSA

health index indicators

**age of the image**

**unapplied updates**




Developed as a **cross-team effort** leveraging Red Hat's Security expertise

**Single item** status (grade A-F) as an aggregated indicator of container health

Leveraging **Red Hat security data** (advisories) for RPMs and images

**Actionable** scan results (RPM, Image)

SUBSCRIPTIONS DOWNLOADS SUPPORT CASES

redhat CUSTOMER PORTAL

Products & Services Tools Security Community

Red Hat Container Catalog bf9f9320b3d2 SEARCH

Explore Get Started FAQ

# Platform for building and running Node.js 4 applications

by Red Hat, Inc. | in Product Red Hat Enterprise Linux

registry.access.redhat.com/rhscl/nodejs-4-rhel7 Updated 4 days ago 4-11.16 : Health Index A

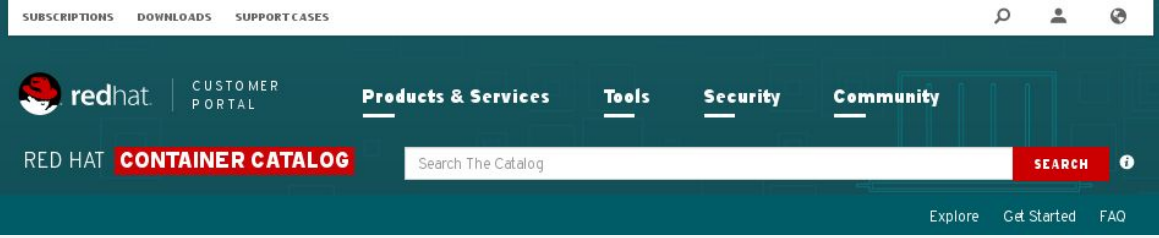
Overview Get this image Tech Details Documentation Tags

| Tag Name | Date Pushed | Image Advisory | Health Index | Docker Image ID |
|---|---|---|---|---|
| 4-11.16 4 latest | 4 days ago | RHBA-2017:1127 | A | 9e8704e70637 |
| 4-11.15 | 16 days ago | RHBA-2017:0975 | C | 79b2e96829e0 |
| 4-11.14 | 2 months ago | RHBA-2017:0404 | C | bf9f9320b3d2 |
| 4-11.13 | 3 months ago | RHBA-2017:0174 | C | 6a532adbfabf |

list of all image versions inside this repository

Container Health Index history

key version attributes



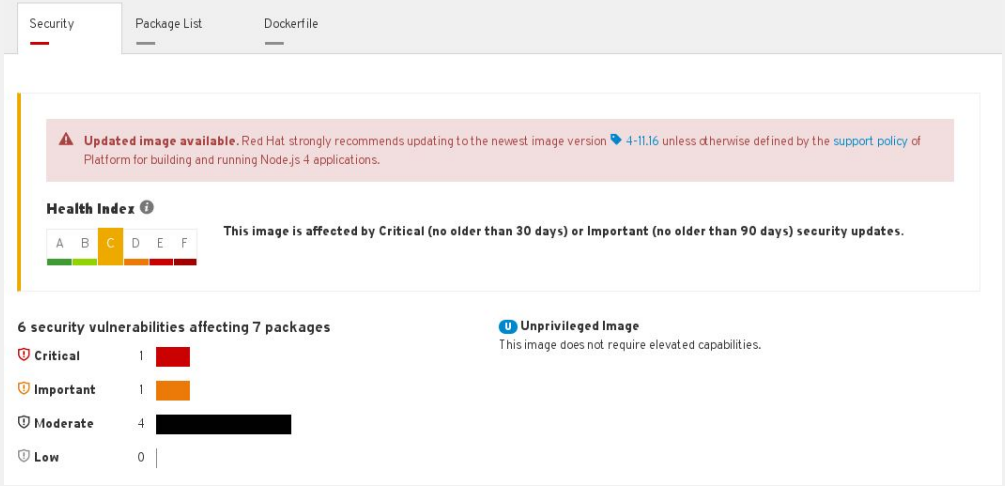
**Carl**

Security

*What is the associated risk with the content inside the image?*

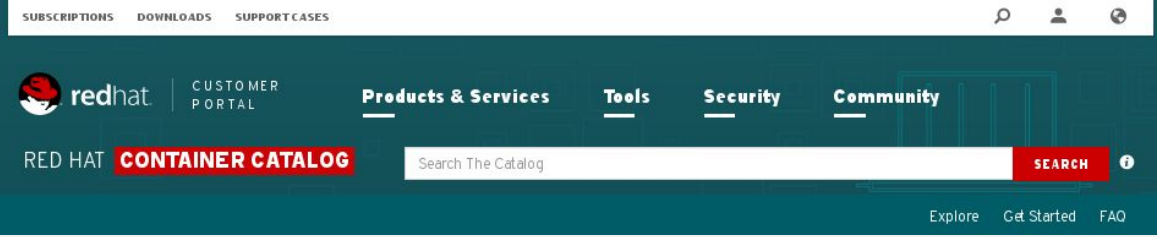
warning if non-current image version

vulnerabilities by advisory severity




Container Health Index based on applicable security updates and its age

privilege requirements



## Carl

Security

*How can I get rid of those vulnerabilities ?*

**Affected Packages**

7 of 528 packages have security-related updates

Search affected packages

| Impact | | Affected Package | RPM Advisory | Fixed in Image |
|---|---|---|---|---|
| Critical | CVE-2017-5461 | nss-util-3.21.3-1.1.el7_3.x86_64 | RHSA-2017:1100 | 4-11.16 |
| Critical | CVE-2017-5461 | nss-sysinit-3.21.3-2.el7_3.x86_64<br>nss-tools-3.21.3-2.el7_3.x86_64<br>nss-3.21.3-2.el7_3.x86_64 | RHSA-2017:1100 | 4-11.16 |
| Important | CVE-2017-2636 | kernel-headers-3.10.0-514.10.2.el7.x86_64 | RHSA-2017:0933 | 4-11.16 |

Red Hat advisory severity

CVE ID

content advisory which contains fix

newer image version which contains fix

# What's next?

Upcoming features of future Red Hat Container Catalog releases

- Ecosystem content incl. Red Hat Certified and OpenShift Primed
- Additional acquire paths, image usage documentation
- OpenShift on-premise / Online enhancements
- Subscribe to notifications for products, images and categories for new images, image versions, advisories, freshness grade changes
- Subscriptions / licenses, support policies, FOSS license compliance

You have feedback?
An idea or feature request?

Let's meet at our **User Experience Design** booth.

**Partner Pavilion**
Exhibit Hall A

Try it out: https://access.redhat.com/containers

# ATOMIC STATE OF THE UNION

## Lightning Talk: The latest and greatest in Red Hat's container initiative

Mike McGrath
Platform Engineering
May 4th, 2017



redhat.

# WAT?

## What is Atomic (for the uninitiated)

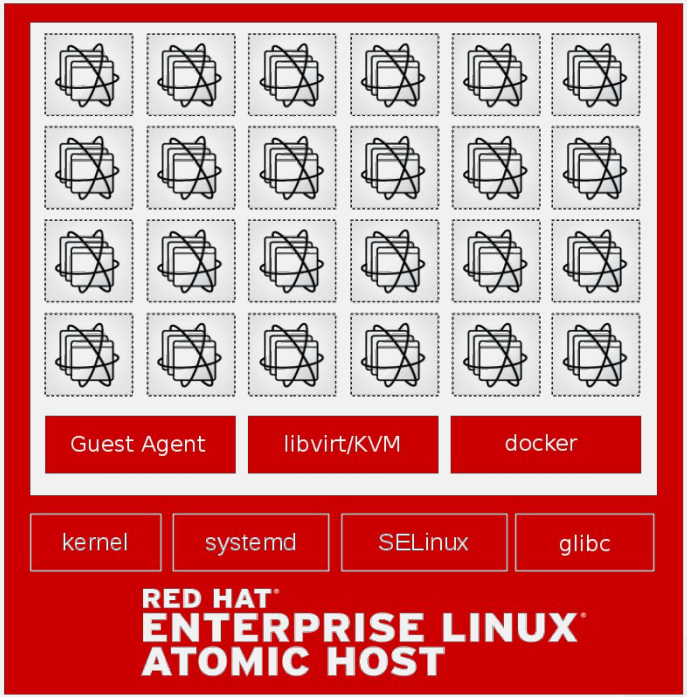
redhat.

# Atomic Host

## A faster moving, purpose built host

Making Atomic Host modular and further isolating software stacks from OS Updates

- Built for containers, hypervisors, embedded systems, storage & network appliances, etc
- rpm-ostree only
  - Highly secure read-only OS (/usr)
  - Reliable upgrade & rollback
  - Flexibility via host extension model

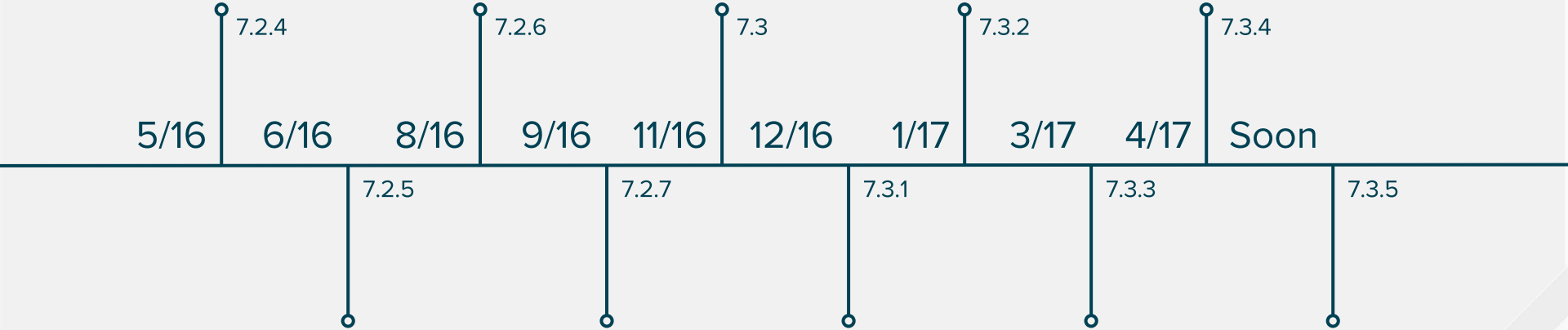





redhat.

# Releases

We've been averaging one release about every 5-6 weeks



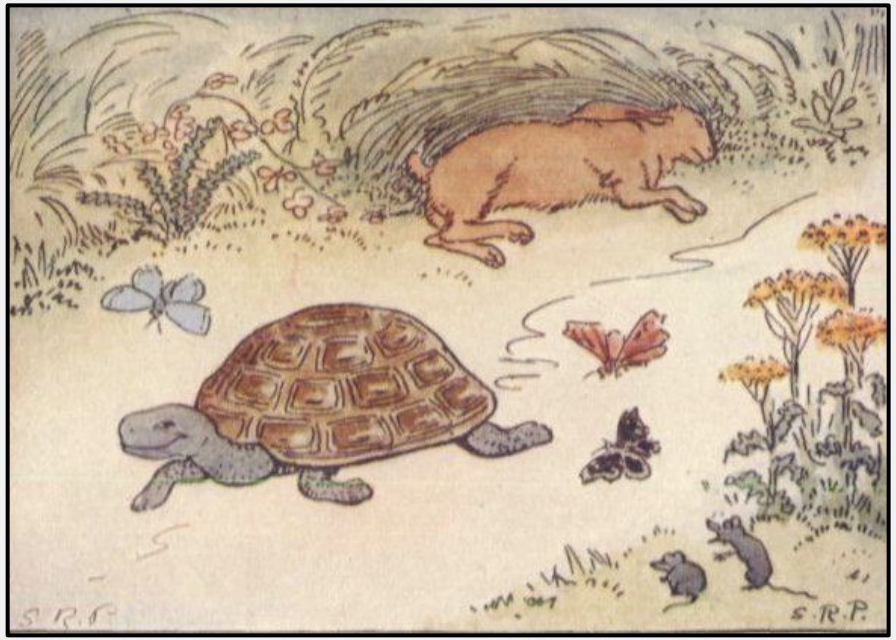

** Excludes asynchronous security updates*



redhat.

# Multi-Docker

Some thought we were going too fast, others thought to slow!

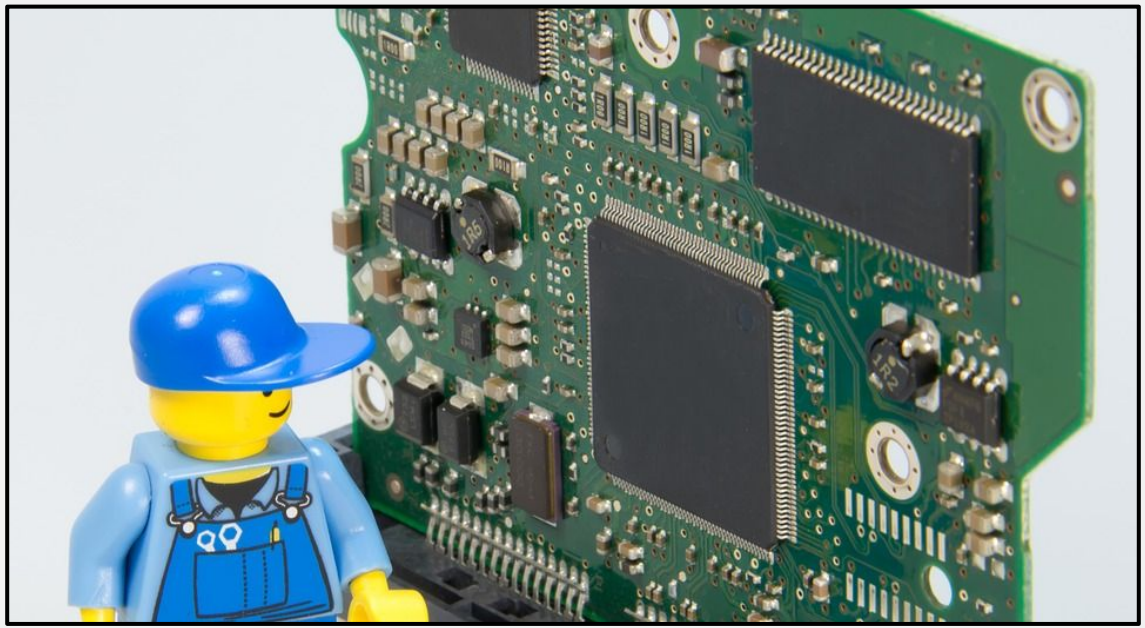




redhat.

# OSTree Unlock

Others wanted easier ways to troubleshoot Atomic Hosts

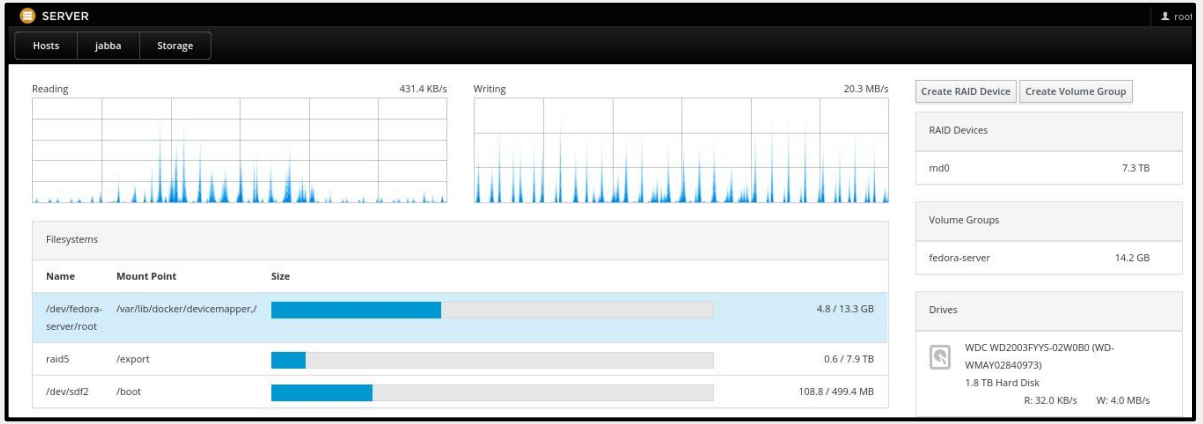




redhat.

# Devmode

Developers asked for an easier way to use Atomic on their workstation






redhat.

# Features

In fact, we've had more than 85 significant features introduced in the last year

- Multiple Docker Versions
- OSTree Unlock
- Package Layering
- Runc
- Skopeo
- Devmode
- System Containers
- MicroDNF
- Containerized Kubernetes

RED HAT® ENTERPRISE LINUX® ATOMIC HOST

# Fedora Atomic Host

At the start of the year we started targeting a release every two weeks (compared to Fedora's 2 times per year cadence)

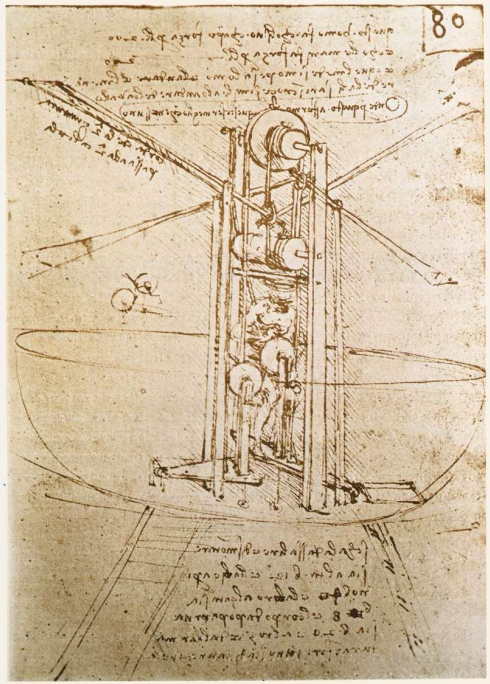
See things first in Fedora!

- 18 releases in the last year
- That's almost one release every three weeks!

redhat.

# Upstream Efforts

- SELinux support with OverlayFS
- POSIX compliance for OverlayFS
- user namespaces
- Shiftfs
- Container live migration
- OpenShift Origin on CentOS and Fedora Atomic Host
- Ongoing containerization





redhat.

# Credits

- Tortoise and hare - https://commons.wikimedia.org/wiki/File:The_Tortoise_and_the_Hare_-_Project_Gutenberg_etext_19993.jpg
- Lego Man - https://pixabay.com/p-499799/?no_redirect
- Confused - https://www.flickr.com/photos/83633410@N07/7658298768



redhat.

RED HAT SUMMIT

# THANK YOU

plus.google.com/+RedHat

facebook.com/redhatinc

linkedin.com/company/red-hat

twitter.com/RedHatNews

youtube.com/user/RedHatVideos

# GPL IN THE WORLD OF CONTAINERS

David Levine
Vice President and Assistant General Counsel

Richard Fontana
Senior Commercial Counsel
May 4, 2017



redhat.

# GPL and Copyleft Basics



redhat.

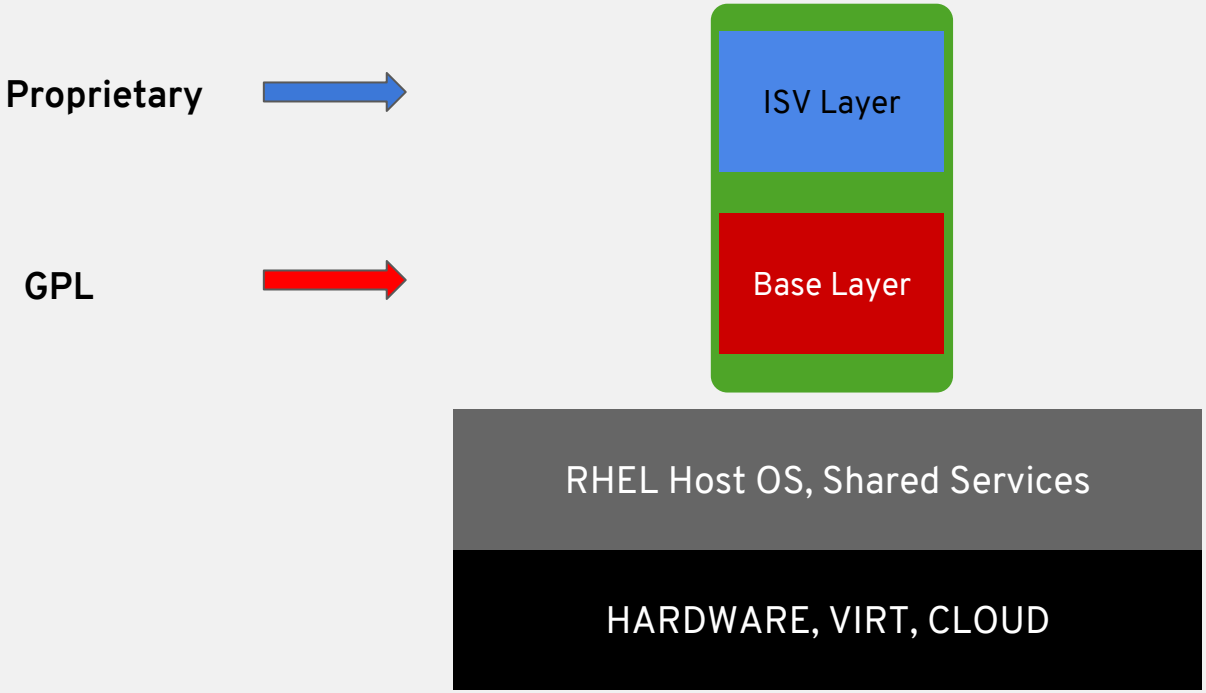
# Copyleft Scope: Single Container Image

Does the combination of GPL and non-GPL software in a single container image create a single program or a derivative work and, therefore, implicate GPL copyleft?



redhat.

# Copyleft Scope: Single Container Image






redhat.

# Copyleft Scope: Single Container Image

- Base layers of images contain GPL-licensed code
- Upper layers contain proprietary ISV app
- GPLv2: mere aggregation clause; GPLv3 "Aggregate"
- Assembly of software into container images does not raise any special GPL copyleft scope issue
  - Container image format uses established packaging (tar format)
  - Share characteristics with RPMs, VM images
  - No basis for analyzing container images differently from past Linux stack distribution media for purposes of GPL copyleft scope



redhat.

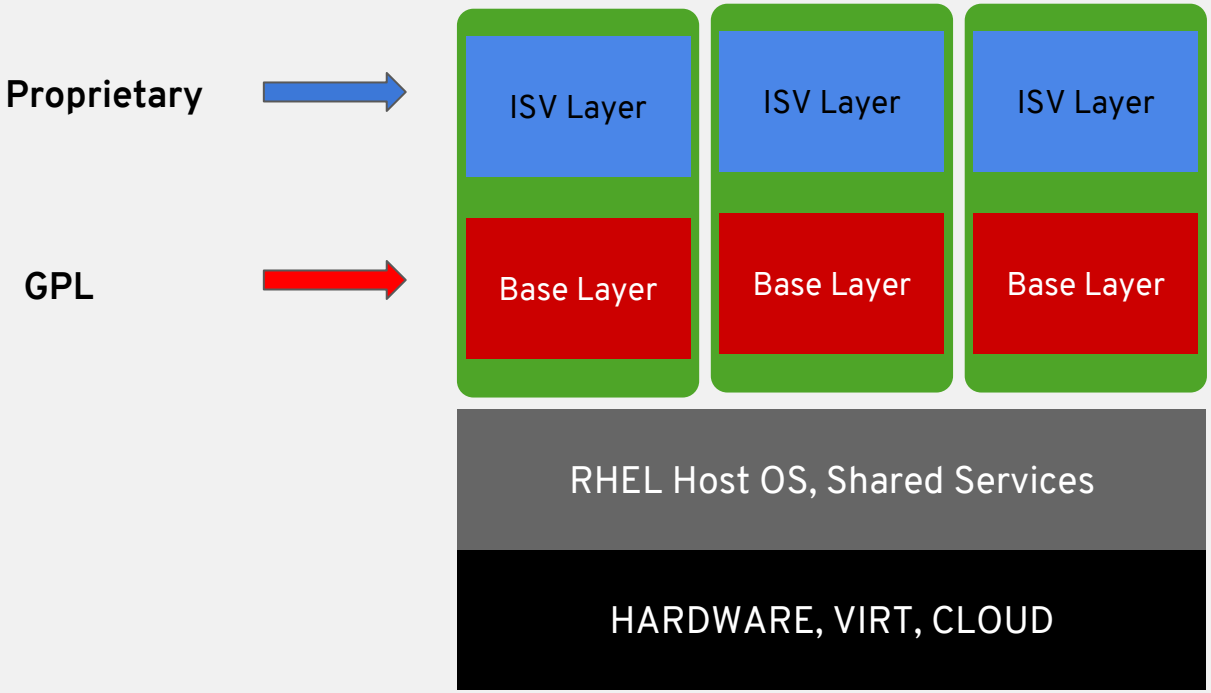
# Copyleft Scope: Multiple Containers

Can software in one container fall within GPL copyleft scope of software in another container?



redhat.

# Copyleft Scope: Multiple Containers






redhat.

# Copyleft Scope: Multiple Containers

- While decomposition into multiple containers is not itself a guarantee, containerization makes technical boundaries between components more apparent and provides a strong indication of 'separateness'.
  - Software in separate containers runs in separate processes, and a process boundary is an indicator of GPL copyleft scope.
  - FSF contrasts:
    - software linked and running in a shared address space (in same copyleft scope)
    - communicating over Unix pipes (separate from a copyleft perspective)
  - Multi-container applications: more like pipes - separate



redhat.

# THANK YOU

plus.google.com/+RedHat

facebook.com/redhatinc

linkedin.com/company/red-hat

twitter.com/RedHatNews

youtube.com/user/RedHatVideos

LEARN. NETWORK.
EXPERIENCE
**OPEN SOURCE.**



redhat.