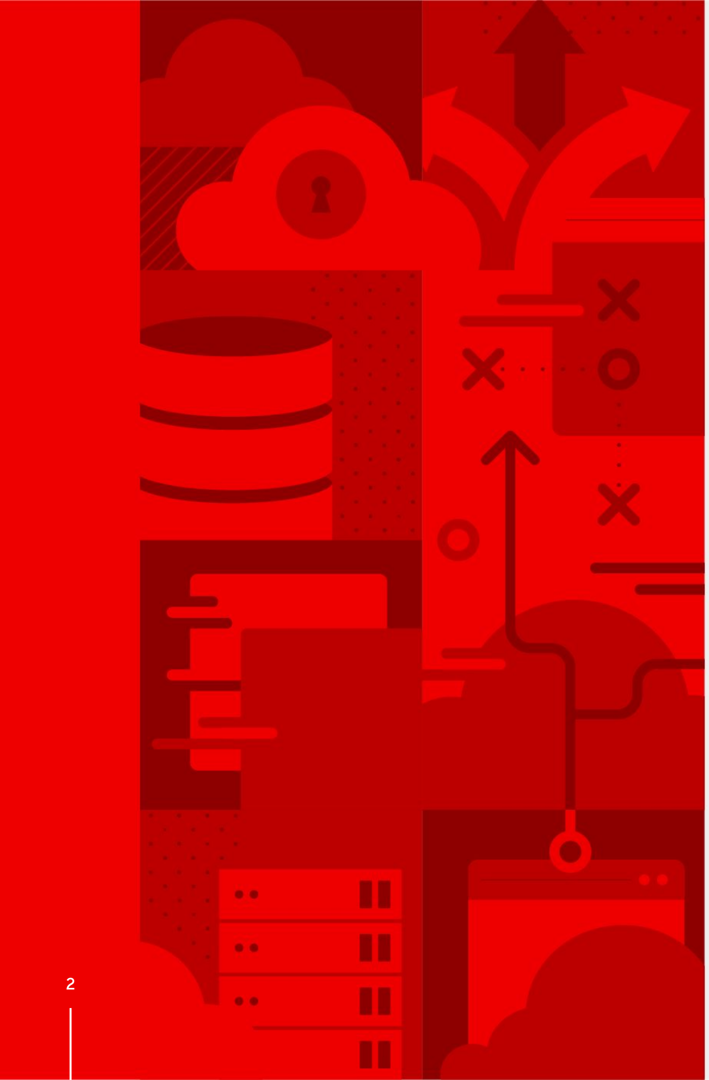
DevSecOps

Building capabilities for the warfighter at the speed of operations

Matt Hermanson
Cloud Solutions Architect
North American Public Sector



AGENDA

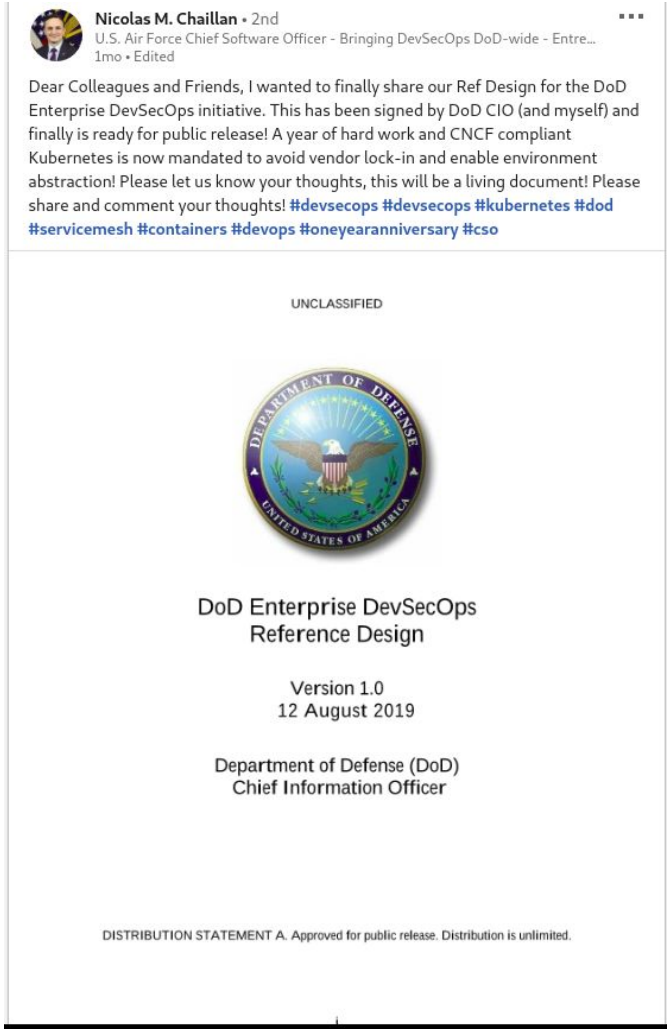
- ❑ DevSecOps
- ❑ Kubernetes - so what?

Understanding DevOps

DevOps is an approach to culture, automation, and platform design intended to deliver increased business value and responsiveness through rapid, high-quality service delivery. This is all made possible through fast-paced, iterative IT service delivery. DevOps means linking legacy apps with newer cloud-native apps and infrastructure.

Understanding DevSecOps

DevOps isn't just about development and operations teams. If you want to take full advantage of the agility and responsiveness of a DevOps approach, IT security must also play an integrated role in the full life cycle of your apps.



Nicolas M. Chaillan • 2nd
U.S. Air Force Chief Software Officer - Bringing DevSecOps DoD-wide - Entre...
1mo • Edited

Dear Colleagues and Friends, I wanted to finally share our Ref Design for the DoD Enterprise DevSecOps initiative. This has been signed by DoD CIO (and myself) and finally is ready for public release! A year of hard work and CNCF compliant Kubernetes is now mandated to avoid vendor lock-in and enable environment abstraction! Please let us know your thoughts, this will be a living document! Please share and comment your thoughts! #devsecops #devsecops #kubernetes #dod #servicemesh #containers #devops #oneyearanniversary #cso

UNCLASSIFIED

DoD Enterprise DevSecOps
Reference Design

Version 1.0
12 August 2019

Department of Defense (DoD)
Chief Information Officer

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.

“Legacy software acquisition and development practices in the DoD do not provide the agility to deploy new software “at the speed of operations”. In addition, security is often an afterthought, not built in from the beginning of the lifecycle of the application and underlying infrastructure. DevSecOps is the industry best practice for rapid, secure software development.” - DevSecOps Reference Design

State of DevOps Report
Key Findings

- **Open source software improves performance**
- Software delivery key competitive advantage
- Outsourcing by function is rarely adopted by elite performers and hurts performance
- How you implement cloud infrastructure matters
- **Key technical practices drive high performance -** *including "continuous testing… integrating security earlier"*
- **Industry not correlated to high performance**

Accelerate State of DevOps 2018
https://cloudplatformonline.com/2018-state-of-devops.html

State of DevOps Report
Key Findings

- Every organization is software-enabled
- Critical differentiators for software
  - Near zero marginal cost for delivery
  - Ability to rapidly iterate
- Software organizations that exploit those differentiators learn more quickly what makes them successful
- DevSecOps approaches **increase organizational success by enabling faster, safer experimentation and learning**

Accelerate State of DevOps 2018
https://cloudplatformonline.com/2018-state-of-devops.html

COMPARING THE ELITE GROUP AGAINST THE LOW PERFORMERS, WE FIND THAT ELITE PERFORMERS HAVE...

46 TIMES MORE
frequent code deployments

2,555 TIMES FASTER
lead time from commit to deploy

7 TIMES LOWER
change failure rate
(changes are 1/7 as likely to fail)

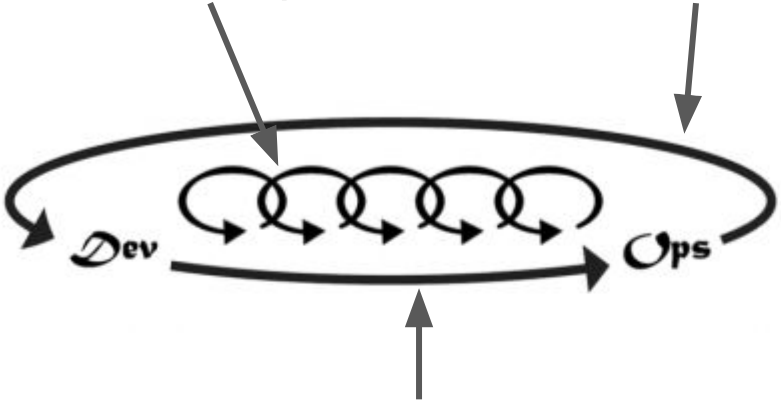
2,604 TIMES FASTER
time to recover from incidents

The Three Ways

1. “Systems thinking”
2. “Amplify feedback loops”
3. “Culture of continual experimentation and learning”

These are deliberately tech agnostic, though often tech-enabled

https://itrevolution.com/the-three-ways-principles-underpinning-devops/



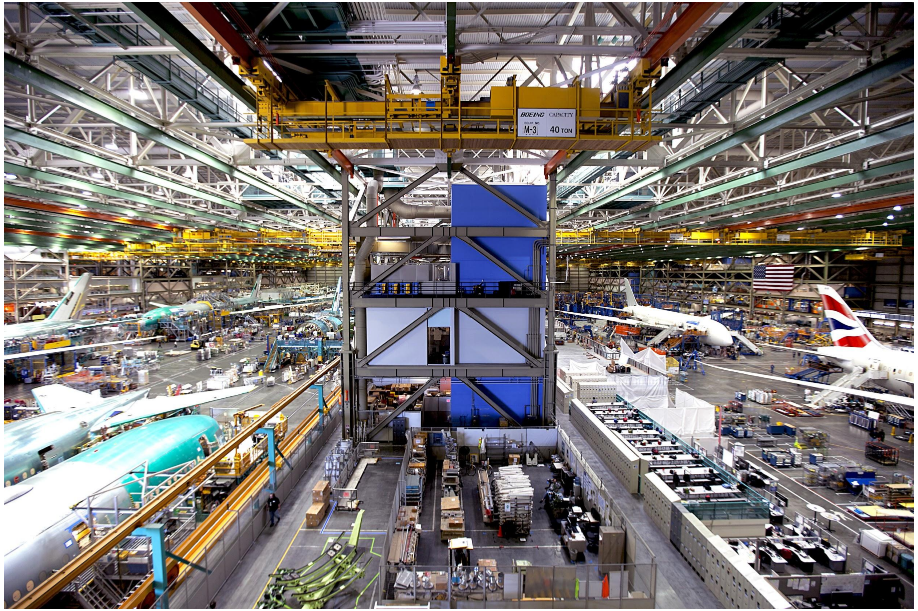
Third Way

Second Way

First Way

Securing the Development Process
DevSecOps

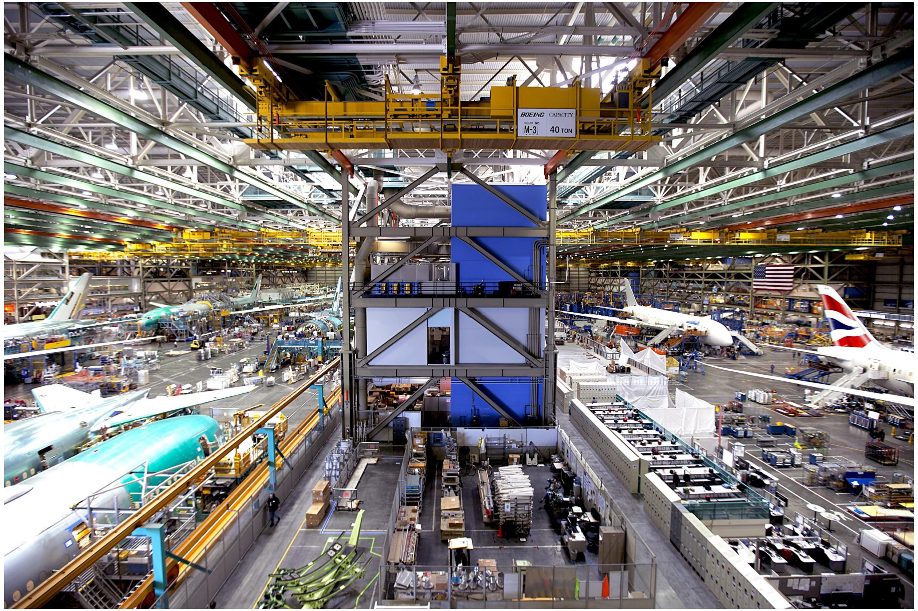
- Potentially lots of parallel builds
- Source code
  - Where is it coming from?
  - Who is it coming from?
- Supply Chain Tooling
  - CI tools (e.g. Jenkins)
  - Testing tools
  - Security Tools (e.g. Black Duck, Sonatype)



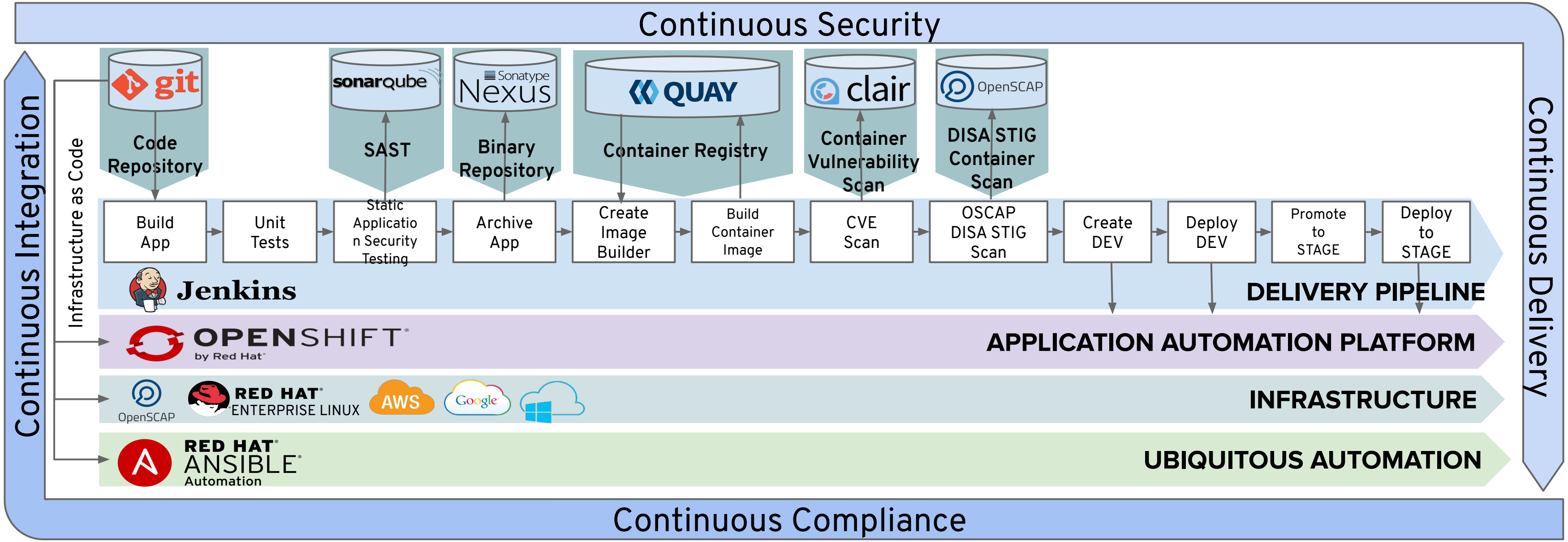
Boeing's Everett factory near Seattle
https://upload.wikimedia.org/wikipedia/commons/c/c8/At_Boeing%27s_Everett_factory_near_Seattle_%289130160595%29.jpg
Creative Commons

Some DevSecOps Specifics

- Developer self-service
- Smaller batch sizes
- Fast feedback
  - Logging
  - Monitoring
  - Telemetry
- **Shifting left on security**
  - Cross functional teams involved earlier in process
  - Some security features are auto-injected via a sidecar



Boeing's Everett factory near Seattle
https://upload.wikimedia.org/wikipedia/commons/c/c8/At_Boeing%27s_Everett_factory_near_Seattle_%289130160595%29.jpg
Creative Commons



- *Remove bottlenecks (including human ones) and manual actions.*
- *Automate as much of the development and deployment activities as possible.*
- *Adopt common tools from planning and requirements*

SECURE SOFTWARE FACTORY: KEY ENABLING TECHNOLOGIES

CONTAINERS

New paradigm unlocked by immutability, image layers, process isolation, portability

CONTAINER ORCHESTRATION

Operating containerized apps in production using a declarative configuration paradigm

CI/CD PIPELINE TOOLS/AUTOMATION

Build, package, and quality assurance processes codified and available on-demand

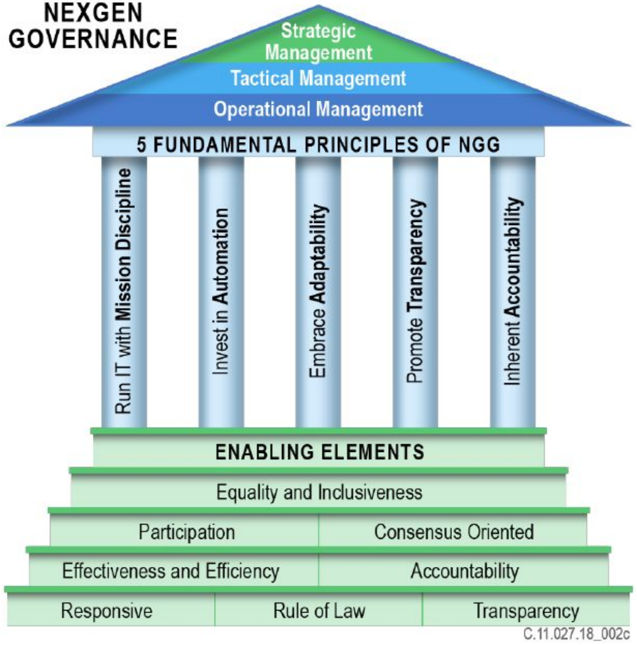
WHAT BEHAVIORS DOES THIS APPROACH PROMOTE?

- Small batch sizes
- Early, frequent testing (TDD)
- Ability to deliver changes quickly
- Supply chain assurance (BOM)

Need to scale to any operational requirement

- Business systems
- Command and Control systems
- Embedded and Weapon systems
- Intelligence analysis systems
- Autonomous systems
- Assisted human operations

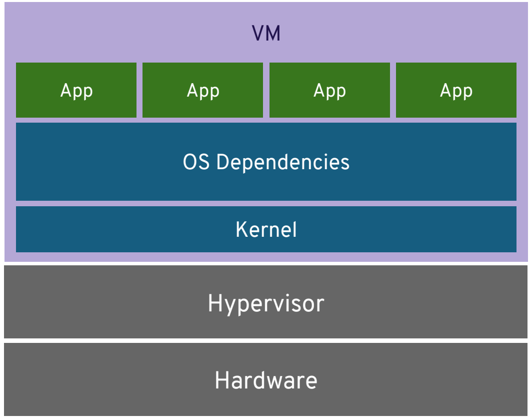
"DoD Instruction (DoDI) 8510.01 is under revision and the following DevSecOps related governance information will be incorporated in the future release."



Kubernetes

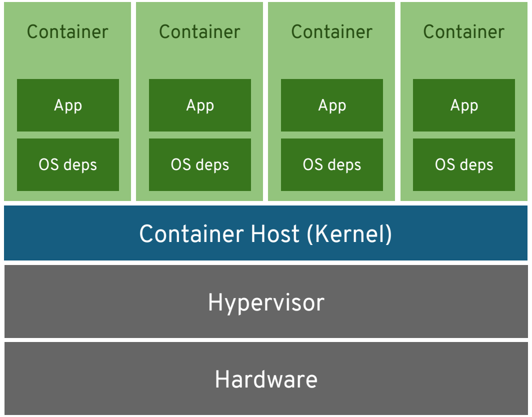
Virtual Machines and Containers

VIRTUAL MACHINES



VM isolates the hardware

CONTAINERS



Container isolates the process

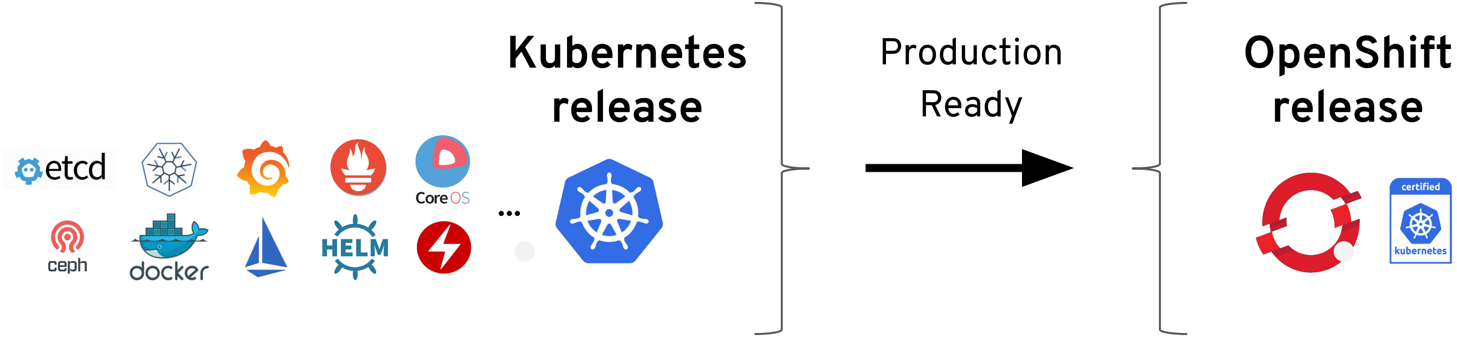
BEYOND CONTAINERS
“Kubernetes is the API of cloud”

- Robust scheduling
- Auto-scale
- Self-healing
- Stateless and Stateful
- Automated Deployments

By any objective measure, the industry has converged on Kubernetes as the container orchestration engine of choice

OPENSHIFT IS ENTERPRISE-READY

KUBERNETES

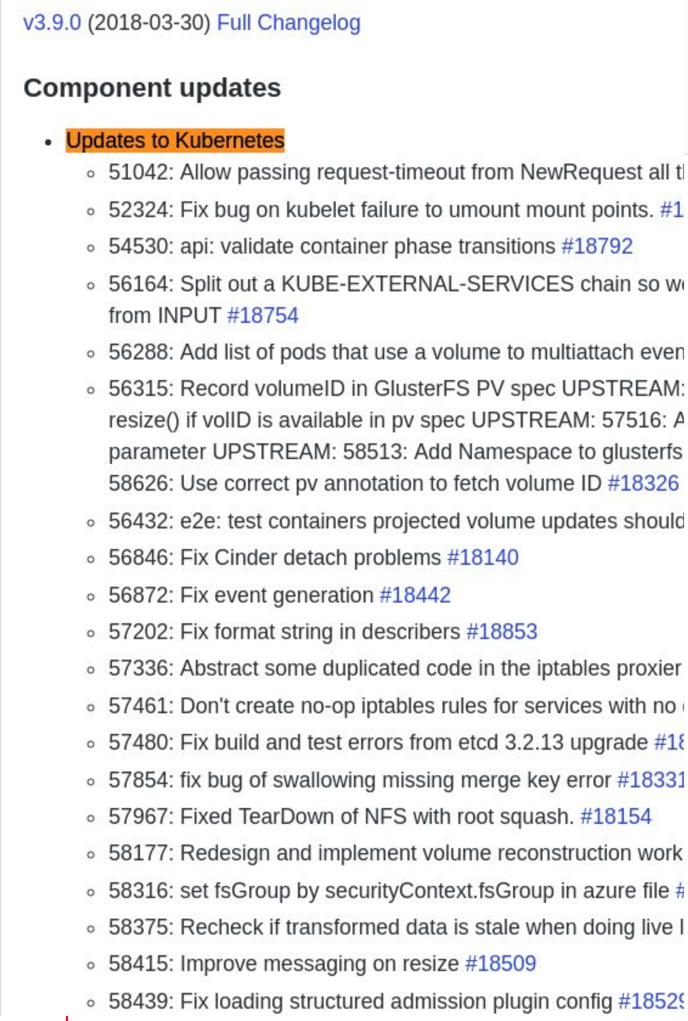


Kubernetes release

Production Ready

OpenShift release

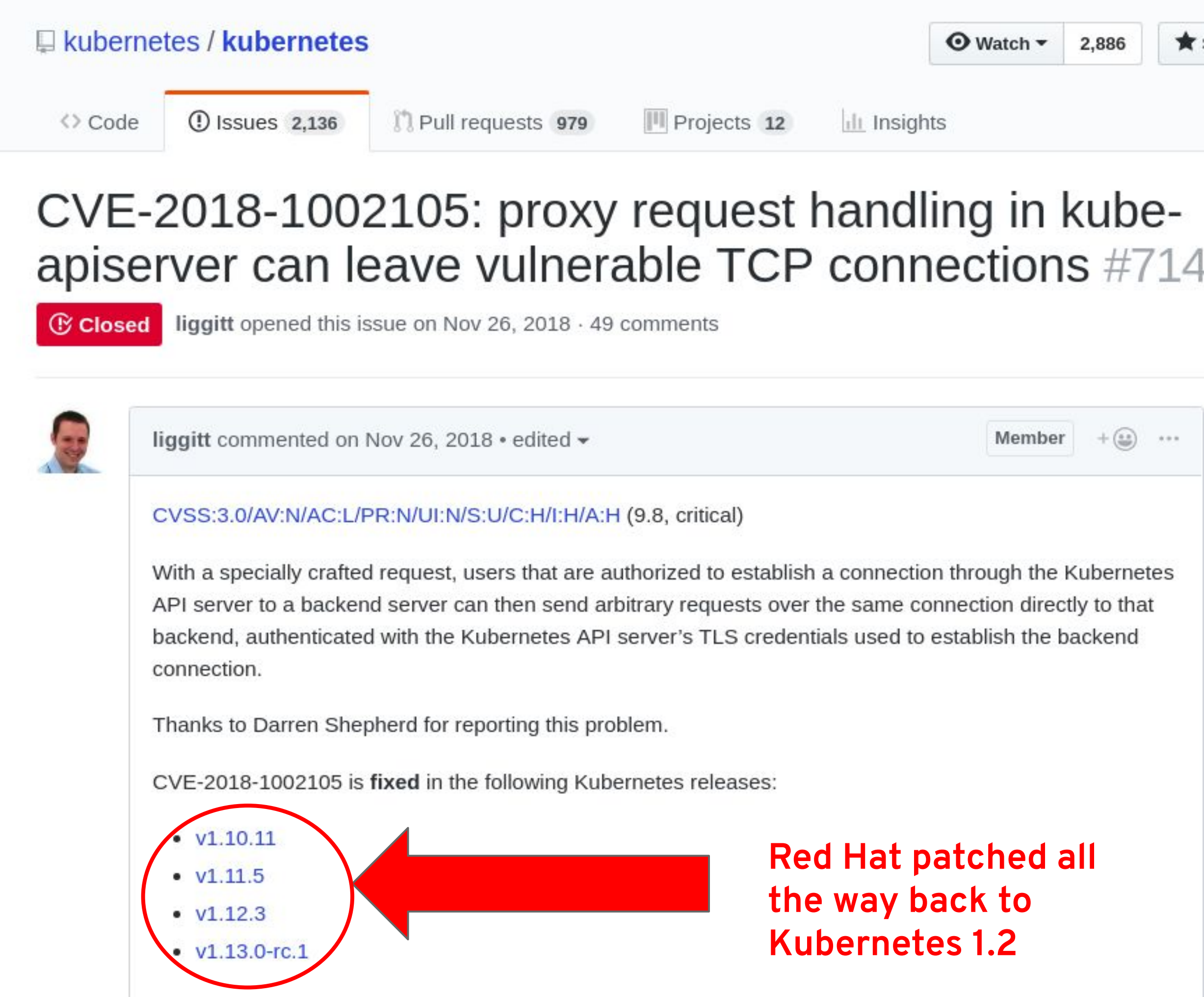
- Hundreds of defect and performance fixes
- 200+ validated integrations
- Certified container ecosystem
- 9-year enterprise life-cycle management
- Red Hat is a leading Kubernetes contributor since day 1



v3.9.0 (2018-03-30) Full Changelog

Component updates

- Updates to Kubernetes
  - 51042: Allow passing request-timeout from NewRequest all t
  - 52324: Fix bug on kubelet failure to umount mount points. #1
  - 54530: api: validate container phase transitions #18792
  - 56164: Split out a KUBE-EXTERNAL-SERVICES chain so w from INPUT #18754
  - 56288: Add list of pods that use a volume to multiattach even
  - 56315: Record volumeID in GlusterFS PV spec UPSTREAM: resize() if volID is available in pv spec UPSTREAM: 57516: A parameter UPSTREAM: 58513: Add Namespace to glusterfs 58626: Use correct pv annotation to fetch volume ID #18326
  - 56432: e2e: test containers projected volume updates should
  - 56846: Fix Cinder detach problems #18140
  - 56872: Fix event generation #18442
  - 57202: Fix format string in describers #18853
  - 57336: Abstract some duplicated code in the iptables proxier
  - 57461: Don't create no-op iptables rules for services with no
  - 57480: Fix build and test errors from etcd 3.2.13 upgrade #18
  - 57854: fix bug of swallowing missing merge key error #18331
  - 57967: Fixed TearDown of NFS with root squash. #18154
  - 58177: Redesign and implement volume reconstruction work
  - 58316: set fsGroup by securityContext.fsGroup in azure file #
  - 58375: Recheck if transformed data is stale when doing live l
  - 58415: Improve messaging on resize #18509
  - 58439: Fix loading structured admission plugin config #1852



CVE-2018-1002105: proxy request handling in kube-apiserver can leave vulnerable TCP connections #714

liggitt opened this issue on Nov 26, 2018 · 49 comments

liggitt commented on Nov 26, 2018 • edited

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H (9.8, critical)

With a specially crafted request, users that are authorized to establish a connection through the Kubernetes API server to a backend server can then send arbitrary requests over the same connection directly to that backend, authenticated with the Kubernetes API server's TLS credentials used to establish the backend connection.

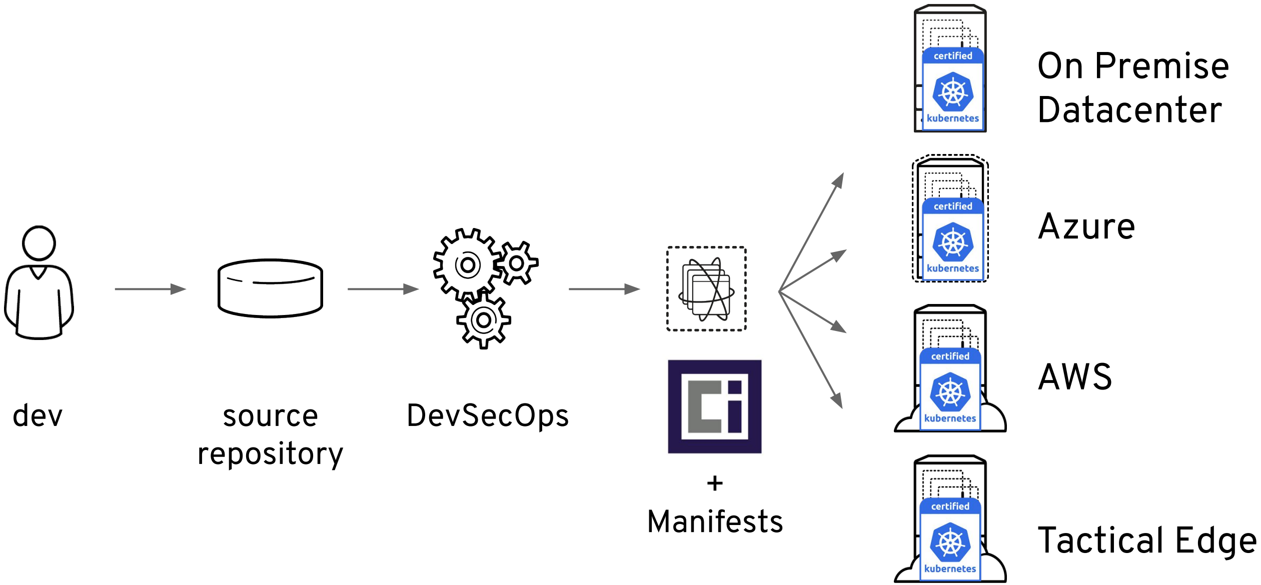
Thanks to Darren Shepherd for reporting this problem.

CVE-2018-1002105 is **fixed** in the following Kubernetes releases:

- v1.10.11
- v1.11.5
- v1.12.3
- v1.13.0-rc.1

Red Hat patched all the way back to Kubernetes 1.2

Federating Apps Between Clouds with Open Standards



dev

source repository

DevSecOps

+ Manifests

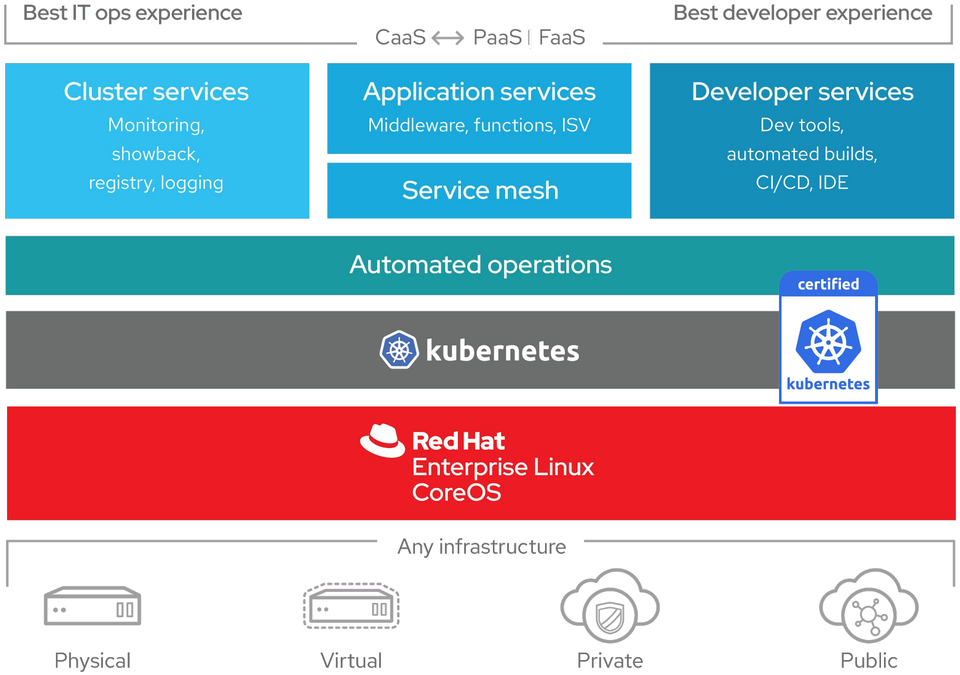
On Premise Datacenter

Azure

AWS

Tactical Edge

OpenShift 4 - A smarter Kubernetes platform



Automated, full-stack installation

Seamless Kubernetes deployment to any infra

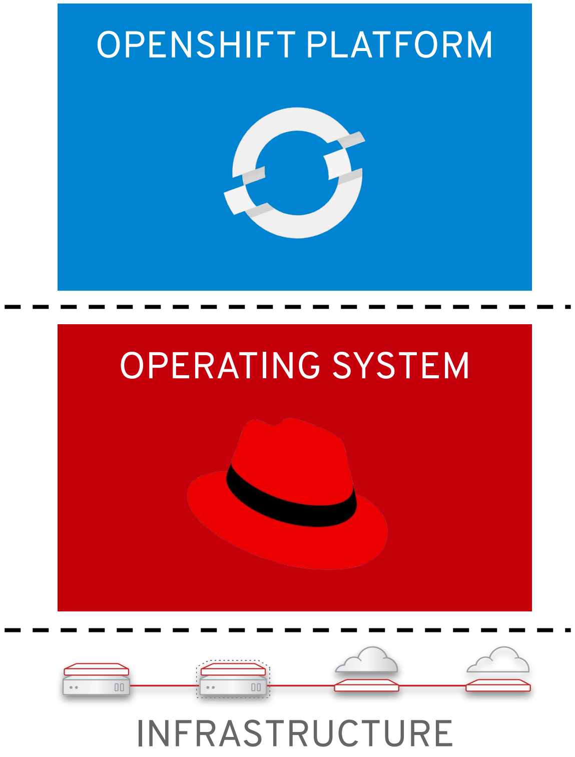
Autoscaling of cloud resources

One-click updates for platform, services, and applications

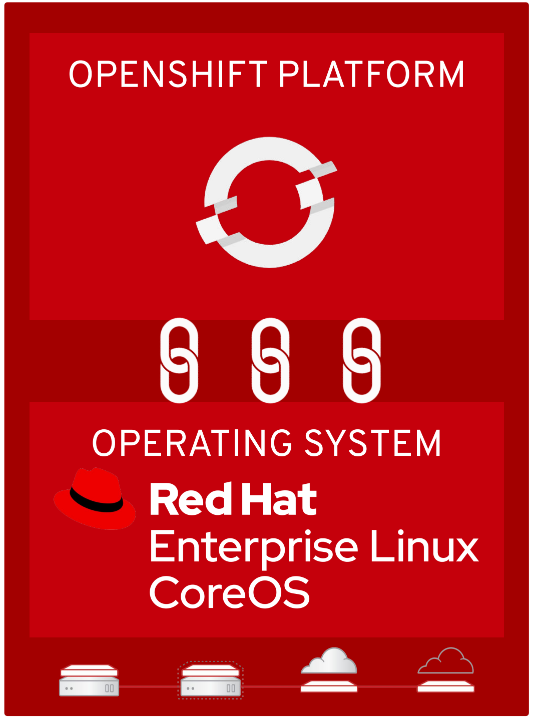
“Deploying immutable infrastructure requires standardization and emulation of common infrastructure components to achieve consistent and predictable results.” - DevSecOps Reference Design

Full-stack automated install

OPENSHIFT 3 & 4

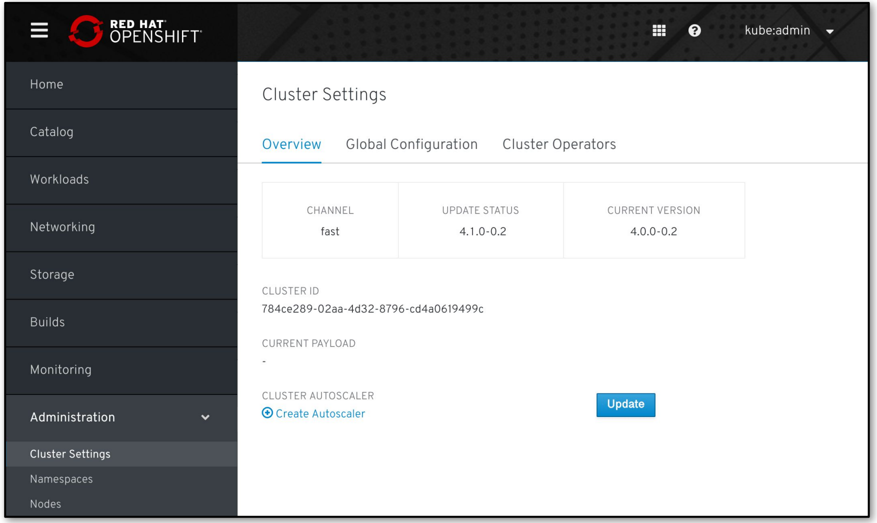


OPENSHIFT 4 (only)



Over the Air (OTA) Updates

- OpenShift retrieves the list of available updates
- Admin selects the target version
- OpenShift is updated over the air
- Auto-update support



Cluster Settings

CHANNEL	UPDATE STATUS	CURRENT VERSION
fast	4.1.0-0.2	4.0.0-0.2

CLUSTER ID
784ce289-02aa-4d32-8796-cd4a0619499c

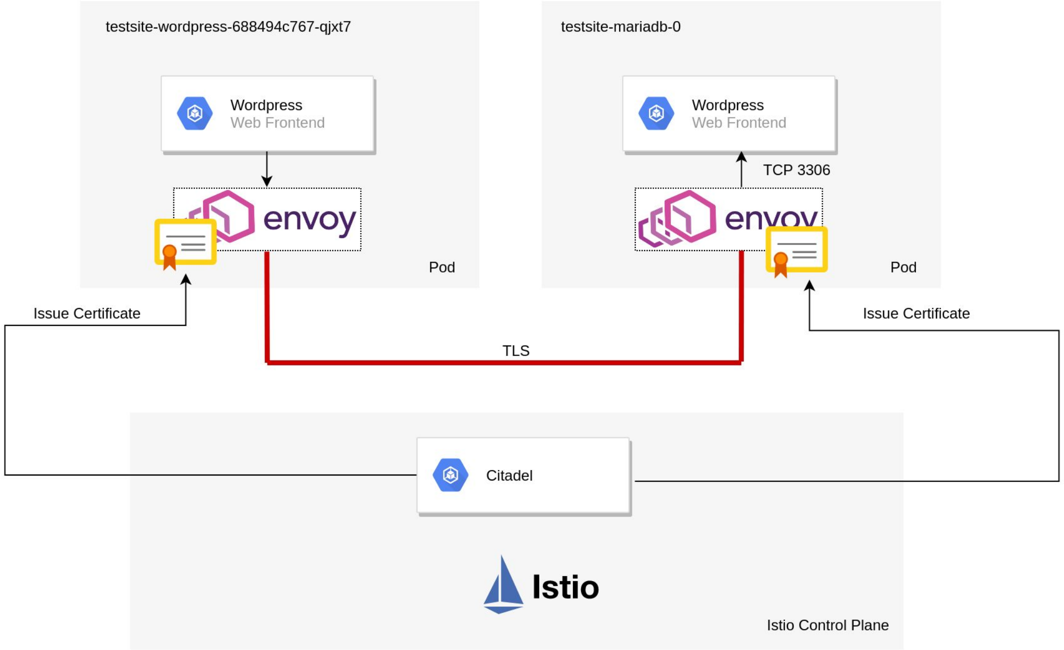
CURRENT PAYLOAD
-

CLUSTER AUTOSCALER

Declarative Security

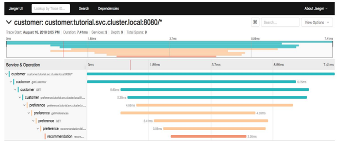
DevSecOps Reference Design requirements for a sidecar

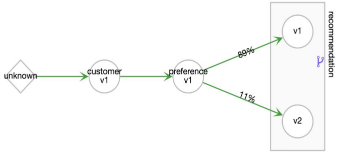
- A logging agent
- Container policy enforcement
  - Preserve DCAR content
  - NIST 800-190 compliance
- Runtime Defense
  - Behavior anomaly detection
  - Signature-based detection
  - Alerting
- Zero Trust (mTLS)
  - Two-way TLS
  - Strong identities
  - MAC / whitelist

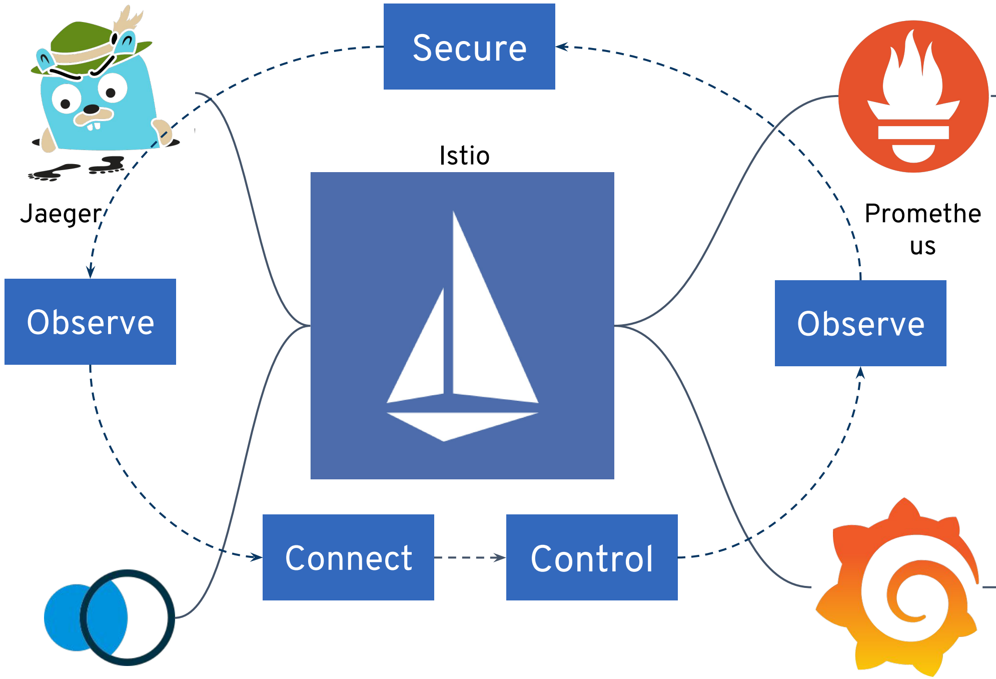


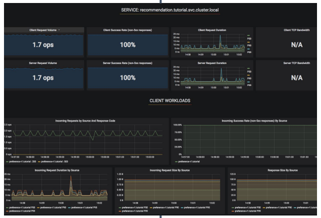
Red Hat

OpenShift Service Mesh


Jaeger UI
Lookup by Trace ID...
Search
Dependencies
About Jaeger
customer: customer.tutorial.svc.cluster.local:8080/*
Search...
View Options
Trace Start: August 16, 2018 3:05 PM
Duration: 7.41ms
Services: 3
Depth: 9
Total Spans: 9
0ms
1.85ms
3.7ms
5.56ms
7.41ms
Service & Operation
customer customer.tutorial.svc.cluster.local:8080/*
customer getCustomer
customer GET
customer preference.tutorial.svc.cluster.local:8...
preference preference.tutorial.svc.cluster.lo...
preference getPreferences
preference GET
preference recommendation:80...
recommendation recom...
6.25ms
5.63ms
5.39ms
4.68ms
4.03ms
3.41ms
3.06ms
2.26ms






SERVICE: recommendation.tutorial.svc.cluster.local
Client Request Volume
1.7 ops
Client Success Rate (non-5xx responses)
100%
Client Request Duration
Client TCP Bandwidth
N/A
Server Request Volume
1.7 ops
Server Success Rate (non-5xx responses)
100%
Server Request Duration
Server TCP Bandwidth
N/A
CLIENT WORKLOADS
Incoming Requests by Source And Response Code
Incoming Success Rate (non-5xx responses) By Source
Incoming Request Duration by Source
Incoming Request Size By Source
Response Size By Source

“One advantage of using the SCSS is that Kubernetes can inject the sidecar automatically”

- DevSecOps Reference Design

No Lock-In Serverless

DevSecOps Reference Design Requirements for Serverless:

- Uses CNCF k8s
- Auto-scale up
- Auto-scale down to 0
- Gradual rollouts
- Network routing

Serving

An event-driven model that serves the container with your application and can "scale to zero".

Eventing

Common infrastructure for consuming and producing events that will stimulate applications.

Thank you

Red Hat is the world's leading provider of

enterprise open source software solutions.

Award-winning support, training, and consulting

services make

Red Hat a trusted adviser to the Fortune 500.

- linkedin.com/company/red-hat
- youtube.com/user/RedHatVideos
- facebook.com/redhatinc
- twitter.com/RedHat