CONTAINERS IN THE ENTERPRISE

TRANSFORM HOW YOU DELIVER APPLICATIONS

Josh Preston
Solutions Architect
Technical Event Series 2016
AGENDA

- What are Linux Containers?
- Enterprise Challenges for Container Adoption and How Red Hat Solves These
- Kubernetes Architecture
- Real World Container Adoption
- Red Hat’s Container Roadmap
- Q&A
What are Linux Containers?
WHAT ARE LINUX CONTAINERS?

Software packaging concept that typically includes an application and all of its runtime dependencies

- Easy to deploy and portable across host systems
- Isolates applications on a host operating system
- In RHEL, this is done through:
  - Control Groups (cgroups)
  - Kernel namespaces
  - SELinux, sVirt, iptables
  - Docker
TRADITIONAL OS VS. CONTAINERS

Packaged dependencies = faster boot times + greater portability
WHY COMPANIES ARE USING CONTAINERS

How important are the following container benefits to your organization? (critical or very)

- Greater application portability: 73%
- Delivering/deploying applications faster: 72%
- Greater deployment flexibility: 70%
- Faster provisioning: 69%

Base: 171 IT and Developer/programmer decision-makers at companies with 500+ employees in APAC, EMEA, and NA
Source: A commissioned study conducted by Forrester Consulting on behalf of Red Hat, January, 2015
BENEFITS COMPANIES USING CONTAINERS ARE SEEING

"What are the top three quantifiable benefits your firm has realized from the use of containers?"

- Higher quality releases: 36%
- Better application scalability: 29%
- Better support for microservices: 22%
- Shorter test cycles: 21%

Base: 171 IT and Developer/programmer decision-makers at companies with 500+ employees in APAC, EMEA, and NA
Source: A commissioned study conducted by Forrester Consulting on behalf of Red Hat, January, 2015
Why are Containers “new” and cool... again?
CONSISTENT PACKAGING FORMAT

Docker provides a language agnostic packaging format and runtime API.
PACKAGED DEPENDENCIES

Package dependencies ensure consistency and portability*

* The one thing not packaged is the Linux Kernel! Therefore host systems need to be the same distribution and version to guarantee portability.
STEP 1 – LAPTOP
> docker run dockerfile/nodejs
SUCCESS!
GAME OVER!
STEP 2 - PRODUCTION
> containerize entire datacenter
...STEP 1.1?
CONTAINER ADOPTION CHALLENGES

Containerizing the datacenter requires planning...

Organizations need a secure and reliable foundation on which they can run and orchestrate multi-container based applications at scale.
CONCERNS ABOUT ENTERPRISE READINESS OF CONTAINERS

Combined with hardened OS technologies & Orchestration, they are

The world of containers doesn't end with Docker

“The open-source app containerization startup has built up quite a bit of momentum, but it's still not entirely ready for enterprise.”

Matt Weinberger
Computerworld | Feb 9, 2015
TOP CURRENT CONTAINER CHALLENGES

What are the top three challenges your organization has experienced using containers?

- Security: 53%
- Performance: 44%
- Integration with dev tools and processes: 41%
- Lack of certification: 35%
- Management: 35%

Base: 171 IT and Developer/programmer decision-makers at companies with 500+ employees in APAC, EMEA, and NA
Source: A commissioned study conducted by Forrester Consulting on behalf of Red Hat, January, 2015
Enterprise Challenge #1: Security
SECURITY IMPLICATIONS

What's inside the container and where it comes from matters
WHAT'S INSIDE THE CONTAINER MATTERS

36% of official images in Docker Hub contain high priority security vulnerabilities

- High vulnerabilities: ShellShock (bash), Heartbleed (OpenSSL), etc.
- Medium vulnerabilities: Poodle (OpenSSL), etc.
- Low vulnerabilities: gcc: array memory allocations could cause integer overflow

AND THAT'S WHY THE OPS GUY IS FREAKING OUT
Container Security

Secure and trusted Linux containers for the enterprise

**ISOLATION OF HOSTS**
Host OS + SELinux maintained by trusted kernel engineers and frequently updated.

**ARE SOURCES TRUSTED?**
36% of Docker Hub official images contain high priority security vulnerabilities.*

**WHAT’S INSIDE CONTAINERS**
Red Hat + Black Duck = secure, trusted model for validating container contents.

**TRUST IS TEMPORAL**
New vulnerabilities are identified daily and containers become stale over time.

Once upon a time there were Three Little Pigs, who had different types of homes to choose from...
SECURITY BEST PRACTICES

Treat container services just like regular services

- Drop privileges as quickly as possible
- Run your services as non Root wherever possible
- Treat root within a container the same as root outside of the container
- Only run containers from trusted parties!
  - “Docker is about running random crap from the internet as root on your host”
IMPORTANCE OF CERTIFICATION

UNTRUSTED

- Will what’s inside the containers compromise your infrastructure?
- How and when will apps and libraries be updated?
- Will it work from host to host?

RED HAT CERTIFIED

- Trusted source for the host and the containers
- Trusted content inside the container with security fixes available as part of an enterprise lifecycle
- Portability across hosts

- Container Development Kit
- Certification as a service
- Certification catalog
- Red Hat Container Registry
FUTURE CONSIDERATIONS
OpenSCAP for Container Compliance

SCAN ALL CONTAINERS FOR KNOWN VULNERABILITIES

# docker-oscap cve --all --download --arf report-arf.xml

  Fetching OVAL definitions for RHSA .......... ok
  Inflating ........ ok
  Scanning rhel7-elasticsearch ...... ok (compliant, no CVE identified)
  Scanning rhel7-mongodb ........... fail (2 CVE found)
  Scanning ubuntu-httpd .............. notchecked (no CVE definitions)
  Exporting Asset Report .......... ok
  CVE Scan finished in 1m35s

https://github.com/OpenSCAP/container-compliance
FUTURE CONSIDERATIONS

OpenSCAP for Container Compliance

MEASURE CONTAINER IMAGE SECURITY POSTURE TO POLICY

```bash
# docker pull fedora
# docker-oscap image fedora xccdf eval \
   --profile xccdf_org.ssgproject.content_profile_common \
   /usr/share/xml/scap/ssg/fedora/ssg-fedora-ds.xml
```

https://github.com/OpenSCAP/container-compliance
Enterprise Challenge #2: Performance
PERFORMANCE-IMPACTING FEAT.

What can we tune for container performance?

- Volumes
  - Bind mount storage from data container (or host)
- Device Mapper
  - Production mature, well documented storage driver
- --net=host
  - Expose host network to container; performs better at a cost
- C Groups
  - CPU Shares, CPUSets, Memory Limits, nsinit
- Sysctls
  - Used to modify kernel parameters at runtime

Can't I just push a button and make it go fast!?!?...
CUSTOM TUNED PROFILES
Create Custom Tuning Profiles

Parents
- throughput-performance
- balanced
- latency-performance

Children
- network-throughput
- desktop
- network-latency

Children/Grandchildren
- Your Web Profile
- Your Database Profile
- Your Middleware Profile

Source: http://redhat.slides.com/jeremyeder/performance-analysis-of-docker#/
TUNED PROFILES
Available Throughout Red Hat's Product Line

| RHEL7 Desktop/Workstation          | balanced               |
| RHEL6/7 KVM Host, Guest           | Virtual-host/guest     |
| Red Hat Storage                   | rhs-high-throughput, vlrt |
| RHEL Atomic                       | atomic-host, atomic-guest |
| RHEL7 Server/HPC                  | throughput-performance |
| RHEV                              | virtual-host           |
| RHEL OSP (compute node)           | virtual-host           |

How do I create my own tuned profile on RHEL7?  
https://access.redhat.com/site/node/731473
MARIA DB BENCHMARK

SysBench Results

Within 1.5-3% of Bare Metal performance

Source: http://redhat.slides.com/jeremyeder/performance-analysis-of-docker/#/
NETWORK LATENCY

Sysbench Results

Small (~2ms) Bridge overhead

Source: http://redhat.slides.com/jeremyeder/performance-analysis-of-docker#/
NETWORK THROUGHPUT

Sysbench Results

Almost no loss of throughput

Source: http://redhat.slides.com/jeremyeder/performance-analysis-of-docker#/

netperf TCP_STREAM-RX

[Graph showing throughput results]

Avg Mbps

Size

8 16 32 64 128 256 512 1024 2048 4096 8192 16384 32768 65536

ExtHost/Host TCP_STREAM-RX
ExtHost/Container TCP_STREAM-RX
Container/Container-2hosts TCP_STREAM-RX
Container/Container-2hosts -net=host TCP_STREAM-RX
Enterprise Challenge #3: Integration
OPENSHIFT
Enabling Dev & Ops

Self-Service
Multi-Language
Automation
Collaboration

Standards Based
Web Scale
Open Source
Enterprise Grade

by Red Hat®
DOCKER BUILDS

Integrated container image builds

Bring existing Docker applications and leverage the orchestration of OpenShift
Source To Image Walk-Through

Code

Build

Deploy

Can configure different deployment strategies like A/B, Rolling upgrade, Automated base updates, and more.

Can configure triggers for automated deployments, builds, and more.
Source To Image Walk-Through

**Code**

Developers can leverage existing development tools and then access the OpenShift Web, CLI or IDE interfaces to create new application services and push source code via GIT. OpenShift can also accept binary deployments or be fully integrated with a customer’s existing CI/CD environment.
Build

OpenShift automates the Docker image build process with Source-to-Image (S2I). S2I combines source code with a corresponding Builder image from the integrated Docker registry. Builds can also be triggered manually or automatically by setting a Git webhook.
Source To Image Walk-Through

Deploy

OpenShift automates the deployment of application containers across multiple Node hosts via the Kubernetes scheduler. Users can automatically trigger deployments on application changes and do rollbacks, configure A/B deployments & other custom deployment types.
Enterprise Challenge #4: Management & Orchestration
CONTAINER ORCHESTRATION

Kubernetes

Docker is an engine, container and image format with limited orchestration & networking between hosts

Kubernetes is a way to

● Describe and launch containers
● Monitor and maintain state
● Do container oriented networking

Kubernetes builds on Docker to make management of many containers like managing containers on a single system

More technical detail later...
FUTURE STATE WITH ANSIBLE

<table>
<thead>
<tr>
<th>DOWNLOAD</th>
<th>RUN</th>
<th>AUTOMATE</th>
<th>SCALE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ansible</td>
<td>Atomic Host</td>
<td>Ansible</td>
<td>Kubernetes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>OpenShift Enterprise/Hosted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Red Hat Storage</td>
</tr>
</tbody>
</table>

RED HAT FUTURE

44
A DEV TEAM’S CONTAINER JOURNEY

WE PROVIDE ALL THE TOOLS

The Atomic+Ansible toolbox contains everything required to help developers make the journey from laptop all the way to Kubernetes & OpenShift.

One developer, first container (how can I docker?)

One developer, first container app (multiple containers)

Dev team, moving fast and breaking things (repeatability is key)

Dev meets Ops (great, how do we manage at scale?)

DevOps (wow, maybe we should have a platform for all this)
OPEN HYBRID CLOUD
Red Hat's Vision for Consistent Container Management

Fully engineered solutions all based on Red Hat Enterprise Linux
Enterprise Challenge #5: Certification & Standards
RED HAT CONTAINER CERTIFICATION

UNTRUSTED
- Will what’s inside the containers compromise your infrastructure?
- How and when will apps and libraries be updated?
- Will it work from host to host?

RED HAT CERTIFIED
- Trusted source for the host and the containers
- Trusted content inside the container with security fixes available as part of an enterprise lifecycle
- Portability across hosts

[Diagram showing container development kit, certification as a service, certification catalog, and Red Hat Container Registry]
CREATING DE FACTO STANDARDS

Red Hat works with the open source community to drive standards for containerization.

- Isolation with Linux Containers
- Container format with Docker
- Orchestration with Kubernetes
- Container registry and discovery
Kubernetes Architecture
KUBERNETES ARCHITECTURE

Nodes

Nodes are instances of RHEL where apps run.
App services run in docker containers on each node
KUBERNETES ARCHITECTURE

Pods run one or more Docker containers as a unit.
Registries are where application images are stored.
Masters leverage Kubernetes to orchestrate nodes/apps.
KUBERNETES ARCHITECTURE

Masters

Master provides authenticated API for users & clients
Master uses etcd key-value store for persistence
KUBERNETES ARCHITECTURE

Masters

Master provides scheduler for pod placement on nodes
Pod placement is determined based on defined policy.
Services allow related pods to connect to each other
Management / Replication controller manages the pod lifecycle
What if a pod goes down?
Replication controller automatically recovers and deploys a new pod
Pods can attach to shared storage for stateful services
Routing layer routes external app requests to pods
Developers can access OpenShift via Web, CLI or IDE
DOCKER & KUBERNETES DEMO
From the lens of OpenShift 3

- Docker
  - Docker Files
  - Basic Docker Commands

- Kubernetes
  - Example YAML config file
  - Dynamically scaling applications
CONTAINER-BASED APPLICATION DELIVERY SOLUTIONS

- Seamlessly manage from infrastructure to applications based on OpenStack
- Develop, build, and manage container-based applications
- Run and orchestrate multi-container based applications at scale
Real World Container Adoption
GOOGLE & OPENSSHIFT ONLINE
Some of the most advanced infrastructures run on containers

“Everything at Google, from Search to Gmail, is packaged and run in a Linux container.”

- Eric Brewer, VP of Infrastructure, Google

Source: http://googlecloudplatform.blogspot.com/2014/06/an-update-on-container-support-on-google-cloud-platform.html
Deploying their new hybrid-cloud on OpenShift 3

- **Enterprise Requirements at Global Scale**
  - 1.6+ billion data requests processed per day
  - 525+ million travel agency bookings processed in 2014
  - 95% of the world’s scheduled network airline seats
  - December 2014
    - At peak: ~210,000 queries per second
    - Average: ~145,000 queries per second
  - 100+ TB of compressed data logged **every day!**

Containerized Docker containers running on commoditized converged hardware using Red Hat Gluster Storage as the persistent storage layer

- Simplified Deployment via containers, with seamless upgrade and rollback
- New service to market quicker and cheaper, increasing subscriber stickiness and satisfaction
- Eliminated forklift upgrades and expensive renewals as the service expands

The initial deployment is a single datacenter and there are plans to roll out to a further 7 DC’s
LINUX CONTAINERS AREN'T NEW

Neither are the technologies that Red Hat is using to secure, isolate and manage containers

- The technologies Red Hat is using for container security,

- In RHEL, this is done through:
  - SELinux, sVirt – RHEL 4
  - Control Groups (cgroups) – RHEL 6
  - Kernel namespaces – RHEL 6
    (include. network)
  - Docker – RHEL 7, Ok… so this one is new!
Red Hat and Containers
There are advantages to packaging applications in a standardized format such as Docker.

More efficiency comes from having a standardized transportation system for containers.

Automation of packing and loading of containers provides even more efficiency.

Manage containers and infrastructure at scale.
RED HAT ATOMIC ENTERPRISE PLATFORM

Run and orchestrate multi-container based applications at scale

An integrated infrastructure platform powered by Red Hat Enterprise Linux that is designed to run, orchestrate, and scale container-based applications and services

- Easily manage and scale applications and infrastructure through a managed cluster of container hosts
- Gain application resiliency and elasticity via orchestration and service aggregation
OPENSHIFT ENTERPRISE

3.x Roadmap Enhancements

- Metric-driven autoscaling
- External service bridge/registry
- Pod/container idling
- SCL 2 image runtime version updates
- Enhanced GIT/SCM & CI integration
- User interface enhancements
- Logging & metrics / ELK integration
- Additional storage plugins
- Networking enhancements
OPENSHIFT DEDICATED

High-availability, scalable OpenShift clusters on the public cloud - installed and backed by Red Hat engineering and operations

- Fully-managed enterprise service with seamless software updates and status portal for cluster updates and notifications
- Red Hat enterprise container technology in a single product with fast time to delivery
- Low lifetime cost and risk with no lock-in compared to other fully-managed or DIY solutions
- Multiple availability regions
- HA master/infrastructure nodes that scale at no additional cost
- Enable persistent storage for containerized applications
- Hardware VPN connection with customizable routing or VPC peering
OPENSHIFT ONLINE

On-demand public cloud services managed by Red Hat

- Scalable application platform for developers and IT professionals
- Supported the creation of over 2.9 million applications and more than 4 Billion requests/day
- Provides on-demand access to v2 OpenShift technology
- OpenShift Online is migrating to v3 technology in developer preview
ANSIBLE and ANSIBLE TOWER

Automation glues all of your processes together

- Simple, Powerful, and Agentless automation
- Describe container payloads, build, and deploy as part of an automated process
- Tower layers in control, knowledge, and delegation
- Together, this is the same automation technology that can automate your traditional IT as well
xPaaS SERVICES
Additional Jboss & Middleware Services

Application Container Services
- JBoss Enterprise Application Platform
- JBoss Web Server / Tomcat
- JBoss Developer Studio

Integration Services
- Fuse *
- A-MQ
- Data Virtualization

Business Process Services
- Business Process Management *
- Business Rules Management System

Mobile Services
- Red Hat Mobile / FeedHenry *

* Coming Soon
RED HAT STORAGE
Enterprise Grade Persistent Storage for Containers

- Red Hat Storage provides the scale, agility and enterprise grade features needed by mission critical application deployed in containers
- Red Hat Storage can provide a dedicated storage cluster, attached to nodes within a Atomic Host or OpenShift cluster
- Red Hat Storage is itself containerized and available via the Red Hat registry
- Red Hat Storage is integrated with RHEL, Atomic Host and OpenShift to provide a choice of volume plugins for developers
RED HAT STORAGE
Hyper Converged Persistent Storage for Containers

- The next step in the evolution of persistent storage for containers is to hyper converge storage containers with application containers
- Red Hat Storage is uniquely positioned to offer this capability

Benefits
- Lower TCO
- Unified Orchestration
- Ease of Use
- Greater control
- Enables the vision of storage as a service
OPENSTACK & CLOUDFORMS
Expanded Integration

- Automating deployment of OpenShift clusters, add & remove Kubernetes Nodes
- Networking provider integration with Neutron
- Storage integration with OpenStack Cinder (Block) and Manila (File)
- Manage OpenStack and OpenShift with CloudForms
CLOUDFORMS
Administration & Container Management

- Cloud Forms functionality now included with OpenShift Enterprise to improve control over apps and infrastructure
- Monitor and manage resource consumption of containers running in OpenShift Enterprise
- Docker and Kubernetes aware (containers, pods, services...)
SATELLITE
Red Hat Satellite & Containers Vision for Registry Federation & Discovery

Container Registries

Satellite 6 serves as an on-premise registry for Linux Containers

Containers managed through lifecycle environments versioned with Content Views

Environments are mirrored to Capsules

Docker Pull to host

Red Hat Registry

Docker Hub Registry

Private On-Prem Registry
APPLICATION PORTABILITY

portability across environments

PHYSICAL  VIRTUAL  PRIVATE CLOUD  PUBLIC CLOUD
WHY RED HAT

Comprehensive offerings and capabilities enable enterprise-wide container adoption.
CONTAINERS IN THE ENTERPRISE
They're ready today with Red Hat

Red Hat transforms application delivery with the first credible hybrid cloud platform for container-based applications and services.
WHERE TO GET STARTED

Next steps

Get Started with Docker Formatted Container Images on Red Hat Systems
http://red.ht/1vcxBVv

Container Discovery Workshops
Consulting services to help your business realize the value of container technologies

Managing Containers with Red Hat Enterprise Linux Atomic Host (RH270)
http://red.ht/1MNkAN5
THANK YOU. QUESTIONS?
Appendix – Additional Links

- Kubernetes Book – Promotion on OpenShift site: https://www.openshift.com/promotions/kubernetes
- Docker Image examples from Project Atomic: https://github.com/projectatomic/docker-image-examples
- OpenShift GitHub including sub-projects like Source-2-Image (STI) and Image-Streams: https://github.com/openshift/
- Integration of OpenShift Enterprise with Red Hat Storage https://url.corp.redhat.com/ec63e59
- Enabling persistent storage for containers https://url.corp.redhat.com/8133023