

Politechnika Warszawska

W Y D Z I A Ł E L E K T R Y C Z N Y



Instytut Elektrotechniki Teoretycznej
i Systemów Informacyjno-Pomiarowych
Zakład Elektrotechniki Teoretycznej
i Informatyki Stosowanej

Praca dyplomowa inżynierska

na kierunku Informatyka
w specjalności Inżynieria oprogramowania

Implementacja i testy wydajności środowiska Kubernetes na
maszynach bezdyskowych

Krzysztof Nazarewski

nr albumu 123456

promotor
mgr inż. Andrzej Toboła

WARSZAWA 2018

Implementacja i testy wydajności środowiska Kubernetes na maszynach bezdyskowych

Streszczenie

Celem tej pracy inżynierskiej jest przybliżenie czytelnikowi zagadnień związanych z uruchamianiem systemu Kubernetes na maszynach bezdyskowych.

Zacznę od wyjaśnienia pojęcia systemu bezdyskowego oraz sposobu jego funkcjonowania na przykładzie sieci uczelnianej i wzorującego się na niej przygotowanie przeze mnie lokalnego środowiska.

Następnie opiszę problem izolacji i przydzielania zasobów systemowych na przykładzie wirtualnych maszyn, chroot i konteneryzacji.

W głównej części dokumentu przedstawię pojęcie orkiestrami kontenerami, w jaki sposób odnosi się do wcześniej postawionych problemów. Opiszę alternatywy Kubernetes, jego architekturę oraz sposoby uruchamiania. Na koniec spróbuję uruchomić Kubernetes na maszynach bezdyskowych, problemy z tym związane oraz przedstawię wyniki.

Słowa kluczowe: praca dyplomowa, LaTeX, jakość

Implementing and testing Kubernetes running on diskless machines

Abstract

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Morbi ac dolor scelerisque, malesuada ex vel, feugiat augue. Suspendisse dictum, elit efficitur vestibulum eleifend, mi neque accumsan velit, at ultricies ex lectus et urna. Pellentesque vel lorem turpis. Donec blandit arcu lacus, vitae dapibus tellus tempus et. Etiam orci libero, mollis in dapibus tempor, rutrum eget magna. Nullam congue libero non velit suscipit, vel cursus elit commodo. Praesent mollis augue quis lorem laoreet, condimentum scelerisque ex pharetra. Sed est ex, gravida a porta in, tristique ac nunc. Nunc at varius sem, sit amet consectetur velit.

Keywords: thesis, LaTeX, quality

WARSZAWA, 1 lutego 1234

POLITECHNIKA WARSZAWSKA
WYDZIAŁ ELEKTRYCZNY

OŚWIADCZENIE

Świadom odpowiedzialności prawnej oświadczam, że niniejsza praca dyplomowa inżynierska pt. Implementacja i testy wydajności środowiska Kubernetes na maszynach bezdyskowych:

- została napisana przeze mnie samodzielnie,
- nie narusza niczyich praw autorskich,
- nie zawiera treści uzyskanych w sposób niezgodny z obowiązującymi przepisami.

Oświadczam, że przedłożona do obrony praca dyplomowa nie była wcześniej podstawą postępowania związanego z uzyskaniem dyplomu lub tytułu zawodowego w uczelni wyższej. Jestem świadom, że praca zawiera również rezultaty stanowiące własności intelektualne Politechniki Warszawskiej, które nie mogą być udostępniane innym osobom i instytucjom bez zgody Władz Wydziału Elektrycznego.

Oświadczam ponadto, że niniejsza wersja pracy jest identyczna z załączoną wersją elektroniczną.

Krzysztof Nazarewski.....

Spis treści

1	Test	1
2	Wstęp	2
3	Systemy bezdyskowe	3
3.1	Proces uruchamiania maszyny bezdyskowej	3
4	Przegląd pojęć i systemów związanych z konteneryzacją	4
4.1	Kubernetes	4
4.2	Open Container Initiative	4
4.3	Zarządzanie Kubernetes bez graficznego interfejsu	5
4.3.1	kubeadm	5
4.3.2	Kubescape	5
4.3.3	OpenShift Ansible	5
4.3.4	Eksperymentalne i deprecowane rozwiązania	5
4.4	Graficzne nakładki na Kubernetes	6
4.4.1	Kubernetes Dashboard	6
4.4.2	Rancher	6
4.4.3	OpenShift by Red Hat	6
4.4.4	DC/OS	6
4.5	Alternatywne rozwiązania zarządzania kontenerami	7
4.5.1	Fleet	7
4.5.2	Docker Swarm	7
4.5.3	Mesos	7
4.5.4	Nomad	7
4.6	Alternatywy Dockera	7
4.7	Architektura	8
4.7.1	Komunikacja sieciowa	8
4.7.2	Składowe kontrolujące klaster	8
4.7.3	Składowe workera	8

5	Przegląd systemów operacyjnych	9
5.1	Konfigurator cloud-init	9
5.1.1	Dostępne implementacje	10
5.2	CoreOS	11
5.2.1	Konfiguracja	11
5.3	RancherOS	11
5.3.1	Konfiguracja	12
5.4	Project Atomic	12
5.4.1	Konfiguracja	12
5.5	Alpine Linux	13
5.5.1	Konfiguracja	13
5.6	ClearLinux	13
5.6.1	Linki	13
6	Sposoby konfiguracji klastra Kubernetes	14
6.1	Rancher 2.0	14
6.2	kubespary-cli	15
6.3	kubespary	17
6.3.1	Kubernetes Dashboard	18
6.3.2	Napotkane błędy	18
7	Q&A	20
7.1	Czy wszystko zawsze trzeba ściągac z netu - nie mozna z lokalnego serwera?	20
7.2	Jak zachować stan bezdyskowego RancherOS'a?	20
7.3	Co musi zawierac cloud-config dla serwera a co dla agentow?	20
	Bibliografia	21

Podziękowania

Dziękujemy bardzo serdecznie wszystkim, a w szczególności Rodzinom i Unii Europejskiej...

Zdolny Student i Pracowity Kolega

Rozdział 1

Test

The seminal work (Pizza i in. 2000)

Rozdział 2

Wstęp

Rozdział 3

Systemy bezdyskowe

3.1 Proces uruchamiania maszyny bezdyskowej

Na uruchamianie maszyn bezdyskowych w protokole PXE składają się 3 podstawowe elementy: 1. serwer DHCP, np. isc-dhcp-server lub dnsmasq 2. firmware wspierające PXE, np. iPXE 3. serwer plików (np. TFTP, HTTP, NFS) i/lub sieciowej pamięci masowej (np. iSCSI)

Rozdział 4

Przegląd pojęć i systemów związanych z konteneryzacją

W związku z mnogością pojęć związanych z izolacją, konteneryzacją i zarządzaniem systemami komputerowymi zdecydowałem się pokrótce przybliżyć najważniejsze pojęcia z tematem związane.

4.1 Kubernetes

Kubernetes¹ jest jednym z najpopularniejszych narzędzi orkiestracji kontenerami i tematem przewodnim tego dokumentu. Został stworzony przez Google na bazie ich wewnętrznego systemu Borg.

- Choosing the Right Containerization and Cluster Management Tool²

4.2 Open Container Initiative

Open Container Initiative³ jest inicjatywą tworzenia i utrzymywania publicznych standardów związanych z formatem i uruchamianiem kontenerów.

Większość projektów związanych z konteneryzacją dąży do kompatybilności ze standardami OCI, m. in.: - Docker⁴ - Kubernetes CRI-O⁵ - Docker on

¹<https://kubernetes.io/>

²<https://dzone.com/articles/choosing-the-right-containerization-and-cluster-management-tool>

³<https://www.opencontainers.org/about>

⁴<https://blog.docker.com/2017/07/demystifying-open-container-initiative-oci-specifications/>

⁵<https://github.com/kubernetes-incubator/cri-o>

FreeBSD⁶ - Running CloudABI applications on a FreeBSD based Kubernetes cluster, by Ed Schouten (EuroBSDcon '17)⁷

4.3 Zarządzanie Kubernetes bez graficznego interfejsu

4.3.1 kubeadm

- kubeadm⁸
- Install with kubadm⁹

4.3.2 Kubespray

- kubespray¹⁰
- zestaw skryptów Ansible konfigurujących klaster na jednym z wielu systemów operacyjnych
- dąży do zostania tzw. Operatorem¹¹ korzystającym z kubeadm

4.3.3 OpenShift Ansible

Konfiguracja OpenShift Origin realizowana jest zestawem skryptów Ansible'owych rozwijanych jako projekt openshift-ansible¹².

4.3.4 Eksperymentalne i deprekowane rozwiązania

- Fedora via Ansible¹³ deprekowane na rzecz kubespray
- Rancher Kubernetes Installer¹⁴

⁶<https://wiki.freebsd.org/Docker>

⁷<https://www.youtube.com/watch?v=akLa9L500NY>

⁸<https://kubernetes.io/docs/reference/setup-tools/kubeadm/kubeadm/>

⁹<https://kubernetes.io/docs/setup/independent/install-kubeadm/>

¹⁰<https://github.com/kubernetes-incubator/kubespray>

¹¹<https://github.com/kubernetes-incubator/kubespray/blob/master/docs/comparisons.md>

¹²<https://github.com/openshift/openshift-ansible>

¹³https://kubernetes.io/docs/getting-started-guides/fedora/fedora_ansible_config/

¹⁴<http://rancher.com/announcing-rke-lightweight-kubernetes-installer/>

4.4 Graficzne nakładki na Kubernetes

4.4.1 Kubernetes Dashboard

Kubernetes Dashboard¹⁵ jest wbudowanym interfejsem graficznym klastra Kubernetes. Umożliwia monitorowanie i zarządzanie klastrem w ramach funkcjonalności samego Kubernetes.

4.4.2 Rancher

Rancher¹⁶ jest platformą zarządzania kontenerami umożliwiającą między innymi zarządzanie klastrem Kubernetes. Od wersji 2.0 twórcy skupiają się tylko i wyłącznie na zarządzaniu Kubernetes porzucając inne rozwiązania.

4.4.3 OpenShift by Red Hat

OpenShift jest komercyjną usługą typu PaaS (Platform as a Service), od wersji 3 skupia się na zarządzaniu klastrem Kubernetes.

Rdzeniem projektu jest open sourcowy OpenShift Origin¹⁷ konfigurowany przez OpenShift Ansible.

- OpenShift Origin vs Kubernetes¹⁸
- The Differences Between Kubernetes and OpenShift¹⁹
- Demo konsoli²⁰ (niestety po hebrajsku)

4.4.4 DC/OS

Datacenter Operating System²¹ jest częścią Mesosphere²² i Mesosa. Niedawno został rozszerzony o Kubernetes²³ jako alternatywnego (w stosunku do Marathon²⁴) systemu orkiestracji kontenerami.

¹⁵<https://github.com/kubernetes/dashboard>

¹⁶<https://rancher.com/>

¹⁷<https://github.com/openshift/origin>

¹⁸https://www.reddit.com/r/devops/comments/59ql4r/openshift_origin_vs_kubernetes/

¹⁹<https://medium.com/levvel-consulting/the-differences-between-kubernetes-and-openshift-ae7780>

²⁰<https://youtu.be/-mFovK19aB4?t=6m54s>

²¹<https://dcos.io/>

²²<https://mesosphere.com/>

²³<https://mesosphere.com/blog/kubernetes-dcos/>

²⁴<https://mesosphere.github.io/marathon/>

4.5 Alternatywne rozwiązania zarządzania kontenerami

4.5.1 Fleet

Fleet²⁵ jest nakładką na systemd²⁶ realizującą rozproszony system inicjalizacji systemów. Kontenery są uruchamiane i zarządzane przez systemd.

4.5.2 Docker Swarm

Docker Swarm²⁷ jest rozwiązaniem orkiestracji kontenerami od twórców samego Docker'a. Proste w konfiguracji, nie oferuje tak dużych możliwości jak niżej wymienione.

4.5.3 Mesos

- Apache Mesos²⁸ zaawansowane narzędzie orkiestracji kontenerami.
- An Introduction to Mesosphere²⁹

4.5.4 Nomad

HasiCorp Nomad vs Kubernetes³⁰

4.6 Alternatywy Dockera

- rkt vs other projects³¹
- Linux Containers³² od Canonical # Kubernetes

²⁵<https://coreos.com/fleet/docs/latest/launching-containers-fleet.html>

²⁶<https://www.freedesktop.org/wiki/Software/systemd/>

²⁷<https://docs.docker.com/engine/swarm/>

²⁸<http://mesos.apache.org/>

²⁹<https://www.digitalocean.com/community/tutorials/an-introduction-to-mesosphere>

³⁰<https://www.nomadproject.io/intro/vs/kubernetes.html>

³¹<https://coreos.com/rkt/docs/latest/rkt-vs-other-projects.html>

³²<https://linuxcontainers.org/>

4.7 Architektura

4.7.1 Komunikacja sieciowa

4 rodzaje sieci: 1. komunikacja wewnątrz Podów (localhost) 2. komunikacja między Podami (SDN/CNI, np. flannel, Calico) 3. komunikacja między Podami i Serwisami (kube-proxy) 4. komunikacja świata z Serwisami

4.7.2 Składowe kontrolujące klaster

- etcd - przechowywanie stanu klastra
- kube-apiserver - interfejs konfiguracyjny klastra (zarówno wewnętrzny jak i zewnętrzny), prowadzi interakcję tylko ze stanem klastra w etcd
- kube-scheduler - proces decydujący na którym węźle klastra uruchamiać Pody (na podstawie dostępnych zasobów, obecnego obciążenia itp.). W skrócie zarządza popytem i podażą na zasoby klastra.
- kube-controller-manager - kontroler klastra dążący do doprowadzenia obecnego stanu klastra do pożądanego na podstawie informacji z kube-apiserver

4.7.3 Składowe workera

- kubelet - monitoruje i kontroluje stan pojedynczego węzła. Na przykład restartuje Pod, który przestał działać na tym samym węźle.
- kube-proxy - proxy i load balancer odpowiedzialny za przekierowanie ruchu do odpowiedniego kontenera
- cAdvisor - monitoruje zużycie zasobów i wydajność kontenerów w ramach jednego węzła

Rozdział 5

Przegląd systemów operacyjnych

Ze względu na obszerność i niejednoznaczność tematu cloud-init rozdział rozpoczne od jego omówienia.

Wszystkie moduły Kubernetes’a są uruchamiane w kontenerach, więc jedynym absolutnie niezbędnym wymaganiem jest uruchamianie Docker’a

Wymaganiami związku z naszym zastosowaniem:

- zdalny dostęp SSH,
- działanie w środowisku bezdyskowym,
- wsparcie narzędzia, którym konfigurujemy Kubernetes

Podstawowe wyznaczniki:

- czy PXE boot działa?
- sposób konfiguracji maszyny
- rozmiar bootowalnego obrazu (kernela i initrd)
- rozmiar minimalnego działającego systemu (z zainstalowanym SSH i Dockerem)
- obsługa NFS/NBD/iSCSI root’a? (zmniejszenie zajmowanego RAMu)

5.1 Konfigurator cloud-init

cloud-init¹ jest standardem oraz implementacją konfiguratora kompatybilnego z wieloma systemami operacyjnymi przeznaczonymi do działania w chmurze.

Standard polega na dostarczeniu pliku konfiguracyjnego w formacie YAML² w trakcie lub tuż po inicjalizacji systemu operacyjnego.

¹<https://cloud-init.io/>

²<http://yaml.org/>

5.1.1 Dostępne implementacje

cloud-init

Referencyjny cloud-init zaimplementowany jest w Pythonie, co częściowo tłumaczy duży rozmiar obrazów przeznaczonych dla chmury. Po najmniejszych obrazach Pythona dla Dockera³ (python:alpine - 89MB i python2:alpine - 72 MB) wnioskuję, że nie istnieje mniejsza dystrybucja Pythona.

```
1 docker pull python:2-alpine > /dev/null
2 docker pull python:alpine > /dev/null
3 docker images | grep alpine
```

Wywiad z developerem cloud-init⁴

coreos-cloudinit

coreos-cloudinit⁵ jest częściową implementacją standardu w języku Go przez twórców CoreOS. Niestety rok temu przestał być rozwijany⁶ i wychodzi z użytku.

RancherOS + coreos-cloudinit

rancher cloud-init⁷ jest spadkobiercą⁸ coreos-cloudinit rozwijanym przez zespół RancherOS, na jego potrzeby.

clr-cloud-init

clr-cloud-init⁹ jest wewnętrzną implementacją standardu dla systemu ClearLinux. Powstała z chęci optymalizacji standardu pod ClearLinux oraz pozbycia się zależności referencyjnej implementacji od Python'a.

³https://hub.docker.com/_/python/

⁴<https://www.podcastinit.com/cloud-init-with-scott-moser-episode-126>

⁵<https://github.com/coreos/coreos-cloudinit>

⁶<https://github.com/coreos/coreos-cloudinit/commit/3460ca4414fd91de66cd581d997bf453fd895b67>

⁷<http://rancher.com/docs/os/latest/en/configuration/>

⁸<https://github.com/rancher/os/commit/e2ed97648ad63455743ebc16080a82ee47f8bb0c>

⁹<https://clearlinux.org/blogs/announcing-clr-cloud-init>

5.2 CoreOS

CoreOS¹⁰ jest pierwszą dystrybucją linuxa dedykowaną zarządzaniu kontenerami. Zawiera dużo narzędzi dedykowanych klastrowaniu i obsłudze kontenerów, w związku z tym zajmuje 342 MB.

- czysta instalacja zajmuje około 600 MB pamięci RAM

5.2.1 Konfiguracja

Konfiguracja przez Container Linux Config¹¹ transpilowany do Ignition¹². Transpiler konwertuje ogólną konfigurację na przygotowaną pod konkretne chmury (AWS, GCE, Azure itp.). Dyskwalifikującą wadą tego typu konfiguracji jest brak wsparcia transpilatora dla systemów z rodziny BSD

Poprzednikiem Ignition jest coreos-cloudinit.

5.3 RancherOS

RancherOS¹³ jest systemem operacyjnym, w którym tradycyjny system inicjalizacji został zastąpiony trzema poziomami Dockera¹⁴:

- `bootstrap_docker` działający w initramie, czyli przygotowujący system,
- `system-docker` zastępuje tradycyjnego inita, zarządza wszystkimi programami systemowymi,
- `docker` standardowy docker, interakcja z nim nie może uszkodzić działającego systemu,

Jego głównymi zaletami są mały rozmiar plików startowych (45 MB) oraz prostota konfiguracji.

- zajmuje 700 MB pamięci RAM,

¹⁰<https://coreos.com/>

¹¹<https://coreos.com/os/docs/latest/provisioning.html>

¹²<https://coreos.com/ignition/docs/latest/>

¹³<https://rancher.com/rancher-os/>

¹⁴<http://rancher.com/docs/os/latest/en/configuration/docker/>

5.3.1 Konfiguracja

RancherOS jest konfigurowany przez własną wersję coreos-cloudinit.

Znaczną przewagą nad oryginałem jest możliwość sekwencyjnego uruchamiania dowolnej ilości plików konfiguracyjnych.

Minimalna konfiguracja pozwalająca na zalogowanie:

```
1 #cloud-config
2 ssh_authorized_keys:
3   - ssh-rsa AAAAB3N...
```

Generuję ją poniższym skryptem na podstawie komendy `ssh-add -L`:

```
1 echo "#cloud-config
2 ssh_authorized_keys:
3 $(ssh-add -L | sed 's/^/ - /g')"
```

Przydatne jest wyświetlenie kompletnej konfiguracji komendą `ros config`
↪ `export --full`¹⁵.

Niestety aktualnie RancherOS nie zawsze czyta `cloud-config`¹⁶.

5.4 Project Atomic

Project Atomic¹⁷ jest grupą podobnie skonfigurowanych systemów operacyjnych dedykowaną środowiskom cloud i kontenerom.

Dystrybucje Project Atomic nazywają się Atomic Host, dostępne są następujące warianty:

- Red Hat Atomic Host¹⁸
- CentOS Atomic Host¹⁹
- Fedora Atomic Host²⁰

5.4.1 Konfiguracja

Atomic Host są konfigurowane systemem `cloud-init`²¹,

¹⁵<https://forums.rancher.com/t/good-cloud-config-reference/5238/3>

¹⁶<https://github.com/rancher/os/issues/2204>

¹⁷<https://www.projectatomic.io/>

¹⁸<https://www.redhat.com/en/resources/enterprise-linux-atomic-host-datasheet>

¹⁹<https://wiki.centos.org/SpecialInterestGroup/Atomic/Download/>

²⁰<https://getfedora.org/atomic/download/>

²¹<https://cloud-init.io/>

5.5 Alpine Linux

Alpine Linux²² jest minimalną dystrybucją Linuxa bazowaną na musl-libc i busybox.

Niestety nie bootuje się w trybie diskless ze względu na błąd, którego twórcy nie umieją naprawić.

5.5.1 Konfiguracja

Alpine Backup²³ - spakowane pliki wypakowywane w sekwencji bootu
Alpine Configuration Framework²⁴

5.6 ClearLinux

ClearLinux²⁵

- “bundle” zamiast pakietów systemowych aktualizowane z całym systemem,
- skoncentrowany na wydajności na procesorach Intel,
- skąpa i trudna w nawigacji dokumentacja systemu,
- lokalizacja wszystkich modyfikacji w /var i /etc (prosty reset),
- instalacja samego docker’a + serwera ssh zajmuje 700 MB w RAMie

5.6.1 Linki

- <https://www.infoworld.com/article/3159658/linux/6-key-points-about-intels-hot-new-linux-distro.html>

²²<https://alpinelinux.org/>

²³https://wiki.alpinelinux.org/wiki/Alpine_local_backup

²⁴http://wiki.alpinelinux.org/wiki/Alpine_Configuration_Framework_Design

²⁵<https://clearlinux.org/>

Rozdział 6

Sposoby konfiguracji klastra Kubernetes

Najpopularniejszym rozwiązaniem konfiguracji klastra Kubernetes jest kops¹, ale jak większość rozwiązań zakłada uruchomienie w środowiskach chmurowych, PaaS lub IaaS. W związku z tym nie ma żadnego zastosowania w tej pracy inżynierskiej.

6.1 Rancher 2.0

Wygodne narzędzie do uruchamiania i monitorowania klastra Kubernetes, ale wymaga interakcji użytkownika. Wersja 2.0 (obecnie w fazie alpha) oferuje lepszą integrację z Kubernetes całkowicie porzucając inne platformy.

```
1 #rancher_version=latest
2 rancher_version=preview
3 docker run --rm --name rancher -d -p 8080:8080 rancher/server:$
  ↪ {rancher_version}
```

Najpierw należy zalogować się do panelu administracyjnego Ranchera i przeprowadzić podstawową konfigurację (adres Ranchera + uzyskanie komendy).

Następnie w celu dodania węzła do klastra wystarczy wywołać jedną komendę udostępnioną w panelu administracyjnym Ranchera na docelowym węźle, jej domyślny format to:

```
1 wersja_agenta=v1.2.9
2 ip_ranchera=192.168.56.1
```

¹<https://github.com/kubernetes/kops>

```

3 skrypt=B52944BEFAA613FOCE90:1514678400000:
  ↪ E2yB6KfxzSix4YHti39BTw5RbKw
4
5 sudo docker run --rm --privileged \
6   -v /var/run/docker.sock:/var/run/docker.sock \
7   -v /var/lib/rancher:/var/lib/rancher \
8   rancher/agent:${wersja_agenta} \
9   http://${ip_ranchera}:8080/v1/scripts/${skrypt}

```

W ciągu 2 godzin przeglądu nie udało mi się zautomatyzować procesu uzyskiwania ww. komendy.

Następnie w cloud-config'u RancherOS'a możemy dodać ww. komendę w formie:

```

1 #cloud-config
2 runcmd:
3 - docker run --rm --privileged -v /var/run/docker.sock:/var/run
  ↪ /docker.sock -v /var/lib/rancher:/var/lib/rancher
  ↪ rancher/agent:v1.2.9 http://192.168.56.1:8080/v1/scripts
  ↪ /...

```

Od wersji 2.0 umożliwia połączenie się z istniejącym klastrem:

```

1 kubectl apply -f http://192.168.56.1:8080/v3/scripts/303
  ↪ F60E1A5E186F53F3F:1514678400000:
  ↪ wstQFdHpOgHqKahoYdmsCXEWMW4.yaml

```

W wersji v2.0.0-alpha10 losowo pojawia się błąd Upgrade Environment².

6.2 kubespray-cli

Jest to narzędzie ułatwiające korzystanie z **kubespray**. Z powodu błędu³ logiki narzędzie nie radzi sobie z brakiem Python'a na domyślnej dystrybucji CoreOS'a, mimo że sam **kubespray** radzi sobie z nim świetnie. Do uruchomienia na tym systemie potrzebne jest ręczne wywołanie roli **bootstrap-os**⁴ z **kubespray** zanim przystąpimy do właściwego deploy'u.

```

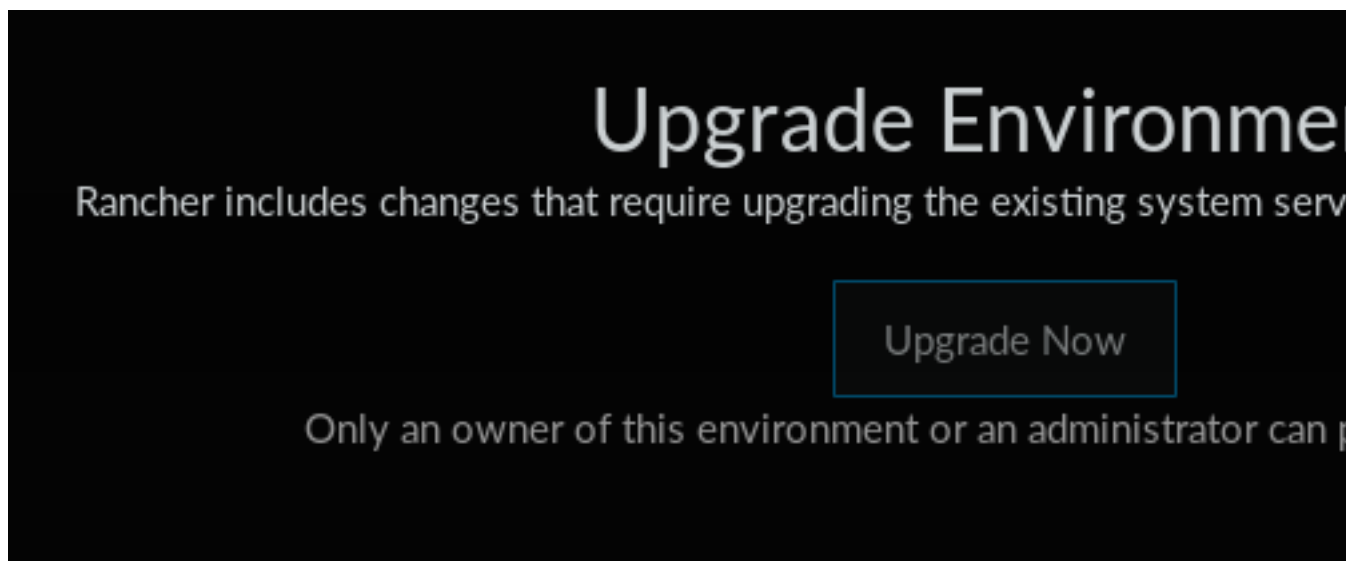
1 #!/usr/bin/env bash
2 set -e

```

²<https://github.com/rancher/rancher/issues/10396>

³<https://github.com/kubespray/kubespray-cli/issues/120>

⁴<https://github.com/kubernetes-incubator/kubespray/blob/master/roles/bootstrap-os/tasks/main.yml>



Rysunek 6.1: Błąd pt. Upgrade Environment

```
3
4 #pip2 install ansible kubespary
5 get_coreos_nodes() {
6     for node in $@
7     do
8         echo -n node1[
9         echo -n ansible_host=${node},
10        echo -n bootstrap_os=coreos,
11        echo -n ansible_user=core,
12        echo -n ansible_default_ipv4.address=${node}
13        echo ]
14    done
15 }
16
17 NODES=$(get_coreos_nodes 192.168.56.{10,12,13})
18 echo NODES=${NODES[@]}
19 kubespary prepare -y --nodes ${NODES[@]}
20 cat > ~/.kubespary/bootstrap-os.yml << EOF
21 - hosts: all
22   become: yes
23   gather_facts: False
24   roles:
25     - bootstrap-os
```



```

26 EOF
27
28 (cd ~/.kubespray; ansible-playbook -i inventory/inventory.cfg
    ↪ bootstrap-os.yml)
29 kubespray deploy -y --coreos

```

Wykrzacza się na kroku czekania na uruchomienie `etcd` ponieważ oczekuje połączenia na NATowym interfejsie z adresem `10.0.3.15` zamiast host network z adresem `192.168.56.10`, stąd `ansible_default_ipv4.address`.

Według użytkowników oficjalnego Slacka `kubespray`⁵ `kubespray-cli` jest deprekowane.

6.3 kubespray

Kod znajduje się w moim repozytorium `kubernetes-cluster`⁶.

```

1  #!/usr/bin/env bash
2  cd $(dirname "$(readlink -f "$0")")
3  source ./setup-cluster-vars
4  cd ${dir}
5
6  based on https://github.com/kubernetes-incubator/kubespray/
    ↪ blob/master/docs/getting-started.md#building-your-own-inventory
7  cp -r inventory -T ${inventory}
8  python3 contrib/inventory_builder/inventory.py ${IPS[@]}
9
10 cat > ${inventory}/group_vars/all.yml << EOF
11 bootstrap_os: coreos
12 #loadbalancer_apiserver:
13 # address: 0.0.0.0
14 # port: 8080
15 kube_basic_auth: true
16 kubeconfig_localhost: true
17 kubectl_localhost: true
18 download_run_once: True
19 EOF
20

```

⁵<https://kubernetes.slack.com/messages/kubespray>

⁶<https://github.com/nazarewk/kubernetes-cluster>

```

21 ansible-playbook -i ${inventory}/inventory.cfg cluster.yml -b -
    ↪ v
22
23 echo Staring kubect1 proxy
24 echo http://localhost:8001/api/v1/namespaces/kube-system/
    ↪ services/https:kubernetes-dashboard:/proxy/#!/login
25 ./kubect1 proxy

```

6.3.1 Kubernetes Dashboard

Dostęp do Dashboardu najprościej można uzyskać:

1. nadanie wszystkich uprawnień roli `kubernetes-dashboard`⁷
2. Wejście na `http://localhost:8001/api/v1/namespaces/kube-system/services/https:kubernetes-dashboard:/proxy/#!/login`
3. Kliknięcie skip

```

1 #!/bin/sh
2 cd $(dirname "$(readlink -f "$0")")/..
3
4 bin/kubect1 create -f dashboard-admin.yml
5 xdg-open http://localhost:8001/api/v1/namespaces/kube-system/
    ↪ services/https:kubernetes-dashboard:/proxy/#!/login

```

Linki:

- <https://github.com/kubernetes/dashboard/wiki/Access-control>
- <https://github.com/kubernetes-incubator/kubespray/blob/master/docs/getting-started.md#accessing-kubernetes-dashboard>

6.3.2 Napotkane błędy

Błąd przy ustawieniu `loadbalancer_apiserver.address` na `0.0.0.0`:

```

1 TASK [kubernetes-apps/cluster_roles : Apply workaround to allow
    ↪ all nodes with cert 0=system:nodes to register]
    ↪ *****
2 Wednesday 17 January 2018  22:22:59 +0100 (0:00:00.626)
    ↪ 0:08:31.946 *****

```

⁷<https://github.com/kubernetes/dashboard/wiki/Access-control#admin-privileges>

```
3 fatal: [node2]: FAILED! => {"changed": false, "msg": "error
  ↳ running kubectl (/opt/bin/kubectl apply --force --
  ↳ filename=/etc/kubernetes/node-crb.yml) command (rc=1):
  ↳ Unable to connect to the server: http: server gave HTTP
  ↳ response to HTTPS client\n"}
4 fatal: [node1]: FAILED! => {"changed": false, "msg": "error
  ↳ running kubectl (/opt/bin/kubectl apply --force --
  ↳ filename=/etc/kubernetes/node-crb.yml) command (rc=1):
  ↳ Unable to connect to the server: http: server gave HTTP
  ↳ response to HTTPS client\n"}
```

Rozdział 7

Q&A

7.1 Czy wszystko zawsze trzeba ściągac z netu - nie mozna z lokalnego serwera?

Można zestawić lokalny rejestr Dockera¹ jako proxy cachujące².

7.2 Jak zachować stan bezdyskowego RancherOS'a?

Jedynym narzędziem do “zachowywania stanu” bezdyskowego Ranchera i praktycznie wszystkich cloudowych systemów uruchamianych bez dysku jest cloud-init.

Normalnie konfigurowany jest przez własny cloud-init, aktualnie nie zawsze działa ze względu na bugi.

7.3 Co musi zawierac cloud-config dla serwera a co dla agentow?

Sam RancherOS nie zarządza kontenerami, do tego potrzebne jest uruchomienie serwera Ranchera.

¹<https://docs.docker.com/registry/>

²<https://docs.docker.com/registry/recipes/mirror/>

Bibliografia

Pizza, Mariagrazia, Vincenzo Scarlato, Vega Masignani, Marzia Monica Giuliani, Beatrice Arico, Maurizio Comanducci, Gary T Jennings, i in. 2000. „Identification of vaccine candidates against serogroup B meningococcus by whole-genome sequencing”. *Science* 287 (5459). American Association for the Advancement of Science:1816–20.