

使用 Rancher 輕鬆打造 K8s DevOps 環境

e-MPower Your E-Biz

Jamie | #824

JSD System Consultant

CALL NOW

+886227316868

www.mpinfo.com.tw

Agenda

- Rancher Overview
- Demo
 - Workload
 - Catalogs
 - Pipeline
 - Service mesh

Rancher Overview

- Rancher 是為企業打造的容器管理平台，簡化了使用 Kubernetes 的流程，開發者可以隨處運行 Kubernetes，並同時滿足 IT 與 DevOps 團隊的需求



Rancher Overview



13,000+
GitHub stars

[Deploy Rancher](#)



9,000+
Users trained

[Free weekly training](#)



2.7M+
Containers managed

[Request a demo](#)



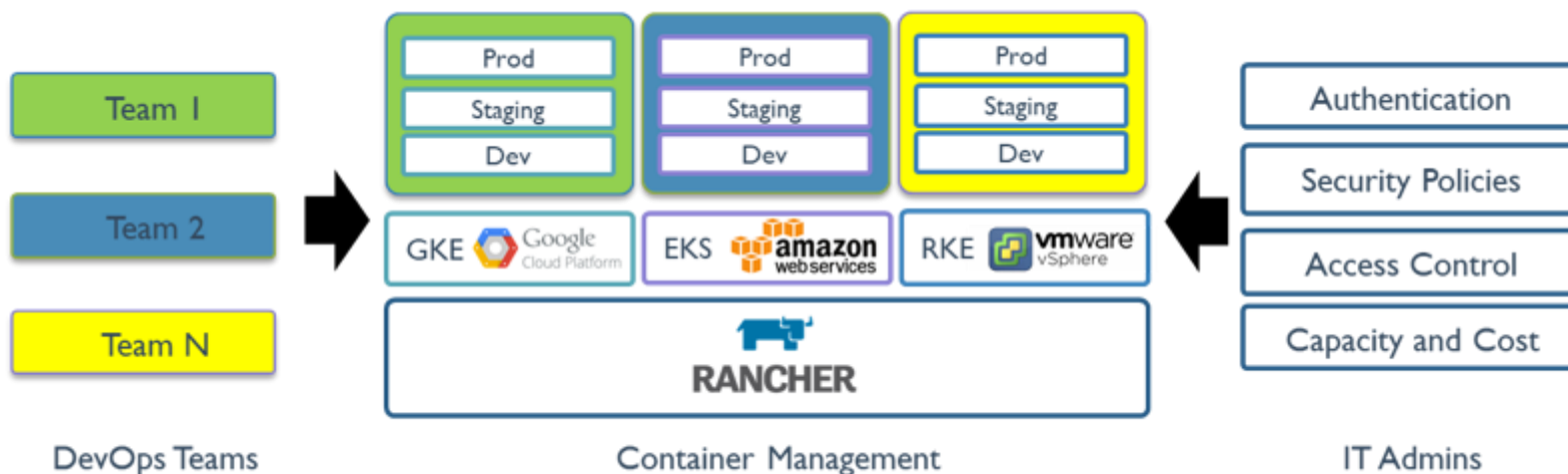
300+
Enterprise customers

[Get support](#)

Rancher Overview



Rancher Overview



Multi-Cluster Management



Global ▾ Clusters Apps Settings Security ▾ Tools ▾



Add Cluster - Select Cluster Type



From existing nodes (Custom)

Create a new Kubernetes cluster using RKE, out of existing bare-metal servers or virtual machines.



Import an existing cluster

Import an existing Kubernetes cluster. For K3S backed clusters, Rancher can manage some aspects of the cluster configuration, such as version upgrades. For standard Kubernetes clusters, the provider will manage provisioning and configuration.

With RKE and new nodes in an infrastructure provider



Amazon EC2



Azure



DigitalOcean



Linode



OpenStack



vSphere

With a hosted Kubernetes provider



Amazon EKS



Azure AKS



Google GKE

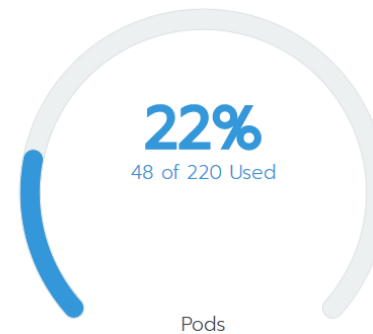
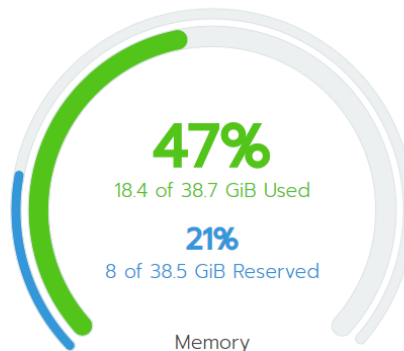
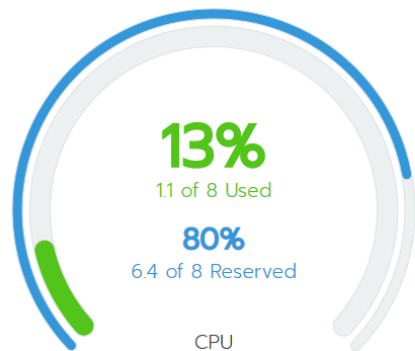
Cancel

Cluster Management

Dashboard: demo

Launch kubectl Kubeconfig File

Provider: Custom | Kubernetes Version: v1.15.10 | Created: 02/26/2020



- ✓ Etcd
- ✓ Controller Manager
- ✓ Scheduler
- ✓ Nodes

Expand All

- Cluster Metrics
Expand to see live metrics Grafana
- Etcd Metrics
Expand to see live metrics Grafana
- Kubernetes Components Metrics
Expand to see live metrics Grafana
- Rancher Logging Metrics



Cluster Management

- UI 開啟 kubectl Shell 訪問和管理叢集

≥ Shell demo

Connected

```
# Run kubectl commands inside here
# e.g. kubectl get all
> kubectl describe pod -n test-1
Name:          test-kata-864b6486d5-q6skc
Namespace:    test-1
Priority:      0
Node:         mp-jad-svr2/192.168.200.58
Start Time:   Mon, 20 Jul 2020 08:57:47 +0000
Labels:       pod-template-hash=864b6486d5
              workload.user.cattle.io/workloadselector=deployment-test-1-test-kata
              workloadID_ingress-b2603927f0e55a55da9dc21ef7371313=true
Annotations:  cattle.io/timestamp: 2020-07-20T08:57:32Z
              cni.projectcalico.org/podIP: 10.42.2.228/32
              field.cattle.io/publicEndpoints: [{"addresses":["172.16.1.80"],"allNodes":true,"hostname":"ing-kata.test-1.172.16.1.80.xip.io","ingressId":"test-1:ing-kata","port":80,"pro...
Status:       Running
IP:          10.42.2.228
IPs:         <none>
Controlled By: ReplicaSet/test-kata-864b6486d5
Containers:
  test-kata:
    Container ID:  docker://afb378ec5508a678861b57dcae1c65c2187df72242beb723c8b7efe53f47d0
    Image:          katacoda/docker-http-server:latest
    Image ID:      docker-pullable://katacoda/docker-http-server@sha256:76dc8a47fd019f80f2a3163aba789faf55b41b2fb06397653610c754cb12d3ee
    Port:          <none>
    Host Port:     <none>
    State:         Running
      Started:     Mon, 20 Jul 2020 08:57:51 +0000
    Ready:         True
    Restart Count: 0
    Environment:  <none>
    Mounts:
      /var/run/secrets/kubernetes.io/serviceaccount from default-token-m6hjl (ro)
Conditions:
  Type           Status
  Initialized    True
  Ready          True
  ContainersReady True
  PodScheduled   True
Volumes:
  default-token-m6hjl:
    Type:          Secret (a volume populated by a Secret)
    SecretName:    default-token-m6hjl
    Optional:     false
QoS Class:       BestEffort
Node-Selectors:  <none>
Tolerations:    node.kubernetes.io/not-ready:NoExecute for 300s
                node.kubernetes.io/unreachable:NoExecute for 300s
Events:         <none>
```

Close

Authentication



Global ▾ Clusters Apps Settings Security ▾ Tools ▾



Authentication

Grid of authentication providers:

- Active Directory (checked)
- Azure AD
- GitHub
- Ping (SAML)
- Keycloak (SAML)
- AD FS (SAML)
- Okta (SAML)
- Shibboleth (SAML)
- FreeIPA (LDAP)
- OpenLDAP (LDAP)
- Google

⚠ Active Directory is not configured

1. Configure an Active Directory server

Enter the address, port, and protocol to connect to your Active Directory server. **389** is the standard port for insecure, **636** for TLS.

Hostname or IP Address *

Port

389

TLS

Server Connection Timeout *

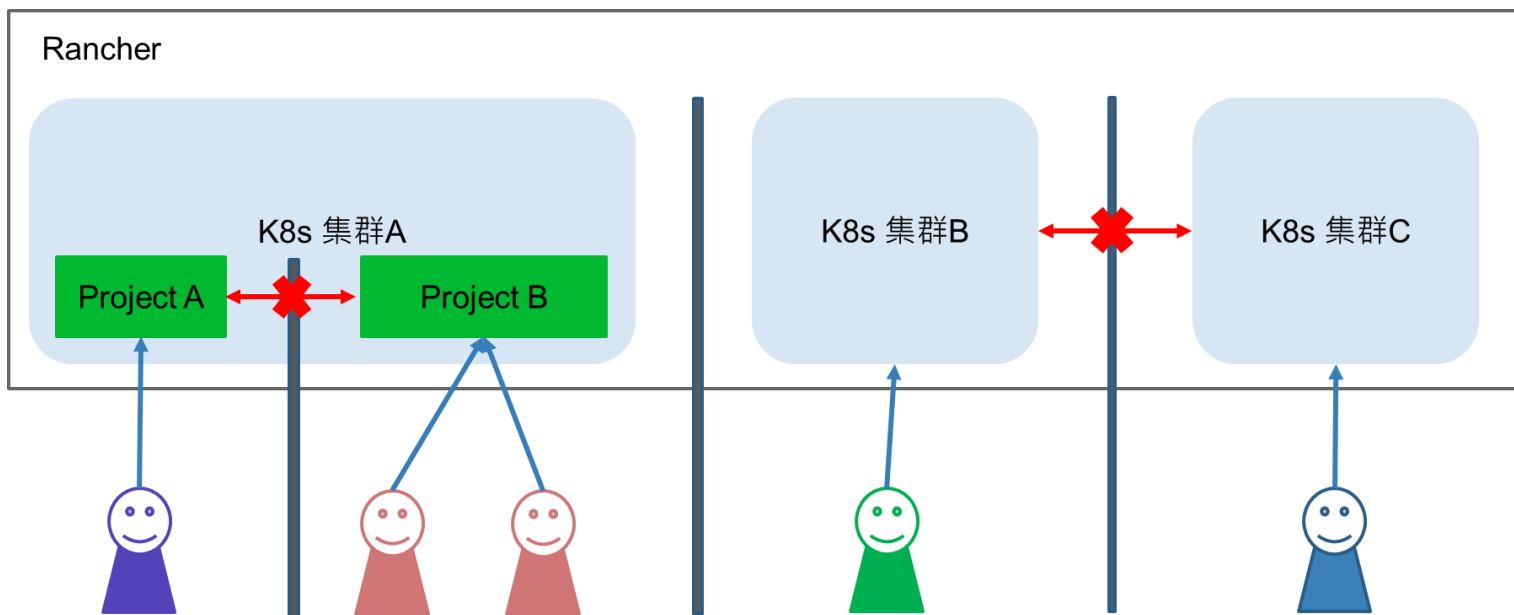
5000

Milliseconds

Rancher needs a service account that has (read-only) access to all of the domains that will be able to login, so that we can determine what groups a user is a member of when they make a request with an API key.

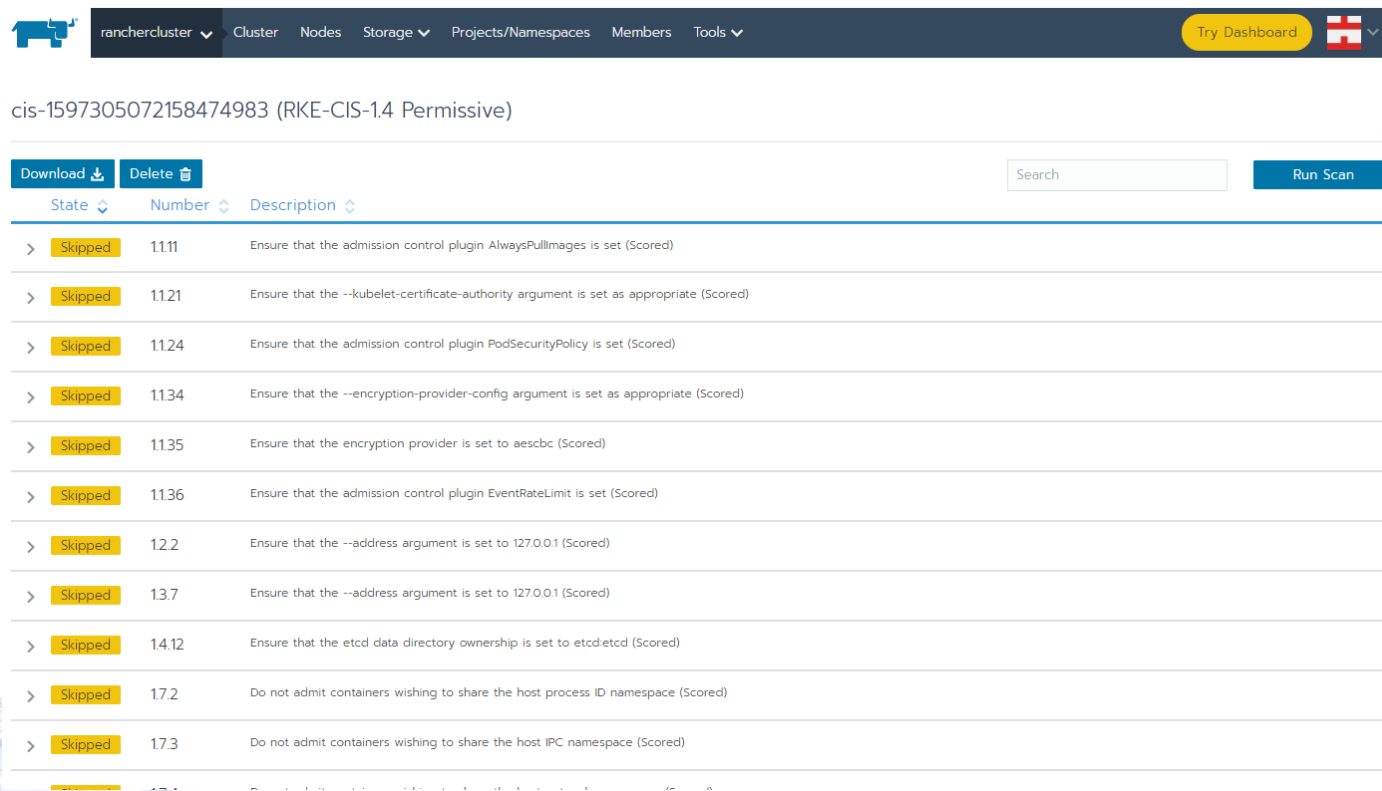
Role Based Access Control

- Global / Cluster / Project 多層級的使用者角色定義



CIS Scans

- 檢查 Cluster 是否符合 CIS (Center for Internet Security) Kubernetes Benchmark 安全標準



cis-1597305072158474983 (RKE-CIS-1.4 Permissive)

Download Delete

Search Run Scan

State	Number	Description
Skipped	1111	Ensure that the admission control plugin AlwaysPullImages is set (Scored)
Skipped	1121	Ensure that the --kubelet-certificate-authority argument is set as appropriate (Scored)
Skipped	1124	Ensure that the admission control plugin PodSecurityPolicy is set (Scored)
Skipped	1134	Ensure that the --encryption-provider-config argument is set as appropriate (Scored)
Skipped	1135	Ensure that the encryption provider is set to aescbc (Scored)
Skipped	1136	Ensure that the admission control plugin EventRateLimit is set (Scored)
Skipped	12.2	Ensure that the --address argument is set to 127.0.0.1 (Scored)
Skipped	13.7	Ensure that the --address argument is set to 127.0.0.1 (Scored)
Skipped	14.12	Ensure that the etcd data directory ownership is set to etcd:etcd (Scored)
Skipped	17.2	Do not admit containers wishing to share the host process ID namespace (Scored)
Skipped	17.3	Do not admit containers wishing to share the host IPC namespace (Scored)

Workload

- 通過 UI 進行容器應用的部署並進行操作

The screenshot shows the Rancher UI interface for managing workloads. The top navigation bar includes 'demo webinar', 'Resources', 'Apps', 'Namespaces', 'Members', and 'Tools'. A 'Try Dashboard' button and a user profile icon are also visible. Below the navigation, there are tabs for 'Workloads', 'Load Balancing', 'Service Discovery', and 'Volumes'. A search bar and a 'Deploy' button are present. The main content area displays a list of workloads in two namespaces: 'p-wmql4-pipeline' and 'test-1'. Each workload entry includes a checkbox, a state indicator (e.g., 'Active'), the name, an image, and a scale indicator. A context menu is open for the 'example-helloserver' workload, showing options: Edit, Clone, Redeploy, Add a Sidecar, Rollback, Execute Shell, Pause Orchestration, View/Edit YAML, View in API, Go to Grafana, and Delete.

State	Name	Image	Scale
Namespace: p-wmql4-pipeline			
Active	docker-registry	registry2 1 Pod / Created 2 months ago / Pod Restarts: 0	1
Active	example-helloserver	127.0.0.1:34777/example-helloserver-2 31385/tcp 1 Pod / Created 2 months ago / Pod Restarts: 0	1
Active	jenkins	rancher/pipeline-jenkins-server-v0.1.4 1 Pod / Created 2 months ago / Pod Restarts: 1	
Active	minio	rancher/minio-minio-RELEASE-2019-09-25T18-25-51Z 1 Pod / Created 2 months ago / Pod Restarts: 1	
Namespace: test-1			
Active	test-kata	katacoda/docker-http-server:latest 80/http 3 Pods / Created a month ago / Pod Restarts: 0	
Active	test-nginx	nginx:latest 1 Pod / Created a month ago / Pod Restarts: 0	

Workload

- 便捷的察看容器訊息與狀態，包括IP位址、鏡像、節點等訊息

The screenshot displays the Kubernetes dashboard interface for a workload named 'test-kata'. The top navigation bar includes the Kubernetes logo, a 'demo webinar' dropdown, and menu items for 'Resources', 'Apps', 'Namespaces', 'Members', and 'Tools'. A 'Try Dashboard' button and a user profile icon are also visible.

The workload details section shows:

- Namespace: test-1
- Image: katacoda/docker-http-server:latest
- Workload Type: Deployment
- Endpoints: 80/http
- Config Scale: 3 (with minus and plus buttons)
- Ready Scale: 3
- Created: 07/06/2020
- Pod Restarts: 0

The 'Pods' section is expanded, showing a list of three running pods:

State	Name	Image	Node
Running	test-kata-864b6486d5-s8fc5	katacoda/docker-http-server:latest 10.42.2.61 / Created a few seconds ago / Restarts: 0	mp-jsd-svr2 192.168.200.58
Running	test-kata-864b6486d5-gwgxk	katacoda/docker-http-server:latest 10.42.1.233 / Created a few seconds ago / Restarts: 0	jsd-gpu-node1 172.16.1.80
Running	test-kata-864b6486d5-g6skc	katacoda/docker-http-server:latest 10.42.2.228 / Created a month ago / Restarts: 0	mp-jsd-svr2 192.168.200.58

Below the pods list, there are sections for 'Workload Metrics' (with a Grafana icon), 'Events' (Events of current Deployment), and 'Environment Variables' (Environment Variables that were added at creation).

Workload

- 直接訪問容器 Shell ，方便後端人員直接對容器進行相關操作

≥ Shell: test-nginx

Connected

ProTip: Hold the Control key when opening shell access to launch a new window.

```
root@test-nginx-766f877bcf-4zqvw:/# ls -l
total 12
drwxr-xr-x  2 root root 4096 Jun  7 00:00 bin
drwxr-xr-x  2 root root   64 May  2 16:39 boot
drwxr-xr-x  5 root root 380 Jul 20 08:57 dev
drwxr-xr-x  1 root root  41 Jul 10 20:26 docker-entrypoint.d
-rwxrwxr-x  1 root root 1202 Jul 10 20:26 docker-entrypoint.sh
drwxr-xr-x  1 root root  13 Jul 20 08:57 etc
drwxr-xr-x  2 root root   64 May  2 16:39 home
drwxr-xr-x  1 root root  56 Jul 10 20:26 lib
drwxr-xr-x  2 root root  34 Jun  7 00:00 lib64
drwxr-xr-x  2 root root   6 Jun  7 00:00 media
drwxr-xr-x  2 root root   6 Jun  7 00:00 mnt
drwxr-xr-x  2 root root   6 Jun  7 00:00 opt
dr-xr-xr-x 471 root root   0 Jul 20 08:57 proc
drwx----- 2 root root  37 Jun  7 00:00 root
drwxr-xr-x  1 root root  38 Jul 20 08:57 run
drwxr-xr-x  2 root root 4096 Jun  7 00:00 sbin
drwxr-xr-x  2 root root   6 Jun  7 00:00 srv
dr-xr-xr-x 13 root root   0 Jul 23 02:37 sys
drwxrwxrwt  1 root root   6 Jul 10 20:26 tmp
drwxr-xr-x  1 root root  66 Jun  7 00:00 usr
drwxr-xr-x  1 root root  19 Jun  7 00:00 var
root@test-nginx-766f877bcf-4zqvw:/# cat /etc/*-release
PRETTY_NAME="Debian GNU/Linux 10 (buster)"
NAME="Debian GNU/Linux"
VERSION_ID="10"
VERSION="10 (buster)"
VERSION_CODENAME=buster
ID=debian
HOME_URL="https://www.debian.org/"
SUPPORT_URL="https://www.debian.org/support"
BUG_REPORT_URL="https://bugs.debian.org/"
root@test-nginx-766f877bcf-4zqvw:/#
```

Close

Workload

- 即時查看應用服務系統日誌

Logs: test-nginx

Connected

ProTip: Hold the Control key when opening logs to launch a new window.

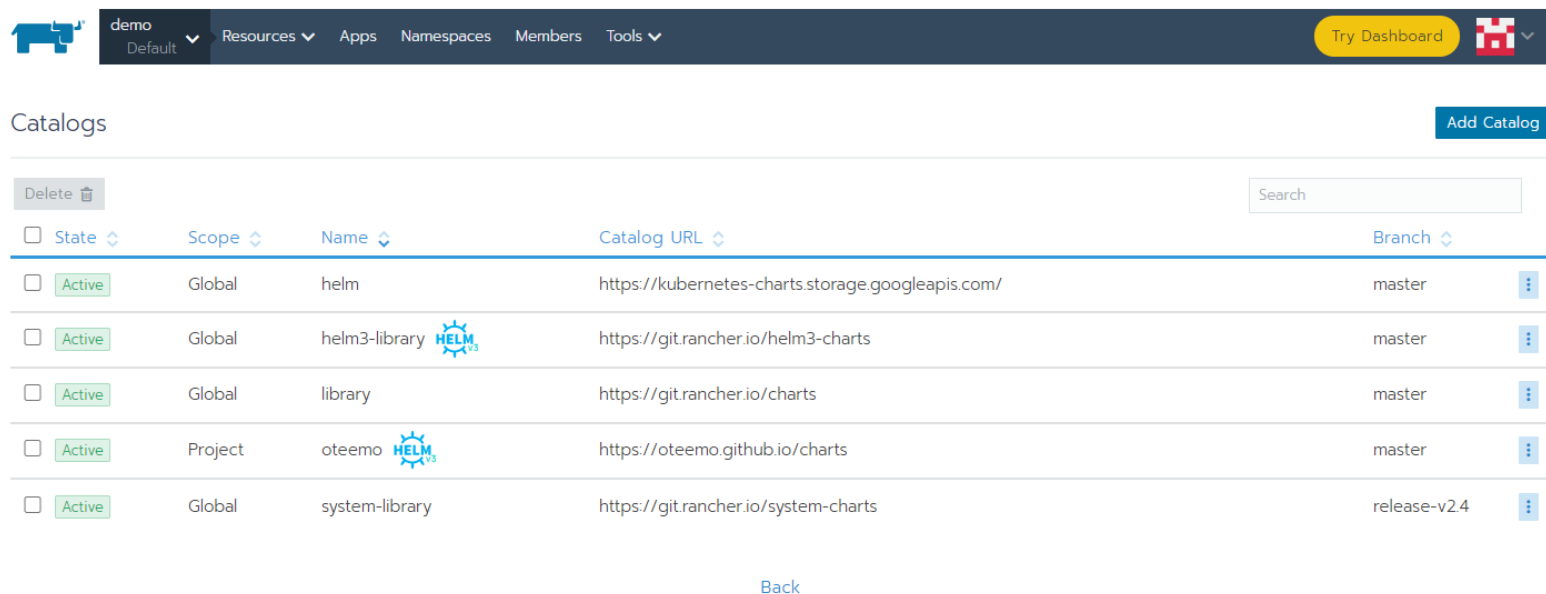
```
2020/7/20 下午4:57:43 /docker-entrypoint.sh: /docker-entrypoint.d/ is not empty, will attempt to perform configuration
2020/7/20 下午4:57:43 /docker-entrypoint.sh: Looking for shell scripts in /docker-entrypoint.d/
2020/7/20 下午4:57:43 /docker-entrypoint.sh: Launching /docker-entrypoint.d/10-listen-on-ipv6-by-default.sh
2020/7/20 下午4:57:43 10-listen-on-ipv6-by-default.sh: Getting the checksum of /etc/nginx/conf.d/default.conf
2020/7/20 下午4:57:43 10-listen-on-ipv6-by-default.sh: Enabled listen on IPv6 in /etc/nginx/conf.d/default.conf
2020/7/20 下午4:57:43 /docker-entrypoint.sh: Launching /docker-entrypoint.d/20-envsubst-on-templates.sh
2020/7/20 下午4:57:43 /docker-entrypoint.sh: Configuration complete; ready for start up
2020/8/17 下午4:07:00 172.16.1.80 - - [17/Aug/2020:08:07:00 +0000] "GET / HTTP/1.1" 200 612 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.125 Safari/537.36"
"..."
2020/8/17 下午4:07:00 2020/08/17 08:07:00 [error] 28#28: *1 open() "/usr/share/nginx/html/favicon.ico" failed (2: No such file or directory), client: 172.16.1.80, server: localhost, request: "GET /favicon.ico
HTTP/1.1", host: "172.16.1.80:31082", referer: "http://172.16.1.80:31082/"
2020/8/17 下午4:07:00 172.16.1.80 - - [17/Aug/2020:08:07:00 +0000] "GET /favicon.ico HTTP/1.1" 404 555 "http://172.16.1.80:31082/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/84.0.4147.125 Safari/537.36" "-"
2020/8/17 下午4:07:01 172.16.1.80 - - [17/Aug/2020:08:07:01 +0000] "GET / HTTP/1.1" 304 0 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.125 Safari/537.36"
"..."
2020/8/17 下午4:07:01 172.16.1.80 - - [17/Aug/2020:08:07:01 +0000] "GET / HTTP/1.1" 304 0 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.125 Safari/537.36"
"..."
2020/8/17 下午4:07:01 172.16.1.80 - - [17/Aug/2020:08:07:01 +0000] "GET / HTTP/1.1" 304 0 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.125 Safari/537.36"
"..."
2020/8/17 下午4:07:02 172.16.1.80 - - [17/Aug/2020:08:07:02 +0000] "GET / HTTP/1.1" 304 0 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.125 Safari/537.36"
"..."
2020/8/17 下午4:07:02 172.16.1.80 - - [17/Aug/2020:08:07:02 +0000] "GET / HTTP/1.1" 304 0 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.125 Safari/537.36"
"..."
2020/8/17 下午4:07:02 172.16.1.80 - - [17/Aug/2020:08:07:02 +0000] "GET / HTTP/1.1" 304 0 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.125 Safari/537.36"
"..."
2020/8/17 下午4:07:02 172.16.1.80 - - [17/Aug/2020:08:07:02 +0000] "GET / HTTP/1.1" 304 0 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.125 Safari/537.36"
"..."
2020/8/17 下午4:07:02 172.16.1.80 - - [17/Aug/2020:08:07:02 +0000] "GET / HTTP/1.1" 304 0 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.125 Safari/537.36"
"..."
```

- Wrap lines
- Previous Container



Scroll to Top Scroll to Bottom Download Logs Clear Screen Close

Catalog Apps

- 容器應用的樣板化和快速佈署
- 提供 Kubernetes 和 Rancher 官方的應用商店
- 可自定義應用商店位址



The screenshot shows the Rancher UI interface for managing Catalogs. The top navigation bar includes a 'demo' dropdown, 'Resources', 'Apps', 'Namespaces', 'Members', and 'Tools'. A 'Try Dashboard' button and a user profile icon are on the right. The main content area is titled 'Catalogs' and features a 'Delete' button, a search input, and an 'Add Catalog' button. A table lists five catalogs with columns for State, Scope, Name, Catalog URL, and Branch. Each row includes a checkbox, an 'Active' status indicator, and a three-dot menu icon.

State	Scope	Name	Catalog URL	Branch
<input type="checkbox"/> Active	Global	helm	https://kubernetes-charts.storage.googleapis.com/	master
<input type="checkbox"/> Active	Global	helm3-library 	https://git.rancher.io/helm3-charts	master
<input type="checkbox"/> Active	Global	library	https://git.rancher.io/charts	master
<input type="checkbox"/> Active	Project	oteemo 	https://oteemo.github.io/charts	master
<input type="checkbox"/> Active	Global	system-library	https://git.rancher.io/system-charts	release-v2.4

[Back](#)

Catalog Apps













demo Default Resources Apps Namespaces Members Tools Try Dashboard

Catalog Refresh All Categories Search

helm3-library HELM Expand

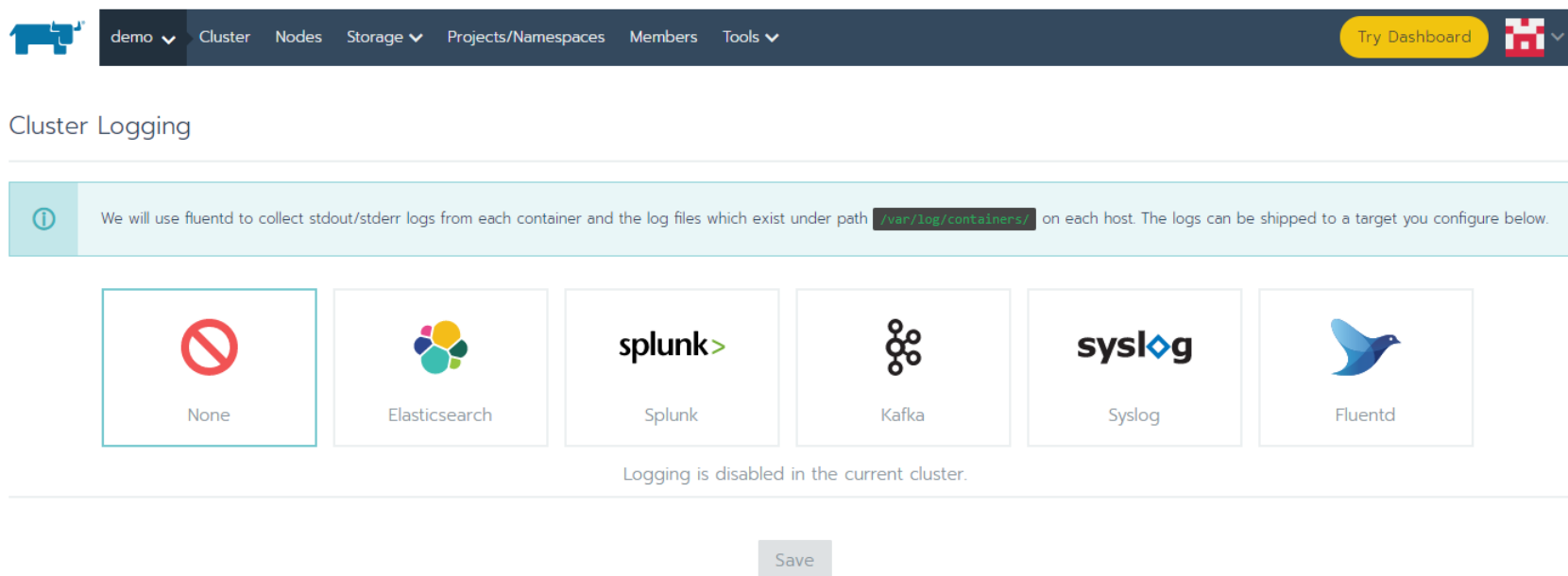
oteemo HELM Expand

library Collapse

 argo-cd	 PARTNER artifactory-ha	 PARTNER artifactory-jcr	 PARTNER aws-event-sources
 chartmuseum	 PARTNER citrix-adc-istio-ingress-gateway	 PARTNER citrix-api-gateway	 PARTNER citrix-cpx-istio-sidecar-injector
 PARTNER citrix-k8s-cpx-ingress-controller	 PARTNER citrix-k8s-ingress-controller	 PARTNER cockroachdb	 kubecost cost-analyzer

Logging

- 整合常見的日誌分析工具



The screenshot shows the Kubernetes Dashboard interface for configuring cluster logging. At the top, there is a navigation bar with the Kubernetes logo, a 'demo' dropdown, and links for 'Cluster', 'Nodes', 'Storage', 'Projects/Namespaces', 'Members', and 'Tools'. A 'Try Dashboard' button and a user profile icon are on the right. Below the navigation bar, the page title is 'Cluster Logging'. A light blue information banner contains a warning icon and the text: 'We will use fluentd to collect stdout/stderr logs from each container and the log files which exist under path `/var/log/containers/` on each host. The logs can be shipped to a target you configure below.' Below this banner, there are six selectable options for log targets: 'None' (with a red prohibition sign), 'Elasticsearch' (with its logo), 'splunk>' (with the Splunk logo), 'Kafka' (with its logo), 'syslog' (with the Syslog logo), and 'Fluentd' (with its logo). Below these options, a message states 'Logging is disabled in the current cluster.' At the bottom center, there is a 'Save' button.



Pipeline

- 支援主流 source code repo



1. Setup a Github application

- 1 For standard GitHub, [click here](#) to go to applications settings in a new window.
 - For Github Enterprise, login to your account. Click on Settings, then Developer settings.
- 2 Click "Register new application" and fill out the form:
 - **Application name:** Anything you like, e.g. My Pipeline
 - **Homepage URL** <https://192.168.200.32>
 - **Application description:** Anything you like, optional
 - **Authorization callback URL** <https://192.168.200.32>
- 3 Click "Register Application"

2. Configure the pipeline to use your Github for authentication

Client ID *

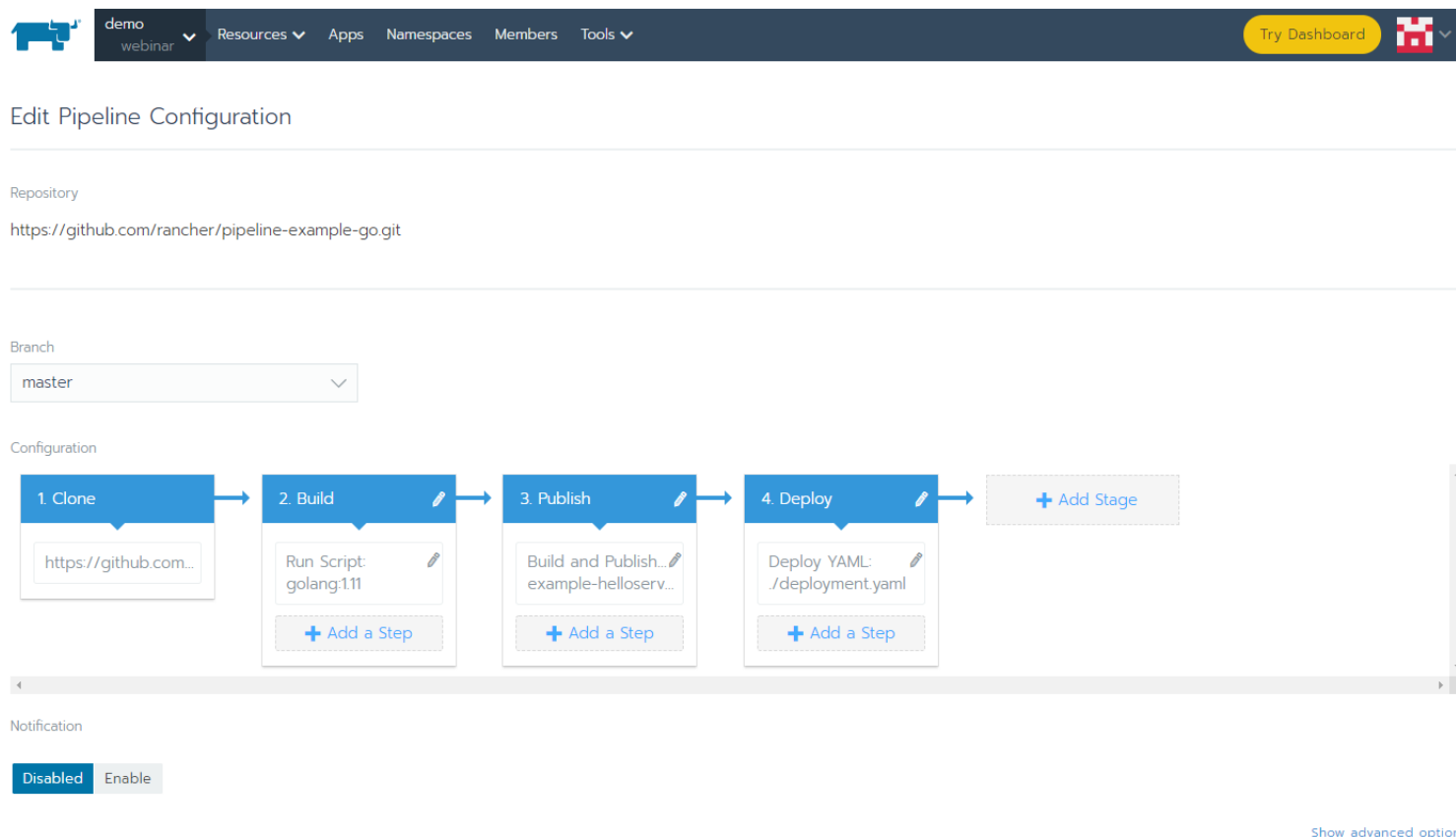
Copy and paste the Client ID and Secret from your newly-created application.

Client Secret *

Use a private github enterprise installation

Pipeline

- 編輯作業流程



The screenshot shows the Rancher Pipeline configuration interface. At the top, there is a navigation bar with the Rancher logo, a dropdown menu for 'demo webinar', and other navigation options like 'Resources', 'Apps', 'Namespaces', 'Members', and 'Tools'. A 'Try Dashboard' button and a user profile icon are also present.

The main content area is titled 'Edit Pipeline Configuration'. It shows the repository URL as `https://github.com/rancher/pipeline-example-go.git` and the branch set to 'master'.

The configuration section displays a sequence of stages:

- 1. Clone**: Contains the repository URL `https://github.com...`
- 2. Build**: Contains the script `Run Script: golang1.11`
- 3. Publish**: Contains the script `Build and Publish... example-helloserv...`
- 4. Deploy**: Contains the script `Deploy YAML: ./deployment.yaml`

Each stage has an 'Add a Step' button. A '+ Add Stage' button is located at the end of the sequence.

At the bottom, there is a 'Notification' section with 'Disabled' and 'Enable' buttons, and a 'Show advanced options' link.

Pipeline

- 即時檢視作業日誌

The screenshot displays the Jenkins Pipeline Run #3 interface. At the top, the navigation bar includes 'demo jamie', 'Resources', 'Apps', 'Namespaces', 'Members', 'Tools', 'Try Dashboard', and a user profile icon. The main header shows 'Pipeline Run: #3' with a 'Success' status and a menu icon.

Below the header, a commit message 'Commit Message: Update .rancher-pipeline.yml file' is shown. The pipeline details table provides the following information:

Pipeline: root/gs-spring-boot	Repository: http://mygitlab.gitlab-ce.172.16.180.xip.io/root/gs-spring-boot	Branch: master
Commit: 7cebce18	Triggered: 6 days ago	Duration: 1 minute, 37 seconds

A 'Collapse All' link is located below the table. The 'Detailed Log' section is expanded, showing the log of the current pipeline run. The log is organized into three main steps:

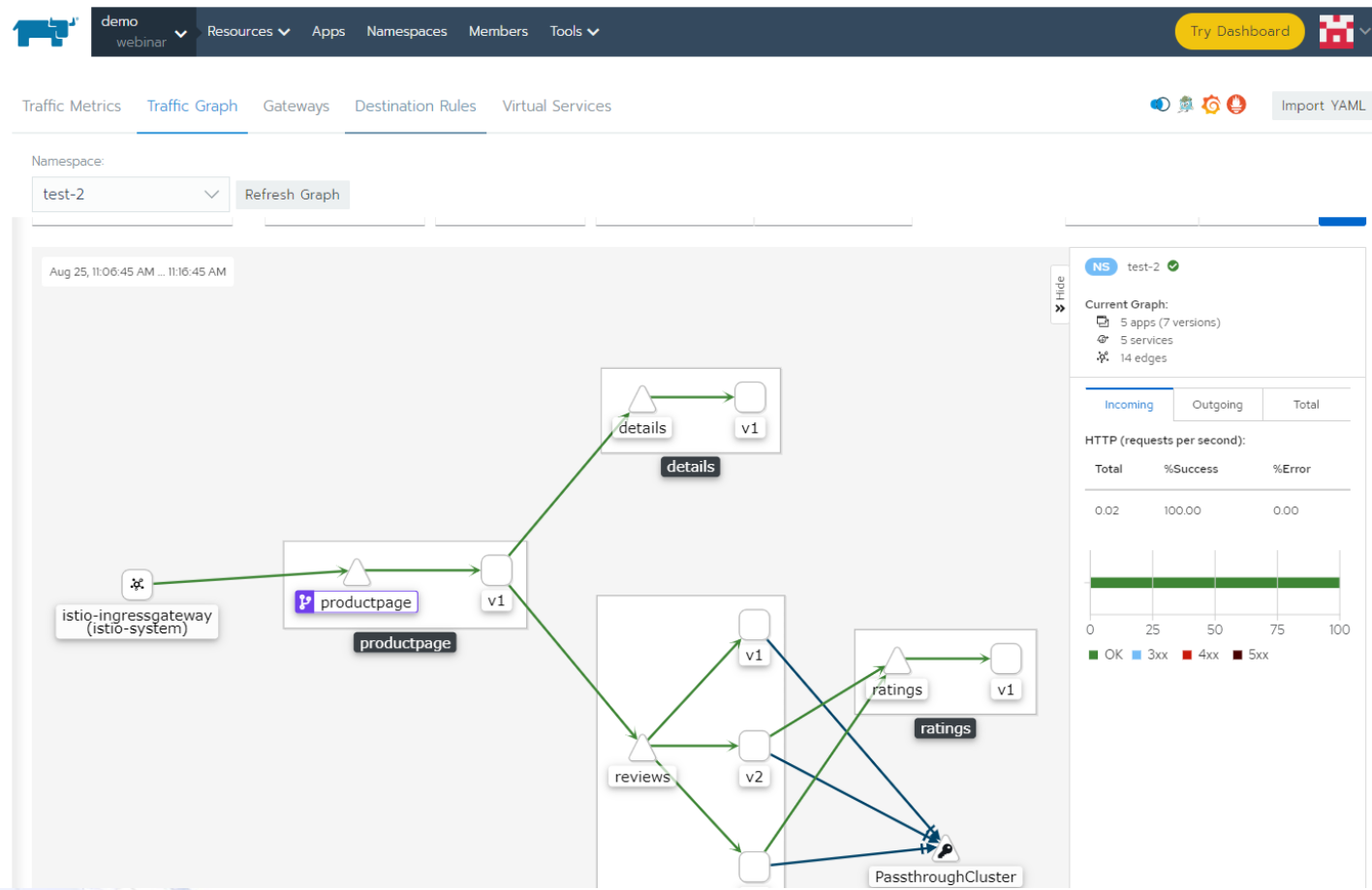
- 1 Clone** (8 seconds):
 - clone (8 seconds) - Success
- 2 Build** (41 seconds):
 - runScript (41 seconds) - Success
- 3 Publish** (20 seconds):
 - publishImage (20 seconds) - Success

The terminal output for the 'runScript' step is as follows:

```
+ cd complete
+ pwd
/home/jenkins/agent/workspace/pipeline_p-fx5tp-3/complete
+ ls
Dockerfile
build.gradle
deployment.yaml
gradle
gradlew
gradlew.bat
mvnw
mvnw.cmd
pom.xml
settings.xml
src
+ mkdir -p /root/.m2
+ mv settings.xml /root/.m2/
+ mvn clean package sonar:sonar -Dsonar.projectKey=gs-spring-boot -Dsonar.host.url=http://mysonaqube-
ing_sonarqube.172.16.1.80.xip.io -Dsonar.login=0a2705c370172763f29578b09234eb8e5bd31e
[WARNING]
[WARNING] Some problems were encountered while building the effective settings
[WARNING] Unrecognised tag: 'demoRepository' (position: START_TAG seen ...</localRepository>\n <demoRepository>... @7:19) @
```

Service Mesh

- 整合 Istio



DEMO



e-MPower Your E-Biz
www.mpinfo.com.tw

Thank You

Presenter

jamielin@mpinfo.com.tw

References :

<https://rancher.com/>

<https://rancher.com/docs/rancher/v2.x/en/>



e-MPower Your E-Biz
www.mpinfo.com.tw