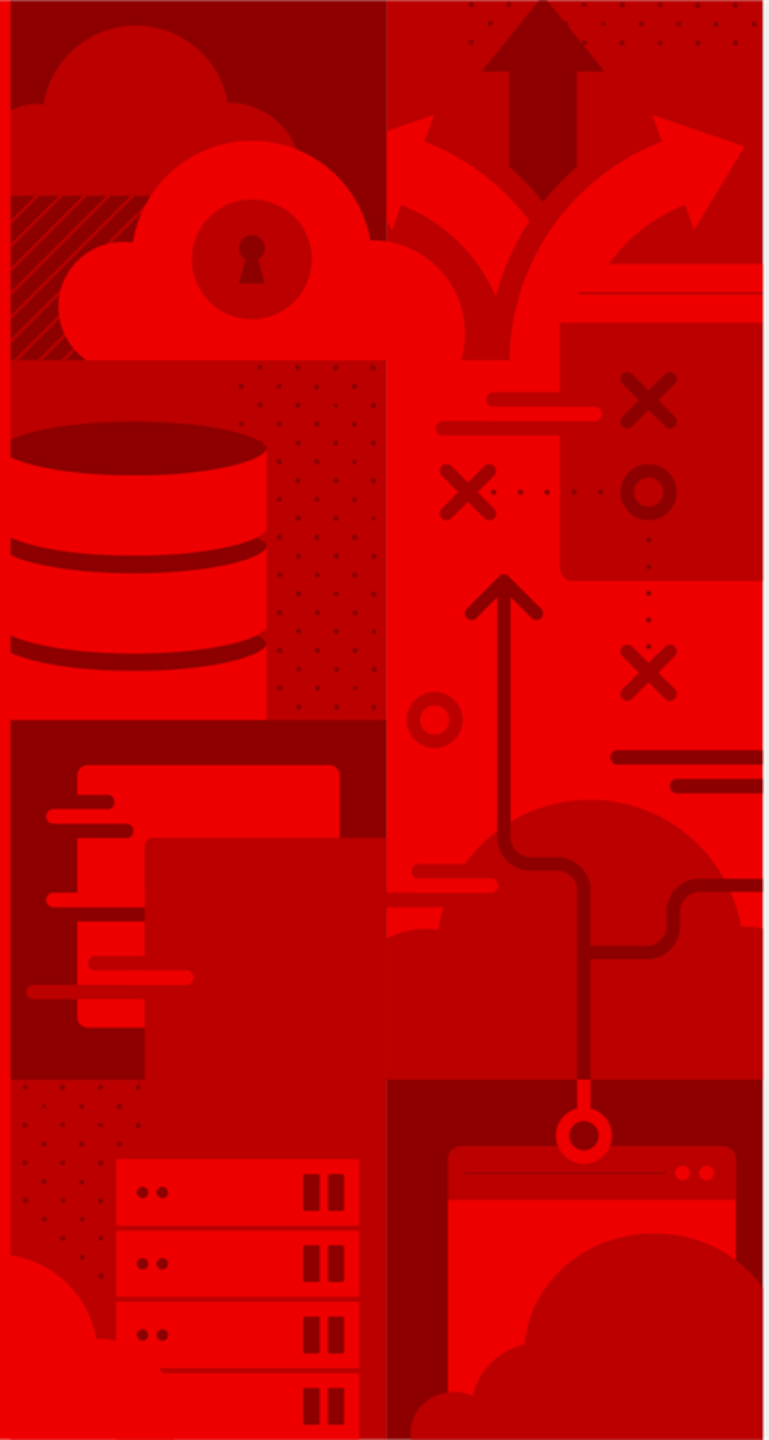


Red Hat OpenShift vs DIY Kubernetes

솔루션 아키텍트 팀
Red Hat Korea
2020.03.26

Red Hat

컨테이너와 쿠버네티스로 무엇을 하고 싶으세요?

당신의 차별점은 애플리케이션을 빠르게 제공하는 능력에 달려 있습니다

클라우드-네이티브 애플리케이션

AI & 머신러닝

블록체인

IoT

문화 혁신

CONTAINERS, KUBERNETES, MICROSERVICES & DEVOPS ARE KEY INGREDIENTS

Red Hat

쿠버네티스를 올바로 사용하는 것은 어렵습니다

INSTALL	DEPLOY	HARDEN	OPERATE
• Templating	• Identity & Security Access	• Platform Monitoring & Alerts	• OS Upgrade & Patch
• Validation	• App Monitoring & Alerts	• Metering & Chargeback	• Platform Upgrade & Patch
• OS Setup	• Storage & Persistence	• Platform Security Hardening	• Image Upgrade & Patch
	• Egress, Ingress & Integration	• Image Hardening	• App Upgrade & Patch
	• Host Container Images	• Security Certifications	• Security Patches
	• Build/Deploy Methodology	• Network Policy	• Continuous Security Scanning
		• Disaster Recovery	• Multi-environment Rollout
		• Resource Segmentation	• Enterprise Container Registry
			• Cluster & App Elasticity
			• Monitor, Alert, Remediate
			• Log Aggregation

75%

의 기업 사용자가 쿠버네티스 채택의 가장 큰 걸림돌로 구현 및 운영의 복잡성을 들었습니다.

Source: The New Stack, The State of the Kubernetes Ecosystem, August 2017

Red Hat

THE KUBERNETES NEWS YOU DON'T WANT

TESLA

- K8s dashboard exposed
- AWS environment with telemetry data compromised
- Tesla's infrastructure was used for crypto mining

Unnecessary Costs

weightwatchers

- No security on K8s dashboard
- IT infrastructure credentials exposed
- Enabled access to a large part of Weight Watchers' network

Unrealized Value

monzo

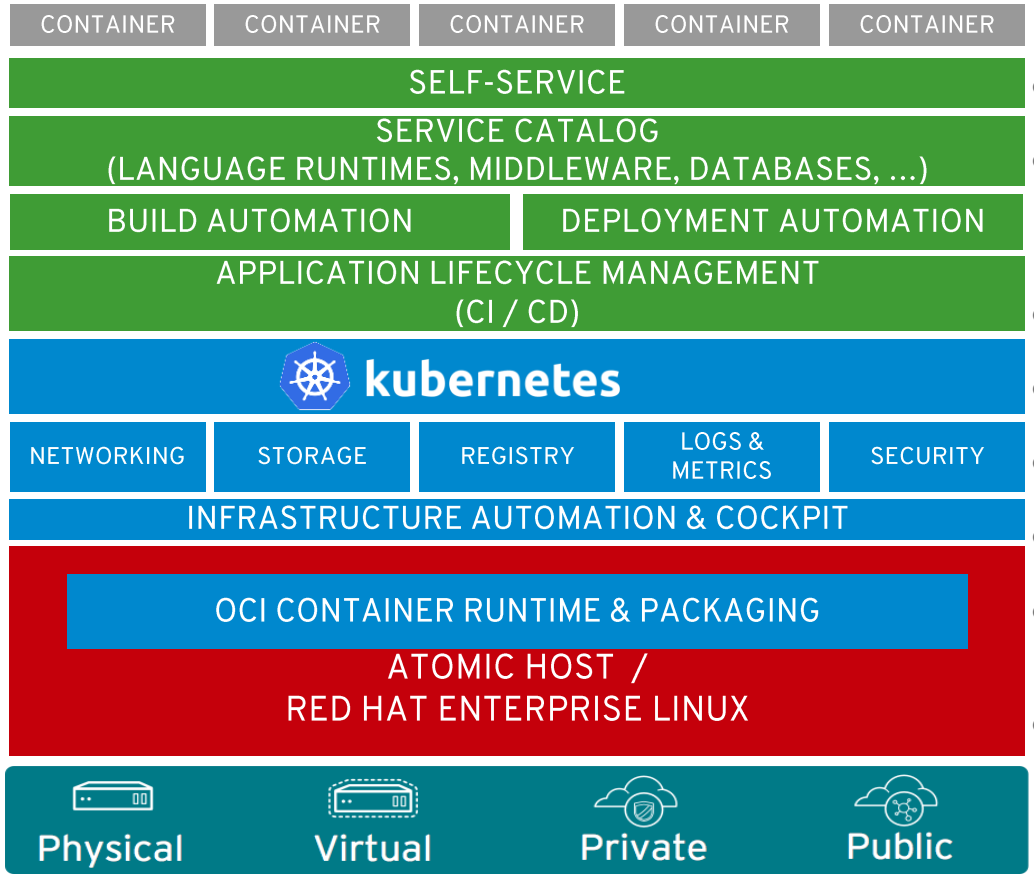
- K8S and etcd bug introduced to servers during update
- New features and changes deployed cause failures
- Restart backend components leading to full platform outage

Increased Risk

Red Hat

OpenShift = Enterprise Kubernetes+

Red Hat
OpenShift



- 개발 및 운영을 위한 다양한 툴 제공(IDE, UX 등)
- 전통적인 WEB/WAS, 최신의 MSA 및 Serverless 아키텍처를 위한 다양한 application runtimes & services 제공
- Auto-Healing으로 Application HA 기능 제공
- Auto-Scaling으로 과부하 대비 기능 제공
- Kubernetes 기반의 컨테이너 오케스트레이션
- Docker/OCI 표준 컨테이너
- 컨테이너 최적화 OS 기반 – Red Hat Enterprise Linux/Atomic Host
- 하이브리드 클라우드 환경에 설치(Bare-Metal, 다양한 VM, Public/Private IaaS 등)

Red Hat

OPENSHIFT 는 엔터프라이즈급 KUBERNETES 플랫폼 입니다

Security fixes
100s of defect and performance fixes
200+ validated integrations
Middleware integrations
(container images, storage, networking, cloud services, etc)
9 year enterprise lifecycle management
Certified Kubernetes

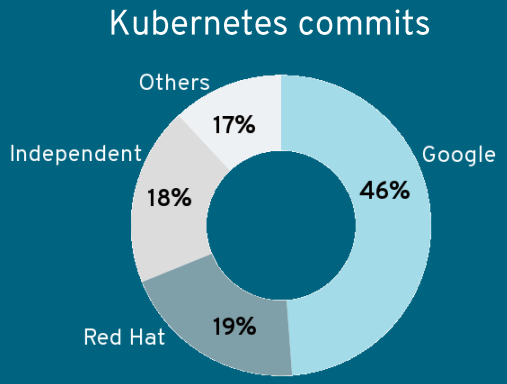
Red Hat

RHOCP 고객 사례(국내)

수행 프로젝트 실적		
발주처	**사업명**	**프로젝트 내용**
행정자치부	정부지식 공유활용기반 사업 (온나라 클라우드)	OpenShift에서 정부부처별 개별 운영되던 정부 표준 그룹웨어를 SaaS on PaaS 형태로 구축
행정안전부	국가기록물 사업	국가기록물 시스템 운영을 위한 컨테이너 플랫폼 구축
국가정보자원관리원	자동자원 확장풀 사업	자동 자원 확장시스템 구축을 위한 컨테이너 플랫폼 도입
SK텔레콤	Mobile App 표준 개발 환경	Mobile App 개발자들의 표준 개발환경을 위한 PaaS 시스템 도입 및 구축
롯데정보통신	대내/대외 PaaS 서비스 구축	대내 및 대외 클라우드(PaaS) 서비스 위한 시스템 구축 및 서비스 활성화
국방부 메가센터	PaaS Pilot 시스템 구축	국방부 메가센터에서 DevOps환경 도입을 위한 Pilot Project 구현
정보통신산업 진흥원	클라우드 지원 센터	개인 또는 스타트업 기업에게 빠른 개발을 위해 PaaS를 제공
두산정보통신	개발 환경 통합 및 B2C 서비스	PaaS 기반의 표준개발환경 구축 및 대내/외 서비스용 시스템 구축
삼성전자	PaaS for MIS	PaaS기반의 내부 MIS 시스템 서비스 구현 및 타당성 확보
eBay Korea	PaaS for Internal Service	Microservice 기반 Application의 서비스를 위한 PaaS 도입 및 구축
롯데카드	차세대 LP 플랫폼 구축 사업	PaaS 플랫폼을 이용하여 MLC 통합 시스템을 구축 및 DevOps 환경의 효율적인 IT 운영 환경 구현
현대중공업	DT를 위한 Private Cloud 구축 사업	IoT 솔루션 도입 및 운영을 위한 Container 기반의 PaaS 솔루션 도입 및 구축
농협정보	PaaS for Cloud Service	IaaS 외에 Container 서비스를 위한 PaaS 검토 및 구축
POSCO	PosFrame 용 컨테이너 플랫폼 구축 사업	Storm/Redis/EAP 등 BigData 분석 운영을 위한 컨테이너 플랫폼 구축
오렌지라이프	MIS용 컨테이너 플랫폼 구축 사업	PaaS 기반 MIS 업무시스템 운영을 위한 컨테이너 플랫폼 구축
신한 은행	글로벌뱅킹 대외계 Open 인터페이스 시스템 구축	컨테이너 플랫폼 기반 글로벌뱅킹 대외계 시스템 구축
KB 은행	더 K 프로젝트 클라우드 기반 구축 사업	비대면 업무를 위한 PaaS 클라우드 플랫폼 기반 구축
KT	KT IPC/EPC PaaS 플랫폼 구축 사업	IPC 및 RPC 용 PaaS 플랫폼을 구축하여 Cloud 서비스 제공

WHY IS RED HAT THE BEST CHOICE?
THE FOUR Cs

CODE



Red Hat은 구글과 주도적인 쿠버네티스 개발자 이자 공헌자.

쉽고, 신뢰할 수 있는 보다 안전한 컨테이너를 개발

CUSTOMERS

운영 환경에 사용 중인 많은 고객 사례 보유

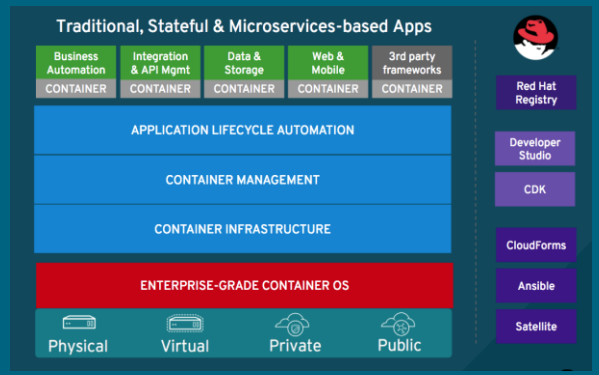
OpenShift Online 과 OpenShift Dedicated 서비스를 수년간 운영한 경험 보유

CLOUD

클라우드 서비스 제공자, ISV와 강력한 파트너쉽

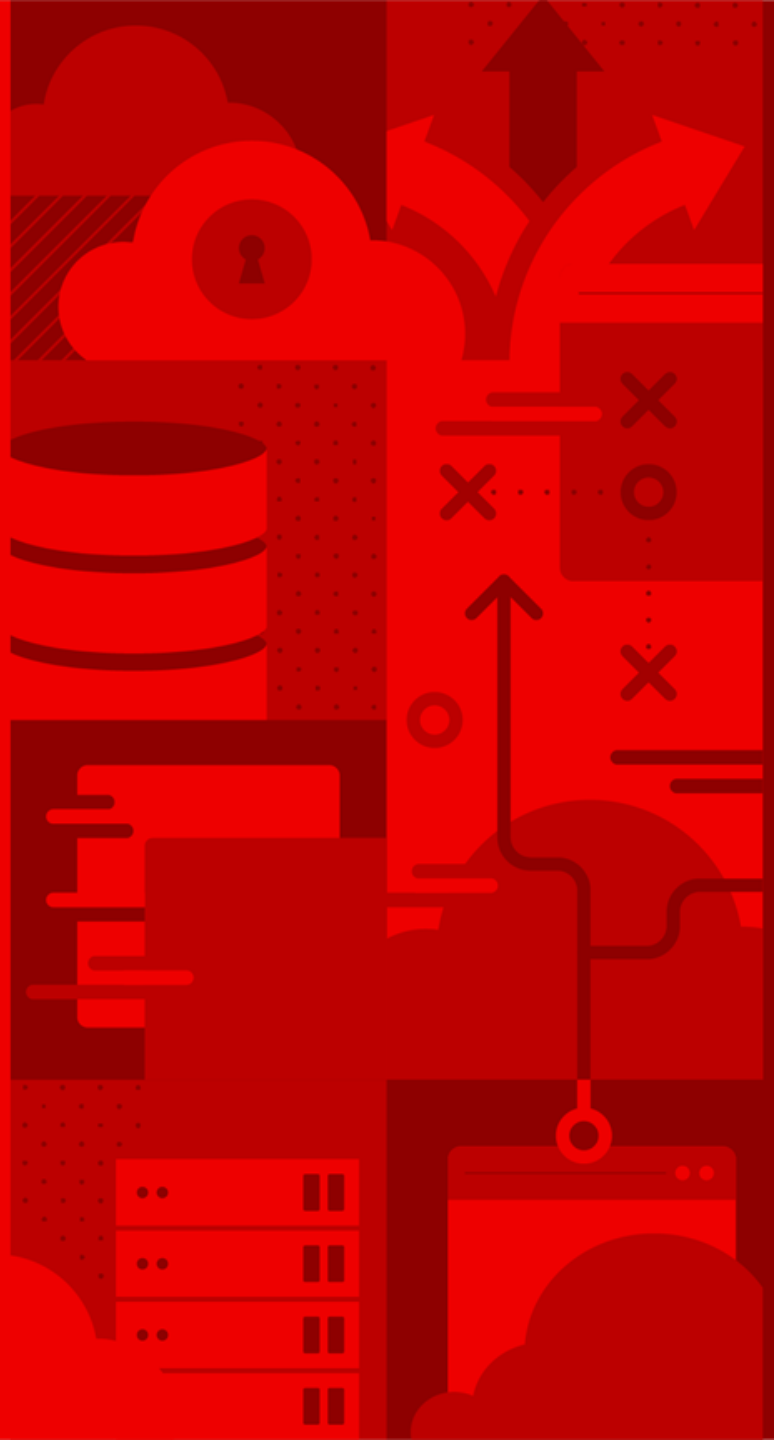
인증된 파트너 이미지의 광범위한 컨테이너 카탈로그

COMPREHENSIVE



개발자 도구, 보안, 애플리케이션 서비스, 스토리지 및 관리를 포함하는 포괄적인 컨테이너 제품 및 서비스 포트폴리오

Source: [1] Stackalytics, *Contribution by Companies*. (Release: All, Projeact type: Kubernetes, Module: kubernetes, Metric: Commits) Retrieved: March 2, 2018.



OpenShift vs DIY

Red Hat

DIY Kubernetes 사용의 위험성

TESLA

- K8s dashboard exposed
- AWS environment with telemetry data compromised
- Tesla’s infrastructure was used for crypto mining

Unnecessary Costs

weightwatchers

- No security on K8s dashboard
- IT infrastructure credentials exposed
- Enabled access to a large part of Weight Watchers' network

Unrealized Value

monzo

- K8S and etcd bug introduced to servers during update
- New features and changes deployed cause failures
- Restart backend components leading to full platform outage

Increased Risk

Red Hat

OPENSHIFT 는 엔터프라이즈급 KUBERNETES 플랫폼 입니다

Security fixes
100s of defect and performance fixes
200+ validated integrations
Middleware integrations
(container images, storage, networking, cloud services, etc)
9 year enterprise lifecycle management
Certified Kubernetes

Red Hat

Automated and Integrated Security with Red Hat

CONTROL
Application Security

- Container Content
- CI/CD Pipeline
- Container Registry
- Deployment Policies

DEFEND
Infrastructure

- Container Platform
- Container Host Multi-tenancy
- Network Isolation
- Storage
- Audit & Logging
- API Management

EXTEND

- Security Ecosystem

컨테이너 보안을 위한 10계층

redhat.

TECHNOLOGY DETAIL

TEN LAYERS OF CONTAINER SECURITY

INTRODUCTION

Containers have broad appeal because they allow users to easily package an application, and all its dependencies, into a single image that can be promoted from development, to test, and to production—without change. Containers make it easy to ensure consistency across environments and multiple deployment targets like physical servers, virtual machines (VMs), and private or public clouds. This helps teams more easily develop and manage the applications that deliver business value.

WHAT ARE CONTAINERS?

It depends on who you ask...

INFRASTRUCTURE

- Sandboxed application processes on a shared Linux OS kernel
- Simpler, lighter, and denser than virtual machines
- Portable across different environments

APPLICATIONS

- Package my application and all of its dependencies
- Deploy to any environment in seconds and enable CI/CD
- Easily access and share containerized components

Enterprises require strong security and anyone running essential services in containers will ask, "Are containers secure?" and "Can we trust containers with our applications?" This paper describes 10 key elements of security for different layers of the container solution stack and different stages of the container life cycle.

facebook.com/redhatinc
@redhatnews
linkedin.com/company/red-hat

redhat.com

http://red.ht/2riSiGI

Red Hat

Kubernetes가 부족한 점

Kubernetes는 기본적인 컨테이너 오케스트레이션을 제공하지만, 실제 운영이 가능 하려면 고객 또는 3rd-party 가 구성, 통합, 운영 및 지원하는 추가적인 인프라스트럭처가 필요합니다.

1. Linux 운영 체제 필요
2. 컨테이너 런타임 (CRI-O, Containerd, Docker 등)이 필요
3. 이미지 레지스트리가 필요
4. SDN(Software-Defined Network)이 필요.
5. 로드 밸런서 및 라우팅 필요
6. 로그 관리가 필요
7. 컨테이너 자원 사용률 측정 항목 및 모니터링 필요
8. 컨테이너 빌드 및 배포(+자동화)

OpenShift는 플랫폼의 일부로 완벽하게 통합되고 완벽하게 테스트 된 모든 구성 요소를 포함

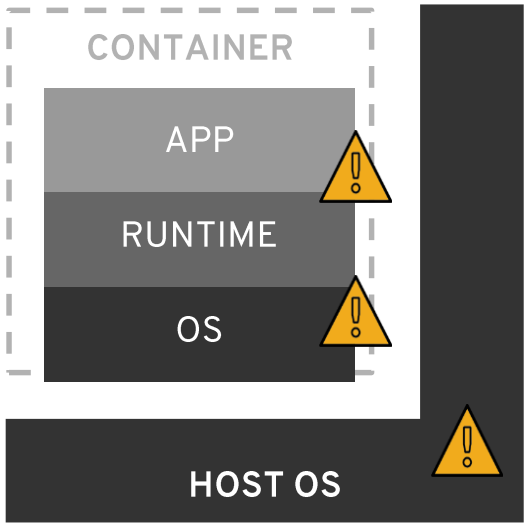
Docker & DIY vs Red Hat Enterprise Linux

UNTRUSTED

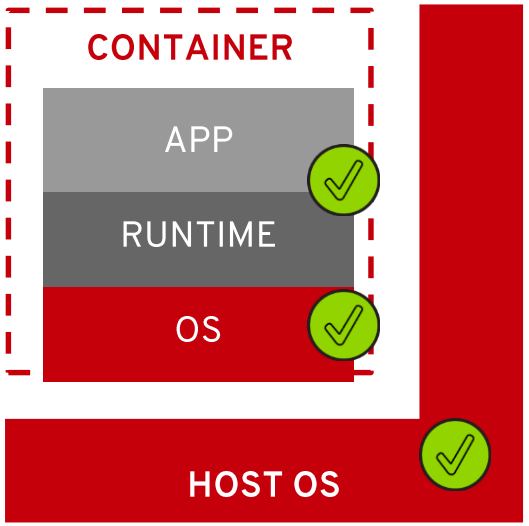
- 컨테이너 내부의 인프라가 손상될 수 있습니까?
- 앱과 라이브러리를 언제 어떻게 업데이트 할 예정입니까?
- 호스트에서 다른 호스트로 이동시 작동합니까?

RED HAT CERTIFIED

- 호스트 및 컨테이너에 대한 신뢰할 수 있는 기반 제공
- 엔터프라이즈 라이프 사이클의 일부로 사용 가능한 보안 픽스가 있는 컨테이너 안의 신뢰할 수 있는 콘텐츠
- 호스트간 이식성 제공



- Certified Container Images
- Certification Middleware
- Red Hat Container Registry
- Container Development Kit
- Certification as a service



Red Hat

OpenShift vs DIY Kubernetes

	Red Hat OpenShift Container Platform	DIY Kubernetes
Container Orchestration	Kubernetes	Kubernetes
Container Image	OCI-compliant/docker	BYO OCI-compliant
Container Runtime	CRIO/docker	BYO OCI-compliant Engine
Container Build	RHCC/S2I/dockerfile	None
Container Registry	**Quay**/OSS docker registry	None
Container Scanner	OSCAP/Clair	None
CI/CD Automation	Jenkins 2	None
IDE	Che	None
Web UX	OpenShift Web Console	Kubernetes Web Console
CLI UX	oc/odo/kubectl	kubectl
Service Catalog	Operators/OSB-API	None
Secrets Management	Kubernetes Secrets	Kubernetes Secrets
Supported/Preferred Runtime	RHOAR (EAP, Spring, vert.x, node.js)	None

OpenShift vs DIY Kubernetes

	Red Hat OpenShift Container Platform	Upstream Kubernetes
Service Mesh	Istio, Jaeger, Kiali, Profana	None
Logging	EFK	None
Metrics	Prometheus/Grafana	None
Storage	OpenShift Container Storage	None
Network	OVN	None
Ingress	Kubernetes Ingress/Routes	Kubernetes Ingress
Ingress Controller	HA Proxy	None
Egress	Egress Router	None
Authentication	Kubernetes Auth/RH-IdM	Kubernetes Auth
App Isolation	Kubernetes scheduler	Kubernetes Scheduler
Infrastructure	Bare Metal, vSphere, KVM, OpenStack, AWS, GCP, Azure	BYO Linux
Infra Automation	Ansible/Terraform/Operators	None
Infra Management	Admin Console	None
Operating System	RHEL or RHEL CoreOS	None
CNCF Certified Kube	Yes	No

OpenShift vs DIY

	OpenShift	Origin	Kubernetes
	Container Platform	Upstream	Orchestration Engine
Stability			
장기간 안정성, 버그 수정 및 보안 패치의 하위 호환성으로 장기 유지 관리 및 지원	●		
보안 및 기능 BackPort	●		
장기간 지원 및 출시주기 관리	●		
대규모 및 엔터프라이즈 운영을 테스트한 최적의 구성 및 설정	●		
임의의 타사 프로젝트 바이너리에 대한 의존성을 이해, 확인 및 유지할 필요가 없음	●		
자동화 된 소프트웨어 업데이트, 경고 및 관리	●		
Patches/Updates			
Red Hat이 제공하고 유지 보수하는 패치	●		
인증 된 핫픽스 / 패치 및 보안 업데이트.	●		
Certifications			
RHEL/RHEL 7.x는 Common Criteria certification- BSI-DSZ-CC-0999 을 획득	●		

OpenShift vs DIY

	OpenShift	Origin	Kubernetes
	Container Platform	Upstream	Orchestration Engine
Security			
공식화 된 엔터프라이즈 보안 해결 프로세스	●		
Red Hat Security Response 팀은 문제를 식별 / 추적하고 해결	●		
보안 : OpenShift는 MCS를 통해 SELinux 사용자 정의 컨텍스트에서 컨테이너를 투명하게 감싸므로 Kuvernnetes 및 OCI 컨테이너가 제공하는 기본 네임 스페이스 보호보다 훨씬 강력한 SELinux 컨테이너 보안을 제공	●	●	
Single Sign On(SSO) 지원(OAuth, SAML)	●	●	
Support			
SLA, 결함 에스컬레이션, 수명 종료 정책 관리	●		
기술지원 포탈	●		
운영환경 Support	●		
제품 개발자가 지원을 제공	●		
향상된 기능 요청을 제출할 수있는 기능	●		
프로젝트 리드에 대한 액세스(Clayton Coleman, Jeremy Eder - etc)	●		

OpenShift vs DIY

	OpenShift	Origin	Kubernetes
	Container Platform	Upstream	Orchestration Engine
Consulting, TAM and Training Certification			
Red Hat 및 인증 파트너의 전문가 컨설팅	●		
교육은 코드 작성자의 영향을 받은 커리큘럼을 통해 출처에서 직접 제공	●		
교육 및 자격증 체계	●		
Quality Assurance			
QA / 확장성 테스트 / Hardening	●		
성능, 확장성, 가용성 및 안정성을 테스트 완료	●		
Ecosystem			
Amazon AWS, Google GCE, Microsoft Azure와 같은 여러 클라우드 공급자 인증	●		
3rd Party Independent Software Vendor 지원 : 예 : 컨테이너 및 통합 환경에서 실행되는 응용 프로그램	●		
Openstack, Openshift (*), Satellite, Cloudforms, 스토리지 (Ceph & Gluster) 및 Another Tower [* - 향후 출시 예정]의 Red Hat Cloud Suite로 테스트 한 전체 스택 통합	●		
Open vSwitch (NetFlow 규칙에 의해 관리되는 VXLAN 솔루션)를 통한 완벽한 확장 가능한 SDN 지원	●		
EBS, Cinder 및 GCE를 통한 영구 볼륨을위한 동적 스토리지 프로비저닝	●	●	●

Red Hat

OpenShift vs DIY

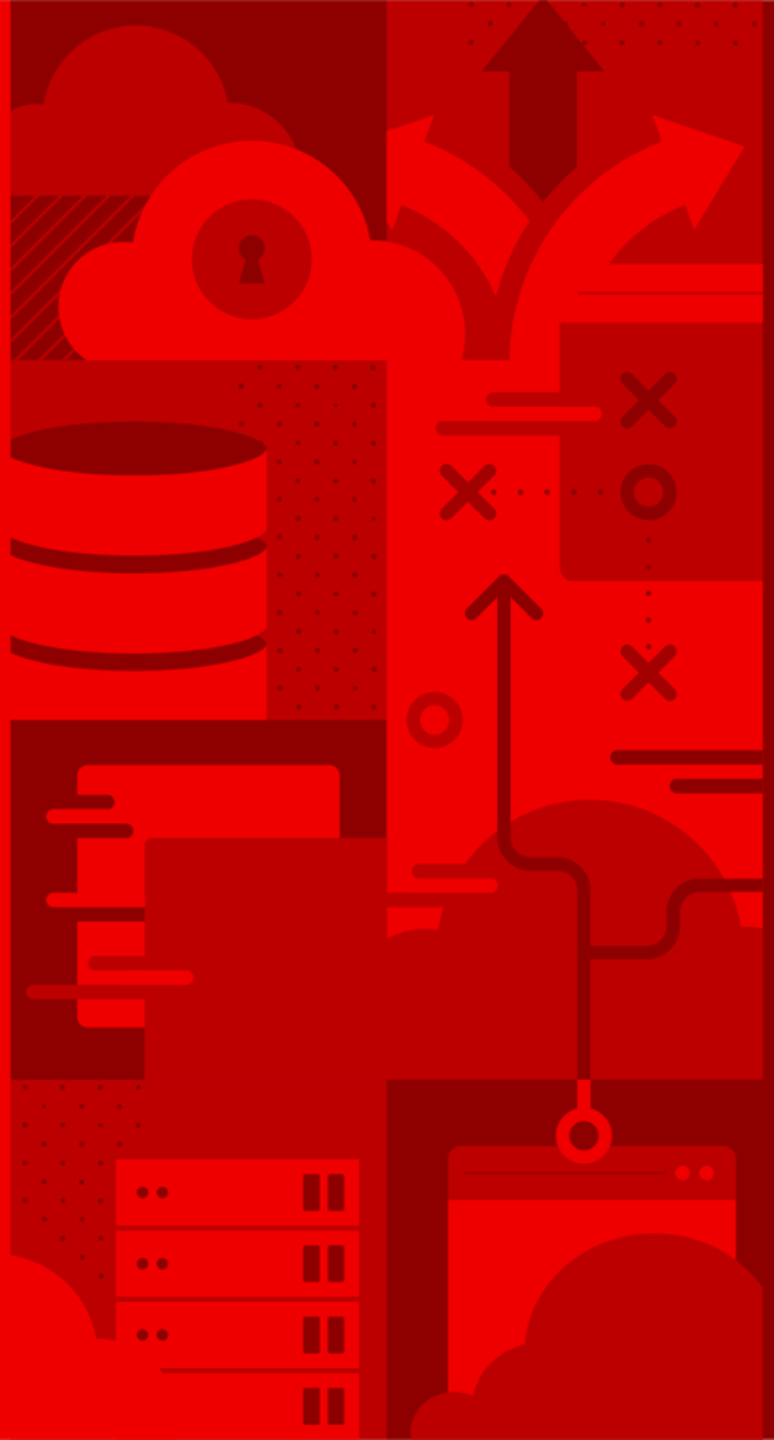
	OpenShift	Origin	Kubernetes
	Container Platform	Upstream	Orchestration Engine
Developer Productivity			
개발자를 위한 Container Development Kit 제공	●	●	
웹브라우저 기반 통합 개발환경(Web IDE) 제공 CodeReady Workspaces	●		
테스트, 보안 및 지원되는 이미지가 있는 Atomic Registry 제공 예 : EAP, BRMS, BPMS, Python 등	●		
멀티-테넌트 기능	●	●	
그래픽 기능	●	●	
Innovation Labs Quick Start/Support	●		
제품 로드맵에 영향(RFE Submissions)	●		
프로젝트 리드에 대한 액세스	●		
CI / CD 통합 : OpenShift는 Jenkins, git 및 기타 업계 표준을 지원	●	●	
Cloudforms와 통합 된 운영 관리	●	●	
레지스트리 : OpenShift는 프로덕션 수준 컨테이너 이미지 레지스트리 (Atomic Registry, Satellite 및 독립 실행형 인스턴스에서도 사용됨)를 제공. Docker 컨테이너의 일부로 제공되는 기본 레지스트리보다 훨씬 기능이 풍부하고 기능이 뛰어남	●	●	

OpenShift vs DIY

	OpenShift	Origin	Kubernetes
	Container Platform	Upstream	Orchestration Engine
Monitoring and telemetry			
EFK (Elasticsearch, FluentD, Kibana - ELK 스택과 비슷 함) 로깅 색인은 새로운 앱을 시작할 때 스스로를 관리	●	●	●
Hawkular / Heapster / Cassandra의 성능 메트릭 스택	●	●	
Role 기반 액세스 컨트롤	●	●	
Third party support			
로드 밸런서 예 : F5, Avinetworks, Amazon ELB 및 기타 주요로드 밸런서 제공 업체의 지원	●	●	
개발 도구 - app dev 도구 공급자로부터 플러그인을 실행하기 위한 인증 예 : Appdynamics	●	●	
여러 클라우드 공급자 인증 예 : Amazon AWS, Google GCE, Microsoft Azure	●		

OpenShift vs DIY

	OpenShift	Origin	Kubernetes
	Container Platform	Upstream	Orchestration Engine
Monitoring and telemetry			
EFK (Elasticsearch, FluentD, Kibana - ELK 스택과 비슷 함) 로깅 색인은 새로운 앱을 시작할 때 스스로를 관리	●	●	●
Hawkular / Heapster / Cassandra의 성능 메트릭 스택	●	●	
Role 기반 액세스 컨트롤	●	●	
Third party support			
로드 밸런서 예 : F5, Avinetworks, Amazon ELB 및 기타 주요로드 밸런서 제공 업체의 지원	●	●	
개발 도구 - app dev 도구 공급자로부터 플러그인을 실행하기 위한 인증 예 : Appdynamics	●	●	
여러 클라우드 공급자 인증 예 : Amazon AWS, Google GCE, Microsoft Azure	●		



교육 프로그램

Red Hat

오픈시프트 관리자 과정

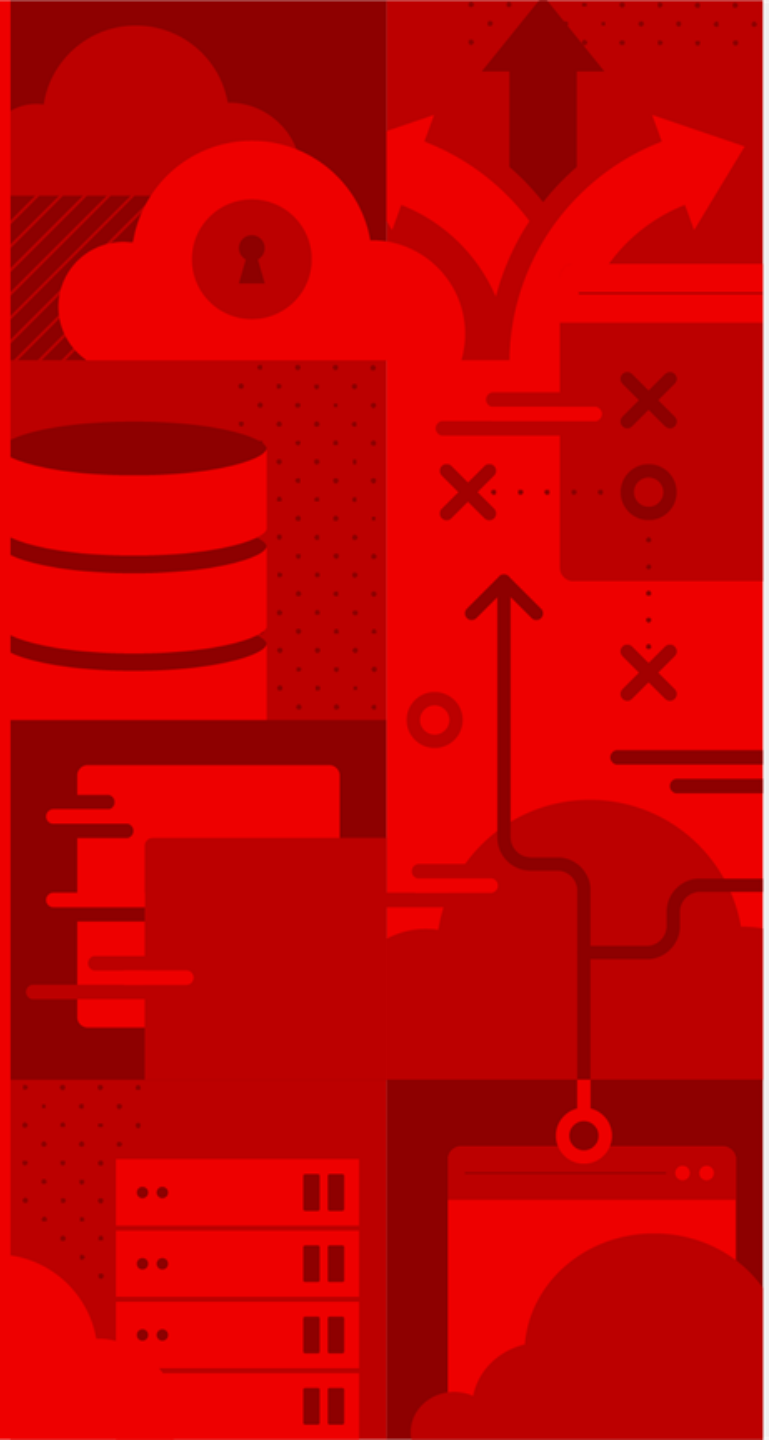
- OpenShift Operator
- OpenShift Administrator

Red Hat

오픈시프트 개발자 과정

- Non-Docker Developer
- OpenShift Developer
- Container Application Developer
- Microservices Developer Deploying to OCP
- JEE Developer Deploying Microservices to OCP

Red Hat



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

facebook.com/redhatinc

youtube.com/user/RedHatVideos

twitter.com/RedHat

Red Hat