

# 東森購物 Design Workshop Red Hat Advanced Cluster Management

Dawson 2023/10/12

## 議程概要 - Day 1

- Red Hat Advanced Cluster Management 介紹
- 建置規劃與功能探討
  - RHACM Installation
  - RHACM Access Control
  - RHACM Observability Service
  - Multicluster Deployment
- 議程總結



## 議程概要 - Day 2

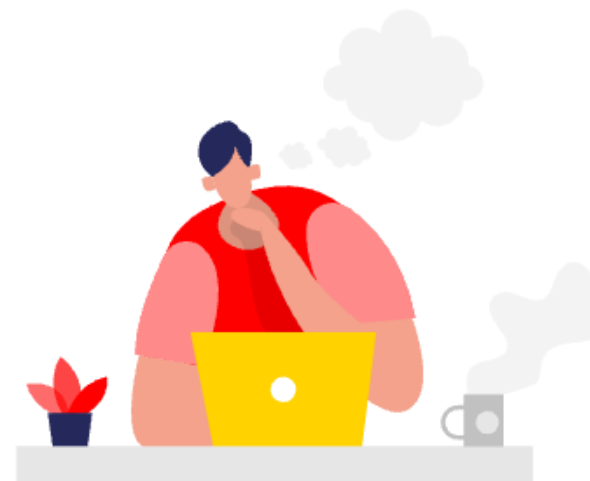
- Red Hat Advanced Cluster Security 介紹
- 建置規劃與功能探討
  - RHACS Installation
  - RHACS Access Control
  - Compliance
  - Vulnerability
  - Prospect of Hybrid Cloud
- 建置方案總結



# Red Hat Advanced Cluster Management

## 多叢集架構可能帶來的困難

- 難以同步設定
- 須對每個 **OCP Cluster** 進行單一操作
- 安全漏洞與稽核困境
- 應用程式上版衝突與版本控制
- 資源偵測難以有統一標準

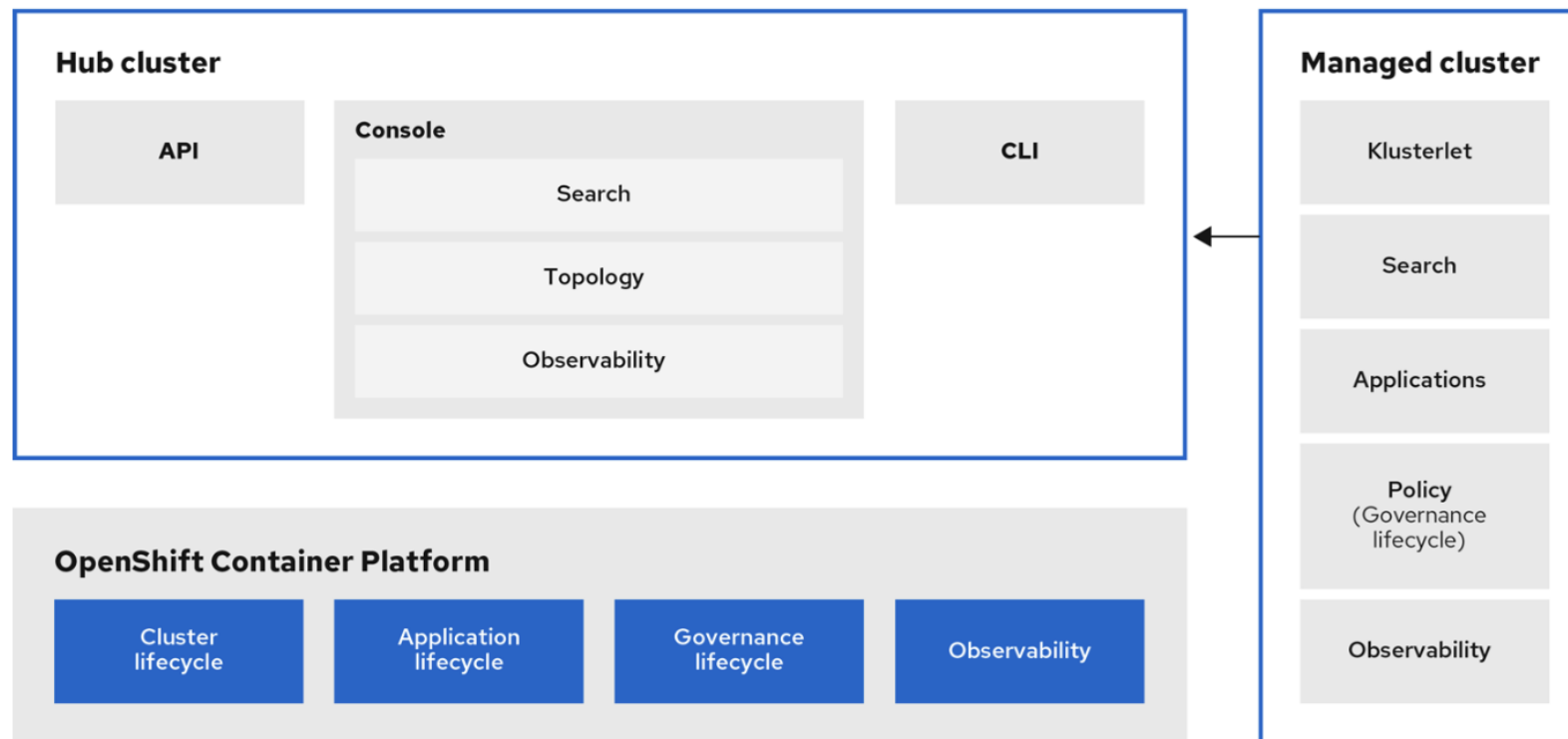


# Red Hat Advanced Cluster Management (RHACM)

- Red Hat 針對 OCP 與 Kubernetes 提供的多叢集管理工具
- 支援公有雲、私有雲與混合雲架構
- 提供使用者網頁介面與 CLI 進行操作
- 對叢集內的成員擁有以下管理功能：
  - 多叢集內 **Cluster** 更新、建立與移除
  - 使用者權限管理
  - 資源監控與管理
  - 應用程式部署
  - 安全性與合規性政策管理

# Red Hat Advanced Cluster Management (RHACM)

RHACM 架構圖示：



# Red Hat Advanced Cluster Management (RHACM)

RHACM 架構分析：

- Hub Cluster
  - 作為 RHACM 的主控點
  - 提供 RHACM API Server 與網頁介面
- Managed Cluster
  - 受管的 OCP Cluster
  - 透過 klusterlet 與 Hub Cluster 進行信息交換



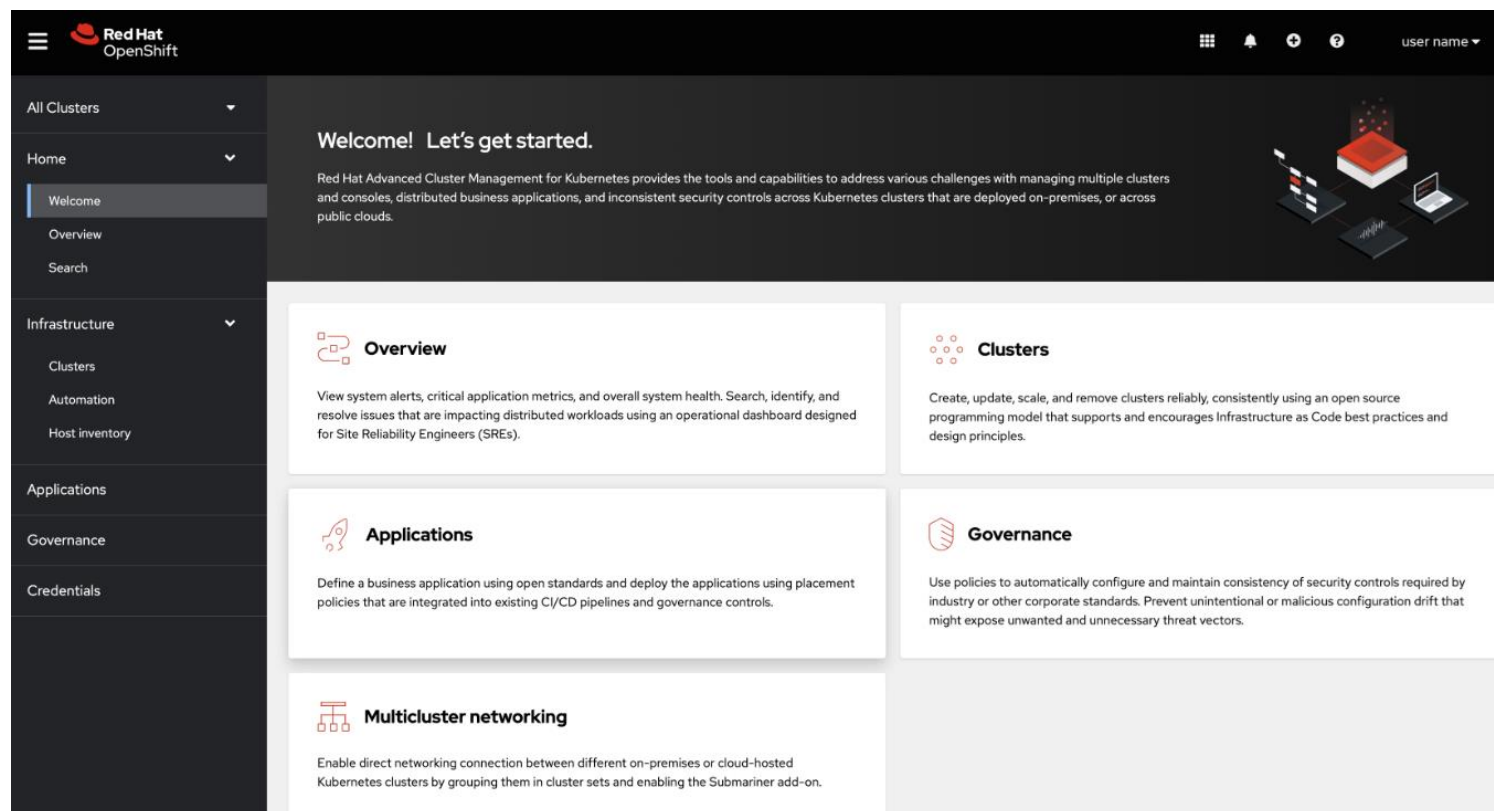
# Red Hat Advanced Cluster Management (RHACM)

RHACM 功能與配置：

- Web Console
- Access Control
- Cluster Management
- Networking
- Applications
- Observability
- Governance
- Add-ons

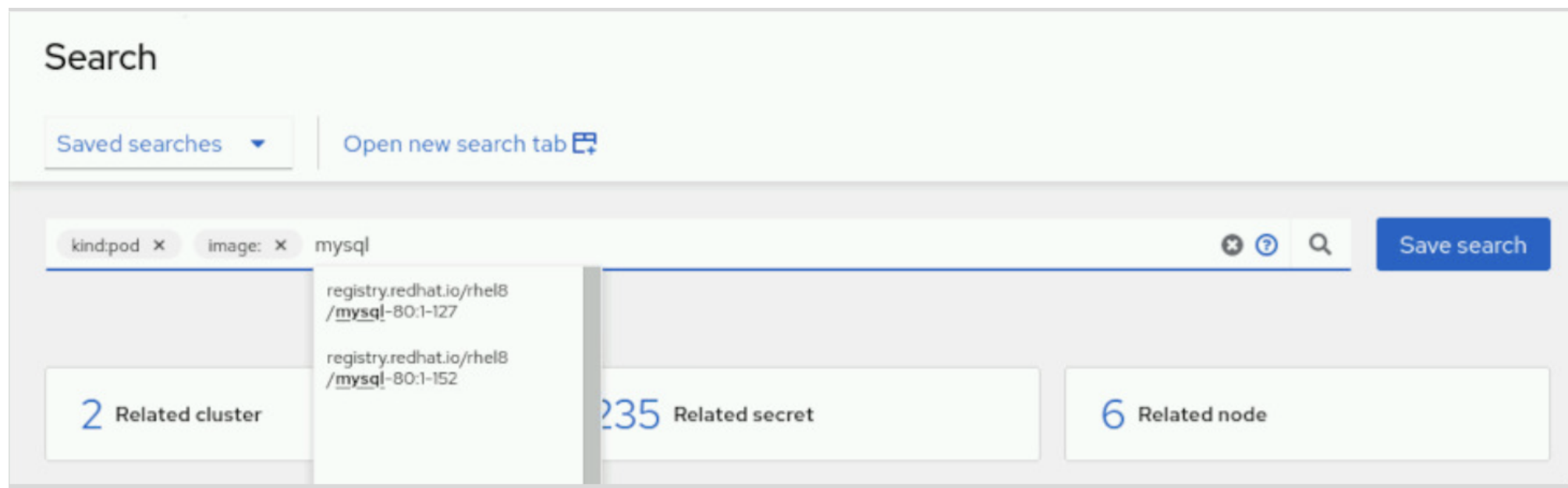
# RHACM Web Console

RHACM 提供網頁操作介面，讓使用者對 OCP 與 Kbernetes 多叢集進行相關功能操作：



# RHACM Web Console

RHACM 擁有 Search Engine，提供使用者在網頁介面進行資源搜索



## RHACM Access Control

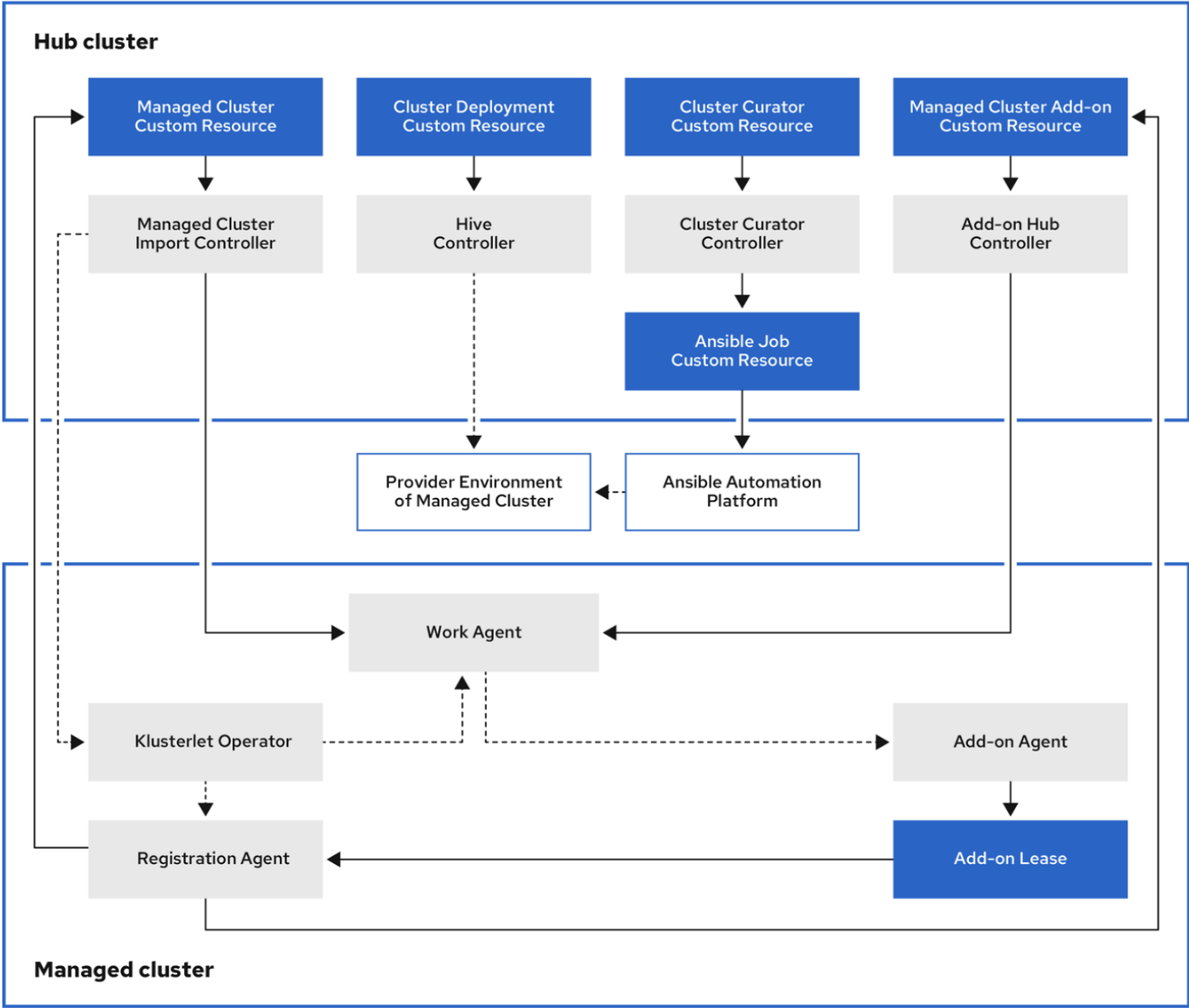
- RHACM 的使用者權限管理與 OCP 雷同
- 透過 Cluster Sets 對 Group 與 User 進行角色劃分
- RHACM 可透過 Cluster Labels 對多個 Cluster 進行相同的 RHACM 權限劃分
- RHACM 透過個別 Cluster 的 OAuth Server 進行登入驗證
- 登入驗證整合 LDAP

# RHACM Access Control

| Role   | Definition   |
|--|--|
| <code>open-cluster-management:cluster-manager-admin</code>                           | RHACM super user, with full access. Can create a <code>ManagedCluster</code> resource.                           |
| <code>open-cluster-management:admin:managed_cluster_name</code>                      | RHACM administrator access to the <code>ManagedCluster</code> resource named <i>managed_cluster_name</i> .       |
| <code>open-cluster-management:view:managed_cluster_name</code>                       | RHACM view access to the <code>ManagedCluster</code> resource named <i>managed_cluster_name</i> .                |
| <code>open-cluster-management:managedclusterset:admin:managed_clusterset_name</code> | RHACM administrator access to the <code>ManagedClusterSet</code> resource named <i>managed_clusterset_name</i> . |
| <code>open-cluster-management:managedclusterset:view:managed_clusterset_name</code>  | RHACM view access to the <code>ManagedClusterSet</code> resource named <i>managed_clusterset_name</i> .          |
| <code>open-cluster-management:subscription-admin</code>                              | Can create Git subscriptions that deploy Kubernetes resources YAML files to multiple namespaces.                 |

# RHACM Cluster Management

- RHACM 整合 **multicluster engine operator** 納管 OCP 與 Kubernetes Cluster :
  - 匯入既有的 **Cluster**
  - 創建與安裝 **Cluster**
  - 移除 **Cluster**，包含所安裝內容
  - 停用 **Cluster**
  - 升級 **Cluster**
  - **Managed Cluster** 節點自動擴展
  - 儲存 **Cluster Credentials**，涵蓋：AWS、Azure、GCP、On-premises ..... 等
  - 與 **Red Hat Ansible Automation Platform** 整合，對節點執行相應任務



# RHACM Cluster Management

- **Cluster 基礎管理**
  - 升級 **Cluster**
  - 查看受管的 **Cluster** 狀態、**Node** 資源量與監控 **Cluster** 資源
- **Managed Cluster 節點自動擴展**，需透過 **Central Infrastructure Management** 實現
  - **Bare Metal 支援**：
    - **Discovery ISO**
    - **iPXE**
    - **BMC form**
    - **Uploading YAML**



# RHACM Cluster Management – Create OCP Cluster

預先準備事項：

- **ACM Cluster Lifecycle** 管理，包含建立、移除、升級，皆須透過 **Multicluster Engine Operator** 進行，**ACM** 安裝時會一起安裝
- 啟用 **Central Infrastructure Management Service**，此服務為 **Multicluster Engine Operator** 提供
- 若安裝標的為 **Bare Metal**，**Hub Cluster** 需安裝 **Bare Metal Operator**
- 需確保 **ACM Hub Cluster** 與 **Managed Cluster** 網路可連通

# RHACM Cluster Management – Create OCP Cluster

建立 OCP Cluster 流程：

1. 定義 ACM Credentials：提供安裝環境的驗證
2. 定義 Release Images：指定 ClusterImageSet 版本，以對應欲安裝的 OCP 版本
3. 建立 ClusterDeployment：Hive 提供的 Cluster 安裝資訊定義檔，可設置主機大小、數量 ..... 等
4. 建立 ClusterPool：Hive 提供的 Multicluster 安裝資訊定義檔，定義以哪個 ClusterDeployment 為安裝範本
5. 定義 ConfigMap：建立額外的欲安裝 OCP Cluster 環境資訊
6. 依據安裝標的環境，繼續流程

# RHACM Cluster Management – Create OCP Cluster

Azure – 建立 OCP Cluster 流程：

7-1. 確保已在 Azure Government 設定 OCP 所需的 Domain

7-2. 至 ACM Web Console > Infrastructure > Clusters

7-3. 確保頁面顯示的 install-config.yaml 所配置的資訊皆正確，Azure region、instance type .....  
等

8. 等待安裝畫面完成，至新安裝的 OCP 登入畫面驗證安裝結果

GCP – 建立 OCP Cluster 流程：

7-1. 確保已在 GCP 設定 OCP 所需的 Domain

7-2. 至 ACM Web Console > Infrastructure > Clusters

7-3. 確保頁面顯示的 install-config.yaml 所配置的資訊皆正確，Azure region、instance type .....  
等



# RHACM Cluster Management – Create OCP Cluster

On-premises – 建立 OCP Cluster 流程：

7-1. 定義 Infrastructure Environment：定義 ISO 與欲安裝主機的連線環境資訊

7-2. 至 ACM Web Console > Infrastructure > Clusters

7-3. 在 Host inventory 選擇欲安裝的 Hosts

7-4. 指定安裝版本與 Cluster 安裝資訊

7-5. 將 ISO 掛在至欲安裝的主機下並啟動

8. 等待安裝畫面完成，至新安裝的 OCP 登入畫面驗證安裝結果

# RHACM Networking

## Hub Cluster 網路設定：

| Direction | Protocol | Port                         | Destination     | Connection  |
|-----------|----------|------------------------------|-----------------|---|
| Outbound  | HTTPS    | 443                          | Managed Cluster | Search Engine 使用                                    |
| Outbound  | HTTPS    | 6443                         | Managed Cluster | 用於聯繫 Managed Cluster API Server                     |
| Outbound  | HTTPS    | 443                          | Channel Source  | 用於聯繫 Channel Source，包含：GitLab、GitOps Server ..... 等 |
| Inbound   | HTTPS    | 443                          | Managed Cluster | Managed Cluster 回傳 Metrics、Alerts 等訊息使用             |
| Inbound   | HTTPS    | 6443                         | Managed Cluster | Managed Cluster 用於觀察 Hub Cluster 變更使用               |
| Outbound  | HTTPS    | 443                          | ObjectStore     | 存儲 Observability 數據                                 |
| Outbound  | HTTPS    | 443                          | ImageRegistry   | 訪問 Image Registry（Quay）使用                           |
| Inbound   | TCP      | 6180<br>6183<br>6385<br>5050 | Managed Cluster | ACM 管理 Managed Cluster Lifecycle 時的溝通管道             |



# RHACM Networking

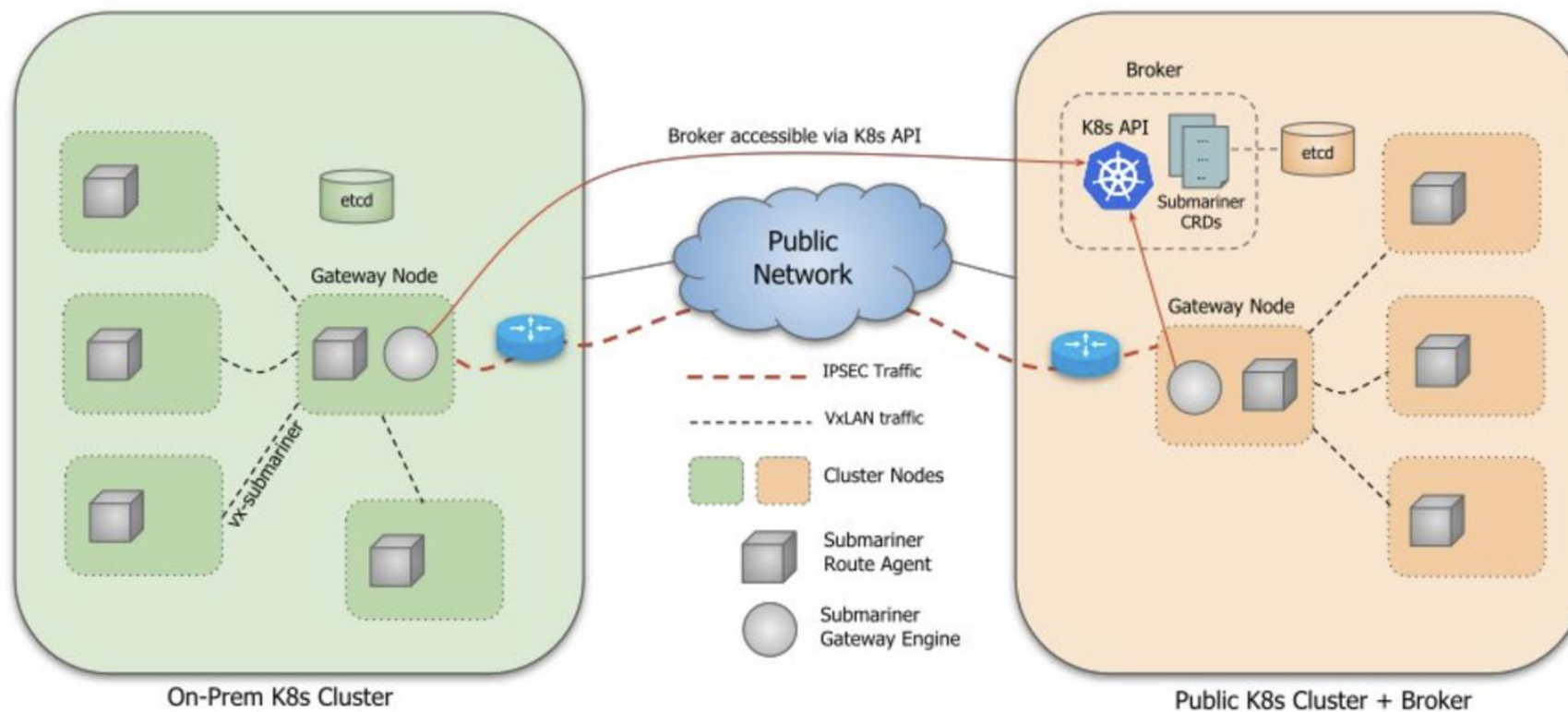
## Managed Cluster 網路設定：

| Direction | Protocol | Port                         | Destination      | Connection  |
|-----------|----------|------------------------------|------------------|---|
| Inbound   | HTTPS    | 443                          | Hub Cluster      | 發送數據給 Search Engine 使用                                  |
| Inbound   | HTTPS    | 6443                         | Hub Cluster      | 用於聯繫 Hub Cluster API Server                             |
| Outbound  | HTTPS    | 443                          | Image Repository | 聯繫 Image Repository ( Quay )                            |
| Outbound  | HTTPS    | 443                          | Hub Cluster      | Managed Cluster 回傳 Metrics 、 Alerts 等訊息使用               |
| Outbound  | HTTPS    | 6443                         | Hub Cluster      | Managed Cluster 用於觀察 Hub Cluster 變更使用                   |
| Outbound  | HTTPS    | 443                          | ChannelSource    | 用於聯繫 Channel Source ， 包含：GitLab 、 GitOps Server ..... 等 |
| Outbound  | TCP      | 6180<br>6183<br>6385<br>5050 | Hub Cluster      | ACM 管理 Managed Cluster Lifecycle 時的溝通管道                 |

## RHACM Networking - Submariner

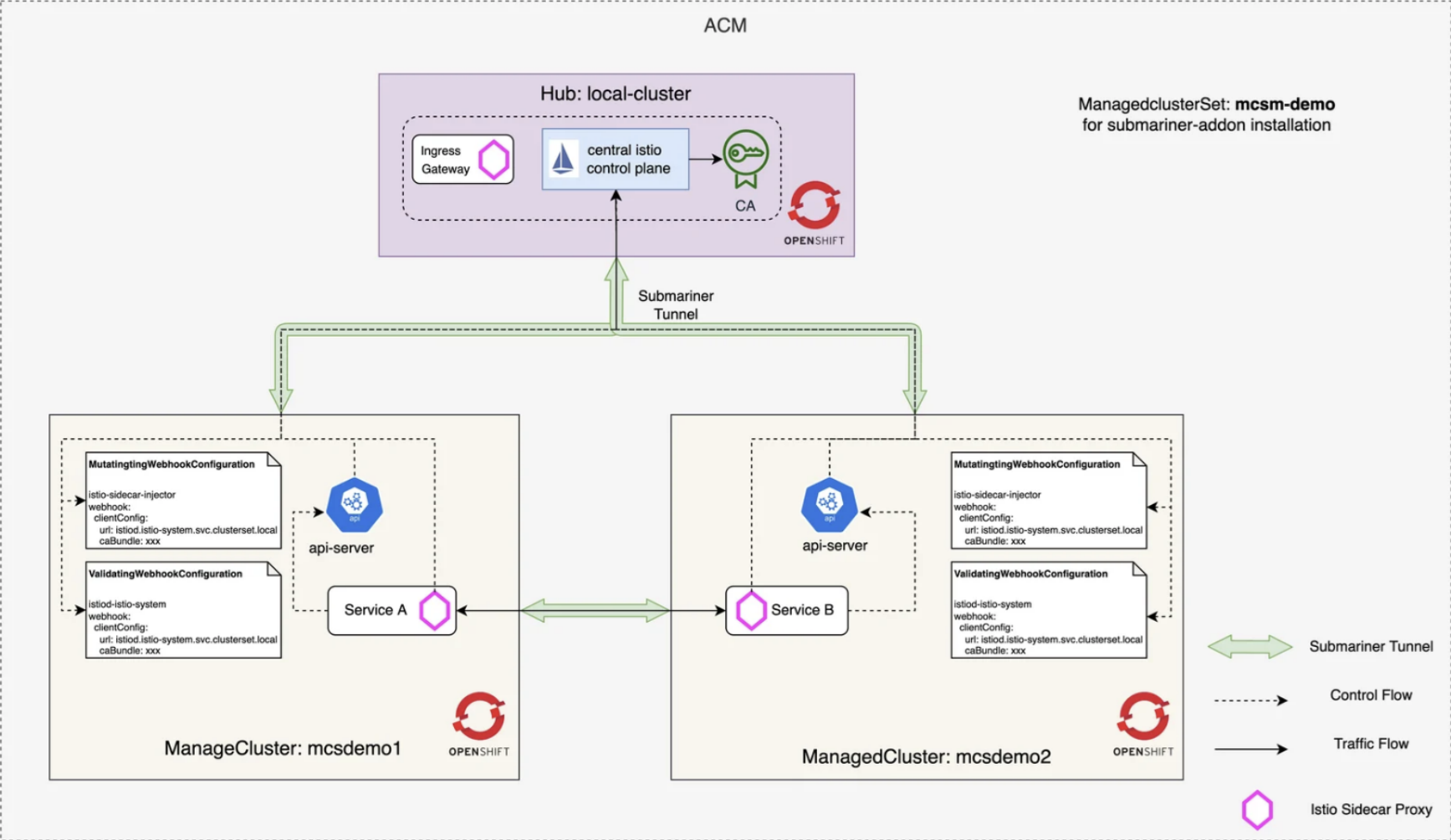
- Submariner 是一個開源專案，用以支援 Kubernetes Cluster 之間的 IPSEC 連接與 Service Discovery
- Submariner 提供 L3 的連線支援
- 支援 Openshift-SDN
- 提供 Openshift Operator 安裝支援
- Submariner 與 Istio 整合官方 Blog：  
<https://cloud.redhat.com/blog/set-up-an-istio-multicloud-service-mesh-with-submariner-in-red-hat-advanced-cluster-management-for-kubernetes>

# RHACM Networking - Submariner



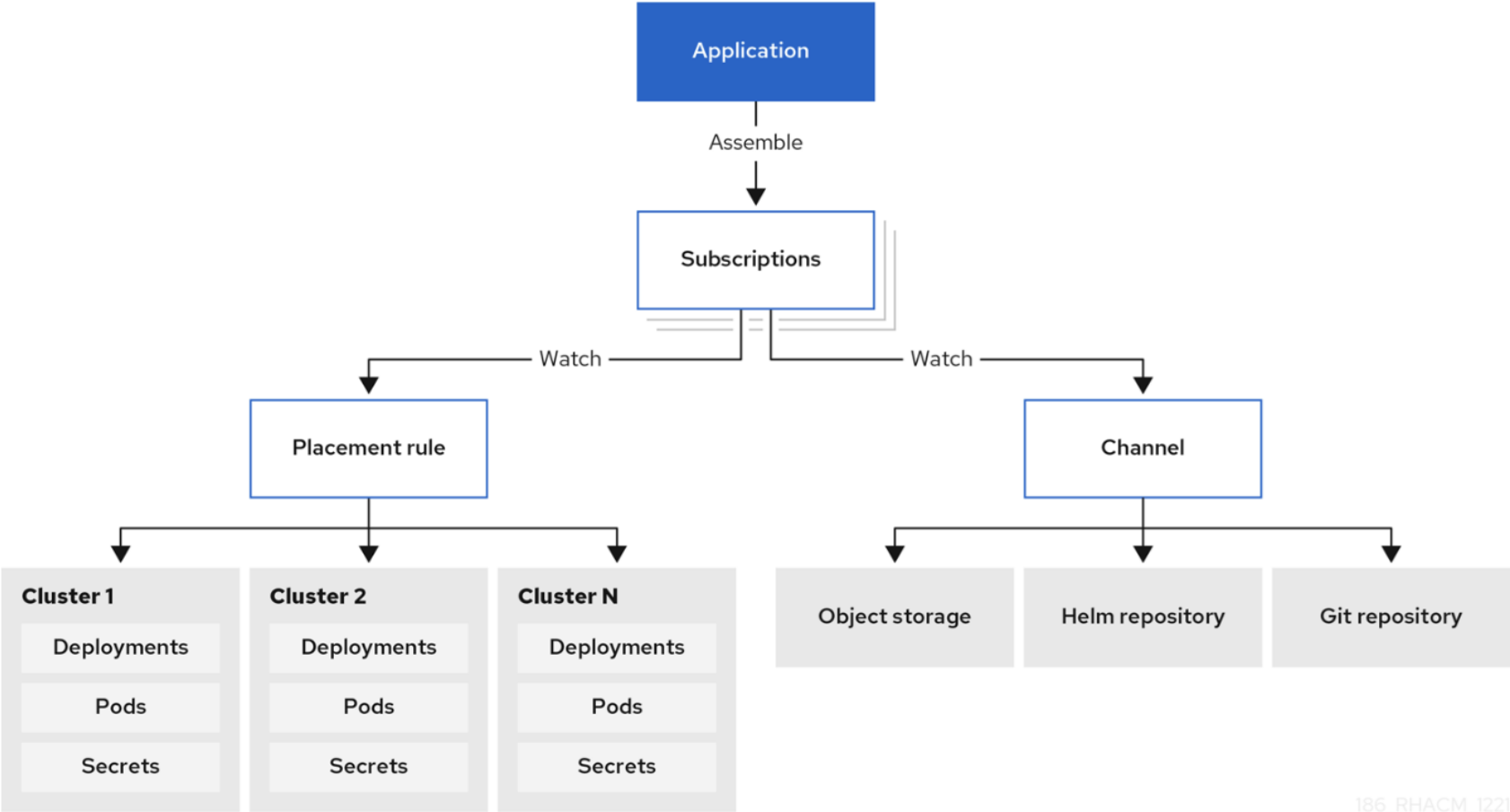


# RHACM Networking - Submariner

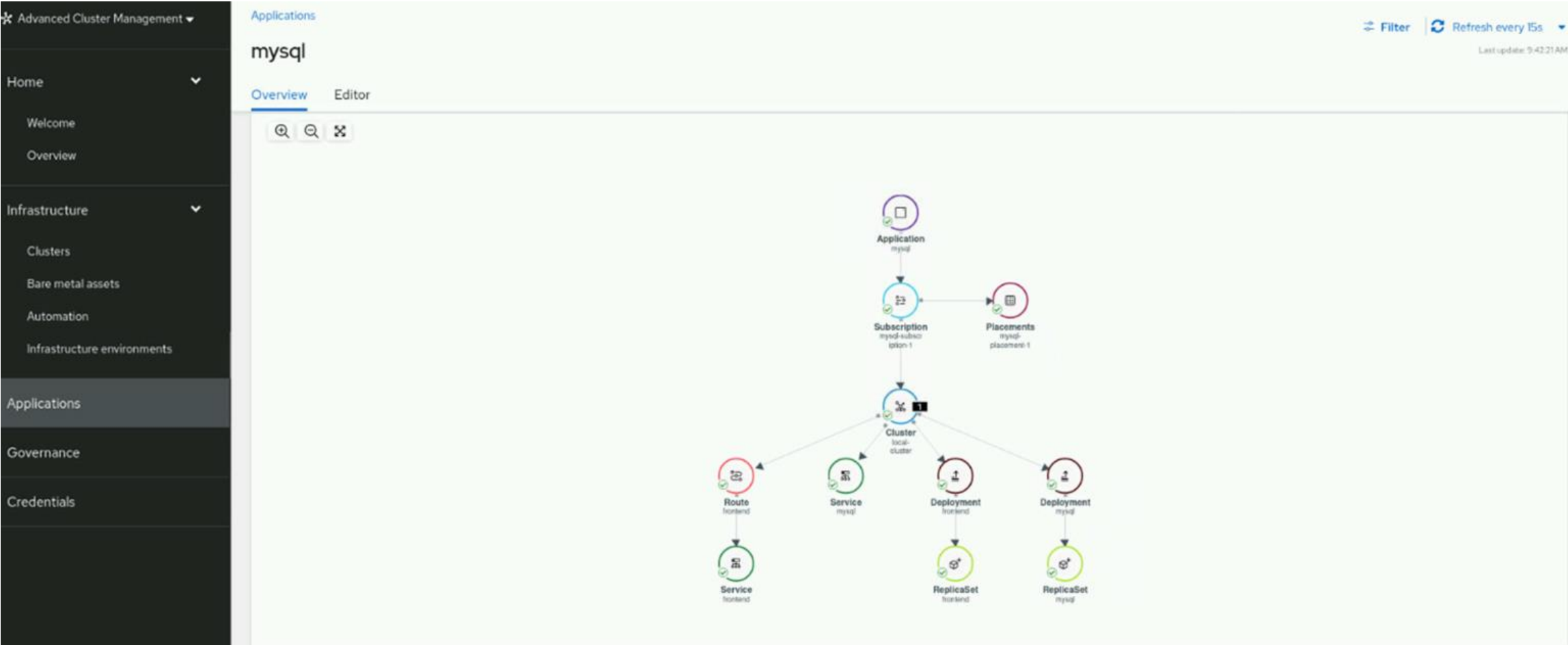


# RHACM Applications

- RHACM Application Management 提供跨 Cluster 的 Application 部署
- 定義 Kubernetes 資源管理部署任務
- 透過與 Git、Helm Chart、Object Storage Repository 整合，進行手動或自動化部署
- Kubernetes 資源定義方式支援 YAML、Helm Chart、Kustomize
- 可透過與 CI/CD 工具與 GitOps Server 整合，完整實現自動化佈署
- 透過以下元件實行：
  - Applications：Kubernetes 資源的集合，皆以 YAML 格式呈現
  - Channel：定義程式碼與設定檔來源，含：GitLab、ArgoCD、Helm Repo .....等
  - Subscription：定義哪個 Cluster 需要透過 Channel 進行部署

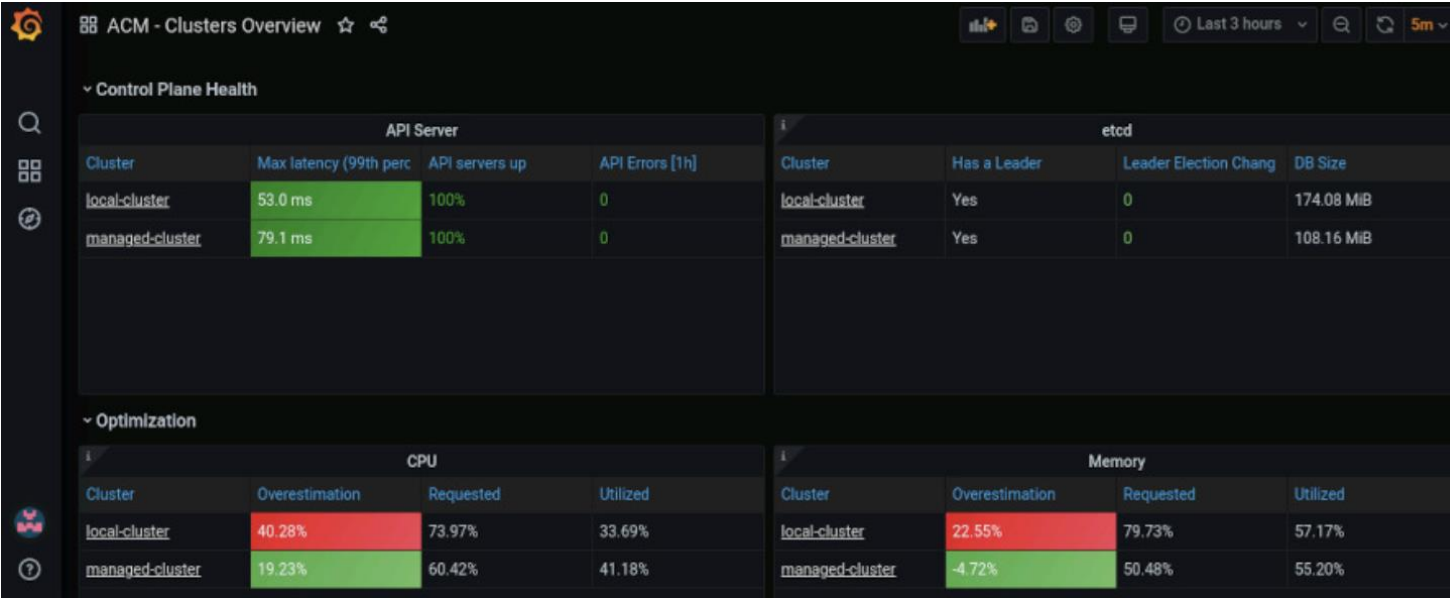


186\_RHACM\_I221



# RHACM Observability

- Observability Service 讓使用者可以蒐集各 Cluster 的運維數據
- 透過 Thanos、AlertManager 與 Grafana 提供監控功能



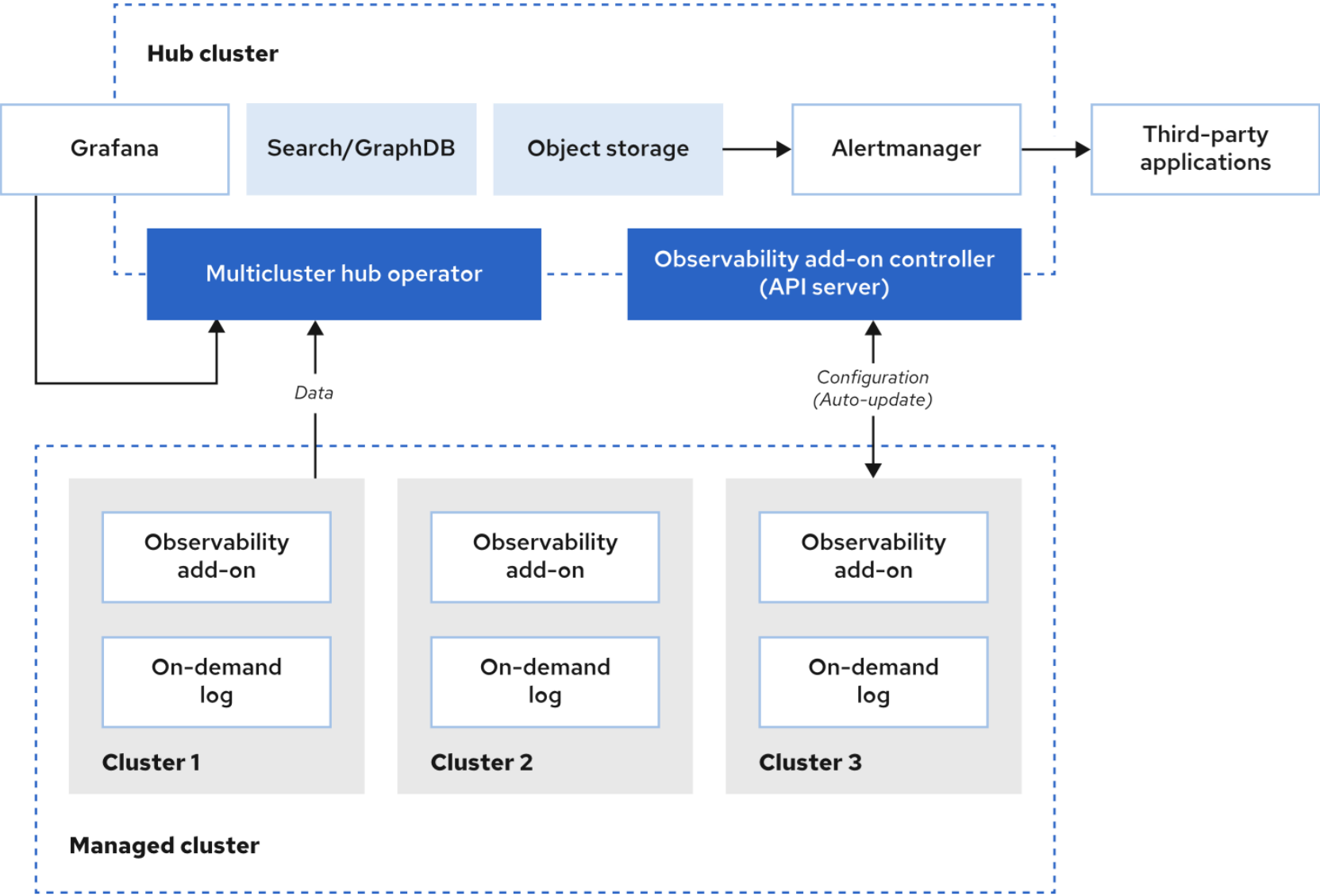
The screenshot displays the 'ACM - Clusters Overview' dashboard. It features a sidebar with navigation icons and a main content area with two sections: 'Control Plane Health' and 'Optimization'. The 'Control Plane Health' section contains two tables: 'API Server' and 'etcd'. The 'API Server' table shows 'Max latency (99th perc)', 'API servers up', and 'API Errors [1h]' for 'local-cluster' and 'managed-cluster'. The 'etcd' table shows 'Has a Leader', 'Leader Election Chang', and 'DB Size'. The 'Optimization' section contains two tables: 'CPU' and 'Memory'. The 'CPU' table shows 'Overestimation', 'Requested', and 'Utilized' for 'local-cluster' and 'managed-cluster'. The 'Memory' table shows 'Overestimation', 'Requested', and 'Utilized' for 'local-cluster' and 'managed-cluster'.

| API Server      |                         |                |                 |
|-----------------|-------------------------|----------------|-----------------|
| Cluster         | Max latency (99th perc) | API servers up | API Errors [1h] |
| local-cluster   | 53.0 ms                 | 100%           | 0               |
| managed-cluster | 79.1 ms                 | 100%           | 0               |

| etcd            |              |                       |            |
|-----------------|--------------|-----------------------|------------|
| Cluster         | Has a Leader | Leader Election Chang | DB Size    |
| local-cluster   | Yes          | 0                     | 174.08 MiB |
| managed-cluster | Yes          | 0                     | 108.16 MiB |

| CPU             |                |           |          |
|-----------------|----------------|-----------|----------|
| Cluster         | Overestimation | Requested | Utilized |
| local-cluster   | 40.28%         | 73.97%    | 33.69%   |
| managed-cluster | 19.23%         | 60.42%    | 41.18%   |

| Memory          |                |           |          |
|-----------------|----------------|-----------|----------|
| Cluster         | Overestimation | Requested | Utilized |
| local-cluster   | 22.55%         | 79.73%    | 57.17%   |
| managed-cluster | -4.72%         | 50.48%    | 55.20%   |



# RHACM Governance

RHACM 提供 **Cluster** 層級的資源檢測，可透過與 Red Hat Advanced Cluster Security 整合，進行更完整的安全性與合規性的檢診，RHACM 所支援的 **Policy** 如下：

- Namespace policy
- Pod policy
- Memory usage policy
- Role policy
- Security content constraints (SCC) policy
- ETCD encryption policy

## RHACM Add-ons

RHACM 可以透過 **klusterlet add-ons** 擴增相關功能，Managed Cluster 會透過 **klusterlet** 部署相關元件，使用者可以針對下列支援的 **Add-ons** 進行安裝：

- application-manager
- cert-policy-controller
- cluster-proxy
- config-policy-controller
- governance-policy-framework
- hypershift-addon
- iam-policy-controller
- managed-serviceaccount
- observability-controller
- search-collector
- submariner
- volsync
- work-manager



# RHACM Installation

- 專案規劃與功能探討

# RHACM 資源建議

- RHACM 資源消耗量基於 Cluster 需要監控的內部資源的多寡、需要部署的政策多寡
- 下表提供資源參考（待測試的單個 Cluster 資源請參考下圖）：

| Node                     | Flavor     | vCPU | RAM (GiB) | Disk type | Disk size (GiB) | Count        | Region    |
|--------------------------|------------|------|-----------|-----------|-----------------|--------------|-----------|
| Master                   | m5.2xlarge | 8    | 32        | gp2       | 100             | 3            | us-east-1 |
| Worker or Infrastructure | m5.2xlarge | 8    | 32        | gp2       | 100             | 3 or 5 nodes | us-east-1 |

- 偵測1個 Cluster 含 5000 個 Kubernetes 資源需要花費 Memory 50 Mi
- 1個 Cluster 1天約消耗 0.2 GiB

## RHACM 安裝規劃

- Hub Cluster : UAT
- Managed Cluster : SIT
- 安裝方式 : OCP Operator
- Networking : Hub Cluster 與 Managed Cluster 需要能互相連線
- SSL 憑證 : 東森自簽憑證

# RHACM Access Control

- 專案規劃與功能探討

# RHACM Access Control

- Access Control：串接 OCP UAT OAuth - Azure AD
- Azure AD SIT 與 UAT 為同一座
- RBAC：以 ClusterSet 區分 UAT 與 SIT
- 保留預設最高管理者 Admin
- RBAC 名單設定之前先發出給東森團隊確認

# RHACM Observability Stack

- 專案規劃與功能探討

## RHACM Observability

- 提供預設架構，使用者可以透過，**Observability Grafana Dashboard** 查看多叢集資訊
- 提供 **Alert** 發送，將警告回報團隊成員
  - **Alert Rule** 比照 **SIT** 環境
  - 建議設定之前先發送 **Alert Rule** 給東森團隊討論

# Multicluster Deployment

- 專案規劃與功能探討



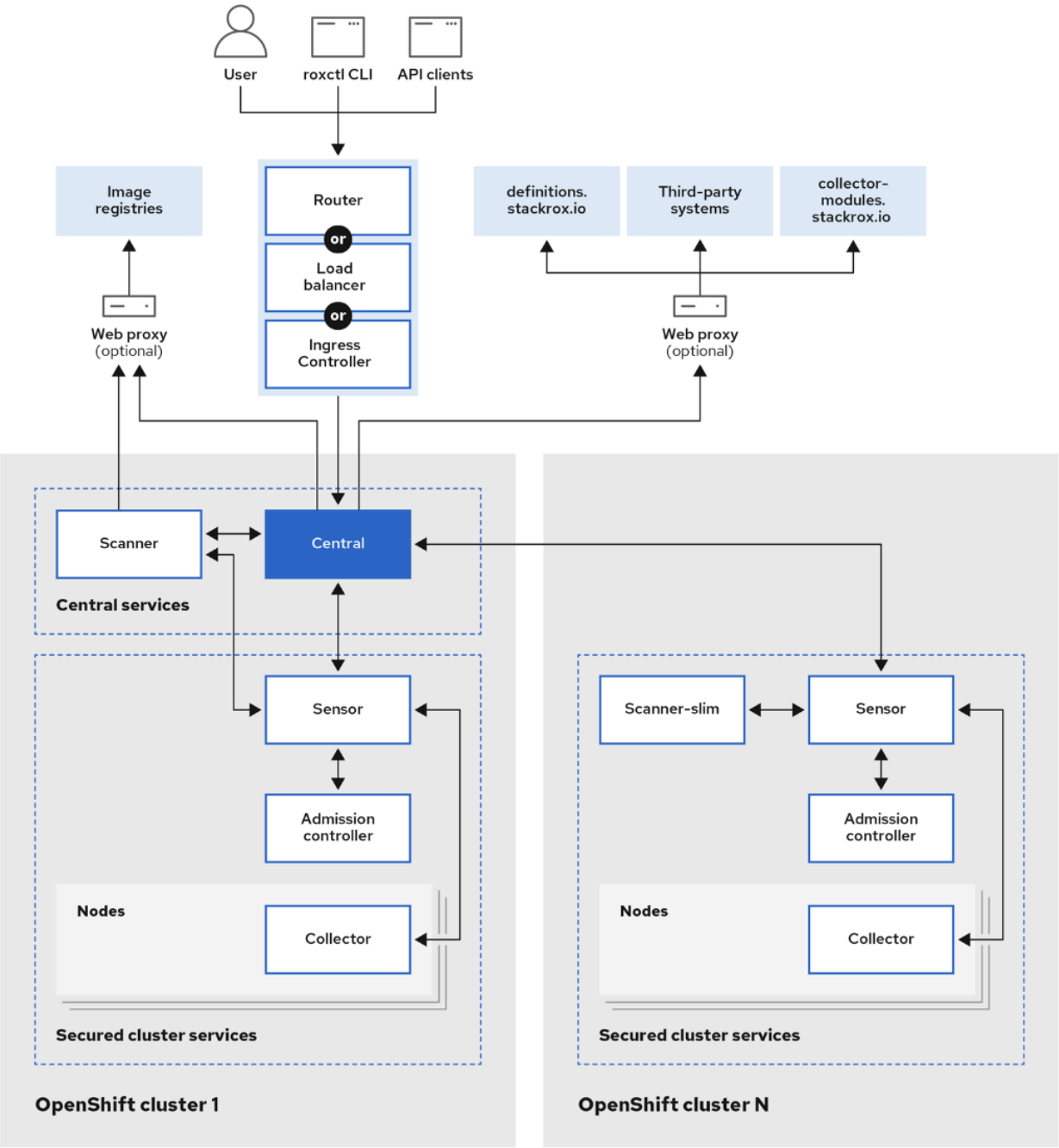
## RHACM 多叢集應用程式部署

- 可整合 GitHub、GitLab、BitBucket、Gogs 進行部署
- 需要 YAML、Helm Chart、Kustomize 定義 Kubernetes 資源
- 透過 Subscriptions、Channel 定義要部署的叢集與來源
- 手動上版或透過特定時程自動上版

# Red Hat Advanced Cluster Security

# Red Hat Advanced Cluster Security (RHACS)

- RHACS 為 Red Hat 提供的 OCP 與 Kubernetes 合規性與安全性檢測平台
- 可透過 OCP Operator 安裝
- 提供下功能：
  - 可視化管理網頁介面
  - 集中查看各叢集的合規性與安全性報告
  - 整合 Quay，進行 Container Image 弱點掃描
  - 合規性檢診
  - 網路連線檢診
  - 叢集安全性檢診

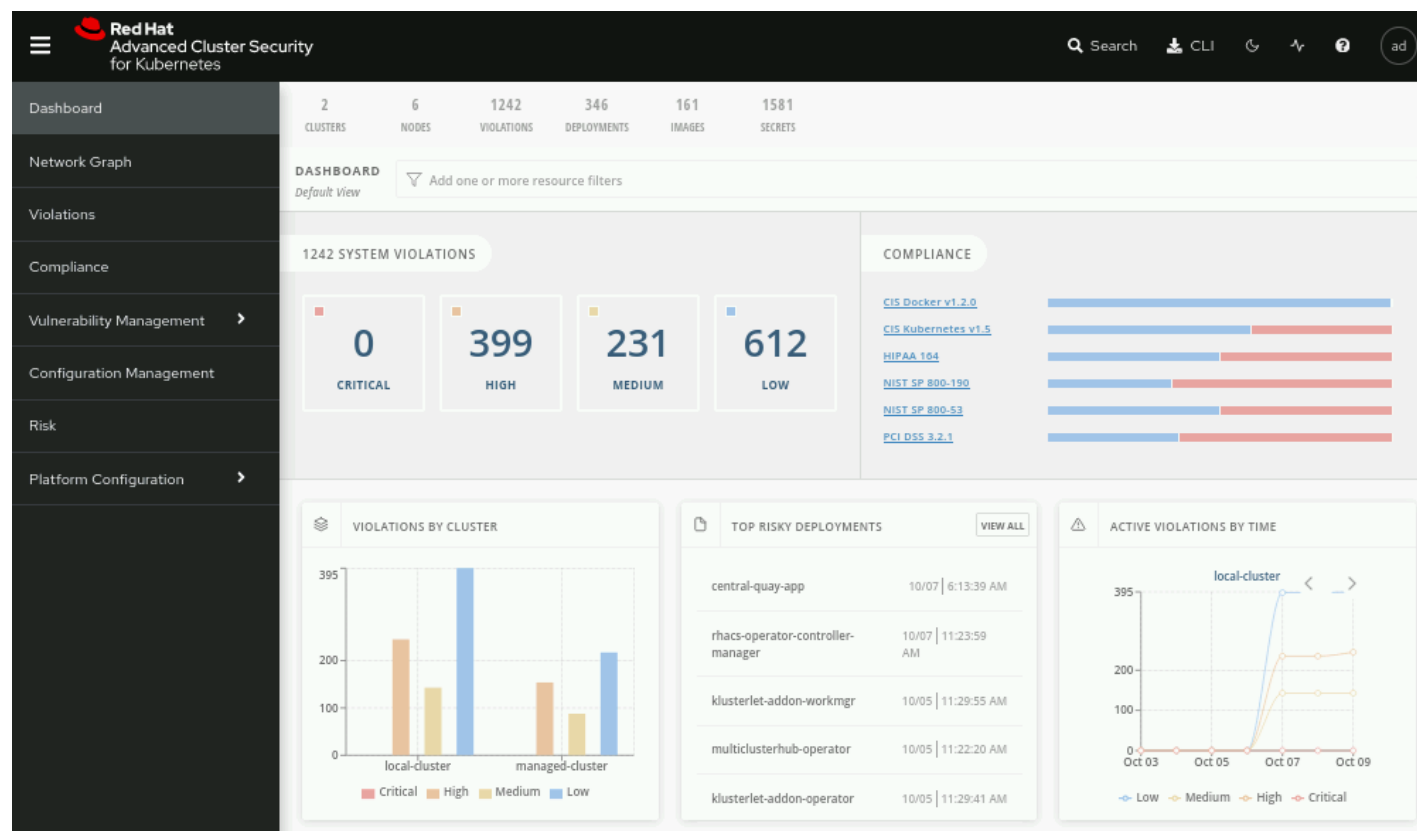


# Red Hat Advanced Cluster Security (RHACS)

- **Central Services**
  - **Central**：RHACS 主控中心，提供 **API** 與網頁介面
  - **Central DB**：儲存 RHACS 運行數據
  - **Scanner**：Container Images 與叢集節點的弱掃工具，針對 **CVEs** 清單提供報告
- **Secured Cluster**：受管的 OCP 或 Kubernetes Cluster
  - **Sensor**：負責分析和監控叢集
  - **Admission Controller**：防止使用者建立違反 RHACS 政策的資源
  - **Collector**：蒐集 Container 運行數據，並回傳給 Sensor
  - **Scanner**：Container Images 與叢集節點的弱掃工具

# RHACS Dashboard

RHACS 提供網頁操作介面，讓使用者查看報表與執行掃描操作



# RHACS Access Control

- RHACS 與 RHACM 相同，皆可透過 OCP OAuth Service 與 LDAP 串接
- RHACS 介面亦提供 RBAC 權限規劃

| System role                        | Description  |
|------------------------------------|--|
| Admin                              | This role is targeted for administrators. Use it to provide read and write access to all resources.  |
| Analyst                            | This role is targeted for a user who cannot make any changes, but can view everything. Use it to provide read-only access for all resources. |
| Continuous Integration             | This role is targeted for CI (continuous integration) systems and includes the permission set required to enforce deployment policies.       |
| None                               | This role has no read and write access to any resource. You can set this role as the minimum access role for all users.                      |
| Sensor Creator                     | RHACS uses this role to automate new cluster setups. It includes the permission set to create Sensors in secured clusters.                   |
| Scope Manager                      | This role includes the minimum permissions required to create and modify access scopes.  |
| Vulnerability Management Approver  | This role allows you to provide access to approve vulnerability deferrals or false positive requests.  |
| Vulnerability Management Requester | This role allows you to provide access to request vulnerability deferrals or false positives.  |
| Vulnerability Report Creator       | This role allows you to create and manage vulnerability reporting configurations for scheduled vulnerability reports.                        |

# RHACM Networking

防火牆網路設定：

| Direction          | Protocol | Port | Connection                                |
|--------------------|----------|------|---|
| Inbound / Outbound | HTTPS    | 8443 | 用於 Central Service 與 Secured Cluster 資訊交換 |



# RHACS Compliance Management

**RHACS** 提供多種合規性標準，可透過設置政策，依據項目排查，網頁介面亦提供報表檢索待處理的漏洞與風險項目

**RHACS** 提供的合規性標準：

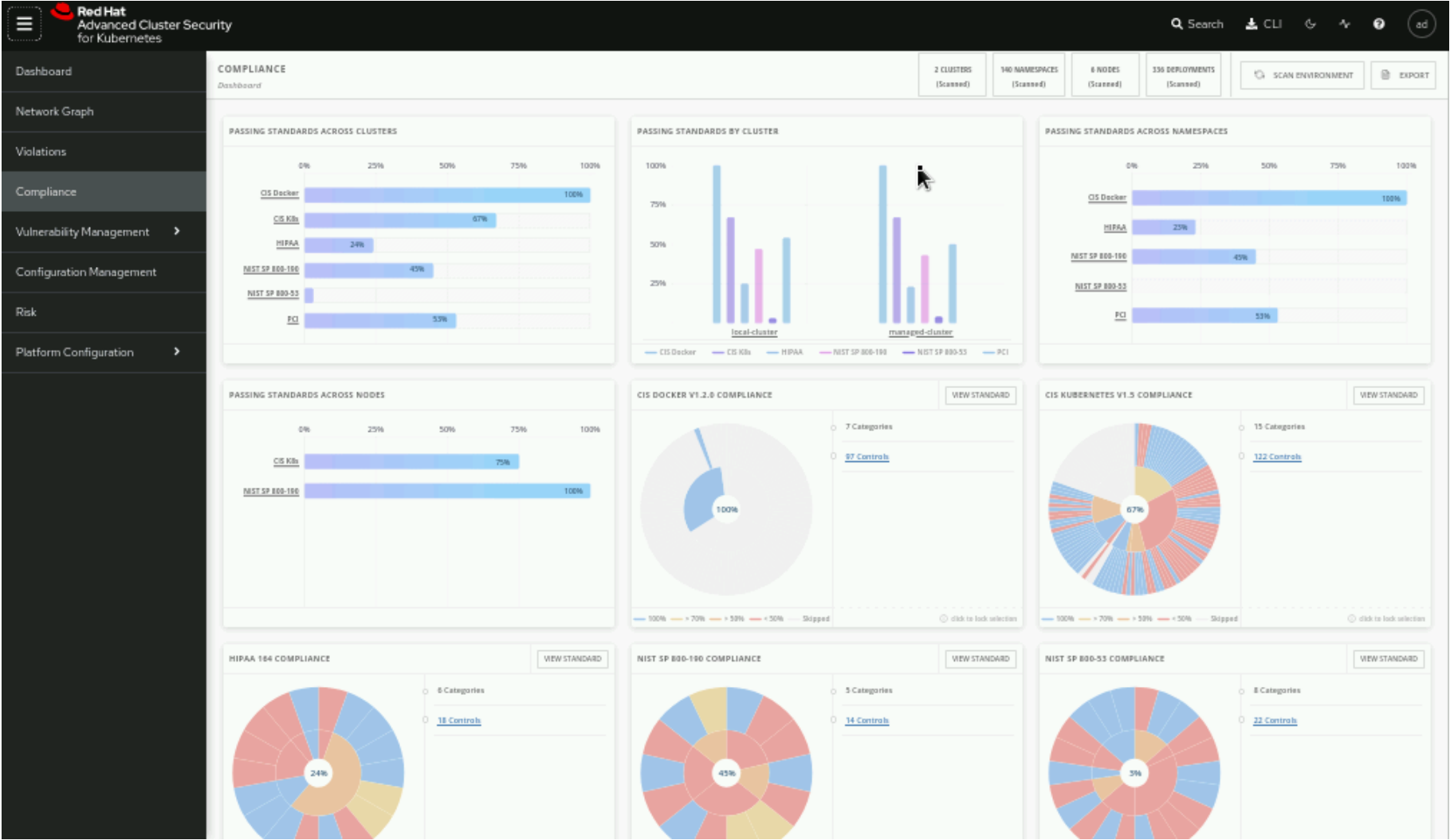
- **CIS Benchmarks**：提供針對 **Docker** 與 **Kubernetes** 的規範標準
- **HIPAA**：適用醫療與保險公司
- **NIST Special Publication 800-190 and 800-53**：包含 **Container** 與 **Kubernetes** 相關的規範標準
- **PCI DSS**：卡片支付安全標準
- **OpenSCAP**：開源的合規性標準，由 **Compliance Operator** 提供

# RHACS Compliance Management

可支援的合規性標準版本：

| Benchmark   | Supported version                                  |
|---|--|
| CIS Benchmarks (Center for Internet Security) for Docker and Kubernetes | CIS Kubernetes v1.5.0 and CIS Docker v1.2.0        |
| HIPAA (Health Insurance Portability and Accountability Act)             | HIPAA 164  |
| NIST (National Institute of Standards and Technology)                   | NIST Special Publication 800-190 and 800-53 Rev. 4 |
| PCI DSS (Payment Card Industry Data Security Standard)                  | PCI DSS 3.2.1                                      |

# RHACS Compliance Management

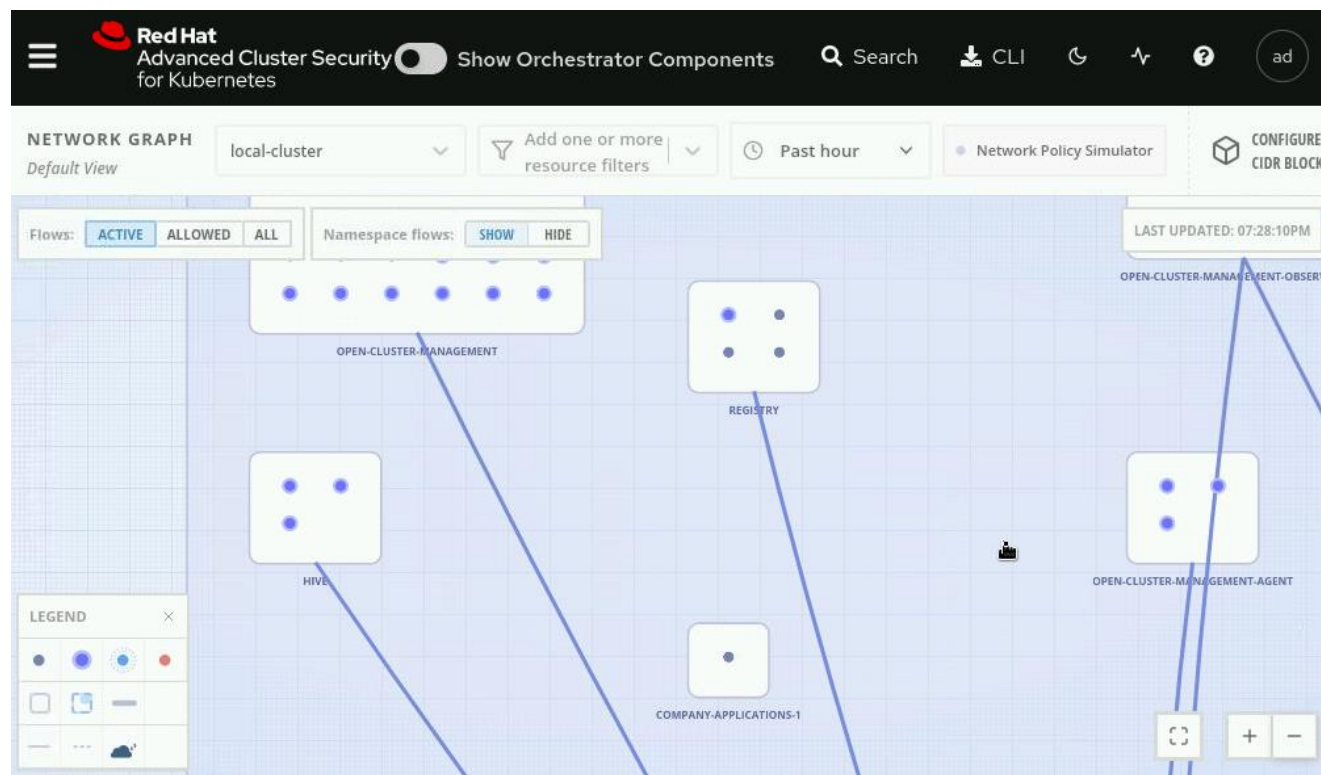


# RHACS Security Policy

- RHACS 提供多種安全性標準，另外也可以自定義政策標準
- RHACS 提供的基礎政策分類如下：
  - Anomalous Activity
  - Cryptocurrency Mining
  - DevOps Best Practices
  - Kubernetes
  - Network Tools
  - Package Management
  - Privileges
  - Security Best Practices
  - System Modification
  - Vulnerability Management

# RHACS Network Policy

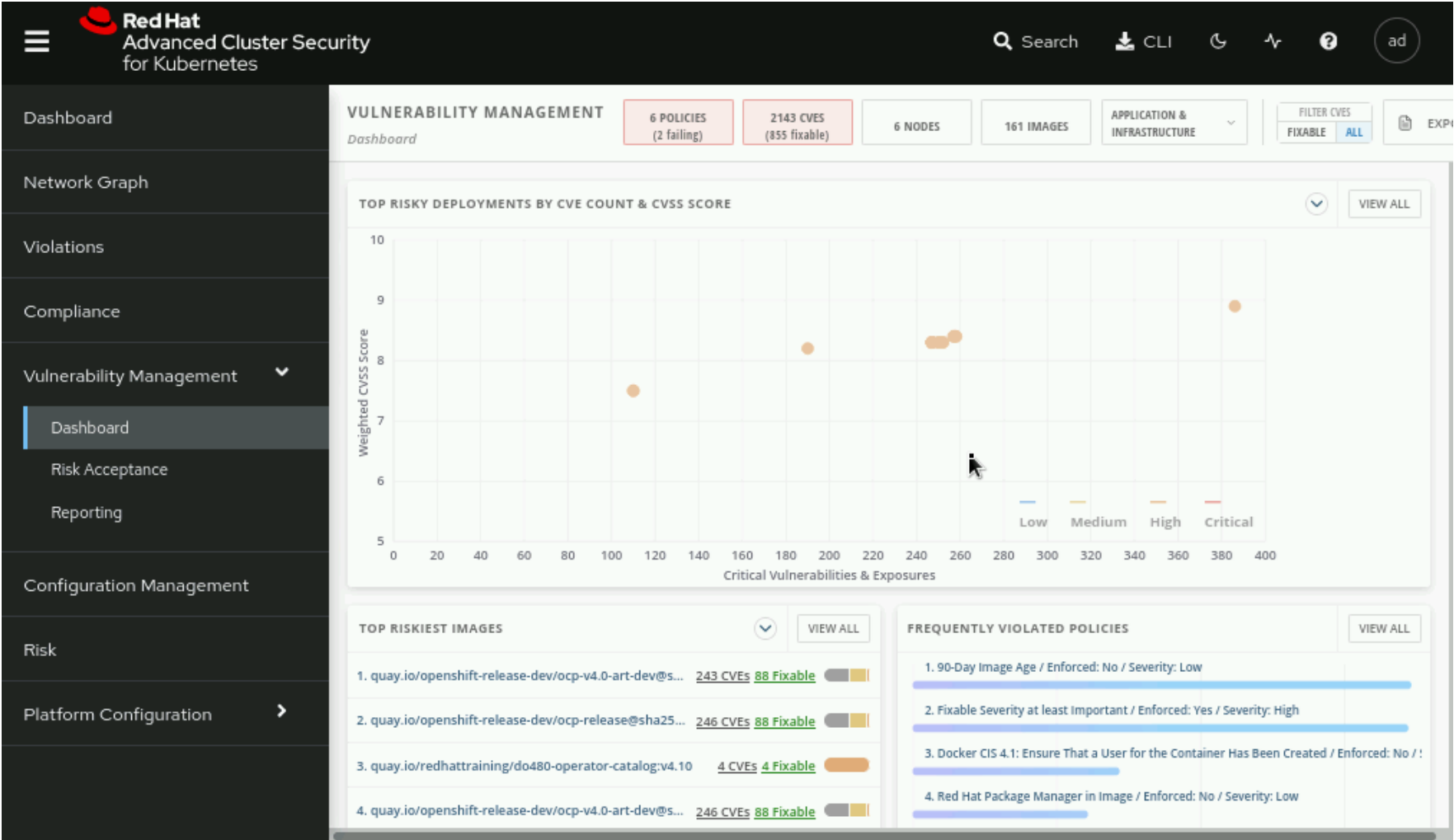
- Kubernetes Network Policy 可以侷限叢集內的 Pod 的連線標的
- RHACS 將 Kubernetes Network Policy 圖像化，讓使用者更直覺的檢診網路架構



## RHACS Image Vulnerability

- RHACS 提供 Cluster 與 Container Image 弱點掃描
- 可以整合 Quay 掃描結果，呈現於 RHACS Image Vulnerability 報表
- CVEs 作為檢測標準
- 提供 CVSS 評分標準
- 可設置弱點偵測通知，將報告透過 e-mail 通知團隊人員
- 離線環境需透過上傳 Scanner Definitions 更新檢測標準，stackrox 為主要更新源

# RHACS Image Vulnerability



# RHACS 合規性與安全性檢索

RHACS 根據所有的政策與漏洞監測，提供報表供排查，包含風險報告 (Risk )與違規報告 (Violations)

Red Hat

Advanced Cluster Security

for Kubernetes

Show Orchestrator Components

Search

CLI

ad

RISK

Default View

Add one or more resource filters

135 DEPLOYM

1

<

>

Central-quay-app

X

| Name                              | Created                 | Cluster         | Namespace                           |
|-----------------------------------|-------------------------|-----------------|-------------------------------------|
| central-quay-app                  | 10/07/2023   6:13:39AM  | local-cluster   | registry                            |
| rhacs-operator-controller-manager | 10/07/2023   11:23:59AM | managed-cluster | rhacs-operator                      |
| klusterlet-addon-workmgr          | 10/05/2023   11:29:55AM | managed-cluster | open-cluster-management-agent-addon |
| multiclusterhub-operator          | 10/05/2023   11:22:20AM | local-cluster   | open-cluster-management             |
| klusterlet-addon-operator         | 10/05/2023   11:29:41AM | managed-cluster | open-cluster-management-agent-addon |

RISK INDICATORS

DEPLOYMENT DETAILS

PROCESS DISCOVERY

VIEW DEPLOYMENT IN NETWORK GRAPH

Policy Violations

Environment Variable Contains Secret (severity: High)

Fixable Severity at least Important (severity: High)

90-Day Image Age (severity: Low)

Red Hat Package Manager in Image (severity: Low)

Suspicious Process Executions

Red Hat

Advanced Cluster Security

for Kubernetes

Search

CLI

ad

Violations

Add one or more resource filters

1242 results found

Row Actions

1 - 50 of 1242

<<

<

>

>>

of 25

| Policy                              | Entity   | Type       | Enforced | Severity | Categories               | Lifecycle | Time                   |
|-------------------------------------|--|------------|----------|----------|--------------------------|-----------|------------------------|
| 90-Day Image Age                    | hello-app in "local-cluster/operate-integrate" | deployment | No       | Low      | Multiple                 | Deploy    | 10/09/2023   5:56:36AM |
| Ubuntu Package Manager in Image     | hello-app in "local-cluster/operate-integrate" | deployment | No       | Low      | Security Best Practices  | Deploy    | 10/09/2023   5:56:36AM |
| Fixable Severity at least Important | hello-app in "local-cluster/operate-integrate" | deployment | No       | High     | Vulnerability Management | Deploy    | 10/09/2023   5:56:36AM |
| Fixable Severity at                 | scanner-db                                     | deployment | No       | High     | Vulnerability            | Deploy    | 10/09/2023             |

56



# RHACS Installation

- 專案規劃與功能探討

## RHACS 資源建議

- OCP Version :  $\geq 4.10$
- Central :

| Central | CPU       | Memory | Storage |
|---------|-----------|--------|---------|
| Request | 1.5 cores | 4 GiB  | 100 GiB |
| Limit   | 4 cores   | 8 GiB  | 100 GiB |

- Central DB :

| Central DB | CPU     | Memory | Storage |
|------------|---------|--------|---------|
| Request    | 4 cores | 8 GiB  | 100 GiB |
| Limit      | 8 cores | 16 GiB | 100 GiB |

## RHACS 資源建議

- Scanner :

| Scanner | CPU     | Memory   |
|---------|---------|----------|
| Request | 1 core  | 1500 MiB |
| Limit   | 2 cores | 4000 MiB |

- Scanner DB :

| Scanner-DB | CPU       | Memory   |
|------------|-----------|----------|
| Request    | 0.2 cores | 200 MiB  |
| Limit      | 2 cores   | 4000 MiB |

## RHACS 資源建議

- Secured Cluster :

| Sensor  | CPU     | Memory |
|---------|---------|--------|
| Request | 2 cores | 4 GiB  |
| Limit   | 4 cores | 8 GiB  |

| Admission controller | CPU        | Memory  |
|----------------------|------------|---------|
| Request              | 0.05 cores | 100 MiB |
| Limit                | 0.5 cores  | 500 MiB |

## RHACS 安裝規劃

- Central : UAT
- Secured Cluster : UAT、SIT
- 安裝方法 : OCP Operator
- 網路環境 : UAT 與 SIT 需互通
- SSL 憑證 : 東森自簽憑證

# Access Control

- 專案規劃與功能探討

# RHACS Access Control

- Access Control：串接 OCP UAT Auth – Azure AD
- RBAC：透過 Group 區分權限

# Policies

- 專案規劃與功能探討



# Red Hat Advanced Cluster Security (RHACS)

- 提供 RHACS 基本合規性政策與安全政策基於：
  - CIS Benchmarks：提供針對 Docker 與 Kubernetes 的規範標準
  - NIST Special Publication 800-190 and 800-53：包含 Container 與 Kubernetes 相關的規範標準

# Vulnerability

- 專案規劃與功能探討

# Red Hat Advanced Cluster Security (RHACS)

- Scanning :
  - 與 Quay 整合提供 CVSS Container Image 評估
  - 提供 Cluster Node CVSS 評估

# Prospect of Hybrid Cloud

- 未來規劃與功能探討

## 混合雲架構的考量

混合雲架構下的 OCP MultiCluster :

- 公有雲、私有雲？ => 混合雲
- 雲端服務商：AWS、Azure、GCP 或是其他服務商？  
=> Azure、GCP
- 標的應用情景 => 大型活動前的服務擴展
- 管理策略與部署機制，先透過初階段的 ACM 功能驗證再行後續規劃，以利更好整合整體架構



# 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://linkedin.com/company/red-hat)



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



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



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

