IThome Kubernetes Summit x Taiwan

Red Hat 企業級 Kubernetes OpenShift容器平台

彭信忠(Jason Peng)
資深解決方案架構師
紅帽軟體 - 東南亞暨港台
2018/06/14

Kubernetes 是一個開源技術，專注於容器化應用在分散式架構下，跨機器間的部署自動化、管理操作、與擴展

kubernetes

KUBERNETES：容器調度技術的業界標準

https://kubernetes.io/partners/

紅帽 x Kubernetes

全球最大企業級開源IT技術與解決方案供應商

MORE THAN
90%
of the
FORTUNE 500
use
RED HAT
PRODUCTS & SOLUTIONS*

~11,900
EMPLOYEES

S&P
500
COMPANY

95
OFFICES

35
COUNTRIES

NYSE
RHT

THE FIRST
$3 BILLION
OPEN SOURCE COMPANY
IN THE WORLD

*Red Hat client data and Fortune 500 list, August 2017

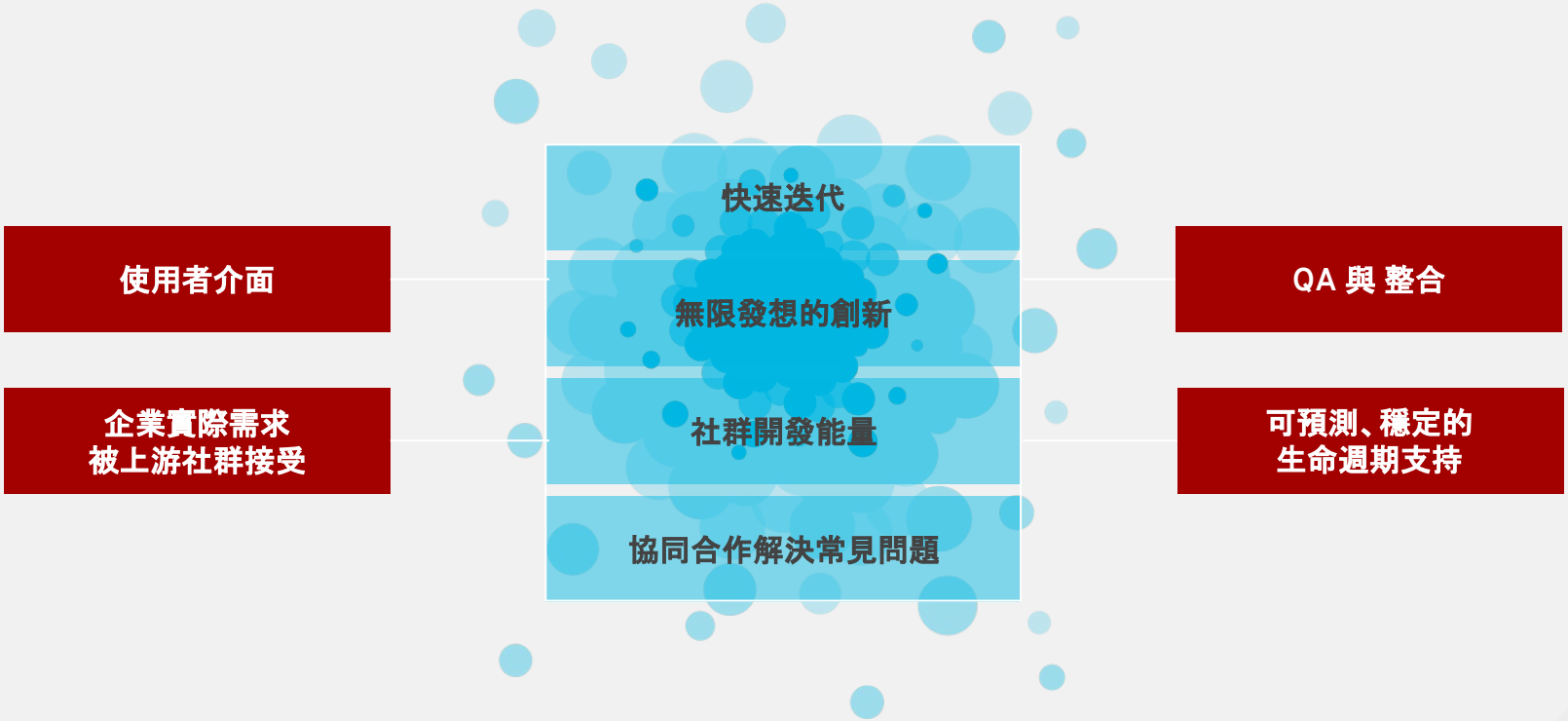
“Red Hat is an enterprise-class software company with an open source development model”

by President and CEO Jim Whitehurst

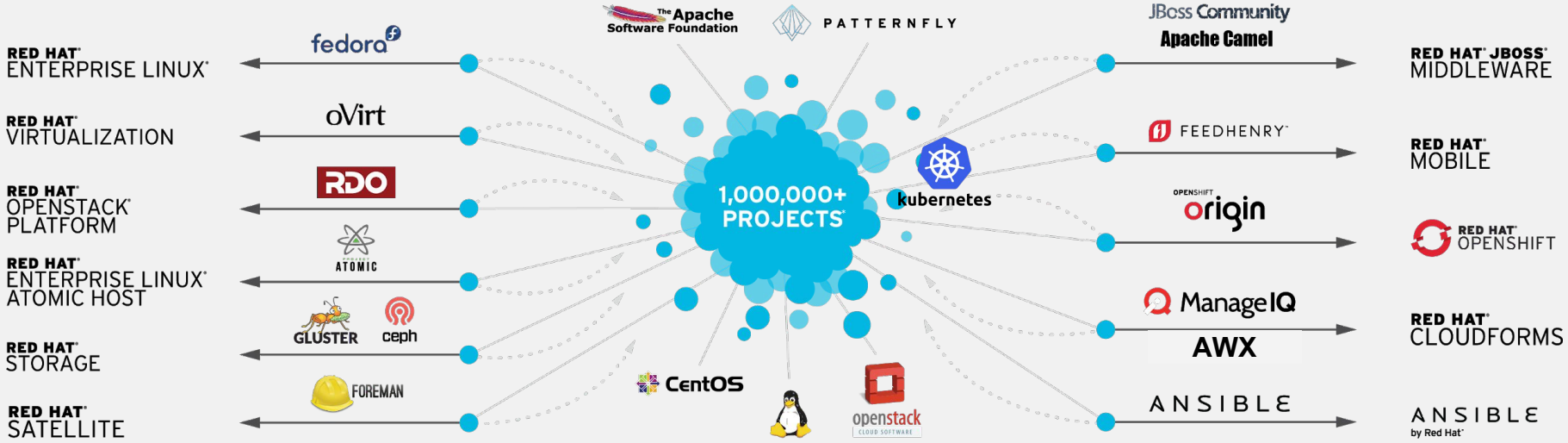
“紅帽是一間企業級軟體供應商採用全開源模式進行產品研發”

by 我老闆 Jim

企業所需要的開源方案


使用者介面
企業實際需求
被上游社群接受
快速迭代
無限發想的創新
社群開發能量
協同合作解決常見問題
QA 與 整合
可預測、穩定的
生命週期支持

從社群創新到企業解決方案



***只要是紅帽產品用到的重點技術，都有紅帽頂尖開發人員參與其中一同發展。**

參與社群

We participate in and create community-powered upstream projects.

整合與創建社群

We integrate upstream projects, fostering open community platforms.

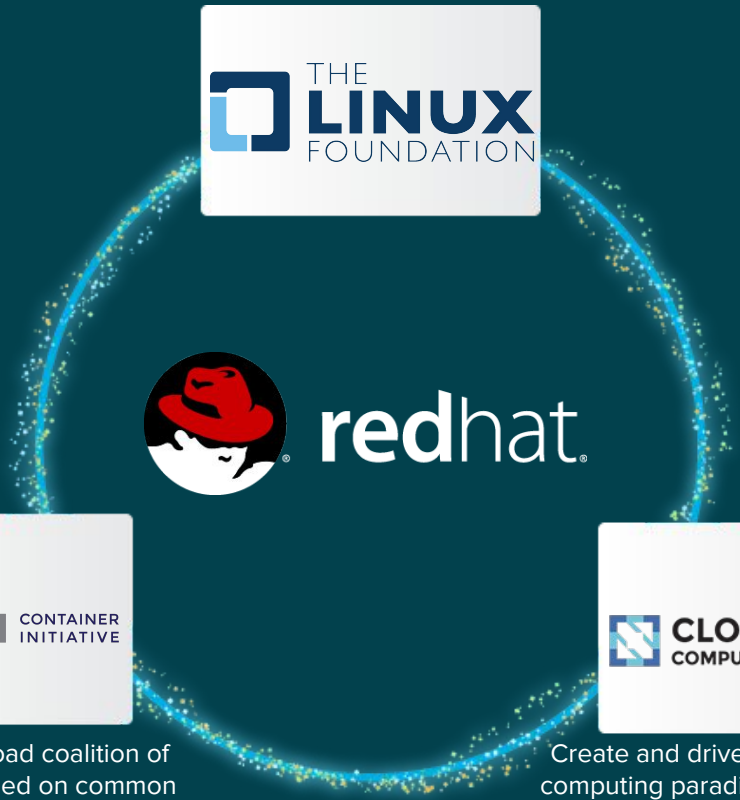
穩定產品

We commercialize these platforms together with a rich ecosystem of services and certifications.

RH0064-3

redhat.

紅帽於容器技術生態圈

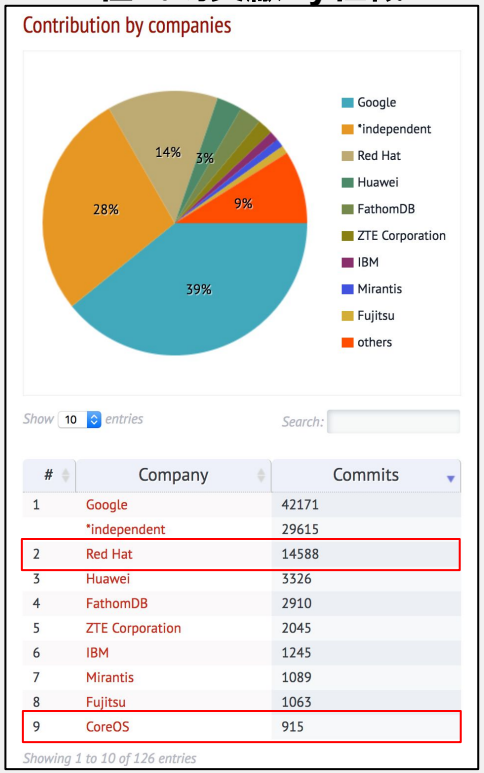


Represented by a broad coalition of industry leaders focused on common standards for software containers

Create and drive the adoption of a new computing paradigm that is optimized for modern distributed systems

紅帽於容器技術生態圈

No.2 程式碼貢獻by組織

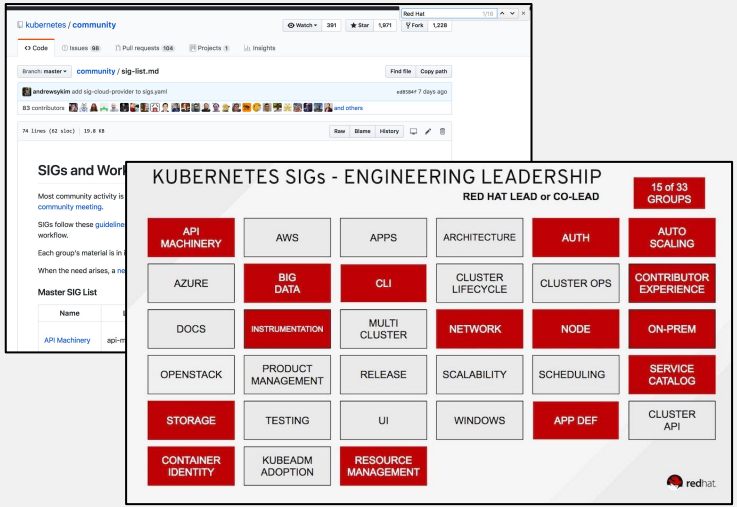


#	Company	Commits
1	Google	42171
	*independent	29615
2	Red Hat	14588
3	Huawei	3326
4	FathomDB	2910
5	ZTE Corporation	2045
6	IBM	1245
7	Mirantis	1089
8	Fujitsu	1063
9	CoreOS	915

Showing 1 to 10 of 126 entries

Source(6/8/2018):
http://stackalytics.com/?project_type=kubernetes-group&release=all&metric=commits

K8S Special Interest Group Lead：
SIG: 12+1/31
Working SIG: 3+1/10



K8s SIG(6/8/2018):
https://github.com/kubernetes/community/blob/master/sig-list.md

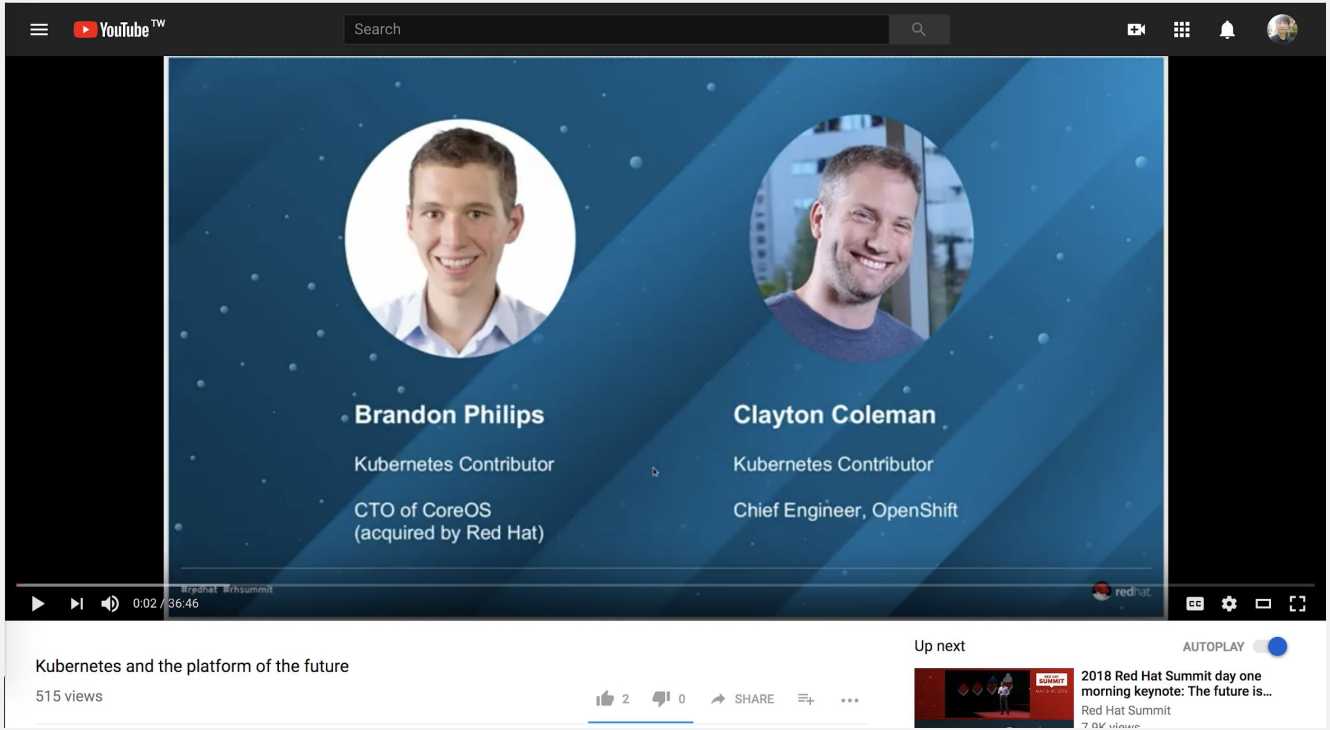
重點SIG

- Network
- Node (cri-o,rkt)
- Instrumentation (metrics, logging, and events)
- Testing
- Auth

Working SIG：

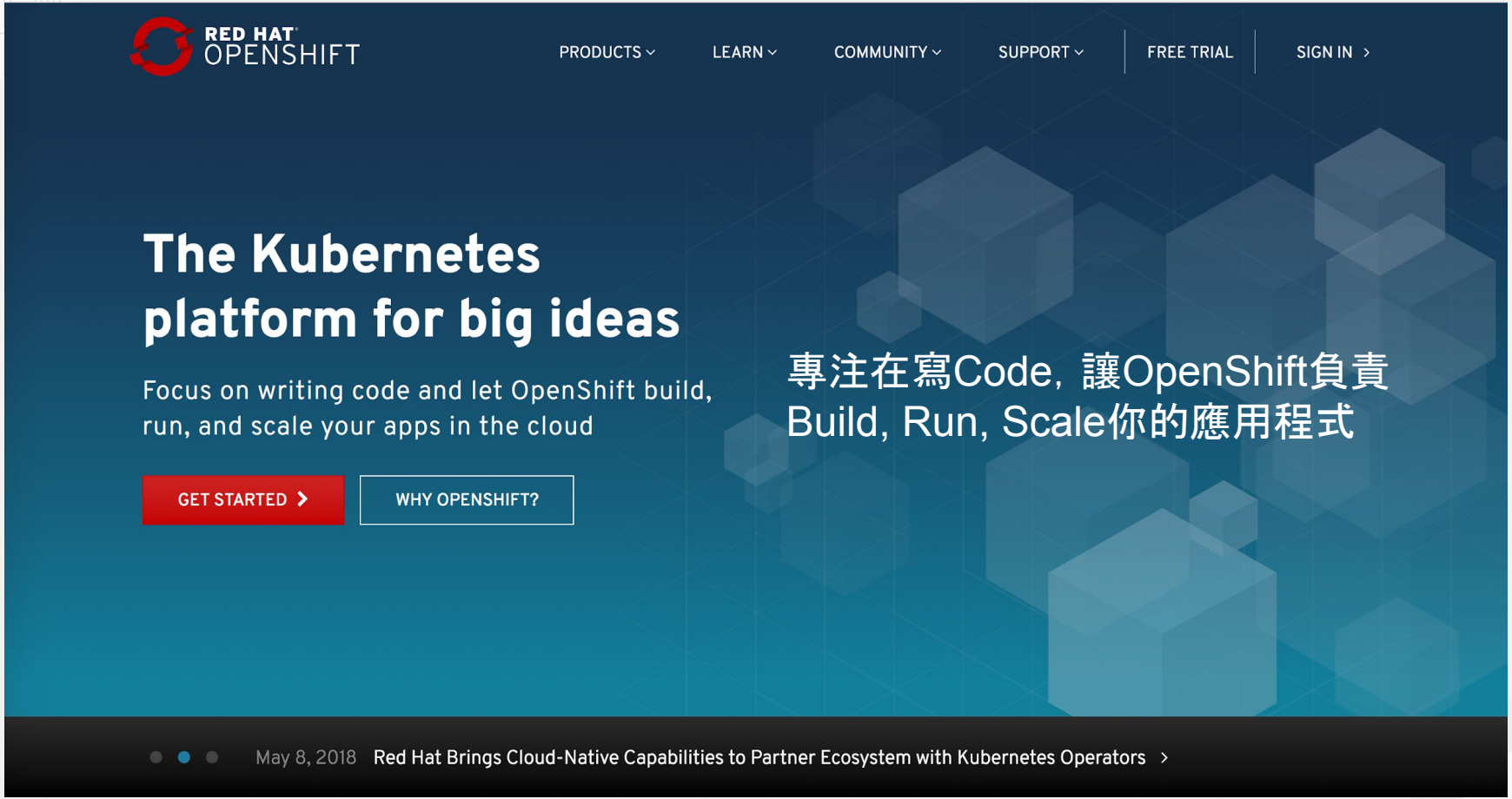
- Security relate (Identity, Policy)
- Resource Mgmt.

紅帽與Kubernetes的那點小歷史



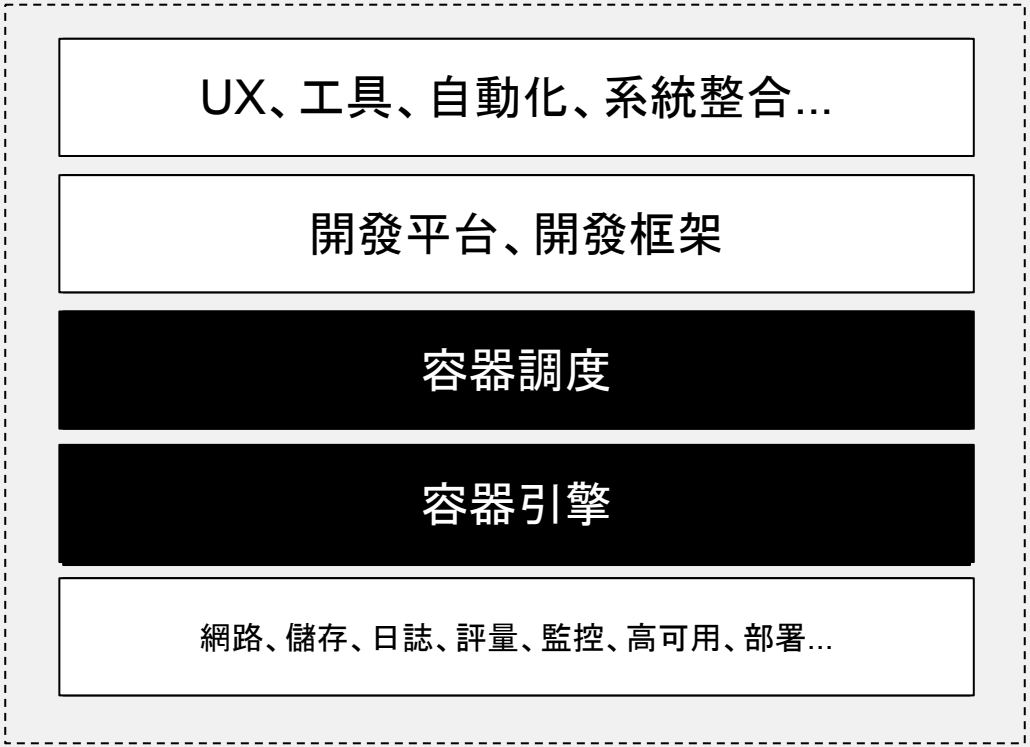
https://www.youtube.com/watch?v=YAFKlOB8vBw&feature=share

OpenShift x Kubernetes

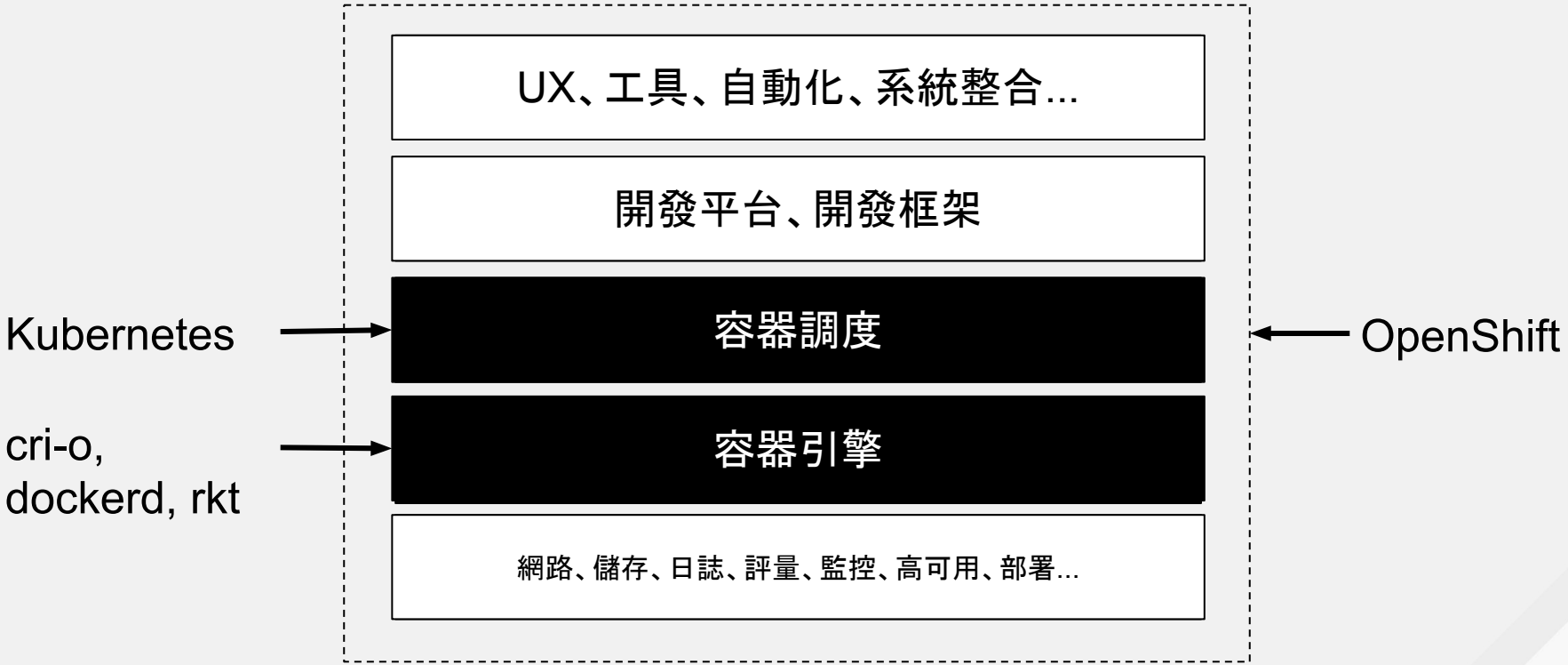


https://www.openshift.com/

企業組織所需要的容器技術



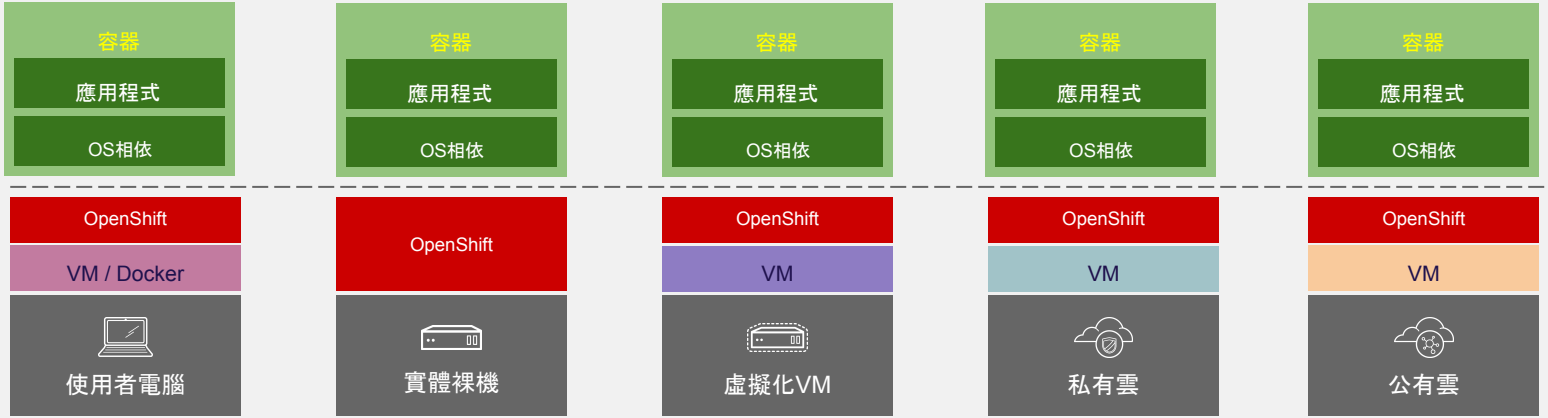
OpenShift = 企業級容器平台



有誰不想要自由？

不受限的應用程式運行環境

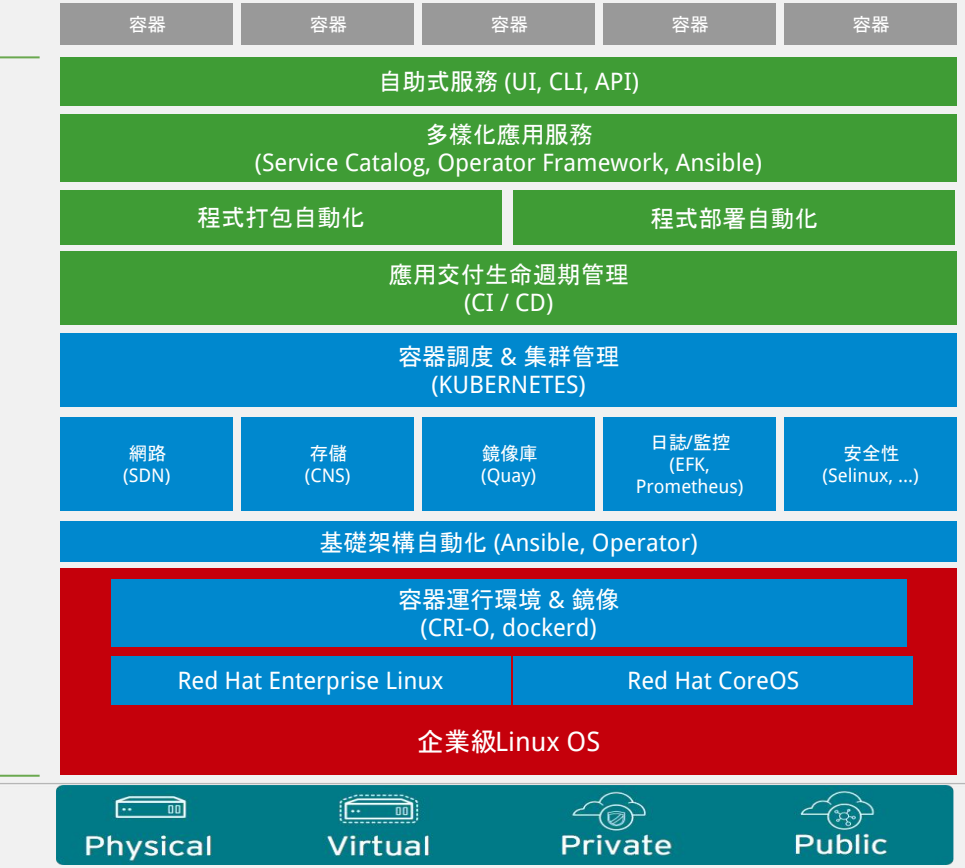
容器 + OpenShift =
確保 應用程式 跨 基礎環境 的能力



為Dev/Test與Ops打造的自動化平台

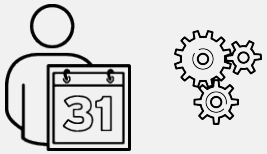
Security保護結合在平台各環節

RED HAT® OPENSHIFT



快速、多樣化
創新

可靠、安全、自動化
基礎架構



redhat.

社群驅動創新

自建

Red Hat代管

Red Hat公有雲

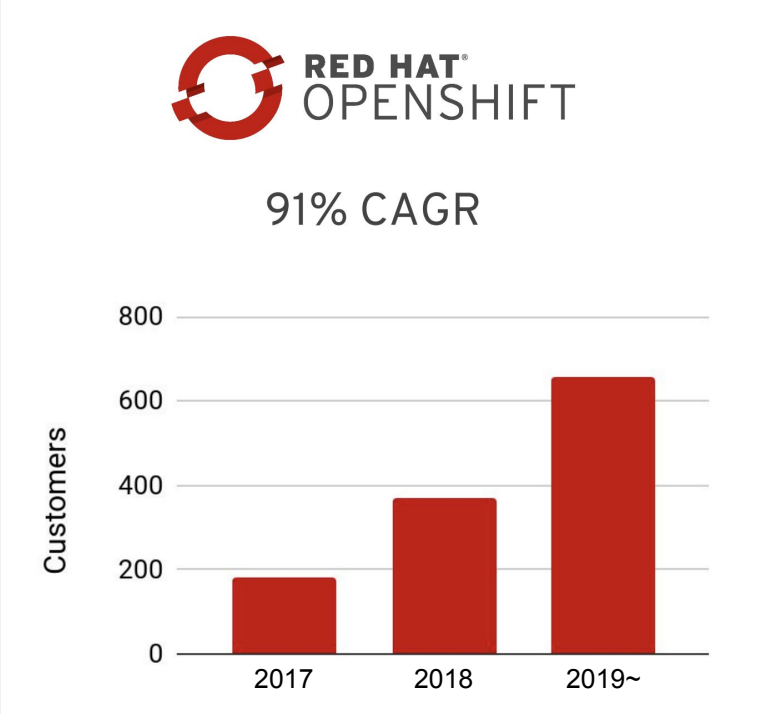
RED HAT® OPENSHIFT CONTAINER PLATFORM

RED HAT® OPENSHIFT DEDICATED

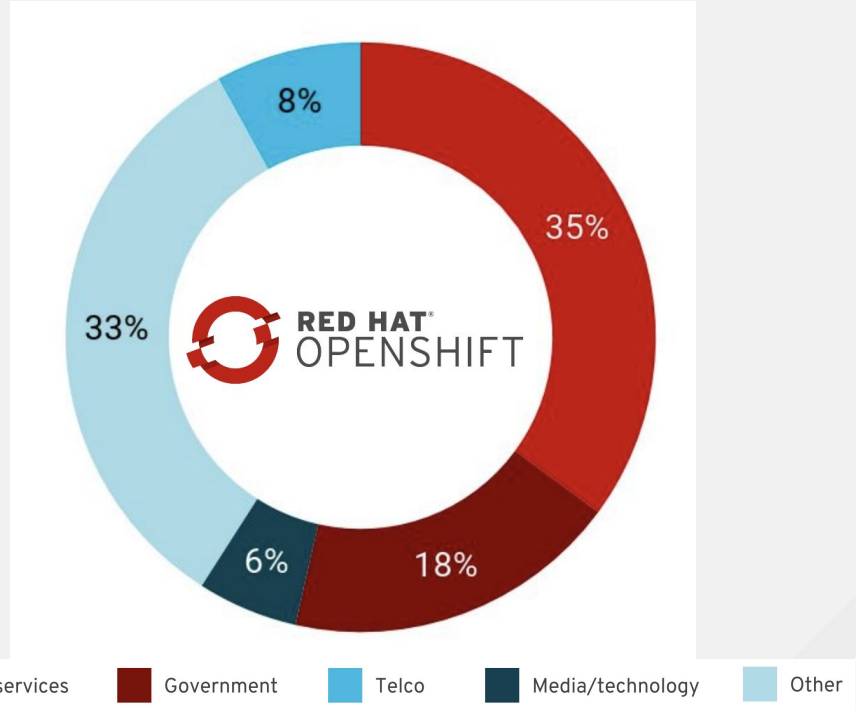
RED HAT® OPENSHIFT Online

redhat

企業採用OpenShift



紅帽OpenShift客戶已超過650+



OpenShift的需求，擴及各行各業

redhat.

RED HAT® OPENSHIFT

Ideas Worth Exploring

MONDAY

- Amadeus
- Barclays
- DHL
- Cisco
- Florida Blue
- Nordea
- Intesa San Paolo
- Clydesdale Bank
- Santander
- BNZ
- Elsevier
- Daimler AG
- Capgemini
- Paychex
- Elisa
- Eficode
- BMO Financial Group
- UPS
- Syngenta
- Lufthansa Technik
- SIX Group
- Vorwerk
- ACI Worldwide
- SOS International

TUESDAY

- Amadeus
- Citi
- IBM
- Cathay Pacific
- Deutsche Bank
- BP
- Experian
- BMW
- Bell Canada
- Swiss Federal Railways
- Microsoft
- Google
- Amazon
- nearForm

WEDNESDAY

- Lufthansa Technik
- UPS
- BBVA
- Social Security Administration
- ELO Cartões
- Bandwidth
- FEMA
- SIA
- BZ WBK / Santander Bank
- US Air Force & Mitre
- Google
- NuoDB
- USAA
- Sabre
- University of North Carolina at Chapel Hill

THURSDAY

- Hilton
- Hitachi
- Google
- Kohl's
- CSX
- Boston Children's Hospital
- Vorwerk
- InComm
- Experian Health
- County of Los Angeles
- La Poste
- Lenovo
- Amazon
- F5 Networks
- BBVA

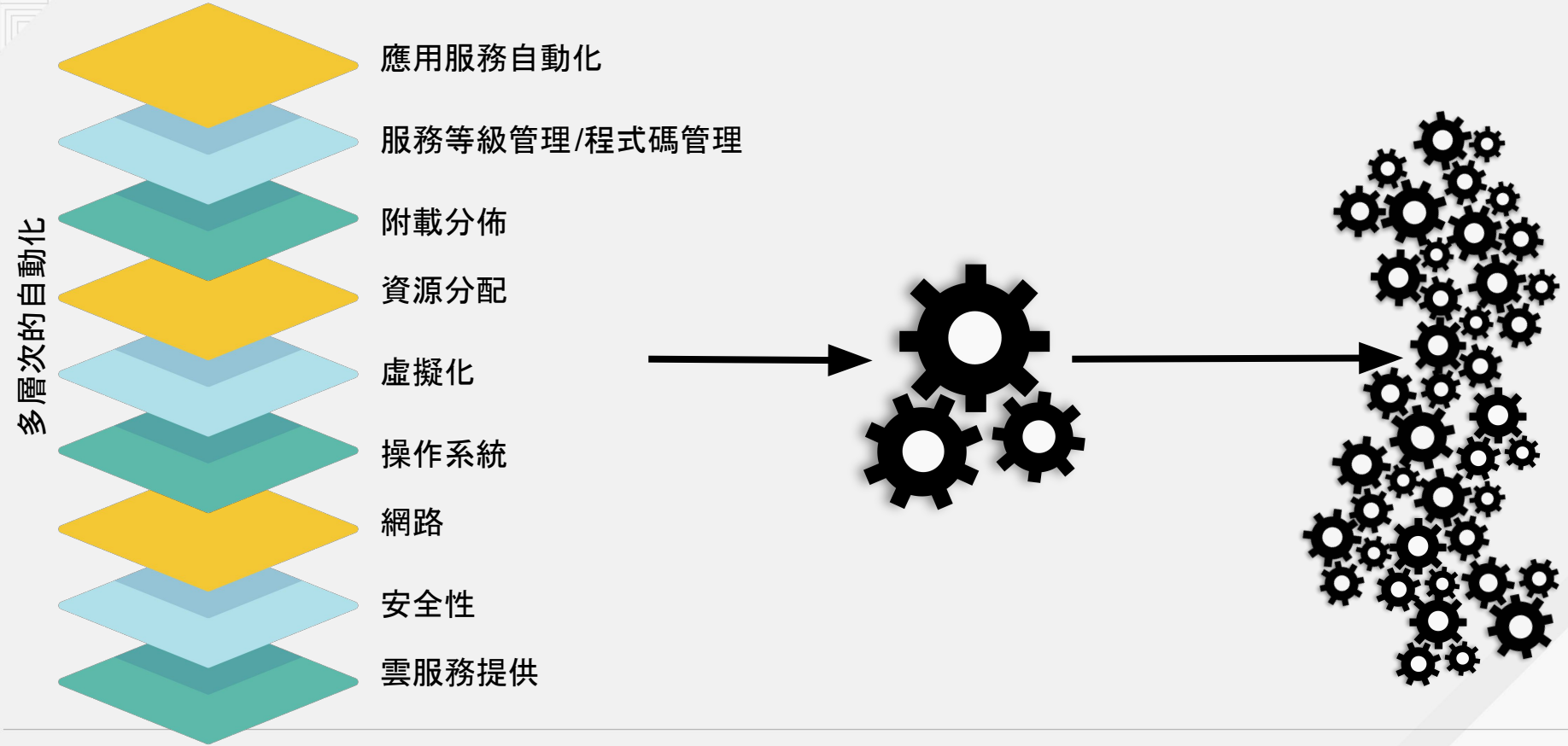
分享全在 :https://www.youtube.com/user/redhatsummit

OpenShift Integrated Solutions & Services

- Accenture
- AVI Networks
- Amazon
- Big Switch Networks
- Black Duck Software
- Cisco
- CloudBees
- VMware NSX
- CyberArk
- Diamanti
- DXC Technology
- Dynatrace
- F5 Networks
- Google
- HPE
- InfluxDB
- Juniper Networks
- Lenovo
- LINBIT
- Microsoft
- NEC
- NetApp
- Neuvector
- NGINX
- Rackspace
- SAP
- Sonatype
- Splunk
- StorageOS
- Sysdig
- T-Systems
- Tata Consultancy Services
- CollabNet
- CoScale
- Couchbase
- Instana
- Intel
- JFrog
- Nuage Networks
- NuoDB
- Arista Networks
- Univa
- Twistlock
- Tigera
- Vizuri
- Thales Security
- Portworx
- Tremolo Security

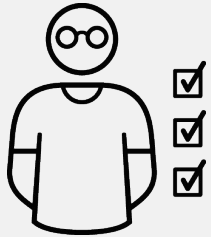
OpenShift x Future

重定義自動化的邊界



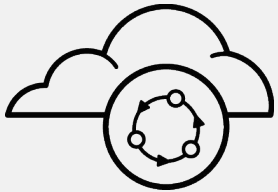
Day 0 - Day 1 - Day2

- Day 1 - 提升租戶效率
  - 使用者/開發者體驗



- Day 2 - 提升運維效率
  - SRE體驗

- Day 0 - 提升平台效率
  - 提升平台建置速度與降低難度
  - 智能自動化

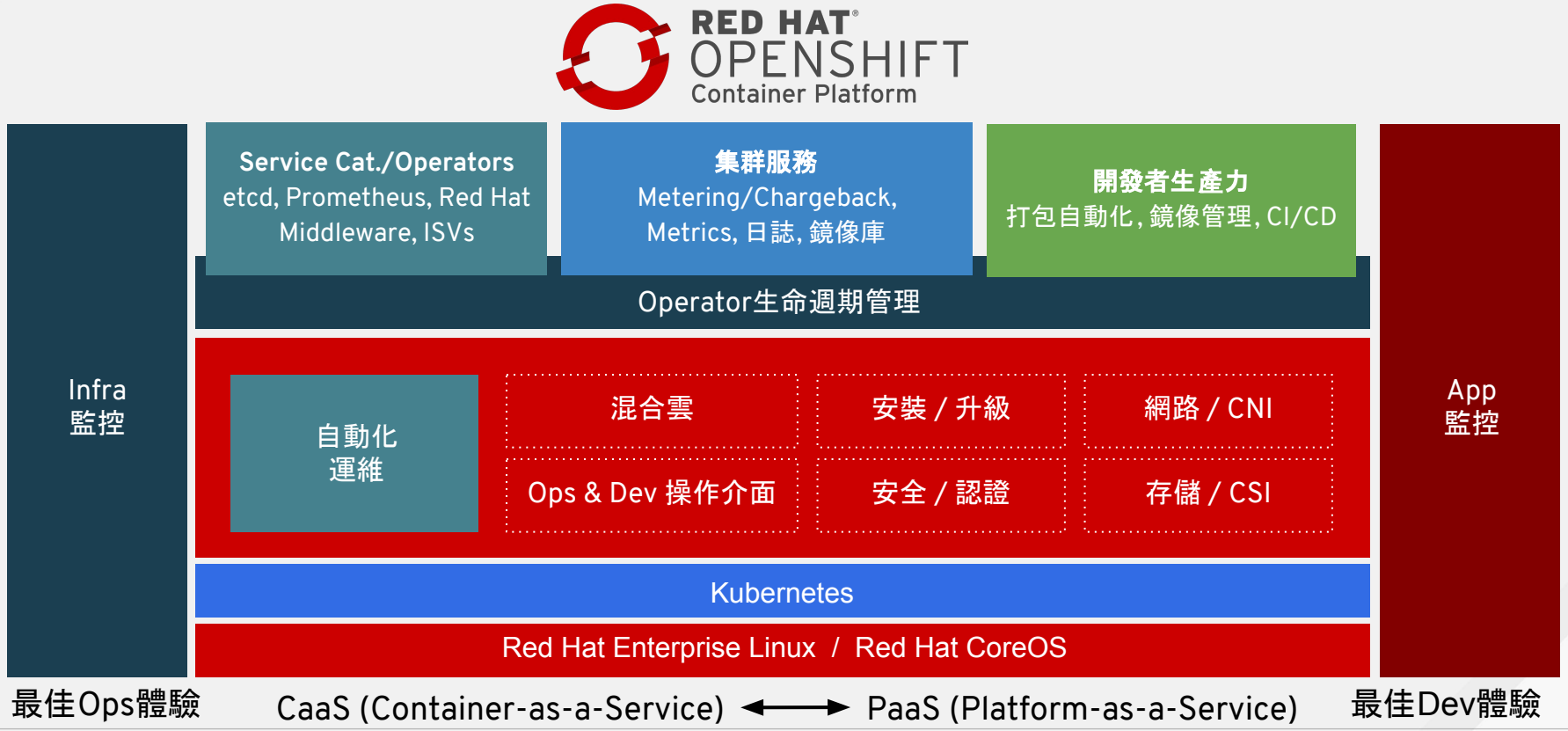


OpenShift + CoreOS 整合

產品融合 & 發展

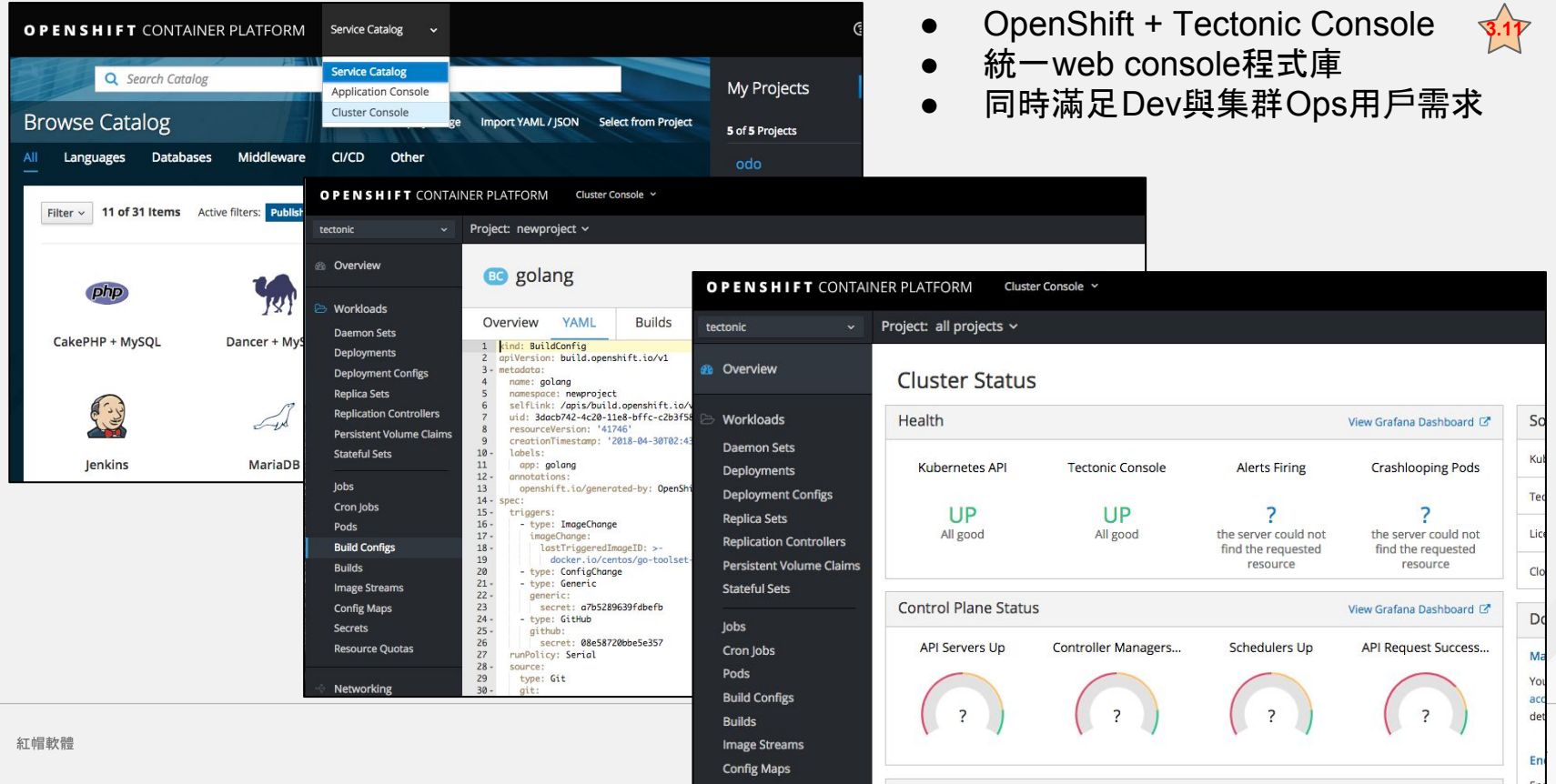
紅帽OpenShift發展第一手資訊 - Red Hat Summit - https://www.youtube.com/watch?v=1AelNjx6BB4

OpenShift + CoreOS 整合



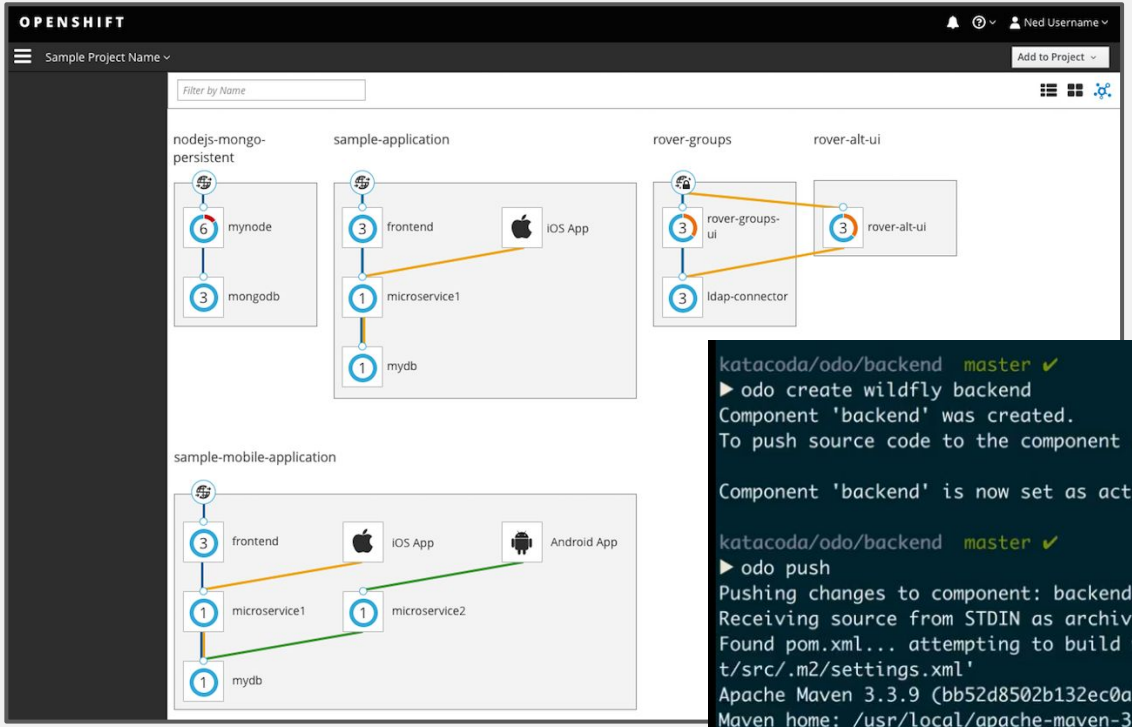
Day 1 - 使用者(Dev-to-Ops)體驗

Dev & Admin 操作介面整合



- OpenShift + Tectonic Console
- 統一web console程式庫
- 同時滿足Dev與集群Ops用戶需求

Application Focused UX



K8s缺少App的概念

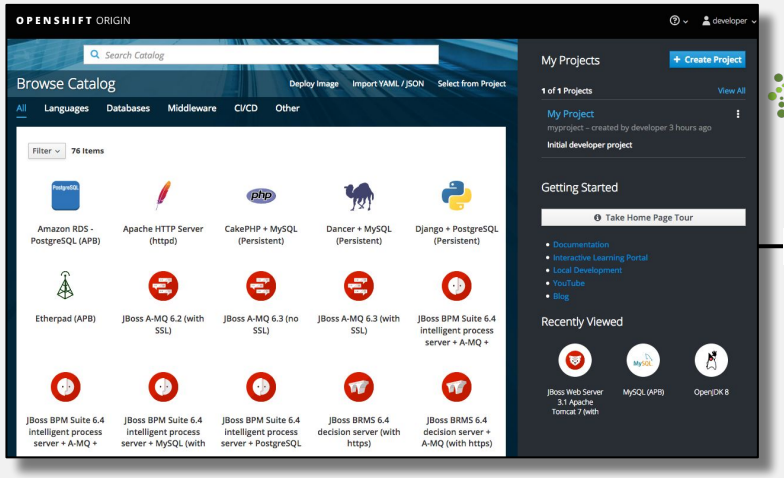
- App關注的UX
- Dev CLI - odo(OpenShift Do)
  - 專注Dev需求

```
katacoda/odo/backend  master ✔                                          8d
▶ odo create wildfly backend
Component 'backend' was created.
To push source code to the component run 'odo push'

Component 'backend' is now set as active component.

katacoda/odo/backend  master ✔                                          8d
▶ odo push
Pushing changes to component: backend
Receiving source from STDIN as archive ...
Found pom.xml... attempting to build with 'mvn package -Popenshift -DskipTests -B -s /opt/app-roo
t/src/.m2/settings.xml'
Apache Maven 3.3.9 (bb52d8502b132ec0a5a3f4c09453c07478323dc5; 2015-11-10T16:41:47+00:00)
Maven home: /usr/local/apache-maven-3.3.9
Java version: 1.8.0_161, vendor: Oracle Corporation
Java home: /usr/lib/jvm/java-1.8.0-openjdk-1.8.0.161-0.b14.el7_4.x86_64/jre
Default locale: en_US, platform encoding: ANSI_X3.4-1968
```

Service Catalog & Brokers

揭露並提供自動安裝服務

*提供Dev真正一致且快速的開發體驗



OPEN SERVICE BROKER API

OpenShift Template Broker → OPENSHIFT — OpenShift Templates

OpenShift Automation Broker → ANSIBLE — Ansible Playbook Bundles

AWS Service Broker → AMAZON WEB SERVICES — Public Cloud Services

Other Service Brokers (Azure Service Broker) → OTHER COMPATIBLE SERVICES — Other Services

OPENSHIFT SERVICE CATALOG

SERVICE BROKERS

Cloud Service

aws

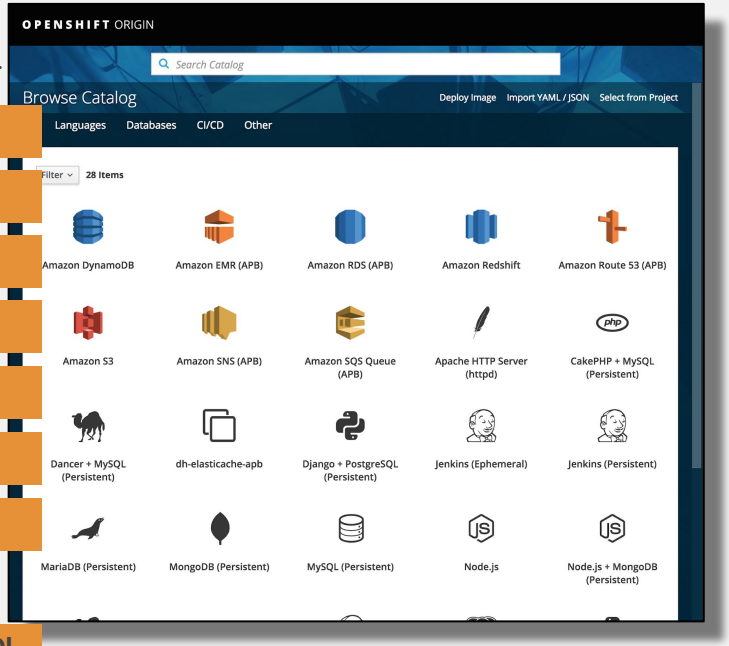
Service Broker

*New **AWS** Services coming:*

- **Kinesis Data Streams**
- **KMS**
- **Lex**
- **Polly**
- **Rekognition**
- **Translate**
- **SageMaker**

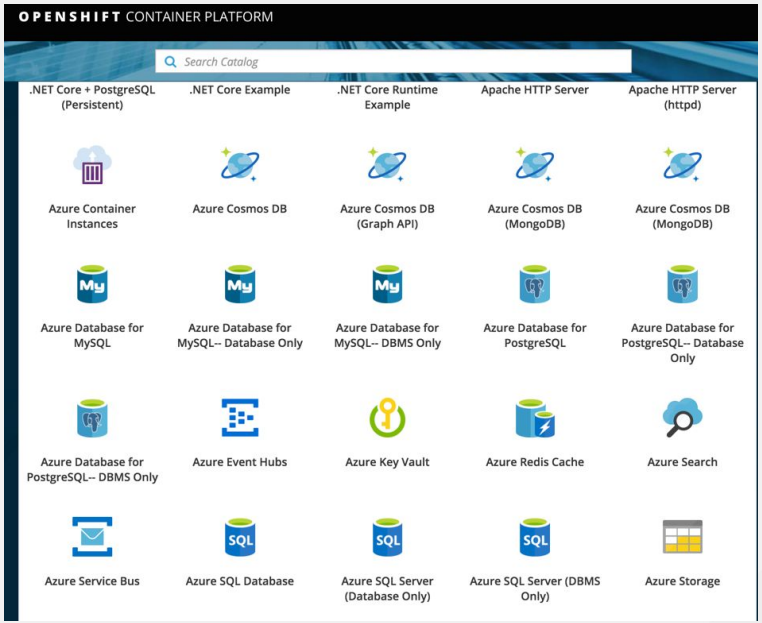
Additional RDS engines:

- **Aurora, MariaDB, PostgreSQL**



Azure

Service Broker

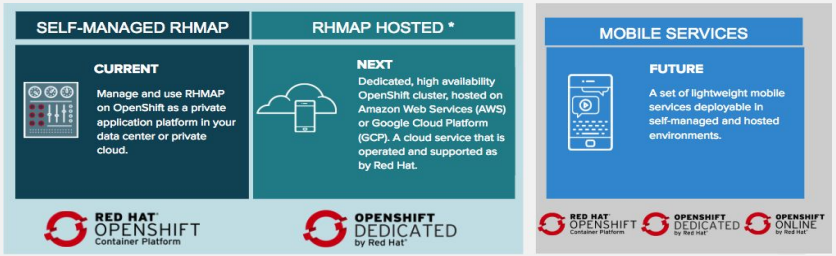


IBM Cloud Private Service broker coming soon ...

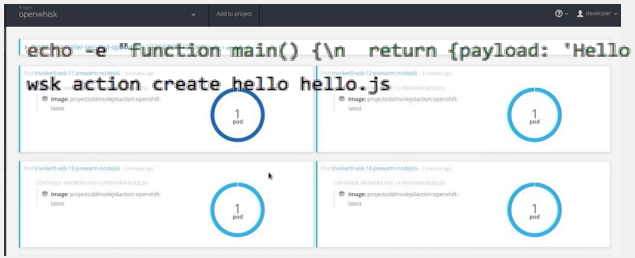
redhat.

整合各式中介軟體與開發工具

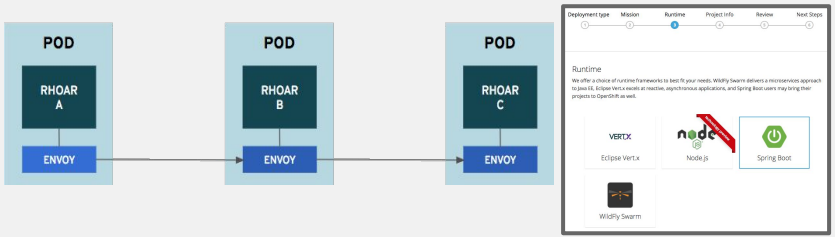
Mobile開發平台



FaaS



各式App Runtime



應用程式/API連結整合

Fuse Standalone

- Single JVM Fuse
- Developer-focused
- Integration where you need it
- **"Classic" integration**

Fuse on OpenShift

- Scale out Fuse
- Replaces Fabric v1
- Developer-focused
- **"Cloud native" integration**

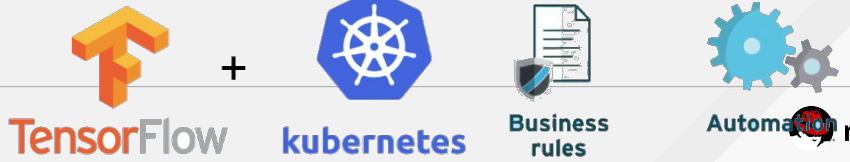
Fuse Ignite (iPaaS)

- Low/no-code UX
- 100% cloud-based
- Integration through a browser
- Fuse for the rest of us - **"Ad Hoc" Integration**

分散式Data Grid

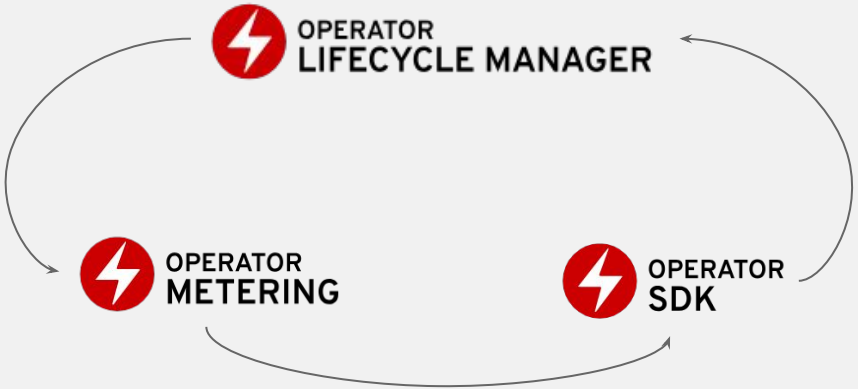
- **Caching Service**
  - Zero configuration
  - Basic caching (k/v store)
  - No durability guarantees / No replication
- **Shared Memory Service***
  - Almost zero configuration
  - Caching + replication
  - HTTP Session off-loading
- **JDG as a service**
  - Full-blown JDG servers
  - Customer managed configurations
  - Red Hat container catalog official images
- **System of records / Primary store ***
  - Zero configuration
  - Fully distributed
  - Backed by a persistent store
  - Indexes, text search, query

資料分析/規則管理



Day 2 - 提升運維效率

自動化容器平台Day 2運維



CONTAINER OPERATORS

封裝與自動化對App的運維知識與行為入單一Package

OPERATOR FRAMEWORK

開源工具，用有效率、自動化、可擴展的方式，管理運行在Kubernetes上的App實例

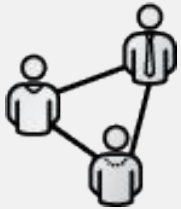
https://github.com/operator-framework

Operator Framework

Developer

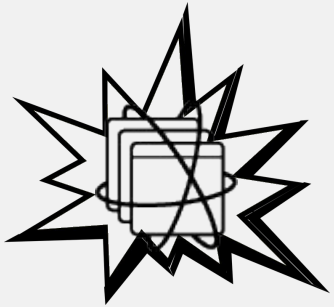
$ oc new-app myapp

30之後 ...



平台服務Team

嘗試控制快速增加的
App framework & runtime



如果這樣會否更美好 ...

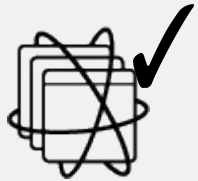
OPERATOR FRAMEWORK

Developer

$ oc create -f myAppsTask.yaml

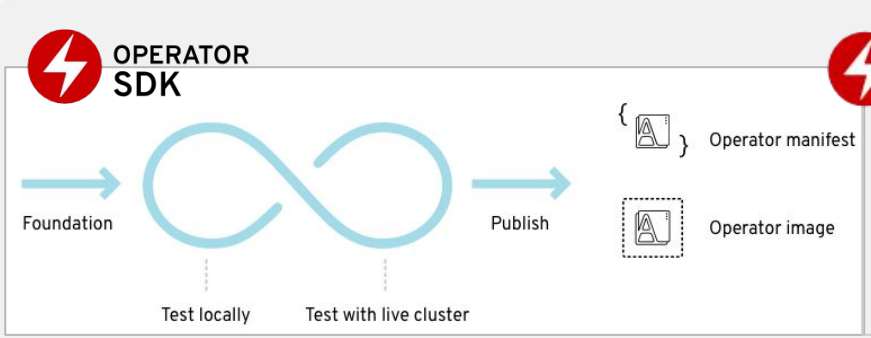
The Platform

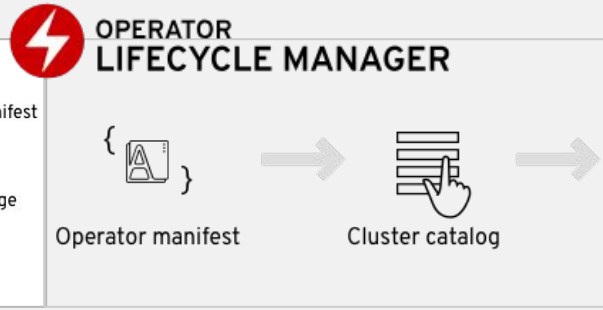
- re-index
- backup
- restore
- de-frag
- recycle
- ...任何Admin task

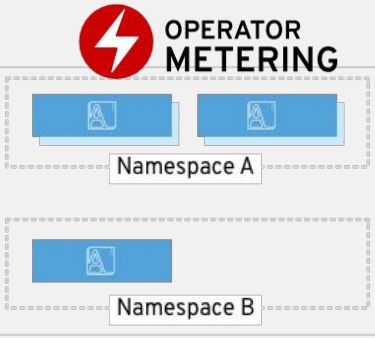


redhat.

透過Operator Frameworks

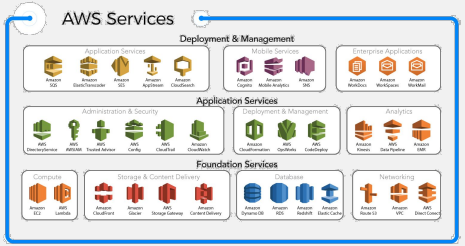






你的應用程式

能夠像這些服務一樣
”聰明自動”



但能跑在...

Microsoft Azure

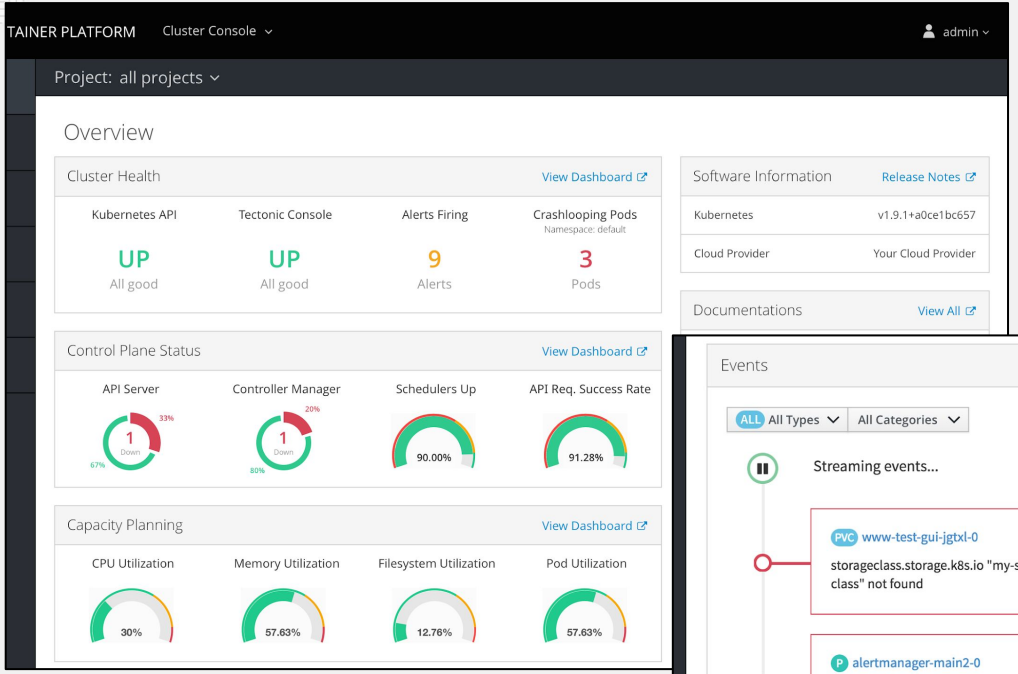
Google Cloud Platform

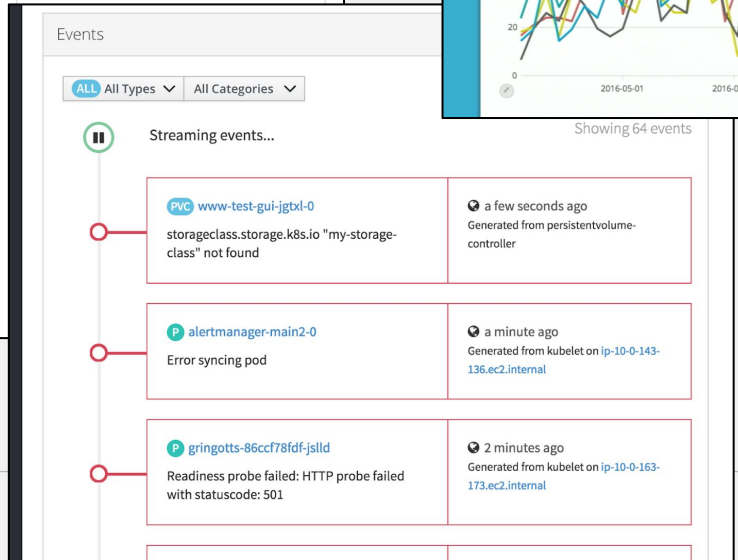
openstack

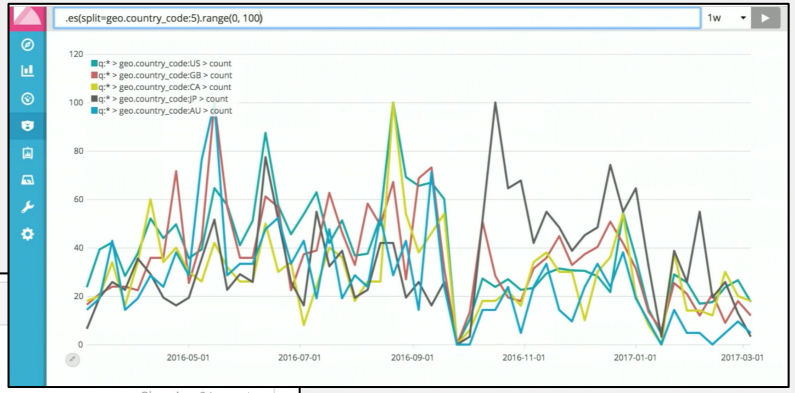
amazon web services

redhat.

監控與日誌







PaaS+CaaS

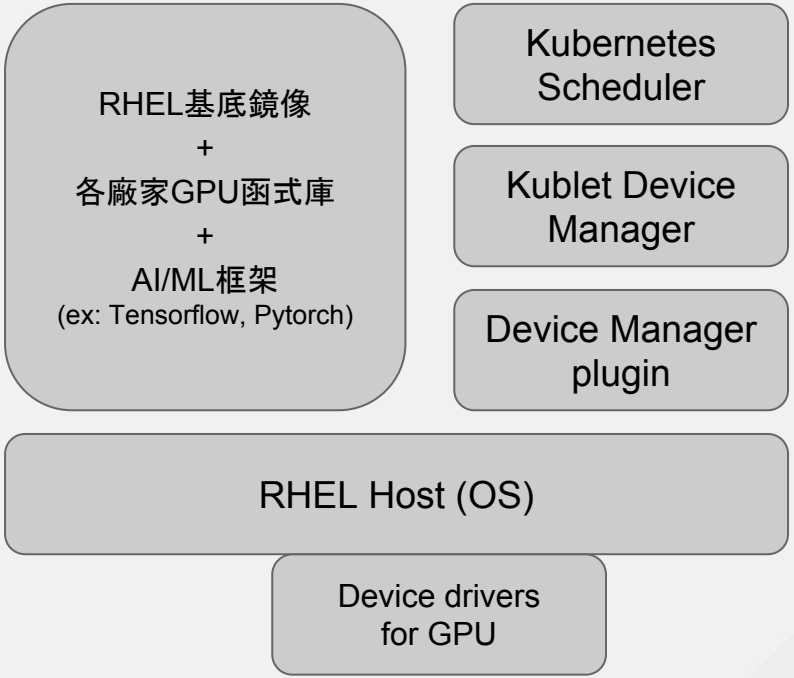
- OpenShift與Tectonic的結合

- ES Stack 5.x

redhat.

於GPU上的OpenShift

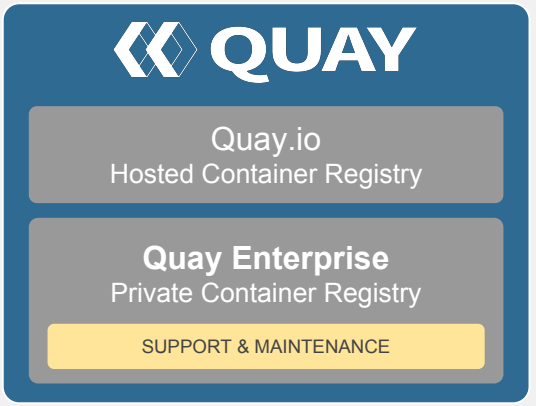
- 與策略合作夥伴於 drivers, plugins, 和container images上的協同合作。
- Device Manager GA
  - 可運行各種device (ex: GPU, dongle)
- Scheduler: Priority and preemption
  - 智慧調度各種device
- 各種device, plugin與相依組建，無縫的安裝體驗
- 於Red Hat Container Catalog上的容器鏡像認證
- 認證與企業支援

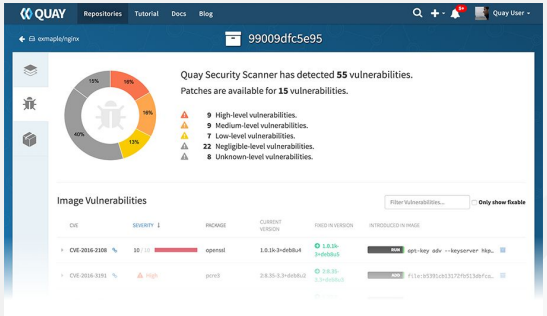


企業級容器鏡像庫：Quay

除了既有OpenShift所提供的內部鏡像庫，Red Hat Quay是一進階、通用型企業級鏡像庫，特色功能如：

- **弱點掃描 (透過Clair專案技術)**
  - 持續性的掃描容器弱點，提供對於已知威脅之能見度，與修復能力。
- **跨區複製與同步**
  - 跨越地理區域，可靠的保存、打包、與發佈容器鏡像
- **自動打包**
  - 當Push行為發生於程式代碼庫，Quay能偵測並自動建構新版本鏡像。
- **鏡像回朔與Time Machine**
  - 檢視鏡像歷史紀錄，並可快速的在多版本 Image Build 間切換。

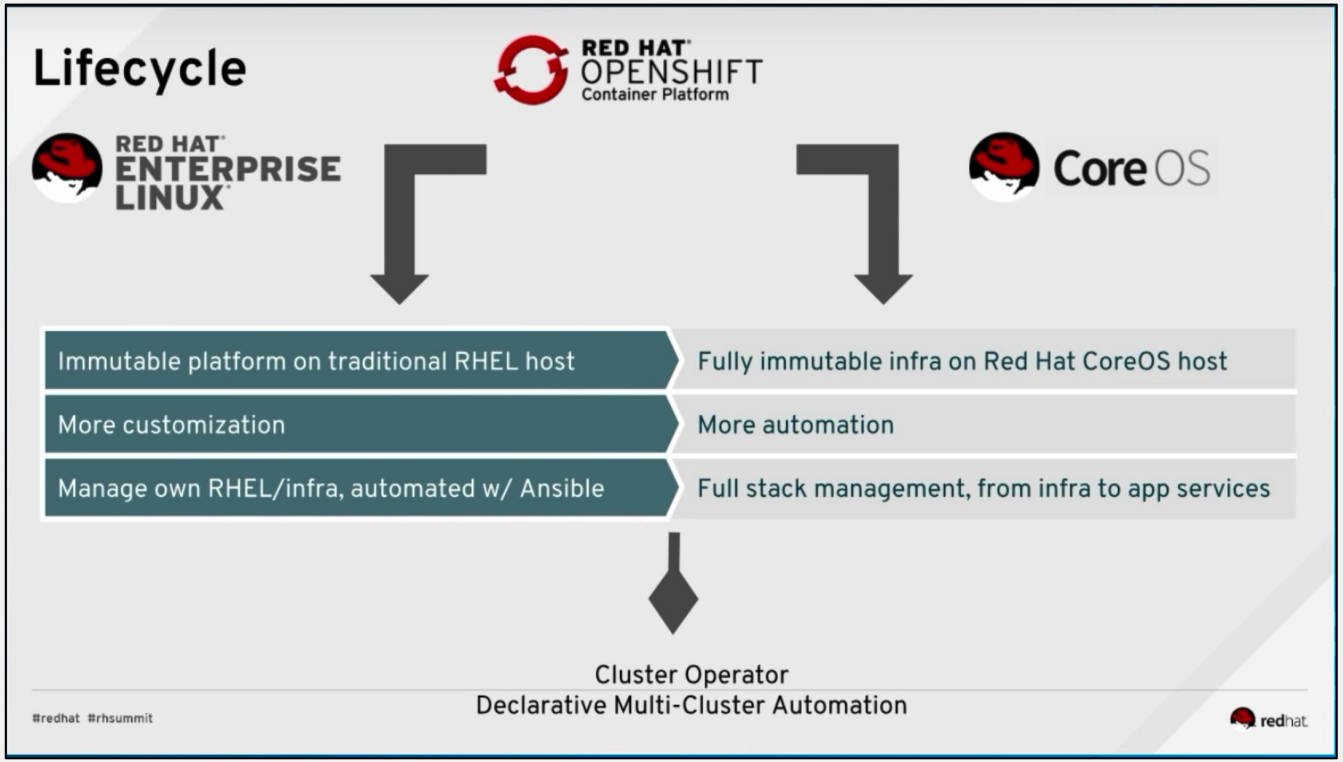


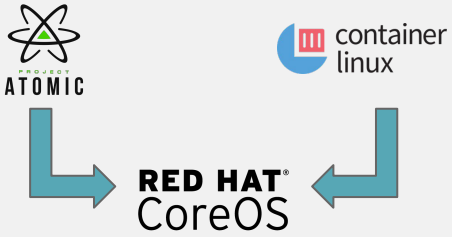


redhat.

Day 0 - 提升平台效率

Immutable平台基礎架構





RHEL與CoreOS兩種選擇

- 客製化 vs 自動化
- 多功能 vs 輕量化
- 通用性 vs 目的專注
- Ansible & Operator

更豐富的自動化Ansible腳本

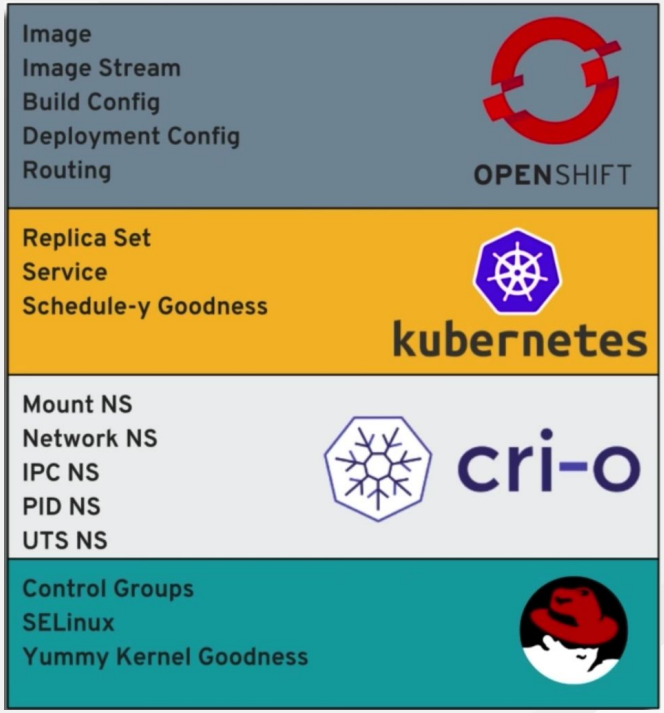
- **AWS Scale Groups:** Ability to create and upgrade AWS scale group to meet demand and conserve resources; immutable infrastructure.
- **Multi-AZ Support:** Ensure applications can survive an AZ outage.
- **Update Certs at Upgrade:** Ensures all generated certs are updated during upgrade so certificates don't expire.
- **Ability to Check Deployment During an Upgrade is Successful:** Standard pattern to follow to ensure updates rollout successfully so it's possible to report a problem updating a component
- **Node Restart Hooks:** Allows admins to be able to execute an arbitrary set of tasks while a node is drained of pods and choose to have the node rebooted rather than services restarted; useful for performing tasks such as OS upgrades.
- **CRI-O Support:** Support for installing and configuring CRI-O container runtime instead of Docker.
- **Control Plane as Static Pods:** Leverage self management of cluster components to reduce direct host management and enable node bootstrapping by default
- **Standardized Node Labels:** Following upstream standards, nodes must now be labeled with node-role.kubernetes.io/{master,compute,infra}=true.
- **Provision Pull Secret for authenticated registries:** Allow the use of content from an authenticated registries.

更輕量、快速、安全、容易使用的容器技術

cri-o

- 專為Kubernetes而設計的輕量、OCI標準的容器runtime.
- 可從任何OCI / Docker registry，運行任何OCI / Docker容器
- 專注在穩定與平台(K8s)生命週期
- 加強改容器安全與規模運作下的效能

Mr. Selinux (Dan Walsh)談容器Runtime：
https://www.youtube.com/watch?v=nBXALsqs1RA



更輕量、快速、安全、容易使用的容器技術

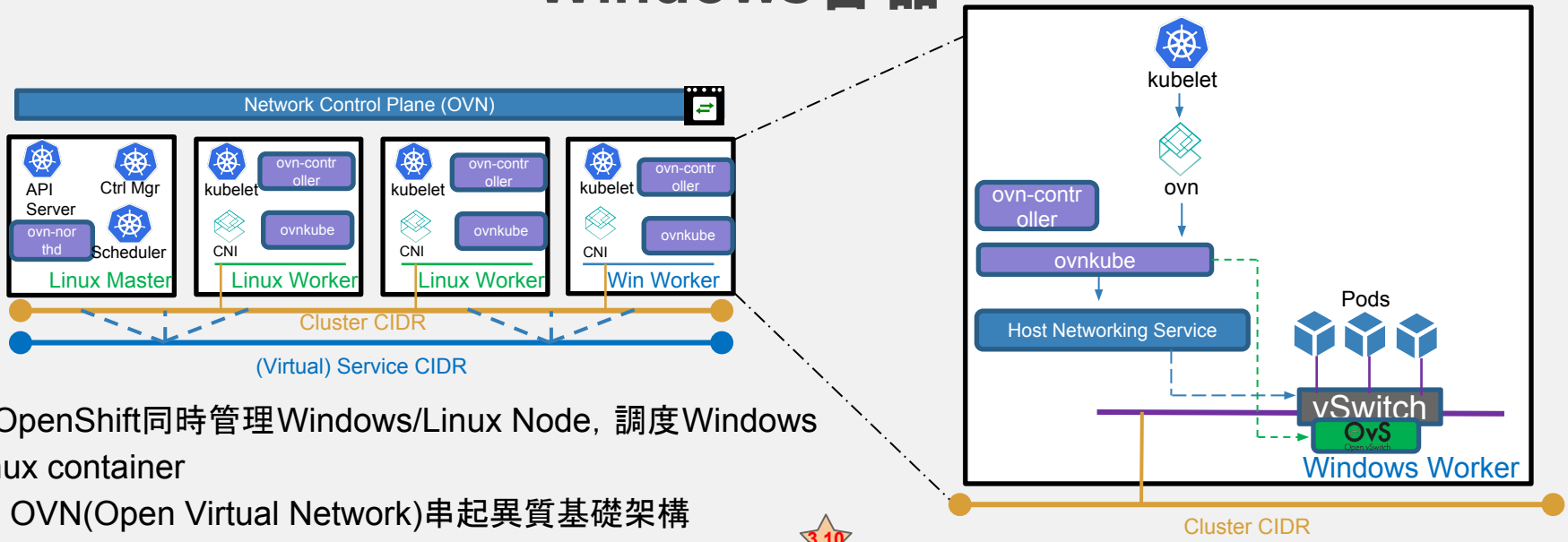
buildah

OCI標準、無Daemon的OCI / Docker Image創建/編輯工具

podman

一個無Daemon的CLI/API工具，提供大家熟悉的查錯、控制OCI標準容器與Pods的體驗

Windows容器



透過OpenShift同時管理Windows/Linux Node，調度Windows與Linux container

- OVN(Open Virtual Network)串起異質基礎架構
- Tech Preview: Windows 1709/1803與OpenShift 3.10 3.10
- 最快Windows 2018 LTS與OpenShift 3.11 GA 3.11
- SMB與iSCSI存儲支持
- 為Life-n-Shift或是整個App發佈而設計(not S2I)

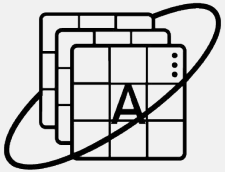
至今的討論都圍繞在...

虛擬化對容器技術來說

”我需要一個地方安裝、運行、跟管理Kubernetes集群“

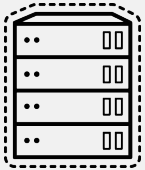
“我需要一種方式好提供更加嚴格的容器隔離”

那運行多年、既有的應用程式怎麼辦呢？



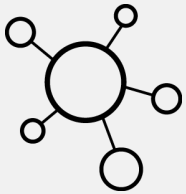
容器基礎架構與調度

像OpenShift這樣，運行容器應用與透過 Kubernetes調度正成為應用程式的**新標準**



虛擬化的應用程式

已虛擬化的應用程式短時間 內不會消失



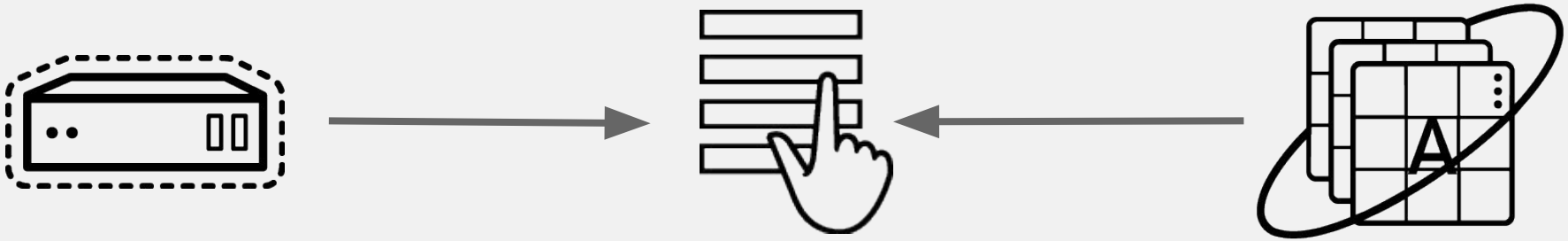
融合的基礎架構

我們不希望維護多套複雜的基礎架構，好同時支援容器與虛擬機

Container Native Virtualization (CNV)

透過CNV技術，OpenShift將成為一個統一、分享的管理調度平台

同時用於建構、修改、與部署容器化與虛擬化的應用程式



預計於OpenShift 3.11將以Tech Preview釋出。

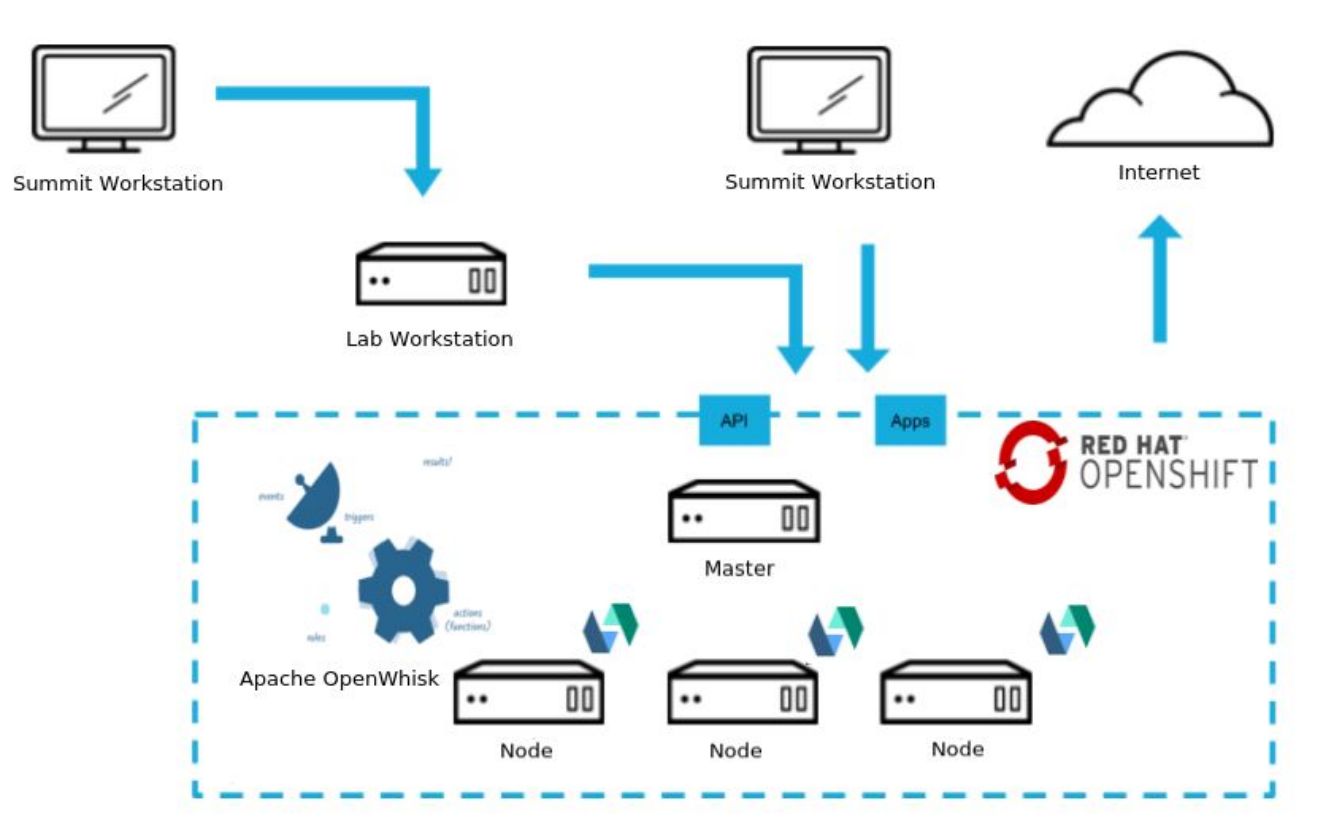
基於KubeVirt專案: http://www.kubevirt.io/

Demo(Red Hat Summit 2018): https://youtu.be/r8e4bT0-zhU?t=45m30s

Demo

FaaS-(Dev), Cloud Native Operation-(Ops)

FaaS


Summit Workstation
Summit Workstation
Internet
Lab Workstation
API
Apps
RED HAT OPENSHIFT
Master
Apache OpenWhisk
Node
Node
Node

OpenShift Roadmap

OpenShift Container Platform 3.10 (July)
- Kubernetes 1.10 and CRI-O option
- Smart Pruning
- Istio (Dev Preview)
- oc client for developers
- Golden Image Tooling and TLS bootstrapping
- Windows Server Containers (Dev Preview))
- Prometheus Metrics and Alerts (Tech Preview)
- S3 Svc Broker

OpenShift Online & Dedicated
- Dedicated self-service: RBAC, limit ranges
- Dedicated encrypted storage, multi-AZ, Azure beta

Q2 CY2018

Q3 CY2018

OpenShift Container Platform 3.11 (Sept)
- Kubernetes 1.11 and CRI-O default
- Infra monitoring, alerting with SRE intelligence, Node Problem Detector
- Etcd, Prometheus, and Vault Operators - Tech preview
- Operator Certification Program and JBoss Fuse Operator
- Autoscaler for AWS and P-SAP features
- Metering and Chargeback (Tech Preview)
- HPA Custom Metric
- Tech preview of ALM
- New web console for developers and cluster admins
- Ansible Galaxy ASB support
- CNV (Tech Preview)
- OVN (Tech Preview for Windows)
- FIPS and other Security PAGs

OpenShift Online & Dedicated
- OpenShift Online automated updates for OS
- Chargeback (usage tracking) for OpenShift Online Starter

Q4 CY2018

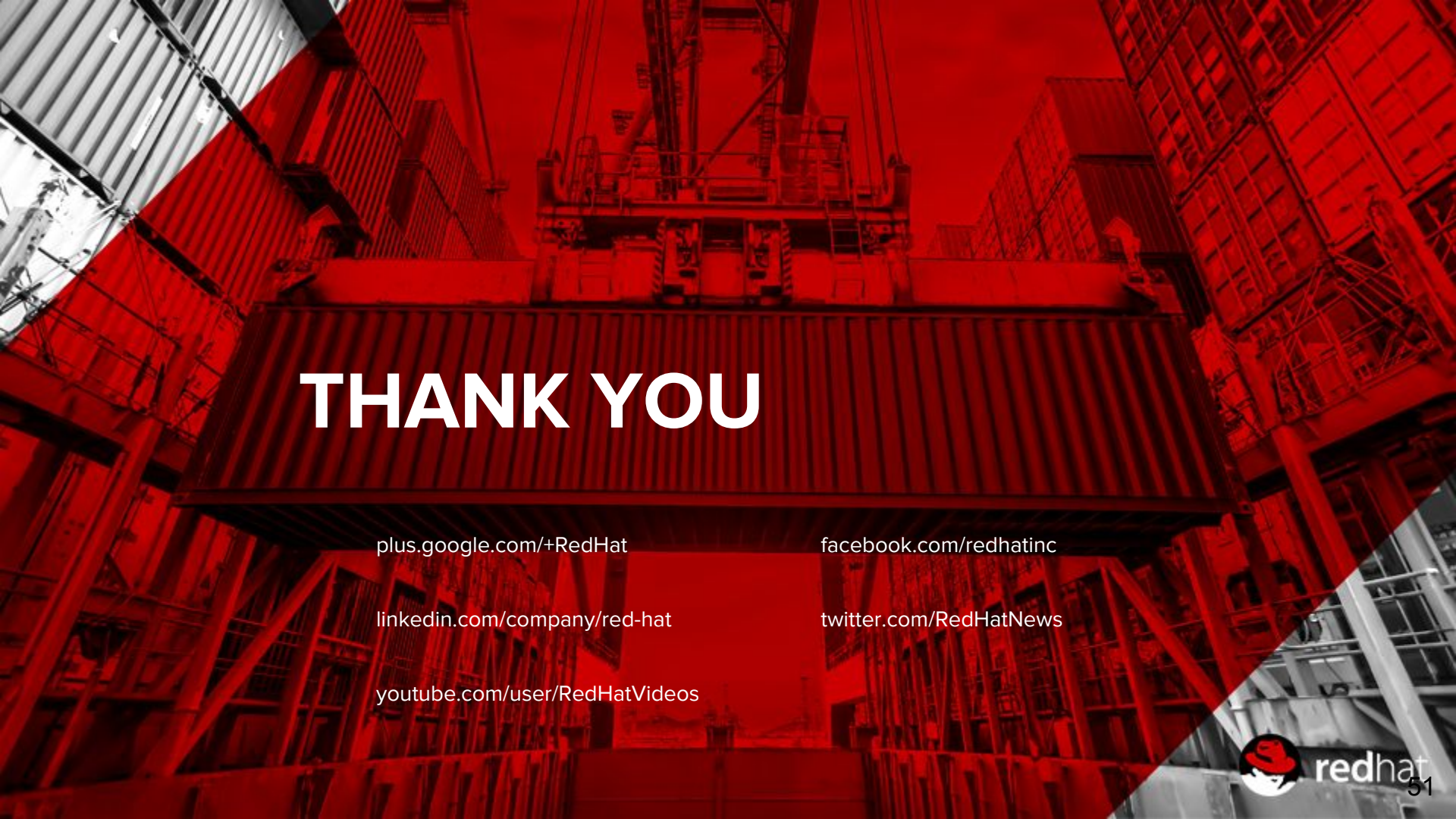
OpenShift Container Platform 3.12 (Dec/Jan)
- Kubernetes 1.12 and CRI-O default
- Converged Platform
- Full Stack Automated Installer
  - AWS, RHEL, Azure, OSP
- Over the Air Updates
- RHCC integrated experience
- Windows Containers GA
- Easy/Trackable Evaluations
- Red Hat CoreOS Container Linux with Ignition Automations
- Cluster Registry
- HPA metrics from Prometheus

OpenShift Online & Dedicated
- Cluster Operator driven installs
- Self-Service Dedicated User Experience

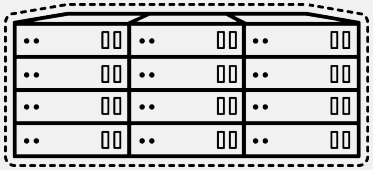
Q1 CY2019

OpenShift Container Platform 3.13 (March)
- Kubernetes 1.13 and CRI-O default
- Full Stack Automation
  - GCP, VMware
- Istio GA
- Mobile 5.x
- Serverless (Tech Preview)
- RHCC for non-container content
- Integrated Quay (Tech Preview)
- Idling Controller
- Federated Ingress and Workload Policy
- OVN GA
- Che (Tech Preview)

OpenShift Online & Dedicated
- OpenShift.io on Dedicated (Tech Preview)


THANK YOU
plus.google.com/+RedHat
facebook.com/redhatinc
linkedin.com/company/red-hat
twitter.com/RedHatNews
youtube.com/user/RedHatVideos
redhat

Admin Console

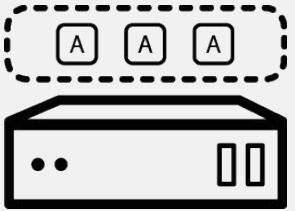


跨集群視野

- 監控
- 事件
- 資源

存取控制

- RBAC
- Service Account
- Projects & Namespaces



管理

- Operators
- Nodes
- Upgrade