

Documentation Complète

Déploiement, Supervision et Administration
de Cluster Via Rancher avec Traefik, MetalLB
et mkcert



Prérequis et Installation

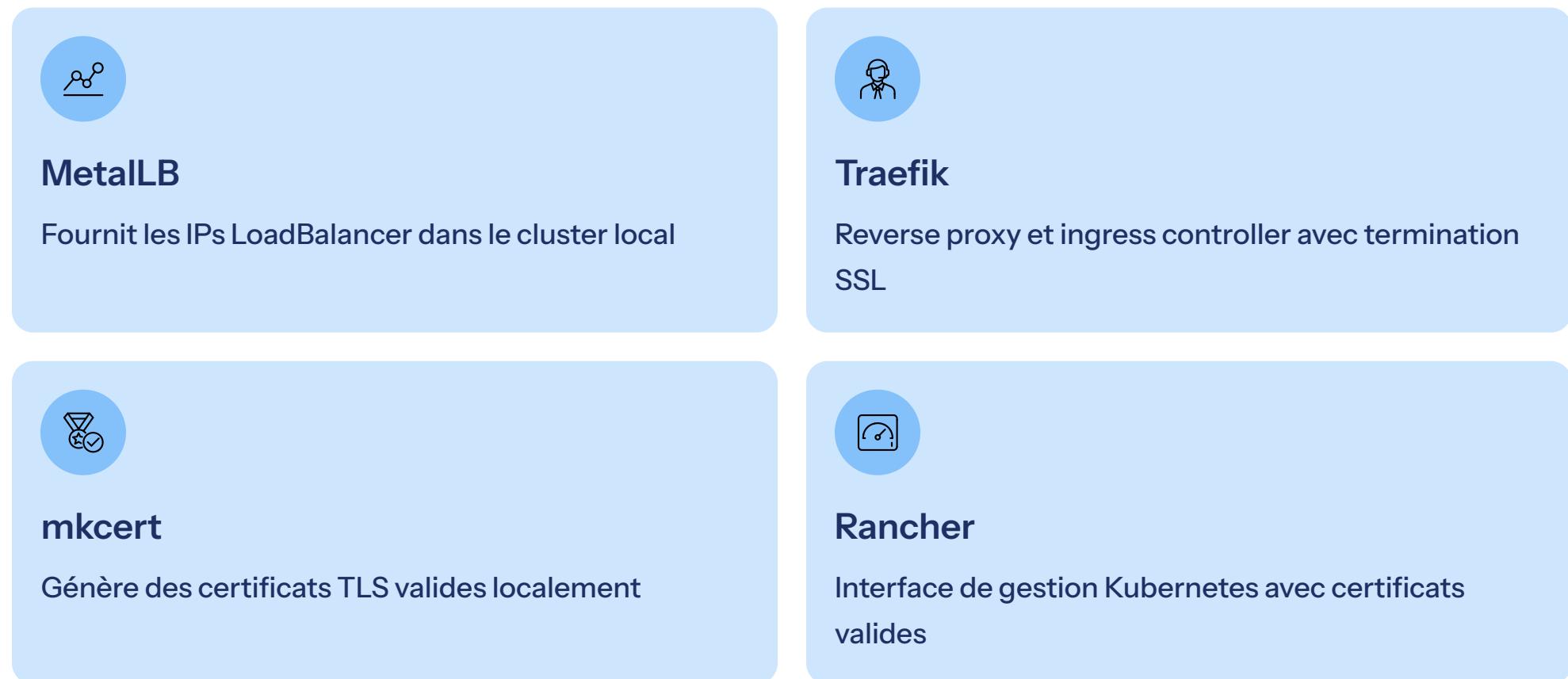
Une solution complète et professionnelle pour déployer Rancher avec des certificats TLS valides dans un environnement, intégrant MetalLB pour le load balancing et Traefik comme reverse proxy.

Architecture et Principe

Schéma d'Architecture



Principe de Fonctionnement



Prérequis et Installation

Prérequis Système

```
# Vérifier l'environnement  
kubectl version --short  
helm version  
ip addr show # Vérifier l'interface WiFi (10.64.13.203/24)
```

Structure du Projet

```
rancher-deployment/  
├── metalib/  
│   └── metalib-config.yaml  
├── namespace/  
│   └── namespace.yaml  
├── render/  
│   ├── rancher-ingress.yaml  
│   └── rancher-values.yaml  
└── scripts/  
    ├── checkstatus.sh  
    └── debug.sh
```

```
└── traefik/  
    └── traefik-values.yaml  
    └──  
        └── rancher-l8s.c1-i.pem  
        └── rancher-l8s.c1-i-key.pem  
        └── rancher-l8s.c1.pem  
    └── deploy.sh  
    └── check-start.sh
```

Configuration mkcert



Installation de mkcert

```
# Téléchargement et installation
wget -O mkcert https://github.com/FiloSottile/mkcert/releases/download/v1.4.4/mkcert-v1.4.4-linux-amd64
chmod +x mkcert
sudo mv mkcert /usr/local/bin/

# Installation de l'Autorité de Certification locale
mkcert -install
```

Génération des Certificats

```
# Générer le certificat pour le domaine et l'IP
mkcert rancher.k8s.ci 10.64.13.211 #votre ip correspondante

# Vérifier les fichiers générés
ls -la *.pem
# rancher.k8s.ci+1.pem # Certificat
# rancher.k8s.ci+1-key.pem # Clé privée
```

Création des Secrets Kubernetes

```
# Secret pour Traefik (format TLS)
kubectl create secret tls tls-rancher-ingress \
-n cattle-system \
--cert=rancher.k8s.ci+1.pem \
--key=rancher.k8s.ci+1-key.pem
```

Déploiement Pas à Pas

01

Préparation des Namespaces

Création des namespaces metallb-system, traefik-system et cattle-system avec les labels appropriés

03

Configuration Traefik

Déploiement de Traefik avec redirection HTTP vers HTTPS, activation TLS et service LoadBalancer

05

Configuration Ingress

Création de l'Ingress Kubernetes pour router le trafic HTTPS vers Rancher via Traefik

02

Configuration MetallB

Configuration de l'IPAddressPool (10.64.13.210-10.64.13.220) et du L2Advertisement pour le load balancing

04

Configuration Rancher

Installation de Rancher avec montage des certificats mkcert et désactivation de l'ingress natif

06

Lancement du Déploiement

Exécution du script deploy.sh pour automatiser l'ensemble du processus

Lancement du Déploiement

```
# Rendre les scripts exécutables  
chmod +x scripts/*.sh
```

```
# Lancer le déploiement complet  
.scripts/deploy.sh
```

Fichiers de Configuration

Configuration MetalLB

metallb/metallb-config.yaml

```
apiVersion: metallb.io/v1beta1
kind: IPAddressPool
metadata:
  name: my-ip-pool
  namespace: metallb-system
spec:
  addresses:
  - 10.64.13.210-10.64.13.220
---
apiVersion: metallb.io/v1beta1
kind: L2Advertisement
metadata:
  name: l2-ad
  namespace: metallb-system
spec: {}
```

Configuration Traefik

traefik/traefik-values.yaml

```
deployment:
replicas: 1
providers:
kubernetesIngress:
publishedService:
enabled: true
ports:
web:
redirectTo: websecure # Redirection HTTP → HTTPS automatique
websecure:
tls:
enabled: true # Activation TLS
ingressRoute:
dashboard:
enabled: true # Activation dashboard Traefik
service:
type: LoadBalancer # MetallB attribuera une IP
```

Configuration Rancher et Ingress

rancher/rancher-values.yaml

```
hostname: rancher.k8s.ci
replicas: 1
# DÉSACTIVATION de l'ingress Rancher - Traefik gère
ingress:
  enabled: false
service:
  type: LoadBalancer
# Montage du certificat mkcert dans Rancher
volumes:
- name: ssl-cert
  secret:
    secretName: tls-rancher-ingress # Secret créé avec mkcert
volumeMounts:
- name: ssl-cert
  mountPath: /etc/rancher/ssl
  readOnly: true
# Variables d'environnement pour utiliser le certificat
extraEnv:
- name: SSL_CERT_DIR
  value: /etc/rancher/ssl
- name: CATTLE_PROMETHEUS_METRICS
  value: "true"
resources:
limits:
  cpu: 1000m
  memory: 1536Mi
requests:
  cpu: 500m
  memory: 1024Mi
```

rancher/rancher-ingress.yaml

```
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: rancher
  namespace: cattle-system
  annotations:
    kubernetes.io/ingress.class: traefik
    traefik.ingress.kubernetes.io/router.entrypoints: websecure
    traefik.ingress.kubernetes.io/router.tls: "true"
spec:
  rules:
  - host: rancher.k8s.ci
    http:
      paths:
      - path: /
        pathType: Prefix
        backend:
          service:
            name: rancher
            port:
              number: 80
    tls:
    - hosts:
      - rancher.k8s.ci
      secretName: tls-rancher-ingress # Utilise le secret mkcert
```

Modification DNS/hosts

```
# Sur ta machine, modifie /etc/hosts pour pointer vers Traefik
sudo nano /etc/hosts

# Ajoute cette ligne :
10.64.13.210 rancher.k8s.ci

# Maintenant teste la validité du certificat
curl -v https://rancher.k8s.ci
```



Résolution des Problèmes

1

Certificat non reconnu

```
# Vérifier le certificat
présenté
openssl s_client -connect
rancher.k8s.ci:443 -
servername rancher.k8s.ci <
/dev/null | openssl x509 -
noout -issuer -subject
```

```
# Vérifier le secret
kubectl get secret -n cattle-
system tls-rancher-ingress -
o yaml
```

```
# Regénérer les certificats si
nécessaire
mkcert -uninstall
mkcert -install
mkcert rancher.k8s.ci
10.64.13.211
```

2

Services non accessibles

```
# Vérifier les IPs attribuées
kubectl get svc -A
```

```
# Vérifier les logs
kubectl logs -n traefik-
system deployment/traefik
kubectl logs -n cattle-system
-l app=rancher
```

```
# Vérifier la résolution DNS
nslookup rancher.k8s.ci
```

3

Ingress non configuré

```
# Vérifier l'ingress
kubectl describe ingress -n
cattle-system rancher
```

```
# Vérifier les endpoints
kubectl get endpoints -n
cattle-system rancher
```



Maintenance et Surveillance

Surveillance des Ressources

```
# Vérifier l'utilisation des ressources
```

```
kubectl top pods -A
```

```
kubectl top nodes
```

```
# Vérifier les événements
```

```
kubectl get events -A --sort-by='.lastTimestamp'
```

Sauvegarde des Certificats

```
# Sauvegarder les certificats mkcert
```

```
cp rancher.k8s.ci+1.pem
```

```
~/backup/
```

```
cp rancher.k8s.ci+1-key.pem
```

```
~/backup/
```

```
# Sauvegarder les secrets
```

```
kubectl get secret -n cattle-system tls-rancher-ingress -o yaml > ~/backup/secret-backup.yaml
```

Mise à Jour

```
# Mettre à jour Rancher  
helm upgrade rancher rancher-latest/rancher -n cattle-system -f rancher/rancher-values.yaml
```

```
# Mettre à jour Traefik
```

```
helm upgrade traefik traefik/traefik -n traefik-system -f traefik/traefik-values.yaml
```

Points Clés de la Solution

Avantages de l'Architecture

- Certificats Valides** : Plus d'avertissemnts de sécurité
- SSL Termination** : Traefik gère le TLS de manière centralisée
- Load Balancing** : MetalLB fournit des IPs stables
- Haute Disponibilité** : Architecture scalable

Flux de Trafic

- Client → HTTPS** avec certificat mkcert valide
- Traefik → Termination SSL et routage**
- Rancher → Service avec certificat monté**
- Réponse → Retour via Traefik avec chiffrement**

Sécurité

- Certificats TLS valides reconnus par les navigateurs
- Communication chiffrée de bout en bout
- Secrets Kubernetes sécurisés
- Contrôle d'accès via Ingress

Résultats

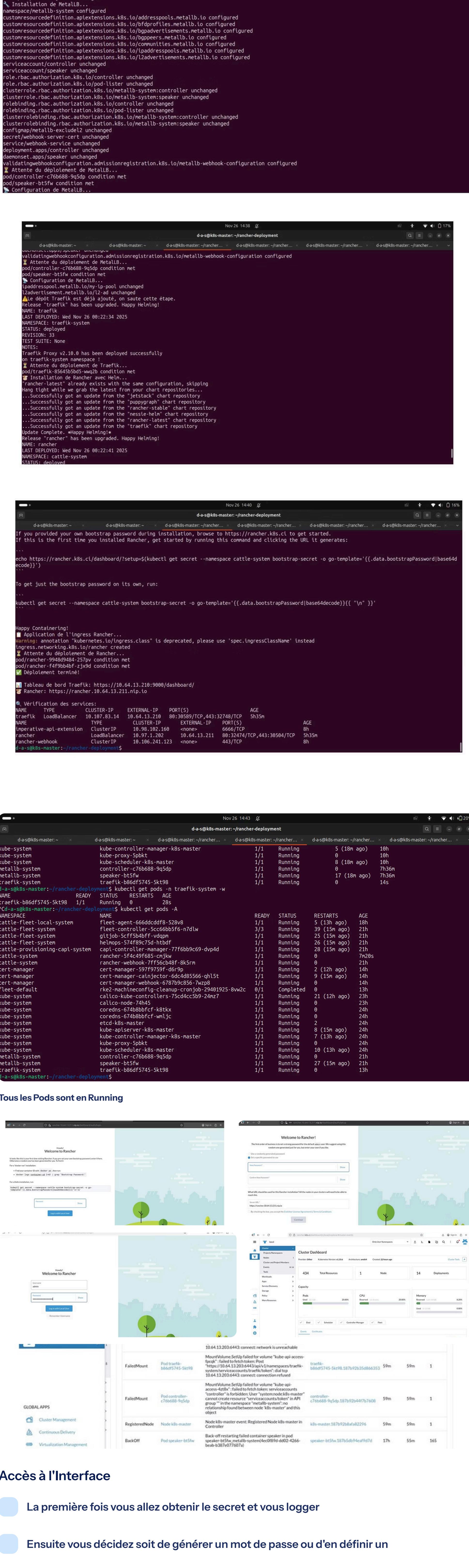
Exécution du Script de Déploiement

```
Nov 26 14:37 d-a-s@k8s-master:~/rancher-deployment
d-a-s@k8s-master:~ x d-a-s@k8s-master:~ x d-a-s@k8s-master:~/rancher... x d-a-s@k8s-master:~/rancher... x d-a-s@k8s-master:~/rancher... x d-a-s@k8s-master:~/rancher...
d-a-s@k8s-master:~/rancher-deployment$ ./scripts/deploy.sh
==> Déploiement de Rancher avec Traefik et MetalLB ==
  Installation des namespaces...
namespace/metalLB-system unchanged
namespace/traefik-system unchanged
namespace/cattle-system unchanged
  Installation de MetalLB...
namespace/metalLB-system configured
customresourcedefinition.apextensions.k8s.io/addresspools.metalLB.io configured
customresourcedefinition.apextensions.k8s.io/bfdprofiles.metalLB.io configured
customresourcedefinition.apextensions.k8s.io/bgpadvertisements.metalLB.io configured
customresourcedefinition.apextensions.k8s.io/bgppeers.metalLB.io configured
customresourcedefinition.apextensions.k8s.io/communities.metalLB.io configured
customresourcedefinition.apextensions.k8s.io/l2addresspools.metalLB.io configured
customresourcedefinition.apextensions.k8s.io/l2advertisements.metalLB.io configured
serviceaccount/controller unchanged
serviceaccount/speaker unchanged
role.rbac.authorization.k8s.io/controller unchanged
role.rbac.authorization.k8s.io/pod-lister unchanged
clusterrole.rbac.authorization.k8s.io/metalLB-system:controller unchanged
clusterrole.rbac.authorization.k8s.io/metalLB-system:speaker unchanged
rolebinding.rbac.authorization.k8s.io/controller unchanged
rolebinding.rbac.authorization.k8s.io/pod-lister unchanged
clusterrolebinding.rbac.authorization.k8s.io/metalLB-system:controller unchanged
clusterrolebinding.rbac.authorization.k8s.io/metalLB-system:speaker unchanged
configmap/metalLB-excludeL2 unchanged
secret/webhook-server-cert unchanged
service/webhook-service unchanged
deployment.apps/controller unchanged
daemonset.apps/speaker unchanged
validatingwebhookconfiguration.admissionregistration.k8s.io/metalLB-webhook-configuration configured
  Attente du déploiement de MetalLB...
pod/controller-c76b688-9q5dp condition met
pod/speaker-bt5fw condition met
Configuration de MetalLB...
```

```
Nov 26 14:38 d-a-s@k8s-master:~/rancher-deployment
d-a-s@k8s-master:~ x d-a-s@k8s-master:~ x d-a-s@k8s-master:~/rancher... x d-a-s@k8s-master:~/rancher... x d-a-s@k8s-master:~/rancher... x d-a-s@k8s-master:~/rancher...
d-a-s@k8s-master:~/rancher-deployment$ ./scripts/deploy.sh
  validating webhook configuration.admissionregistration.k8s.io/metalLB-webhook-configuration configured
  Attente du déploiement de MetalLB...
pod/controller-c76b688-9q5dp condition met
pod/speaker-bt5fw condition met
  Configuration de MetalLB...
ipaddresspool.metalLB.io/my-ip-pool unchanged
l2advertisment.metalLB.io/l2-ad unchanged
⚠️ Le dépôt Traefik est déjà ajouté, on saute cette étape.
Release "traefik" has been upgraded. Happy Helming!
NAME: traefik
LAST DEPLOYED: Wed Nov 26 00:22:34 2025
NAMESPACE: traefik-system
STATUS: deployed
REVISION: 33
TEST SUITE: None
NOTES:
Traefik Proxy v2.10.0 has been deployed successfully
on traefik-system namespace !
  Attente du déploiement de Traefik...
pod/traefik-85645b5bd-wqzqb condition met
  Installation de Rancher avec Helm...
"rancher-latest" already exists with the same configuration, skipping
Hang tight while we grab the latest from your chart repositories...
...Successfully got an update from the "jetstack" chart repository
...Successfully got an update from the "poppygraph" chart repository
...Successfully got an update from the "rancher-stable" chart repository
...Successfully got an update from the "nessie-helm" chart repository
...Successfully got an update from the "rancher-latest" chart repository
...Successfully got an update from the "traefik" chart repository
Update Complete. *Happy Helming*
Release "rancher" has been upgraded. Happy Helming!
NAME: rancher
LAST DEPLOYED: Wed Nov 26 00:22:41 2025
NAMESPACE: cattle-system
STATUS: deployed
Nov 26 14:40 d-a-s@k8s-master:~/rancher-deployment
d-a-s@k8s-master:~ x d-a-s@k8s-master:~ x d-a-s@k8s-master:~/rancher... x d-a-s@k8s-master:~/rancher... x d-a-s@k8s-master:~/rancher... x d-a-s@k8s-master:~/rancher...
d-a-s@k8s-master:~/rancher-deployment$ echo https://rancher.k8s.ci/dashboard/?setup=$(kubectl get secret --namespace cattle-system bootstrap-secret -o go-template='{{.data.bootstrapPassword|base64decode}}')
...
To get just the bootstrap password on its own, run:
...
kubectl get secret --namespace cattle-system bootstrap-secret -o go-template='{{.data.bootstrapPassword|base64decode}}'{{"\n" }}'
...
Happy Containering!
  Application de l'ingress Rancher...
Warning: annotation "kubernetes.io/ingress.class" is deprecated, please use 'spec.ingressClassName' instead
ingress.networking.k8s.io/rancher created
  Attente du déploiement de Rancher...
pod/rancher-9948d9484-257pv condition met
pod/rancher-f4f9b4bf-zjx9d condition met
  Déploiement terminé!
  Tableau de bord Traefik: https://10.64.13.210:9000/dashboard/
  Rancher: https://rancher.10.64.13.211.ngrok.io

  Vérification des services:
  NAME   TYPE   CLUSTER-IP   EXTERNAL-IP   PORT(S)   AGE
  traefik LoadBalancer  10.107.83.14  10.64.13.210  80:30589/TCP,443:32748/TCP  Sh35m
  NAME   TYPE   CLUSTER-IP   EXTERNAL-IP   PORT(S)   AGE
  imperative-api-extension ClusterIP  10.98.102.160  <none>    6666/TCP  8h
  rancher   LoadBalancer  10.97.1.202  10.64.13.211  80:32474/TCP,443:30504/TCP  Sh35m
  rancher-webhook ClusterIP  10.106.241.123  <none>    443/TCP   8h
d-a-s@k8s-master:~/rancher-deployment$ kubectl get pods -n traefik-system -w
NAME          READY   STATUS    RESTARTS   AGE
traefik-b86df5745-5kt98  1/1     Running   0          28s
d-a-s@k8s-master:~/rancher-deployment$ kubectl get pods -n traefik-system -A
NAMESPACE   NAME          READY   STATUS    RESTARTS   AGE
cattle-fleet-local-system fleet-agent-666ddcdff8-528v8  1/1     Running   5 (13h ago)  18h
cattle-fleet-system   fleet-controller-5cc66bb5f6-n7dlw  3/3     Running   39 (15m ago)  21h
cattle-fleet-system   gitjob-5cff4bcbf7-vdqpr  1/1     Running   25 (15m ago)  21h
cattle-fleet-system   helmops-574f89c75d-htbdf  1/1     Running   26 (15m ago)  21h
cattle-provisioning-capi-system capi-controller-manager-77f6bb9c69-dvp4d  1/1     Running   28 (15m ago)  21h
cattle-system   rancher-5f4c49f685-cmjkw  1/1     Running   0          7m20s
cattle-system   rancher-webhook-7ff56cb4bf-8k5rm  1/1     Running   0          21h
cert-manager   cert-manager-597f9759f-d6r9p  1/1     Running   2 (12h ago)  14h
cert-manager   cert-manager-cainjector-6dc4d85566-qhl5t  1/1     Running   9 (15m ago)  14h
cert-manager   cert-manager-webhook-6787b9c856-7wz8p  1/1     Running   0          14h
fleet-default   rke2-machineconfig-cleanup-cronjob-29401925-8w2c  0/1     Completed  0          13h
kube-system   calico-kube-controllers-75cd4cc5b9-24mz7  1/1     Running   21 (12h ago)  23h
kube-system   calico-node-74h45  1/1     Running   0          23h
kube-system   coredns-674b8bbfcf-k8tx  1/1     Running   0          24h
kube-system   coredns-674b8bbfcf-wmljc  1/1     Running   0          24h
kube-system   etcd-k8s-master  1/1     Running   2          24h
kube-system   kube-apiserver-k8s-master  1/1     Running   8 (15m ago)  24h
kube-system   kube-controller-manager-k8s-master  1/1     Running   7 (13h ago)  24h
kube-system   kube-proxy-5pbkt  1/1     Running   0          24h
kube-system   kube-scheduler-k8s-master  1/1     Running   10 (13h ago)  24h
metallb-system controller-c76b688-9q5dp  1/1     Running   0          21h
metallb-system speaker-bt5fw  1/1     Running   27 (15m ago)  21h
traefik-system traefik-b86df5745-5kt98  1/1     Running   0          13h
d-a-s@k8s-master:~/rancher-deployment$
```

Tous les Pods sont en Running



Accès à l'Interface

La première fois vous allez obtenir le secret et vous logger

Ensuite vous décidez soit de générer un mot de passe ou d'en définir un

On se connecte

On peut voir les informations sur notre Cluster

On peut superviser notre cluster s'il y a des erreurs ou tout s'est bien passé, voir l'état du cluster et administrer, gérer le cluster et plein d'autres choses, Amusez-Vous !

Cette documentation fournit une solution complète et professionnelle pour déployer Rancher avec des certificats TLS valides dans un environnement.