

#zad.1

[404 Not Found \(sslip.io\)](#)

cała usługa została utworzona przy użyciu webui ranchera za wyjątkiem obrazu który został zbudowany i wrzucony do repo lokalnie

#zad.2

zainstalowano ręcznie wymagane paczki i aktywowano brakujący moduł kernela, następnie zainstalowano longhorna przy użyciu webui

```
2. Kubectl: potyczki [X] v
# Run kubectl commands inside here
# e.g. kubectl get all
kkubec> kubectl get pods -n longhorn-system
NAME                                READY   STATUS    RESTARTS   AGE
csi-attacher-5859bc989f-p5cxx       1/1     Running   0           14m
csi-attacher-5859bc989f-qdf4s       1/1     Running   1 (9m26s ago)  14m
csi-attacher-5859bc989f-v2qlv       1/1     Running   0           14m
csi-provisioner-c7ffcc5cc-n9djt     1/1     Running   1 (9m26s ago)  14m
csi-provisioner-c7ffcc5cc-p895d     1/1     Running   0           14m
csi-provisioner-c7ffcc5cc-s7mkh     1/1     Running   0           14m
csi-resizer-777857494b-r27t2       1/1     Running   1 (9m7s ago)   14m
csi-resizer-777857494b-rjfs4       1/1     Running   0           14m
csi-resizer-777857494b-tdtqm       1/1     Running   1 (9m27s ago)  14m
csi-snapshotter-64cdff5bb4-dvst4   1/1     Running   0           14m
csi-snapshotter-64cdff5bb4-mbtjx   1/1     Running   1 (9m26s ago)  14m
csi-snapshotter-64cdff5bb4-mk5f4   1/1     Running   0           14m
engine-image-ei-933d45a5-kp9ff     1/1     Running   0           14m
instance-manager-c5eb1aa090442e3cfb2cb4451545711b  1/1     Running   0           14m
longhorn-csi-plugin-mm2df          3/3     Running   0           14m
longhorn-driver-deployer-c77dd9cd6-2c4js  1/1     Running   0           15m
longhorn-manager-82lqn             1/1     Running   2 (15m ago)   15m
longhorn-ui-77ddf5bdf-gp62v       1/1     Running   0           15m
longhorn-ui-77ddf5bdf-sdxb1       1/1     Running   0           15m
> █
```

#zad. 3

dodaję repozytorium rodeo do aplikacji, without authentication

instaluję aplikację z webui

[SUSE Demo: Tetris Game \(sslip.io\)](#) tetris działa i ma się dobrze

#zad. 4

neuvectore zainstalowany z webui

autoscan włączony

#zad.5

dodano repo i włączono cykliczne skany

wynik skanowania

Repository	Image ID	Created at	OS	Size	Vulnerabilities ↓	Scan Status	Scanned at
nvbeta/node:latest	08e93041fe885bdce864...	Aug 04, 2017 22:57:18	ubuntu:14.04	410.9 MB	1294 826	Finished	Apr 08, 2024 11:40:10

nvbeta/node:latest ma najwięcej podatności

#zad. 6

Aby zachować PersistentVolume po przeskalowaniu do 0 i automatycznie podłączyć się do niego ponownie przy wznowieniu usługi, możemy wykorzystać StatefulSet zamiast Deployment. StatefulSet jest przeznaczony do zarządzania stanowymi aplikacjami, takimi jak bazy danych, które wymagają stałego identyfikatora w klastrze.

W pliku YAML (nie-usuwaj.yaml) zmieniamy rodzaj zasobu z Deployment na StatefulSet. Aby zmodyfikować używamy komendy `kubectl apply -f nie-usuwaj.yaml`

np. nie-usuwaj.yaml:

```
---
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: ubuntu-pvc
spec:
  accessModes:
    - ReadWriteOnce
  storageClassName: longhorn
  resources:
    requests:
      storage: 1Gi
---
apiVersion: apps/v1
kind: StatefulSet
```

```
metadata:

  labels:

    app: ubuntu

  name: ubuntu

spec:

  replicas: 1

  selector:

    matchLabels:

      app: ubuntu

  template:

    metadata:

      labels:

        app: ubuntu

    spec:

      volumes:

        - name: test-vol

          persistentVolumeClaim:

            claimName: ubuntu-pvc

      containers:

        - name: ubuntu

          image: busybox:latest

          command:

            - sleep

            - "86400"

          volumeMounts:

            - mountPath: /shared_files

              name: test-vol
```

```
volumes:

  - name: volv

    persistentVolumeClaim:

      claimName: longhorn-volv-pvc
```

PersistentVolume: Create

Name *

ubuntu-pvc

Description

Any text you want that better describes this resc

Volume Plugin *

Longhorn

▼

Capacity *

10

GiB

Plugin configuration

Customize

Plugin configuration

Filesystem Type

e.g. ext4

Volume Handle *

unique-handle

Read Only

☐ Yes

☒ No

Options

Key	Value	
size	2Gi	Remove
numberOfReplicas	3	Remove
staleReplicaTimeout	20	Remove

PersistentVolume: Create

Name *
ubuntu-pvc

Description
Any text you want that better describes this resou

Volume Plugin *
Longhorn

Capacity *
10
GiB

Plugin configuration
Customize

Customize

Access Modes

☒ Single Node Read-Write
☐ Many Nodes Read-Only
☐ Many Nodes Read-Write

Assign to Storage Class
longhorn

Node Selectors

Add Node Selector

Mount Options ⓘ

Add Option

podjęliśmy też próbę wykonania tego w rancherze

#zad. 7

metoda 1:

kubectl get all -n <nazwa_namespace>

np. kubectl get all -n nginx

wyberamy resource, którego konfigurację chcemy wyświetlić, u mnie replicaset.apps/nginx-deployment-7f975d9949

kubectl edit <nazwa_resource> -n <nazwa_namespace>

np. `kubectl edit replicaset.apps/nginx-deployment-7f975d9949 -n nginx`

otwiera nam się konfiguracja yaml

metoda 2:

Należy wejść w klaster->projects/namespaces->wybrać projekt, np. Project: web-server i tam kliknąć np. w nginx-> kliknąć resource, który chcemy, np. configmaps -> pod nazwą ConfigMaps będzie przycisk Download YAML, który po kliknięciu pobierze plik yaml zasobu

#zad.8

Gateway w Kubernetes to zasób, który reprezentuje instancję infrastruktury obsługującej ruch. GatewayClass opisuje klasę dostępnych bram dla użytkownika, a HTTPRoute definiuje reguły specyficzne dla protokołu do przekierowywania ruchu do usług w klastrze. Narzędzie to umożliwia dynamiczne zarządzanie infrastrukturą sieciową i trasowanie ruchu.

#zad. 9

Deployment umożliwia łatwe wdrożenie nowych wersji aplikacji, automatycznie tworząc lub usuwając pody.

Deployment obsługuje aktualizacje w trybie “rolling”, zapewniając płynne przejście między wersjami, pozwala wrócić do poprzedniego deploymentu jeśli nowy jest niestabilny

Natomiast ReplicaSet utrzymuje określoną liczbę replik podów, zapewniając dostępność określonej liczby podów, nie ma wbudowanych mechanizmów do aktualizacji wersji.

Deployment korzysta z ReplicaSet jako mechanizmu do zarządzania replikami

#zad.10

dobrą praktyką przed zaktualizowaniem klastra albo czegokolwiek jest zrobienie backupu więc wykonaliśmy snapshota

złą praktyką jest potencjalne uszkodzenie całego systemu pół godziny przed końcem czasu więc tego nie zrobiliśmy (mam nadzieję)

ale można to zrobić tutaj:

Cluster: Custom - potyczki Active

Namespace: fleet-default Age: 32 days

Making changes to cluster configuration may result in nodes reprovisioning. For more information see the [documentation](#).

Cluster Name *
potyczki

Cluster Description
Any text you want that better describes this cluster

Cluster Configuration

Basics

Member Roles

Add-On Config

Agent Environment Vars

Cluster Agent

etcd

Fleet Agent

Labels & Annotations

Networking

Registries

Upgrade Strategy

Advanced

Basics

Kubernetes Version

v1.26.13+rke2r1 (current) (deprecated)

^

v1.27.12+rke2r1 (experimental)

v1.26.15+rke2r1

v1.26.13+rke2r1 (current) (deprecated)

v1.25.16+rke2r1

Cloud Provider

Default - RKE2 Embedded

▼

Security

CIS Profile

(None)

▼

Pod Security Admission Configuration Template

Default - RKE2 Embedded

▼

☐ Project Network Isolation

System Services

☒ CoreDNS ☒ NGINX Ingress ☒ Metrics Server

Cancel

Edit as YAML

Save

#zad.11

użytkownik muhammed.yassuff z hasłem DSYoyt7AQNrT9neR (obowiązek zmiany hasła przy logowaniu)

użytkownik muhammad.yussuff z hasłem Ygo3aak1ElbuVenS (obowiązek zmiany hasła przy logowaniu)

#zad.12

kontener crashuje przy uruchamianiu

zwiększenie ilości dostępnej pamięci do 512mib eliminuje problem

#zad.13

Add group



Group Name *

nginx-group

Comment

Criteria

namespace=nginx



Add Criteria

Sample: container=myServer, namespace!=default, node=ubuntu*, image=*nginx*, address=216.58.194.0/24, address=0.0.0.0/0, address=0.0.0.0-255.255.255.255, address=*.neuvector.com, container~k8s_zoo[12] or key=value for label ("=" exactly match, "!" not, "?" and "*" wildcards, "~" regex)

Cancel

Add

Edit rule



ID

1000000

Comment

save_logs_when_nginx_gets_packets

From *

*

To *

nginx-group

Applications

Syslog



Add Applications

Ports

Action



Status



Cancel

Update

jeśli dobrze rozumiem nie ma blokować tych pakietów i powinny się zapisywać logi, gdy coś przyjdzie do nginx

The 'Edit rule' dialog box contains the following fields and controls:

- ID:** 8
- Security Event:** A dropdown menu.
- Group:** nginx-group
- Comment:** webhook for nginx-group
- Add Criteria:** A section with a sample text: "Sample: level:Critical, name:Container.Suspicious.Process".
- Action*:** Three checkboxes: ☒ Webhook, ☐ Suppress Log, and ☐ Quarantine.
- Status*:** A toggle switch labeled "Enabled".
- Buttons:** "Cancel" and "Update".

The 'Edit Vulnerability Profile Entry' dialog box contains the following fields and controls:

- Vulnerability Name:** nginx-vun (with a sample: CVE-2021-4534, CVE-2021-* or *).
- Vulnerability Reported Within:** A radio button and a text field for "Day(s)".
- Vulnerability Reported Within:** A radio button and a text field for "Day(s) without Fix".
- Comment:** A text input field.
- Images:** A section with a label "Type and Press Enter", a text input "Add Images", and a sample: "nginx:1.23,*node*:latest".
- Namespaces:** A section with a label "Type and Press Enter", a text input "Add Namespaces ...", a dropdown menu showing "nginx", and a sample: "default,*kafka*".
- Buttons:** "Cancel" and "Update".

vulnerabilities wyświetlą się w Security Risks->Vulnerabilities

Analiza pakietów to proces monitorowania, przechwytywania i badania ruchu sieciowego w celu zrozumienia, diagnozowania i rozwiązywania problemów związanych z siecią. Narzędzia do analizy pakietów pozwalają na szczegółowe badanie pojedynczych pakietów, identyfikację anomalii, wykrywanie ataków oraz optymalizację wydajności sieci. Możemy do tego użyć np. Wireshark

#zad. 14

kubectl create namespace adrian

adrian nie przypisał limitów zasobów oraz dodał healthchecki które nie przechodzą i zabijają kontener

możliwa naprawa to wyłączenie healthchecków lub zmienienie konfiguracji nginxa żeby przechodziły

my wyłączyliśmy healthchecki

#zad. 15

Add group

×

Group Name *

nginx-group

Comment

Criteria

namespace=nginx

×

Add Criteria

Sample: container=myServer, namespace!=default, node=ubuntu*, image=*nginx*, address=216.58.194.0/24, address=0.0.0.0/0, address=0.0.0.0-255.255.255.255, address=*.neuvector.com, container~k8s_zoo[12] or key=value for label ("=" exactly match, "!" not, "?" and "*" wildcards, "~" regex)

Cancel

Add

Add rule

Comment

blokowanie_polaczen_wychodzacych_z_nginx

From *

nginx-group

To *

external

Applications

Ports

Action

Cancel

Add

Edit rule

Type

Deny

Comment

Criterion*

Operator*

Namespace is one of [nginx]

Criteria

Mode

Use Global Mode

Monitor

Protect

Status

Enabled

Cancel

Update

zadanie 17

do pliku yml zakradł się błąd w linii 21. zmiana `MYSQL_ROT_PASSWORD` na `MYSQL_ROOT_PASSWORD` pozwala na uruchomienie poda

zadanie 18

adrian korzystał z repozytorium nieposiadającego obrazu dla architektury x86_64

zmiana repozytorium na poprawne powoduje uruchomienie się kontenera i wyświetlenie wiadomości w logach

```
Mon, Apr 8 2024 12:20:08 pm
2024-04-08T12:20:08.742824068+02:00 Hello from Docker!
2024-04-08T12:20:08.742832553+02:00 This message shows that your installation appears to be working correctly.
2024-04-08T12:20:08.742837188+02:00
2024-04-08T12:20:08.742840824+02:00 To generate this message, Docker took the following steps:
2024-04-08T12:20:08.742844324+02:00 1. The Docker client contacted the Docker daemon.
2024-04-08T12:20:08.742847879+02:00 2. The Docker daemon pulled the "hello-world" image from the Docker Hub.
2024-04-08T12:20:08.742851658+02:00    (amd64)
2024-04-08T12:20:08.742855499+02:00 3. The Docker daemon created a new container from that image which runs the
2024-04-08T12:20:08.742859039+02:00    executable that produces the output you are currently reading.
2024-04-08T12:20:08.742862573+02:00 4. The Docker daemon streamed that output to the Docker client, which sent it
2024-04-08T12:20:08.742866042+02:00    to your terminal.
2024-04-08T12:20:08.742869297+02:00
2024-04-08T12:20:08.742873296+02:00 To try something more ambitious, you can run an Ubuntu container with:
2024-04-08T12:20:08.742876819+02:00 $ docker run -it ubuntu bash
2024-04-08T12:20:08.742880144+02:00
2024-04-08T12:20:08.742883964+02:00 Share images, automate workflows, and more with a free Docker ID:
2024-04-08T12:20:08.742887431+02:00 https://hub.docker.com/
2024-04-08T12:20:08.742890702+02:00
2024-04-08T12:20:08.742894318+02:00 For more examples and ideas, visit:
2024-04-08T12:20:08.742901689+02:00 https://docs.docker.com/get-started/
2024-04-08T12:20:08.742905051+02:00
```