

# OpenShift Plus 企業 快速擴展叢集的好助手

完整的容器跨雲管理平台

Michael Suen

Solution Architect , Red Hat

2022/10/18

# Agenda

- ▶ Multi Hybrid Cloud 的趨勢
- ▶ Multi Hybrid Cloud 的挑戰
- ▶ 多混合雲的兩大門神 – ACM、ACS
- ▶ 多雲的擴展 – 邊緣運算
- ▶ 總結

# Multi Hybrid Cloud 的趨勢

# 雲原生時代的痛點

您是否擁有能夠抵禦安全風險的穩定系統？

您能否更快的為業務需求提供解決方案？

您的系統是否能夠擴展以滿足不斷增長的需求？



## 穩定的困難

- ▶ 不一致的系統和配置
- ▶ 安全弱點
- ▶ 人為錯誤



## 敏捷的困難

- ▶ 不斷複雜多元的技術堆疊
- ▶ 過多人為流程
- ▶ 老舊系統

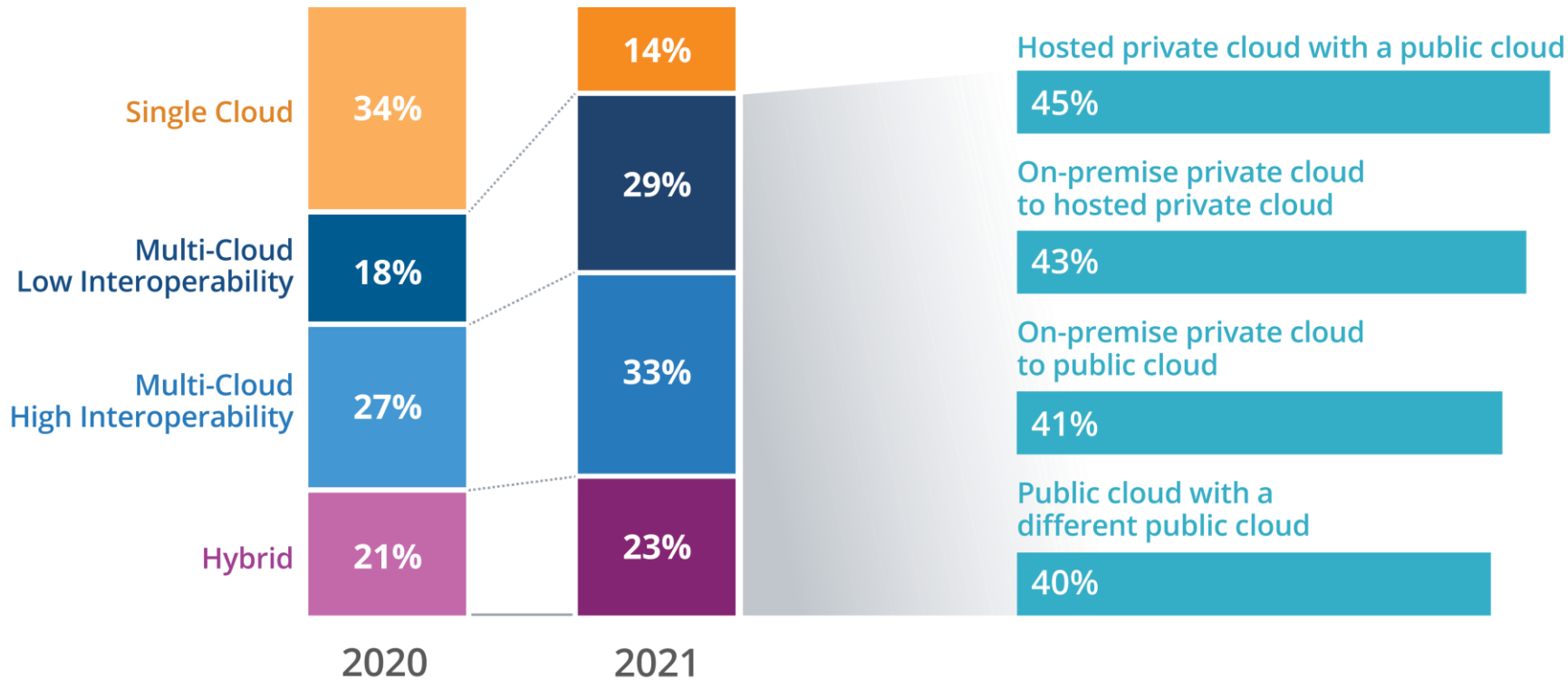


## 擴展的困難

- ▶ 太多系統需要管理
- ▶ 太多人為流程
- ▶ 太過勞力密集

# 多雲環境是產業目標

QC31: how would you describe your organizations use of different on-premise & off-premise cloud environments? [2020 actual compared to 2021 actual]

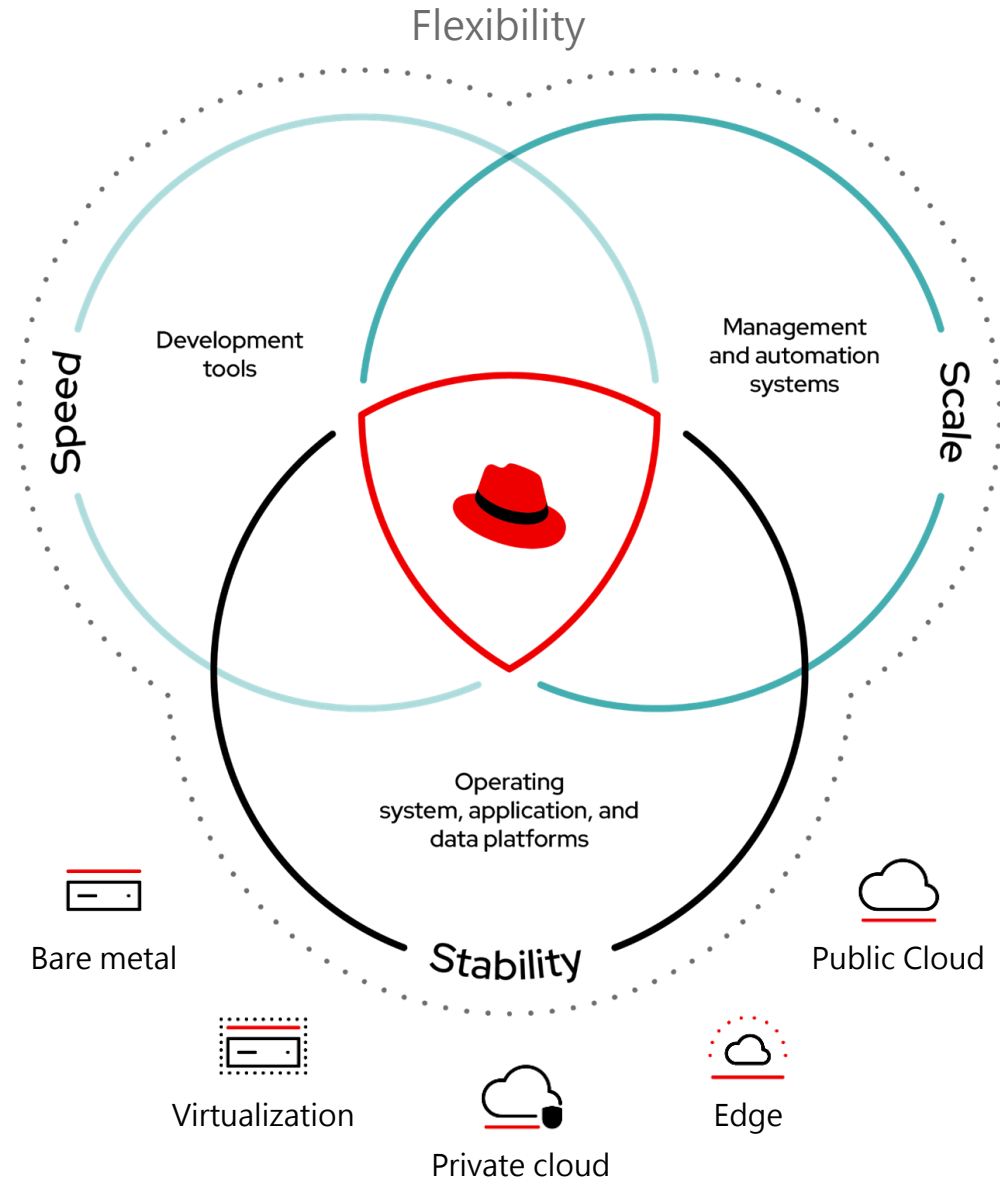


由於管理工具和治理能力的進步，混合雲和多雲環境在過去12個月中呈現翻倍的成長速度

隨著混合雲穩定增長，單一雲的使用率持續下降

# 開放混合雲

為了發展數位轉型的速度、穩定和擴展性，讓轉型的應用、基礎設施和流程，能提高真正彈性且安全的雲體驗，**開放混合雲**是 Red Hat 的建議策略。



# Multi Hybrid Cloud 的挑戰

# 多雲應用的挑戰

## 路由

保證統一訪問入口，  
但根據為置優化  
hops，並管理地理  
中斷

## 應用設計

雙活是一個需求。  
需處理複雜的應用  
模式，像是實時傳  
播、排序、全域共  
享上下文等

## 通訊安全

以最小的應用成本  
確保零信任安全。  
位置需理想的透明  
化

## 上線流程

避免配置管理災難：  
讓事情盡可能的簡  
化，同步叢集狀態



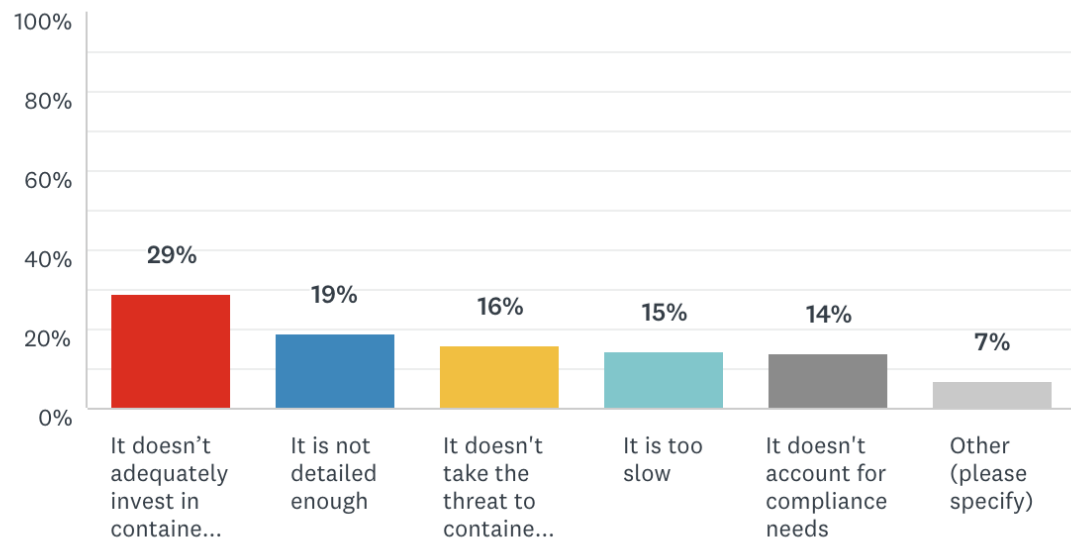
# 多雲的挑戰 – 管理

## 如何跨環境執行標準化和整合關鍵功能？



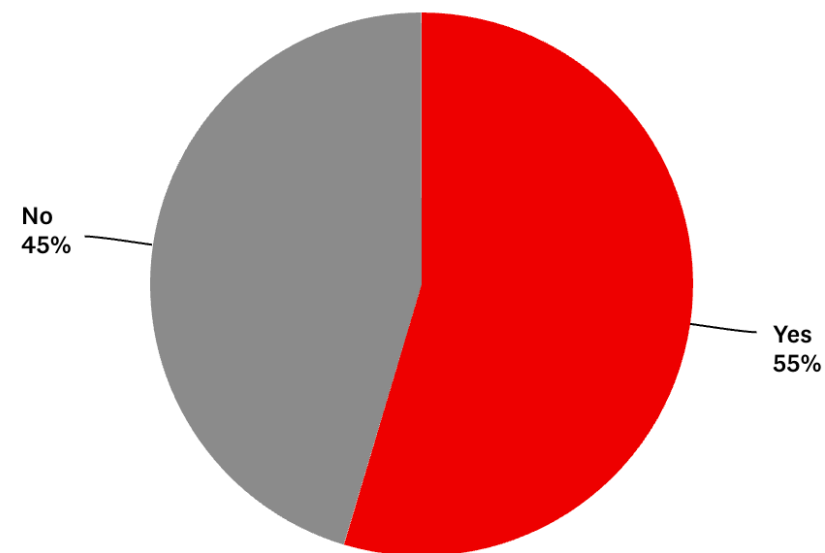
# 多雲的挑戰 – 安全

What is your biggest concern about your company's container strategy?



|  |     |
|--|-----|
| ▼ It doesn't adequately invest in container security | 29% |
| ▼ It is not detailed enough                          | 19% |
| ▼ It doesn't take the threat to containers seriously | 16% |
| ▼ It is too slow                                     | 15% |
| ▼ It doesn't account for compliance needs            | 14% |
| ▼ Other (please specify)                             | 7%  |

Have you ever delayed or slowed down application deployment into production due to container or Kubernetes security concerns?



# 多混合雲兩大門神 - ACM

# 一致的多叢集管理

The screenshot displays the Red Hat Advanced Cluster Management for Kubernetes interface. The top navigation bar includes the Red Hat logo and the text "Advanced Cluster Management for Kubernetes". The main content area is divided into several sections:

- Overview:** A dashboard showing cluster counts for different providers: Google (3 Clusters), Amazon (5 Clusters), Microsoft (1 Cluster), and IBM (1 Cluster).
- Summary:** A section showing 4 Applications.
- Cluster compliance:** A donut chart indicating 63% compliance, with 120 compliant and 69 non-compliant clusters.
- Cluster management:** A detailed table listing clusters with columns for Name, Status, Provider, Distribution, Labels, and Nodes.

| Name                    | Status | Provider              | Distribution                       | Labels  | Nodes |
|-------------------------|--------|-----------------------|------------------------------------|---|-------|
| foxtrot-gcp-europe      | Ready  | Google Cloud Platform | OpenShift 4.6.16 Upgrade available | apps.pacman=deployed apps.ship-tracker=deployed region=europe-west3 +4  | 6     |
| foxtrot-us-west-1       | Ready  | Amazon Web Services   | OpenShift 4.6.16 Upgrade available | apps.pacman=deployed apps.ship-tracker=deployed enforceSecureImages=true region=us-west-1 +4                      | 6     |
| foxtrot-whiskey         | Ready  | Amazon Web Services   | OpenShift 4.6.16 Upgrade available | apps.ship-tracker=deployed enforceSecureImages=true purpose=production region=us-east-1 shipcommander=deployed +4 | 6     |
| local-cluster           | Ready  | Amazon Web Services   | OpenShift 4.6.9 Upgrade available  | local-cluster=true +6   | 13    |
| sberens-aro-central     | Ready  | Microsoft Azure       | OpenShift 4.5.30                   | +4  | 6     |
| sberens-eks-west        | Ready  | Amazon Web Services   | v1.18.9-eks-d1db3c                 | +3  | 2     |
| sberens-gke-central     | Ready  | Google Cloud Platform | v1.18.12-gke.1206                  | +3  | 3     |
| sberens-osd-gcp-central | Ready  | Google Cloud Platform | OpenShift 4.6.17                   | +4  | 7     |
| sberens-roks-south      | Ready  | IBM Cloud             | OpenShift 4.5.24                   | region=us-south-1 +4  | 3     |
| sberens-rosa-west       | Ready  | Amazon Web Services   | OpenShift 4.6.16 Upgrade available | region=us-west-1 +4   | 7     |

- 統一的叢集生命週期管理
- 跨域休眠或恢復叢集
- 配置從集池以簡化管理
- 跨域查詢或修改任何資源
- 快速排查及解決問題

# 基於策略的監管、風控和合規

Governance

Refresh every 10s   
 Last update: 1:50:36 PM   
 Create policy

|                             |                            |  |
|-----------------------------|----------------------------|--|
| NIST SP 800-53              | NIST-CSF                   | HIPAA  |
| 1 / 1<br>Cluster violations | 1 / 2<br>Policy violations | 1 / 6<br>Cluster violations  |
| 1 / 2<br>Policy violations  | 1 / 2<br>Policy violations | No violations found<br>Based on the industry standards, there are no cluster or policy violations. |
| NIST 800-53                 | PCI                        |  |

Create policy

All fields marked with an asterisk (\*) are mandatory.

Name \*   
 policy-gatekeeper-operator

Namespace \*   
 The namespace to create and store the policy on the hub cluster.

Specifications \*   
 Custom specifications x Custom specifications

Cluster selector   
 environment: "dev" x environment: "dev"

Standards   
 NIST SP 800-53 x NIST SP 800-53

Categories   
 CM Configuration Ma... x CM Configuration Management

Controls   
 CM-2 Baseline Config... x CM-2 Baseline Configuration

Remediation \*   
  Inform - Reports the violation, which requires manual remediation.   
  Enforce - Automatically runs remediation action that is defined in the source, if this feature is supported.

Disable policy   
  Disabled

```
28   apiVersion: operators.coreos.com/v1alpha1
29   kind: Subscription
30   metadata:
31     name: gatekeeper-operator-product
32     namespace: openshift-operators
33   spec:
34     channel: stable
35     installPlanApproval: Automatic
36     name: gatekeeper-operator-product
37     source: redhat-operators
38     sourceNamespace: openshift-marketplace
39 - objectDefinition:
40   apiVersion: policy.open-cluster-management.io/v1
41   kind: ConfigurationPolicy
42   metadata:
43     name: gatekeeper
44   spec:
45     remediationAction: Inform
46     severity: high
47   object-templates:
48     - complianceType: musthave
49     objectDefinition:
50       apiVersion: operator.gatekeeper.sh/v1alpha1
51       kind: Gatekeeper
52       metadata:
53         name: gatekeeper
54       spec:
55         audit:
56           logLevel: INFO
57           replicas: 1
58         image:
59           image: "registry.redhat.io/rhacm2/gatekeeper-rhel8-v3.3.0"
60         validatingWebhook: Enabled
61         mutatingWebhook: Disabled
62         webhook:
63           emitAdmissionEvents: Enabled
64           logLevel: INFO
65           replicas: 2
66
67   apiVersion: policy.open-cluster-management.io/v1
68   kind: PlacementBinding
69   metadata:
70     name: binding-policy-gatekeeper-operator
71   placementRef:
72     name: placement-policy-gatekeeper-operator
73     kind: PlacementRule
74   apiGroup: apps.open-cluster-management.io
75   subjects:
76     - name: policy-gatekeeper-operator
77       kind: Policy
78     apiGroup: policy.open-cluster-management.io
79
80   apiVersion: apps.open-cluster-management.io/v1
81   kind: PlacementRule
82   metadata:
83     name: placement-policy-gatekeeper-operator
84   spec:
85     clusterConditions:
86       - status: "True"
87       type: ManagedClusterConditionAvailable
88     clusterSelector:
89       matchExpressions:
90         - key: environment, operator: In, values: ["dev"]
```

- 集中執行應用、安全、基礎設施規範
- 可視化配置稽核
- 透過 Ansible Automation Platform 執行自動化補救措施
- 內建合規策略和稽核檢查，並整合 GitOps
- 可視化合規狀況

# 簡化的多叢集應用生命週期管理

The screenshot displays the OpenShift console interface. On the left, the 'Create an application' form is visible, with fields for Name (newapp) and Namespace (default). Below this, the 'Repository location for resources' section shows 'Git' as the selected repository type, with a URL, branch (master), and path (.s2i) specified. The 'Reconcile option' is set to 'merge'. On the right, the 'Application YAML' editor shows the configuration for a Subscription, including matchExpressions and componentKinds. Below the form, the 'Resource topology' view shows a hierarchical diagram of resources. At the top is the 'Application' (pacman-app), which is linked to a 'Subscription' (pacman-app). The Subscription is linked to 'Placements' (pacman-dev-clusters), which are linked to a 'Cluster' (foxrot-gcp-us-west-1). The Cluster is linked to various resources: 'Service mongo', 'Route fs-gsb-pacman', 'Route pacman', 'Deployment mongo', 'PersistentVolumeClaim mongo-storage', 'Deployment pacman', 'Service pacman', 'Replicaset mongo', and 'Replicaset pacman'. On the far right, a 'Cluster' details panel shows information for 'foxrot-gcp-europe' and 'foxrot-us-west-1', including namespace, status, CPU, and memory usage.

- 快速簡易的部署應用
- 多來源部署 (GIT / HELM / Object Storage)
- 整合 OpenShift GitOps (Argo CD).
- 自動化檢測並可視化 Argo CD 應用
- 可視化跨集群的應用關係

# OpenShift GitOps/ArgoCD ApplicationSets

直接從介面即可定義和管理 ArgoCD

ApplicationSet

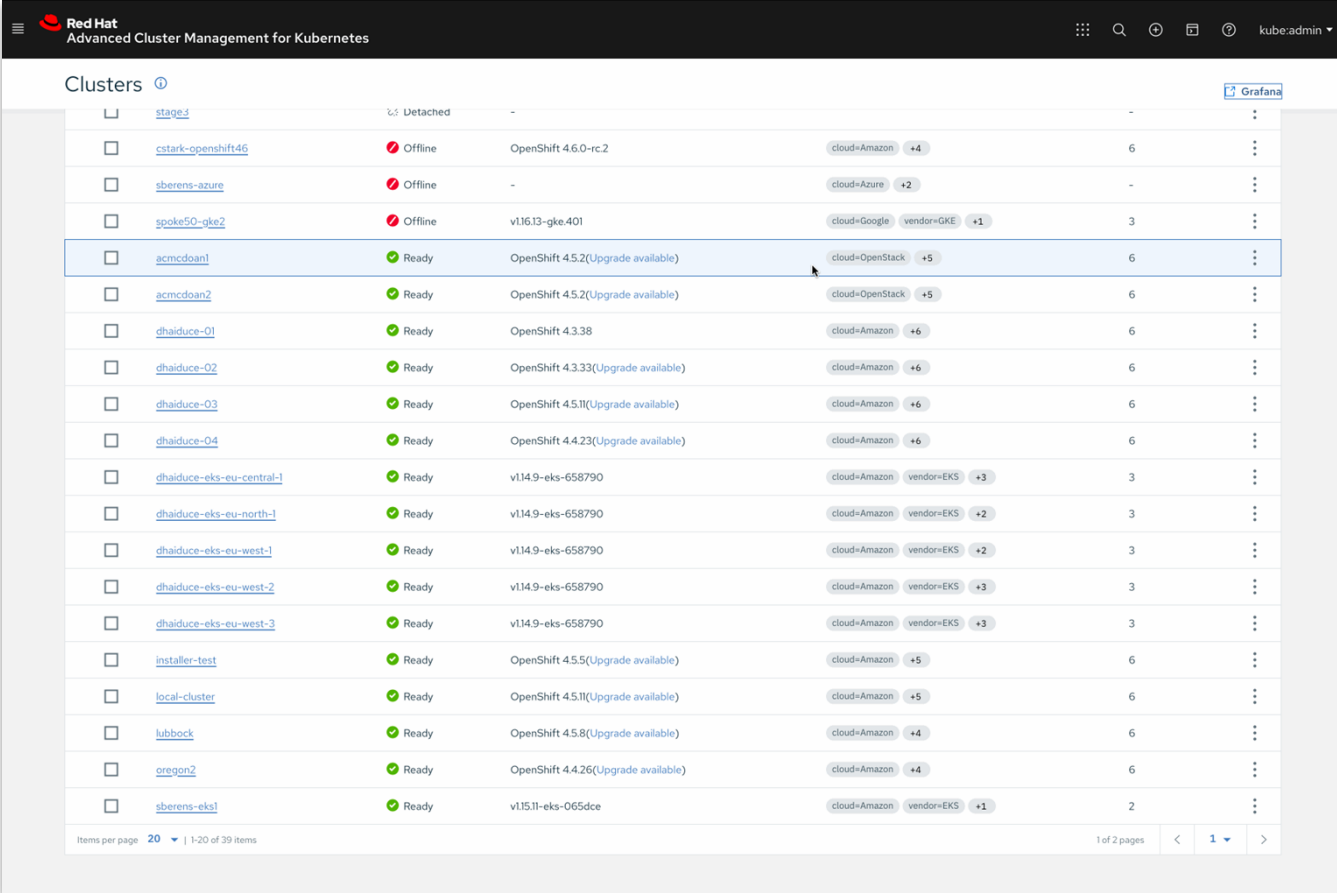
允許非特特權叢集使用者部署 ArgoCD

應用，而無須叢集管理員介入

The image displays two screenshots of the Red Hat Advanced Cluster Management for Kubernetes console. The top screenshot shows the 'Applications' overview page. A red box highlights the 'Create application' button, and another red box highlights the 'Argo CD ApplicationSet' option in the dropdown menu, which is marked as a 'Technology Preview'. The bottom screenshot shows the 'engineering-dev-guestbook' application details page. A red box highlights the 'Launch Argo editor', 'View application set', 'Search resource', and 'Search all related applications' links.

# 多叢集的可視化能力

- 開箱即用的全域查詢視圖，以及構建客製查詢的能力
- 集中告警和通知，並轉發到第三方系統 (PagerDuty / Slack)
- 專注於叢集管理的集中資料庫
- 觀察指標趨勢、警報模式、支持物件儲存

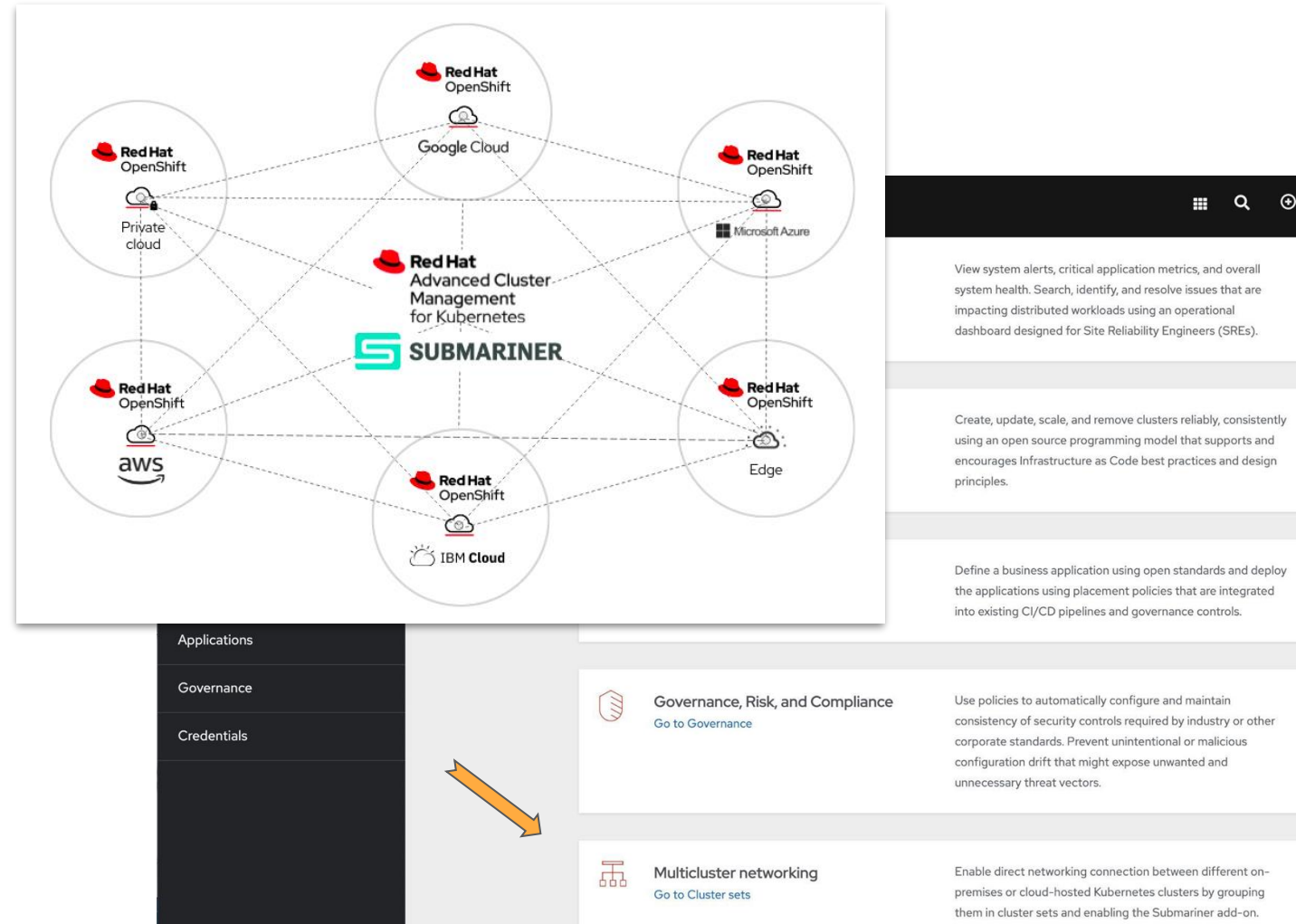


| Cluster Name              | Status   | Version                             | Cloud Provider             | Nodes |
|---------------------------|----------|-------------------------------------|----------------------------|-------|
| stage4                    | Detached | -                                   | -                          | -     |
| cstark-openshift46        | Offline  | OpenShift 4.6.0-rc.2                | cloud=Amazon +4            | 6     |
| sberens-azure             | Offline  | -                                   | cloud=Azure +2             | -     |
| spoke50-gke2              | Offline  | v1.16.13-gke-401                    | cloud=Google vendor=GKE +1 | 3     |
| acmcdon1                  | Ready    | OpenShift 4.5.2(Upgrade available)  | cloud=OpenStack +5         | 6     |
| acmcdon2                  | Ready    | OpenShift 4.5.2(Upgrade available)  | cloud=OpenStack +5         | 6     |
| dhaiduce-01               | Ready    | OpenShift 4.3.38                    | cloud=Amazon +6            | 6     |
| dhaiduce-02               | Ready    | OpenShift 4.3.33(Upgrade available) | cloud=Amazon +6            | 6     |
| dhaiduce-03               | Ready    | OpenShift 4.5.11(Upgrade available) | cloud=Amazon +6            | 6     |
| dhaiduce-04               | Ready    | OpenShift 4.4.23(Upgrade available) | cloud=Amazon +6            | 6     |
| dhaiduce-eks-eu-central-1 | Ready    | v1.14.9-eks-658790                  | cloud=Amazon vendor=EKS +3 | 3     |
| dhaiduce-eks-eu-north-1   | Ready    | v1.14.9-eks-658790                  | cloud=Amazon vendor=EKS +2 | 3     |
| dhaiduce-eks-eu-west-1    | Ready    | v1.14.9-eks-658790                  | cloud=Amazon vendor=EKS +2 | 3     |
| dhaiduce-eks-eu-west-2    | Ready    | v1.14.9-eks-658790                  | cloud=Amazon vendor=EKS +3 | 3     |
| dhaiduce-eks-eu-west-3    | Ready    | v1.14.9-eks-658790                  | cloud=Amazon vendor=EKS +3 | 3     |
| installer-test            | Ready    | OpenShift 4.5.5(Upgrade available)  | cloud=Amazon +5            | 6     |
| local-cluster             | Ready    | OpenShift 4.5.11(Upgrade available) | cloud=Amazon +5            | 6     |
| lubbock                   | Ready    | OpenShift 4.5.8(Upgrade available)  | cloud=Amazon +4            | 6     |
| oregon2                   | Ready    | OpenShift 4.4.26(Upgrade available) | cloud=Amazon +4            | 6     |
| sberens-eks1              | Ready    | v1.15.11-eks-065dce                 | cloud=Amazon vendor=EKS +1 | 2     |



# 多叢集網路

- 整合 Submariner
- 實現不同叢集間 Pod 間的網路直接溝通即服務發現能力
- 利用 Cluster Sets 共享
- Globalnet – 支持重疊的 CIDRs
- 其他叢集網路整合能力



# ACM 解決多叢集管理問題

Red Hat OpenShift and Red Hat Advanced Cluster Management for Kubernetes



從開發到生產  
的加速



提供應用的可  
用性



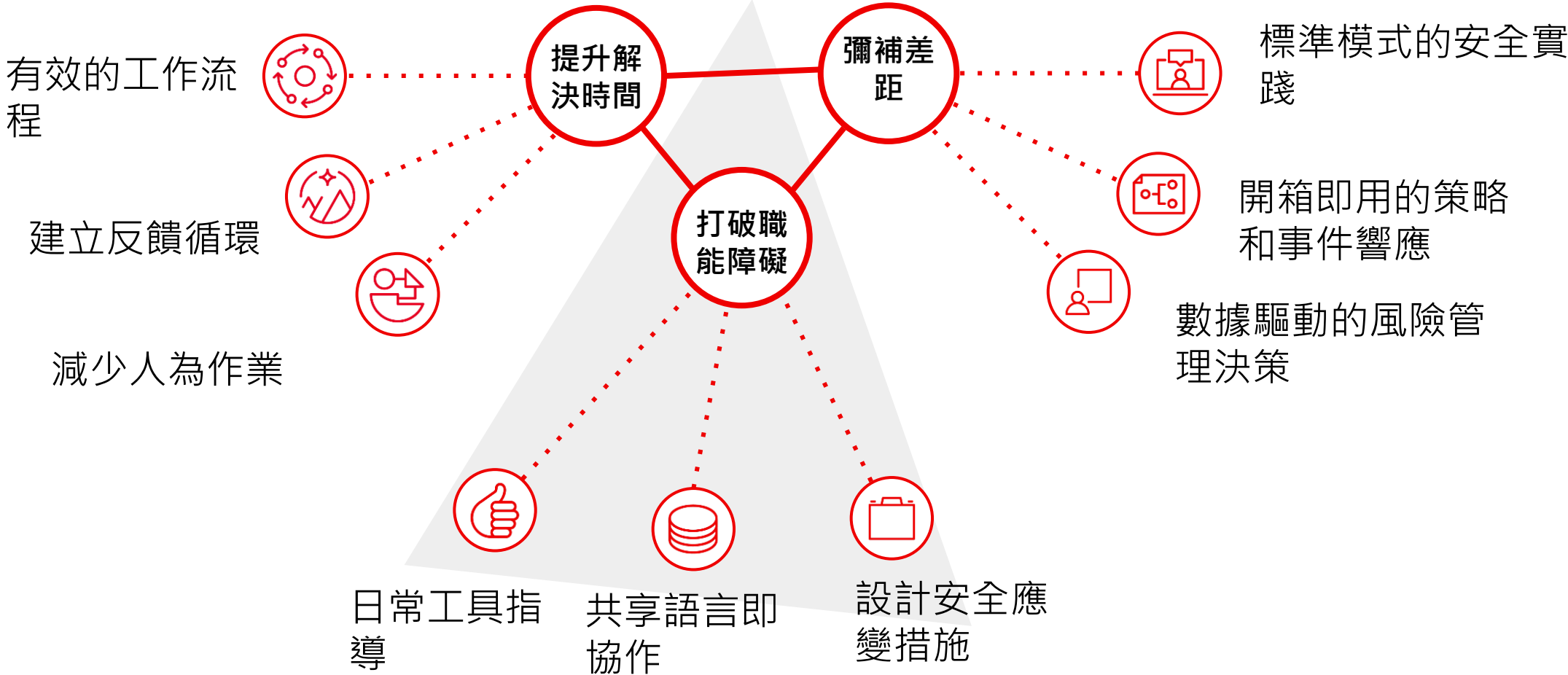
減少成本



簡化合規

# 多混合雲兩大門神 - ACS

# 安全如何和快速開發融合



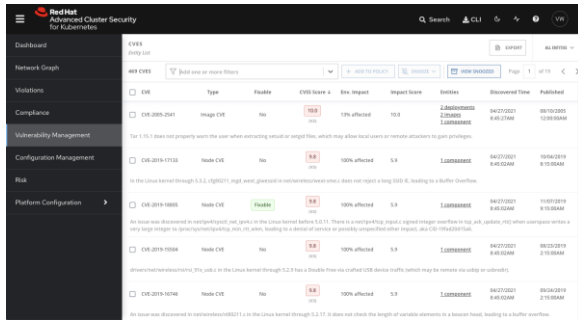
提供上述屬性的安全計劃容易成功

# Kubernetes 原生的安全模式

Shift left

供應鏈安全

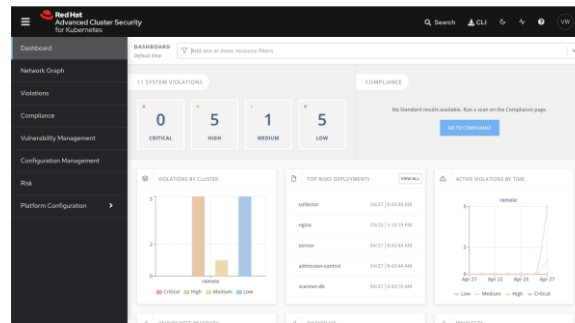
將掃描和合規延伸到開發  
供應鏈 (DevSecOps)



Kubernetes security  
posture management  
(KSPM)

基礎設施安全

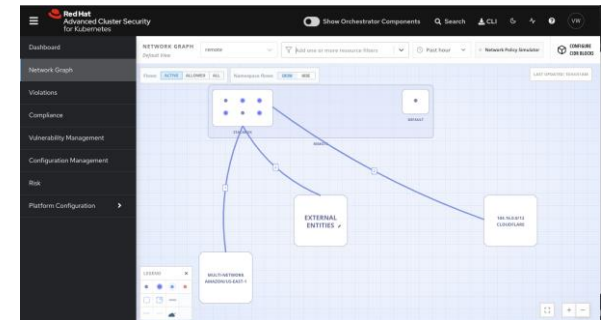
利用內建的 Kubernetes 安  
全狀態管理來識別和修復系  
統配置及應用部署



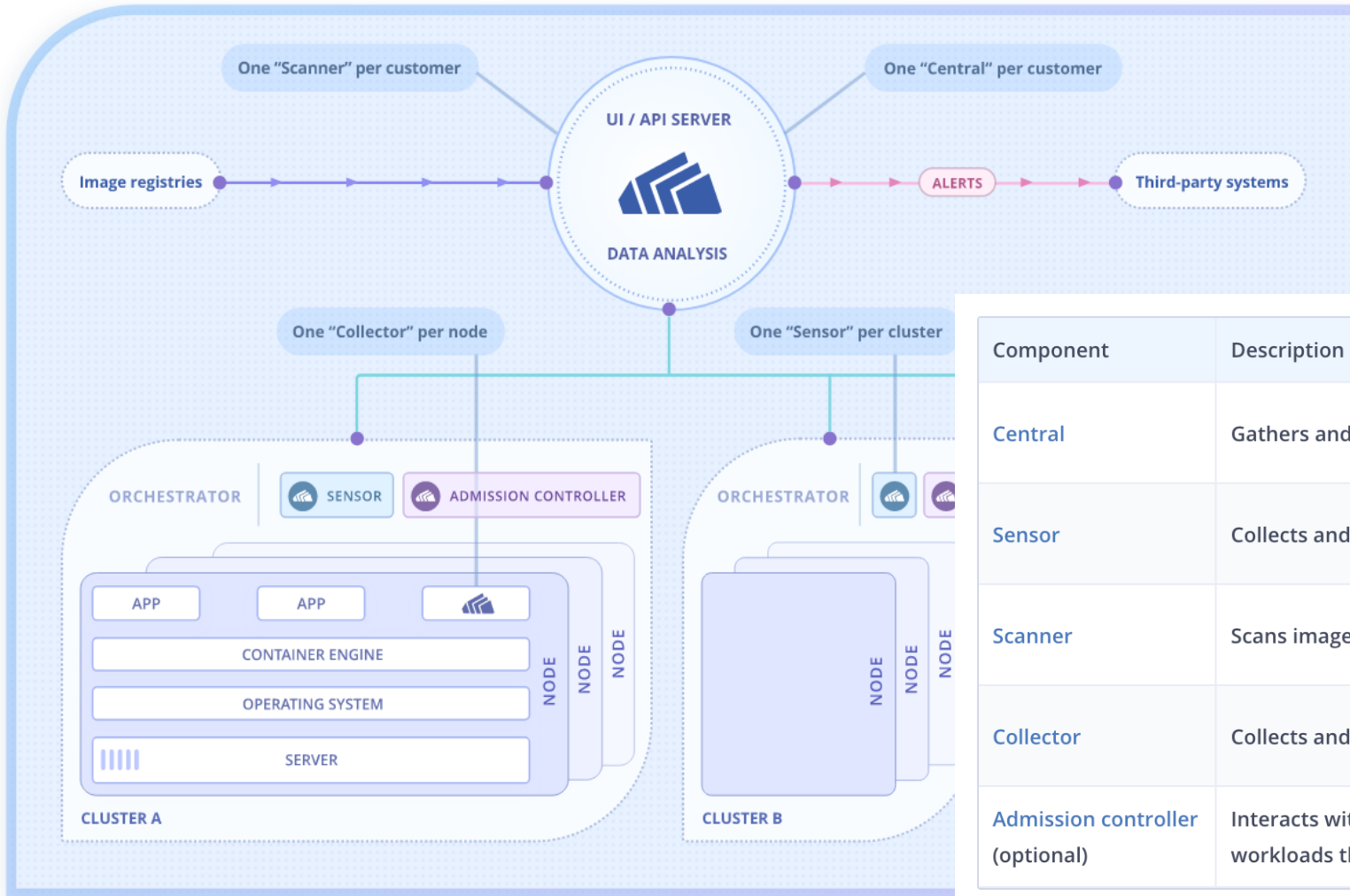
Cloud workload  
protection (CWPP)

工作負載安全

維護和實施「零信任執行」  
方法來保護工作負載



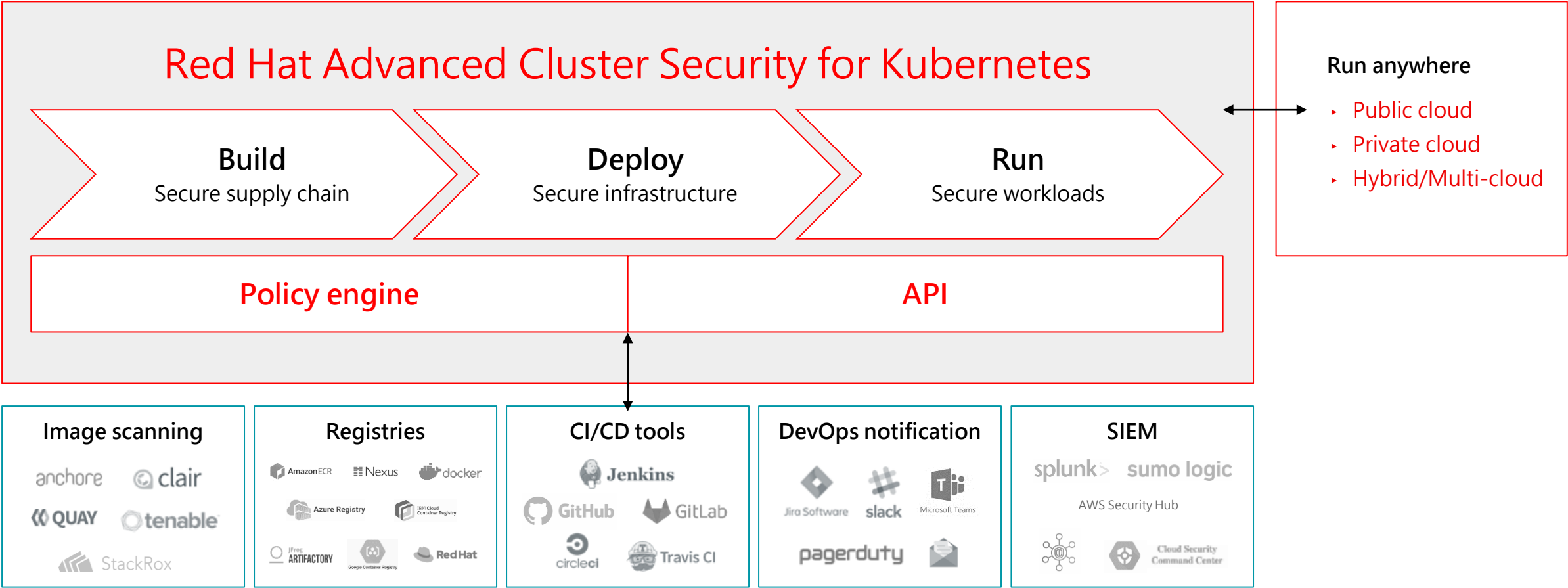
# 統一多叢集的安控平台



- ▶ RHACS 以容器的方式部署在 OpenShift 叢集中
- ▶ 可透過 Helm charts 或 OpenShift Operator 部署

| Component                       | Description  | Quantity                 |
|---------------------------------|--|--------------------------|
| Central                         | Gathers and displays information from other components.  | 1 for multiple clusters. |
| Sensor                          | Collects and augments data from the Collector.   | 1 for each cluster.      |
| Scanner                         | Scans images for vulnerabilities.  | 1 for multiple clusters. |
| Collector                       | Collects and monitors container activities.  | 1 on each node.          |
| Admission controller (optional) | Interacts with Kubernetes API server and prevents creating workloads that don't adhere to security policies. | 1 for each cluster.      |

# DevSecOps 的整合能力



# 一站式多叢集安全

**Red Hat Advanced Cluster Security for Kubernetes**

Dashboard Overview:

- 421 SYSTEM VIOLATIONS
- 0 CRITICAL, 40 HIGH, 184 MEDIUM, 197 LOW
- COMPLIANCE: CIS Docker v1.2.0 (100%), CIS Kubernetes v1.5 (100%), NIST SP 800-190 (100%), NIST SP 800-53 (100%), PCI DSS 3.2.1 (100%)
- VIOLATIONS BY CLUSTER: production
- TOP RISKY DEPLOYMENTS

**Red Hat Advanced Cluster Security for Kubernetes**

Configuration Management:

- 43 POLICIES, 219 CONTROLS, APPLICATION & INFRASTRUCTURE, RBAC VISIBILITY & CONFIGURATION
- POLICY VIOLATIONS BY SEVERITY: 2 Labeled as High, 3 Labeled as Medium, 1 Labeled as Low, 12 policies without violations
- CIS DOCKER V1.2.0: 1 Control Failing, 8 Controls Failing, 16 Controls N/A

**Red Hat Advanced Cluster Security for Kubernetes**

Network Graph:

- production cluster
- Network Policy Simulator
- Network Analysts Tools

**Red Hat Advanced Cluster Security for Kubernetes**

101 DEPLOYMENTS

| Name              | Created                 | Cluster    | Namespace     | Priority |
|-------------------|-------------------------|------------|---------------|----------|
| mangodb           | 11/17/2020   8:43:41PM  | production | psname        | 1        |
| access            | 11/27/2020   10:59:59AM | production | ssd           | 3        |
| ssd               | 09/21/2020   3:32:29PM  | production | ssdemo        | 5        |
| access-postgresql | 11/27/2020   11:00:00AM | production | ssd           | 6        |
| ssd-mysql         | 09/21/2020   3:32:29PM  | production | ssdemo        | 6        |
| pathfinder-server | 05/18/2021   4:07:41PM  | production | mg-pathfinder | 7        |

**Red Hat Advanced Cluster Security for Kubernetes**

77 POLICIES

| Name            | Created   | Cluster       | Namespace | Priority |
|-----------------|---|---------------|-----------|----------|
| Kubernetes      | Alerts when Kubernetes resource is controlled in container  | Runtime       | Medium    | High     |
| Access          | Alerts when Kubernetes API receives port forward request to ingress                                   | Runtime       | Medium    | High     |
| KubernetesAlert | Alert on the presence of dashboard the Kubernetes dashboard deployed                                  | Deploy        | Low       | High     |
| Labels          | Alert on deployments with missing or no 'label'   | Build, Deploy | Low       | High     |
| Labels          | Alert when the 'selector' or 'grouped' label is missing, which can be used to add a new label group   | Runtime       | High      | High     |
| Labels          | Denies when the 'selector' or 'selector' label is missing, which can be used to add a new label group | Runtime       | High      | High     |
| Labels          | Alert on deployments with volume mount on docker socket   | Deploy        | Medium    | High     |
| Labels          | Processes that indicate high-privilege  | Runtime       | High      | High     |
| Mount           | Alert on deployments with volume mount on docker socket   | Deploy        | Medium    | High     |

Enforcement Behavior:

- BUILD:** If enabled, Stackrox will fail your CI builds when images match the conditions of this policy. Download the CLI above to get started.
- DEPLOY:** If enabled, Stackrox will automatically block creation of deployments that match the conditions of this policy. In clusters with the Stackrox Admission Controller enabled, the Kubernetes API server will block noncompliant deployments. In other clusters, Stackrox will edit noncompliant deployments to prevent pods from being scheduled.
- RUNTIME:** If enabled, Stackrox will either kill the offending pod or block the action taken on the pod. Executions within a pod that match the conditions of the policy will result in the pod being killed. Actions taken through the API server that match policy criteria will be blocked.

**Red Hat Advanced Cluster Security for Kubernetes**

77 POLICIES

Network Analysts Tools:

- Enforcement Behavior: BUILD, DEPLOY, RUNTIME

**Red Hat Advanced Cluster Security for Kubernetes**

COMPLIANCE

PASSING STANDARDS ACROSS CLUSTERS:

- CIS Docker: 100%
- CIS K8s: 75%
- NIST SP 800-190: 20%
- NIST SP 800-53: 40%
- PCI: 10%

PASSING STANDARDS BY CLUSTER:

- production: 100%
- stg: 100%
- dev: 100%

**Red Hat Advanced Cluster Security for Kubernetes**

VULNERABILITY MANAGEMENT

- 8 POLICIES (1 being), 192 CVEs (287 total), 4 NVDs, 265 IMAGES
- TOP RISKY DEPLOYMENTS BY CVE COUNT & CVSS SCORE

**Red Hat Advanced Cluster Security for Kubernetes**

421 VIOLATIONS

| Deployment                | Cluster    | Namespace             | Policy                                     | Enforced | Severity | Categories               | Lifecycle | Time                    |
|---------------------------|------------|-----------------------|--|----------|----------|--------------------------|-----------|-------------------------|
| redhat-operators-grad     | production | openshift-marketplace | No RESOURCE_ATTRIBUTES or LIMITS specified | No       | Medium   | Multiple                 | Deploy    | 05/11/2021   5:25:14PM  |
| karfa-deployment          | production | giuseppe-camel-test   | Red Hat Package Manager ID 33889           | No       | Low      | Security Best Practices  | Deploy    | 05/11/2021   4:54:08PM  |
| community-operators-7g5td | production | openshift-marketplace | No RESOURCE_ATTRIBUTES or LIMITS specified | No       | Medium   | Multiple                 | Deploy    | 05/11/2021   2:28:33PM  |
| community-operators-7g5td | production | openshift-marketplace | Exits CVEs >= 7                            | No       | High     | Vulnerability Management | Deploy    | 05/11/2021   2:28:33PM  |
| community-operators-7g5td | production | openshift-marketplace | Red Hat Package Manager ID 33889           | No       | Low      | Security Best Practices  | Deploy    | 05/11/2021   2:28:33PM  |
| karfa-deployment          | production | giuseppe-camel-test   | Latest ID6                                 | No       | Low      | DevOps Best Practices    | Deploy    | 05/11/2021   10:29:55AM |
| karfa-deployment          | production | giuseppe-camel-test   | No RESOURCE_ATTRIBUTES or LIMITS specified | No       | Medium   | Multiple                 | Deploy    | 05/11/2021   10:29:55AM |
| certified-operators-gtq5  | production | openshift-marketplace | No RESOURCE_ATTRIBUTES or LIMITS specified | No       | Medium   | Multiple                 | Deploy    | 05/10/2021   2:28:33PM  |
| certified-operators-gtq5  | production | openshift-marketplace | Exits CVEs >= 7                            | No       | High     | Vulnerability Management | Deploy    | 05/10/2021   11:39:30PM |
| certified-operators-gtq5  | production | openshift-marketplace | Red Hat Package Manager ID 33889           | No       | Low      | Security Best Practices  | Deploy    | 05/10/2021   11:39:30PM |
| redhat-marketplace        | production | openshift-marketplace | No RESOURCE_ATTRIBUTES                     | No       | Medium   | Multiple                 | Deploy    | 05/10/2021   11:39:30PM |



# ACS 解決多叢集安全問題

Red Hat OpenShift and Red Hat Advanced Cluster Security for Kubernetes



弱點管理



合規



風險分析



安全配置管理



網路分段

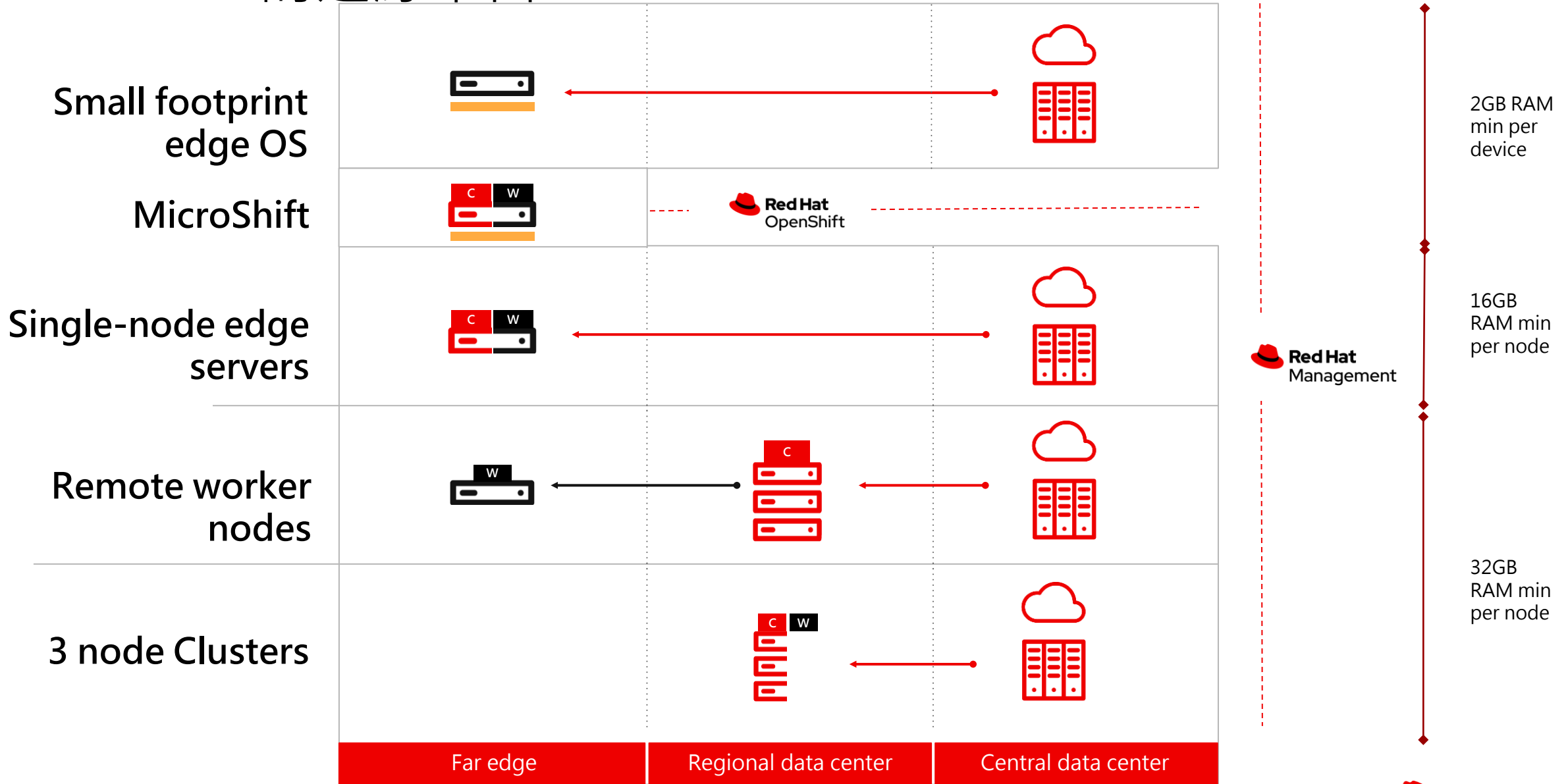


運行檢測和回應

# 多雲的擴展 - Edge

# Red Hat 的邊緣平台

Red Hat Enterprise Linux



← Cluster management and application deployment

← Kubernetes node control

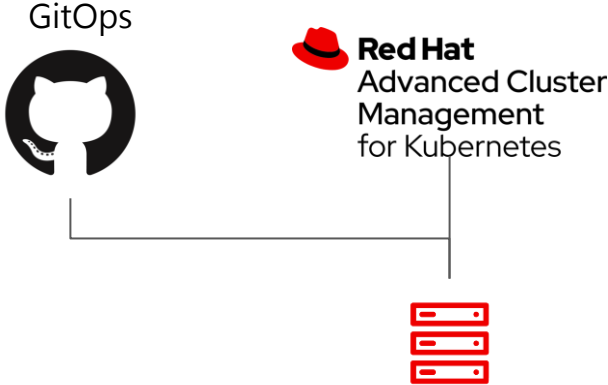
(C) Control node

(W) Worker node

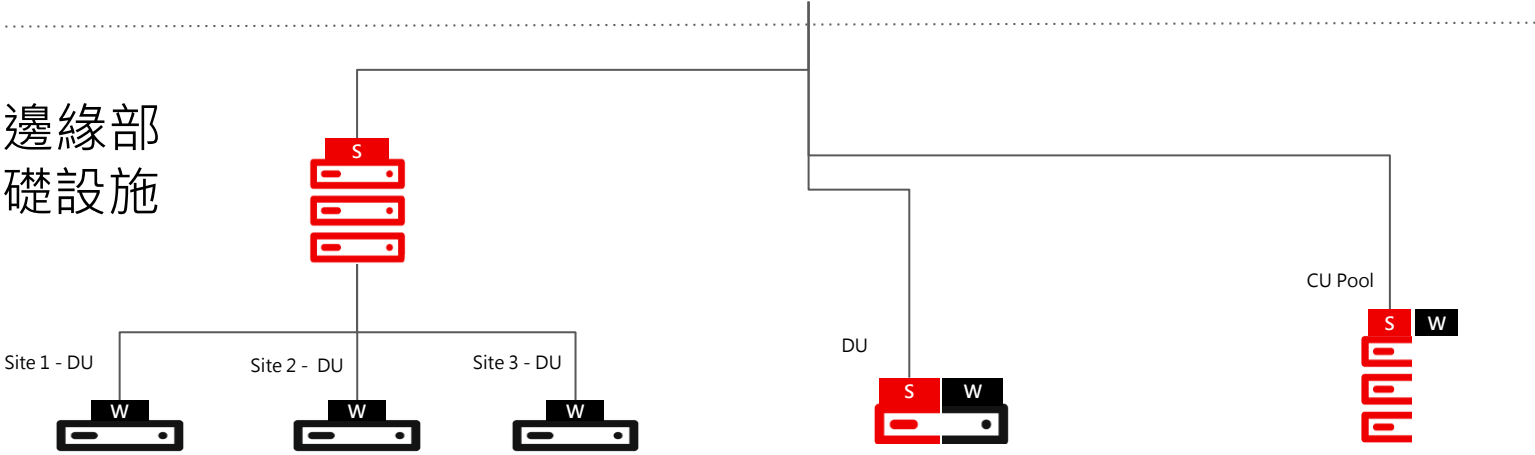
Red Hat

# 邊緣部署

管理中心叢集



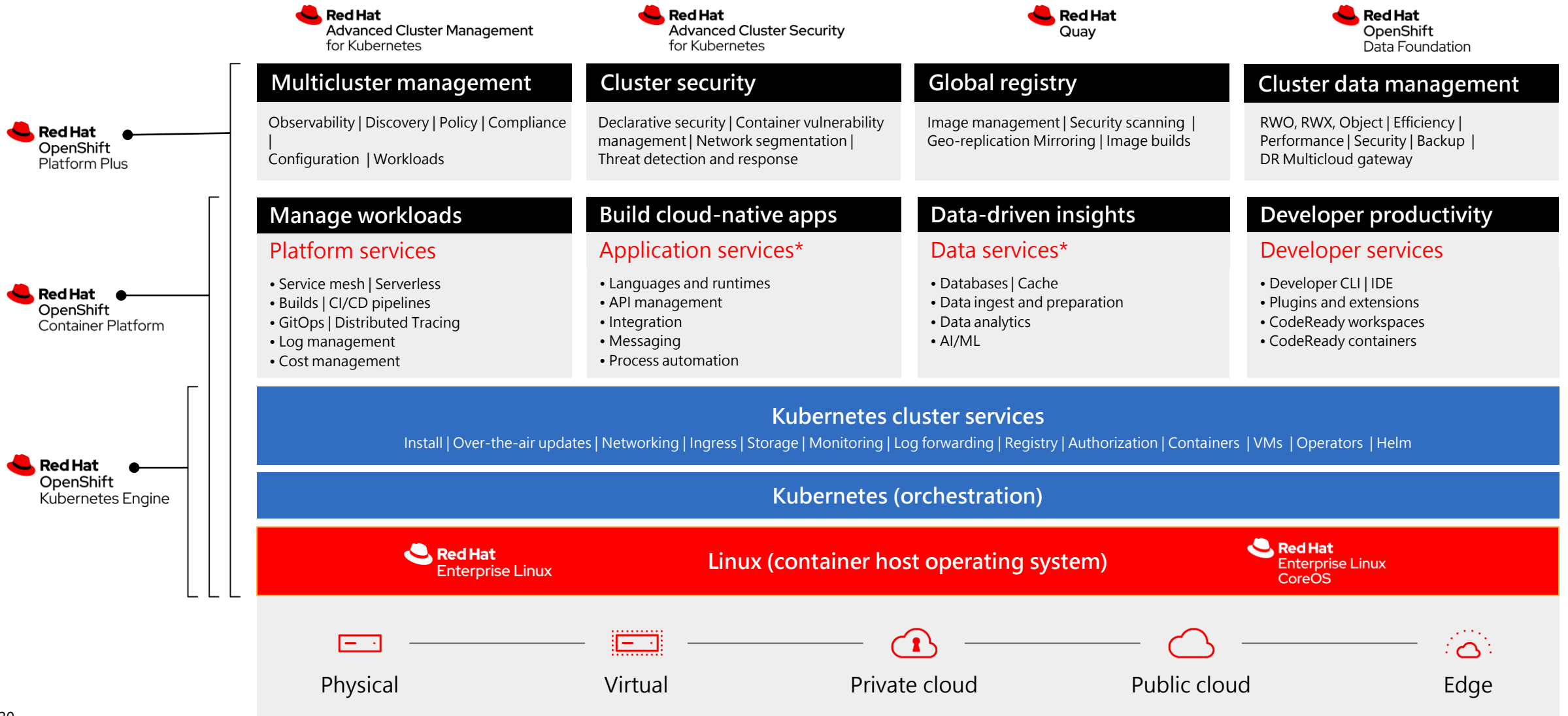
ZTP 邊緣部署基礎設施



ZTP - Zero Touch Provisioning  
DU - Distributed Unit  
CU - Central Unit

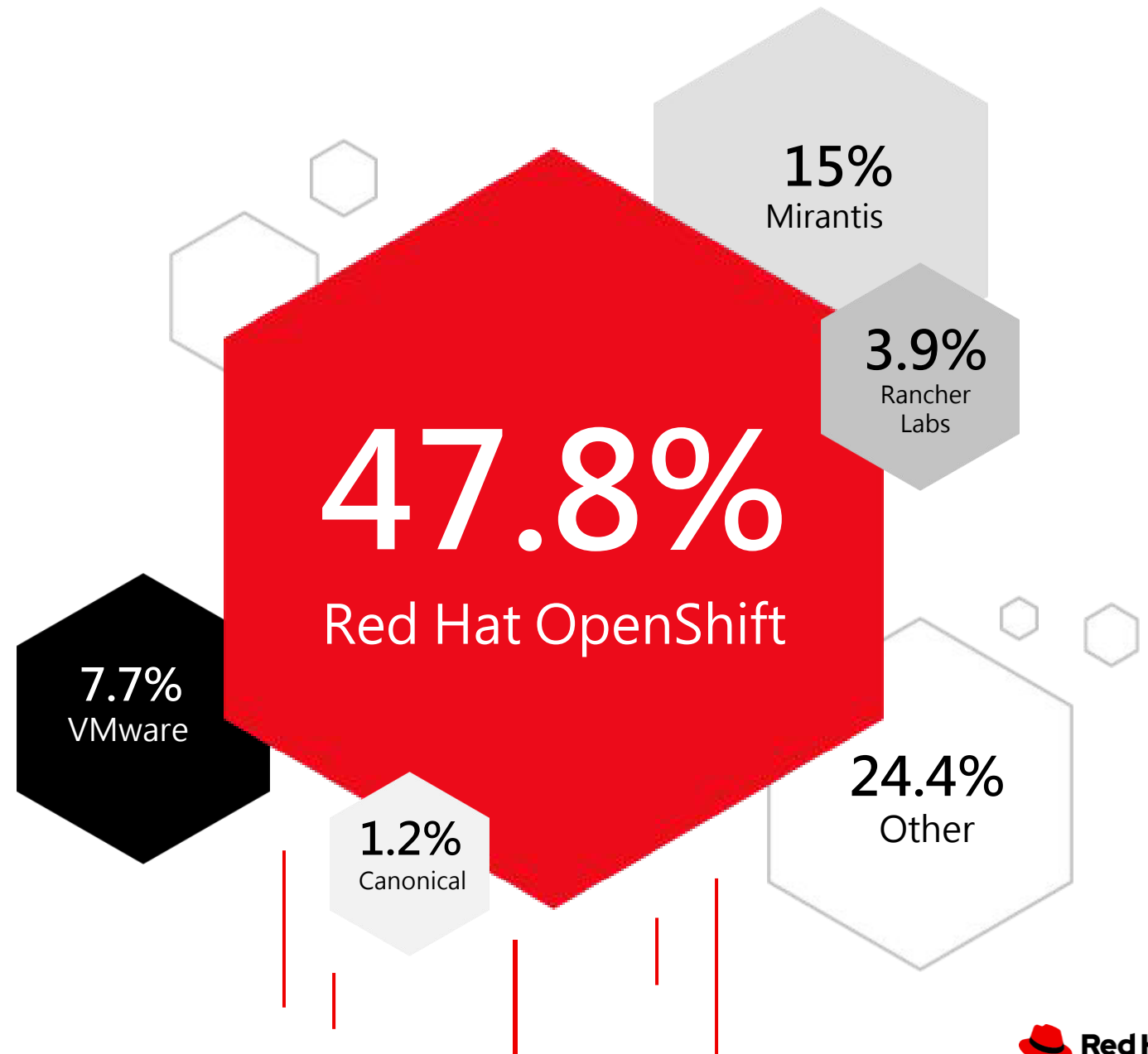
# 總結

# 容器平台導入完整樣貌



# Red Hat OpenShift in container market share

*Source: Who's Winning in the Container Software Market, IT Pro Today, Jun 29, 2021.*



# 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](https://www.linkedin.com/company/red-hat)

 [youtube.com/user/RedHatVideos](https://www.youtube.com/user/RedHatVideos)

 [facebook.com/redhatinc](https://www.facebook.com/redhatinc)

 [twitter.com/RedHat](https://twitter.com/RedHat)